



Information Assurance Branch

Security+ Review Course

*Version 3.51*

## Overview

The skills and knowledge measured by the CompTIA Security+ examination were derived and validated through input from a committee and over 1,000 subject matter experts representative of industry. A job task analysis (JTA), global survey, beta examination and beta results review were each milestones in the development process. The results of these milestones were used in weighing the domains and ensuring that the weighting assigned to each domain is representative of the relative importance of the content.

The CompTIA Security+ certification is an internationally recognized validation of the technical knowledge required of foundation-level security practitioners. A CompTIA Security+ certified individual has successfully proven holding a foundation-level of skill and knowledge in General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography and Operational / Organizational Security. Candidates are recommended to have two years experience in a networking role with preexisting knowledge of TCP/IP, experience in a security related role, CompTIA Network+ or equivalent certification, and adequate training and self-study materials. All candidates are encouraged to review the CompTIA Security+ objectives thoroughly prior to attempting the exam. This examination includes blueprint weighting, test objectives and example content. Example concepts are included to clarify the test objectives and should not be construed as a comprehensive listing of the content of the examination.

The table below lists the domains measured by this examination and the extent to which they are represented in the examination. CompTIA Security+ (2011 Edition) exams are based on these objectives.

### **CompTIA Security+ Certification Domains % of Exam\***

Network Security, 21%  
Compliance and Operational Security, 18%  
Threats and Vulnerabilities, 21%  
Application, Data, and Host Security, 16%  
Access Control and Identity Management, 13%  
Cryptography, 11%

\* All percentages are approximate and are subject to change.

*CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.*

## Table of Contents

<b>Domain 1 - Cryptography</b> .....	<b>6</b>
Domain Objectives .....	6
General Concepts .....	6
Hashing .....	13
Common Hashing Functions .....	14
Attacks on Hashing Algorithms (Hash Collision) .....	15
Symmetric Cryptography .....	18
Asymmetric Cryptography .....	22
Public Key Encryption .....	22
Hybrid Cryptosystem .....	26
Protecting Web Communications .....	28
Email Security Concepts .....	30
Certificate Management .....	31
Key Management .....	38
<b>Domain 2 – Network Security</b> .....	<b>42</b>
Review of OSI and TCP/IP Models .....	42
Open Systems Interconnect (OSI Model) .....	42
Implement and use of common ports and protocols .....	44
TCP/IP Addressing .....	47
Common Transport Protocols .....	55
Transmission Media .....	58
Network Security Tools .....	77
Wireless Networking .....	80
Analyze and differentiate among types of wireless attacks .....	86
Wireless Vulnerabilities .....	86
Wireless Vulnerabilities Mitigations .....	90
<b>Domain 3 – Access Control and Identity Management</b> .....	<b>93</b>
Explain the fundamental concepts and best practices related to authentication, authorization and access control .....	93
Identification vs. Authentication .....	93
Directory Services .....	100
Common Access Control Models .....	104
Logical Access Control Methods .....	105
Trusted OS .....	108

<b>Domain 4 Threats and Vulnerabilities .....</b>	<b>110</b>
A Security+ candidate is expected to: .....	110
Analyze and differentiate among types of malware.....	110
Malicious Code.....	110
Denial of Service (DoS) .....	114
Distributed Denial of Service (DDoS) .....	117
Analyze and differentiate among types of Network attacks.....	120
Man-in-the-Middle Attacks.....	120
Malicious Internal/Insider Threats .....	124
Analyze and differentiate among types of social engineering attacks .....	126
Social Engineering.....	126
Analyze and differentiate among types of application attacks.....	128
Buffer Overflows.....	128
Analyze and differentiate among types of mitigation and deterrent techniques .....	135
Manual bypassing of electronic controls: .....	135
Physical Access Security.....	137
Implement assessment tools and techniques to discover security threats and vulnerabilities .....	140
<b>Domain 5 – Compliance and Operational Security.....</b>	<b>148</b>
Domain Objectives .....	148
Risk Related Concepts.....	148
Policies Used for Reducing Risk .....	150
Risk Management .....	152
Incident Response Procedures .....	153
Basic Forensic Procedures .....	155
The Importance of Security Related Awareness and Training .....	157
Disaster Recovery Procedures .....	159
Business Continuity Planning (BCP) .....	159
Impact and Proper Use of Environmental Controls .....	160
Execute Disaster Recovery Plans and Procedures.....	164
Disaster Recovery Planning (DRP).....	164
<b>Domain 6 – Application, Data, and Host Security.....</b>	<b>173</b>
Explain the Importance of Application Security .....	173
Carry out appropriate procedures to establish host security .....	181
Importance of Data Security.....	183

**Appendix A – Practical Exercises ..... 186**  
**Appendix B – Ports and Protocols ..... 196**  
**Appendix D – Algorithms ..... 197**  
**Appendix E – Glossary ..... 198**  
**Appendix F – Acronyms ..... 231**  
**Appendix G – Resources ..... 235**  
**Appendix H – Domain Review Questions ..... 238**  
**References ..... 258**

# Domain 1 - Cryptography

## Domain Objectives

A Security+ candidate is expected to:

- Explain general cryptography concepts
- Explain basic hashing concepts and map various algorithms to appropriate applications
- Explain basic encryption concepts and map various algorithms to appropriate applications
- Explain and implement protocols
- Explain core concepts of public key cryptography
- Implement PKI and certificate management

---

## General Concepts

**Cryptography has 4 primary functions:**

1. **Confidentiality**-Confidentiality by ensuring only authorized parties can access data. Encryption is used to protect information from unauthorized individuals.
2. **Integrity**-Integrity by verifying that data has not been altered in transit. Hashing algorithms are used to ensure information has not been modified in transit and on the hard drive.
3. **Authentication**-Process of verifying that the sender is who they say they are. The use of Digital Signing validates the sender's authentication.
4. **Non-repudiation**-Prevents one party from denying actions they carried out. A combination of integrity and authentication, (Provided via Session ID's, Digital Signatures, Biometric devices, etc.)

---

**Terms to know:**

**Cryptography:** The process of converting readable text into unreadable series of characters and symbols.

**Cryptanalysis:** The study and practice of finding weaknesses in ciphers (finding faster alternatives than brute force).

**Algorithm:** The series of steps/processes/formulas that are followed to arrive at a result.

**Cipher:** A method used to encode characters to hide their value

**Plain text or clear text:** Information which is transferred or stored without cryptographic protection.

**Cipher text:** The result of encryption performed on plaintext using an algorithm.

### Substitution Cipher

Type of coding or ciphering system that changes one character or symbol into another

Example: Caesar's shift cipher

Plain text: Security is never convenient

Cipher: VHFXULWB LV QHYHU FRQYHQLHQW

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Substitution code is defined as substitution at the level of words or phrases

- Example: The Navajo code

Actual word	Code word	Navajo translation
Bombs	Eggs	<i>A-ye-shi</i>
Amphibious Vehicle	Frog	<i>Chal</i>
Battleship	Whale	<i>Lo-tso</i>
Destroyer	Shark	<i>Ca-lo</i>
Submarine	Iron fish	<i>Besh-lo</i>

### Transposition

Changing the positions of plaintext letters with in a sentence is a form of transposition encryption.

- Example:
 

meet me at noon	Plaintext
noontaemteem	Cipher text

A transposition cipher (also referred to as a transposition code) involves transposing or scrambling the letters in a certain manner. Typically, a message is broken into blocks of equal size, and each block is then scrambled

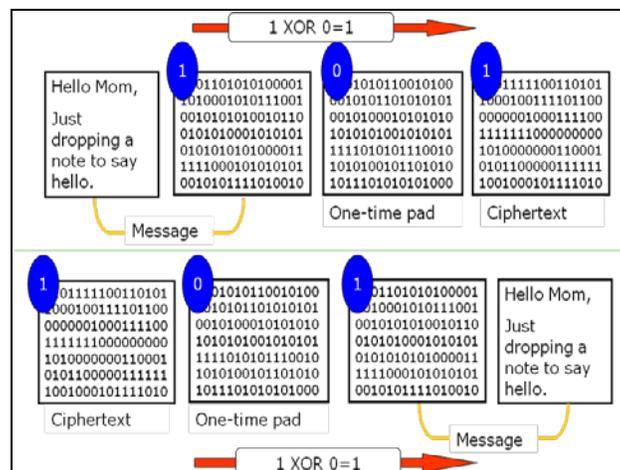
### Exclusive-OR (XOR) Operation

- Binary mathematical operation which compares two bits to produce an output
- Plaintext is XORed with a random keystream to generate ciphertext
  - If values are same, result is 0
  - If values are different, result is 1

Converted Plaintext	0101 0001
Keystream	<u>0111 0011</u>
Output of XOR	0010 0010

### One-Time Pad

- **Considered unbreakable**  
 A one-time pad (OTP) is a type of encryption, which has been proven to be impossible to crack if used correctly.
- Each pad in the scheme must meet the following requirements:
  - **Made up of truly random values and used only once**  
 If the key is truly random, as large as or greater than the plaintext, never reused in whole or part, and kept secret, the ciphertext will be impossible to decrypt or break without knowing the key.
  - **Must be at least as long as the message**  
 Each bit or character from the plaintext is encrypted by a modular addition with a bit or character from a secret random key (or pad) of the same length as the plaintext, resulting in a ciphertext.
  - **Securely distributed to destination and protected at sender's and receiver's sites**  
 It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys.



### Cons of a One-Time-Pad

- **Each pair of entities in the communication must receive it in a secure fashion.**
- **Requires more overhead than it is worth.**

However, practical problems have prevented one-time pads from being widely used.

The theoretical perfect security of the one-time-pad applies only in a theoretically perfect setting; no real-world implementation of any cryptosystem can provide perfect security because practical considerations introduce potential vulnerabilities.

These practical considerations of security and convenience have meant that the one-time-pad is, in practice, little-used. Implementation difficulties have led to one-time pad systems being broken, and are so serious that they have prevented the one-time pad from being adopted as a widespread tool in information security.

- **The sender and receiver must be perfectly synchronized with each other's pad.**
- 

### Frequency Analysis

In cryptanalysis, **frequency analysis** is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.

Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language.

---

### Initialization Vectors

- Random values used with algorithms to ensure patterns are not created during the encryption process
- Used with both stream and block keys
- Are not encrypted when being sent to the destination
- If Initialization Vectors are not used, an attacker can break the encryption key (keyspace) because of patterns resulting from the encryption process

Randomization is crucial for encryption schemes to achieve security and to prevent repetition in the encryption process. IV's are used in both stream and block ciphers and they are also referred to as a nonce. WEP utilizes IV's but they can be a short, 24-bit IV. This can lead to reused IVs with the same key, which can lead to it being easily cracked.

---

**Steganography** (also called electronic watermarking)

- The Greek word steganos means “covered, or hidden”; graphein, “to write”
- Process of hiding one’s message in another in order to prevent it from being detected
- Examples
  - **Graphics –**
    - By removing all but the last 2 bits of each color (red, green, blue) component (pixel) in a graphic this way the color difference undetectable to the human eye. By combining all of the last 2 bits from each pixel, the hidden message or graphic is revealed.
  - **Sound files-**
    - Old Way: Playing a record backwards on a record player would reveal a hidden message.
    - New Way: In an MP3 steganographic file system, Audio steganography is similar to the process of modifying the Least Significant Bit of image files. By modifying the LSB of several bits of an audio file, only minor changes occur in the sound, most of which can't be differentiated by the human ear.
    - Audio stego can also be done by using frequencies that cannot be heard by the human ear.

In theory, doing steganography prevents analysts (steganoanalysis) from detecting the real message. You could encode your message in another file or message and use that file to hide your message. This type of encryption can be somewhat harder to detect, but it’s still breakable.

---

**Alternate Data Streams (ADS)**

- Provides hackers with a method of hiding tools on a breached system and executing them without being detected
- Allow for compatibility with the Macintosh Hierarchical File System
- used legitimately by a variety of programs
- ADS executable appear to run as the original file, undetectable to process viewers like Windows Task Manager
- Not only possible to hide a file, but to also hide the execution of an illegitimate process
- Example:
  - Create a document behind a text file:  
C:\notepad.exe mike.txt:mikehidden.txt (you will be asked to create the file if it don't exist. If the file exists then it will open the hidden file.)
  - Copy a program behind another program:  
Start C:\adstest>Type c:\windows\system32\notepad.exe>  
calc.exe:notepad.exe
  - Run the hidden program:  
C:\adstest> Start c:\adstest\calc.exe:notepad.exe

A compatibility feature of NTFS, ADS is the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer. Found in all version of NTFS, ADS capabilities were originally conceived to allow for compatibility with the Macintosh Hierarchical File System, HFS; where file information is sometimes forked into separate resources. Alternate Data Streams have come to be used legitimately by a variety of programs, including native Windows operating system to store file information such as attributes and temporary storage.

Once injected, the ADS can be executed by using traditional commands like type, or start or be scripted inside typical scripting languages like VB or Perl. When launched, the ADS executable will appear to run as the original file - looking undetectable to process viewers like Windows Task Manager. Using this method, it is not only possible to hide a file, but to also hide the execution of an illegitimate process.

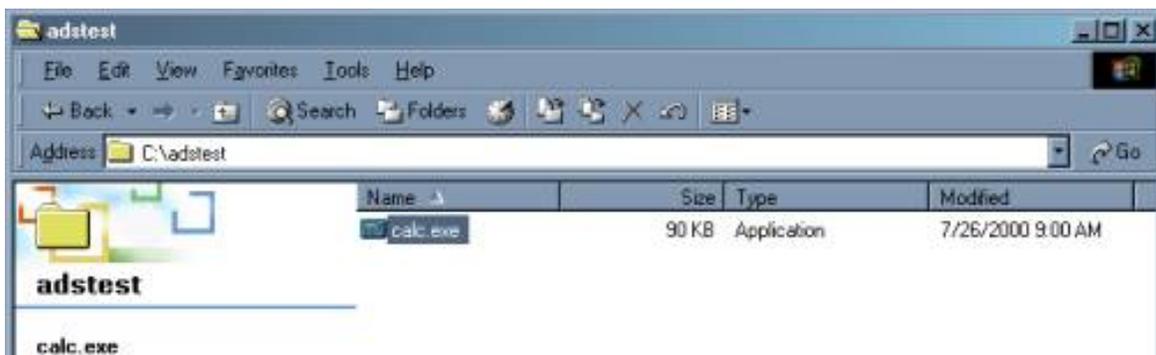


Figure 1

Figure1 shows the executable file for the standard windows program calculator, calc.exe. The original size of 90KB and a date modified time stamp of 7/26/2000.

```

Directory of C:\adstest
02/14/2004 04:47p <DIR> .
02/14/2004 04:47p <DIR> ..
07/26/2000 09:00a          91,408 calc.exe
                1 File(s)          91,408 bytes
                2 Dir(s)        684,425,216 bytes free

C:\adstest>type c:\winnt\system32\notepad.exe>calc.exe:notepad.exe

C:\adstest>dir
Volume in drive C has no label.
Volume Serial Number is 8C3F-115B

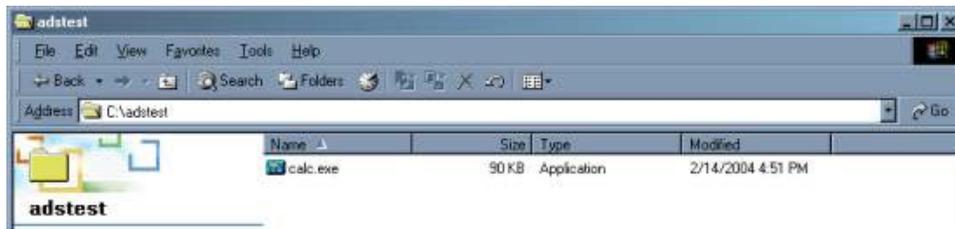
Directory of C:\adstest
02/14/2004 04:47p <DIR> .
02/14/2004 04:47p <DIR> ..
02/14/2004 04:51p          91,408 calc.exe
                1 File(s)          91,408 bytes
                2 Dir(s)        684,371,968 bytes free

C:\adstest>

```

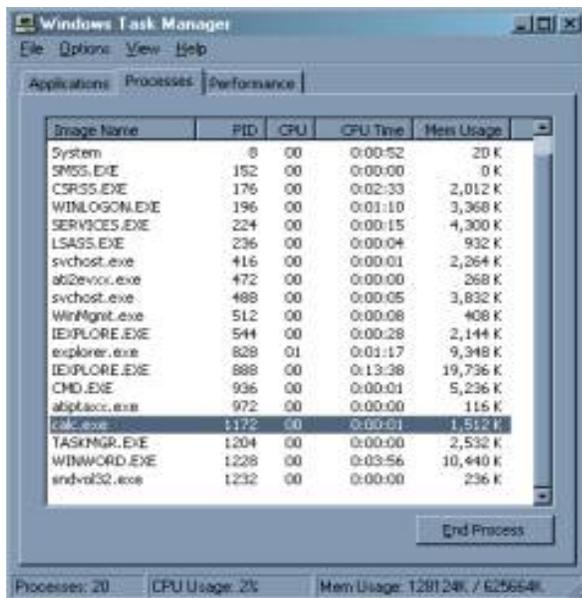
Figure 2

Figure 2 show the commands used to append an alternate data stream to calc.exe with another standard windows program, notepad.exe.



**Figure 3**

Figure 3 shows that while notepad.exe is 50KB, the file size of calc.exe has not changed from the original 90KB. But notice that the date modified time stamp has changed.



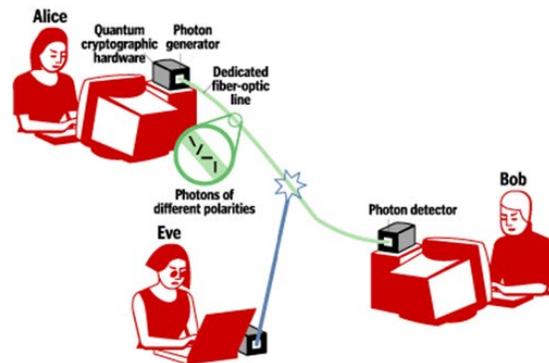
**Figure 4**

Figure 4 Execution of the new ADS notepad.exe using the standard command start. On the desktop, the program notepad is executed however; an examination of the Windows Task Manager shows the original file name calc.exe. (Figure 5).

**Figure 5**

### Quantum Cryptography

- Based on the Heisenberg Uncertainty Principle
- In the process of measuring results, the results have changed
- If photons are intercepted, some photons will change polarity
- Currently only implemented using fiber-optic technology
- Best-known application of quantum cryptography is quantum key distribution



In quantum cryptography, a message is sent using a series of photons. If the receiver knows the sequence and polarity of the photons, they can decode the message. Otherwise, the photons look like random noise. If someone intercepts the photons, some of the photon positions will change polarity and the message will be altered.

Quantum cryptography has become a solution available for private users, although it's very expensive and has a limited range.

---

## Hashing

- Algorithm that takes a variable-length input and generates a fixed-length output
- The algorithm is public
- One-way encryption function
- Ensures data integrity
- Used to create checksums or message digests

Mathematical cryptography deals with using mathematical processes on characters or messages. The most common is a function called hashing. Hashing refers to performing a calculation on a message and converting it into a numeric hash value.

Many password-generation systems are based on a **one-way hashing** (encryption) approach. You can't take the hash value and reverse it to guess the password. In theory, this makes it harder to guess or decrypt a password.

The hash **ensures data integrity** (i.e. the data has not been altered). The receiving device computes a checksum and compares it to the **checksum** included with the file. If they do not match, the data has been altered.

A good hash function should not produce the same hash value from two different inputs. This is known as a **collision**. A collision occurs when two different inputs produce the same hash output.

---

## Common Hashing Functions

Name	Hash Length
MD5	Digest size: <b>128 bits</b>
SHA-1,	Digest size: <b>160 bits</b>
SHA-2 SHA-224/256	Digest sizes: <b>224, 256 bits</b>
SHA-2 SHA-384/512	Digest size: <b>512 bits</b>
RIPEMD-160	Digest sizes: <b>128,160, 256, and 320 bits</b>
HAVAL	Digest sizes: <b>128 bits, 160 bits, 192 bits, 224 bits, and 256 bits</b>
Whirlpool	Digest size: <b>512 bits</b>

### Hashing - MD5 Example

The following demonstrates a 43-byte ASCII input and the corresponding MD5 hash:

**MD5 ("The quick brown fox jumps over the lazy dog") =**

**9e107d9d372bb6826bd81d3542a419d6**

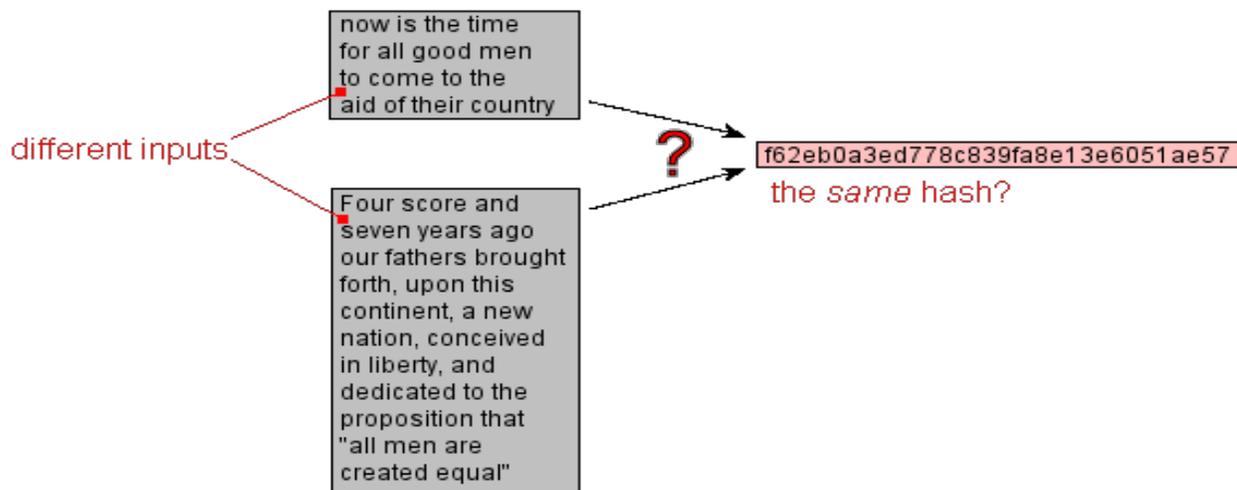
Even a small change in the message will result in a completely different hash, due to the avalanche effect. See what happens when d gets changed to e:

**MD5 ("The quick brown fox jumps over the lazy eog") =**

**ffd93f16876049265fbaef4da268dd0e**

---

## Attacks on Hashing Algorithms (Hash Collision)



**Brute Force Attacks:** Accomplished by applying every possible combination of characters that could be the key. Time is a factor.

**Dictionary Attack:** Uses a dictionary of common words to reveal the user's password.

**Rainbow Table (Rainbow Crack):** A rainbow table is a lookup table used to recover an unknown password using its known cryptographic hash, making attacks against hashed passwords feasible. It allows recovering the plaintext password from a "password hash" generated by a hash function.

**Birthday Attack:** Built on the premise that if 23 people are in a room, there is some probability that 2 people will have the same birthday. Probability increases as more people enter the room. If your key is hashed, the possibility is that given enough time, another value can be created that will give the same hash value.

Birthday attacks are often used to find collisions of hash functions. To avoid this attack, the output length of the hash function used for a signature scheme can be chosen large enough so that the birthday attack becomes computationally infeasible.

**Countermeasure for hashing attacks:**

**SALT:** A randomly generated value that is calculated into the hashing process which adds more complexity and makes it harder to conduct Rainbow Table and Collision attacks.

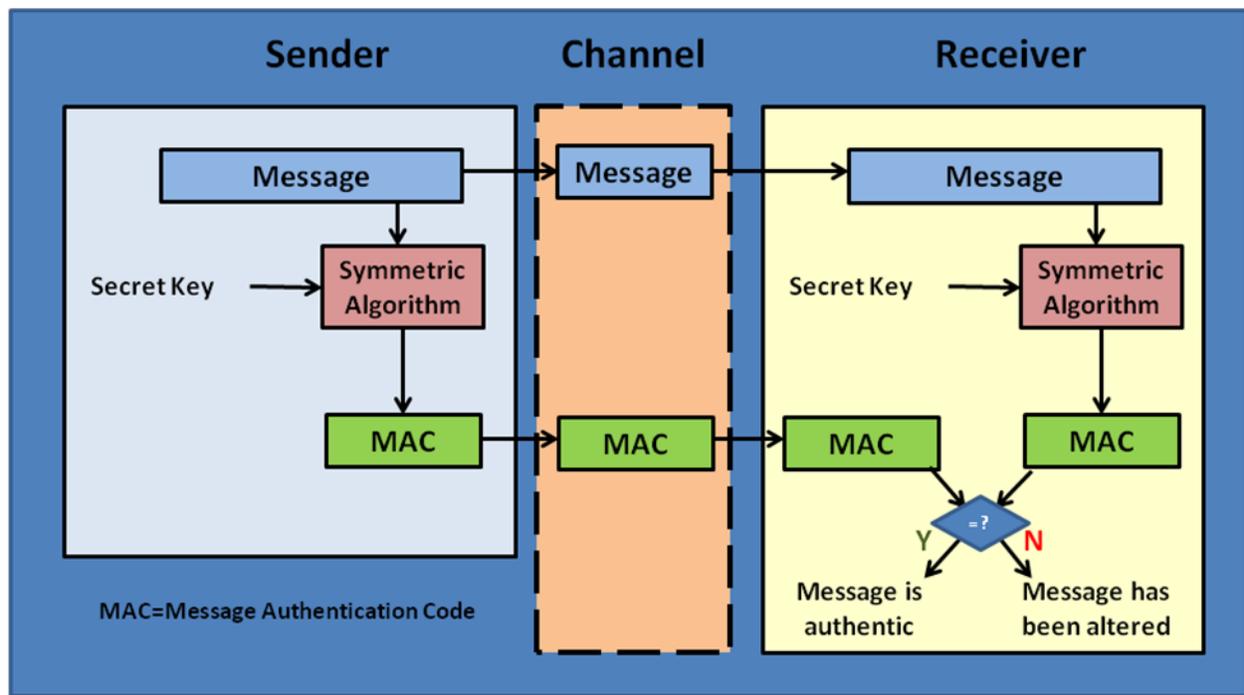
## Message Authentication Code (MAC)

- Used to verify integrity and data origin
- Value generated by running a message through a symmetric key (DES) only
- Recipient creates a MAC using the same secret key and compares it to the MAC received
- Requires the sender and the receiver to share a secret key

The purpose of a MAC is to authenticate both the source of a message and its integrity **without the use of any additional mechanisms**. Different than digital signatures,

MACs are **computed and verified with the same secret key**, so that they can only be verified by the intended recipient.

MAC values resulting from running it through DES can be 16 or 64 bits in length.

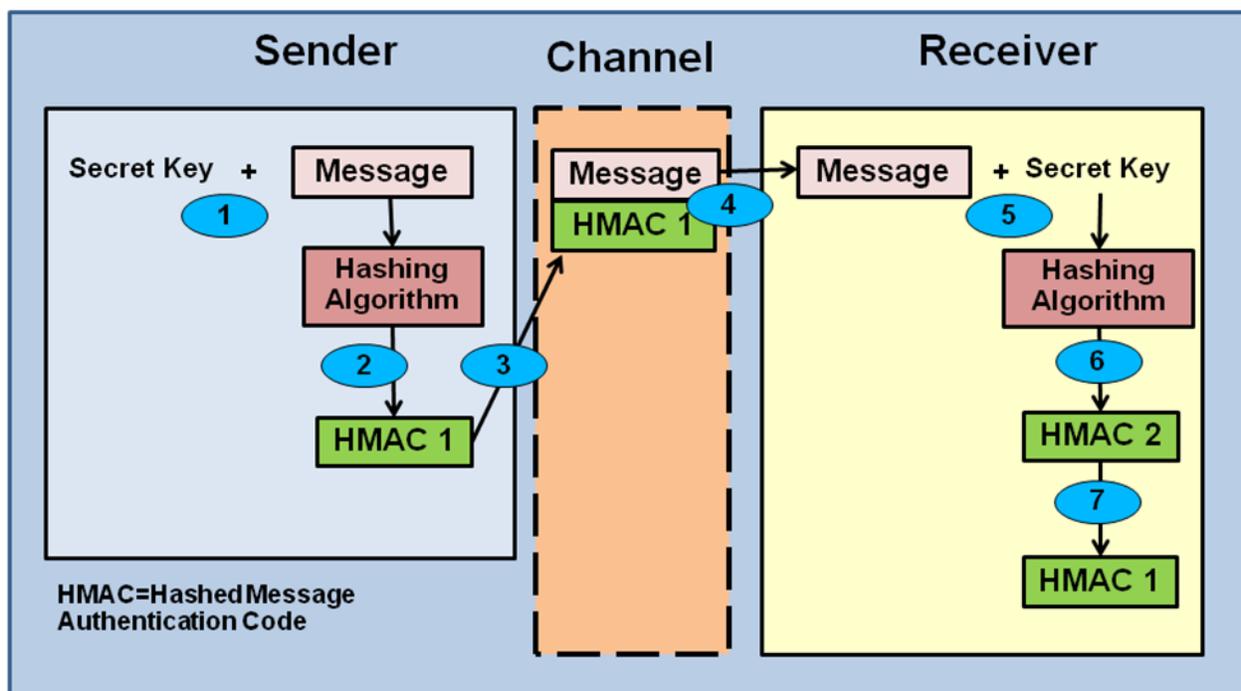


## Hashed MAC (HMAC)

Type of MAC calculated using a hash function (MD5 or SHA-1) and a symmetric key

- The shared symmetric key is appended to the data to be hashed
- Creates a more rapid message digest (MAC uses DES, which is slow)
- Used in Internet Protocols such as IPSec, SSL/TLS, and SSH

HMAC is a type of message authentication code (MAC) calculated **using a specific algorithm** involving a **cryptographic hash function in combination with a secret key**. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed **HMAC-MD5** or **HMAC-SHA-1** accordingly.



1. The sender concatenates a key with the message
2. The result is put through a hashing algorithm and generates MAC1 value
3. The MAC1 value is appended to the message
4. The sender sends the message to the receiver (not the key)
5. The receiver concatenates a key with the message
6. The result is put through a hashing algorithm and generates MAC2 value
7. The result of MAC2 is compared with MAC1. If equal then data integrity is proved.

## Symmetric Cryptography

- Uses one key to encrypt and decrypt the information
- Both parties share the same key
- Best suited for bulk encryption; much faster (smaller key size) than asymmetric cryptography
- a.k.a. Secret Key, Private Key, Shared Key, Same Key, Single Key, Session Key

Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a key that must be protected. A symmetric key sometimes referred to as a secret key or private key is a key that isn't disclosed to people who aren't authorized to use the encryption system. The disclosure of a private key breaches the security of the encryption system. If a key is lost or stolen, the entire process is breached.

---

## Symmetric Encryption Methods

### Stream Cipher

- Data encrypted bit-by-bit (or byte-by-byte)
- Plaintext mixed with a keystream controlled by a key
- Usually implemented in hardware
- Requires no memory
- Data is encrypted on-the-fly
- A very fast mathematical operation

A stream cipher is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time. Stream ciphers are often used for their speed and simplicity of implementation in hardware, and in applications where plaintext comes in quantities of unknowable length—for example, a secure wireless connection

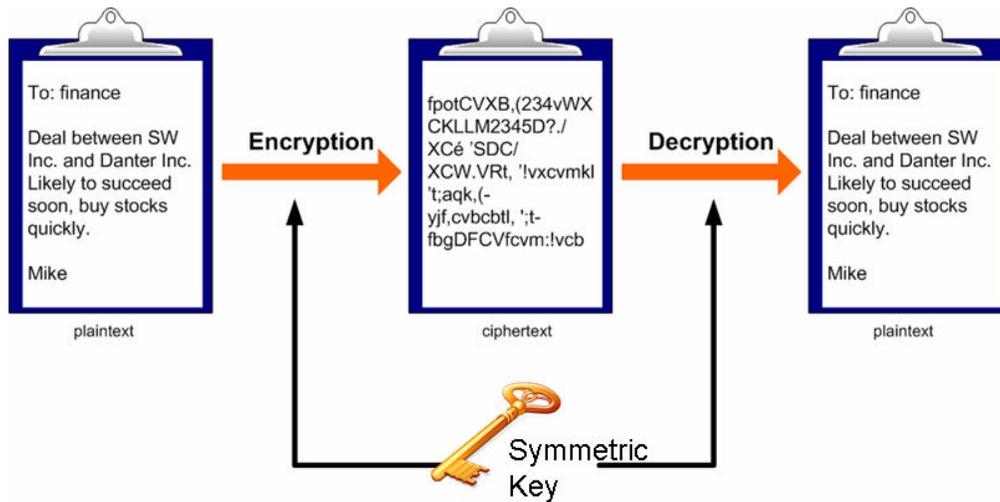
---

### Block Cipher

- Usually implemented in software
- Transforms fixed-length blocks of plaintext into cipher text of the same length
- Data is encrypted block-by-block
- Uses substitution and transposition ciphers
- Stronger than stream-based ciphers
- Slow and resource intensive

A block cipher is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group, rather than to one bit at a time.

## Symmetric Key Encryption



### Advantages:

- Less computationally intensive
- Produces a smaller file size
- Allows for faster transmissions

### Disadvantages

- Exchanging of the shared secret key: Key distribution (getting the keys to all parties securely)
- Trust between parties sharing the key
- Key Management: In order to ensure secure communications between everyone in a population of people (n), a total of  $n(n-1)/2$  keys are needed.
- No “non-repudiation” offered with symmetric key encryption.

## Symmetric Key Algorithms

<b>DES</b> <b>(Data Encryption Standard)</b>	<ul style="list-style-type: none"> <li>• Based on IBM's Lucifer algorithm</li> <li>• 64-bit block (56-bit key + 8 bits for parity)</li> <li>• Algorithm: DEA (Data Encryption Algorithm)</li> <li>• Easily broken</li> </ul>
<b>3DES</b> <b>(Triple-DES)</b>	<ul style="list-style-type: none"> <li>• Upgrade of DES (still in use)</li> <li>• Applies DES three times</li> <li>• 168-bit key (+24 for parity)</li> </ul>
<b>AES</b> <b>(Advanced Encryption Standard)</b>	<ul style="list-style-type: none"> <li>• Current standard (replaced DES)</li> <li>• 128 bit block</li> <li>• Algorithm: Rijndael</li> <li>• Key sizes: 128, 192, and 256 bits</li> </ul> <p>Block sizes of 128, 160, 192, 224, and 256 bits are supported by the</p>

	<p>Rijndael algorithm, but only the 128-bit block size is specified in the AES standard.</p> <p><i>Source: FIPS 197 publication (<a href="http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf">http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf</a>, page 9)</i></p>
<b>Blowfish</b>	<ul style="list-style-type: none"> <li>• “Fastest of the symmetric algorithms”</li> <li>• 64-bit block cipher</li> <li>• Variable-length keys (32 to 448-bits)</li> </ul>
<b>Twofish</b>	<ul style="list-style-type: none"> <li>• 128-bit block cipher</li> <li>• Variable-length keys (128, 192, or 256-bits)</li> <li>• Finalist for AES</li> </ul>
<b>CAST</b>	<ul style="list-style-type: none"> <li>• Developed in 1996, by Carlisle Adams and Stafford Tavares</li> <li>• CAST-128 <ul style="list-style-type: none"> <li>○ 64-bit block size</li> <li>○ Variable key lengths (40 to 128-bits)</li> </ul> </li> <li>• CAST-256 <ul style="list-style-type: none"> <li>○ 128-bit block size</li> <li>○ Variable key lengths (128, 160, 192, 224, 256-bits)</li> </ul> </li> <li>• Used by Pretty Good Privacy (PGP)</li> </ul>
<b>Rivest Cipher (Ron’s Code or RC)</b>	<ul style="list-style-type: none"> <li>• RC4 (stream): Variable key length (0 to 2048 bits)</li> <li>• RC5 (block): Variable block (32, 64, 128-bits) <ul style="list-style-type: none"> <li>○ Variable key length (0 to 2048)</li> </ul> </li> <li>• RC6 (block): Variable block (128-bits) <ul style="list-style-type: none"> <li>○ Variable key length (0 to 2048)</li> </ul> </li> </ul>
<b>IDEA (International Data Encryption Algorithm)</b>	<ul style="list-style-type: none"> <li>• 64-bit block cipher</li> <li>• 128-bit key length</li> <li>• Developed by the Swiss</li> <li>• Used in PGP and other encryption software</li> </ul>
<b>Skipjack</b>	<ul style="list-style-type: none"> <li>• A <b>block cipher algorithm</b> developed by the U.S. <b>National Security Agency (NSA)</b>. Initially classified, it was originally intended for use in the controversial <b>Clipper chip</b>.</li> <li>• The heart of this concept was key escrow. In the factory, any new telephone or other device with a Clipper chip would be given a "cryptographic key", that would then be provided to the government in "escrow". If government agencies "established their authority" to listen to a communication, then the key would be given to those government agencies, who could then decrypt all data transmitted.</li> </ul>
<b>SAFER (Secure And Fast Encryption Routine)</b>	<ul style="list-style-type: none"> <li>• Used in <b>Bluetooth</b> for key derivation, not for encryption</li> <li>• SAFER+ <ul style="list-style-type: none"> <li>○ Secure and Fast Encryption Routine</li> <li>○ 128-bit block cipher</li> </ul> </li> <li>• SAFER++</li> <li>• 64 and 128-bit block cipher</li> </ul>

---

## Comparative Strengths of Symmetric Key Algorithms

- 40-bit encryption yields about 1 trillion possible results
- 128-bit encryption yields:  
340,282,366,920,938,463,463,374,607,431,768,211,456 possible results

Key Length (bits)	1995	2000	2005
40	68 seconds	8.6 seconds	1.07 seconds
56	7.4 weeks	6.5 days	19 hours
64	36.7 years	4.6 years	6.9 months
128	6.7e17 millennia	8.4e16 millennia	1.1e16 millennia

---

### Whole Disk Encryption (Full disk encryption)

- Software or hardware which encrypts every bit of data on a disk or disk volume
  - Some software can leave the Master Boot Record (MBR) unencrypted
  - Some hardware-based encryption systems encrypt the entire boot disk, including the MBR(TPM)
  - AES algorithm primarily used
- 

#### Software:

- PGP Whole Disk Encryption (Windows and MAC-OS X)
- Bitlocker
- Check Point Endpoint Security Full Disk Encryption

#### Hardware based:

- Can use small symmetric keys (40 bits) which can make this technology susceptible to Brute Force attacks. However the latest disk encryption hardware uses 256 bit keys.
- The key is stored in hardware-based encryption within the storage device, or hardware-based elsewhere (such as CPU or host bus adaptor).

## Asymmetric Cryptography

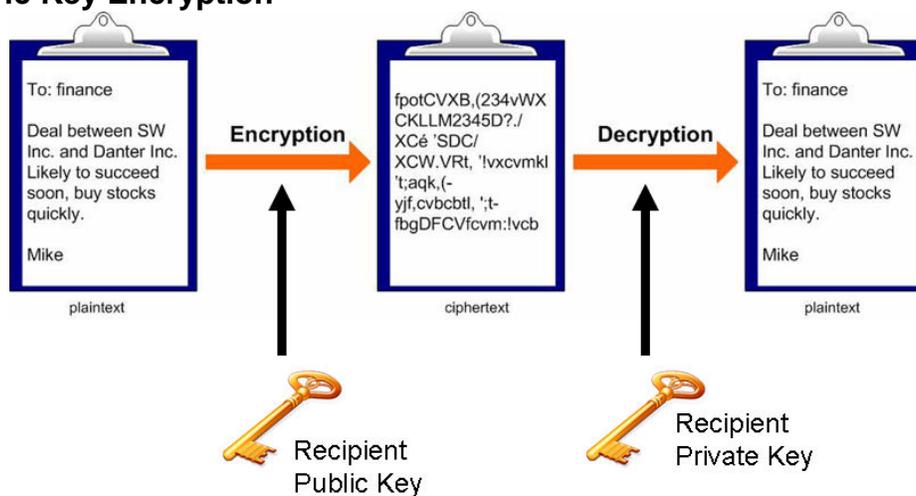
### Public Key Encryption

- Based on mathematical number theory
- Each user has two keys: Public/Private
  - Public key is available to everyone
  - Private key is kept secret
- Both keys are mathematically related
  - Considered a key pair
  - Whatever is encrypted with one key, can only be decrypted with the other

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The public key can be used by the sender to encrypt a message, and the private key can be used by the receiver to decrypt the message.

The public key may be truly public or it may be a secret between the two parties. The private key is kept private and is known only by the owner (receiver). If someone wants to send you an encrypted message, they can use your public key to encrypt the message and then send you the message. You can use your private key to decrypt the message. One of the keys is always kept private. If both keys become available to a third party, the encryption system will not protect the privacy of the message.

### Asymmetric Key Encryption



### Advantages

- Key Management (n\*2)
- Public key can be freely distributed
- Offers: Digital signatures, integrity checks, key exchange, and non-repudiation

### **Disadvantages**

- Typically 100 to 1000 times slower than symmetric key algorithms
  - The resulting file size of an encryption is larger
- 

## **Asymmetric Key Algorithms**

### **Diffie-Hellman**

- First asymmetric algorithm
- Provides for Key Exchange
- Based on the difficulty of computing discrete logarithms
- Variable key length
  - 512-bit to arbitrarily long
  - 1024-2048 considered secure
- About the same strength as a 3072-bit RSA key

Dr. Whitfield Diffie and Dr. Martin Hellman conceptualized the Diffie-Hellman key exchange. They are considered the founders of the public/private key concept; their original work envisioned splitting the key into two parts.

This algorithm is used primarily to send keys across public networks. The process is not used to encrypt or decrypt messages; it's used merely for the transmission of keys in a secure manner.

For long term security with the use of Diffie-Hellman, 2048 bits is recommended. The supporting key size higher than 4096 bits can create a denial of service. There are implementations of up to 8192 bits, but it can go higher.

---

### **EI Gamal**

- Encryption, Digital Signatures, Key Exchange
- Based upon the Diffie-Hellman
- Main drawback is performance (slower than other comparable algorithms)

EI Gamal is an algorithm used for transmitting digital signatures and key exchanges. The method is based on calculating logarithms and the process used is similar to the Diffie-Hellman key exchange. The EI Gamal algorithm was first published in 1985. The Digital Signature Algorithm (DSA) is based on EI Gamal.

---

### **RSA (Rivest, Shamir, Adleman)**

- Encryption, Digital Signatures, Key Exchange
- De facto standard
- Based on the difficulty of factoring N, a product of two large prime numbers
- Variable Block and Key length

- 512-bit to arbitrarily long
- 1024-2048 considered secure
- Used in PGP

RSA is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is an early public-key encryption system that uses large integer numbers as the basis of the process. It is widely implemented, and it has become a de facto standard. RSA is used in many environments, including Secure Sockets Layer (SSL).

First algorithm known to be suitable for signing as well as encryption

RSA is very strong, but very slow in speed. It is 100 times slower than conventional encryption in software; and 1,000 – 10,000 times slower than conventional encryption in hardware.

---

### **ECC (Elliptic Curve Cryptography)**

- Encryption, Digital Signatures, Key Exchange
- Based on the idea of using points on a curve to define the public/private key
  - Requires less computing power
- An ECC key of 160-bits is equivalent to 1024-bit RSA key
- Implemented on hardware devices such as wireless devices and smart cards

Elliptical Curve Cryptography (ECC) provides similar functionality to RSA. ECC is being implemented in smaller, less-intelligent devices such as cell phones and wireless devices. It is smaller than RSA and requires less computing power. ECC encryption systems are based on the idea of using points on a curve to define the public/ private key pair. This process is less mathematically intensive than processes such as RSA.

---

### **Digital Signatures**

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and authenticates the sender (non-repudiation). The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message. The following exhibit illustrates this concept.

The document passes through a hashing algorithm to produce a message digest, then encrypts (signing) the digest with the senders private key.

---

#### **Signature creation:**

- Three items are used to create the Signature
  - E-mail Message
  - Hashing Algorithm
  - Sender's Private Key
- To verify or authenticate the signature use the sender (matching) public key

## Digital Signature Process

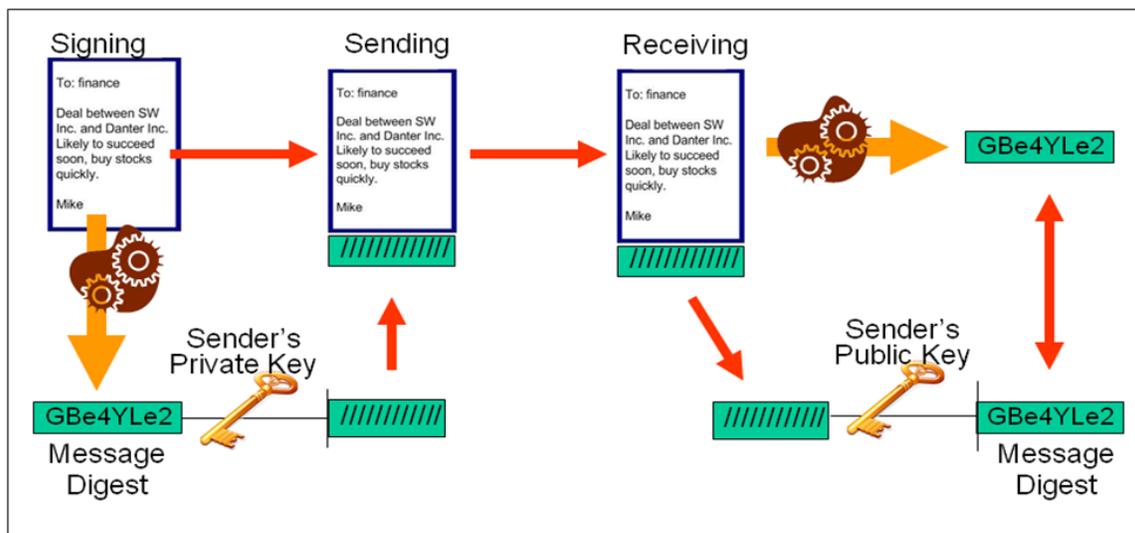
The Sender:

- Creates an email message
- Creates a message hash
- Uses the sender's private key to encrypt the hash
- The encrypted hash becomes the digital signature and is sent with the message to the recipient

The recipient uses the same hashing algorithm to create a message digest, decrypts the sender's signature using the sender's public key, then compares the message digests.

The Recipient:

- Hashes the received message
- Uses the sender's public key to decrypt the message hash that was sent
- Two hashes are compared; if the hashes match, the received message is valid and the sender is verified



## Digital Signature Algorithm

- Used only for digital signatures
- Does not provide confidentiality
- A public key algorithm with a variable key size from 512 to 4096 bits
- Follows NIST/FIPS **Digital Signature Standard (DSS)** and goes up to 1024 bits and uses on SHA- 1 for integrity
- Faster at verifying signatures than RSA

**DSA two goals:**

- Assure the recipient that the message truly came from the claimed sender
- Assure the recipient that the message was not altered while in transit
  - Assure the recipient that the message was not altered while in transit

**Digital Signature Algorithm relies on SHA-1** for input. DSA is a public key algorithm with a variable key size from 512 to 4096 bits. **The U.S. Government standard, DSS,** goes up to 1024 bits.

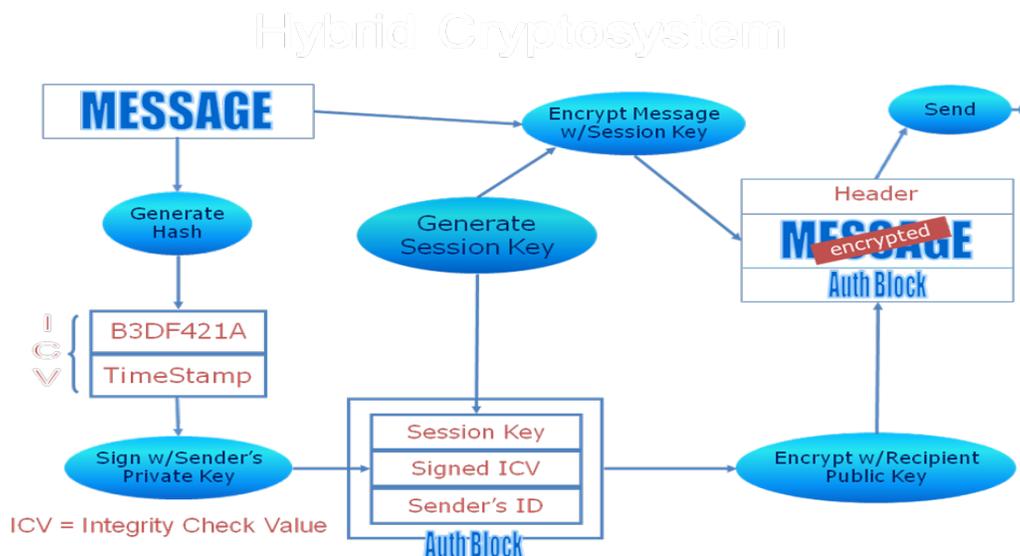
---

**Hybrid Cryptosystem**

Hybrid cryptosystem can be constructed using a combination of cryptosystems:

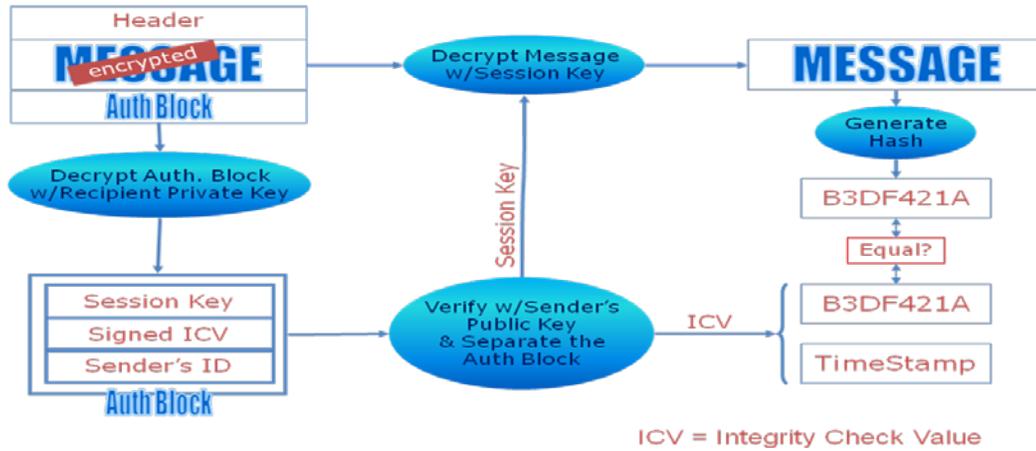
- A symmetric cryptosystem for data encapsulation
- A asymmetric cryptosystem for key encapsulation
- A cryptographic hash can also be used to provide data integrity
- Hybrid examples: PGP, S/MIME, TLS, SSH, IPsec

**Sender's side:**



**Recipient's side:**

# Hybrid Cryptosystem



## Protecting Web Communications

### Secure Socket Layer (SSL)

- Establishes a secure connection between two TCP-based machines
- Uses a handshake method for establishing a session
- Uses X.509v3 certificates for authentication
- Vulnerabilities:
  - Small key sizes; expired digital certificates; compromised keys

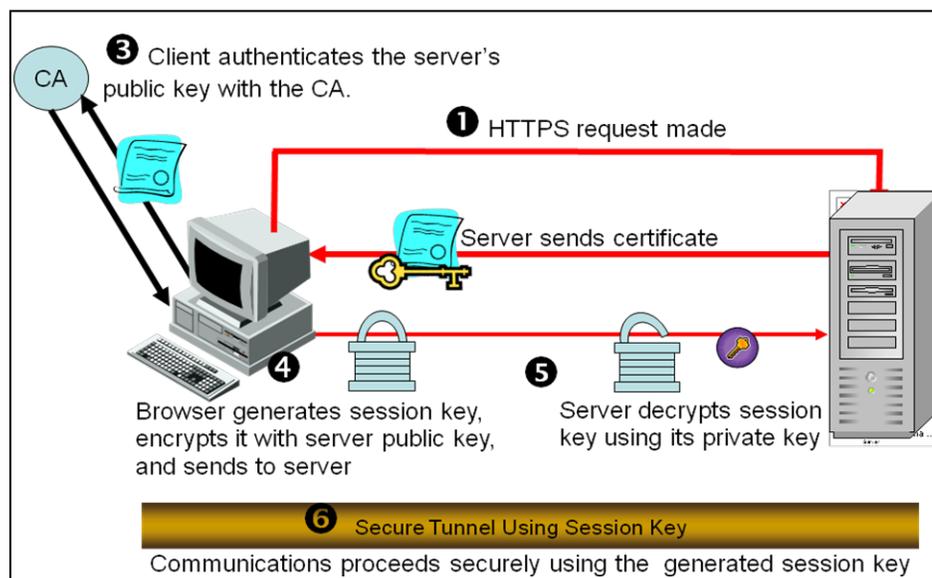
### SSL Provides for:

- Confidentiality: AES, IDEA, 3DES, DES, RC4, RC2
- Message Integrity: SSLv3 MAC with a shared secret key (similar to HMAC) with MD5 or SHA-1
- Key Exchange: RSA, Diffie-Hellman

### SSL Uses

- Can be used to secure a wide range of communications protocols, including:
 

Telnet	HTTP
NNTP	SMTP
FTP	IMAP
- SSL provides the ability to implement Mutual Authentication
- Uses TCP port 443



## Transport Layer Security (TLS)

- IETF developed standard
  - Operates much like SSL
    - a.k.a. SSL 3.1 (minor modification of SSL 3.0)
    - Not interoperable with SSL
  - More secure hashing than SSL
  - WTLS is the wireless version of TLS used in WAP 1.x; TLS is used in WAP 2.x
  - Uses TCP port 443 (works at higher ports)
- 

### TLS Provides for:

- Confidentiality
    - AES, IDEA, 3DES, DES, RC4, RC2
  - Message Integrity
    - HMAC
  - Key Exchange
    - RSA and Diffie-Hellman
  - More alerts codes than SSL
- 

## HTTPS vs. S-HTTP

### HTTPS

- HTTP over SSL (port 443)
- Encrypts the communication channel

Hypertext Transport Protocol Secure (HTTPS) is the secure version of HTTP, the language of the World Wide Web. HTTPS uses SSL to **secure the channel (session)** between the client and server. Many e-business systems use HTTPS for secure transactions. An HTTPS session is identified by the https in the URL and by a key that is displayed on the web browser.

### S-HTTP (Secure HTTP)

- Developed by Netscape to provide security over standard page requests over port 80
- Encrypts **individual messages**
- Does not require client-side public key certificates, as it supports symmetric key-only

Secure Hypertext Transport Protocol (S-HTTP) is HTTP with message security (added by using RSA or a digital certificate). Whereas HTTPS creates a secure channel, S-HTTP creates a secure message. S-HTTP can use multiple protocols and mechanisms to protect the message. It also provides data integrity and authentication.

---

### **Secure Shell (SSH)**

- Secures remote terminal communications
- Secure replacement for Telnet and FTP
- Protects against sniffing, spoofing, and man-in-the-middle attacks
- Encrypts data using a symmetric algorithms
- Establishes connection and authentication using public key cryptography
- Uses TCP port 22
- Example: Putty, OpenSSH

SSH provides an alternative, security-equivalent, program for programs like Telnet, FTP and many other communications-oriented programs. The use of session keys protects the integrity of the data. SSH encrypts the session before the username and password are transmitted (confidentiality).

---

## **Email Security Concepts**

Email exploitation is a result of a weakness in many common email clients. Modern email clients offer many shortcuts, lists, and other capabilities to meet user demands. A popular exploitation of email clients involves accessing the client address book and propagating viruses. There is virtually nothing a client user can do about these exploitations, although antivirus software that integrates with your email client does offer some protection.

### **Simple Mail Transport Protocol (SMTP)**

- Transmits mail from e-mail clients to e-mail servers and between e-mail servers
- Uses TCP port 25

### **Post Office Protocol v.3 (POP3)**

- Downloads e-mail from an inbox on an e-mail server to an e-mail client
- Uses TCP port 110

### **Internet Message Access Protocol v.4 (IMAP4)**

- Downloads e-mail from an inbox on an e-mail server to an e-mail client
  - Uses TCP port 143
- 

### **Multipurpose Internet Mail Extensions (MIME)**

- Defines how e-mail clients handle non-plaintext content

### **Secure/MIME (S/MIME)**

- Follows the X.509 standard
- Provides protection for email and attachments
- Provides authentication, integrity, confidentiality, and non-repudiation using the following algorithms:
  - AES, 3DES, DES, or RC2)
  - Diffie-Hellman with DSS or RSA
  - SHA-1 and MD5

Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard used for encrypting email. S/MIME contains signature data and is the most widely supported standard used to secure email communications.

S/MIME is the de facto standard for email messages. It provides encryption, integrity, and authentication when used in conjunction with PKI. S/MIME version 3, the current version, is supported by IETF.

---

### **Pretty Good Privacy (PGP)**

- Freeware e-mail encryption system
- Uses a web of trust model (not X.509)
- GnuPG is the GNU projects complete and free implementation of the OpenPGP Standard
- Considered a cryptosystem
- Asymmetric: RSA, DSS, Diffie-Hellman
- Symmetric: AES, IDEA, CAST-128, IDEA, Twofish, or 3DES
- Hash Coding: SHA-2, SHA-1, MD5, RIPEMD-160

The program PGP (Pretty Good Privacy) was initially published by Phil Zimmermann in 1991. He released his first version of PGP (Pretty Good Privacy) in response to the threat by the FBI to demand access to the plaintext of the communications of citizens. PGP is considered a “cryptosystem” because it has symmetric key algorithms, asymmetric key algorithms, message digest algorithms, keys, protocols, and other components.

PGP uses Hybrid Encryption: Symmetric for Bulk Encryption and Asymmetric for Key Encapsulation. It also uses **its own digital certificates rather than what is used in PKI**; each user generates and distributes their own public key. Users keep a file referred to as a key ring, which is a collection of public keys received from other users. PGP5 and later required commercial environments to pay fees, so in 1999, the Gnu Privacy Guard (GPG) project was developed to provide PGP for free.

---

## **Certificate Management**

Certificates provide the primary method of identifying that a given user is valid. Certificates can also be used to store authorization information. Another important factor is verifying or certifying that a system is using the correct software and processes to communicate.

- Enables the authentication of the parties involved in a secure transition
- A typical certificate contains the following:
  - The certificates issuer’s name
  - Valid from date / to date
  - The owner of the certificate (subject)
  - The subject’s public key
  - Time stamp
  - The certificates issuer’s digital signature

## Public Key Infrastructure (PKI)

- A framework for managing private keys and certificates
- Provides a standard for key generation, authentication, distribution, and storage
- Establishes who is responsible for authenticating the identity of the owners of the digital certificates
- Follows the X.509 standard

The Public Key Infrastructure (PKI) is a first attempt to provide all the aspects of security to messages and transactions that have been previously discussed. The need for universal systems to support e-commerce, secure transactions, and information privacy is one aspect of the issues being addressed with PKI.

PKI is a two-key, asymmetric system with four key components: Certificate Authority (CA), Registration Authority (RA), RSA, and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

## Digital Certificates

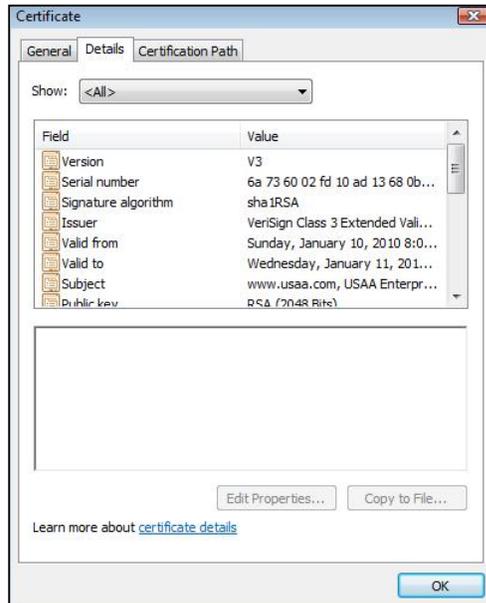
- Follow the X.509v.3 standard
  - International Telecommunication Union (ITU) standard for defining digital certificates
  - Defines the formats and fields for public keys
  - Defines procedures for distributing public keys

The most popular certificate used is the X.509 version 3. The X.509 standard is a certificate format supported by the International Telecommunications Union (ITU) and many other standards organizations. Adopting a standard certificate format is important for systems to be assured interoperability in a certificate-oriented environment.

The Public-Key Infrastructure X.509 (PKIX) is the working group formed by the IETF to develop standards and models for the PKI environment. The PKIX working group is responsible for the X.509 standard.

```

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 1 (0x1)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
        OU=Certification Services Division,
        CN=Thawte Server CA/emailAddress=server-certs@thawte.com
  Validity
    Not Before: Aug  1 00:00:00 1996 GMT
    Not After : Dec 31 23:59:59 2020 GMT
  Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
        OU=Certification Services Division,
        CN=Thawte Server CA/emailAddress=server-certs@thawte.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
        68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
        85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
        6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
        6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
        29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
        6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
        5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
        3a:c2:b5:66:22:12:d6:87:0d
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints: critical
      CA:TRUE
  Signature Algorithm: md5WithRSAEncryption
07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:
a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
e7:20:1b:8b:ca:a4:af:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:99:bc:a3:ff:8a:23:2e:
70:47
  
```



### Certificate Authority (CA)

- Organization responsible for issuing, storing, revoking, and distributing certificates
- Authenticates the certificates it issues by signing them with their private key

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. A certificate is nothing more than a mechanism that associates the public key with an individual. It contains a great deal of information about the user. Each user of a PKI system has a certificate that can be used to verify their authenticity.

### Registration Authority (RA)

- Middleman between subscribers and CA
- Can distribute keys, accept registrations for the CA, and

validate identities

- RA does not issue certificates on their own

A registration authority (RA) offloads some of the work from a CA. An RA system operates as a middleman in the process: It can distribute keys, accept registrations for the CA, and validate identities. The RA doesn't issue certificates; that responsibility remains with the CA.

### Enrollment

- The subject must first prove their identity to the CA before a digital certificate is created
- Form data with an interview, physically appearing with an agent with ID, credit report data, etc.
- Once satisfied your certificate is made containing your ID info, public key, etc.
- CA then digitally signs the certificate with their private key

### Certificate Policy

- Dictates the circumstances in which a certificate can be used
- Protects the CA from claims of loss if the certificate is misused
- Should identify the user's community, names of the CA and RA, and the object identifier

Certificate policies define what certificates do. Certificate policies affect how a certificate is issued and how it's used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification.

The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes. This is a voluntary process in that each organization involved can decide what and how to approve certificate use.

The receiving organization can use this policy to determine whether the certificate has come from a legitimate source. Think about it this way: A PKI certificate can be generated any number of ways using any number of servers. The policy indicates which certificates will be accepted in a given application.

---

### **Certificate Practice Statement (CPS)**

Detailed statement of the procedures and practices the CA uses to manage the certificates and should cover:

- How the CA is structured
- How the certificate will be managed
- How the subscriber's identity is validated
- How to request a certificate revocation
- Which standards and protocols are used

A Certificate Practice Statement (CPS) is a detailed statement the CA uses to issue certificates and implement its policies of the CA. The CA provides the CPS to users of its services. These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules CA users must follow in order to maintain their certificate eligibility. If a CA is unwilling to provide this information to a user, the CA itself may be untrustworthy, and the trustworthiness of that CA's users should be questioned.

---

### **Certificate Server**

- A central repository for storing certificates
  - Allows administrators to set policies in one location and to centrally manage all users certificates
- 

### **Online Certificate Status Protocol (OCSP)**

- Checks for revoked certificates
- OCSP queries a CA or RA that maintains a list of expired certificates
- Server sends a response with a status of valid, suspended, or revoked

OCSP allows for on-line checking of certificate validity, by sending a request to a web site containing information on valid certificates. Thus, it tends to use more up-to-date data than the CRL.

---

### **Certificate Revocation**

- Certificates are revoked due to:
    - Key theft
    - Loss
    - Illegal activity
    - Significant changes in the organization (change in name, ISP, or key personnel)
  - Not revoked due to normal expiration
- 

### **Certificate Revocation List (CRL)**

- Identifies revoked certificates
- Expired certificates are not on the CRL

Certificate revocation is the process of revoking a certificate before it expires. A certificate may need to be revoked because it was stolen, an employee moved to a new company, or someone has had their access revoked.

A certificate revocation is handled either through a Certificate Revocation List (CRL) or by using the Online Certificate Status Protocol (OCSP). A repository is simply a database or database server where the certificates are stored.

---

### **Certificate Suspension**

- Certificates can be suspended
  - Ensures the key is unusable for a period of time
  - Suspend rather than expire certificates to make them temporarily invalid
- 

### **Certificate Expiration**

- If a certificate expires, a new certificate must be issued
  - Expired certificates are NOT added to the CRL
- 

### **Certificate Renewal**

- Unexpired certificates can be renewed close to the end of the expiring certificate's lifetime
  - Allows the same certificate to be used past the original expiration time
  - Not a good practice
- 

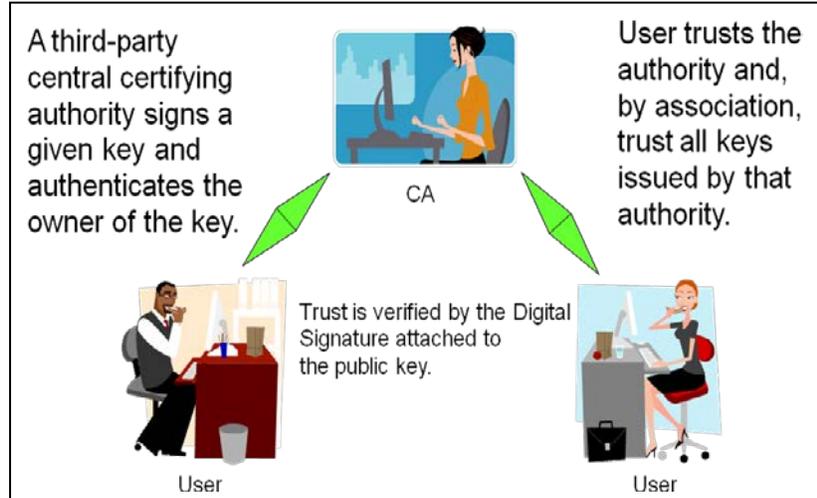
### **Certificate Destruction**

- Establish policies for destroying old keys
  - When a key or certificate is no longer useful, destroy and remove from the system
  - When destroyed, notify the CA so the CRL and OCSP servers can be updated
  - Deregistration should occur when a key is destroyed, especially if the key owner no longer exists (such as a company out of business)
- 

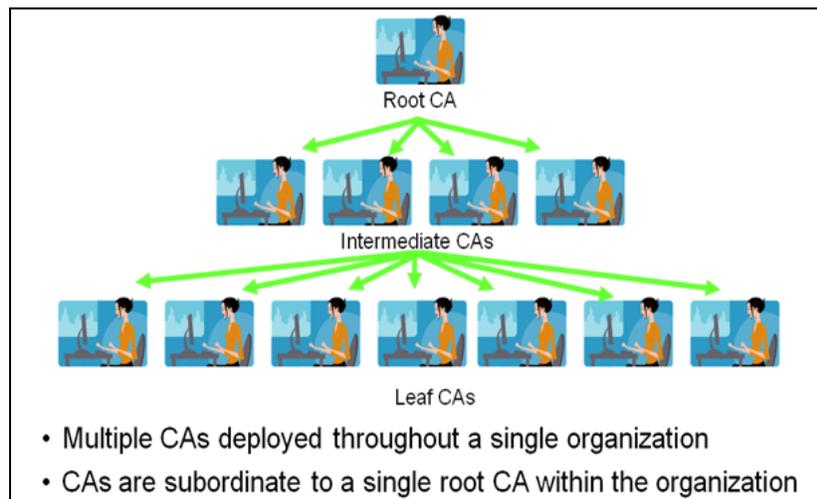
### **Trust Models**

- Trust models explain how users can establish a certificate's validity
- Common models:
  - Single-Authority Trust (a.k.a. third-party trust)
  - Hierarchical Trust
  - Bridge Trust
  - Web of Trust (a.k.a. peer-to-peer)

## Single-Authority Trust (third-party trust)



## Hierarchical Trust

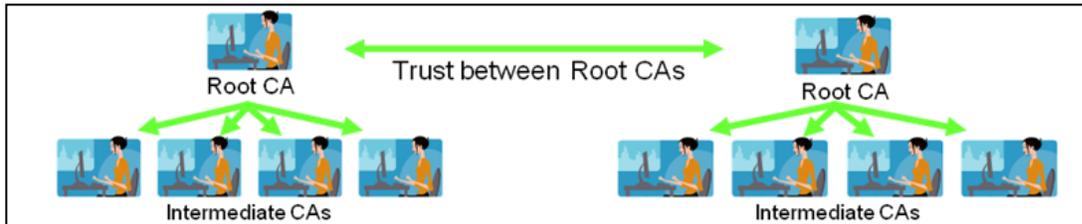


In a hierarchical trust model, also known as a tree, a root CA at the top provides all the information. The intermediate CAs is next in the hierarchy, and they only trust information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't. This arrangement allows a high level of control at all levels of the hierarchical tree.

Root CA systems can have trusts between them, and there can be trusts between intermediate and leaf CAs. A leaf CA is any CA that is at the end of a CA network or chain.

## Bridge Trust

- Two or more separate authorities establish a trust relationship amongst each other
- Best suited for peer-to-peer relationships, such as business partners



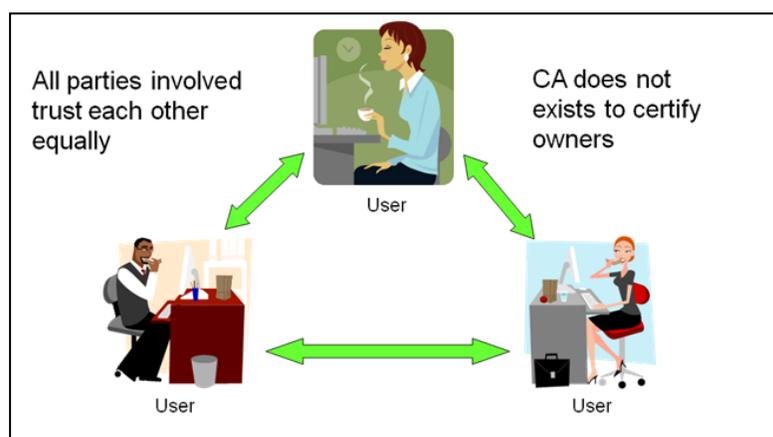
In a bridge trust model, a peer-to-peer relationship exists between the root CAs. The root CAs can communicate with each other, allowing cross certification. This arrangement allows a certification process to be established between organizations or departments. Each intermediate CA trusts only the CAs above and below it, but the CA structure can be expanded without creating additional layers of CAs.

Additional flexibility and interoperability between organizations are the primary advantages of a bridge model. Lack of trustworthiness of the root CAs can be a major disadvantage. If one of the root CAs does not maintain tight internal security around its certificates, a security problem can be created. Hence, an illegitimate certificate could become available to all the users in the bridge structure and its subordinate or intermediate CAs.

A Hybrid Trust Model can use the capabilities of any or all of the structures discussed in the previous sections. You can be extremely flexible when you build a hybrid trust structure. The flexibility of this model also allows you to create hybrid environments. The major difficulty with hybrid models is that they can become complicated and confusing. A user can unintentionally acquire trusts that they shouldn't have obtained.

---

## WEB of Trust (Peer-to-Peer Trust)



## Key Management

How you are going to protect private keys?

- The strength of asymmetric cryptographic lies in the secrecy and security of its private keys.
  - If the private key is stolen or discovered, the certificate must be revoked and a new one issued to take its place.
  - If the private key is lost, there should be a mechanism for recovering data and obtaining new key pairs
- 

### Key Length

- Use sufficiently long keys to protect against attacks aimed at discovering the private key
- The more valuable the data, the longer the key should be

### Crypto period

- Establish policies for setting key lifetimes
- The more valuable the data, the shorter the key lifetime should be

Key management refers to the process of working with keys from the time they are created until the time they are retired or destroyed. It is one of the key aspects of an effective cryptographic system. Keys are the unique passwords or pass codes used to encrypt or decrypt messages.

The term key life cycle describes the stages a key goes through during its entire life. If any aspect of a key's life is not handled properly, the entire security system may become nonfunctional or compromised.

How you are going to protect private keys?

The strength of an asymmetric algorithm lies in the secrecy and security of its private keys.

If the private key is stolen or discovered, the certificate must be revoked and a new one issued to take its place. If the private key is lost, there should be a mechanism for recovering data and obtaining new key pairs.

---

### Centralized Key Management

- A centralized entity is in charge of issuing keys (users do not have control of their keys)
- The central authority keeps a copy of the key

Centralized key generation allows the key-generating process to take advantage of large-scale system resources. Key-generating algorithms tend to be extremely processor intensive. Using a centralized server, this process can be managed with a large single system. However, problems arise when the key is distributed.

Centralized generation has the advantage of allowing additional management functions to be centralized. A major disadvantage is that the key archival and storage process may be vulnerable to an attack against a single point instead of a network. Reliability, security, and archiving can be addressed if the proper systems, procedures, and policies are put into place and followed.

---

### **Decentralized Management**

- The end user generates their own keys
- Does not provide for key escrow, so key recovery is not possible

Decentralized key generation allows the key-generating process to be pushed out into the organization or environment. The advantage of this method is that it allows work to be decentralized and any risks to be spread. This system isn't vulnerable to a single-point failure or attack. Decentralized generation addresses the distribution issue, but it creates a storage and management issue.

---

### **Key Storage**

- The private key must be safely stored to protect it from being compromised or damaged
  - There are two methods for key storage:
    - Software-based:
      - Subject to access violations and intrusions
      - Easily destroyed
      - Subject to the security of the access control system
    - Hardware-based:
      - The most secure form of digital certificate storage
      - More expensive than software solutions
      - Relies on physical security
      - Smart cards or flash drives
- 

### **Key Archival**

- The storage of keys and certificates for an extended period of time
  - Essential element of business continuity and disaster recovery planning
  - Addresses the problem of lost keys and recovery of encrypted data from previous keys
  - Normally done by the CA, a trusted third party, or the key holder
- 

### **Key Escrow**

- Keys needed to decrypt ciphertext are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys
- Allows for key recovery
- Keys must be secured on the Key Escrows network/systems

One of the proposed methods of dealing with key escrow involves the storage of key information with a third party, referred to as a *key escrow agency*. Key escrow systems can also be a part of the key recovery process.

---

### Recovery Agent

- Someone with authority to remove keys from escrow

Key recovery is an important part of an encryption system. Information that is stored using older keys will be inaccessible using a new key. Key recovery allows you to access information that is encrypted with older keys.

### M of N Control

- Requires two or more recovery agents
- There must be multiple key escrow recovery agents (N) in any given environment
- A minimum number of agents (M) must work together to recover a key

Many recovery and archive systems use the *M of N Control* method of access. This method, simply stated, says that in order to access the key server if  $n$  number of administrators have the ability to perform a process,  $m$  number of those administrators must authenticate for access to occur. This would ensure that no one person could compromise the security system.

---

### Multiple Key Pairs

- Keep one key pair fully private
  - Do not need an escrow service
  - Eliminates the possibility of the escrow being compromised and your key pairs used in impersonation attacks
- 

### Revoking Keys

- Conducted when the keys are compromised, the authentication process has malfunctioned, people are transferred, or other security risks occur
- Revoking a key keeps it from being misused.
- A revoked key must be assumed to be invalid or possibly compromised.

Systems such as PKI use a CRL to perform a check on the status of revoked keys. Revocations are permanent. Once a certificate is revoked, it can't be used again; a new key must be generated and issued.

### Suspending Keys

- Temporary situation
- Ensures the key is unusable for a period of time

A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their

absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring. The temporary suspension would give administrators or manager's time to sort out what is happening.

Checking the status of suspended keys is accomplished by checking with the certificate server or by using other mechanisms. In a PKI system, a CRL would be checked to determine the status of a certificate. This process can occur automatically or manually. Most key or certificate management systems provide a mechanism to report the status of a key or certificate.

---

### **Renewing Keys**

- Defines the process of enabling a key for use after its scheduled expiration date
- A key would be reissued for a certain time
- Bad practice and should not be performed

Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys occurs for a given time frame. Many systems include means to prevent rolling keys over.

In general, key renewals are a bad practice and should not be performed except in the direst of situations. The longer a key is used, the more likely it is to be compromised. It is always better to renew keys than to do a key rollover.

---

### **Destroying Keys**

- Process of destroying keys that have become invalid

Key destruction is the process of destroying keys that have become invalid. For example, an electronic key can be erased from a smart card.

## Domain 2 – Network Security

A Security+ candidate is expected to:

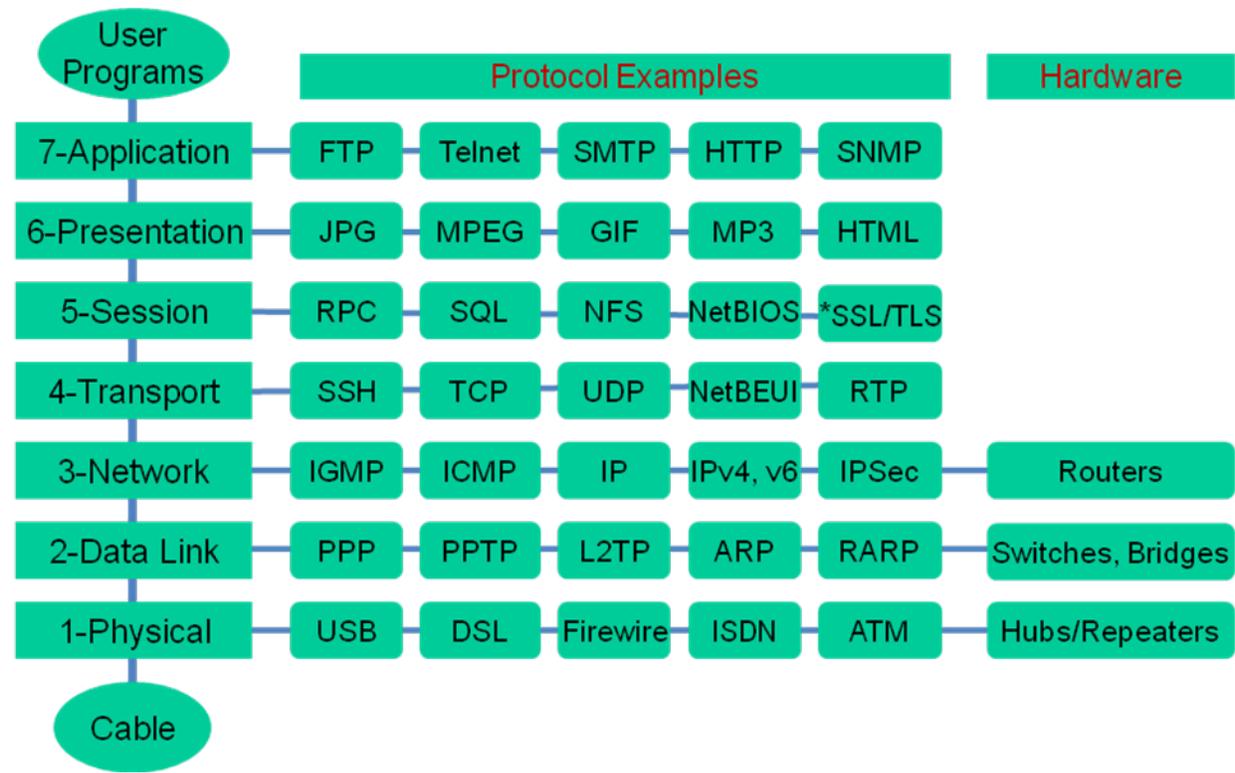
- Explain the security function and purpose of network devices and technologies
- Apply and implement secure network administration principals
- Distinguish and differentiate network design elements and compounds
- Implement and use common protocols
- Identify commonly used default network ports
- Implement wireless networks in a secure manner

### Review of OSI and TCP/IP Models

#### Open Systems Interconnect (OSI Model)

OSI	Usage
7 - Application	Main interface between network and application
6 - Presentation	Puts into a format all computers can understand Encryption, translation, compression
5 - Session	No security Connection establishment between applications
4 -Transport	Keeps track of segments Handles error recovery and flow control
3 - Network	Creates packets End-to-end communication across one or more subnetworks
2 - Data-Link	Transmission of frames over a single network connection
1 - Physical	Converts bits into voltage

#### Protocols and the OSI Model



### TCP/IP Model

- a.k.a. DoD Model
- Layers:
  - Application Layer
  - Host-to-host (Transport) Layer
  - Internet Layer
  - Network Interface Layer

The TCP/IP protocols were developed as part of the research network developed by the United States Defense Advanced Research Projects Agency (*DARPA* or *ARPA*) in 1969. Initially, this network, called the *ARPAnet*, was designed to use a number of protocols that had been adapted from existing technologies. The developers of the new network recognized that trying to use these existing protocols might eventually lead to problems as the *ARPAnet* scaled to a larger size and was adapted for newer uses and applications. In the early 1980s, the TCP/IP protocols were developed. In 1983, they became standard protocols for *ARPAnet*.

One of the key points in understanding this layering process is the concept of encapsulation. Encapsulation allows a transport protocol to be sent across the network and utilized by the equivalent service or protocol at the receiving host. The IP suite uses encapsulation to provide abstraction of protocols and services. Generally a protocol at a higher level uses a protocol at a lower level to help accomplish its aims.

## OSI and TCP/IP Model Comparison

OSI Reference Model		TCP/IP Model	
7	Application	4	Application
6	Presentation		
5	Session		
4	Transport	3	Host to Host
3	Network	2	Internet
2	Data Link	1	Network Interface
1	Physical		

---

## Implement and use of common ports and protocols

### TCP/IP Protocol Overview

- A suite of protocols working together to enable network communications
- The most widely used networking protocol
- Key protocols in the suite include:
  - **Transmission Control Protocol (TCP):** offers full-duplex, connection-oriented, reliable delivery.
  - **User Datagram Protocol (UDP):** offers "best effort" delivery with no error correction or flow control.
  - **Internet Protocol (IP):** is used for addressing.
  - **Internet Control Message Protocol (ICMP):** is used for network connections.

---

### Common definitions:

- **Addresses:** Identifies networks and devices on a network
- **Port Numbers:** Identifies specific services running on a device
- **Messages:** Typically addressed to both the device and the port number of the service
- **Socket:** IP address: port number
- **Socket Pairs**
  - Client IP address: port number and the Servers IP address: port number (177.41.72.6:3022 communicating to 41.199.222.3:80)

We are sending an HTTP request from our client at 177.41.72.6 to the Web site at 41.199.222.3. The server for that Web site will use well-known port number 80, so its socket is 41.199.222.3:80, as we saw before. We have ephemeral port number 3,022 for our Web browser, so the client socket is 177.41.72.6:3022. The overall connection between these devices can be described using this socket pair: (41.199.222.3:80, 177.41.72.6:3022)

The primary method of connecting systems using the Internet is the TCP/IP protocol. This protocol establishes connections and circuits using a combination of the IP address and a port. A port is an interface that is used to connect to a device. Sockets are a combination of the IP address and the port.

---

### Internet Control Message Protocol (ICMP)

- Used for network troubleshooting
- Reports errors and reply to requests ping and traceroute use ICMP
- Several different types
  - 0 - Echo Reply
  - 3 - Destination Unreachable
  - 8 - Echo
  - 30 - Traceroute

Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

ICMP, documented in RFC 792, is a required protocol tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation. Of course, since ICMP uses IP, ICMP packet delivery is unreliable, so hosts can't count on receiving ICMP packets for any network problem. Some of ICMP's functions are to:

- Announce network errors, such as a host or entire portion of the network being unreachable, due to some type of failure. A TCP or UDP packet directed at a port number with no receiver attached is also reported via ICMP.
- Announce network congestion, when a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it will generate ICMP *Source Quench* messages. Directed at the sender, these messages should cause the rate of packet transmission to be slowed. Of course, generating too many Source Quench messages would cause even more network congestion, so they are used sparingly.
- Assist Troubleshooting, ICMP supports an *Echo* function, which just sends a packet on a round-trip between two hosts. Ping, a common network

management tool, is based on this feature. Ping will transmit a series of packets, measuring average round-trip times and computing loss percentages.

- **Announce Timeouts**, if an IP packet's TTL field drops to zero, the router discarding the packet will often generate an ICMP packet announcing this fact. TraceRoute is a tool which maps network routes by sending packets with small TTL values and watching the ICMP timeout announcements.

---

## Port Assignments

- Assigned by the IANA (Internet Assigned Numbers Authority) <http://www.iana.org/assignments/port-numbers>
  - **Well-Known Ports: 0 – 1023** (TCP or UDP ports that direct packets to the appropriate application on the server)
  - **Registered Ports: 1024 – 49151**
  - **Dynamic and/or Private Ports: 49152 - 65535**

There are 65,535 TCP and UDP ports on which a computer can communicate and are divided up between well-known ports, registered ports, and dynamic (or private) ports. Many of these ports are unsecure which can be used for exploitation. The configuration process should start with enabling only the services necessary for the device to function.

---

## Ephemeral Ports

Ports used when an application does not bind the socket to a specific port number.

### The Ephemeral Port Range

A TCP/IPv4 connection consists of two endpoints, and each endpoint consists of an IP address and a port number. Therefore, when a client user connects to a server computer, an established connection can be thought of as the 4-tuple of (server IP, server port, client IP, client port). Usually three of the four are readily known (client machine uses its own IP address and when connecting to a remote service, the server machine's IP address and service port number are required).

What is not immediately evident is that when a connection is established that the client side of the connection uses a port number. Unless a client program explicitly requests a specific port number, the port number used is an ephemeral port number. Ephemeral ports are temporary ports assigned by a machine's IP stack, and are assigned from a designated range of ports for this purpose. When the connection terminates, the ephemeral port is available for reuse, although most IP stacks won't reuse that port number until the entire pool of ephemeral ports have been used. So, if the client program reconnects, it will be assigned a different ephemeral port number for its side of the new connection.

Ephemeral ports are typically used by TCP, UDP, or the SCTP as ports for the client end of a client-server communication when the application does not bind the socket to a specific port number, or by a server application to free up a well-known service

listening port and establish a service connection to the client host. The allocations are temporary and only valid for the duration of the communication session. After completion of the communication session, the ports become available for reuse, although most implementations may simply increment the last used port number until the ephemeral port range is exhausted.

---

### Most common Ports and Protocols

PORT	Service	PORT	Service
20/21	FTP-Data/Control	119	NNTP
22	SSH/SFTP/SCP	137-139	NETBIOS
23	Telnet	139	NetBIOS
25	SMTP	143	IMAP v4
53	DNS	161/162	SNMP
67/68	DHCP	389	LDAP
69	Trivial FTP	443	SSL/TLS/HTTPS
80	HTTP	636	Secure LDAP
88	Kerberos	1702	L2TP
110	POP3	1812	RADIUS
115	SFTP (Simple)	3389	RDP

Ports identify how a communication process occurs. They are special addresses that allow communication between hosts. A port number is added from the originator, indicating which port to communicate with on a server. If a server has this port defined and available for use, it will send back a message accepting the request. If the port is not valid, the server will refuse the connection.

A port is nothing more than a bit of additional information added to either the TCP or UDP message. This information is added in the header of the packet. The layer below it encapsulates the message with its header.

## TCP/IP Addressing

- Unique identifiers to differentiate one host from another
- Two addressing schemes for TCP/IP:
  - IPv4
  - IPv6

---

### IPv4 Addressing

- Made up of a 32-bit address or four-octet address
- Referred to as dotted decimal representation of a binary number

Example: the IP address of 195.142.67.2 is actually the following binary:

<b>11000011</b> <b>195</b>	<b>10001110</b> <b>142</b>	<b>01000011</b> <b>67</b>	<b>00000010</b> <b>2</b>
-------------------------------	-------------------------------	------------------------------	-----------------------------

---

### IPv4 Address Classes

- IP addresses are grouped into different classes
- Can determine which class any IP address is in by examining the first 4 bits of the IP address
- Address classes are supported by IPv4:
  - Class A 0.0.0.0 – 127.255.255.255
  - Class B 128.0.0.0 – 191.255.255.255
  - Class C 192.0.0.0 – 223.255.255.255
  - Class D 224.0.0.0 – 239.255.255.255 (multicasting)
  - Class E 240.0.0.0 – 255.255.255.255 (experimental)
  - Class 127.x.x.x is for the loopback address.

---

### IPv4 Subnetting

IP addresses are actually two addresses:

- Network address
- Host address

The class and subnet mask determines the network and the host.

- Used to divide large groups of hosts into smaller collections
- Allows an IP address to be split within 32 bits
- Controls traffic (Traffic between subnets can be monitored and restricted at the routers)

---

### Advantages of Subnetting

- Decreased network traffic
- Broadcasts limited to individual subnets
- Improved troubleshooting
- Faster to trace a problem on a subnet
- Improved utilization of addresses
- No wasted IPs
- Flexibility
- Customization of number of hosts on a subnet

---

### Classless Inter-Domain Routing (CIDR)

- CIDR is based on variable-length subnet masking (VLSM) to allow allocation on arbitrary-length prefixes
- An IP address is composed of two parts:
  - a network-identifying prefix
  - a host identifier

The number of addresses of a subnet defined by the mask or prefix can be calculated as  $2^{\text{address size} - \text{mask}}$ . For example: a mask of /29 gives:  $2^{32-29} = 2^3 = 8$  addresses for an IPv4 network.

### IPv4 Private Network Addressing

- Used for networks not connecting directly to the Internet
- Internet Assigned Numbers Authority (IANA) set aside addresses for intranets:
  - Class A: 10.0.0.0 – 10.255.255.255
  - Class B: 172.16.0.0 – 172.31.255.255
  - Class C: 192.168.0.0 – 192.168.255.255
- Routers connecting to the Internet typically filter out any reference to these addresses.
- Two most common examples:
  - Networks with no need to connect to the Internet
  - Networks connecting to the Internet through an application gateway that remaps

### IPv6

- Allows for growth of addresses
- 79 octillion addresses
- 128 bits total: 8 blocks (4 hexadecimal digits)
  - 3FFE:0B00:0800:0002:0000:0000:0000:000C
- Zero compression rule -Drop more than one grouping of zero octets
  - 3FFE:B00:800:2::C

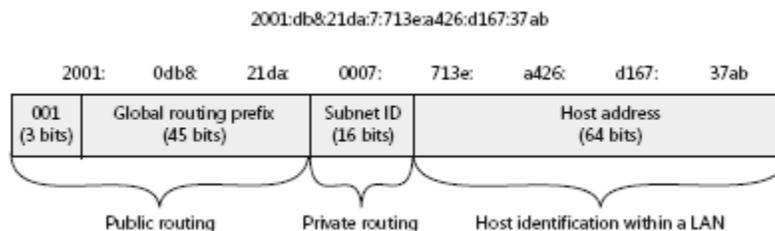
The IP v6 Loopback address is 0000:0000:0000:0000:0000:0000:0000:0001

### IPv6 Addresses

- Upstream Supplier Address
- Provided by ISP/NSP
- Local Address
  - ::1/128, Defines the local host
- Link-Local Address
- Address for the local subnet

### Global address

Global address is the equivalent to public addressing in IPv4, and used on the Internet. The address prefix used (first block) is **2000-3FFF**.



### Link-Local Addresses

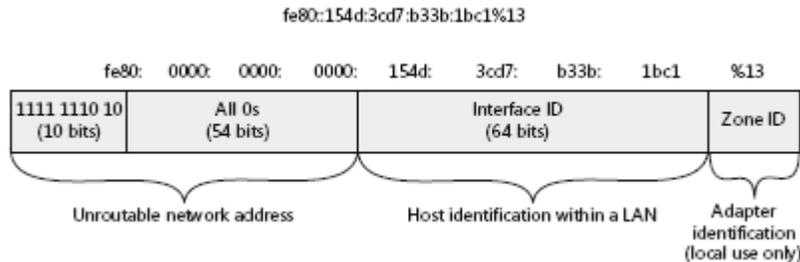
Link-Local addresses are similar to APIPA address (169.254.0.0/16) in IPv4, self-configured and non-routable.

A Link-Local address always begins with “**fe80**” in the first block.

First half: fe80:000:000:000 – Identifies that it is self-configured

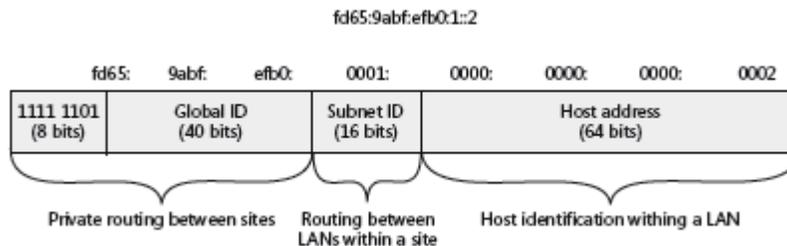
Second Half: Interface ID - Identifies the host in the LAN

Last: zone ID in the form of “%ID” Identifies multiple adapters connected to different networks.



### Unique Local Address

Unique Local Address is the equivalent to IPv4 private address. They are routable between subnets on a private network only. Such addresses begin with “**fd**”.



### File Transfer Protocol (FTP)

- Used to transfer files between systems on the Internet
- Ports TCP 20 and TCP 21
- Active/Passive
- Vulnerabilities:
  - Username
  - Password
  - Commands and files are sent in plaintext

FTP has two standard data transmission methods: active FTP and passive FTP. The terms “active” and “passive” refer to the server’s role in setting up the TCP session.

### Blind FTP

User cannot see names of files in the directory as they upload files to the server.

- **Bounce vulnerabilities:** The specification for FTP, RFC 2577, permits connected clients to open other connections on any port on the FTP server. A user with an anonymous FTP connection can use this to attack other systems by opening a service port on the third system and sending commands to that service.
- **File sharing exploitation:** FTP servers can be exploited as unauthorized file-sharing locations. For example, FTP servers can be hijacked to create warez servers, where illegal software is posted and shared
- **“Glob” vulnerabilities:** Because some FTP servers enable clients to use wildcard characters such as the asterisk (\*) in file operations, attackers can delete or copy large numbers of files in a single operation, especially when those files follow standard DOS 8.3 naming conventions.

### Anonymous FTP

- Gains access by using the login “anonymous” and a password usually in the form of an email address
- Have limited privileges sufficient to allow you to transfer files from/to designated areas

While anonymous access protects account information because the passwords are generic, it does not provide authentication or access control mechanisms that can prevent malicious activity. Anonymous FTP servers could be used for illegal or unauthorized activity. Blind FTP sites permit anonymous access, but to one directory only, which provides some protection to other areas on the server.

---

### S/FTP (Secure FTP) uses the Secure Shell (SSH) (port 22)

- A tunneling protocol that allows access to remote systems in a secure manner. SSH allows connections to be secured by encrypting the session between the client and the server.

### FTPS

- Session is encrypted, but not the data
- FTPS includes full support for the TLS and SSL cryptographic protocols (port 443)

### Simple FTP

- No security (port 115)

---

### Secure Shell (SSH)

- Secures remote access and remote terminal communications
- Secure replacement for Telnet and FTP
- Protects against man-in-the-middle attacks and spoofing
- Symmetric cryptography for encryption
- PKC for connection/authentication
- Uses TCP Port 22
- SSH suite (SSH, SCP, SFTP, Slogin)

### **SCP (Secure Copy Protocol)**

- Means of securely transferring files using Secure Shell (SSH) protocol
- Program to perform secure copying
- Uses port 22
- Used on Unix/Linux(scp) or Windows (Win SCP)
- Unlike rcp or FTP, scp encrypts both the file and any passwords exchanged

SSH uses Public Key Cryptography (PKC) for connection and authentication. SSH enables VPN-like tunnels that are encrypted and authenticated via RSA public/private key pairs. These safeguards help to prevent spoofing and packet sniffing.

---

### **Simple Network Management Protocol (SNMP) (v.3)**

- Manages and monitors devices in a network
- Application Layer Protocol
- No authentication capabilities prior to v.3

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

---

## **Network Name Resolution Protocols**

### **Network Basic Input Output Systems (NetBIOS)**

- 15-character naming convention for resources
- Broadcast oriented network protocol
- Uses ports 137, 138, 139, 445
- Filter traffic on NetBIOS ports
- Disable NetBIOS to reduce null sessions

NetBIOS opens a port for file and print sharing. The port can be accessed across the Internet as well as by devices on the local LAN.

- NetBIOS name service: port 137
  - NetBIOS datagram service: port 138 (for name resolution)
  - NetBIOS session service: port 139
- 

### **NetBIOS Extended User Interface (NetBEUI)**

- Transports NetBIOS traffic on a LAN
- Non-routable
- Traffic easily intercepted

NetBIOS Extended user Interface (NetBEUI) is used to transport NetBIOS traffic in a LAN. NetBEUI is a non-routable protocol (can't be sent across routers) and its traffic is easily intercepted with a sniffer.

### **Windows Internet Naming Service (WINS)**

- Translates NetBIOS names to IP addresses
- Runs as a service on a server
- Pre-Windows 2000

WINS: As of Windows 2000, DNS provides the favored alternative to WINS, as part of Active Directory. In theory, if DNS is available, WINS is only necessary if pre-Windows 2000 clients or servers need to resolve names. WINS is a software service that dynamically maps IP addresses to computer names (NetBIOS names). This allows users to access resources by name instead of requiring them to use IP addresses that are difficult to recognize and remember. WINS servers support clients running Windows NT 4.0 and earlier versions of Microsoft operating systems.

---

### **Domain Name Service (DNS)**

- An IETF standard naming system for resources connecting to the internet
- Translates domain names to IP addresses

Domain Name Service (DNS) servers resolve hostnames to IP addresses. DNS servers can be used internally for private functions as well as externally for public lookups.

### **Local Host File**

- Stores information on nodes in a network
  - Maps hostnames to IP addresses
  - The hosts file is used as a supplement DNS
- 

### **DNS Zones**

- The portion of the DNS domain name space over which a DNS server has authority
- A portion of a namespace, not a domain
- Can contain one or more contiguous domains

### **Zone Transfers**

- Publishes information about the domain and the name servers of any domains subordinate

DNS zone transfer is a type of DNS transaction. It is one of the many mechanisms available for administrators to employ for replicating the databases containing the DNS data across a set of DNS servers.

DNS zone transfers have several potential security issues. The data contained in an entire DNS zone may be sensitive in nature. Individually, DNS records are not sensitive,

but if a malicious entity obtains a copy of the entire DNS zone for a domain, they may have a complete listing of all hosts in that domain. That makes the job of a computer hacker much easier. A computer hacker needs no special tools or access to obtain a complete DNS zone if the name server is promiscuous and allows anyone to do a zone transfer.

The default behavior for DNS zone transfer permits any host to request and receive a full zone transfer for a Domain. This is a security issue since DNS data can be used to decipher the topology of a company's network. The information obtained can be used for malicious exploitation such as DNS poisoning/spoofing. This is like an anonymous person calling the receptionist to request and receive the entire company's telephone and address book.

---

### DNS Record Types

- DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses.
- Different record types are used for different purposes.
- Examples:
  - **A**- Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host
  - **CERT**- Certificate Record
  - **MX**- Maps a domain name to a list of message transfer agents for that domain
  - **NS**- Delegates a DNS zone to use the given authoritative name servers

**Example of "A" Record with Syntax:** example.com. IN A 69.9.64.11

Where:

- IN indicates Internet
- A indicates the Address record.

The above example indicate that the IP Address for the domain example.com is 69.9.64.11

---

### DNS Poisoning

- Incorrect DNS data that is introduced into a primary DNS server
- Redirects traffic to incorrect sites

DNS poisoning may also be referred to as DNS cache poisoning, because it affects the information that is cached.

### Domain Name Kiting

- Process of registering for a domain name; using that registered name for a 5 day grace period; at the end of the 5 days, not paying

A newly registered domain name can be deleted or dropped with a full refund of the registration fee during the initial five-day window. DNS kiting refers to the practice of taking advantage of this five-day grace period to monopolize domain names without ever paying for them.

---

### Remote Desktop Protocol (RDP)

- Allows a user to control a networked computer
- Software referred to as either:
- Remote Desktop Connection (RDC) or
- Terminal Services Client (TSC)
- Port should always be blocked by the firewall rule for inbound traffic
- Server listens by default on TCP port 3389

Operating system clients that use RDP: Windows (including handheld versions), Linux/Unix, Mac OS X and other modern operating systems.

Microsoft refers to RDP as Terminal Services or Remote Desktop Services. In Windows Server 2008 R2, Terminal Services has been renamed to Remote Desktop Services.

---

## Common Transport Protocols

### Tunneling

- Virtual dedicated connection between two systems or networks
- Sends private data across a public network by encapsulating data into other packets
- Usually includes data security as well as encryption
- Most Popular: Layer 2 Tunneling Protocol

Tunneling refers to creating a virtual dedicated connection between two systems or networks. You create the tunnel between the two ends by encapsulating the data in a mutually agreed upon protocol for transmission. In most tunnels, the data passed through the tunnel appears at the other side as part of the network.

Tunneling protocols usually include data security as well as encryption. Several popular standards have emerged for tunneling, with the most popular being the Layer 2 Tunneling Protocol (L2TP).

---

### Point-to-Point Protocol (PPP)

- Used for establishing remote connections over a serial line or dial-up connection
- Allows TCP/IP traffic to be transmitted over telecommunication lines
- **No encryption**
- EAP, CHAP, or PAP Authentication

---

### Layer 2 Forwarding (L2F) (CISCO)

- Used for dial up connection
- Authentication, but no data encryption
- Added mutual authentication
- Operates at Layer 2 and uses UDP port 1701

---

### Point-to-Point Tunneling Protocol (PPTP) (Microsoft)

- Encapsulates and encrypts PPP packets
- Negotiation in the clear

- After negotiation is completed, channel is encrypted
- Uses MPPE to encrypt data
- Authentication: PAP, CHAP, MS-CHAP, or EAP-TLS
- Operates at Layer 2 and uses TCP port 1723

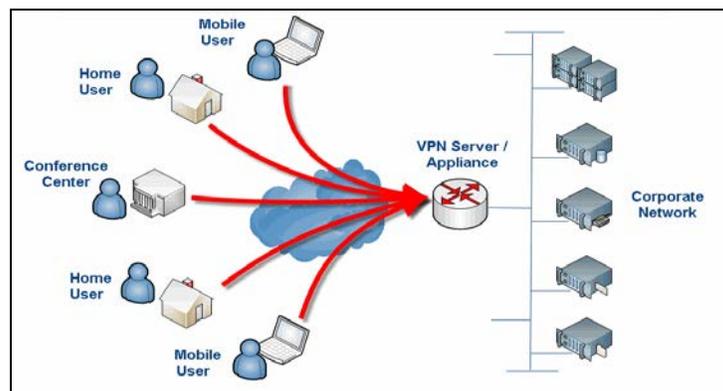
---

### Layer 2 Tunneling Protocol (L2TP) (RFC Standard)

- Hybrid of PPTP and L2F
  - No data encryption
  - Uses IPSec to provide data encryption and integrity
  - Authentication: PAP, CHAP, MS-CHAP, or EAP-TLS
  - Operates at Layer 2 and uses UDP port 1701
- 

### Virtual Private Networks (VPN)

- Private network connection that occurs through a public network
  - Can provide security
  - Established via Tunneling Protocols
    - L2TP-IPSec
    - PPTP (MPPE)
- 



**Virtual Private Networks Figure**

---

### Internet Protocol Security (IPSec)

- Most widely deployed VPN technology
- Requirement for IP Version 6
- Can be used to encrypt any traffic supported by IP
- Includes both encryption and authentication
- Can be used with L2TP or alone
- Requires either certificates or pre-shared keys
- Operates at Layer 3

IPSec is a security protocol that provides authentication and encryption across the Internet. IPSec is becoming a standard for encrypting virtual private network (VPN) channels. It is available on most network platforms, and it's considered to be highly secure.

One of the primary uses of IPSec is to create VPNs. IPSec, in conjunction with Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F), creates packets that are difficult to read if intercepted by a third party.

---

### IPSec Modes

- Transport Mode
    - Used for end-to-end encryption of data
    - Packet data is protected, but the header is left intact
  - Tunnel Mode
    - Used for link-to-link communications
    - Both the packet contents and the header are encrypted
  - *“Transport on the LAN and Tunnel on the WAN”*
- 

### Primary protocols used by IPSec

- Authentication Header (AH)
  - Offers authentication and integrity
  - Uses HMAC with SHA-1 or MD5
  - IP protocol # 51
- Encapsulating Security Payload (ESP)
  - Offers authentication, integrity, and confidentiality
  - Uses AES, 3DES, or DES
  - IP protocol # 50

The two primary protocols used by IPSec at the bottom layer are Authentication Header (AH) and Encapsulating Security Payload (ESP). Both can operate in either the transport or tunnel mode.

---

### IPSec Security Association (SA)

- Authenticates and negotiates end users and manages secret keys
- Negotiates a shared secret key to be used for protecting the traffic
- Established either by IKE or by manual user configuration
- Unidirectional
- When SAs are established for IPSec, the SAs for both directions are established

All implementations of IPSec must have a security association. The security association is a one-way connection that affords security services to the traffic carried by it. This means that in an encrypted session, there are two security associations - one for each direction. Security services are offered by either the Authentication Header (AH) or the Encapsulating Security Payload (ESP), but not both.

A separate pair of IPSec SAs is set up for AH and ESP. Each IPSec peer agrees to set up SAs consisting of policy parameters to be used during the IPSec session. The SAs are unidirectional for IPSec, so that peer 1 will offer peer 2 a policy. If peer 2 accepts this policy, it will send that policy back to peer 1. This establishes two, one-way SAs,

between the peers. So, two-way communication consists of two SAs, one for each direction.

### Internet Security Association and Key Management Protocol (ISAKMP)

- Defines procedures and packet formats to establish, negotiate, modify, and delete Security Associations
- Defines payloads for exchanging key generation and authentication data
- Typically utilizes IKE for key exchange, although other methods can be implemented

UDP port 500

### Internet Key Exchange (IKE)

- Standard automated method for negotiating shared secret keys in IPSec
- Used to generate, exchange, and manage keys
- Supports pre-shared keys and X.509 certificates for authenticating VPN peers
- Uses UDP port 500
- **Uses Oakley**

When using IKE to establish the security associations for the data flow, the security associations are established when needed and expire after a period of time (or volume of traffic).

### Oakley Key Determination

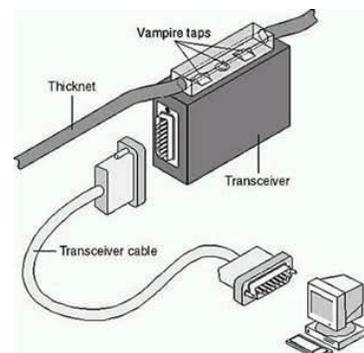
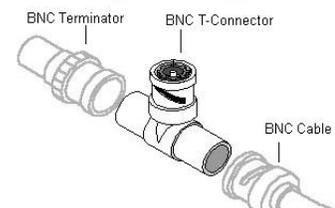
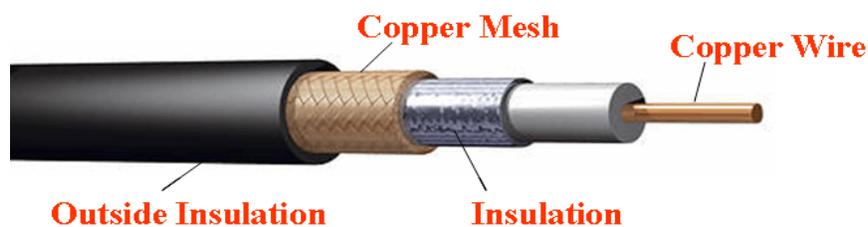
- A key-agreement protocol that performs the negotiation of keying material across an insecure connection
- **Uses Diffie-Hellman** for exchanging keys

## Network Devices and Physical Media

### Transmission Media

#### Coaxial

- BNC Connectors
- Vulnerabilities:
  - Sniffer attached to T connector or vampire tap
  - DoS through break in the cable



Coaxial cabling is one of the oldest media used in networks. Coax is built around a center conductor or core that is used to carry data from point to point. The center conductor has an

insulator wrapped around it, a shield over the insulator, and a nonconductive sheath around the shielding. This construction allows the conducting core to be relatively free from outside interference. The shielding also prevents the conducting core from emanating signals externally from the cable.

Coax supports both baseband and broadband signaling. Baseband signaling means that a single channel is carried through the coax (Thicknet and Thinnet) and broadband refers to multiple channels on the coax (Cable TV/Internet).

Coax has two primary vulnerabilities from a security perspective. The most common is the addition of a T-connector attached to a network sniffer. This sniffer would have unrestricted access to the signaling on the cable. The second and less common method involves a connection called a vampire tap.

Vampire Taps: Clamps onto and "bites" into the coaxial cable (hence the vampire name). It forces a spike through a hole drilled through the outer shielding. The spike contacts the inner conductor while other spikes bite into the outer conductor.

---

### **Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP)**

- -Most popular: CAT 5e/6
- -Vulnerabilities:
  - -Electromagnetic Interference (EMI)
  - -Wire tapping
  - -How and where wires are ran in a building
- Plenum: fire safety

UTP cabling and STP cabling are similar in function with the exception that STP wraps a shield, like a coax, over the wires.

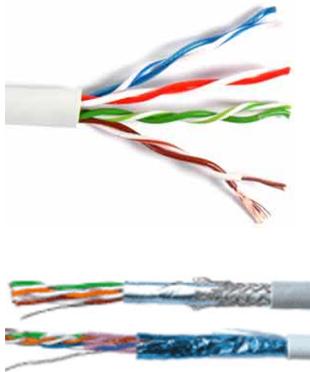
UTP and STP cabling isn't as secure as coax, because it can be easily tapped into, and it's used primarily for internal wiring. It's more difficult to splice into a twisted-pair cable, but three-way breakout boxes are easy to build or buy.

The limit of cable segment length of twisted pair for use with Ethernet is 100 Meters, beyond this the attenuation of the cables may cause reliability problems.

Category 5E (Enhanced): This cable has all the characteristics of Category 5, but is manufactured with higher quality to minimize crosstalk. The cable has more twists than traditional Category 5. It is rated at frequencies up to 200 MHz, which is double the transmission capability of traditional Category 5. However, at these frequencies, crosstalk can be a problem, and the cable does not have shielding to reduce crosstalk.

---

## Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP)



Category	Speed	Usage
CAT 1	Voice	POTS
CAT 2	4 Mbps	Token Ring
CAT 3	10Mbps	10Base-T
CAT 4	16-20Mbps	16 MB Token Ring
CAT 5e	1000Mbps	10-, 100- & 1000Base-T
CAT 6	1000Mbps	High speed - broadband
CAT 7	1000Mbps	Proposed standard

**Fiber Optics**

- Expensive, used for backbone
- Cannot be tapped into easily
- Fiber Taps
  - With a sharp bend in the strand, some light can escape
  - Fiber tap device captures light
  - Easy to detect due to the attenuation in the line

Fiber, as a media, is relatively secure because it can't be tapped easily. Fiber's greatest security weakness is at the connections to the fiber-optic transceivers. Passive connections can be made at the connections, and signals can be tapped from there. The other common security issue associated with fiber optics is that fiber connections are usually bridged to wire connections.

**Layer 1 - Physical Devices****Network Interface Card (NIC)**

- Device that connects a host to the network
- Contains a ROM chip with a MAC address
- MAC identifies the host uniquely on the LAN
- Works at Layer 1

a.k.a. Network Interface Controller

**Hub**

- Allows hosts to communicate with each other through the use of physical ports
- Connects segments of a LAN
- Traffic is broadcast to all ports of the hub, so all segments of the LAN can see all packets
- No path determination
- Works at Layer 1

**Modems**

- Modulator-Demodulator
- Device which enables a computer to transmit digital signals over analog telephone lines
- Short for modulator-demodulator
- Works at Layer 1

A modem converts the digital information in a computer into analog data. Traditional modems can operate at a top speed of 56Kbps, though most do not go that fast on today's phone lines.

Susceptible to war dialing on dial up modems in a company's network. War dialing is attacks were an individual runs an application that will dial all the phone numbers in a prefix range in order to identify modems. The can then focus their efforts on accessing the network via vulnerabilities with the modem.

---

**Layer 2 - Data Link Devices****Bridge**

- Connects network segments
  - Analyzes the information from each Ethernet frame it receives to determine delivery
  - Looks at the MAC address
  - Works at Layer 2
- 

**Switch**

- Connects multiple network segments
  - Improves network efficiency
  - Uses MAC addressing for delivery determination
  - Works at Layer 2
- 

**Switch Loop Protection**

- Prevents ports from moving into a forwarding state that would result in a loop opening up in the network
- Loops occur when there is more than one Layer 2 path between two endpoints
- Can bring down the network, Broadcast Storm, affecting availability
- Use spanning tree protocol (STP) on switches
  - Prevent loops in the LAN and selects the fastest network links
  - In the event that a link goes down, STP will failover to an alternate link

Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing ports from moving into a forwarding state that would result in a loop opening up in the network. A loop-free network in spanning-tree topologies is supported through the

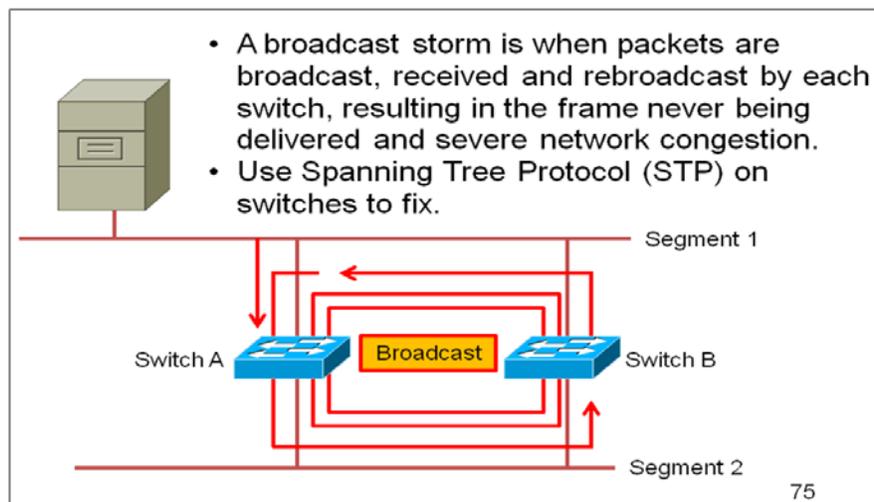
exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPDUs to communicate.

Ultimately, the exchange of BPDUs determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic.

However, a blocking interface can transition to the forwarding state in error if the interface stops receiving BPDUs from its designated port on the segment. Such a transition error can occur when there is a hardware error on the switch or software configuration error between the switch and its neighbor.

When loop protection is enabled, the spanning-tree topology detects root ports and blocked ports and makes sure both keep receiving BPDUs. If a loop-protection-enabled interface stops receiving BPDUs from its designated port, it reacts as it would react to a problem with the physical connection on this interface. It doesn't transition the interface to a forwarding state, but instead transitions it to a loop-inconsistent state. The interface recovers and then it transitions back to the spanning-tree blocking state as soon as it receives a BPDU.

## Switch Broadcast Storms



Example, imagine that Node B is connected to Switch A, and needs to communicate with Node A on Segment B. Switch A does not know who Node A is, so it floods the packet.

The packet travels via Segment A or Segment C to the other two switches (B and C). Switch B will add Node B to the lookup table it maintains for Segment A, while Switch C will add it to the lookup table for Segment C.

If neither switch has learned the address for Node A yet, they will flood Segment B looking for Node A. Each switch will take the packet sent by the other switch and flood it back out again immediately, since they still don't know who Node A is. Switch A will receive the packet from each segment and flood it back out on the other segment. This

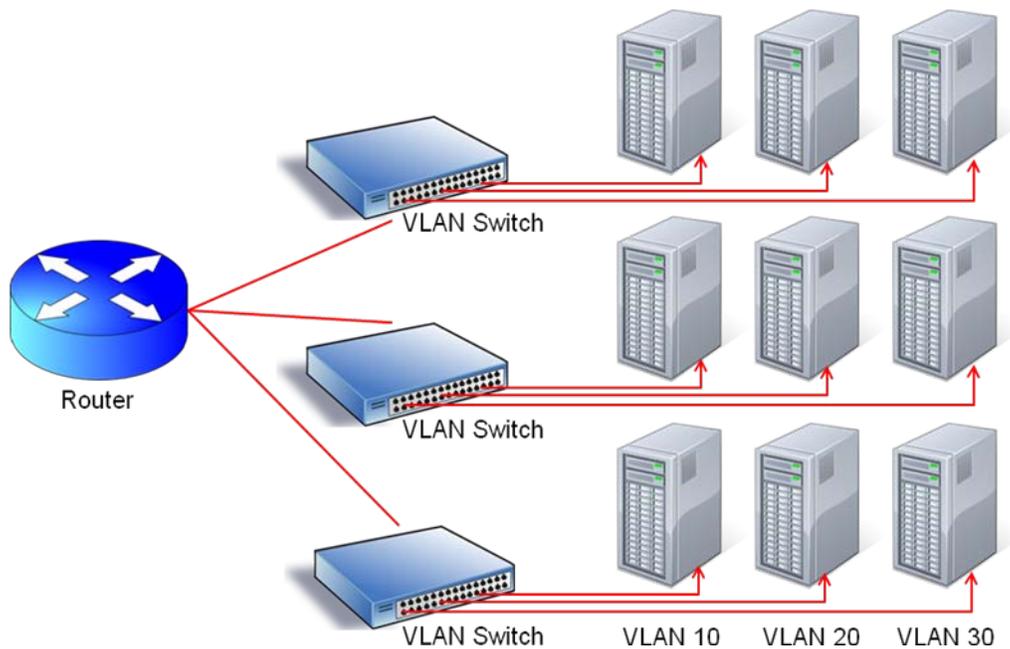
causes a broadcast storm as the packets are broadcast, received and rebroadcast by each switch, resulting in potentially severe network congestion.

### Virtual LAN (VLAN)

- Devices on the same physical network are divided into multiple logical networks
- Segments users or groups on a network
- Created using VLAN-capable switches
- Benefits:
  - Decreases broadcast traffic
  - Reduces traffic interception

A virtual local area network (VLAN) allows you to create groups of users and systems and segment them on the network. This segmentation lets you hide segments of the network from other segments and thereby control access. You can also set up VLANs to control the paths that data takes to get from one point to another. A VLAN is a good way to contain network traffic to a certain area in a network.

Shrinking the size of the LAN by segmenting it into smaller groups (VLANs) reduces the size of the broadcast domains. The advantages of doing this include reducing the scope of the broadcasts, improving performance and manageability, and decreasing dependence on the physical topology



## Layer 3 - Network Layer Devices

### Router

- Provides connectivity between two or more networks
- Routes packets based upon IP addressing
- Standard Protocols:
  - RIP (Routing Information Protocol)
  - BGP (Border Gateway Protocol)
  - OSPF (Open Shortest Path First)
- Works at Layer 3

Routers are intelligent devices, and they store information about the networks to which they're connected. Most routers can be configured to operate as packet filtering firewall and be used to translate from LAN framing to WAN framing (as a border router).

Routers establish communication by maintaining tables about destinations and local connections. A route contains information about the systems connected to it and where to send requests if the destination is not known.

**RIP:** Private Networks - A simple protocol that is part of the TCP/IP protocol suite. Routers use RIP to broadcast the status and routing information of known routers. RIP also finds routes between systems using the smallest number of hops or connections.

**OSPF:** Private Networks - Routing table information can be updated faster than with RIP.

**BGP:** Internet - Allows groups of routers to share routing information to ensure effective and efficient routing.

---

### Secure Router Configuration

- Establishing and documenting a router's configuration is the first step
- Perform the initial configuration from the console and back it up securely
- Change default settings
- Avoid using TFTP without SSL
- Save each configuration change and document all modifications

---

### Access Control List

- Rule based access control set on network device that regulate traffic
  - Can be applied to inbound/outbound traffic
  - Usually simple packet filtering that blocks traffic by:
    - Source and destination IP address
    - Port
    - Protocol
  - The last line is the implicit deny statement (Cisco)
-

**Cisco Standard ACL example**

```
access-list 1 permit 192.168.16.1 0.0.0.0
access-list 1 deny any
```

**Cisco Extended ACL example**

```
access-list 101 permit tcp any any eq http
access-list 101 deny tcp any any eq 23
access-list 101 deny ip any any
```

Standard ACL only filter by source IP. In the first example, packets only with the source ip address of 192.168.16.1 would be permitted (This would of course depend on whether it was applied inbound or outbound on the interface.). Line 2 would deny any other source ip addresses, this line does not need to be entered into the ACL because of the implicit deny statement, however some administrators do add it.

Extended ACL filter consist of; source and destination ip addresses, port and protocol. The first line will permit any source to any destination using http. The second line would deny any telnet connection and the third line would deny any ip protocols. These are just simple examples of some ACL's

**Firewalls and Services****Firewall Rules**

- Allow a computer to send traffic to, or receive traffic from, programs, system services, computers, or users
- Created for either inbound traffic or outbound traffic
- Casually take one of two actions
  - Allow/permit/accept
  - Block/deny/reject

**What is an inbound rule?**

Inbound rules explicitly allow, or explicitly block, inbound network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly allow traffic secured by IPsec for Remote Desktop through the firewall, but block the same traffic if it is not secured by IPsec. When Windows is first installed, all unsolicited inbound traffic is blocked. To allow a certain type of unsolicited inbound traffic, you must create an inbound rule that describes that traffic.

**What is an outbound rule?**

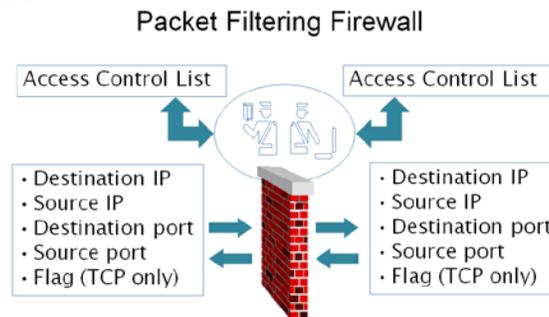
Outbound rules explicitly allow, or explicitly block, network traffic originating from the computer that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to a computer (by IP address) through the firewall, but allow the same traffic for other computers. Because outbound traffic is allowed by default, you typically use outbound rules to block network traffic that you do not want.

**Types of Firewalls**

## Packet Filtering Firewall

- Filters traffic to specific addresses based on the IP header of each packet that it receives
- Packets are compared against the ACL and will either be forwarded or dropped depending on the active policy
- Works at Layer 3

Example: One line in ACL states packets w/ IPs in the 172.168.00 range must be denied; another may not allow packets using Telnet; another may not permit traffic heading towards port 443.



## Stateful Inspection Firewall

- Tracks each TCP connection in a state table
- May examine the header information and/or the contents of the packet
- Filtering is based on rules and on context that has been established by prior packets
- Works at Layers 3 and 4
- a.k.a. Stateful packet filtering
- Maintains a state table. It looks at its state table to see if the connection has already been made. If no previous connection, then it looks at its ACL, else allows it.
- Once a connection has been allowed, stateful inspection continues to evaluate network packets to ensure that each packet is valid within the context of the connection.
- Stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid
- It also monitors the state of the connection and compiles the information in a state table



**Application Level Gateway**

- Acts as an Application Proxy
  - Traffic is evaluated by user, group policies, and content/protocol/application
  - Slowest form of a firewall
  - Works at Layer 7
- 

**Circuit Level Proxy**

- Monitors traffic between trusted and un-trusted hosts via virtual circuits or sessions
- Filtering is based on sessions rather than content of packets
- Works at Layer 5
- Evaluates the connections; doesn't deal with the contents of the packet
- PuTTY is an example of Circuit Level Proxy

It creates a circuit (connection) between the internal host and the outside server by acting as an agent without interpreting the application level information. It is more like a packet filter with the ability to hide the client. The advantage of circuit-level proxies is that they can be implemented with a large number of protocols as they don't have to comprehend the information at the protocol level. The disadvantage is that once a connection is established it is always possible to send malicious data in the packets.

---

**SOCKS**

- Network protocol designed to allow clients to communicate with Internet servers through firewall
- Proxy configuration option in popular Web browsers and instant messaging programs

**SOCKS V4 and SOCKS V5**

SOCKS is a protocol that can be used to create proxy connections through a firewall. Originally developed by David Koblas and Ying-Da Lee at NEC Systems Laboratory, SOCKS has been made a standard by a number of Request for Comments (RFC) documents and is widely used on the Internet.

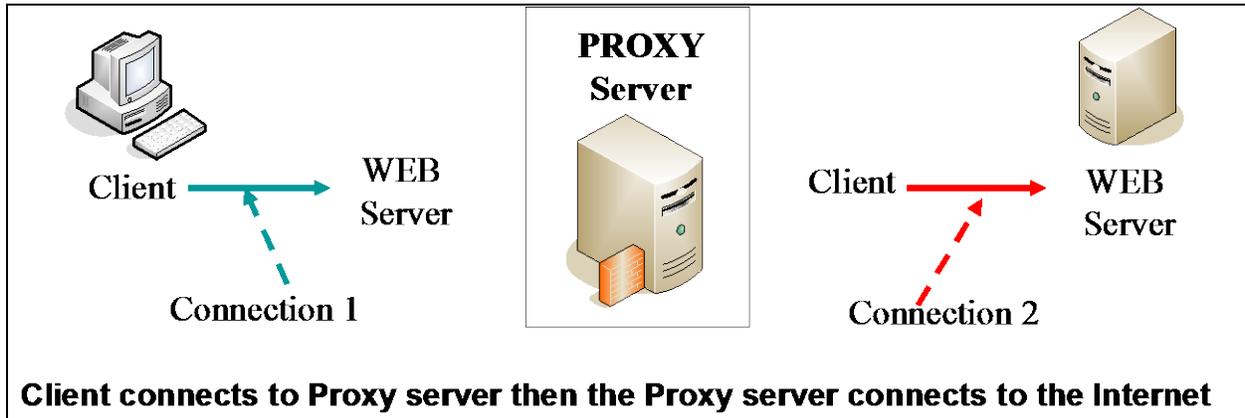
The SOCKS protocol can be used to allow a host on one side of the SOCKS server to interact with a host on the other side, subject to authentication, without passing IP packets directly between them.

Example:

Bill wishes to communicate with Jane over the internet, but a firewall exists on his network between them and Bill is not authorized to communicate through it himself. Therefore, he connects to the SOCKS proxy on his network and sends to it information about the connection he wishes to make to Jane. The SOCKS proxy opens a connection through the firewall and facilitates the communication between Bill and Jane.

## Proxy Server

- A border device used to protect security zones
- Can be configured to:
- Improve performance by caching content locally
- Use ACLs to filter content for inbound/outbound traffic



## Network Address Translation (NAT)

- Translates a private address into a public address
- Hides devices in a private network
- Allows sharing of a single public IP address or a pool of public IP addresses
- Types of NATs:
  - Dynamic NAT
  - Static NAT
  - Port Address NAT

The following address ranges have been reserved for use on private networks

Class A—10.0.0.0 to 10.255.255.255 (10.0.0.0/8)

Class B—172.16.0.0 to 172.31.255.255 (172.16.0.0/12)

Class C—192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

**Network Address Translation (NAT)** creates a unique opportunity to assist in the security of a network. Originally, NAT extended the number of usable Internet addresses. Now it allows an organization to present a single address to the Internet for all computer connections.

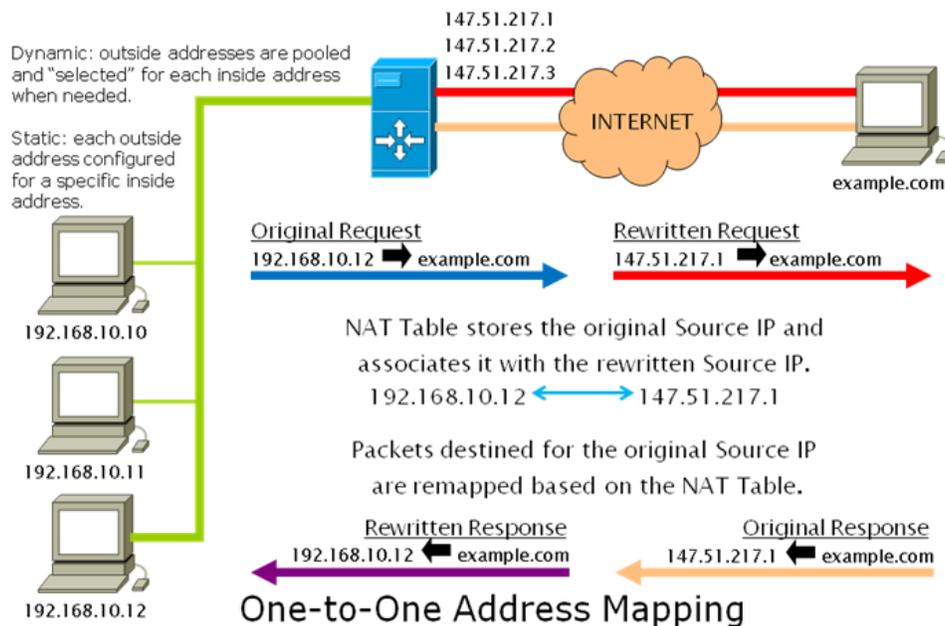
The NAT server/device provides IP addresses to the hosts or systems in the network and tracks inbound and outbound traffic. It presents a single connection to the network, so the connection may be through a router or a NAT server, but the only information that an intruder will be able to get is that the connection has a single address.

NAT effectively hides your network from the world, making it much harder to determine what systems exist on the other side of the router. The NAT server effectively operates as a firewall for the network.

Most NAT implementations assign internal hosts private IP address numbers and use public addresses only for the NAT to translate to and communicate with the outside world.

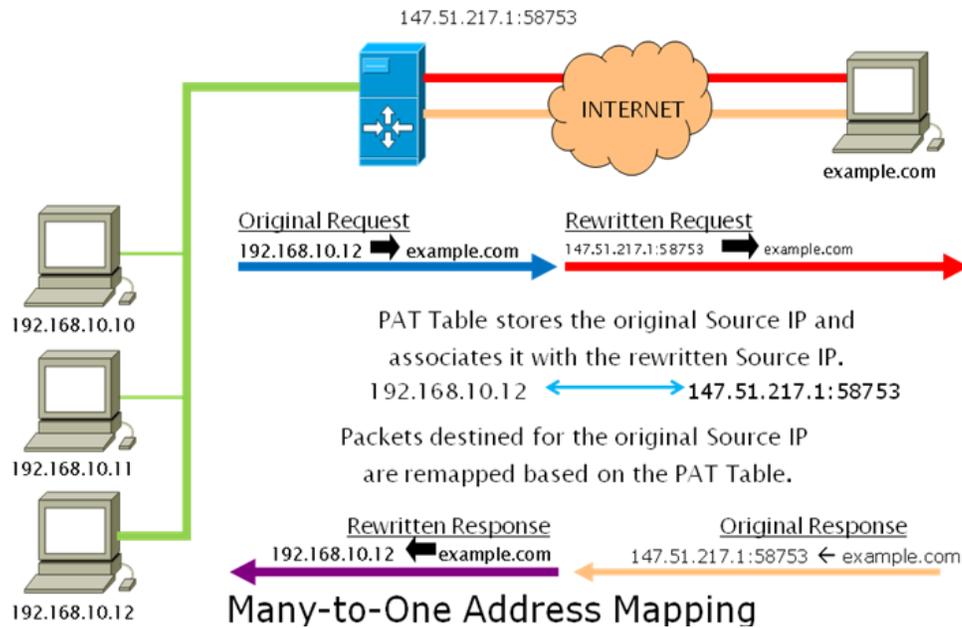
**Dynamic NAT:** A pool of public IP addresses is shared by an entire private IP subnet. Connections initiated by private hosts are assigned a public address from a pool

**Static NAT:** Accomplished by a straightforward, stateless implementation that transforms only the network part of the address, leaving the host part intact. The payload of the packet must also be considered during the translation process.



### Port Address Translation (PAT)

- Allows many hosts to share a single IP address by multiplexing streams differentiated by TCP/UDP port numbers
- Ports are selected at random for each inside address which generates a request



## Security Zones

- DMZ: contains public facing servers
  - Bastion hosts: any hardened system located in the DMZ (File Server, Web Server, etc.)
- Intranet: internal network to include systems and workstations you do not want anyone outside of your network to directly connect to.
- Extranet: segment of your network set aside for trusted partners, organizations
- Internet: unsecured security zone

The term security zone describes design methods that isolate systems from other systems or networks. You can isolate networks from each other using hardware and software.

You can configure some machines on the network to be in a certain address range and others to be in a different address range. This separation makes the two networks invisible to each other unless a router connects them. Some of the newer data switches also allow you to partition networks into smaller networks or private zones.

Security zone design is an important aspect of computer security. You can use many different approaches to accomplish a good solid design. Some of the design trade-offs involve risk and money. It's important to remember that after you have a good security design, you should revisit it on a regular basis based on what you learn about your security risks.

## VPN Concentrator

- A single device that handles large number of VPN tunnels
- Primarily used for remote access VPN's

- Usually two flavors; SSL or IPSec (some can do both, ie. Cisco)
- Examples:
  - Cisco
  - Netgear
  - Juniper

For a client to access the IPSec VPN, it must have the client-side software configured. While this adds security, it provides additional cost to implement and leads to additional time and energy spent, this is what leads many toward an SSL solution.

SSL is already built in to the capabilities of pretty much all computers through Web browsers. Thus, there is no additional work to install and configure the client side. In addition, rather than residing at the network layer, allowing access to all aspects of a network, SSL lets administrators allow access a bit more precisely toward applications that are Web-enabled. In addition, administrators can establish a finer level of control over users with SSL VPN connections.

On the negative angle, however, being that you can only utilize SSL VPNs through a Web browser, only Web-based applications will work. With a little bit of work, you can Web-enable additional applications, but this adds to the configuration time and may make SSL an unattractive solution for some.

---

### All in One Appliance

- Device that combines numerous security functions into one
- -Example:
  - Cisco Adaptive Security Appliances (ASA) 5500's
- ASA combines the
  - PIX firewall (Routing, ACL, NAT)
  - 4200 Series IPS (IPS functions)
  - 3000 Series VPN concentrator (VPN management)
- Also known as Unified Threat Management (UTM)

### Flood Guards

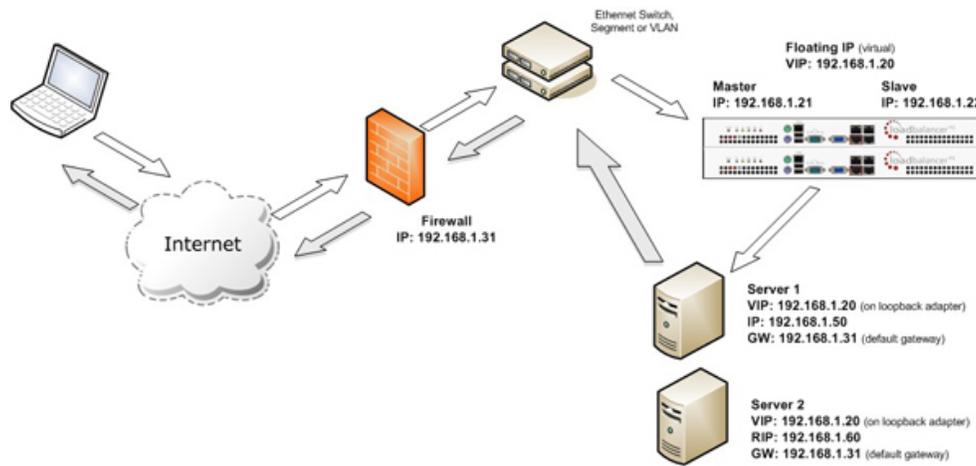
- A network device, firewall/router, that has the ability to prevent some flooding DoS attacks
- DoS attacks prevented could be
  - Fraggle
  - Smurf
  - Syn
  - Authentication DOS attacks
- Examples: Cisco's floodguard

## Layer 4 – Transport Layer Devices

### Load Balancers

- Used to distribute workload across multiple computers or network links
- Can be used to implement failover
- In the event of server or application failure, load balancers facilitate automatic failover to ensure continuous availability
- Can be hardware/software

Examples: Barracuda, Cisco, Foundry, F5



For Internet services, the load balancer is usually a software program that is listening on the port where external clients connect to access services. The load balancer forwards requests to one of the "backend" servers, which usually replies to the load balancer. This allows the load balancer to reply to the client without the client ever knowing about the internal separation of functions. It also prevents clients from contacting backend servers directly, which may have security benefits by hiding the structure of the internal network and preventing attacks on the kernel's network stack or unrelated services running on other ports.

Load balancing can be useful when dealing with redundant communications links. For example, a company may have multiple Internet connections ensuring network access even if one of the connections should fail.

A failover arrangement would mean that one link is designated for normal use, while the second link is used only if the first one fails.

With load balancing, both links can be in use all the time. A device or program decides which of the available links to send packets along, being careful not to send packets along any link if it has failed. The ability to use multiple links simultaneously increases the available bandwidth.

---

**Load Balancing - Server Clustering / Failover Cluster** - A failover cluster is a group of independent computers that work together to increase the availability of applications and services. The clustered servers (called nodes) are connected by physical cables and by software. If one of the cluster nodes fails, another node begins to provide service (a process known as failover). Users experience a minimum of disruptions in service.

---

## Layer 7 - Application Layer Devices

**Internet Content Filters** (Content-control software or Web Filtering Software)

- Filters content permitted by a user
- By URLs, Content, and Certificates
  
- Pros:
  - Prevents employees from viewing inappropriate websites
- Cons:
  - Can incorrectly block legitimate websites

---

**Web Security Gateway / Proxy**

- Maximizes security by detecting, filtering and blocking web threats
- Inspects all content in transit while remaining transparent to users
- Detects malware (viruses, spyware, adware)
- Filters URL content
- Some offer data leakage protection (DLP)
- Examples:
  - Websense
  - Bluecoat
- **Data Leakage Prevention (DLP):** Inspection of outbound communications for sensitive/confidential data, even when hiding in HTTPS connections.

Web security gateways combine several existing technologies and features offered by point solutions. Instead of having separate devices for URL filtering, malicious code filtering, instant messaging and other application controls, Web security gateways provide a single high-performance security gateway that shares a common threat database and policy management framework. The Web security gateway market is a mix of software and appliance vendors as well as managed service providers.

A Web security gateway is a multifunction solution that filters unwanted software and malware from user-initiated Internet traffic while enforcing corporate policy compliance. To accomplish this, Web security gateways use URL filtering, malicious code detection and filtering, and controls for Web-based applications such as IM and Skype. It's important to clarify the purpose of a Web security gateway: to protect clients on the internal network and their users from infection while surfing the Web and enforce company policies.

---

## Cloud Computing

- Software, data access, and storage services that do not require user knowledge of the location and configuration of the system delivering services
- Computing is "in the cloud" (internet)
- Three layers
  - Software as a Service(application)
  - Platform as a Service(platform)
  - Infrastructure as a Service(infrastructure)
- Example: web based e-mail like Yahoo or Hotmail, ISP's

The key characteristic of cloud computing is that the computing is "in the cloud" (internet) i.e. the processing (and the related data) is not in a specified, known or static place(s). This is in contrast to a model in which the processing takes place in one or more specific servers that are known.

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.

The term "cloud" is used as a metaphor for the Internet, based on the cloud drawing used in the past to represent the telephone network, and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents. Typical cloud computing providers deliver common business applications online that are accessed from another Web service or software like a Web browser, while the software and data are stored on servers.

Most cloud computing infrastructures consist of services delivered through common centers and built on servers. Clouds often appear as single points of access for consumers' computing needs. Commercial offerings are generally expected to meet quality of service (QoS) requirements of customers, and typically include service level agreements (SLAs).

---

## Software as a Service

- Software as a service over the Internet
- Eliminates the need to install/run applications on customer's computers
- No local software applications needed (just web site connectivity)

## Platform as a Service

- Facilitates deployment of applications reducing cost and complexity
- Vendors allow apps to be created and run on their infrastructure

### **Infrastructure as a Service**

- Typically a platform virtualization environment
- Clients purchase resources/services (servers, software, certain network devices, data center space)

**Software as a Service**-sometimes referred to as "software on demand," is software that is deployed over the internet and/or is deployed to run behind a firewall on a local area network or personal computer. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, in a "pay-as-you-go" model, or (increasingly) at no charge when there is opportunity to generate revenue from streams other than the user, such as from advertisement or user list sales. This approach to application delivery is part of the utility computing model where all of the technology is in the "cloud" accessed over the Internet as a service.

**Platform as a Service**-the delivery of a computing platform and solution stack as a service. PaaS offerings facilitate deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities, providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet. PaaS provides all the infrastructure needed to run applications over the Internet. It is delivered in the same way as a utility like electricity or water. Users simply "tap in" and take what they need without worrying about the complexity behind the scenes. And like a utility, PaaS is based on a metering or subscription model so users only pay for what they use.

**Infrastructure as a Service**-a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

---

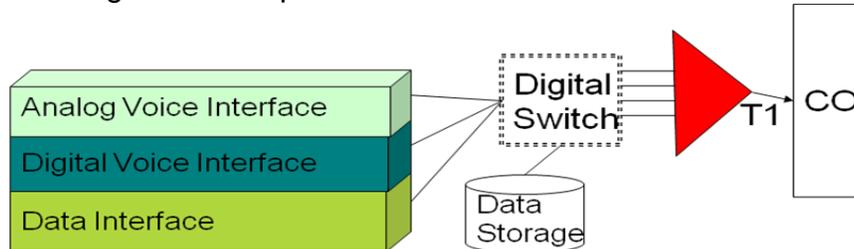
### **Cloud Computing Vulnerabilities**

- All Your Eggs in One Basket
    - Example: you or the cloud provider lose network connectivity
  - Reliance on Passwords
    - Any account is only as secure as the password used to access it
    - User locking account could be issue, you don't have the same capabilities you would locally
  - Encrypting Data in the Cloud
    - Virtual machines don't always use random numbers needed to properly encrypt data
-

## Telephone Security

### Telecom/PBX

- Private Branch Exchange (PBX)
- Allow users to connect voice, data, pagers, networks
- Subject to the similar issues associated with network components
- Phreaker
- Network Design and Components



### Dealing with Telephony Issues

Telephone Technology + Information Technology = Telephony

When telephone technology is married with information technology, the result is known as telephony. A breach in your telephony infrastructure is just as devastating as any other violation and can lead to the loss of valuable data.

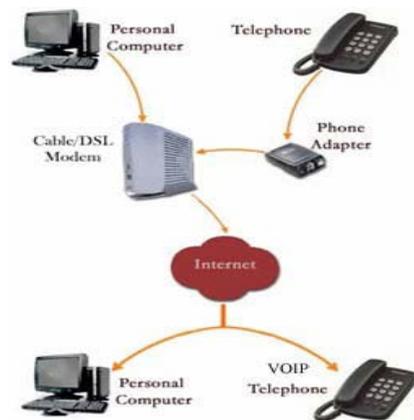
### Private Branch Exchange (PBX) security implementations

- Replace remote access or long distance calling with credit/calling card systems
- Restrict dial in and dial out features
- Disable unassigned accounts
- Create an AUP and train users properly
- Maintain physical access controls to all closets, and connection centers
- Log and audit all activities
- Change all default configurations

### VoIP (Voice over IP)

- VoIP services convert your voice into a digital signal that travels over the Internet
- Establish a IP Phone VLAN
- Use Voice Firewalls

Voice over IP (VoIP) converts the voice signal from your telephone into a digital signal that can travel over the Internet. If you are calling a regular telephone number, the signal is then converted back at the other end.



## Network Security Tools

**Network monitoring:** The process of using a data-capturing device or other method to intercept information from a network.

---

### Intrusion Detection Systems (IDS)

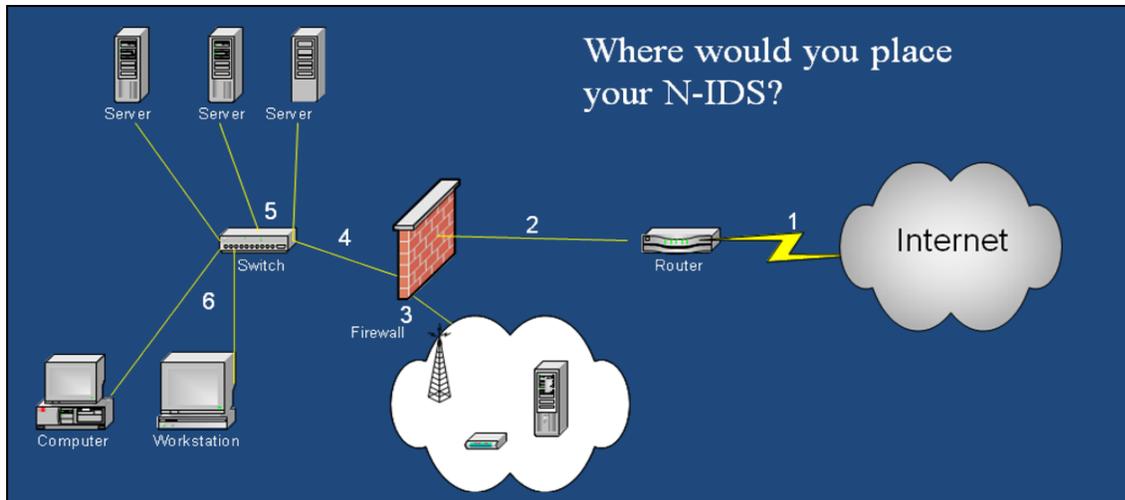
- Monitoring system which collects and analyzes traffic
  - Used to Detect:
    - Attacks coming from outside the network
    - Attacks and misuse from within the network
  - IDS Types:
    - Network Based
    - Host Based
- 

### IDS Terms

- Administrator: Person responsible for setting the security policy for an organization; makes decisions about the deployment and configuration of the IDS
  - Alert: Message from the analyzer indicating that an event of interest has occurred
  - Analyzer: The component or process that analyzes the data collected by the sensor
  - Data Source: The raw information that the IDS uses to detect suspicious activity
  - Event: An occurrence in a data source that indicates that a suspicious activity has occurred
  - Manager: The component or process the operator uses to manage the IDS (the IDS console is a manager)
  - Notification: The process or method by which the IDS manager makes the operator aware of an alert
  - Operator: The person primarily responsible for the IDS
  - Sensor: The IDS component that collects data from the data source and passes it to the analyzer for analysis
- 

### Network IDS (NIDS)

- Monitor's network traffic in real time
  - Particularly suited for detecting port scanning and DoS attacks
  - Analyzes protocols and other relevant packet information
  - Can send alerts or terminates connections
  - Cannot analyze encrypted traffic
  - Sensors are deployed and usually report back to a system running a management console
  - Systems with sensor application installed are usually dual homed
-



### Network IDS Placement

- Attach the system on the network segment where it can monitor all network traffic
- Placement in front of the firewall allows you to monitor all the traffic going into the network
  - Requires a huge amount of data to be processed
- Placement behind the firewall allows you to see the traffic that penetrates the firewall

### Host IDS (HIDS)

- Installed on a host
- Detects attacks against the host and the level of their success
- Relies on the auditing and logging capabilities of the operating system
- Can view encrypted data in transit
- Is detectable and can be a target of attack

A host-based IDS is installed on a host and monitors all traffic coming into the host (anti-virus software is the most common form of host-based IDS). Host-based IDSs monitor the activity only on the host that it is installed on. It does not monitor any other network devices.

Host-based IDSs examine the machine logs, system events, and applications interactions; they normally don't monitor incoming network traffic to the host. Host-based IDSs are popular on servers that use encrypted channels or channels to other servers.

Two major problems with Host-based IDSs are not easily overcome. The first problem involves a compromise of the system. If the system is compromised, the log files the IDS reports to may become corrupt or inaccurate. This may make fault determination difficult or the system unreliable. The second major problem with Host-based IDSs is that it must be deployed on each system that *needs* it. This can create a headache for administrative and support staff.

One of Host-based IDS's major benefits is the potential to keep checksums on files. These checksums can be used to inform system administrators that files have been altered by an attack. Recovery is simplified because it's easier to determine where tampering has occurred.

Host-based IDSs typically respond in a passive manner to an incident. An active response would theoretically be similar to those provided by network-based IDS.

---

### **Passive IDS**

- Looks for security breaches, but effectively takes no action
- Logs suspicious activity
- Generates alerts if the attack is deemed to be severe
- The network analyst interprets the degree of the threat and responds accordingly

### **Active IDS**

- Can be configured to take specific actions
- Can automate responses including dynamic policy adjustment and reconfiguration of supporting network devices

### **Passive vs. Active**

An Intrusion Detection System (IDS) is software that runs on either individual workstations or network devices to monitor and track network activity. By using an IDS, a network administrator can configure the system to respond just like a burglar alarm. An IDS can be configured to evaluate systems logs, look at suspicious network activity, and disconnect sessions that appear to violate security settings.

Firewalls by themselves will prevent many common attacks, but they do not usually have the intelligence or the reporting capabilities to monitor the entire network. An IDS, in conjunction with a firewall, allows both a reactive posture with the firewall and a preventive posture with the IDS.

---

### **IDS Methods**

- Signature-based
    - a.k.a. Misuse-Detection MD-IDS, Knowledge-based, and Rule-based
    - Evaluates attacks based on a database of signatures written by the vendor
  - Anomaly-based or (Heuristic)
    - a.k.a. Behavior based and Statistical-based
    - Looks for unexpected events
    - Must learn what activities are normal and acceptable
- 

### **IDS Issues**

- False Positives
  - IDS reports legitimate activity as an intrusion
- False Negatives
  - IDS fails to detect malicious network activity

- Caused by:
  - New attacks not yet identified by vendor
  - Poorly written signatures
  - Outdated signature files

---

### **Intrusion Prevention Systems (IPS)**

- Monitors network traffic for malicious activity and can block, reject, or redirect traffic in real time
- Focuses on prevention as opposed to detection
- Encrypted traffic is not inspected

---

### **IDS/IPS Clipping Levels**

- Thresholds placed on certain activities
- Keeps the number of false readings to a minimum
- Example:
  - Failed logon attempts to the admin account will not be reported, unless it occurs three times in a row over a short period of time

---

### **Network Access Control (NAC)**

- Evaluates system security status before connecting to the network
- Anti-virus status
- System update level
- Configuration settings
- Software firewall enabled

NAC examines the current state of a system or network device before it is allowed to connect to the network. The goal of NAC is to prevent computers with suboptimal security from potentially infecting other systems in the network.

---

## **Wireless Networking**

Wireless systems, plainly put, are systems that don't use wires to send information, but rather transmit it through the air. The growth of wireless systems creates several opportunities for attackers. These systems are relatively new, they use well-established communications mechanisms, and they are easily intercepted.

### **802.11? Wireless Protocols**

- Four major wireless standards
  - 802.11 Wireless Local Area Network (WLAN)
  - 802.15 Wireless Personal Area Network (WPAN)
    - Bluetooth is an implementation of WPAN
  - 802.16 Wireless Metropolitan Area Network (WMAN)

## Wireless Networking

- IEEE 802.11x working group
  - 802.11x is a term used to denote current of future 802.11 amendments (i.e. 802.11a or 802.11b)
- SSID used for network identification
  - Broadcast vs. Non-broadcast
- Association
  - Once authentication is complete, mobile devices can associate (register) with an AP/router to gain full access to the network. Association allows the AP/router to record each mobile device so that frames may be properly delivered.

---

## Wireless Networking Cont...

- Uses radio waves to transmit data
  - Other wireless Methods: infrared, satellite
- Wireless networking is not considered a form of remote access
- Uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - CSMA/CA: a station wishing to transmit has to first listen to the channel for a predetermined amount of time, so as to check for any activity on the channel. If the channel is sensed "idle," then the station is permitted to transmit. If the channel is sensed as "busy," the station has to defer its transmission.
  - One of the problems of wireless LANS is that it is not possible to listen while sending, therefore collision detection is not possible.

---

## Wireless LAN Communication

- DSSS (Direct Sequence Spread Spectrum)
  - Generates redundant bit patterns to ensure accuracy over multiple frequencies
  - Spreads data over multiple frequencies (for higher throughput) and is more vulnerable to interference from EM devices. It is faster than FHSS
- FHSS (Frequency Hopping Spread Spectrum)
  - Changes frequency in a pattern known to both transmitter and receiver
  - Moves from one frequency to another; to an unintended receiver, FHSS appears to be short-duration impulse noise
- OFDM (Orthogonal Frequency Division Multiplexing)
  - Breaks data into sub-signals and transmits them simultaneously
  - Transmissions occur on different frequencies or sub-bands

---

## Common Wireless 802.11 Standards

Protocol	Speed	Frequency	Distance I/O
802.11a	54 Mbps	5 GHz	50-100 feet
802.11b	11 Mbps	2.4 GHz	150-300 feet
802.11g	54 Mbps	2.4 GHz	150-300 feet
802.11n	600 Mbps	2.4/5 GHz	300-600 feet

---

### WLAN Security

- Avoid WEP, use WPA (TKIP w/RC4) or WPA2 (CCMP w/ AES)
    - CCMP-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol CCMP uses the Advanced Encryption Standard (AES) algorithm. Unlike in
    - TKIP, key management and message integrity is handled by a single component built around AES using a 128-bit key, a 128-bit block, and 10 rounds of encoding per the FIPS 197 standard.
  - Deploy EAP with 802.1x authentication
  - MAC filtering and disabling SSID broadcast
    - MAC Filtering and disabling the SSID will not completely secure the AP. MAC filters can be spoofed and SSID can be found in probe packets.
  - Antenna placement and power level controls
    - The access point needs to be physically secure and you want to place it where it will cover the intended area. The power level needs to be attenuated so that the signal does not reach outside of your facility. This is a difficult task as most hackers/war drivers will use powerful antennas that still may discover the access point.
- 

### Wired Equivalent Privacy (WEP)

- Intended to provide the equivalent security of a wired network protocol
    - It was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.
  - Encrypts data using RC4 algorithm
    - WEP uses the RC4 symmetric algorithm that utilizes a combination of secret user keys and system-generated values. The original implementations of WEP supported so-called 40-bit encryption, having a key of length 40 bits and 24 additional bits of system-generated data (64 bits total). Research has shown that 40-bit WEP encryption is too easy to break, and consequently product vendors today employ 128-bit encryption (having a key length of 104 bits, not 128 bits) or better (including 152-bit and 256-bit WEP systems).
-

- There are two WEP types of authentication:
  - **Open system authentication** (or null authentication) - access is freely granted

The following steps occur when two devices use Open System Authentication:

1. The **client sends an authentication request** to the access point.
2. The **access point authenticates** the client.
3. The **client associates** with the access point and joins the network.

After the authentication the WEP key is then used to encrypt the data traffic.

- **Shared key authentication** - each station uses a shared secret key

In Shared Key authentication, the WEP key is used for authentication in a four step challenge-response handshake:

1. The client sends an authentication request to the Access Point.
2. The **Access Point** replies with a **clear-text challenge**.
3. The **client encrypts** the **challenge-text** using the configured **WEP shared key** and sends it back in another authentication request.
4. The **Access Point decrypts the response**. If the decrypted challenge-text **matches** the challenge-text the Access Point sends back **authentication will be granted**.

Using WEP, either open system or shared key is recommended because of the weakness of WEP. Open is more secure than shared key authentication. Shared key authentication uses the challenge-response handshake which exposes the WEP key to reverse engineering. It is possible to derive the keystream used for the handshake by capturing the challenge frames in Shared Key authentication.

---

### WEP Problems

- Static keys: Acquire enough keystream (IV and key) allows for cracking of the WEP key
- Allows IV space will be reused throughout the same wireless session
  - IV too short at 24 bit
- Integrity Check Value (ICV) uses Cyclic Redundancy Check (CRC-32 8-chr hash)
  - Relatively weak and payload could be modified without detection
- Key lengths are small (40 bit or 104 bit)
- No protection from replay attacks

---

### IV attacks

- IV is the main weakness in WEP
- Randomization is crucial for encryption schemes to achieve security
- Weakness in the IV process can lead to certain algorithms being more susceptible to attacks (brute force, dictionary)

An initialization vector (IV) is a block of bits that is used to randomize the encryption and hence to produce distinct ciphertexts even if the same plaintext is encrypted multiple times, without the need for a slower re-keying process

WEP uses a short, 24-bit IV, leading to reused IVs with the same key, which led to it being easily cracked. Packet injection allowed for WEP to be cracked in times as short as several seconds. This ultimately led to WEP being considered broken. Such a small space of initialization vectors guarantees the reuse of the same key stream. A busy access point, which constantly sends 1500 byte packets at 11Mbps, will exhaust the space of IVs after 5 hours.

---

### Wi-Fi Protected Access (WPA)

- Created to address core issues with WEP
- WPA implements most of IEEE 802.11i which specifies security mechanisms for wireless networks
- WPA Enhancements:
  - **Dynamic Keys:** Per-user, per-frame keying based upon the key-mixing input: sends MAC address, TSC, and temporal key (Temporal Key Integrity Protocol (TKIP))
  - **Per-frame sequence counter:** Drops frames received out of order. Mitigates replay attacks
  - **Larger IV:** TSC/IV value change with each frame sent, dynamic component to the key mixing process It is extremely unlikely that the IV space will be exhausted.
  - **Message Integrity Code (MIC):** More secure in addition to the payload, the destination and source address are protected. Frames that fail IC are dropped. MIC failures are logged. Two failures in 60 second shuts down the reception of TKIP messages for 60 second periods.

**WPA** is a security technology for wireless networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). In fact, WPA was developed by the networking industry in response to the shortcomings of WEP. One of the key technologies behind WPA is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the encryption weaknesses of WEP. Another key component of WPA is built-in authentication that WEP does not offer. With this feature, WPA provides roughly comparable security to VPN tunneling with WEP, with the benefit of easier administration and use.

---

### 802.11i - Specifies *Security Mechanisms* for Wireless Networks

#### Wi-Fi Protected Access 2 (WPA2)

- Implements the full IEEE 802.11i standard
- Mandatory to be Wi-Fi certified
- National Institute of Standards and Technology (NIST) FIPS 140-2 compliant
- Uses AES encryption

- Two versions:
    - **WPA2-Personal** - protects unauthorized network access by utilizing a set-up password.
    - **WPA2-Enterprise** - verifies network users through a server. WPA2 is backward compatible with WPA. WPA-2 uses the 802.1 X/EAP frameworks as part of the infrastructure that ensures centralized mutual authentication and dynamic key management and offers a pre-shared key for use in home and small office environments.
- 

### **Wireless Application Protocol (WAP)**

- Commonly used in small mobile devices such as cell phones that have a web browser
- Functions are equivalent to TCP/IP Suite
- “Gap in the WAP”
  - WAP 2.0 fixes decryption issue

The WAP Gap is the result of the necessity of the WAP gateway having to decrypt WTLS (Wireless Transport Layer Security) transmissions and then re-encrypting them using TLS/SSL, this means that data is exposed as it traverses the WAP gateway.

WAP 2.0 fixes this problem by eliminating WTLS and replacing it with TLS (Transport Layer Security) on the wireless device. The translation process is no longer required. In WAP 2.0, all data remains encrypted as it passes through the gateway.

---

### **WAP 1.x Stack**

- Wireless Application Environment (WAE)
  - Wireless Session Protocol (WSP)
  - Wireless Transaction Protocol (WTP)
  - Wireless Transport Layer Security (WTLS)
  - Wireless Datagram Protocol (WDP)
  - Uses Wireless Markup Language (WML)
    - a smaller version of HTML (for internet displays)
- 

### **Wireless Transport Layer Security (WTLS)**

- Security layer for WAP applications
  - Provides authentication, encryption, and data integrity for wireless devices:
    - Class 1: Anonymous Authentication
    - Class 2: Server Authentication
    - Class 3: Mutual Client/Server Authentication
  - Used in the older versions of WAP (1.x)
  - Current devices use TLS (due to the “Gap”)
-

## Analyze and differentiate among types of wireless attacks

### Wireless Vulnerabilities

The most common threat of a wireless network comes from eavesdropping

#### Rogue Access Points:

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a cracker to conduct a man-in-the-middle attack.

Prior to deploying a wireless network, you should conduct a site survey. The site survey looks for advantages and problems with the wireless network and its surroundings.

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a cracker to conduct a man-in-the-middle attack.

---

### Discovering Rogue Access Points

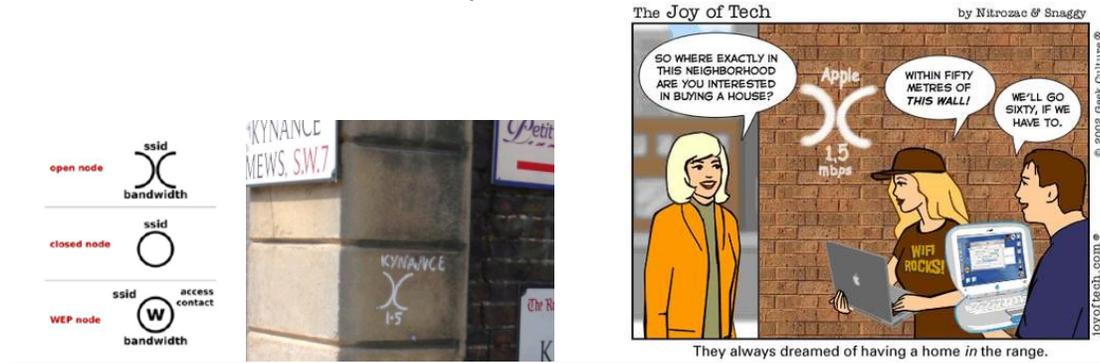
#### War Driving Tools

- NetStumbler
- Kismet
- AirSnort
- Flying Squirrel
- Comparing with known internal MAC addresses
- Hackers drive past businesses and residential areas looking for open wireless access points.
- Driving around looking for Wireless Access Points.



## War Chalking

War Chalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the war chalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. Those offering Wi-Fi service might also draw such a symbol to advertise the availability of their Wi-Fi location, whether commercial or personal.



## Interference

Degradation in range or throughput of your wireless device by something else in the footprint

Caused by:

- Microwave ovens: Using your microwave oven near your computer, Bluetooth device, or Wi-Fi base station may cause interference.
- Certain external electrical sources such as power lines, electrical railroad tracks, and power stations.
- Wireless phones 2.4 GHz or 5 GHz: A cordless telephone that operates in this range may cause interference with wireless devices or networks when used.
- Video senders (transmitters/receivers) that operate in the 2.4 GHz or 5 GHz bandwidth.
- Wireless speakers that operate in the 2.4 GHz or 5 GHz band.
- Certain external monitors and LCD displays: Certain displays may emit harmonic interference, especially in the 2.4GHz band between channels 11 and 14. This interference may be at its worst if you have a portable computer with the lid closed and an external monitor connected to it. Try changing your access point to use 5 Ghz or a lower 2.4 GHz channel.
- Any other "wireless" devices that operate in the 2.4 GHz or 5 GHz bandwidth (microwaves, cameras, baby monitors, neighbors wireless devices, and so on).
- A hacker conducting a Dos attack against the wireless network

### Interference may result in:

- A decrease in wireless range between devices.
- A decrease in data throughput over a Wi-Fi network.
- Intermittent or complete loss of connection.
- Difficulty during the discovery phase when pairing Bluetooth devices.

### Mitigations

- Consider changing the channel up or down
  - Consider purchasing an 802.11 n router
  - Choose a cordless phone that uses the 5.8-GHz, 1.9-GHz, or 900-megahertz (MHz) band
- 

### Evil Twin

The act of configuring a laptop as an access point in a public environment

- Usually set up near free hotspots (airports, cafés, hotels or libraries)
- Configured to pass data through to the legitimate access point while monitoring the traffic of the victim
- Attacker can eavesdrop; possibly collect usernames and passwords, etc.

Evil Twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications.

This type of attack may be used by a hacker to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent Web site and luring people there.

By imitating the name of another, legitimate wireless device, they can fool people into trusting the internet services that they are providing. When the users log into bank or e-mail accounts the attacker has access to the entire transaction, since it is sent through their equipment.

Hackers typically setup Evil twin attacks near free hotspots, such as airports, cafes, near student residences, hotels or libraries.

---

### Bluetooth Vulnerabilities

- Discovery Mode Attacks
  - Many devices are left in pairing/discoverable mode and default PIN/code is not changed;
  - Leaves device open and visible to other devices
- Older Bluetooth systems (pre 2007) are equipped with "auto pairing" and have a PIN that cannot be changed

When a Bluetooth device is discoverable, it is very easy to scan for it using a PC and download private data. This approach can easily contribute to some high profile attacks on celebrities and famous people, who often do not understand the Bluetooth technology.

Setting Bluetooth to a "non-discoverable" mode prevents BT devices from appearing on the list during a BT device search process. However, it is still visible to those devices and users who are familiar with its Bluetooth MAC address, which would be the case for previously paired devices (devices that have communicated with each other at least once before).

Malicious hackers benefit from mobile phone owners who simply keep their Bluetooth devices in discoverable mode. This happens most often because one mobile phone is required to be in discoverable mode before pairing with a new device. Often device owners simply forget to disable the discoverable mode afterwards - it is very easy to do. Or more likely, they simply do not understand what discoverable mode is.

---

### **Bluebugging**

- Taking control of a Bluetooth device for personal gain (phone calls, etc.)

Manipulates a target phone into compromising its security, this to create a backdoor attack before returning control of the phone to its owner. Once control of a phone has been established, it is used to call back the hacker who is then able to listen-in to conversations.

The Bluebug program also has the capability to create a call forwarding application whereby the hacker receives calls intended for the target phone.

Under ideal conditions, a BlueBug attack takes only a few seconds (depending on the things, which are done during the attack). Due to the limited transmit power of class 2 bluetooth radios, the distance of the victim's device to the attacker's device during the attack should not exceed 10-15 meters. Similar to wardriving, also for bluetoothing a directional antenna can be attached to the radio in order to increase the range. Since the BlueBug security loophole allows you to issue AT commands via a covert channel to the vulnerable phones without prompting the owner of the phone, this security flaw does allow a vast number of things that may be done when the phone is attacked via bluetooth:

- Initiating phone calls
- Sending SMS to any number
- Reading SMS from the phone
- Reading phonebook entries
- Writing phonebook entries
- Setting call forwards
- Connecting to the internet
- Forcing the phone to use a certain service provider

### **Bluejacking**

- Sending of unsolicited messages over Bluetooth

BlueJacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers. BlueJacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacked will only send a text message, but with modern phones it's possible to send images or sounds as well.

## Bluesnarfing

- Theft of information from a wireless device through a Bluetooth connection

Bluesnarfing is the unauthorized access of information through a wireless device, using a Bluetooth connection. This allows access to a calendar, contact list, emails and text messages and on some phones users can copy pictures and private videos.

Bluetooth Sniper Rifle: Can perform attacks using this device from up to 1 Km.

---

The BlueJacking was initiated from a different pocket PC device, running a simple tool which is capable of searching for remote devices that are in discoverable mode. To be subject to this attack, a device doesn't need to be in discoverable mode, then the tool allows the user to define a custom message that gets set as the Bluetooth Device Name.

---

## Packet Sniffing

- Captures all of the data that pass through a given network interface
  - Promiscuous Mode: sniffer is capable of capturing ALL packets traversing the network
  - Possible to capture both wireless and wired packets
  - Can capture and read plaintext data
  - Tools:
    - Wireshark
    - tcpdump
    - ettercap
    - Cain and Able
    - snoop,
    - netstumbler
    - kismet
- 

## Wireless Vulnerabilities Mitigations

- Employ mutual authentication and encryption
- Detect Rogue Access Points
- Perform Site Surveys
- Disable SSID Broadcast
- Change default SSID
- Change default password
- Use strong encryption

## Site Survey

Prior to deploying a wireless network, you should conduct a site survey. The site survey looks for advantages and problems with the wireless network and its surroundings.

*For example:* The site survey might look for physical obstructions or interference sources that might impede communications. It also examines the physical location to

determine the best location for wireless access points for area coverage, signal strength, and security.

When implementing a wireless network, consider the following recommendations:

- Implement some form of encryption to protect wireless communications.
- Do not locate a wireless access point against a perimeter wall. This extends the wireless signal past the physical boundary of your location, making it possible for persons on the outside to detect and connect to the wireless network.

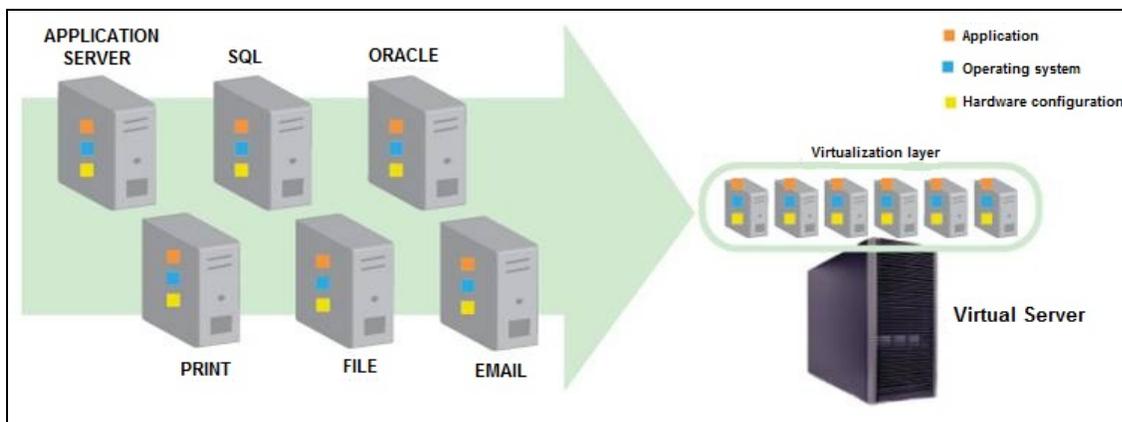
### Service set Identifiers, or SSIDs

A client device will receive broadcast messages from all access points within range advertising their SSIDs

This method prevents casual detection of the network; it is not secure against determined hackers, because every time someone connects to the network, the SSID is transmitted in clear text so an eavesdropper can passively sniff the wireless traffic.

## Virtualization Technology

- Multiple instances of operating systems on one machine
- Virtualized environments are used to help secure networks
- Controlled by Hypervisor
- Examples: VMware, Virtual PC



### Types of Hypervisor

- **Type 1 (or native, bare-metal)**
  - Hypervisors are software systems that run directly on the host's hardware to control the hardware and to monitor guest operating-systems.
  - *Examples: ESX, ESXI*
- **Type 2 (or hosted)**
  - Hypervisors are software applications running within a conventional operating-system environment.
  - *Examples: V-PC, VMware player*

### **Benefits**

- Virus-If a workstation in a virtualized environment is infected with a virus, that virus will be contained in that virtual machine and not affect the host or other virtual systems on the host.
- [http://download.parallels.net/resources/whitepapers/Virus\\_Protection\\_White\\_Paper.pdf](http://download.parallels.net/resources/whitepapers/Virus_Protection_White_Paper.pdf)
- Risk-Because of the use of virtual machines, research can be conducted with little to no risk to the equipment and surrounding environments.
- Cost-savings are due to reduced hardware, utilities (electricity and environmental controls), etc.

### **Vulnerabilities**

- The biggest issue with virtual machines is the host itself.
- If it gets attacked and brought down then all virtual machines and their services will also come down.
- The host must be protected at all cost.
- Single point of failure for all VM's

## Domain 3 – Access Control and Identity Management

### A Security+ candidate is expected to:

- Explain the function and purpose of authentication services
- Explain the fundamental concepts and best practices related to authentication, authorization and access control
- Implement appropriate security controls when performing account management

---

### Explain the fundamental concepts and best practices related to authentication, authorization and access control

#### Identification vs. Authentication

- Security of system resources follows a three-step process of Authentication, Authorization, and Accounting (AAA)
- Begins with identification of the entity seeking access to secured systems
  - Identification
  - Authentication

Security of system resources generally follows a three-step process of authentication, authorization, and accounting (AAA). This AAA model begins with positive identification of the person or system seeking access to secured information or services (authentication). That person is granted a predetermined level of access to the resources (authorization), and the use of each asset is then logged (accounting). The most critical step in the process is authentication. Without a positive identification, other steps are worthless, because they cannot distinguish between the authorized user and an imposter.

---

#### Identification

- Process of identifying an entity for authentication
- User Identification Guidelines
- Uniqueness
- Non-descriptive
- Issuance secure
- Most common forms:
  - User Name, User ID, Account Number

An entity must provide an identity to start the process of authentication, authorization, and accountability (username, smartcard, or biometrics).

#### User Identification Guidelines:

- **Uniqueness:** User identification must be unique identifier to provide positive identification.

- **Non-descriptive:** User identification should not expose the associated role or job function of the user.
  - **Issuance:** The process of issuing identifiers must be secure and documented.
- 

### Authentication

- Reconciliation of a user's identity
- Accomplished by challenging the claim about who is accessing the resource
- Authentication systems are based on one or more of these three factors:
  - *Something you know*
  - *Something you have*
  - *Something you are*

Authentication proves that a user or system is actually who they say they are. This is one of the most critical parts of a security system. The identification process starts when a user ID or logon name is typed into a sign-on screen. Authentication is accomplished by challenging the claim about who is accessing the resource. Without authentication, anybody can claim to be anybody.

---

### Type 1 - Something you know

- PINs or passwords
- Secure passwords
- Minimum length 8 characters
- Complex (use upper-lower case, numbers, special characters)
- Self-service password resets
- One-time Passwords

**Self-service password reset (Cognitive):** Allows users who have either forgotten their password or triggered an intruder lockout to authenticate with an alternate factor:

Your mother's maiden name  
The model or color of your first car  
The city where you were born

**One-time Password** (passwords that are good for only one login, changes each time)

-Not vulnerable to replay attacks  
-Difficult for human beings to memorize

---

### Strong Passwords

- Upper, Lower, #, Symbols
  - No part of username or e-mail
  - Change every:
    - 60 to 90 days standard
    - 30 to 45 days for high security facilities
  - Implement account lockout and duration
  - Retain password history to prevent re-use
-

**Password Policy**

- Should be as long as possible
- Minimum length 8 characters

# of Characters	Possibilities (in millions)
4	14
5	~ 920
10	$8.4 \times 10^{17}$

**Type 2 - Something you have**

- ATM card
- Smart card
- Personal identification verification card
- CAC / Fortezza card
- Digital Certificates or Tokens



**Authentication Tokens**

- Passive or Stored Value
  - Storage devices that store some type of key
  - Typically they will use a magnetic strip or an optical bar code
- Active
  - Contains a processor that computes a one-time password.

There are three categories of token authentication:

**Static Password Token**

- Owner authenticates to the token by entering a PIN, password, or a biometric scan
- Token then gives the user a complex password that is used to log onto the system
- Least secure and not considered a one-time password



### **Synchronous Dynamic Token**

- User enters a valid password with a PIN to authenticate (fairly secure)
- Considered a one-time password
- Two types:
  - Time-based: synced with internal clock
  - Counter-based: authentication service will advance to the next value



---

### **Asynchronous Dynamic Token**

- a.k.a. Challenge Response Token
- Considered a one-time password

Process:

1. User initiates logon and the system issues a challenge
2. User enters the challenge answer with a personal PIN
3. Token generates a response that the user enters into the system
4. Match allows the user access the system



---

### **Type 3 - Something you are**

#### **Biometrics**

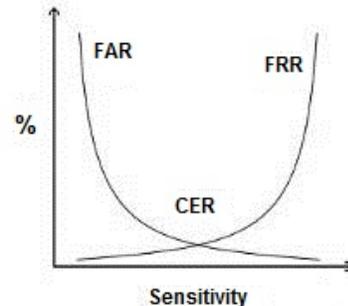
- Authentication based on something intrinsic to the principal (fingerprint, retina, iris, etc.)
  - Cannot be lent or stolen
  - Offers non-repudiation
  - Issues to consider
    - Performance
    - Difficulty
    - Reliability
    - Acceptance
    - Cost
-

Biometrics Examples:

Biometric	Advantage	Disadvantage
Fingerprints (Physiological)	Easy to use	Associated with criminals
Iris (Physiological)	High Accuracy and non-intrusive	Expensive
Retina (Physiological)	High accuracy	Intrusive and expensive
Face (Physiological)	Easy to use	Accuracy issues
Hand (Physiological)	Easy to use	Accuracy issues
Voice (Behavioral)	Inexpensive and non-intrusive	Accuracy issues
Signature (Behavioral)	Inexpensive and non-intrusive	Accuracy issues

**Biometric Error Rates**

- Type I Error: False Reject Rate (FRR)
- Type II Error: False Accept Rate (FAR)
  
- Crossover Error Rate (CER)
  - The point at which the FRR equals the FAR
  - Usually this is impacted by sensitivity
  - The smaller the value, the more accurate the system



**Multi-factor / Two-factor**

- Identity of individual verified using at least two different of the three factors of authentication (something you know, have, are)
- Strong authentication Example: multiple forms of the same authentication factor

**Strong authentication**

- Example: multiple types of the same factor

**Mutual Authentication**

- Both parties authenticate with each other before communicating

**Certificate-Based Authentication**

- More secure than password-based authentication
- Can significantly reduce logon time for users
- A certificate is mapped to a user account in one of two ways:

- **One-To-One Mappings:** Match individual client certificates to individual user accounts on a one-to-one basis.
- **Many-to-one Mapping:** Allows you to map many certificates to one user account. After you have trusted the enterprise root CA of a partner organization, you can map all certificates issued by the partner organization CA to one account that you create in your local domain.

---

## Authentication Protocols:

### Password Authentication Protocol (PAP)

- Weakest form of authentication
- Username and password is sent 'in the clear'
- Maintained primarily for interfacing with legacy systems

### Challenge Handshake Authentication Protocol (CHAP)

- Encrypts passwords during logon
- Challenge/response method of authentication
- Re-authenticates to protect against man-in-the middle attacks
- Credentials are hashed using MD5

### Extensible Authentication Protocol (EAP) 802.1X

- Authentication framework, not a specific authentication mechanism
- Used over PPP and Wireless LANs
- Provides over 40 authentication methods

Some of the most commonly deployed EAP authentication types include EAP-MD-5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-Fast, and Cisco LEAP.

---

## Single Sign-On (SSO)

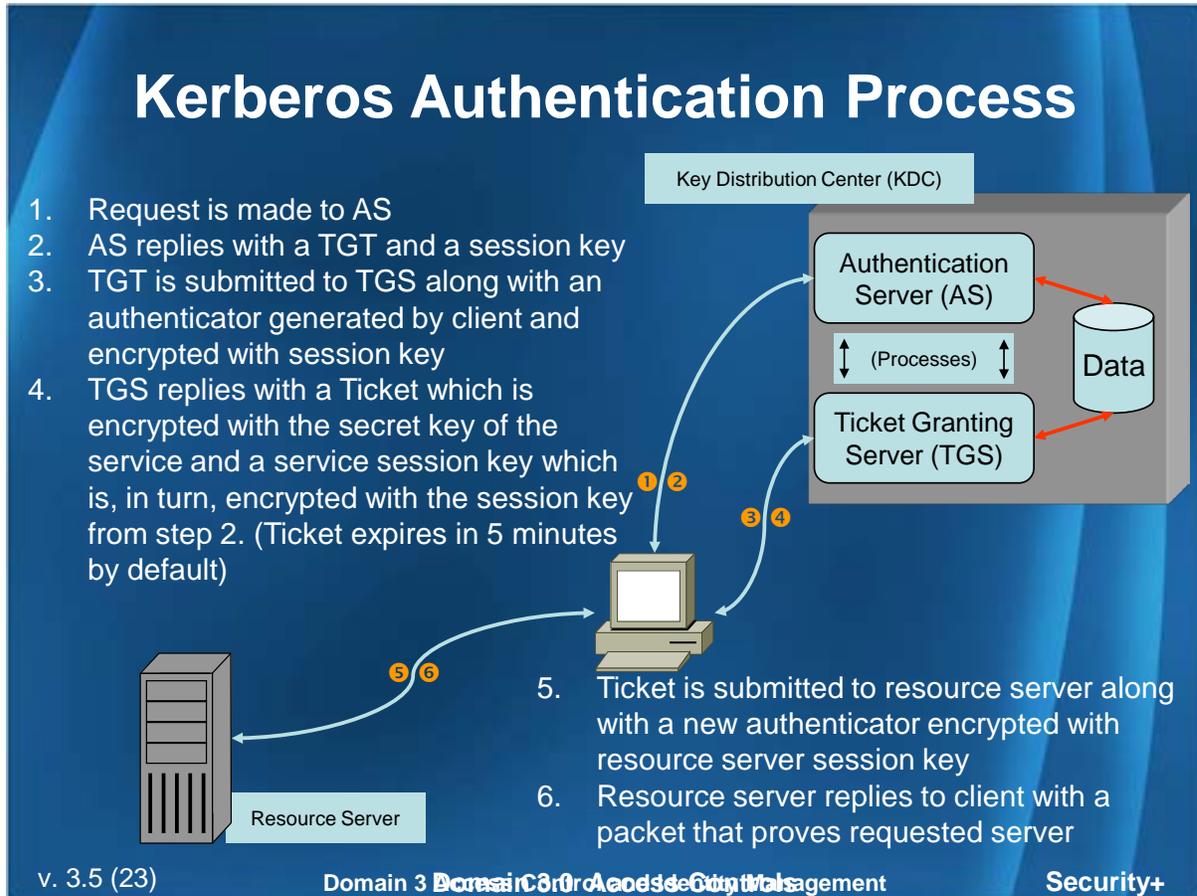
- Provides access to all authorized resources with a single instance of authentication (authenticate only once)
- Uses centralized authentication servers: Once authenticated, subjects can use the network/resources without being challenged again.
- If account is compromised, malicious subject has unrestricted access
- Examples: Kerberos, SESAME, directory services

---

## Kerberos

- Principal
- Realm
- Key Distribution Center (KDC)
  - Authentication Service (AS)
  - Ticket-Granting Service (TGS)
  - Ticket-Granting Ticket (TGT)
  - Remote Ticket-Granting Server (RTGS)

- Authenticates users (principals) to other entities on a network
- Symmetric Key Cryptography
- Shares a different secret key with every entity on the network
- Supports mutual authentication
- Kerberos v5: primary authentication protocol for Windows
- Kerberos uses port 88



### Kerberos Weaknesses

- KDC is a single point of failure
- KDC must be able to handle lots of requests in a timely manner
- Initial authentication is vulnerable to password guessing
- Tickets are temporarily stored on the user's workstation and could be compromised
- Network traffic is not protected by Kerberos
- Vulnerable to DoS attacks
- Access to AS allows attacker to impersonate any authorized user

- If a user changes a password, it changes the secret key, the KDC database must be updated
  - Computers in the domain must be synced within 5 minutes of each other
- 

### **Directory Services**

- Allows centralized security management
- Provides a logical means of organizing resources (users, printers, etc.)
- Uses ACLs to control access to resources
- X.500 standard

Directory services or a naming service is a software system that stores, organizes, and provides access to information in a directory. Each resource on the network is considered an object on the directory server. Information about a particular resource is stored as attributes of that object in the directory database. Information within objects can be made secure so that only users with the available permissions are able to gain access.

### **Common Directory Services**

- Microsoft's Active Directory
  - Novell's eDirectory
- 

### **Lightweight Directory Access Protocol (LDAP)**

- Standardized directory access protocol that allows queries to be made of directories
  - Follows the X.500 standard
  - Directory uses a hierarchical design with a root object at the top followed by Organization and OU containers for logical organization
  - Port 389
  - Port 636 LDAP over TLS/SSL
- 

### **LDAP Authentication**

Three ways to authenticate to LDAP:

#### **Anonymous**

- Only a username is required to authenticate

#### **Simple**

- Username and password in the clear
- Uses port 389 by default; port 636 over SSL

#### **Simple Authentication and Security Layer (SASL)**

- Can utilize Kerberos, MD5, S/Key, IPSec, TLS, and other authentication mechanisms
-

**LDAP Vulnerabilities**

- **Compromise of username/password**
  - Deploy simple authentication with SSL or SASL
  - Employ strong passwords and educate users
- **Improper directory security settings**
  - Tightly manage ACLs
  - Use auditing and privilege testing to identify users with too many rights
- **Man-in-the-middle**
  - Employ SASL for mutual authentication

**Active Directory Structure**

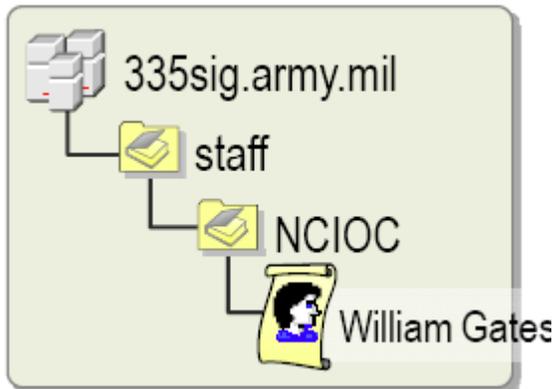
**Directory Services**

- Microsoft's Active Directory
- Backbone for all security, access, and network implementations
- One or more servers manage AD functions
- Tree structure to allow sharing and control
- 
- **Distinguished Names (DN)** exists for every object in AD. There cannot be duplicates and it must be unique. It is **the full path** of the object, including any containers.
  - Uniquely identifies an AD object
  - DN = “Relative Path” + “Common Name”
  - Must be unique within an AD Forest
- **Relative Distinguished Names (RDN)** must be unique in an OU but do not have to be unique in a domain. RDN also derives from X.500. The RDN is the portion of the DN that is an object attribute.
- **User Principal Name (UPN):** often referred to as a friendly name. It consists of the user account and the user’s domain name and is used to identify the user.
- **Common Name (CN):** the object name.

LDAP DN/RDN Naming Convention	Active Directory Naming Convention
<b>cn</b> = common name	<b>cn</b> = common name
<b>ou</b> = organizational unit	<b>ou</b> = organizational unit
<b>dc</b> = domain component	<b>dc</b> = domain component
<b>o</b> = organization	(not supported)
<b>c</b> = country	(not supported)

Microsoft implemented a directory service called Active Directory (AD) with Windows 2000. AD is the backbone for all security, access, and network implementations. AD gives administrators full control of resources. It is a proprietary directory service that provides services for other directory services, such as LDAP. One or more servers

manage AD functions; these servers are connected in a tree structure that allows information to be shared or controlled through the entire AD structure.



**LDAP DN Name:**

cn=William Gates, ou=NCOIC, ou=staff, dc=335sig, dc=army, dc=mil

**Canonical Name:**

335sig.army.mil/staff/NCOIC/William Gates

**The LDAP database**

– Each client computers uses **Lightweight Directory Access Protocol**

- Distinguished Names (DN) to represent Active Directory objects
- LDAP can be queried by DN (primary key) and by other attributes
- LDAP provides DNs and RDNs for objects

– **Two naming conventions:**

- **LDAP Distinguished Name.** LDAP v2 and LDAP v3  
cn=JSmith, ou=Garrison, ou=Infantry, dc=dcTheatreName, divisionName.dc=mil
- **LDAP-based Active Directory Names** (Canonical Names)  
theatreName.divisionName.mil/Infantry/Garrison/ JSmith

---

**Remote Network Access**

**Remote Authentication**

- Communication with a remote host through a dial-up connection
- Clients connect to a Remote Access Server (RAS) to gain access to remote resources or a remote network
- Can support modems, broadband, and VPN connections

Remote authentication refers to any technology used to verify the identity of remote users, whether connecting via VPN, over dial-up, or wireless.

---

**Remote Access Policies**

- Outlines and defines acceptable methods for users remotely connecting to the internal network
- Should cover:
  - All available methods for remote access
  - When they can be accessed
  - By whom

### **Remote Access Services**

- Hardware/software that enables remote access to a network of IT devices
  - Authentication protection
  - User-specific access control
  - Restrict dial-in hours
  - Logging
  - Callback \ Caller ID
- 

### **Remote Authentication Dial-In User Service (RADIUS)**

- Centralized system for authentication, authorization, and accounting (AAA)
  - Supports PAP, CHAP, and EAP
  - Authentication and Authorization combined
  - The IANA assigned ports for RADIUS are
    - Uses UDP port 1812 for Authentication, port 1813 for Accounting
- 

### **RADIUS Client**

- Typically a network access server such as a Dial-up Server, VPN server, or Wireless AP

### **RADIUS Server**

- Stores all user authentication and network service access information
- Ability to implement auditing and accounting

RADIUS authenticates remote users, authorizes their access, and enables remote access servers to communicate with a central server. Authentication requests from multiple RAS servers are forwarded to a single RADIUS server.

In RADIUS, the Authentication and Authorization checking are bundled together. When the client request authentication from the server; the server replies with the authentication attributes, as well as the authorization attributes.

---

### **Diameter**

- AAA protocol suite designed to handle broadband and other connections
  - Supports end-to-end encryption through IPSec, TLS, or both
  - Message tampering can be detected
  - Mutual authentication
  - Challenge/Response user authentication
  - Uses TCP port 3868
- 

### **Terminal Access Controller Access Control System (TACACS+)**

- Alternative to RADIUS
- AAA performed separately
- Supports PAP, CHAP, and EAP
- Allows use of multi-factor authentication
- Allows a RAS to forward user credentials to an authentication server
- Uses TCP port 49

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

---

### **Best Practices for Access Control**

Explicit Deny: You specifically deny a subject (person, IP address, etc.) access to an object (file, server, etc.).

Implicit Deny: By not specifically allowing access, you have denied them access.

Least Privilege: Give users only the permissions they need to do their work and no more.

Need to Know: Used by government and other organizations and describes the restriction of data which is considered very sensitive. You may have a Secret clearance, but not the need to know everything that is secret.

Separation of Duties: Prevents fraud by requiring more than one person to complete a critical process. The term collusion is when two or more people have to establish an agreement to commit a crime.

Job Rotation: You should rotate critical jobs on a frequent enough basis that you are not putting yourself and your data at the mercy of any one administrator. Just as you want redundancy in hardware, you want redundancy in abilities.

Mandatory Vacation: Required vacation time used by the company to check for fraudulent workers.

---

## **Common Access Control Models**

### **Non-Discretionary Access Controls**

#### **Mandatory Access Control (MAC) - Nondiscretionary**

- Primarily used in Government and Military systems
- Follows the Lattice Model
- Access to objects based on clearance and need to know
- Objects are assigned security labels
- Subjects are assigned clearance levels

It is an access policy that restricts subjects' access to objects based on the security clearance of the subject and the classification of the object. The system enforces the security policy and users cannot share their files with other users.

---

#### **Role-Based Access Control (RBAC) - Nondiscretionary**

- Based on responsibilities that an individual user or process has in an organization
- Review frequently to avoid privilege creep

RBAC is a type of model that provides access to resources based on the role the user holds within the company or the tasks that the user has been assigned. As the number of objects and users grow, users are bound to be granted unnecessary access to some objects, which violates least privilege. To mitigate this issue, have data owners review roles for specific systems every 6 months.

---

**Rule-Based Access Control - Nondiscretionary**

- Form of an access control list (ACL) that looks at every request and performs a comparison
- Access is granted depending on the result
- Normally found in firewalls and routers

Rules can be set to deny all but those who appear on a list or deny only those who specifically appear on the list. Rule-based models are often used in conjunction with Role-based to add greater flexibility.

---

**Discretionary Access Control (DAC)**

- Each object (like a file) has an owner (user)
- Owner establishes privileges to the information they own
- Allows information to be shared easily between users
- Access granted/denied based on an ACL (Access Control List)

DAC primarily use in the corporate world and the most commonly used model. It is an access control model and policy that restricts access to objects based on the identity of the subjects and the groups to which those subjects belong. DAC establishes an access control list (ACL) that identifies the users who have authorization to access that information

---

**Logical Access Control Methods**

- Access Control Lists (ACLs) - These hold permissions for users and groups, and each entry in an ACL can specify what type of access is given, such as Read-Only, Change, or Full Control.
- Group Policies - One of the easiest ways to restrict access to operating system components and resources is through the use of group policies. The settings defined within a policy are automatically applied.
- Password Policy – (Discussed in Domain 4) The password policy needs to define what you are willing to accept as password values: minimum number of characters, required use of non-alphabetic characters, unique values, and so forth.
- Domain Password Policy - The domain password policy gives permission to reset the password of a user object, and thus the policy should restrict this privilege/power to only administrators.
- Username and Passwords - Consistency is crucial when defining policies related to usernames and passwords. The more standardization you can apply, the more secure the system can become.

- Time-of-day restrictions - Most users need to access the system only during working hours, and by restricting their access to these times, you increase security by decreasing the likelihood that a miscreant can access the system using a hijacked account after hours.
- Account Expiration - Every account should be configured to expire. As the account continues to be used, the expiration should be deferred, but any account not being used should be allowed to expire.
- Logical Tokens - Similar to certificates, tokens contain the rights and access privileges of the token bearer.

---

### Default Accounts

- Operating Systems (Admin\ Root)
- Databases (MS SQL Server\ Oracle)
- Devices (Routers\ Switches)
- Service Accounts (PBX\ user accounts)

### Mitigation:

- Change default passwords
- Disable service accounts unless needed
- Change service account passwords often
- Do not place in code, text files, or the registry
- Privileges vs. Rights

---

### Security Roles (Directory Services)

- Can create Organizational Units (OU)
- Allows the establishment of role areas, such as Finance OU, Logistics OU, etc.
- Each of the OUs can and should have their own security policy applied to those units

### Security Groups

- Security groups are created inside of Organizational Units (OU) to allow for more granular assignments of permissions on users, groups of users, and systems

As an administrator, one of your goals should be to always simplify your security implementation as much as possible. The simpler you can make it, the easier it is to enforce. The easiest way to simplify network security is to organize users into groups and computers into roles. Rather than managing each user individually, you manage each group collectively. The group(s) the user is placed into should always be based upon the roles they need to perform their jobs with the minimum set of rights and privileges.

Users and computers have to be organized into appropriate security groups and roles while distinguishing between appropriate rights and privileges.

### **Privileges vs. Rights**

- Privileges
    - Given to an individual because of where they work or the group they belong to
  - Rights
    - Assigned to an individual based upon their need-to-know
  - Permissions
    - Based upon users need-to-know
    - File Controls
- 

### **Privilege Creep**

- An individual gains a higher level of access than they normally need
  - Caused by activities such as:
    - Temporary access
    - Accidental access
    - Transferring from departments
    - Maintenance hooks left in software
    - Establish new access rights
- 

### **Privilege Escalation**

- The act of exploiting a bug or design flaw in a software application to gain access

#### **Vertical Privilege Escalation**

- Lower privilege user accesses functions or content reserved for higher privilege users

#### **Horizontal Privilege Escalation**

- Normal user accesses functions or content reserved for other users

Privilege escalation occurs when an application with elevated privileges has a bug that allows security to be bypassed, or alternatively, flawed assumptions about how it will be used.

---

### **Authentication Issues**

- Audit for excessive failed logon attempts
- Consider the capabilities of the people affected by complex passwords
  - Complex password implementation may generate numerous locked accounts
- Identity proofing (Cognitive passwords)
  - Users are asked alternative personal information in order to establish identity

Example:

- Cognitive – ex: security breach with Palin's e-mail

Sarah Palin's E-mail – David Kernell, the 20-year-old son of Tennessee Democratic state representative Mike Kernell, was indicted for intentionally accessing Palin's Yahoo! e-mail account without authorization. He reset the account's password by answering several password recovery security questions, he read Palin's e-mail, made

screenshots, and he posted that information and the account's password on a public Web site. Kernell faces a maximum of five years in prison, a \$250,000 fine, and three years of supervised release if convicted.

---

### **Trusted OS**

- Refers to an operating system that provides sufficient support for multilevel security meets a particular set of government requirements

### **Common Criteria**

- Most common set of criteria for trusted operating system design
- 

### **Common Criteria (CC)**

The Common Criteria certification has replaced the US's Trusted Computer Systems Evaluation Criteria (TCSEC) and Europe's Information Technology Security Evaluation Criteria (ITSEC) system for certification.

- Internationally agreed upon set of standards to evaluate IT security
- Outlines a comprehensive set of evaluation criteria
- Evaluation Assurance Levels (EALs)

The standard outlines a comprehensive set of evaluation criteria and is broken down into seven Evaluation Assurance Levels (EAL).

---

### **Evaluation Assurance Levels (EALs)**

- EAL 1: Functionally Tested
- EAL 2: Structurally Tested
- EAL 3: Methodically Tested and Checked
- EAL 4: Methodically Designed, Tested and Reviewed
- EAL 5: Semi formally Designed and Tested
- EAL 6: Semi formally Verified Design and Tested
- EAL 7: Formally Verified Design and Tested

The recommended level of certification for commercial systems is EAL4.

- EAL 1: Primarily used when the user wants assurance that the system will operate correctly, but threats to security aren't viewed as serious.
- EAL 2: Requires product developers to use good design practices. Security isn't considered a high priority in EAL 2 certification.
- EAL 3: Requires conscientious development efforts to provide moderate levels of security.
- EAL 4: Requires positive security engineering based on good commercial development practices.
- EAL 5: Intended to ensure that security engineering has been implemented in a product from the early design phases. It is intended for high levels of security assurance. The EAL documentation indicates that special design considerations will most likely be required to achieve this level of certification.

- EAL 6: Provides high levels of assurance of specialized security engineering. This certification indicates high levels of protection against significant risks. Systems with EAL 6 certification will be highly secure from penetration attackers.
- EAL 7: Intended for extremely high levels of security. The certification requires extensive testing, measurement, and complete independent testing of every component.

## Domain 4 Threats and Vulnerabilities

### A Security+ candidate is expected to:

- Analyze and differentiate among types of malware
- Analyze and differentiate among types of attacks
- Analyze and differentiate among types of social engineering attacks
- Analyze and differentiate among types of wireless attacks
- Analyze and differentiate among types of application attacks
- Analyze and differentiate among types of mitigation and deterrent techniques
- Implement assessment tools and techniques to discover security threats and vulnerabilities
- Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning
- Carry out the appropriate procedures to establish application security
- Implement security applications

---

### Analyze and differentiate among types of malware

#### Malicious Code

Virus	Spam
Worm	Adware
Trojan Horse	Spyware
Logic bomb	Zombies
Rootkit	Botnets

Malicious code refers to a broad category of threats to your network and systems, including viruses, Trojan horses, bombs, and worms. When these types of attacks are successful, they can be devastating to systems, and can spread through an entire network.

---

#### Virus

- Software designed to infect a computer system
- Goals:
  - Renders your system inoperable
  - Spreads to other systems
- Symptoms:
  - Programs on your system start to load more slowly
  - Unusual files appear or disappear
  - Program sizes change from the installed versions

## Domain 4 - Threats and Vulnerabilities

880800A virus is a program that can replicate itself on a system but cannot spread by itself from system to system or network to network without assistance. It requires an installation vector, such as an executable file attached to an e-mail message or a floppy disk. A virus infects other programs on the same system and can be transferred from machine to machine through e-mail attachments or some form of media.

Most viruses are really worms (misnamed by media). Melissa virus was really a worm.

### Virus Types

<b>Armored</b>	Makes itself difficult to detect or analyze Contains protective code that stops debuggers or disassemblers from examining the code
<b>Retrovirus</b>	Designed to avoid discovery by actively attacking the anti-virus programs attempting to detect it
<b>Stealth</b>	Hides itself by intercepting disk access requests When an anti-virus program tries to read files or boot sectors to find the virus, the stealth virus feeds the anti-virus program a clean image of file or boot sector
<b>Boot Sector</b>	Spreads by infecting boot sectors
<b>File Infector Virus (Parasitic Virus)</b>	Copies themselves into other programs When an infected file is executed, the virus is loaded into memory and tries to infect other executables
<b>Macro Viruses</b>	Malware that is encoded as a macro embedded in a document Programs such as Word and Excel allow programmers to expand the capability of the application. Macro viruses are application-specific rather than OS specific and propagate very rapidly via e-mail. Many are Visual BASIC scripts that exploit commonly used MS apps (such as Word, Excel, & Outlook).
<b>Multipartite (multi-part virus)</b>	<ul style="list-style-type: none"><li>• Propagates by using both the boot sector and file infector methods (i.e. DOS executables)</li><li>• Every part needs to be removed, to prevent re-infection</li></ul> When the virus attaches to the boot sector, it will in turn affect the system's files, and when the virus attaches to the files, it will in turn infect the boot sector
<b>Companion</b>	<ul style="list-style-type: none"><li>• Attaches itself to legitimate programs</li><li>• Creates a program with a different file extension</li><li>• File may reside in your system's temporary directory</li></ul> When a user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointer in the Registry so that they point to the infected program. The infected program may perform its dirty deed and then start the real program. Instead of modifying an existing program, the companion virus uses

## Domain 4 - Threats and Vulnerabilities

	<p>the DOS 8.3 naming system to disguise itself as a program with the same name, but different extension.</p> <p>For example, creating “solitaire.com” to emulate “solitaire.exe”. When the user executes “solitaire”, the virus infects the system and then runs the real program so it appears normal.</p>
<b>Polymorphic</b>	<p>Mutates by padding its own code to avoid detection</p> <p>Makes pattern recognition hard</p>
<b>Metamorphic</b>	<p>Recompiles itself into a new form, so the code is constantly changing</p> <p>Functionality (a.k.a. payload) changes</p> <p>Can disassemble themselves, change their code, then reassemble themselves into an executable form</p>

### Worms

- Computer program that propagates on its own
- Does not need a host application to be transported
- Self contained

A worm is different from a virus, as worms can self reproduce without a host application and they are a self-contained program. Worms can propagate by using mail, website downloads, etc.

### Trojan Horse

- A program that is disguised as another program
- May be included as an attachment or as part of an installation program

A Trojan horse is a program that is disguised as another program and performs its malicious activity in the background. A Trojan horse program depends on tricking a user into running it.

**Examples of a Trojan horse:** Notepad.exe could be something else (could still run and simultaneously manipulate files without user knowing it).

You might download what you think is a game, but when you run it, you find that it deletes all of the executable files on your computer’s hard disk.

The best preventive measure for Trojan Horse attacks is to not allow them entry into your system. Immediately before and after you install a new software program or operating system, back it up! If you suspect a Trojan horse, you can reinstall the original programs, which should delete the Trojan horse. A port scan may also reveal a Trojan horse on your system. If an application opens a TCP or UDP port that is not regularly used in your network, you can notice this and begin corrective action.

---

### Logic Bomb

- Malware inserted into a system which sets off an action when specific conditions are met
- Logic Bomb Examples: Michelangelo and Chernobyl

A logic bomb is a malicious program or malicious components of a program that is left behind by an attacker. It is designed to be activated at a later point. For example, programmers have incorporated routines into programs that delete crucial data, and then they have activated these routines when their employment was terminated.

### Rootkits

- Malware that has the ability to hide spyware blockers, anti-virus program, and system utilities
- Runs at the root level or admin access

“Root” comes from UNIX (root: user with the most privileges). A rootkit is a technique that allows malware to hide from computer operating systems and from computer users. Rootkit techniques create stealth programs that run at a "lower" level than the user can see with normal software utilities. Malware attempts to use this method to avoid detection by security software.

---

### Backdoors

- Allows access to a computer (i.e. server, workstation, network device)
- Full access to every aspect of the device
- Can be spread via malware
- Examples: Back Orifice or NetBus

### Mitigation:

- Up-to-date Anti-virus
- IDS/IPS

a.k.a. Maintenance or Programming Hook a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a Rootkits.

Backdoors are also placed into applications and network devices for maintenance. The SANS Institute is pushing vendors (especially hardware vendors) to remove the hooks, because the user IDs and passwords are getting to be known by attackers.

A backdoor is a program or a set of related programs that a hacker installs on the victim computer to allow access to the system at a later time. A backdoor's goal is to remove the evidence of initial entry from the systems log. But a sophisticated backdoors will allow a hacker to retain access to a machine they have penetrated even if the intrusion factor has been detected by the system administrator. A trivial example of a backdoor is a default BIOS, router or switch passwords set either by careless manufacturers or

security administrators. A hacker could simply add a new user account with administrator privileges and this would be a sort of backdoor, but far less sophisticated and easy detectable.

Backdoor and remote access programs such as Loki, NetCaZ, Masters Paradise, Back Orifice, BO2K and NetBus find their way to a computer via Trojan horses or as a worm or virus payload.

---

### Adware

- Frequently refers to any software which displays advertisements
- Some are spyware or malware

Adware is a spyware program that monitors the user's activity and responds by offering unsolicited pop-up advertisements, gathers information about the user to pass on to marketers, or intercepts personal data such as credit card numbers. Some types of adware are also spyware or malware.

### Spyware

- Malware that works on collecting information about the system and what it is used for.
- Spreads to machines by users who inadvertently ask for it

Spyware is secretly installed on a computer to intercept or take partial control over the user's interaction with the computer, without the user's consent. It could capture surfing habits, keystrokes, passwords, system information, or install a backdoor.

---

### Denial of Service (DoS)

- Prevents access to resources for authorized users
- Common DoS attacks:
  - Ping-of-Death
  - Land Attack
  - Teardrop
  - SYN Flood

Denial-of-service (DoS) attacks prevent access to resources by users authorized to use those resources. Most simple DoS attacks occur from a single system, and a specific server or organization is the target.

---

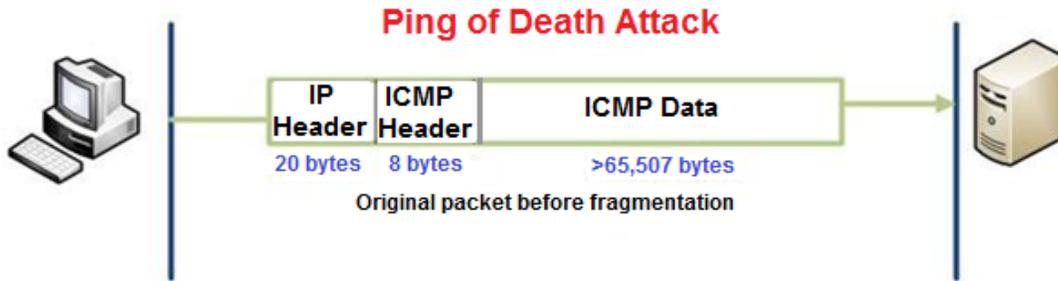
### Ping of Death

- A form of buffer overflow attack
- Sending numerous, large (>65,535 bytes) ping packets to a system
- At a command line: **ping -l 65550 192.168.2.13**
- Systems were not designed to handle this packet and could crash

Ping of Death is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 56 bytes in size (or 84 bytes

when IP header is considered); historically, many computer systems could not handle a ping packet larger than the maximum IPv4 packet size, which is 65,535 bytes. Sending a ping of this size could crash the target computer.

There is a specific ICMP echo variation that could cause a system crash. The difference of the echo request from the normal ones is the large size of IP packet it contains. RFC 791 specifies that the maximum size of an IP packet is 65,535 bytes. An ICMP echo request with more than 65,507 (65,535-20-8) bytes of data could cause a remote system to crash while reassembling the packet fragments.

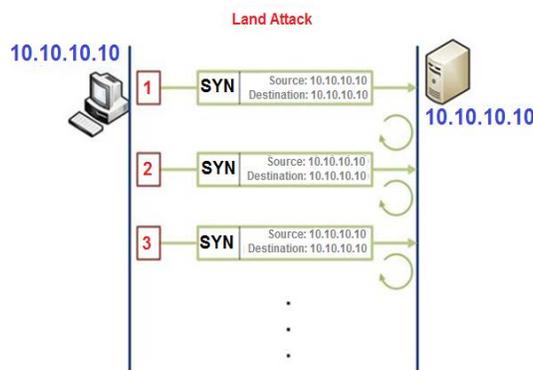


**Countermeasure: Registry Hack**

**Land Attack**

- An attacker creates a packet with the source and destination IP addresses set as the victim
- If a system is not configured correctly it cannot process the flood of packets from itself
- The system goes into a dead end loop and cannot process legitimate requests

When the attacker initiates a SYN Flood attack using the IP address of the victim as source and destination IP address, then it is said that the attacker has launched a "land attack". If the victim has not taken any precautions for this type of attack, it could end up trying to establish a connection with itself falling into a dead-end loop that exists until the idle timeout value is reached.



The attacker is sending spoofed SYN packets to the system it is spoofing. Basically the victim system thinks it is receiving packets from itself, as it tries to process them it receives more and more putting it in a loop. If the system is not configured to handle these types' packets from itself it could then crash.

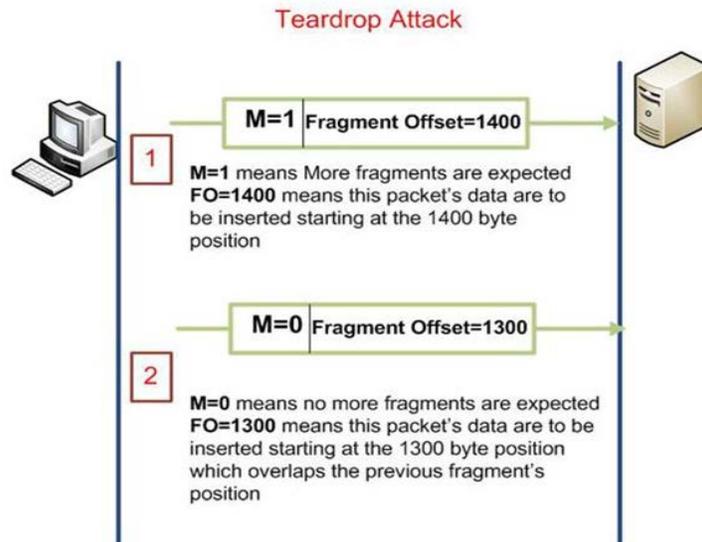
### Teardrop Attack (Fragmentation attack)

- An attacker creates a large packet
- One of the processes of IP is to fragment the packet and set offset bits for reconstruction at the distant end
- The attacker overlaps the offset bits, when the receiving system tries to reconstruct the packet it crashes

This type of attack deals with fragmentation and reassembly of IP packets. The IP header contains the necessary fields to handle fragmentation issues. Basically there are three fields within an IP datagram related to fragmentation and reassembly; these areas:

- Do not fragment bit
- More fragments bit
- Fragment Offset

The Fragment Offset field, which is the crucial field in our case, is used to indicate the starting position of each fragment relative to the original un-fragmented packet. An attacker could start transmitting fragmented IP packets containing overlapped Fragment Offsets making the victim unable to reassemble them exhausting the victim's resources and possibly crashing it.



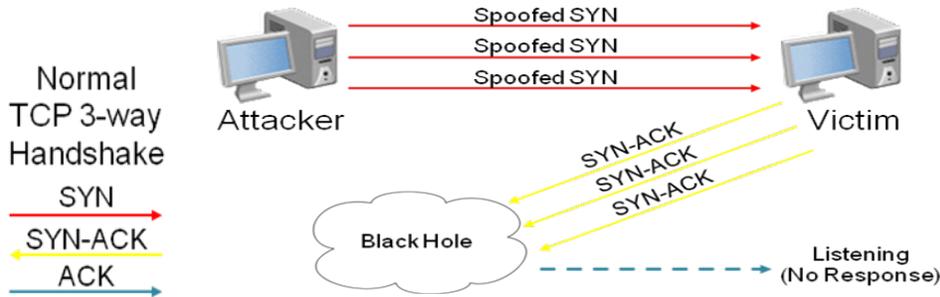
In this example the 1<sup>st</sup> fragment has an offset set at the 1400 byte position, when the second fragment arrives it has instructions stating it's the last fragment and it is to be inserted at the 1300 byte position, contradicting the previous fragment instructions. The system tries to reconstruct the packet but cannot, this could cause the system to crash

or the system cannot handle legitimate requests as it is trying to complete this processes.

---

### TCP SYN Flood or TCP ACK Attack

- Attacker sends a succession of SYN requests to a target
- Can be mitigated on most modern networks



There are two TCP attack methods, but both involve the server not receiving the ACK.

1. A malicious client can skip sending this last ACK message
2. By spoofing the source IP address in the SYN, it makes the server send the SYN-ACK to the falsified IP address, and thus never receive the ACK.

In both cases, the server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK.

TCP operates using synchronized connections. The synchronization = handshake.

Normal TCP connection process (3-way handshake):

1. The client requests a connection by sending a SYN (synchronize) message to the server.
2. The server acknowledges this request by sending SYN-ACK back to the client.
3. The client responds with an ACK, and the connection is established.

### SYN Flood Problems:

The server queue fills up with requests which will lead to a DoS

**Countermeasures:** Registry Hack- SYN-ACK - 3

---

### Distributed Denial of Service (DDoS)

- Amplifies a DoS by using multiple computers to conduct an attack against a single entity (Smurf Attack)
- Uses Zombies/Botnets to multiply the number of attackers

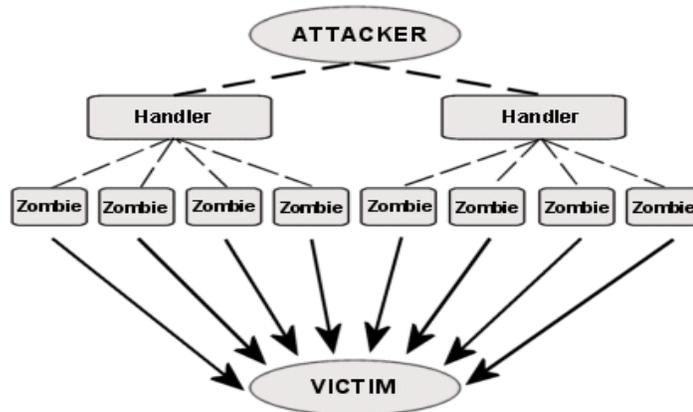
A distributed denial-of-service (DDoS) attack is similar to a DoS attack. A DDoS attack amplifies the concepts of DoS by using multiple computer systems to conduct the attack against a single organization.

### Zombies

- A computer compromised by a hacker that is used to perform malicious tasks under remote direction

### Botnets

- A network of compromised systems containing malware which acts as a robot
- Bots are programs that run automated tasks
  - Compromised systems obey a master or author of the code
- 
- These attacks exploit the inherent weaknesses of dedicated networks such as DSL and cable. These permanently attached systems usually have little, if any, protection. An attacker can load an attack program onto dozens or even hundreds of computer systems that use DSL or cable modems.
- 
- The attack program lies dormant on these computers until they get an attack signal from a master computer. The signal triggers the systems, which launch an attack simultaneously on the target network or system. The following exhibit shows an attack occurring and the master controller orchestrating the attack.



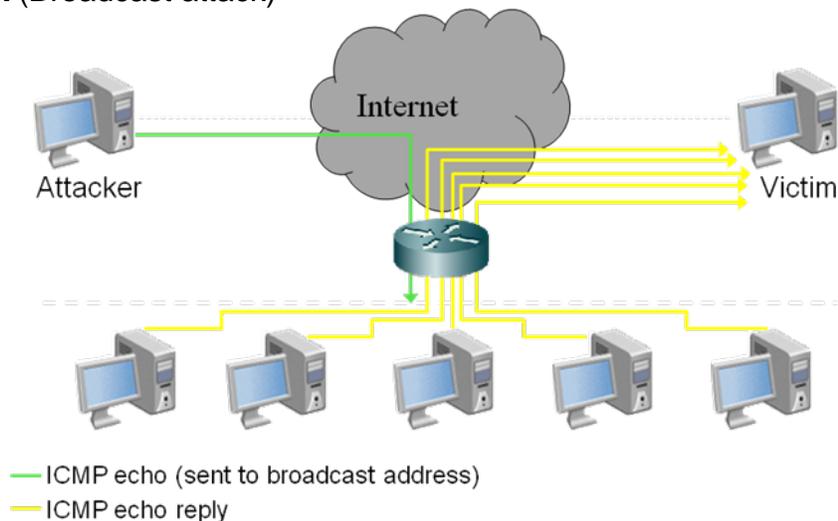
- The master controller may be another unsuspecting user. The systems taking direction from the master control computer are referred to as zombies. These systems merely carry out the instruction they've been given by the master computer.
- 
- The nasty part of this type of attack is that the machines used to carry out the attack belong to normal computer users. The attack gives no special warning to those users. When the attack is complete, the attack program may remove itself from the system or infect the unsuspecting user's computer with a virus that destroys the hard drive, thereby wiping out the evidence.



### Spammer botnet

1. A botnet operator sends out viruses or worms, infecting ordinary users' computers, whose payload is a malicious application—the *bot*.
2. The *bot* on the infected PC logs into a particular C&C server (often an IRC server, but, in some cases a web server).
3. A spammer purchases the services of the botnet from the operator.
4. The spammer provides the spam messages to the operator, who instructs the compromised machines via the IRC server, causing them to send out spam messages.

### Smurf Attack (Broadcast attack)



In a Smurf attack, an attacker sends a large amount of ICMP echo requests (ping) traffic to IP broadcast addresses, all of it having a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the

IP broadcast to all hosts (for example via a layer 2 broadcast), most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, hundreds of machines might reply to each packet.

A Fraggle attack is similar to a Smurf attack, but uses UDP rather than ICMP. The attacker sends spoofed UDP packets to broadcast addresses and the UDP packets are directed to port 7 (Echo) or port 19 (Chargen). When connected to port 19, a character generator attack can be run.

---

### Analyze and differentiate among types of Network attacks

#### Man-in-the-Middle Attacks

- Occurs when someone/-thing intercepts data and retransmits to another entity

This type of attack is also an access attack, but it can be used as the starting point for a modification attack. The method used in these attacks clandestinely places a piece of software between a server and the user that neither the server administrators nor the user is aware of.

The software intercepts data and then sends the information to the server as if nothing is wrong. The server responds back to the software, thinking it's communicating with the legitimate client. The attacking software continues sending information on to the server, and so forth as shown in the following exhibit:



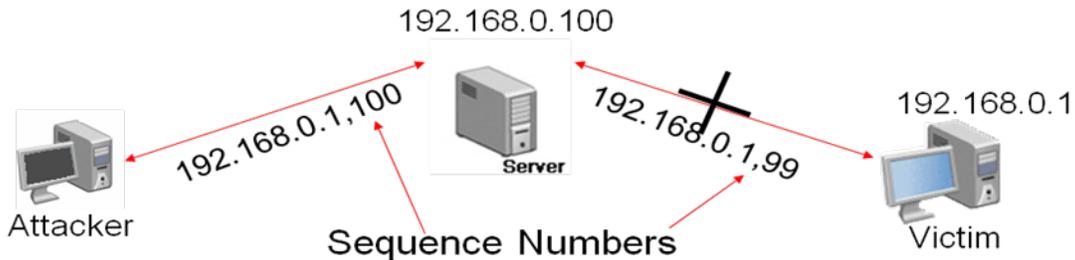
MITM software may be recording information for someone to view later, altering it or in some other way compromising the security of your system and session.

**Countermeasures:** Random sequence numbers, encryption, mutual authentication

---

#### Session Hijacking

- a.k.a. TCP/IP Hijacking
- Takes control of an active TCP session by using sequence number guessing



Hijacking is when an attacker takes control of a session between the server and a client. This starts as a man-in-the-middle attack. The result is that the client gets kicked out of the session, while the attacker's machine still communicates with the server. The attacker intercepts the source-side packets and replaces them with new packets that are sent to the destination.

**Countermeasures:** Random sequence numbers, encryption, mutual authentication

---

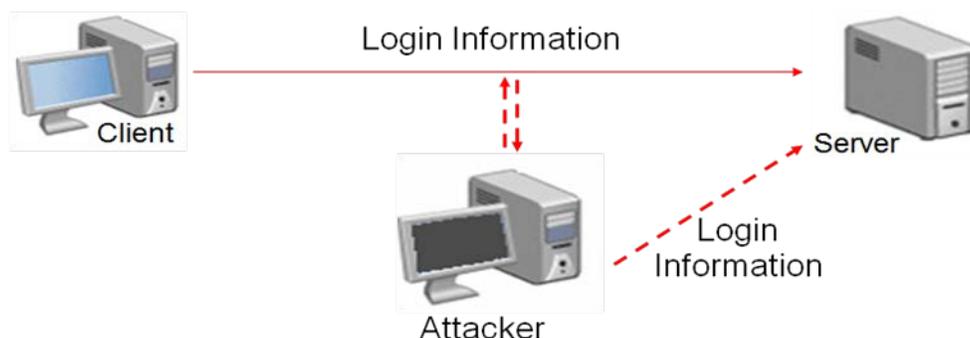
### Replay Attack

- Information (credentials) captured over a network and replayed later

Replay attacks are becoming quite common. They occur when information is captured over a network, and then “replayed” back through the network by someone else. A replay attack is a kind of access or modification attack. In a distributed environment, logon and password information is sent between the client and the authentication system and in some instances those credentials can be captured and replayed.

The attacker can capture the information and replay it again later. This can also occur with security certificates from systems such as Kerberos: The attacker resubmits the certificate, hoping to be validated by the authentication system and circumvent any time sensitivity.

The following exhibit shows an attacker presenting a previously captured certificate to a Kerberos-enabled system. In this example, the attacker gets legitimate information from the client and records it. Then, the attacker attempts to use the information to enter the system. The attacker later relays information to gain access.



If this attack is successful, the attacker will have all the rights and privileges from the original certificate. This is the primary reason that most certificates contain a unique session identifier and a time stamp: If the certificate has expired, it will be rejected and an entry should be made in a security log to notify system administrators.

**Countermeasures:** Random sequence numbers, encryption, mutual authentication

---

### Spoofting

Spoofting is a situation in which one person or program successfully masquerades as another by falsifying data.

- Impersonating someone/something else by falsifying data
  - Comes in many forms:
    - **IP address spoofing** is the creation of TCP/IP packets using someone else's IP address.
    - **MAC spoofing** is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device.
    - **ARP poisoning**- an attacker (on the same switched network) forges ARP replies to a victim system and a device like the default gateway. The attacker is placed in the clients ARP table as the default gateway, the attacker is placed in the default gateways ARP table as the client. All data from the client goes to the attacker, (who can do a variety of things with it during the MITM attack) who then forwards it to the default gateway. Neither the default gateway nor the legitimate client system is aware of the attacker.
    - **Web spoofing** the attacker creates a convincing but false copy of the entire Website. The false site looks just like the real one: it has all the same pages and links. However, the attacker controls the spoofed site. The attacker has created this page to dupe the victim into providing information such as usernames, passwords, credit card numbers, etc. These pages can be part of a Man in the Middle attack.
    - **DNS spoofing**-You are redirected because the DNS server resolving the URL name to IP address has been poisoned.
- 

### Drive-by-Download

Malware automatically downloaded to your computer without your consent or even your knowledge

Can be initiated:

- by visiting a Web site
- by viewing an HTML e-mail message
- along with a user-requested application

Some spyware authors infect a system by attacking security holes in the Web browser or in other software. When the user navigates to a Web page controlled by the spyware author, the page contains code which attacks the browser and forces the download and installation of spyware.

---

### Repudiation Attacks

- Cannot tell who the authenticator of the request is
- If this attack takes place, the data stored on log files can be considered invalid or misleading

A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions.

This attack can be used to change the authoring information of actions executed by a malicious user in order to log wrong data to log files.

Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages.

---

### Xmas Attack

- Scans/attack conducted with Xmas packets
- Packet with every single option set for whatever protocol is in use
- By observing how a host responds to the packet, assumptions can be made regarding the host's operating system

Christmas tree packets can be used as a method of divining the underlying nature of a TCP/IP stack by sending the packets and awaiting and analyzing the responses. When used as part of scanning a system, the TCP header of Christmas tree packets has the flags FIN, URG and PSH set. Many operating systems implement their compliance with the Internet Protocol standard (RFC 791) in varying or incomplete ways. By observing how a host responds to an odd packet, such as a Christmas tree packet, assumptions can be made regarding the host's operating system.

Christmas tree packets can be easily detected by intrusion-detection systems or more advanced firewalls. From a network security point of view, Christmas tree packets are always suspicious and indicate a high probability of network reconnaissance activities.

---

### Transitive Access

- A service that invokes another service to satisfy an initial request
- Problem arises from a poor choice of access control mechanism, one that uses authentication to make access decisions

### Example;

A program run by Alice invokes a service run by Bob. In order to satisfy Alice's request, Bob's invokes a service run by Carol. Bob may have some rights not granted to Alice.

Alice may have some rights not granted to Bob. If Bob's rights are used, he may do something on behalf of Alice that she is not allowed to do. If Alice's rights are used, Bob may take an action that Alice would not approve.

### Client-side attacks

These are attacks that target vulnerabilities in client applications that interact with a malicious server or process malicious data.

A typical example of a client-side attack is a malicious web page targeting a specific browser vulnerability that, if the attack is successful, would give the malicious server complete control of the client system.

---

### Malicious Internal/Insider Threats

An Organizations employees can be one of its' largest vulnerabilities/threats

- Reasons
  - Disgruntled
  - Corporate Espionage/Fraud
  - Careless
  - Lack of training
  - They are already in your network/facility

In the wake of the WikiLeaks disclosures, all the soul searching and mandated risk assessments have made one thing painfully clear: Some of the most damaging security breaches originate from inside an agency's firewalls.

According to the 2011 CyberSecurity Watch Survey conducted by CSO magazine, security breaches caused by once-trusted employees and contractors account for one in five attacks across all industry sectors. Such developments are spurring agencies to redouble their efforts to strengthen internal defenses while still balancing the need for trusted insiders to appropriately access sensitive information for their jobs. There's just one problem: No matter how diligent agencies might be about security, there are no easy answers. No combination of technology and policy will fully protect against someone with special access privileges who decides to betray that trust.

---

### Internal/Insider Threat Mitigations

- Least Privilege
  - Keep good logs
  - Keep good backups
  - Separation of duties
  - Account management:
    - Use individual credentials as you setup new accounts
    - Verify and review accounts
    - Suspend accounts
  - Conduct regular User Awareness Training
-

### Social Engineering (Network Oriented)

#### Spam

- Unsolicited Bulk E-mail (UBE) or Unsolicited Commercial E-mail (UCE)
- Unwanted, unsolicited email
- Can be infected with viruses and worms
- SPIM = SPAM over Instant Messaging
- SPIT = SPAM over Internet Telephony

#### Cost of Spam:

- Loss of productivity
- ISP cost for increased storage space for clients
- Bandwidth cost for increased traffic

There is no one technique that will be a complete solution to the spam problem.

While spam is not truly a virus or a hoax, it is one of the most annoying things an administrator can contend with. Spam is defined as any unwanted, unsolicited e-mail, and not only can the sheer volume of it be irritating, it can often open the door to larger problems. Some of the sites advertised in spam may be infected with viruses, worms, and other unwanted programs. If users begin to respond to spam by visiting those sites, then your problems will only multiply.

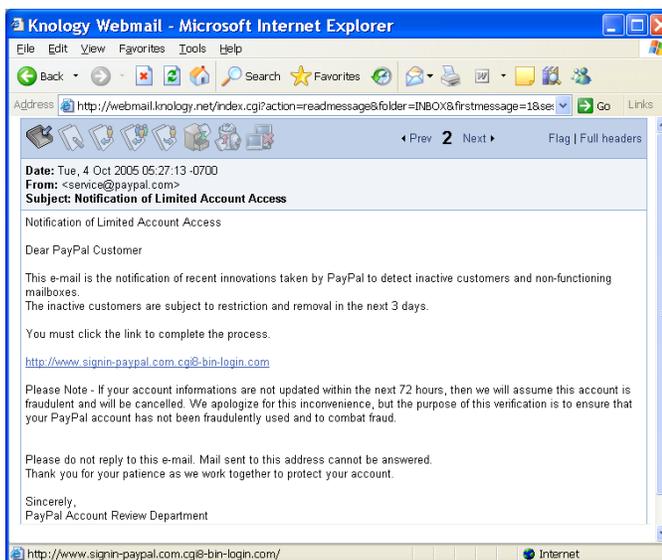
Just as you can, and must, install good antivirus software programs, you should also consider similar measures for spam. Filtering the messages out and preventing them from ever entering the network is the most effective method of dealing with the problem.

---

**Phishing Attacks:** Uses social engineering (Emails) to steal personal identity data and financial account credentials.

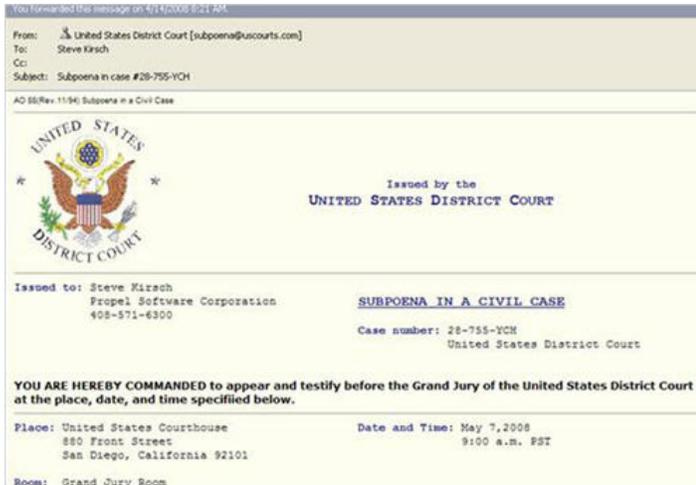
**Vishing:** Using phone calls to steal personal identity data and financial account credentials.

**Pharming:** Attack in which a user can be fooled into entering sensitive data such as a password or credit card number into a malicious web site that impersonates a legitimate web site



**Spear Phishing:** Email/IM scam to a particular target, some inside information about the organization or individual is needed.

**Whaling:** Spear phishing directed towards senior executives or someone of great importance in an organization



---

## Analyze and differentiate among types of social engineering attacks

### Social Engineering

Exploits human nature by convincing someone to reveal information or perform an activity

Examples include:

- Impersonating support staff or management
- Asking for someone to hold open a door rather than using a key for entrance
- Spoofed e-mails that ask for information or ask you to do things
- Looking on or under desks for usernames and passwords

---

### Specific Attacks

- Dumpster Diving
- Shoulder Surfing
- Piggybacking (Tailgating)
- Impersonating
- Hoaxes

---

### Dumpster Diving

Looking in the trash for sensitive information



---

**Shoulder Surfing**

Looking over the shoulder of someone working on a laptop/PC



---

**Piggybacking (Tailgating)**

Entering a secured building/area by following an authorized employee



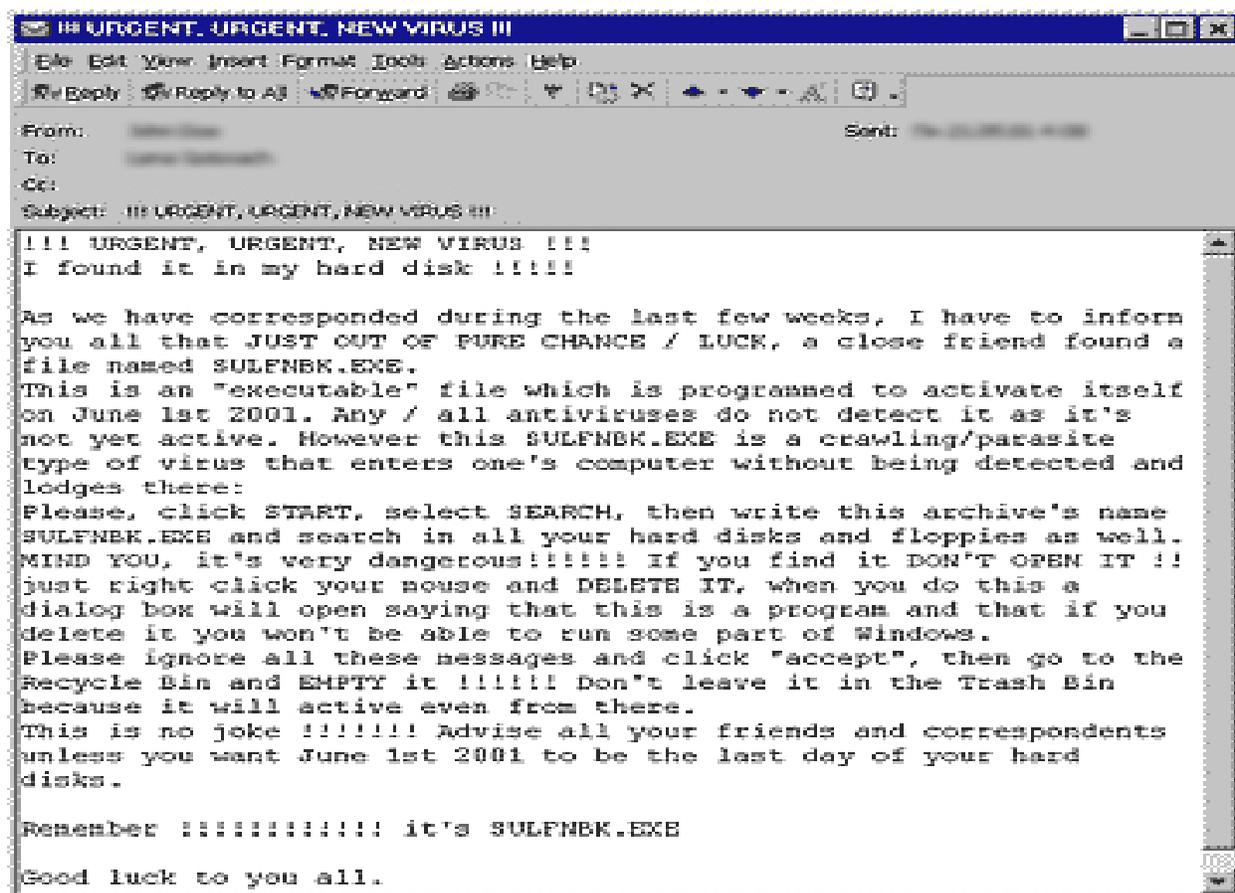
---

**Impersonating**-Pretending to be someone you are not in an attempt to gain access to an area you should not. Spoofing falls in the realm of impersonating. An individual pretending to be support staff over the phone, someone who dresses as a maintenance person to gain access to a facility, someone who dresses nice to appear to be in a position of authority, etc are all examples.



Example; That's Mr. Harry Potter.

**Virus hoaxes** are false virus warnings that circulate over email and are designed to cause alarm or damage. At best, they waste time and cause undue fear or distress. At worst, they can lead to widespread computer damage and data loss. Sadly, such damage is almost always the result of hoax recipients themselves who are tricked into harming their own PCs by following a set of persuasive instructions that promise to "fix" or "disinfect" a perfectly healthy machine.



The above is a typical virus hoax. **SULFNBK.EXE** is actually a critical Windows file and would render the PC inoperable if deleted.

---

### Analyze and differentiate among types of application attacks

#### Buffer Overflows

- Most common attack against Web servers
- More information is placed in a buffer (memory stack or heap) than it can hold, which then overflows into the next buffer
- Attacker can create a DoS or run code with elevated privileges
- Application can be terminated
- Writes data beyond the allocated space

- Safeguards:
    - Input validation
    - Patch/Upgrade
- 

### **Cross-Site Scripting (XSS)**

- Vulnerability where an attacker can add comments/code to web pages which allows code injection
- Code could redirect valid data to the attacker
- Safeguards:
  - Input validation (phone number – server side routine could remove all character other than digits).
  - Set web apps to tie session cookies to the IP address of the original user and only permit that IP to use the cookie.

XSS a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

Vulnerabilities of this kind have been exploited to craft powerful phishing attacks and browser exploits. As of 2007, cross-site scripting carried out on websites were roughly 80% of all documented security vulnerabilities. Often during an attack "everything looks fine" to the end-user who may be subject to unauthorized access, theft of sensitive data, and financial loss.

Additionally, attackers can change web pages to link to malicious web sites that appear to be legitimate, add advertising to web pages, change user settings, and more. Every week between 3 and 5 new Cross Site Scripting exploits are discovered, each using a different method and affecting the victim in a different way.

---

### **SQL Injection**

- Code injected into a database via a web form
- Allows an attacker to query data from the database
- DoS is the most common SQL attack
  - User ID = ' ' or 1=1;

#### **Safeguards:**

Input validation! The underlying code needs to verify the correct input using a white list. If the input is verified against a white list using a regular expression then the input could be rejected and the end user would need to input the correct data.

SQL injection, cross-site scripting, and buffer overflow vulnerabilities exists primarily due to lack of input validation.

In all of the following examples the attackers have already sent through numerous commands just to see what responses they would get back from the database. The login page had a traditional username-and-password form, but also an email-me-my-password link; the latter proved to be the downfall of the whole system.

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'x'; DROP TABLE members; --'; -- Boom!
```

Example 1: If this command was executed remotely by the attacker, what would happen? It would delete all of the member information from the member's field.

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'x';
UPDATE members
SET email = 'steve@unixwiz.net'
WHERE email = 'bob@example.com';
```

Example 2: The attackers find they cannot add their information to the database (cannot create a member), but they can modify an existing one. So in the first part of example 2 they update Bob's info, with Steve's (e-mail address).

Now Steve can't log in at the moment because he doesn't know Bob's password. No problem, Steve goes to the home page and clicks "Forgot Password" and the company is nice enough to send Bob's password to Steve's e-mail.

```
From: system@example.com
To: steve@unixwiz.net
Subject: Intranet login
```

```
This email is in response to your request for your Intranet log in information.
Your User ID is: bob
Your password is: hello
```

### LDAP Injection:

- Can occur anywhere that underlying code could use some type of input for LDAP searches, queries, or any other LDAP function
- Implementation of simple precautions during development
  - Controlling the types and numbers of characters that are accepted by input boxes
  - Input validation

LDAP injection is a specific form of attack that can be employed to compromise Web sites that construct LDAP (Lightweight Directory Access Protocol) statements from data provided by users. This is done by changing LDAP statements so dynamic Web applications can run with invalid permissions, allowing the attacker to alter, add or delete content. Take, for example, a page that has a search box to search for users in an application. This search box could ask for a username. The underlying code would take this search query information and generate the LDAP query that will be used to search the LDAP database.

### XML Injection

- Attack technique used to manipulate or compromise the logic of an XML application or service
- Injection can cause the insertion of malicious content into the resulting message/document

Because of its platform independence, flexibility and relative simplicity, the extensible markup language (XML) has found use in applications ranging from remote procedure calls to systematic storage, exchange and retrieval of data. However, because of its versatility, XML is vulnerable to a wide spectrum of attacks. One such attack is called XML Injection. When a user has the ability to add structured XML as input, he can override the contents of an XML document by injecting XML tags in data fields. These tags are interpreted and classified by an XML parser as executable content and as a result, may cause certain data members to be unintentionally overridden. Prevention of XML Injection involves input validation and XML sanitization in a context akin to SQL injection. Compliance to regulations requires appropriate input validation and data sanitization.

It is also possible for a man-in-the-middle attacker to modify a client-validated XML stream over an unsecured link. For this reason, server side validation of XML data is indispensable. For this reason, if a client sends XML data containing user input to a server, the client must sanitize the user input, and the server must validate the client's XML.

### Example XML

1. The price of the widget is 500.00 for 1.

```
<item>
  <description>Widget</description>
  <price>500.0</price>
  <quantity>1</quantity>
</item>
```

2. Malicious individual adds a string to line 4, with this input.

```
1</quantity><price>1</price><quantity>1
```

3. A parser interprets the input and resolves the second price, overriding the first. The widget now costs 1.0 for 1.

```
<item>
  <description>Widget</description>
  <price>500.0</price>
  <quantity>1</quantity><price>1.0</price><quantity>1</quantity>
</item>
```

---

### Cookies

- Text file associated with your current web session and/or user information for a site
- Saves your internet activity locally (not data)
- Browsers offer settings to help control vulnerabilities from cookies
- Transient vs. Persistent cookies

Cookies do not contain info such as credit card #'s, phone numbers, addresses, etc. (stored on the server's DB). Information is kept on the website's database (linked by a UID). Web page designers need to take special care in not allowing user names and passwords to reside in cookies. Some cookies have time stamps to ensure secure connections timeout.

Cookies are text files and cannot carry viruses. Cookies cannot be used to "steal" information about you or your computer system. They can only be used to store information that you have provided at some point.

Cookies can be hijacked (via use of a sniffer) to allow an attacker to take over the session or divert it to a rogue server.

- *Transient cookies* - are active only during a browsing session
- *Persistent cookies* – store user identification information over an extended period

---

### Safeguards:

- Delete some or all of your cookies
- Have your browser warn you when it is about to send a cookie to a server, and give you the option of not sending it
- Choose to save cookies only for the duration of this web browsing session
- Disable all use of cookies by your browser
- Third party cookies

Third Party Cookies:

- Automatically accept or reject cookies from certain sites of your own choosing
- Disallow cookies that are to be sent to sites other than the main one you're browsing (which protects against the kind of cross-site tracking)

### Mobile Code

---

#### Active X

Created by Microsoft to customize controls, icons, and other features to help increase the usability of web-enabled systems and how it runs on the client systems.

Authenticode is the method used for security. Authenticode is a type of certificate technology that allows ActiveX components to be validated by a server.

- PKI aware authenticode (code is digitally signed); relies on digital signatures and trusting certificate authorities.
- A Microsoft technology involving Object Oriented Programming (OOP) and based on Component Object Model (COM) objects and Distributed Component Object Model (DCOM).
- Executed within the security context of the current user account, meaning that they can access any resource and perform any action that the current user is able to perform
- Unlike Java Applets, ActiveX controls are downloaded to the user's hard drive when they choose the functionality provided. This presents a serious security issue, because the code segments can be accessed again in the future by any active process.
- Browser security levels determine if they are done automatically or with the user's consent

---

#### ActiveX Vulnerabilities

- Controls are saved to the hard drive
- Controls are executed within the security context of the current user account
- Once user accepts author, then it is always accepted (no re-verification)

---

#### ActiveX Safeguards

- Deploy patches to fix vulnerabilities
- Browser should be configured NOT to allow ActiveX to run by default
- Under Internet Explorer Options go to: Security tab and choose the level of security to control how ActiveX responds to enabling, disabling, or prompting

---

#### Java Applets

- Stand alone mobile code downloaded from a server to a client, then runs from the browser
- Platform independent (due to bytecode)
- Sandbox
  - A virtual machine architecture
  - Limits the applet's access to system resources
  - Digitally signed applets can run outside the sandbox

---

#### Java Applet Vulnerabilities

- Applets may perform malicious operations

- Errors in the Java virtual machine may allow some unsigned applets to run outside the sandbox

### Java Applet Safeguards

- Install the latest browser version
  - Deploy patches to fix vulnerabilities
  - Disable Java Applets
  - Limit browser plug-ins
- 

### JavaScript

- Scripting language used for web pages
  - Runs in a client's browser or web server and can be seamlessly embedded into HTML documents and email
  - Uses
    - Opens new windows (controls size and position)
    - Detects user's actions such as keystrokes
    - Changes images with mouse-move over's
- 

### JavaScript Vulnerabilities

- Runs within the web page security level of permission settings
- Can allow remote execution of programs
- Interfaces with an OS, so potentially can damage systems or be used to send information to unauthorized persons

### JavaScript Safeguards

- Apply JavaScript patches for browsers
- Disable JavaScripts

JavaScript provide the potential for malicious authors to deliver scripts to run on a client computer via the web.

XSS (Cross Site Scripting) attacks can be carried out using Javascript.

---

### Directory Traversal

- Goal is to order an application to access a computer file that is not intended to be accessible
- Attack exploits a lack of security as opposed to exploiting a bug in the code

With a system vulnerable to Directory Traversal, an attacker can make use of this vulnerability to step out of the root directory and access other parts of the file system. This might give the attacker the ability to view restricted files, or even more dangerous, allowing the attacker to execute powerful commands on the web server which can lead to a full compromise of the system.

To prevent users from accessing unauthorized files on the Web server, Web servers provide two main security mechanisms: the root directory and access controls lists. The root directory limits users' access to a specific directory in the Web server's file system.

All files placed in the root directory and in its sub-directories are accessible to users. To limit users' access to specific files within the root directory, administrators use access control lists. Using access control lists, administrators can determine whether a file can be viewed or executed by users, as well as other access rights.

The root directory prevents attackers from executing files such as cmd.exe on Windows platforms or accessing sensitive files such as the "passwd" password file on Unix platforms, as these files reside outside of the root directory. The Web server is responsible for enforcing the root directory restriction. By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute powerful commands on the Web server, leading to a full compromise of the Web server.

---

### **Zero Day Attacks**

- Threat that exploits vulnerabilities that are unknown to others or the software developer
- Occur during the vulnerability window

Vulnerability Window-time between when vulnerability is first exploited and when software developers start to develop a counter to that threat.

For viruses, Trojans and other zero-day attacks, the vulnerability window follows this time line:

1. Developer creates software containing an unknown vulnerability
2. Attacker finds the vulnerability before the developer does
3. Attacker writes and distributes an exploit while the vulnerability is not known to the developer
4. Developer finds the vulnerability and starts developing a fix

---

### **Malicious Add-On's**

- Software add-on's used to view certain web content/web pages
- Some are created with malicious intent, such as exploiting a vulnerability in a browser
- Have been created for every browser

---

## **Analyze and differentiate among types of mitigation and deterrent techniques**

---

### **Manual bypassing of electronic controls:**

- **Fail Secure** - System that is able to resort to a secure state when an error or security violation is encountered
- **Fail Safe** - A device, in the event of failure, responds in a way that will cause no harm, to other devices or danger to personnel

- **Fail Soft** - A fail-soft system is a system designed to shut down any nonessential components in the event of a failure, but keep the system and programs running on the computer.
- 

- **Fail Closed**- Device/system fails and denies everything
  - Examples:
    - A firewall fails and rejects all packets
    - A door fails and cannot be unlocked
    - An IPS fails and stops all traffic
    - Have to consider personnel safety for some physical security implementations (Locks)

Say you're building a corporate firewall. What happens when it encounters a fatal error and can't figure out what's a good packet and what's a bad packet? Should it shut down and leave the device open (fail open), or should it just stop evaluating and reject every packet (fail closed)? Arguments could be made for both options.

What if you're building a system to regulate the flow of oxygen to a deep sea submersible? Say the software encounters an error and has to shut down. Without regulation from the software, should the valve stay open or closed?

Think about magnetically controlled doors. Does the magnet hold the bar in the locked position against the tension device trying to unlock it? Or does the magnet hold the bar in the unlocked position, against the tension device trying to lock it? The answer is the difference between whether the door is locked or unlocked on a power failure (assuming the magnet needed power to have force). One answer is good for complete security (lock on power failure), but then what happens to the fire escapes?

---

### Monitoring system logs

#### Logging Procedures

- Any information possibly needed to reconstruct events should be logged
- Do not over audit
- Retention policy should be in place
- Hash the logs for integrity checking

Most systems generate security logs and audit files of activity. These files do absolutely no good if they aren't periodically reviewed for unusual events. Many web servers provide message auditing, as do logon, system, and application servers. The amount and volume of information these files contain can be overwhelming. You should establish a procedure to review them on a regular basis.

Audit files and security logs may also be susceptible to access or modification attacks. The files often contain critical system information, including resource sharing, security status, and so on. An attacker may be able to use this information to gather more detailed data about your network.

### Logging Types

- Syslog
  - Windows Logs
  - Application/Software Logs
  - Network Device Logs:
    - Firewalls
    - Routers
    - WAP/RADIUS
    - DNS
    - Domain Controller
- 

### Log Storage

- Restrict access to all logs
- Security Policy
  - Address the size of logs
  - How often they should be archived
  - Retention times
  - Storage Media

Restrict access to all logs. By default, users have read permission on all logs except the security log. Only those who have been assigned to manage logs should have access to them.

---

## Physical Access Security

### Keys and Locks

- Most common form of access control
- Key locks
- Combination locks
- Keypad/Cipher locks
- Smart locks
- Key Log
- Physical access logs/lists

Key Log: All key distribution should be logged and updated whenever keys are issued or recalled.

Physical access logs/lists: When a card reader or cipher lock is used, it can create a log file of all access into and out of a building or room. Sign-in logs are used for logging visitors to a controlled environment.

---

### Mantrap

- Controls access and authentication
- Requires visual identification to gain access.
- Prevents Piggybacking/Tailgating
- Dual locked door facility

### **Closed Circuit Television (CCTV)**

- Used as a deterrent and detective mechanism after an event
- CCTV may introduce privacy concerns
- Inform users they are being recorded

CCTV monitors areas to detect intruders and emergency situations. CCTV can also be used as a detective mechanism after an event has occurred when investigators review footage to identify suspects

CCTV can also be used as a deterrent to make intruders think twice about trespassing if they understand that they will be recorded.

---

**Lighting:** should be adequate for the camera type being used; Infrared (IR) lighting is available for use in total darkness.

**Lenses:** fixed lenses are cheaper; zoom lenses give the ability to see at greater distances or view a wider area.

**Recording:** policies should be in place regarding how long recordings from CCTV are held. Recordings, whether digital or analog, should be protected from tampering and theft.

**Pan Tilt Zoom (PTZ):** offers the ability to change the focal area of a camera.

Human monitoring: motion detection and analysis software can supplement human monitoring, but a human should always be monitoring CCTV signals to help identify problems and sound alarms.

**Human monitoring** – motion detection and analysis software can supplement human monitoring, but a human should always be monitoring CCTV signals to help identify problems and sound alarms

---

### **Fencing**

- A perimeter defining device
  - Include a wide range of components, materials and construction methods
    - Chain link
    - Barbed wire
    - Concrete walls
    - Invisible (lasers)
  - Deterrents:
    - 3 to 4 feet (deter casual trespassers)
    - 6 to 7 feet (deter most intruders)
    - 8 feet or > with barbed wire (deter determined intruders)
-

## Bollards



## Proximity Readers

- Used for physical access
- Contactless
- User has a card, when placed in proximity to the reader the card is powered and transmits the cards ID to the reader, granting access
- Physical theft of card a concern

A Proximity reader radiates a 1" to 20" electrical field around itself. Cards use a simple LC circuit. When a card is presented to the reader, the reader's electrical field excites a coil in the card. The coil charges a capacitor and in turn powers an integrated circuit. The integrated circuit outputs the card number to the coil which transmits it to the reader.

---

## Port Security

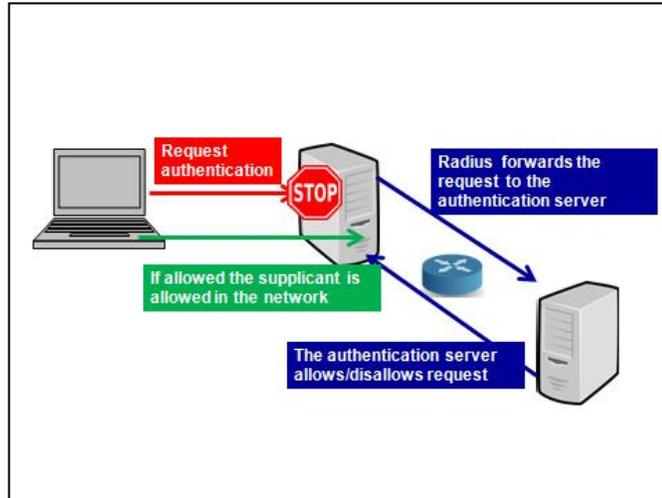
### MAC Filtering

- Restricting access to a network via authorized MAC address
- Can be used to strengthen security on a switch or AP
- Can be circumvented, MAC's can be spoofed

MAC filtering is like handing a security guard a pad of paper with a list of names. Then when someone comes up to the door and wants entry, the security guard looks at the person's name tag and compares it to his list of names and determines whether to open the door or not. Do you see a problem here? All someone needs to do is watch an authorized person go in and forge a name tag with that person's name. The comparison to a wireless LAN here is that the name tag is the MAC address.

### Extensible Authentication Protocol (EAP) 802.1X - Pass through port authentication

- Authentication framework, not a specific authentication mechanism
- Used over PPP and Wireless LANs
- Provides over 40 authentication methods



---

## Implement assessment tools and techniques to discover security threats and vulnerabilities

### Software Testing

An investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing also provides an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include, but are not limited to, the process of executing a program or application with the intent of finding software bugs. Software testing can also be stated as the process of validating and verifying that a software program/application/product:

- Meets the business and technical requirements that guided its design and development
- Works as expected
- Identify common security misconfigurations .

Software testing, depending on the testing method employed, can be implemented at any time in the development process. However, most of the test effort occurs after the requirements have been defined and the coding process has been completed. As such, the methodology of the test is governed by the software development methodology adopted.

---

Three testing methods can be utilized for testing software

### Black Box

- Examines a program from a user perspective
- Testers do not have access to internal code

### White Box

- Examines the internal logical structures of a program, line by line, for errors

### Gray Box

- Combines both (White and Black)
- Testers approach the software as a user, and have access to the source code (Source code is used to develop tests to be run as a user)

### More examples:

**Black box** testing treats the software as a "black box"—without any knowledge of internal implementation.

**White box testing** is when the tester has access to the internal data structures and algorithms including the code that implement these.

The following types of white box testing exist:

- API testing (application programming interface) - testing of the application using public and private APIs
- Code coverage- creating tests to satisfy some criteria of code coverage (e.g., the test designer can create tests to cause all statements in the program to be executed at least once)
- Fault injection methods - improving the coverage of a test by introducing faults to test code paths
- Mutation testing methods
- Static testing- White box testing includes all static testing

**Gray box testing** involves having knowledge of internal data structures and algorithms for purposes of designing the test cases, but testing at the user, or black-box level.

---

### Vulnerability Assessments

- Process of identifying, quantifying, and prioritizing vulnerabilities in a system
- Accomplished by:
  - **System scanning:** uses tools to test the effectiveness of your security perimeter by actively looking for system vulnerabilities. Scanning helps assure the effectiveness of an organization's security policy, security mechanism implementations, and deployed countermeasures.
  - **Footprinting:** the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the

## Domain 4 - Threats and Vulnerabilities

environment. It is the combination of active and passive reconnaissance techniques for the purposes of establishing a strategy of attack.

- **Fingerprinting:** the process of discovering the underlying operating system on a device
- Audit should give detailed information on tools used, when scan was conducted, vulnerabilities found with risk levels
- Senior management approval needed

---

### Risk Mitigation

- Implement countermeasures to protect against potential risks.
- Perform a Cost Benefit Analysis.
- Sometimes, the cost of some countermeasures may outweigh the cost of their targeted risks.

#### Identify Threats

- Natural
- Manmade

#### Threat Motivations

- Disgruntled Employee
- Espionage

#### Threat Capabilities

- Script Kiddies
- Organized Crime

For a risk to be realized, an asset must be lost which also means that a threat must be present. For each risk that is identified, a related threat should be listed.

---

## Network and Systems Security Threats

### Protocol Analyzers

- Hardware or software that gathers packet-level traffic across the network
- Placed in-line or between devices
- Used for logging, sniffing, network monitoring, troubleshooting, etc.
- Tools:
  - Wireshark
  - Snort
  - Kismet

---

### Packet Sniffing on the Network

- When a wired NIC (Network Interface Card) is put in promiscuous mode, the NIC captures all traffic on the network segment it is installed.
- When a wireless Interface Card (WIC) is put in monitor mode, the WIC captures all traffic on the frequencies it monitors.

### **Penetration Testing (Pen Test)**

- An attempt to break into your own secured network
- Third party is preferred
- Typically performed from the internet
- Get written approval prior to conducting tests

The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution.

---

Penetration Testing looks for vulnerabilities such as:

- Poor or improper system configuration
- Known or unknown hardware or software flaws
- Application weaknesses
- Can involve active exploitation of vulnerabilities

Report presented to system owner

- Lists vulnerabilities discovered
  - An assessment of impact vs. probability
  - A proposal for mitigation or a technical solution
- 

### **Vulnerability Scanning**

- Running software which contains a database of known vulnerabilities against a system
- Detects potential vulnerabilities
- Tools
  - Protocol Analyzers
  - Vulnerability Scanners (OVAL)
  - Port Scanners
  - Network Mappers
  - Password Crackers

Vulnerability scanning tools can help secure a network or it can be used by the attackers to identify weaknesses in your system. These tools should be used by security professional identify and fix these weaknesses before intruders use them against you. Different scanners accomplish this goal through different means and some work better than others.

Retina and Gold Disk are vulnerability scanning tools used by the Department of Defense.

---

### **Open Vulnerability and Assessment Language (OVAL)**

- Sponsored by the US Department of Homeland Security
- Standardizes vulnerability testing
  - How described and reported
  - An XML schema and repository of vulnerabilities

The Open Vulnerability and Assessment Language (OVAL) is a community standard written in XML that strives to promote open and publicly available security content. It consists of a language, interpreter, and repository and is meant to standardize information between security tools.

The language standardizes the three main steps of the assessment process:

- Representing configuration information of systems for testing
- Analyzing the system for the presence of the specified machine state vulnerability, configuration, patch state, etc.)
- Reporting the results of this assessment

The repositories are collections of publicly available and open content that utilize the language.

---

### **Network Mappers**

- Used to create network maps
- Tools:
  - Nmap
  - SolarWinds
  - Whats Up Gold

### **Mapping Techniques:**

- Active Probing
- Route Analytics
- SNMP

There are three main techniques used for network mapping:

- Active Probing approach: relies on a series of Trace route-like probe packets in order to build the network map
  - Route Analytics approach: relies on information from the routing protocols to build the network map
  - SNMP: retrieves data from Router and Switch MIBs in order to build the network map
- 

### **Password Crackers**

- Software utility that allows direct testing of a user's logon password strength
- Deciphers passwords using:

- Brute force decryption
- Dictionary look-up

Examples:

- Cain and Abel
- L0phtCrack
- John the Ripper

Password guessing attacks occur when an account is attacked repeatedly. This is accomplished by utilizing applications known as password crackers, which send possible passwords to the account in a systematic manner. The attacks are initially carried out to gain passwords for an access or modification attack.

These types of password-guessing attacks were covered early in module 1:

**Brute-force attack**

**Dictionary attack**

**Rainbow Attack**

---

### **Vulnerability Scanners**

Computer program designed to assess computers, computer systems, networks or applications for weaknesses

- Port scanner
- Ping scanner
- Network enumerator
- Network vulnerability scanner
- Web application security scanner
- Database security scanner
  
- Vulnerability scanners:
  - Nessus
  - SAINT
  - NMAP
  - Retina

**Nessus** is a vulnerability scanner. It scans one or more computers remotely via the network:

- It does a port scan and tries various exploits on the open ports
- It searches for misconfiguration, (e.g. open mail relay, database)
- It checks for missing security patches
- It searches for trojans and backdoors that are listening on a port
- It tries to provoke buffer overflows
- It searches default passwords and blank passwords
- It tries DOS attacks sending mangled packets
- It can remotely detect the version of installed antivirus software

- It can check for improper network segmentation
- The scanner can be scheduled to scan the company network every night

---

### Port Scanners

- Probes for all enabled TCP/UDP ports
- Used by system administrators or attackers
- Prot scanners tools:
  - SuperScan
  - NMAP
  - Nessus

### PING Scanner

Uses ping (ICMP) messages to identify systems that are on the network

Ping is an administration utility used to test whether a particular device is reachable across a network. It sends ICMP echo request packets to a target device and waits for an ICMP response. Ping also measures the round-trip time for packets sent from the local host to a destination host, including the local host's own interfaces.

---

### Honey Pots

- A bogus system that appears to be a production server
- Configured with pseudo flaws
- Can be used to learn the hacking techniques and methods that hackers employ
- Padded Cell
- HoneyNet
- Enticement vs. Entrapment

The purpose of a honey pot is to allow itself to succumb to an attack. During the process of “dying,” the system can be used to gain information about how the attack developed and what methods were used to institute the attack. The benefit of a honey pot system is that it draws attackers away from a higher-value system or allows administrators to gain intelligence about an attack strategy.

*Enticement* : is the process of luring someone into your plan or trap. You might accomplish this by advertising that you have free software, or you might brag that no one can break into your machine. If you invite someone to try, you’re enticing them to do something that you want them to do.

*Entrapment*: is the process in which you encourage or induce a person to commit a crime when the potential criminal expresses a desire not to go ahead. Entrapment is a valid legal defense in a criminal prosecution.

---

### Configuration Baselines (CB)

- Establishes the mandatory settings that systems must have in place to be accepted for use in the network

## Domain 4 - Threats and Vulnerabilities

- May also mark an approved security configuration item, e.g. security templates, that have been signed off for execution

For information assurance, Configuration Baselines can be defined as the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

---

### Code Review

- Systematic examination of computer source code
- Intended to find and fix mistakes overlooked in the initial development phase
- Can often find and remove common vulnerabilities
- Program managers schedule meetings throughout the process
- Development personnel walk through the code looking for design/security flaws

Code reviews should be a regular part of your development process. Security code reviews focus on identifying insecure coding techniques and vulnerabilities that could lead to security issues. The review goal is to identify as many potential security vulnerabilities as possible before the code is deployed. The cost and effort of fixing security flaws at development time is far less than fixing them later in the product deployment cycle.

---

### Design Reviews

- Part of the development process for a secure system
- Determine how various parts of the system will interoperate
- Coding milestones are laid out by the design management team
- Review meeting is conducted to ensure that everyone is in agreement and the process is still on track

## Domain 5 – Compliance and Operational Security

### Domain Objectives

A Security+ candidate is expected to:

- Explain risk related concepts
  - Carry out appropriate risk mitigation strategies
  - Execute appropriate incident response
  - Explain the importance of security related awareness and training
  - Compare and contrast aspects of business continuity
  - Explain the impact and proper use of environmental controls
  - Execute disaster recovery plans and procedures
  - Exemplify the concepts of confidentiality, integrity and availability
- 

### Risk Related Concepts

#### Security Control Types

- Methods used to classify controls are based on:
    - Nature of control
    - Objective of the control
  - Three popular control types
    - Technical
    - Management
    - Operational
- 

#### Technical Controls

Technical measures within the organization to enhance security of a network or system

- Strong User authentication
- Firewall technologies (hardware and software)
- Antivirus protection
- IDS/IPS implementation
- ACL's on routers
- Filtering of content
- Encryption technologies

Technical security controls are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information.

Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems

---

### Management Controls

Policies and procedures put into place to define and guide employee actions in dealing with sensitive information:

- Proper data classification
- Security Awareness program
- Configuration management

Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information.

For example, a human resources policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information.

Requiring that information be classified and the process to classify and review **information classifications** is another example of an administrative control.

The organization **security awareness program** is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.

### Configuration Management

IT configuration management is the process of “creating and maintaining an up-to-date record of all the components of the infrastructure,” according to Wikipedia, including related configuration details, documentation, and other information that describes the various computer systems that make up an architecture. For software, this can include versions, updates, and patches. For servers and other hardware, it may encompass the location and address of each device.

---

### Operational Controls

- Operational controls define how people in the organization should handle data, software and hardware.
- Mechanisms and daily procedures that provide protection for systems
- Should be transparent to users
- Should also include environmental and physical protections as described below:
  - **Physical security:** which shields the organization from attackers attempting to gain access to its premises; examples include sensors, alarms, cameras, and motion detectors.
    - Protection of computing facilities: by physical means such as guards, electronic badges and locks, biometric locks, and fences.

## Domain 5 – Compliance and Operational Security

- Physical protection for end-user systems: including devices such as mobile computer locks and alarms and encryption of files stored on mobile devices.
  - Media access control and disposal procedures: to ensure that only authorized personnel have access to sensitive information and that media used for storing such data is rendered unreadable by degaussing or other methods before disposal.
  - Backup systems and provisions for offsite backup storage: to facilitate the restoration of lost or corrupted data. In the event of a catastrophic incident, backup media stored offsite makes it possible to store critical business data on replacement systems.
  - **Environmental security**: which safeguards the organization from environmental threats such as flood and fires; examples include smoke and fire detectors, alarms, sensors, and flood detectors.
    - Fire protection system: such as automated fire suppression systems and fire extinguishers, which are essential tools for the guarding the organization's key assets.
    - Temperature and humidity control systems: that extend the life of sensitive electrical equipment and help to protect the data stored on them.
    - Emergency backup power: which can save sensitive electrical systems from harm during power brownouts and blackouts; they can also ensure that applications and operating systems are shutdown gracefully manner to preserve data and transactions.
- 

### Control Categories

- **Preventive** – Stop unwanted / unauthorized activity
  - **Deterrent** – Discourage a potential attacker
  - **Detective** – Identify an incident's activities
  - **Corrective** – Fix systems after an incident
  - **Recovery** – Restores resources and capabilities
  - **Directive** – Controls put in place due to regulation or environmental requirement
  - **Compensating** – Provide alternatives to other controls (security policy, personnel supervision)
- 

### Policies Used for Reducing Risk

#### Security Policy

- Dictates the security structure of an organization

## Domain 5 – Compliance and Operational Security

- Establishes the goals of the security program how it is organized, and the responsibilities, etc.
- Should be made available both in print and online through secure internal access
- To be effective, the security policy must be:
  - **Planned:** Good security is the result of good planning.
  - **Maintained:** A good security plan must be constantly evaluated and modified as needs change.
  - **Implemented:** The most common failure of a security policy is the lack of user awareness. The most effective way of improving security is through user awareness.
- Should address the following:
  - Mandatory Vacations
  - Job Rotation
  - Separation of Duties
  - Least privilege
  - Need to Know

---

### A good security policy should cover the following:

#### Privacy Policy Requirements

- Organization must clearly state what information can and can't be disclosed
- State who is entitled to ask for information within the organization
- Covers what types of information are provided to employees
- Policy should clearly state to employees that they should have no expectations of privacy
  - Desks, files and other items may be searched
  - E-mail, voice communications are monitored

#### Acceptable Use Policy

- Deals primarily with computers and information provided by the company
- Should clearly stipulate what activities are allowed and not allowed
- Must be enforced
- Some of the areas covered:
  - Web access
  - Telephone usage
  - Information usage
  - System usage

Acceptable Use Policy (AUP) is a set of rules applied by the owner/manager of a network, website or large computer system that restrict the ways in which the network site or system may be used. AUP documents are written for corporations, businesses, universities, schools, internet service providers, and website owners often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

## Domain 5 – Compliance and Operational Security

Acceptable Use Policies are an integral part of the framework of information security policies; it is often common practice to ask new members of an organization to sign an AUP before they are given access to its information systems. For this reason, an AUP must be concise and clear, while at the same time covering the most important points about what users are, and are not, allowed to do with the IT systems of an organization. It should refer users to the more comprehensive security policy where relevant. It should also, and very notably, define what sanctions will be applied if a user breaks the AUP. Compliance with this policy should, as usual, be measured by regular audits.

---

### Risk Management

- The process of identifying, reducing, and controlling risks to an acceptable level.
  - Includes:
    - Risk Analysis
    - Evaluation of Safeguards
    - Cost Benefit Analysis
    - Implementation of Safeguards
- 

### Risk Analysis Calculations

In order to understand the result of a risk you will be to consider the following:

- **Likelihood** - How likely could this risk happen in our environment?
  - **Annualized Loss Expectancy (ALE)** – If the risk happen how much would it cost us a year to recover from it.
  - **Impact** – What will this risk do to my company's reputation, recovery time etc.
- 

### Two major risk analysis types:

- **Quantitative Analysis**
    - Assigns "real" numbers to the costs of damages and countermeasures
    - Assigns concrete probability percentages to risk occurrence
  - **Qualitative Analysis**
    - Uses scenarios to identify risks and responses
    - Does not produce hard numbers
- 

### Quantitative Analyses Process

- Identify threats, vulnerabilities, and impacts
  - Determine relative risk for each threat against each asset
  - Used in a cost benefit analysis
  - Used to identify estimated cost in dollars
- 

### Uses Cost-Benefit Formulas:

- **Exposure Factor (EF):**
  - % of loss experienced by a *realized* risk
- **Single Loss Expectancy (SLE):**
  - Asset Value \* Exposure Factor

## Domain 5 – Compliance and Operational Security

- **Annualized Rate of Occurrence (ARO):**
    - Frequency of Occurrence per Year
  - **Annualized Loss Expectancy (ALE):**
    - Maximum amount that should be spent on the countermeasure (SLE \* ARO)
- 

### Risk Mitigation Countermeasures

- Implement countermeasures to protect against potential risks

### Perform a Cost Benefit Analysis

Sometimes, the cost of some countermeasures may outweigh the cost of their targeted risks. The following could be the result:

- **Risk avoidance**
    - Not performing an activity that could carry risk
  - **Risk transference**
    - Shifting of the burden of loss to another party through legislation, contract, insurance or other means
  - **Risk acceptance**
    - Cost of a countermeasure outweighs the loss due to a risk
    - A risk has been identified, accepted and the organization accepts the consequences of the loss if the risk is realized
  - **Risk Deterrence**
    - Put something in place that will make it so the attacker will not want to perform the **malicious** act because of the consequences.
  - **Risk Mitigation**
    - Reducing either the probability or consequences of a threat. These may range from physical measures (protective fences) to financial measures (stockpiling cash, insurance)
- 

### Carry out appropriate risk mitigation strategies:

- **Change Management**
    - Ensure changes do not reduce security
  - **Incident Management**
    - Incidents are handled in the accordance with your Incident Response policy/plan
  - **User Rights and Permission Reviews**
    - Prevents users from having elevated privileges
  - **Routine audits**
    - Discovers fraud within the organization
  - **Data loss or theft prevention policy**
    - Mitigates the chances of data from an organization being lost or stolen
- 

## Incident Response Procedures

### Incident Response Policy

## Domain 5 – Compliance and Operational Security

- Defines how an organization will respond to an incident
  - Develop procedures to respond to incidents before they occur
  - Due diligence up front will help the business survive in the event of a disaster
- 

- At a minimum, establish the following:
    - Policies and procedures regarding how to handle the incident
    - Procedures to gather and secure evidence
    - List of information that should be collected about the incident
    - Outside agencies that should be contacted or notified in case of an incident
    - Outside experts who can be used to address issues if needed
- 

### Steps to Incident Response

1. **Preparation** setting up systems to detect threats and policies for dealing with them, including identifying roles staff will play in incident response, and creating emergency contact lists

2. **Identification** identifying what the threat is, and/or the effects it is having on your systems/networks, including keeping records of the time/systems involved/what was observed, and making a full system backup as soon after the intrusion was observed, as possible, to preserve as much information about the attack as you can

3. **Containment** limiting the effects of an incident by confining the problem to as few systems as possible, freezing the scene so that nothing further happens to the compromised system(s) by disconnecting its network connections and possibly console keyboard

4. **Eradication** getting rid of whatever the attacker might have compromised by deleting files or doing a complete system reinstall – should err on the side of deleting MORE rather than less in order to restore a system to production, since the intruder may have left very-well disguised Trojan Horse binaries around the system, to be activated once the system is reconnected to the Internet

5. **Recovery** getting back into business, by putting the system back into normal operations, reconnecting it to the network, restoring from backups if necessary, etc.

6. **Follow up** if possible tightening security so that the intrusion cannot happen again, determining the “cost” of the intrusion based on staff time/lost data/lost user work time (don’t skip this! It may help justify security expenditures in the future), considering which, if any, additional tools might have helped handle the incident better than it may have been handled, reflecting on “lessons learned” from both the intrusion and the organization’s response to it and tweaking policies as required).

### Types of Evidence

## Domain 5 – Compliance and Operational Security

**Best-** Primary evidence used in trial as it provides the most reliability; e.g. when a signed document is used as evidence, the original must be used.

**Secondary-** Copies of the original; not viewed as reliable and strong; oral evidence, such as testimony of a witness, or copies of a signed document.

**Direct -** Oral testimony based on evidence gathered through the witness's five senses; can prove a fact all by itself, does not need backup info to refer to; can be testimony from an eye witness.

**Conclusive-** Irrefutable and cannot be contradicted, stands by itself without corroboration (DNA).

**Opinion-** A witness testifies only to the facts not their opinion of the facts. An expert witness is the exception when their opinion is what is needed.

**Circumstantial-** Can prove an intermediate fact that can be then used to deduce or assume the existence of another fact.

**Hearsay-** What someone has told the witness.

### Evidence Life Cycle

- Ensures data integrity
    - Identification
    - Preservation
    - Transportation
    - Presentation in court
    - Return to owner, destroy, permanent archive
- 

### Basic Forensic Procedures

**Order of volatility:** Should proceed from the most volatile to the least

- Example;
    1. Register Cache
    2. Routing Table, Memory
    3. Temporary File System
    4. Disks or other storage media
    5. Remote logging and monitoring data
- 

### Capturing a system image

- **Data acquisition:** Taking possession of or obtaining data and adding it to evidence
- **Data duplication**
  - Making a copy of data acquired to preserve the original
  - It is crucial that data is not lost during the acquisition process

## Domain 5 – Compliance and Operational Security

- Once acquired and duplicated, forensic work is done on the copies (protects against malware threats, preserves the original)
- 

- Common methods for acquiring data from a system:
  - **Bit-stream disk to image file**
    - Most common, image original disc to another disc
    - Can create numerous copies
  - **Bit-stream disk to disk copy**
    - Streaming programs that copy data from one disk to another
  - **Sparse data copy**
    - Data only pertinent to the case is copied (i.e. certain files or folders)
- 

### Network traffic and logs

- Ports used, last logged in, UserID used, URL accessed

### Capture any video evidence

- Any surveillance video needs to be identified and secured

### Record time offset

- Systems clocks may be out of sync with local time
- 

### Take hashes

- Used to verify the integrity of your digital evidence

### Screenshots

- Take pictures of any alarms generated, and pictures of the desktop screen

### Witnesses

- Identified, initial interview, sign a witness consent form

### Track man hours and expense

---

### Damage and loss control

- Powered off computers
    1. If switched off, leave off
    2. Do not want to change the state of the device
  - Powered on computers
    1. Stop and think before taking any action
    2. RAM may contain vital information, if powered off and it could be lost
    3. Take photos of screen if viewable
- 

### Chain of Custody

- Process to keep track of individuals that have accessed evidence
  - Improper evidence handling could result in legal complications, which can consequently prevent prosecution
  - Carefully manage the chain of custody form during and after the forensic investigation
- 

### Chain of Custody Form

- Form should include:

## Domain 5 – Compliance and Operational Security

- Individuals that discovered the evidence
  - Exact location of evidence discovery
  - Date/time when the evidence was discovered
  - Individuals who initially processed the evidence
  - If the evidence changed possession, then the exchanging parties should sign the document
- 

### Preservation of Evidence

- Digital evidence must be handled with care
  - After removing it from the system it should be:
    - Placed in a container
    - Properly labeled (Use permanent marker)
    - Sealed
    - Signed / Dated (Use permanent ink)
    - Container should be locked
  - A copy of the evidence should be used for analysis
- 

### First Responder

The person who first arrives at the crime scene and accesses the system once the incident has been reported. They may be:

- A network administrator
- Law enforcement officer
- Investigating officer
- Person from the forensics lab

They will conduct the initial investigation and are responsible for protecting, integrating and preserving the evidence so it is acceptable in a court of law.

---

## The Importance of Security Related Awareness and Training

### User Awareness Training

- Ensure that information is conveyed to the appropriate people in a timely manner
  - The more staff is aware of security, the more likely to support, uphold, and strengthen the security program
  - Security Awareness Education
  - Security Policy should cover:
    - Training
    - Sign document (placed in personnel file)
- 

Security planning should not end with documentation. After the plan is formulated, users need to know about it.

The best plan isn't any good unless people follow it. Therefore, the plan should include procedures on:

- How to keep users aware of the items of the plan
- How to train users

## Domain 5 – Compliance and Operational Security

- How to educate users
  - How to make documentation available to users
- 

### Areas to cover

- Protection of Personally Identifiable Information (SSN, bank account number, etc)
  - Compliance with laws, BBP's, standards
  - Proper data labeling, handling and disposal
  - Proper user habits;
    - Password protection
    - Data handling
    - Clean desk policy
    - Social Engineering Prevention (Tailgating, dumpster diving, etc)
    - Personally owned devices (USB, CD's, etc)
-

### Threat Awareness

- New malware
  - Phishing schemes/attacks
  - Zero day exploits
  - Security issues with:
    - Social Networking sites (Facebook, MySpace, etc)
    - P2P file sharing (Bitorrents, Kazaa, Frostwire)
- 

## Disaster Recovery Procedures

### Business Continuity Planning (BCP)

- Goal is to maintain business operations with reduced or restricted infrastructure
- Implement policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes
  
- Business Impact Analysis
- Assessing Risk

Business continuity planning (BCP) is the planning which identifies the organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, whilst maintaining competitive advantage and value system integrity. The logistical plan used in BCP is called a business continuity plan. The intended effect of BCP is to ensure business continuity, which is an ongoing state or methodology governing how business is conducted.

In layman's terms, BCP is working out how to stay in business in the event of disaster. Incidents include local incidents like building fires, regional incidents like earthquakes, or national incidents like pandemic illnesses.

---

**Avoid/Remove Single points of failure** - Clustering servers, redundant network protocols/devices, redundant power, backups, etc

### Properly plan and test your BCP

**Continuity of operations-** -various measures designed to ensure that the organization continues operating

**Disaster Recovery** - subset of business continuity

**Succession planning**-process for identifying and developing internal people to fill key leadership positions

---

### Business Impact Analysis (BIA)

- Identify critical business functions

## Domain 5 – Compliance and Operational Security

- Prioritize critical business functions
  - Establish a timeframe of critical systems loss
  - Estimate tangible and intangible impact
  - Assessing Risk
    - Identify exposed risks to the organization
    - Identify risks that need to be addressed
    - Coordinate with BIA
- 

### Impact and Proper Use of Environmental Controls

#### Environmental Factors

- Building location and construction
  - HVAC
  - Fire suppression
  - Power supply
  - Shielding
- 

#### Location

- The type of data should be considered when determining facility locations
  - Location Considerations
  - Visibility
  - Accessibility
  - Propensity for environmental problems

Many organizations place their facilities in areas where the buildings will be unnoticeable or indistinguishable from other buildings in the area. Also popular are areas with mountainous terrain that can block electrical signals coming from equipment within the facility. Such terrain can counteract any malicious eavesdropping. The surrounding area should be analyzed based on crime statistics, location of emergency response facilities (such as police, fire, and medical), and any other potential hazards, such as factories producing explosive or combustible materials.

Other factors in selection are the impacts of traffic and the location of major transportation arteries, including airports, train stations, and freeways. The site should have adequate access for the smooth entrance and exit of personnel and emergency response vehicles, but be restrictive enough to maintain a secure environment.

---

#### Heating, Ventilation, Air Conditioning (HVAC)

The location of your computer facility is critical to its security. Computer facilities must be placed in a location that is physically possible to secure. Additionally, the location must have the proper capabilities to manage temperature, humidity, and other environmental factors necessary to the health of your computer systems.

- Temperature
  - Between 60 and 75 degrees Fahrenheit
    - Possible heat damage (>75 degrees)
- Humidity
  - Between 40% and 60%

## Domain 5 – Compliance and Operational Security

- Electrostatic damage (<40%)
- Condensation/corrosion (>60%)

Constant Increases and decreases in temperature over time can loosen some hardware from their connectors (RAM chips for instance). This loosening of hardware is often referred to as chip creep. Chip creep can also occur when there are fluctuations in power flowing through the device. While chip creep is still a concern with systems, it has been mitigated by devices such as chip anchors, and clips to hold and retain the hardware in place.

**Hot aisle/cold aisle:** Is an accepted best practice for cabinet layout within a data center. The design uses air conditioners, fans, and raised floors as a cooling infrastructure and focuses on separation of the inlet cold air and the exhaust hot air.

Cabinets are adjoined into a series of rows, resting on a raised floor. The fronts of the racks face each other and become cold aisles, due to the front-to-back heat dissipation of most IT equipment. Computer Room Air Conditioners (CRACs) or Computer Room Air Handlers (CRAHs), positioned around the perimeter of the room or at the end of hot-aisles, push cold air under the raised floor and through the cold aisle, Perforated raised floor tiles are placed only in the cold aisles concentrating cool air to the front of racks to get sufficient air to the server intake.

---

### Fire Suppression

Fire suppression is a key consideration in computer-center design. Fire suppression is the act of actually extinguishing a fire versus preventing one. Two primary types of fire-suppression systems are in use: fire extinguishers and fixed systems.

Fire extinguishers are portable systems. The selection and use of fire extinguishers is critical. Four primary types of fire extinguishers are available, classified by the types of fires they put out: A, B, C, and D.

Class	Use	Suppression Medium
A	Common Combustible	Water or foam
B	Liquids	CO <sub>2</sub> , Halon, foam, or dry powder
C	Electrical	CO <sub>2</sub> , Halon, or dry powder
D	Metal	Dry powder

Fixed systems are usually part of the building systems. The most common fixed systems combine fire detectors with fire-suppression systems, where the detectors usually trigger either because of a rapid temperature change or because of excessive smoke. The fire-suppression system uses either water sprinklers or fire-suppressing gas. The one drawback to water-based systems is that they cause extreme damage to energized electrical equipment such as computers. These systems can be tied into

## Domain 5 – Compliance and Operational Security

relays that terminate power to computer systems before they release water into the building.

Gas-based systems were originally designed to use carbon dioxide and later Halon gas. Halon gas damages the ozone layer and is being phased out of systems; environmentally acceptable substitutes are now available. The principle of a gas system is that it displaces the oxygen in the room, thereby removing this necessary component of a fire. The major drawback to gas-based systems is that they require sealed environments to operate. Special ventilation systems are usually installed in gas systems to limit air circulation when the gas is released. Gas systems are also expensive, and they're usually only implemented in computer rooms or other areas where water would cause damage to technology or other intellectual property.

---

### Water-based Systems

- **Wet pipe system:** always full of water and once the trigger is activated the suppression medium is released into the environment.
  - **Dry pipe system:** full of air. When the trigger is activated the air is released allowing the pipe to fill with water and to immediately release into the environment.
  - **Deluge system:** an extension of a wet or dry pipe system which enables all release heads simultaneously rather than just those heads triggered by the fire.
  - **Pre-action System:** a dry pipe system with two triggering mechanisms. The first trigger is activated, the pipes fill with water. Only after the second trigger is activated is the water released into the environment to suppress the fire. A pre-action system gives you the option of disabling the release of water if the fire is contained or in the case of a false alarm. The ability to halt the release of the suppression medium makes it the most suitable for a data center.
- 

### Utilities

Basic utilities such as electricity, water, and gas are key aspects of business continuity. Usually, these are restored pretty quickly at least on an emergency basis. In the case of a major disaster though, they may be unavailable for days, weeks, or months. As an administrator you need to be aware of problems and how you are going to approach them. You can't plan for every conceivable situation, but you need to plan for those that have a high likelihood of occurring.

---

### Power Considerations

Computer systems are susceptible to power and interference problems. A computer requires a steady input of AC power to produce reliable DC voltage for its electronic systems. Power systems are designed to operate in a wide band of power characteristics; they help keep the electrical service constant, and they ensure smooth operations.

### Uninterruptible Power Supply (UPS)

- An UPS uses batteries to maintain power until the primary power supply is restored

## Domain 5 – Compliance and Operational Security

- UPS units can operate on a standby basis or as online systems. Standby units stay inactive until a critical power event occurs. The system has sensors that can detect fluctuations and respond accordingly.
- The capacity and size of a UPS should be related to how critical the devices being powered are to the network. If they are vital networking pieces, the UPS should have considerable battery power to maintain critical networking function until power is restored.

### Backup generator

If a considerable outage occurs, a backup power source, such as a generator, may be needed.

The size and type of an appropriate generator depends on what's needed at the facility and should be directly correlated to just how important the equipment in the facility is.

**Surge protectors:** Protect electrical components from momentary or instantaneous increases (spikes) in a power line.

**Power conditioners:** Active devices that effectively isolate and regulate voltage in a building. These monitor the power in a building and clean it up.

**Redundant power source:** If possible (and depending on criticality of availability), have power source come from 2 different substations.

---

### Shielding

- Prevent emissions from computer systems
  - Electromagnetic Interference (EMI)
  - Radio Frequency Interference (RFI)
- Properly shielded wires should be used in local area networks
- Fiber optics is immune to EMI
- Faraday Cage
- TEMPEST

**Shielding** refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and to preventing outside electronic emissions from disrupting your information-processing abilities. In a fixed facility, such as a computer center, surrounding the computer room with a Faraday cage can provide electronic shielding.

A **Faraday cage** usually consists of an electrically conductive wire mesh or other conductor woven into a “cage” that surrounds a room. The conductor is then grounded. Because of this cage, few electromagnetic signals can either enter or leave the room, thereby reducing the ability to eavesdrop on a computer conversation. In order to verify the functionality of the cage, radio frequency (RF) emissions from the room are tested with special measuring devices.

**TEMPEST:** U.S. government project that became a standard. TEMPEST shielding protection means that a computer system doesn't emit any significant amounts of EMI or RFI.

---

## Execute Disaster Recovery Plans and Procedures

### Disaster Recovery Planning (DRP)

- Goal is to recover from the disaster and restore critical functions to normal operations
- Anticipates a major and very disruptive event
- Practice recovery procedure scenarios

---

### Backups, execution and frequency

#### Backup Types

Type	Backup Process	Archive Bit Reset
Full	Backs up all files regardless of the archive bit	Yes
Incremental	Backs up files on which the archive bit is set to 1 Backs up all newly created or modified files since last full or incremental backup	Yes
Differential	Backs up files on which the archive bit is set to 1 Backs up all newly created or modified files since last full backup	No
Copy	Backs up all files regardless of the archive bit status	No

If a file is changed or created, then the archive bit is set to 1. With a Full and Incremental backup, the archive bit is cleared (set to 0) after the backup.

---

#### Full Backup

- Backup Characteristics
  - May Require large tapes for each backup
  - May take a long time to perform each backup
- Restore Characteristics
  - Restore only the last backup
  - Takes the longest to make a backup, but is the fastest method to make a complete restore

### Full + Incremental

- Backup Characteristics
    - Fastest backup method
  - Restore Characteristics
    - Restore the last full backup, then every subsequent incremental backup
    - Provides a good balance between backup and restore time
- 

### Full + Differential

- Backup Characteristics
    - Takes progressively longer to complete, as time elapses since the last full backup
  - Restore Characteristics
    - Restore the last full backup, then the last differential backup
    - Next to a full backup, this is the fastest restore method
- 

### Backup Plans

**The Grandfather, Father, Son method** is based on the philosophy that a full backup should occur at regular intervals. It assumes that the most recent backup after the full backup is the son. As newer backups are made, the son becomes the father and the father becomes the grandfather. This backup is stored in an offsite facility for a period of a year and each monthly backup replaces the monthly backup from the previous year. The major drawback in the Grandfather, Father, Son method is trying to keep track of all the storage media coming and going between the storage facility and the computer center.

**The Full Archival method** works on the assumption that any information created on any system is stored forever. All backups are kept indefinitely and effectively eliminates the potential for data loss

**The Backup Server method** has a server with large amounts of disk space to back up data. It will examine and copy all the files that have been altered every day and the server can be backed up on a regular basis. The advantage to this method is all backed up data is available online for immediate access.

---

### Recovery Time Objective (RTO)

- Acceptable amount of data loss measured in time
  - What an organization determines is an "acceptable loss" in a disaster situation
  - If the RTO of a company is two hours:
    - all data must be restored to within two hours of the disaster
    - the company has acknowledged that data in the two hours immediately preceding the disaster may be lost
- 

### Onsite storage

- Location on site at the computer center
- Containers designed and rated for fire, moisture, and pressure resistance

## Domain 5 – Compliance and Operational Security

Onsite storage usually refers to a location on the site of the computer center that is used to store information locally. Onsite storage containers are available that allow computer cartridges, tapes, and other backup media to be stored in a reasonably protected environment in the building.

Onsite storage containers are designed and rated for fire, moisture, and pressure resistance. These containers are not fireproof in most situations, but they are fire rated. A fireproof container should be guaranteed to withstand damage regardless of the type of fire or temperature, whereas fire ratings specify that a container can protect the contents for a specific amount of time in a given situation.

### Offsite Storage

Prevents the same disaster from affecting the network and the backup media  
Offsite storage refers to a location away from the computer center where paper copies and backup media are kept. Offsite storage can involve something as simple as keeping a copy of backup media at a remote office or it can be as complicated as a nuclear-hardened high-security storage facility. The storage facility should be bonded, insured, and inspected on a regular basis to ensure that all storage procedures are being followed.

---

### Restoration / Secure Recovery

- Regularly test backups to ensure necessary data has been saved and can successfully restore
- Backup plan should include procedures for proper restoration of the data
- Training should be conducted where backups are actually restored to a system
- Validates the backup and recovery procedures and keeps personnel trained

When a system fails, you will be unable to reestablish operation without regenerating all of the system's components. This process includes making sure hardware is functioning, restoring or installing the operating systems, restoring or installing applications, and restoring data files. It can take several days on a large system. With a little forethought, you may be able to simplify the process and make it easily manageable.

When you install a new system, make a full backup of it before any data files are created. If stored onsite, this backup will be readily available for use. If you have standardized your systems, you may need just one copy of a base system that contains all the common applications you use. The base system can usually be quickly restored, which allows for reconnection to the network for restoration of other software. Many newer operating systems now provide this capability, and system restores are very fast.

When the base system has been restored, data files and any other needed files can be restored from the last full backup and any incremental or differential backups that have been performed. The last full backup should contain most of the data on the system;

## Domain 5 – Compliance and Operational Security

the incremental backup or differential backups contain the data that has changed since the full backup.

An important recovery issue is to know the order in which to progress. If a server is completely destroyed and must be re-created, ascertain which applications are the most important and should be restored before the others.

---

### Redundancy and Fault Tolerance Planning

#### Redundancy

- Systems that are either duplicated or that fail-over to other systems in the event of malfunction
- Fail-Over
  - Process of reconstructing a system or switching to other systems when a failure is detected
  - Allows services to continue uninterrupted until the primary can be restored

Redundancy refers to systems that are either duplicated or that fail over to other systems in the event of a malfunction. Fail-over refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This allows service to continue uninterrupted until the primary server can be restored. In the case of a network, processing switches to another network path in the event of a network failure in the primary path.

---

#### Fault Tolerance

- The ability of a system to sustain operations in the event of a component failure
- Continues operations even though a critical component has failed (by switching over)
- Addition of redundant components:
  - Hardware
  - Utilities
  - Backups

Fault tolerance is primarily the ability of a system to sustain operations in the event of a component failure. Fault-tolerant systems can continue operation even though a critical component, such as a disk drive, has failed. This capability involves over-engineering systems by adding redundant components and subsystems.

Since computer systems cannot operate in the absence of electrical power, it is imperative that fault tolerance be built into your electrical infrastructure as well. At a bare minimum, an uninterruptible power supply (UPS), with surge protection, should accompany every server and workstation. The UPS should be rated for the load it is expected to carry in the event of a power failure (factoring in the computer, monitor, and any other device connected to it) and be checked periodically as part of your preventative maintenance routine to make sure the battery is operational.

---

## Domain 5 – Compliance and Operational Security

### High Availability

The process of keeping services and systems operational during an outage

Goal: Five nines availability (99.999%/5.36 minutes per year)

- Need to implement:
  - Fault tolerant systems
  - Redundant technology
  - Backup communication channels

High availability refers to the process of keeping services and systems operational during an outage. In short, the goal is to provide all services to all users, where they need them and when they need them. With high availability, the goal is to have key services available 99.999 percent of the time (also known as five nines availability).

---

### Redundant Array of Independent Disks

- RAID Level 0: Disk Striping
- RAID Level 1: Disk Mirroring
- RAID 0 + 1:
- RAID Level 3: Disk Striping with Parity (dedicated disk)
- RAID Level 5: Disk Striping with Parity (distributed across all disks)

www.acnc.com

---

RAID Level	Description	Strengths	Weaknesses
0	Striping	Highest performance	No redundancy; 1 fail = all fail
1	Mirroring	Duplicates data on other disks	Expensive; double cost of storage
0 + 1	Striping and Mirroring	Highest performance, highest data protection (can tolerate multiple drive failures)	Expensive; double cost of storage
3/4	Striped with dedicated parity	Excellent performance; fault tolerance	Write requests suffer from same single parity-drive
5	Block-level striping with distributed parity	Best cost/performance for networks; high performance; high data protection	Write performance is slower than RAID 0 or RAID 1

### RAID Fault tolerance

- RAID 3 is no longer used because its performance degraded when a lot of small requests were made to the disk, as with databases.
- RAID 5 is most commonly used today because it strikes a balance between redundancy and performance.
- Hardware implementation will run faster than software implementation

### Redundant (Clustered) Servers

- The use of multiple computers and redundant interconnections to form what appears to be a single highly available system
  - Provides fail-over capabilities
    - Ensures if one system fails then another in the cluster will take over
  - Can provide load balancing
  - Active/Active Clustering vs. Active/Passive Clustering
- 

### Clustering

Clustering is a technology in which several servers jointly perform a single task. Server clustering is also used for fault tolerance: when one server goes down, another takes over. Many operating systems, including Windows 2000 Advanced Server, Novell NetWare 6, and Linux, are capable of clustering to provide fail-over capabilities.

**Active/Active Clustering-**Traffic intended for the failed node is either passed onto an existing node or load balanced across the remaining nodes. This is usually only possible when the nodes utilize a homogeneous software configuration. In Active/Active clustering, both nodes are accessible and active. If a node fails, then its resources would shift to the other active node. The node that survives would then carry the load for both nodes.

**Active/Passive Clustering-** Provides a fully redundant instance of each node, which is only brought online when its associated primary node fails. This configuration typically requires the most extra hardware. If your active node failed, then its defined resources would shift to the passive node and it would become active. The passive node is not accessible unless an accident occurs and the resources shifted.

---

### Redundant ISPs

- Allows another path through a different backbone in case of disruption
  - Provides an alternative way for the organization to maintain their connection
  - Costly due to number of systems involved
- 

### Alternate Sites

- Provide for the restoration of business functions in the event of a large-scale loss
  - Cost of a site should be considered
  - Location should preferably not be in close proximity to your organization's current location
- 

### Hot Site

- A fully configured and functional facility
- Available within hours
  - Necessary when an organization cannot tolerate any downtime
- Requires constant maintenance
- Expensive to maintain

## Domain 5 – Compliance and Operational Security

A hot site is a fully configured facility with power, A/C, phone lines, chairs, and fully functional servers and clients that are up-to-date, mirroring the production system. Databases can be kept up-to-date using network connections. Hot sites are expensive, and they are primarily suitable for short-term situations.

---

### Warm Site

- Facility with power, A/C, and partially configured systems
- Available within a couple days
  - Adequate when an organization's Maximum Tolerable Downtime (MTD) or Recovery Time Objective (RTO) is a short time period
- Less expensive than a hot site
  - Lower administrative and maintenance resources consumed

A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations.

For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement. A warm site requires more advanced planning, testing, and access to media for system recovery.

---

### Cold Site

- Basic facility with wiring, ventilation, plumbing, and flooring
  - No hardware infrastructure
- Not immediately available
- Relatively low cost
- Useful if there is some forewarning of a potential problem

A cold site is useful if there is some forewarning of a potential problem: i.e. potential storm and would not need to be up and running in the facility for a day or 2; such as a regional office. Cold sites work well when an extended outage is anticipated. The major challenge is that the customer must provide all the capabilities and do all the work to get back into operation.

---

### Service Bureau

- A contracted site that provides all alternate backup processing services
  - Quick response and availability
  - Testing may be possible
  - Expense and may be resource contention during a large emergency
    - Common for the service provider to oversell its processing capabilities
- 

### Reciprocal / Mutual Aid Agreements

- Agreement with another organization
  - Both parties back up and store each other's data
- Cost effective

## Domain 5 – Compliance and Operational Security

- Contract should be detailed
    - Equipment availability, facility repair, security, etc.
  - Companies should not be in the same geographic area that can be affected by the same disaster
  - Short term fix
- 

### **Service Level Agreement (SLA)**

An agreement between you or your company and a service provider, typically a technical support provider

Can include guarantees for:

- Mean Time Between Failures (MTBF)
- Mean Time To Repair (MTTR)
- Maximum Tolerable Downtime(MTD)
- System utilization rates
- System up-times
- Volume of transactions

A service-level agreement (SLA) is usually part of network availability and other agreements. They stipulate the performance you can expect or demand by outlining the expectations a vendor has agreed to meet. They define what is possible to deliver and makes sure what is delivered is what was promised.

---

**The Mean Time Between Failure (MTBF)** is the measure of the anticipated incidence of failure for a system or component. This measurement determines the component's anticipated lifetime. If the MTBF of a cooling system is one year, you can anticipate that the system will last for a one-year period; this means you should be prepared to replace or rebuild the system once a year. MTBF is helpful in evaluating a system's reliability and life expectancy.

**The Mean Time to Repair (MTTR)** is the measurement of how long it takes to repair a system or component once a failure occurs. In the case of a computer system, if the MTTR is 24 hours, this tells you it will typically take 24 hours to repair it when it breaks.

**Recovery Time Objectives (RTO)** is the time period after a disaster at which business functions need to be restored.

**Recovery Point Objectives (RPO)** is point in operation before a disruption occurred.

### Domain Summary Objectives

#### A Security+ candidate is expected to:

- Explain risk related concepts
- Carry out appropriate risk mitigation strategies
- Execute appropriate incident response
- Explain the importance of security related awareness and training
- Compare and contrast aspects of business continuity
- Explain the impact and proper use of environmental controls

## Domain 6 – Application, Data, and Host Security

---

A Security+ candidate is expected to:

Explain the importance of application security

Carry out appropriate procedures to establish host security

Explain the importance of data security

---

### Explain the Importance of Application Security

#### Fuzzing

- Used to test for security problems in software or computer systems
- Used in large software development projects that employ black-box testing
- An assurance of overall quality rather than a bug-finding tool
- Often finds odd oversights and defects which human testers would fail to find

Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions. Fuzzing is commonly used to test for security problems in software or computer systems.

Fuzzing programs fall into two different categories;

- Mutation based fuzzers mutate existing data samples to create test data
- Generation based fuzzers define new test data based on models of the input

#### Types of bugs found

Straight-up failures such as crashes, assertion failures, and memory leaks are easy to detect. The use of a memory debugger can help find bugs too subtle to always crash. Fuzz testing is especially useful against large applications, where any bug affecting memory safety is likely to be a severe vulnerability. It is these security concerns that motivate the development of most fuzzers.

Since fuzzing often generates invalid input, it is especially good at testing error-handling routines, which are important for software that does not control its input. As such, simple fuzzing can be thought of as a way to automate negative testing. More sophisticated fuzzing tests more "main-line" code, along with error paths deep within it.

Fuzzing can also find some types of "correctness" bugs. For example, it can be used to find incorrect-serialization bugs by complaining whenever a program's serializer emits something that the same program's parser rejects. It can also find unintentional differences between two versions of a program or between two implementations of the same specification.

A trivial example:

Let's consider an integer in a program, which stores the result of a user's choice between 3 questions. When the user picks one, the choice will be 0, 1 or 2, which makes three practical cases. But what if we transmit 3, or 255? We can, because integers are stored a static size variable. If the default switch case hasn't been implemented securely, the program may crash and lead to "classical" security issues: exploitable buffer overflows, DoS, etc.

Fuzzing is the art of automatic bug finding, and its role is to find software implementation faults, and identify them if possible.

---

## Secure Coding Concepts

- Exception handling
  - A mechanism designed to handle the occurrence of exceptions that change the normal flow of program execution
- Error handling
  - Refers to the anticipation, detection, and resolution of programming, application, and communications errors.
    - Takes place during the execution of a program
    - Adverse system parameters or invalid input data are often the cause

Exception handling ensures that the code can handle error conditions. In order to establish that exception handling routines are sufficiently robust, it is necessary to present the code with a wide spectrum of invalid or unexpected inputs, such as can be created via software fault injection and mutation testing (which is also sometimes referred to as fuzz testing). One of the most difficult types of software for which to write exception handling routines is protocol software, since a robust protocol implementation must be prepared to receive input that does not comply with the relevant specification(s).

In order to ensure that meaningful regression analysis can be conducted throughout a software development lifecycle process, any exception handling verification should be highly automated, and the test cases must be generated in a scientific, repeatable fashion. Several commercially available systems exist that perform such testing.

Error handling refers to the anticipation, detection, and resolution of programming, application, and communications errors. Specialized programs, called error handlers, are available for some applications. The best programs of this type forestall errors if possible, recover from them when they occur without terminating the application, or (if all else fails) gracefully terminate an affected application and save the error information to a log file.

In programming, a development error is one that can be prevented. Such an error can occur in syntax or logic. Syntax errors, which are typographical mistakes or improper use of special characters, are handled by rigorous proofreading. Logic errors, also

called bugs, occur when executed code does not produce the expected or desired result. Logic errors are best handled by meticulous program debugging. This can be an ongoing process that involves, in addition to the traditional debugging routine, beta testing prior to official release and customer feedback after official release.

A run-time error takes place during the execution of a program, and usually happens because of adverse system parameters or invalid input data. An example is the lack of sufficient memory to run an application or a memory conflict with another program. On the Internet, run-time errors can result from electrical noise, various forms of malware or an exceptionally heavy demand on a server. Run-time errors can be resolved, or their impact minimized, by the use of error handler programs, by vigilance on the part of network and server administrators, and by reasonable security countermeasures on the part of Internet users.

---

### **Input Validation**

- The process of validating all the input to an application
- Critical to application security
- Effects: An attacker could input unexpected values causing a program crash or excessive consumption of resources.
  
- Used in attacks like this are:
  - Buffer overflows
  - XSS
  - SQL injection

---

### **Configuration Baselines (CB)**

- Establishes the mandatory settings that systems must have in place to be accepted for use in the network.
- Usually start with host, application, and network hardening principles.
- May also mark an approved security configuration item, e.g. security templates that have been signed off for execution.

For information assurance, Configuration Baselines can be defined as the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

### **Security Baselines**

The process of baselining involves both the configuration of the IT environment to conform to consistent standard levels, such as password security and the disabling of non-essential services, combined with the identification of what constitutes typical behavior on a network or computer system (such that malicious behavior can more easily be identified should it occur during the baselining process).

The baselining process involves the hardening the key components of the IT architecture to reduce the risks of attack. The three main areas requiring hardening are operating system, network and applications.

---

### **OS Hardening Best Practices**

The operating system has to be protected against attacks, which involves keeping software versions up-to-date, keeping the system patched, and ensuring configuring settings comply with the security policy.

### **OS Hardening**

- **Removing unnecessary programs/services**

It is important that an operating system only be configured to run the services required to perform the tasks for which it is assigned. For example, unless a host is functioning as a web or mail server there is no need to have HTTP or SMTP services running on the system.

- **Password Management**

- Disable unnecessary accounts
- Remove/reconfiguring default accounts
- Password protected
- Account lockout and duration configured

Most operating systems today provide options for the enforcement of strong passwords. Utilization of these options will ensure that users are prevented from configuring weak, easily guessed passwords. As an additional levels of security include enforcing the regular changing of passwords and the disabling of user accounts after repeated failed login attempts.

- **Enable auditing and logging**

It is important to ensure that the operating system is configured to log all activity, errors and warnings.

---

- **Applying patches, hotfixes, service packs**

- **Hotfixes:** A single, cumulative package a specific customer situation and may not be distributed outside.
- **Service Packs:** Service packs are a collection of updates, fixes and/or enhancements.
- **Patches:**  
Patches are small piece of software designed to fix problems.  
Patch management is an automated strategy and plan of what patches should be applied to which systems at a specified time.

– **Patch Management Software:**

**Windows Server Update Services (WSUS):** Enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

**Hercules:** A patch-management solution that provides automated patch distribution and installation across enterprise networks. Hercules enables users to conduct both scanner-based and agent-based vulnerability assessments, automate enforcement and audit compliance. Hercules creates and enforces technical and business policies; noncompliant systems are quarantined until all identified issues are fixed. It also allows you to track key assets on your network.

---

## Application Hardening

- Remove all applications not being used
- Restrict access to the application, provide access only to those who must have it
- Update all applications to the latest patches
- Code-review internally developed applications for security weaknesses
- Proper input validation
- Use encryption for application communications

Applications are the most difficult parts of an IT infrastructure to secure because of their complexity and because they often need to accept input from a variety of users.

## Application Hardening

Application hardening is the process that addresses application security weaknesses by implementing the latest software patches, hotfixes and updates, using the latest and secured versions of protocols and following procedures and policies to reduce attacks and system down time. The critical applications that need hardening are Web servers, email servers, DNS servers, file servers, database systems, etc.

Here are guidelines to lowering the risk of a system intrusion because of an application flaw:

- Assume all installed applications are flawed—don't rely on the security programmed into them.
- Physically remove from the system all applications not being used.
- Use firewalls, content filters and OS user authentication features to restrict access to the application, and provide access only to those who absolutely must have it.
- Update all applications to the latest patches when security bulletins are released.
- Internally developed applications need to be code-reviewed for security weaknesses.

- Consider an external security review for critical applications.
- Externally facing Web applications are high-risk applications because they are a bridge between the outside world and internal customer databases. Be sure to add code that can block or otherwise safely deal with all of the following hostile inputs: missing page parameters, parameters that are unusually long, parameters with nulls or hexadecimal encoding, parameters with Web browser script blocks (which are used to create server-side scripting attacks), and parameters with quotes and semicolons (likely attempts to send hostile SQL commands through to the database).
- If possible, write applications in languages that run in virtual machines--such as Java, Visual Basic .Net or C#--because they provide an extra layer of security protection.
- Avoid C and C++ because they make it easy to write applications that allow buffer overflow attacks.

---

## ***Network Hardening***

Updating Software and Hardware - An important part of network hardening involves an ongoing process of ensuring that all networking software together with the firmware in routers are updated with the latest vendor supplied patches and fixes.

Password Protection - Most routers and wireless access points provide a remote management interface which can be accessed over the network. It is essential that such devices are protected with strong passwords.

Disable Unnecessary Protocols and Services - All unnecessary protocols and services must be disabled and, ideally, removed from any hosts on the network. For example, in a pure TCP/IP network environment it makes no sense to have AppleTalk protocols installed on any systems.

Block Unneeded Ports - A hardened network should have any unneeded ports blocked by a firewall and associated services disabled on any hosts within the network. For example, a network in which none of the hosts acts as a web server does not need to allow traffic for port 80 to pass through the firewall.

Restricted Network Access - A variety of steps should be taken to prevent unauthorized access to internal networks. The first line of defense should involve a firewall between the network and the internet. Other options include the use of Network Address Translation (NAT) and access control lists (ACLs). Authorized remote access should be enabled through the use of secure tunnels and virtual private networks (VPNs).

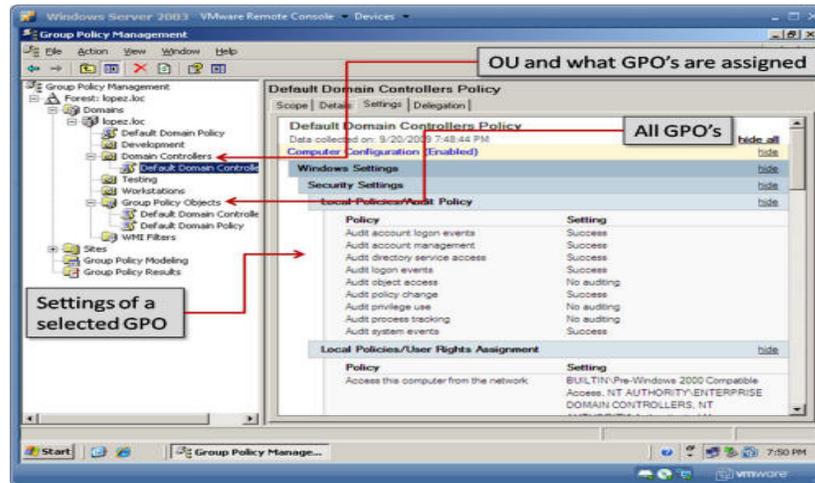
Wireless Security - Wireless networks must be configured to highest available security level. For older access points WEP security should be configured with 128-bit keys. Newer routers should implement WPA or WPA2 security measures.

Deploy NIDS or NIPS on the network – Ensure monitoring of the network traffic to detect or stop attacks that were able to get through the network devices.

### Group Policies

- Allows administrators to have more control over the system settings
- Allows for centralized control of all Windows operating system in the enterprise environment
- In Server 2008 they can be configured with the Group Policy Management Console

### Group Policy Management Console



### Domain GPO Design

Windows uses Group Policy Object (GPO) to manage the settings on containers and objects

#### Types of containers:

<b>Site</b>	All domains in a site replicate data with each other
<b>Domains</b>	Used to group objects together to make management easier and more efficient All objects share a common domain name
<b>Organizational Units (OUs)</b>	Grouping objects within a domain into containers called Organizational Units (OU) Allows for finer control of objects within the OU Usually setup by departments within the company

#### GPO Inheritance:

All Security policies placed on a domain will be inherited by all OUs and child OUs. Policies that are not security related are inherited by OUs, but child OUs can override these policies from their parent OUs. Just like in real life, if the parent wants the child to

live by their laws then the parent OU can select “No override” and this will force the inheritance on the child.

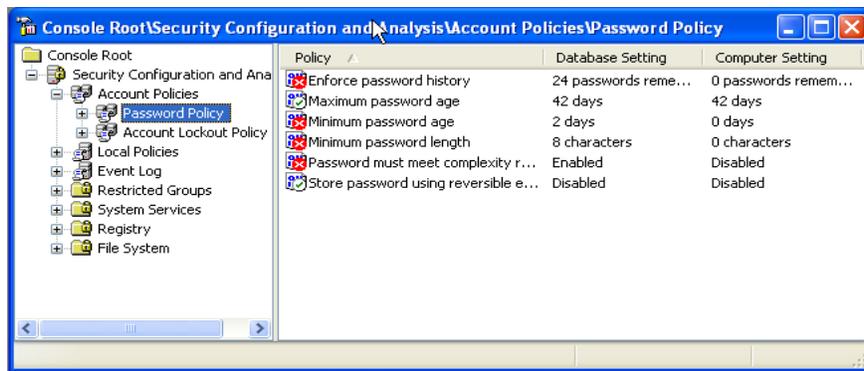
## Security Templates

- Used to support the organization’s system security policy
- Can be used as a baseline configuration for all the systems on the network
- Can also be used to compare a system’s settings to the baseline settings
- A group policy is normally used to create the template

Security templates cover the security-related settings on a compliant workstation or server. They can be applied by using the Secedit.exe command line utility or the Security Configuration and Analysis snap-in. The Security Configuration and Analysis snap-in will show the differences between the template and the current system settings.

Some predefined security templates for use with Windows operating systems are:

- Securedc.inf: Used to secure a domain controller
- Securews.inf: Used to secure a workstation and members servers

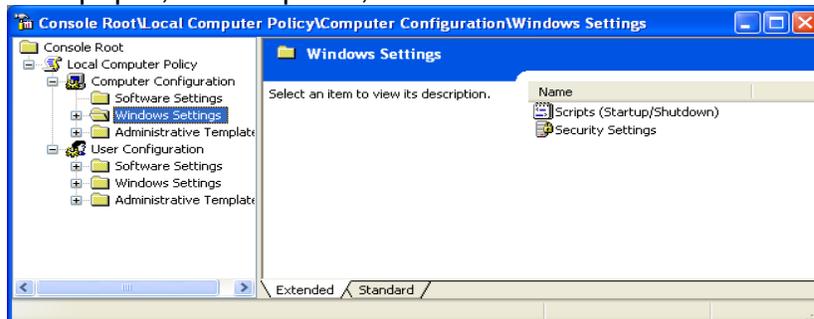


## Local Group Policies

- Computer Configuration
- Used to configure the settings on a system regardless of who is logged on
- User Configuration

Used to configure the settings that control what the user’s preferences are and what they can and cannot do in the system

- Examples: wallpaper, control panel, etc.



## Carry out appropriate procedures to establish host security

### Anti-virus Software

- Looks for the virus code in files, memory, and boot sectors
- Signature-based
- Heuristic-based examination techniques
  - Identifies virus code based on behavior
  - Not definition based
- Keep software version up-to-date
- Keep definition/pattern files current
- Scan frequently

Antivirus software scans a computer's memory, disk files, and incoming and outgoing email. The software typically uses a virus definition file that is updated regularly by the manufacturer. If these files are kept up-to-date, the computer system will be relatively secure. Unfortunately, most people do not keep their virus definition files up-to-date.

---

### Pop-up Blockers

- Pop-ups are used to open a window on-top of the window that is currently open
- Valid uses:
  - Login windows
  - Warning about a website
- Illegitimate uses:
  - Unwanted advertisements
- Close properly

---

### Personal Software Firewalls

- An application which controls network traffic to and from a computer
- Personal firewalls are typically designed for use by end-users
- A personal firewall will usually protect only the computer on which it is installed

### Common Personal Firewall Features

- Alerts the user about outgoing connection attempts.
  - Allows the user to control which programs can and cannot access the local network and/or Internet.
  - Hides the computer from port scans by not responding to unsolicited network traffic.
  - Monitors applications that are listening for incoming connections Monitor and regulate all incoming and outgoing Internet users.
  - Prevents unwanted network traffic from locally installed applications.
  - Provides the user with information about an application that makes a connection attempt.
  - Provides information about the destination server with which an application is attempting to communicate.
-

## Anti-Spam

- Software that can reduce the amount of Spam delivered to a user's inbox
  - **Blocking/Filtering** via both black and white lists, IP address, server, email address, country code
  - **Protection of user** from email that contains worms, viruses, Trojans, attachments with embedded malware
- 

## Anti-Spyware

- Software that helps protect your computer against the security threats caused by spyware
  - Examples;
    - Windows Defender
    - Spybot Search and Destroy
    - Malwarebytes
- 

## Hardware Security

- **Cable Locks:** used for securing laptops/desktops, prevent theft
- **Rack Locks:** server or network device rack locks, used for preventing physical access
- **Cabinet Locks:** used for securing paper documents
- **Safes:** securing paper documents, backups, etc

Sensitivity of data will determine storage of paper documents as well as data on a network. A locked cabinet may not provide a high enough level of security in which case the data may need to be stored in a secure safe. The sensitivity level of data on a system or data that traverses a network will need a higher level of physical security as well to prevent unauthorized access or theft.

---

## Mobile Device Security

### Screen Lock

Screen lock is the first security layer of protection from unauthorized access to the device. The screen “locks” after a certain amount of non-use. The user would have to enter a password or pin to access the device. The shorter the amount of time it is set, the more secure.

### Strong Password/PIN

It is critical that users be required to turn on device authentication so that lost devices cannot be easily accessed by any person that finds or steals a device.

- Passwords - 8 characters or longer that incorporate 2 capital letters, 2 special characters, and 2 numbers.
- PIN - 4 to 6 digits.

### **Device/Voice Encryption**

Data stored on the phone as well as voice and web communications need to be encrypted.

### **Remote Wipe**

Give IT staff the ability to remotely access and disable devices in the event of loss or theft. This could be very handy in a situation where, say, an executive loses his or her device at a conference—along with yearly sales projections and strategies stored within. With the remote capability all it would take is a quick call to IT and they'll take care of it.

### **Proper Sanitization**

Many mobile device users sell their old smart phones everyday not knowing they left personal data on the device. Restore the phone to the factory default settings or contact the manufacturer to get proper instructions to sanitize the phone.

### **GPS Tracking**

Used in several mobile devices, if the phone is stolen or lost you can find the device as it emits a GPS signal. Has to be configured on the device and is not always set by default.

### **Secure Bluetooth**

Change the default PIN, do not have device set in discoverable mode.

---

## **Importance of Data Security**

### **Data Loss Prevention (DLP)**

- Monitors system contents to make sure that contents are not deleted or removed. The best known DLP is MyDLP (open source) and Microsoft Forefront.
- Provides data protection even if your physical and logical security implementations fail

### **Data Encryption**

- Whole/Full Disk
  - Database encryption
  - Individual File encryption
  - Removable Media encryption
  - Mobile Devices encryption
- 

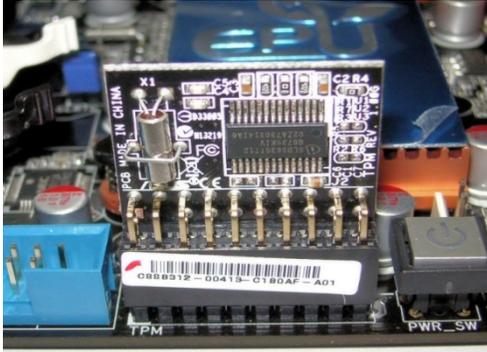
### **Hardware Based Encryption Devices**

- Trusted Platform Module (TPM)
- Hardware Security Model (HSM)
- USB encryption
- Hard drive encryption

---

### Trusted Platform Module (TPM)

- A microcontroller that stores keys, passwords, and digital certificates
- Typically affixed to the motherboard of a PC
- More secure from external software attack and physical theft
- Access to data and secrets in a platform could be denied, if the boot sequence is not as expected



### Asus TPM Chip

A Trusted Platform Module (TPM) can be used to assist with hash key generation. A TPM is the name assigned to a chip that can store cryptographic keys, passwords, or certificates. The TPM can be used to generate values used with whole disk encryption as well as protect cell phones and devices other than PCs.

TPM can be used to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication

For example, it can be used to verify that a system seeking access is the expected system.

Generally, pushing the security down to the hardware level in conjunction with software provides more protection than a software-only solution that is more easily compromised by an attacker.

---

### Hardware Security Model (HSM)



A Hardware Security Module (HSM) is a secure crypto processor with the main purpose of managing cryptographic keys and offer accelerated cryptographic operations using such keys. The modules typically offer protection features like strong authentication and physical tamper resistance. Main features of an HSM include on board key generation and storage, accelerated symmetric and asymmetric encryption and backup of sensitive material in encrypted form.

Traditionally HSMs have been used in the banking sector to secure large amounts of bulk transactions. Other common usage areas are to secure CA keys in PKI

deployments and SSL acceleration. In the last couple of years with the advent of DNSSEC (DNS Security Extensions) an increased focus has been placed on storing DNSSEC keys, and encrypting zone records using an HSM.

## Appendix A – Practical Exercises

### MD5/SHA-1 Practical Exercise

The purpose of this PE is to become familiar of how a hashing algorithm is used and how the output of the hash and its changes can reflect changes in the source document.

Go to the CD and from the tools folder, drag **md5sums.exe** and **sha1.exe** to the desktop. Once you have located and dragged the files over, open up a command prompt and change your directory to that of the desktop.

1. First create a file to hash. Type: **echo I love security+ class > file.txt**
2. Hash the file. Type: **md5sums file.txt**
3. Notice the output of the hash. Now modify the file you have just hashed. Type: **echo I want to stay here all day >> file.txt**
4. Now hash the modified file. Type: **md5sums file.txt**
5. Do the MD5 digests match? \_\_\_\_\_
6. Create a second file to hash with SHA-1. Type: **echo I hate security+ class > file1.txt**
7. Hash the file with SHA-1. Type: **sha1 file1.txt**
8. Now modify the file. Type: **echo I am lying >> file1.txt**
9. Now hash the modified file with SHA-1. Type: **sha1 file1.txt**
10. Do the SHA-1 digests match? \_\_\_\_\_
11. Create a new file to hash. Type: **echo I am hungry > file2.txt**
12. Hash it with MD5. Type: **md5sums file2.txt**
13. Now create an Alternate Data Stream that links to the file. Type: **notepad file2.txt:ads.txt**
14. Click OK if presented with a box asking if you are creating a new file. Write something and save it. Close notepad when you are completed.

15. Do a directory listing of your desktop and try and find the file you just created.  
Type: **dir** (look for the file ads.txt)
16. Do you see the file listed? \_\_\_\_\_
17. Do a MD5 hash to see if the Alternate Data Stream has affected the file. Type:  
**md5sums file2.txt**
18. Hash the MD5 digest changed from step 12? \_\_\_\_\_
19. Try hashing the ads.txt file. Type: **sha1 ads.txt**
20. Did it work? \_\_\_\_\_
21. Try hashing it by using file2.txt as a location. Type: **sha1 file2.txt:ads.txt**
22. Did it work this time? \_\_\_\_\_
23. It is safe to conclude that Alternate Data Streams exist, can only be accessed via their base files, and do not modify or change anything in the base file.

**END OF PE**

## WireShark PE

This practical exercise utilizes the predominant open source packet analysis tool available. The Wireshark project got its start as Ethereal. In this exercise we will learn how to analyze a raw packet and understand how the packet values are interpreted by Wireshark.

PE Requirements:

1. One machine running windows 2003 server (networked)
2. Current version of Wireshark (windows version)
3. Folder containing sample capture files

**NOTE 1:** When opening new capture files, make sure that your display filter value is blank.

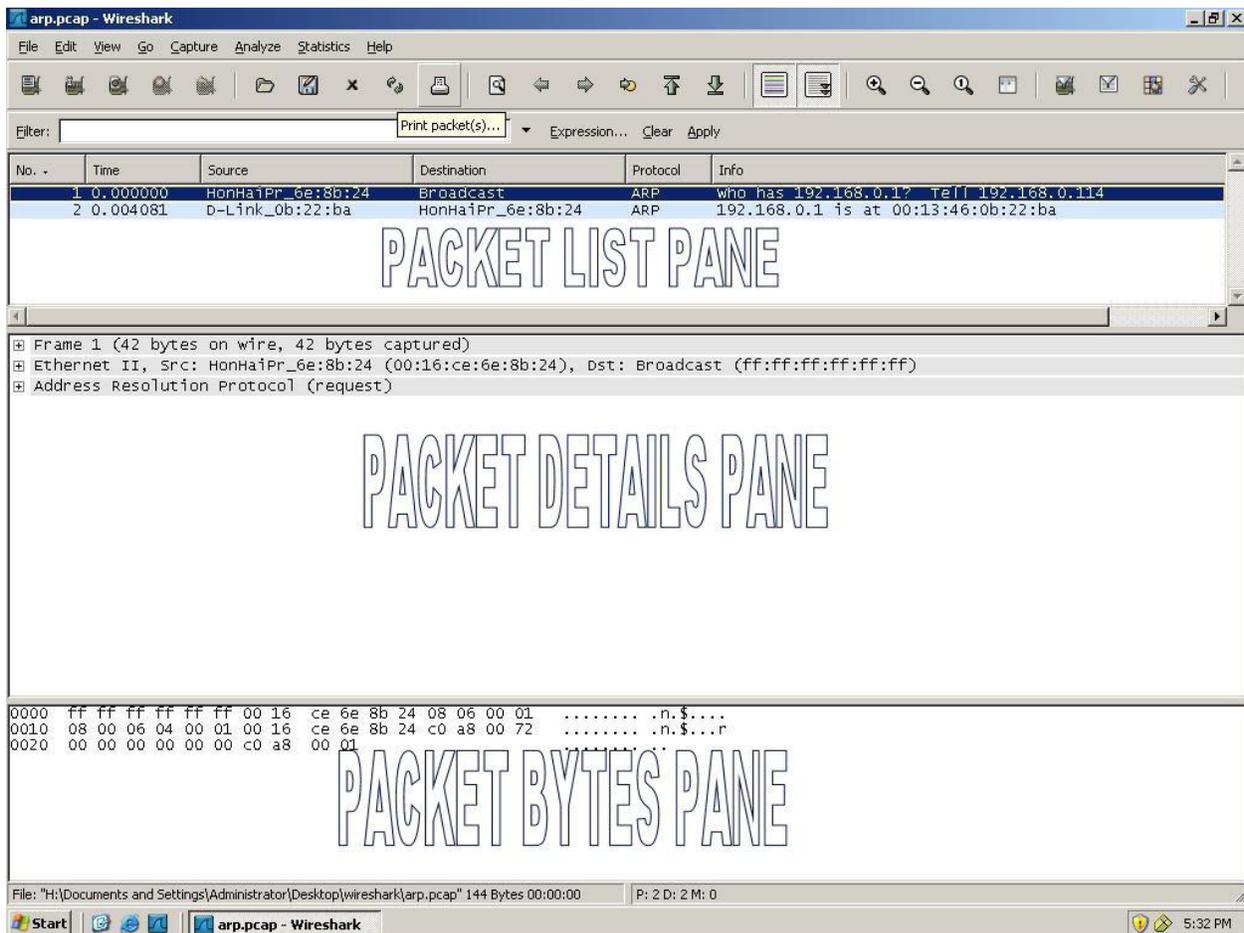
**NOTE 2:** If you try to open a file and it doesn't want to load, close Wireshark and double click on the .pcap file from the captured packets folder. This will bring up a fresh copy of Wireshark with the .pcap file loaded.

1. Install Wireshark from its folder on the CDROM
2. During install it will check your system for WinPcap. If you do not have it or have an earlier version, Wireshark will uninstall and install a newer and compatible version during installation. If prompted for WinPcap installation, install it and accept any defaults.
3. Your CDROM should contain a folder of captured packet files. Copy the folder to the desktop.
4. Click on **<START><PROGRAMS><WIRESHARK>Wireshark**
5. Go to the Wireshark menu bar and click on **<EDIT><PREFERENCE>**
6. On the left menu, click on **<CAPTURE>**
7. **Uncheck** the box that says "Hide capture info dialog"
8. Click **<OK>**
9. Go to the **<START><ALL PROGRAMS><ACCESSORIES>** and click on **calculator**.
10. The calculator will most likely pop up in standard view. Go to **<VIEW>** and click on **scientific**.
11. You should see a radio button selected for Dec (decimal). Click on the button marked **Hex** (hexadecimal).
12. We will be using this to convert packet values into the decimal values you see presented by Wireshark. To convert from Hex to Dec, just type in the Hex value and click the Dec radio button. This will also work in the reverse for converting Dec to Hex.
13. In Wireshark, click on **<FILE><OPEN>**. Go to the folder where the capture files are stored. It should be named traces. The capture file to select is named "**begin.cap**". Click on **<OPEN>** when you've selected it.

14. Wireshark provides you with three viewing windows. The top pane (**packet list pane**) has a table of all packets in the current capture or capture file. You'll see information such as packet number, source address, destination address, protocol, and info

15. The middle pane (**packet details pane**) is a hierarchical display of info about a single packet which is highlighted in the packet list pane.

16. The bottom pane (**packet bytes pane**) shows the raw data that was transmitted over the wire. Highlight a packet in the packet list pane and you'll see its tree structure in the packet details pane. Highlight a portion of the packet details and you'll see the corresponding raw data in the packet bytes pane.



17. This capture is a fairly simple one. It involves 26 packets. Click on **<STATISTICS><PROTOCOL HIERARCHY>**

18. This will list all of the protocols used in a packet in the order that they occur in the protocol stack. Look at the packets and bytes columns. These list information that pertains to all the packets of the specified protocol. You'll notice that you see Internet Protocol, Transmission Control Protocol, User Datagram Protocol, and Hypertext Transfer protocol listed in the protocol column. You will notice that the line for the Internet Protocol lists all 26 packets as being part of this layer. As this was a capture on an Ethernet device, all packets would have layer 3 routing information in them. The transport layer is divided between TCP and UDP packets. All traffic in

this capture was HTTP in nature but the TCP was not recorded as such as the port number used in this capture was not the standard port 80. The port used was 5678.

19. Close the Protocol hierarchy window

20. Look at the first 16 packets in the top viewing pane. You'll see that they are all TCP. This communications was that of a web login to a cable modem router. The first 16 packets reflect the transfer of the web page from the router web server to the user PC.

21. Re-open the Protocol Hierarchy window as you did in step 17.

22. Notice that the TCP packet count is 16 but only 6 are identified as containing data. TCP says that 10 packets not carrying data accounted for 566 bytes (see End Bytes column) and the 6 with data accounted for 4,336 bytes. This gives a total of 4,902 bytes transferred. Packets (4,5,6,8,9, 11) have data in them. The actual file that was transferred for web login is only 3,459 bytes in size. The overhead for the protocol layers was 1443 bytes which gives us the 4,902 total reported. You can close the Protocol Hierarchy window now.

23. If you look at packet 4 it is the client making a request of the server for web login. Packet 5 is the response from the server. Packets 6,8,9,11 are the actual xml web page being downloaded to the client browser.

24. We will be looking at packet 11 and following its data through the protocol stack. Highlight packet 11 in the top pane.

25. In the middle pane you should see 5 lines (Frame, Ethernet, Internet Protocol, Transmission Control Protocol, and Data). We will be looking at each level individually.

26. Click on the Frame line in the middle pane. Notice that all the data in the bottom pane (raw data) becomes highlighted. This shows that all the data is part of the frame that came across the physical medium. Each numerical pair in the bottom frame represents a byte of data. These pairs are hexadecimal numbers. The frame line says that 75 bytes were captured and if you count them you should see 75 pairs of Hexadecimal numbers.

27. Now click on the Ethernet line of the middle pane. Notice that the highlighted portion in the bottom pane has shrunk down to just the first 14 bytes. The first 6 pairs represent the Destination address, the next 6 represent the source address, and the last 2 represent the type. The last two have a value of 08 00 which is expressed as 0x0800. This says pass this info to the IP layer. The lower left part of the Wireshark window will confirm the byte totals. You should see that it is listing 14 bytes.

28. In the middle pane, open up the Ethernet II line and you will see the destination, source, and type displayed in ascii format. If you click on destination, source, or type, you will see the corresponding byte pairs being highlighted in the bottom pane.

29. Notice that the destination and source addresses are the physical MAC addresses of the two NICs. They are hexadecimal matches to what is in the bottom pane.

30. Next select the Internet protocol Layer. You will see that there are 20 bytes highlighted now. 1 byte is the version number, 1 byte for the header length, 1 byte for the differentiated service field, 2 bytes for total length, 2 bytes for identification, 1 byte for flags, 2 bytes for the fragment

offset, 1 byte for time to live, 1 byte for protocol, 2 bytes for checksum of the header, and four bytes for each of the source and destination addresses.

31. Open up the Internet Protocol line in the middle pane. Highlight the time to live line. You should see a value of 150 and in the lower pane a value highlighted of 96. If you use your calculator you'll see that they are the same, 96 being the Hex value of decimal 150.

32. Highlight the protocol line. You'll see that it says TCP (0x06). This is the value that Wireshark looked for when it labeled the protocol for the packets as TCP.

33. If you click on the source and destination IP lines, you'll see that 4 pairs are highlighted for each. Using your calculator you would be able to convert c0 a8 00 01 into 192.168.0.1 and c0 a8 00 65 into 192.168.0.101.

34. Click on the Transmission Control Protocol line in the middle pane. You'll see that 20 bytes are highlighted in the bottom pane.

35. Open up the Transmission Control Protocol line in the middle pane. The first line is the source port. It lists as 5678. Highlighting the source port line reveals a highlighted 16 2e in the bottom pane. Converting that in the calculator should give you 5678.

36. Highlight the destination port and you should see that 08 06 converts into 2054 as well.

37. The sequence number is a bit trickier to play with. Notice that it states a number of 3565 but highlights a number when converted equals 1624395229. This obviously doesn't match up. So now we need to look at how sequence numbers are computed. Notice that if you highlight the next sequence number it doesn't highlight any part of the bottom pane data. This is because it isn't part of the transmission. It is calculated based on the current sequence number and the size of the packet data. If you look in the middle pane the data shows itself to be 21 bytes in size. This fits the picture as our current sequence number is 3565 and our next one is 21 bigger at 3586. To compute our huge sequence number value we need to go back to the last data packet (9) and look at its sequence number and data size.

38. Go to packet 9 and open up the TCP line in the middle pane. Highlight the sequence number of 2419 and compute the highlighted value in the bottom pane. It should be 1624394083. Subtract this number from the 1624395229 of packet 11. You should come up with the value of 1146.

39. Go to the data value of packet 9 in the middle pane. Its data size is 1146 bytes. Do you see the correlation? Sequence numbers are augmented by the size of the last packet received.

40. Go back to packet 11 and highlight the data line in the middle pane. You will see the last 21 bytes are highlighted.

41. If you were to count there are 21 bytes characters in "</device>..</root >.." If you look to an ascii conversion table you'll be able to identify the various letters and symbols from the hex values in the bytes.

42. Go to packet 17 and let's see what a UDP packet looks like. You'll see that the Ethernet and IP headers are similar to TCP. The UDP header is only 8 bytes long and has less overhead than that of TCP. As there is the chance of loss with UDP, you will see that 10 identical packets

were sent in less than a 10th of a second. Packets 17 through 26 differ only by the time they were generated.

43. The SSDP protocol packets were simple service discovery packets that look for universal plug and play devices. Notice the multicast address used and the source port of 1901 and destination port of 1900. These were sent by the router.

44. **End of PE**

## Single Loss Expectancy / Annual Loss Expectancy PE

$$(SLE = \text{Asset value} \times EF)$$

$$(ALE = SLE \times ARO)$$

Find the SLE and the ALE for each line of the table below...

Asset	Value	EF (%)	ARO	SLE	ALE
Trade Secret	50,000	10	.01		
Customer CC info	300,000	30	3.0		
Data warehouse	150,000	25	0.1		

Answer the following questions...

1. You're the administrator for a research firm that works on only one project at a time and collects data through the Web to a single server. The value of each research project is approximately \$100,000. At any given time, an intruder could commandeer no more than 90 percent of the data. The industry average for ARO is 33%.

SLE =

ALE =

2. You're the administrator of a web server that generates \$25,000 per hour in revenue. The probability of the web server failing is estimated to be 25 percent, and a failure would lead to three hours of downtime and cost \$5,000 in components to correct.

SLE =

ALE =

3. You work at the help desk for a small company. One of the most common requests you must respond to is to help retrieve a file that has been accidentally deleted by a user. On average, this happens about 20 times annually. About 40 percent of the time the files cannot be recovered, requiring the company to recreate them. The cost to the company is two hours of labor at \$25 an hour.

SLE =

ALE =

4. Your company has installed new network servers, changing its network from a peer-to-peer network to a client/server-based network. The network consists of 200 users who make an average of \$20 an hour. Previously, none of the workstations involved in the network had anti-virus software installed on the machines. This was because there was no connection to the Internet, and the workstations didn't have floppy disk drives or Internet connectivity, so the risk of viruses was deemed minimal. Currently, one of the new servers provides a broadband connection to the Internet, which employees can now use to send and receive email, and surf the Internet. One of the IT managers read a report stating that other companies reported an 80 percent chance of viruses infecting their network and that it took an average of three hours to restore data. A vendor will sell licensed copies of anti-virus software for all servers and workstations at a cost of \$4,700 per year. The company has asked you to determine the annual loss that can be expected from viruses, and determine if it is beneficial in terms of cost to purchase licensed copies of anti-virus software.
  - A. What is the Annualized Rate of Occurrence (ARO) for this risk?
  - B. Calculate the Single Loss Expectancy (SLE) for this risk.
  - C. Using the formula  $ARO \times SLE = ALE$ , calculate the Annual Loss Expectancy.
  - D. Determine whether it is beneficial in terms of monetary value to purchase the anti-virus software by calculating how much money would be saved or lost by purchasing the software.

## Single Loss Expectancy / Annual Loss Expectancy

### Answer Sheet

Asset	Value	EF (%)	ARO	SLE	ALE
Trade Secret	50,000	10	.01	5,000	50
Customer CC info	300,000	30	3.0	90,000	270,000
Data warehouse	150,000	25	.1	37,500	3,750

1. The SLE is \$90,000 ( $100,000 \times .9$ ), and the ARO is .33. Therefore, the ALE is \$29,700 ( $90,000 \times .33$ ).
2. The SLE is \$80,000 ( $\$25,000 \times 3 \text{ hours} + \$5000$ ), and the ARO is .25. Therefore the ALE is \$20,000 ( $\$80,000 \times .25$ ).
3. The SLE is \$20 ( $\$50 \times .4$ ), and the ARO is 20. Therefore the ALE equals \$400 ( $\$20 \times 20$ ).
4. The Annualized Rate of Occurrence (ARO) is the likelihood of a risk occurring within a year. The scenario states that trade magazines calculate an 80% risk of virus infection after connecting to the Internet, so the ARO is 80% or .8.

The Single Loss Expectancy (SLE) is the dollar value of the loss that equals the total cost of the risk. In the case of this scenario, there are 200 users who make an average of \$20 per hour. Multiplying the number of employees who are unable to work due to the system being down by their hourly income, this means that the company is losing \$4,000 an hour ( $200 \times \$20 = \$4000$ ). Because it may take up to three hours to repair damage from a virus, this amount must be multiplied by three because employees will be unable to perform duties for approximately three hours. This makes the SLE \$12,000 ( $\$4,000 \times 3 = \$12,000$ ).

The ALE is calculated by multiplying the ARO by the SLE ( $\text{ARO} \times \text{SLE} = \text{ALE}$ ). In this case, this would mean that you would multiply \$12,000 by 80 percent (.8) to give you \$9,600 ( $.8 \times \$12,000 = \$9,600$ ). Therefore, the ALE is \$9,600.

Because the ALE is \$9,600, and the cost of the software that will minimize this risk is \$4,700 per year, this means that the company would save \$4,900 per year by purchasing the software ( $\$9,600 - \$4,700 = \$4900$ ).

## Appendix B – Ports and Protocols

**Port Numbers** - are divided into three ranges:

**Well Known Ports:** ports number 0 - 1023

**Registered Ports:** ports number 1024 - 49151

**Dynamic and/or Private Ports:** 49152 – 65535

7	Echo
19	Chargen
20	FTP (File Transfer Protocol) - data
21	FTP (File Transfer Protocol) - control
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
49	TACACS+
53	DNS (Domain Name Service)
67/68	DHCP (Dynamic Host Control Protocol)
69	Trivial File Transfer Protocol
79	Finger
80	HTTP (HyperText Transfer Protocol)
88	Kerberos
110	POP3 (Post Office Protocol, version 3)
111	RPC (Remote Procedure Call) SUN
115	SFTP (Simple File Transfer Protocol)
119	NNTP (Network News Transfer Protocol)
123	NTP (Network Time Protocol)
135	RPC (Remote Procedure Call) Microsoft Locator
137,138,139	NetBIOS
143	IMAP (Internet Message Access Protocol)
161/162	SNMP (Simple Network Management Protocol)
194	IRC (Internet Relay Chat); 994 over SSL/TLS
389	LDAP (Lightweight Directory Access Protocol)
443	SSL (Secure Socket Layer)
636	Secure LDAP
1433/1434	Microsoft SQL Server
1701	L2TP, L2F
1723	PPTP
1812	RADIUS
3389	Remote Desktop Protocol
5000	Yahoo Messenger

## Appendix D – Algorithms

Name	Type	Algorithm	Size
DES	Symmetric	Block cipher	Block: 64 bits; Key 64 bits (56 + 8 parity)
3DES	Symmetric	Block cipher (used in PGP/GPG)	Block: 64 bits; Key 192 bits (168 + 24 parity)
AES	Symmetric	Rijndael Block cipher (used in PGP/GPG)	Block: 128; Key: 128, 192, 256 bits
Blowfish	Symmetric	Block cipher	Block: 64 bits; Key: variable 32 to 448 bits
Twofish	Symmetric	Block cipher (used in PGP/GPG)	Block: 128 bits; Key: variable 128, 192, 256 bits
CAST-128	Symmetric	Block cipher; used in PGP/GPG	Block: 64 bits; Key: variable 40 to 128
CAST-256	Symmetric	Block cipher; used in PGP/GPG	Block: 128 bits; Key: Variable (128, 160, 192, 224, 256)
RC4	Symmetric	Stream cipher (used in WEP)	Stream; Variable key size (40-2048 bits)
RC5	Symmetric	Block cipher	Block: 32, 64, 128 bits; Key: Variable (0 to 2048)
RC6	Symmetric	Block cipher	Block: 128 bits; Key: variable 0 to 2048; (includes integer multiplication and four 4-bit registers, instead of two)
IDEA	Symmetric	Block cipher (used in PGP/GPG)	Block: 64 bits; Key: 128 bits
SAFER+	Symmetric	Block cipher (bluetooth for key derivation)	Block; 128 bits Key: 128, 192 and 256 bits
SAFER++	Symmetric	Block cipher (bluetooth for key derivation)	Block: 64 bits and 128 bits; Key: 64 and 128 bits
RSA	Asymmetric	Key Exchange, Encryption, Digital Signatures; used in PGP/GPG	Large prime numbers; Based on the difficulty of factoring $N$ , a product of two large prime numbers Key: 512-bit to arbitrarily long (1024-2048 considered safe)
Diffie-Hellman	Asymmetric	Key Exchange (used in PGP/GPG)	Based on discrete logarithms Key: 512-bit to arbitrarily long (1024-2048 considered safe)
El Gamal	Asymmetric	Key Exchange, Encryption, Digital Signatures	Based on discrete logarithms; very slow when used to create digital signatures Key: 256-bit to arbitrarily long (1024-2048 considered safe)
ECC	Asymmetric	Key Exchange, Encryption, Digital Signatures (used in cell phones and wireless devices)	Based on points on an elliptic curve
HMAC	Hash		Variable
MD5	Hash		512-bit block processing / 128 bit digest
SHA-1	Hash	used in PGP/GPG	512-bit processing / 160 bit digest
Whirlpool	Hash		512 bit block processing / 512 bit digest

## Appendix E – Glossary

### **3DES**

Also known as Triple Digital Encryption Standard (DES). A block cipher algorithm used for encryption.

### **802.11a**

The standard that provides for bandwidths of up to 54Mbps in the 5GHz frequency spectrum.

### **802.11b**

The standard that provides for bandwidths of up to 11Mbps in the 2.4GHz frequency spectrum. This standard is also called Wireless Fidelity (Wi-Fi) or 802.11 high rate.

### **802.11g**

The standard that provides for bandwidths of 20Mbps in the 2.4GHz frequency spectrum.

### **802.11n**

A proposed amendment to the 802.11 standard that provides for bandwidths of 74Mbps in the 2.4GHz and 5GHz frequency spectrums. The standard is expected to be released in 2009.

## **A**

### **Acceptable Use Policy**

Agreed-upon principles set forth by a company to govern how the employees of that company may use resources such as computers and Internet access.

### **Access Control**

The means of giving or restricting user access to network resources. Access control is usually accomplished through the use of an access control list (ACL).

### **Access control list (ACL)**

A table or data file that specifies whether a user or group has access to a specific resource on a computer or network.

### **Access Point (AP)**

The point at which access to a network is accomplished. This term is often used in relation to a wireless access point (WAP).

### **Accounting**

The act of keeping track of activity. Most often, this term is used to refer to tracking users' interactions with network resources via log files that are routinely scanned and checked.

**Acknowledgment (ACK)**

A message confirming that a data packet was received. Acknowledgment occurs at the Transport layer of the Open Systems Interconnection (OSI) and TCP/IP models.

**Active Directory**

A directory service that is the replacement for NT Directory Service (NTDS) and is included with Windows 2000/2003.

**Active Sniffing**

Involves an attacker gaining access to a host in the network through a switch and logically disconnecting it from the network.

**ActiveX**

A Microsoft technology that allows customized controls, icons, and other features to increase the usability of web-enabled systems.

**Address Resolution Protocol (ARP)**

Protocol used to map known IP addresses to unknown physical addresses.

**AD-IDS**

Anomaly-detection intrusion detection system. An AD-IDS works by looking for deviations from a pattern of normal network traffic.

**Advanced Encryption Standard (AES)**

A FIPS publication that specifies a standard cryptographic algorithm for use by the U.S. government.

**Adware**

Software that gathers information to pass on to marketers or intercepts personal data such as credit card numbers and makes them available to third parties.

**Alert**

A notification that an unusual condition exists and should be investigated.

**Algorithm**

The series of steps/formulas/processes that is followed to arrive at a result.

**Analyzer**

The component or process that analyzes the data collected by the sensor.

**Annual Loss Expectancy (ALE)**

A calculation that is used to identify risks and calculate the expected loss each year.

**Annualized Rate of Occurrence (ARO)**

A calculation of how often a threat will occur. For example, a threat that occurs once every five years has an annualized rate of occurrence of 1/5, or 0.2.

### **Anomaly Detection**

The act of looking for variations from normal operations (anomalies) and reacting to them.

### **Anonymous Authentication**

Authentication that does not require a user to provide a username, password, or any other identification before accessing resources.

### **Antivirus**

A category of software that uses various methods to prevent and eliminate viruses in a computer. It typically also protects against future infection.

### **Application Layer**

The seventh layer of the Open Systems Interconnection (OSI) model. This layer deals with how applications access the network and describes application functionality, such as file transfer, messaging, and so on.

### **Application Programming Interface (API)**

An abstract interface to the services and protocols provided by an operating system.

### **Armored Virus**

A virus that is protected in a way that makes disassembling it difficult. The difficulty makes it “armored” against antivirus programs that have trouble getting to, and understanding, its code.

### **ARP Table**

The table that the Address Resolution Protocol uses. Contains a list of known TCP/IP addresses and their associated physical addresses. The table is cached in memory so that ARP lookups don't have to be performed for frequently accessed addresses.

### **Asset**

Any resource of value that you want to secure and protect.

### **Asymmetric Encryption**

Encryption in which two keys must be used. One key is used to encrypt data, and the other is needed to decrypt the data. Asymmetric encryption is the opposite of symmetric encryption, where a single key serves both purposes.

### **Attack**

Any unauthorized intrusion into the normal operations of a computer or computer network. The attack can be carried out to gain access to the system or any of its resources.

### **Auditing**

The act of tracking resource usage by users.

### **Authentication**

The means of verifying that someone is who they say they are.

### **Authentication Header (AH)**

A header used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays.

### **Availability**

The ability of a resource to be accessed, often expressed as a time period. Many networks limit users' ability to access network resources to working hours, as a security precaution.

## **B**

### **Back Door (backdoor)**

An opening left in a program application (usually by the developer) that allows additional access to data. Typically, these are created for debugging purposes and aren't documented. Before the product ships, the back doors are closed; when they aren't closed, security loopholes exist.

### **Backup**

A usable copy of data made to media. Ideally, the backup is made to removable media and stored for recovery should anything happen to the original data.

### **Biometrics**

The science of identifying a person by using one or more of their features. The feature can be a thumbprint, a retinal scan, or any other biological trait.

### **BIOS**

The basic input/output system for an IBM-based PC. It is the firmware that allows the computer to boot.

### **Birthday Attack**

A probability method of finding collision in hash functions.

### **Blowfish**

A type of symmetric block cipher created by Bruce Schneier.

### **Boot Sector**

Also known as the Master Boot Record (MBR). The first sector of the hard disk, where the program that boots the operating system resides. It's a popular target for viruses.

### **Brute Force Attack**

A type of attack that relies purely on trial and error.

**Buffer Overflow Attack**

A type of denial of service (DoS) attack that occurs when more data is put into a buffer than it can hold, thereby overflowing it (as the name implies).

**Business Continuity Planning (BCP)** A contingency plan that allows a business to keep running in the event of a disruption to vital resources.

**Business Impact Analysis (BIA)** A study of the possible impact if a disruption to a business's vital resources were to occur.

**C**

**Certificate**

A digital entity that establishes who you are and is often used with e-commerce. It contains your name and other identifying data.

**Certificate Authority (CA)**

An issuer of digital certificates (which are then used for digital signatures or key pairs).

**Certificate Policies**

Policies governing the use of certificates.

**Certificate Practice Statement (CPS)**

The principles and procedures employed in the issuing and managing of certificates.

**Certificate Revocation**

The act of making a certificate invalid.

**Certificate Revocation List (CRL)**

A list of digital certificate revocations that must be regularly downloaded to stay current.

**Chain of Custody**

The log of the history of evidence that has been collected.

**Challenge Handshake Authentication Protocol (CHAP)**

A protocol that challenges a system to verify identity.

**Change Documentation**

Documentation required to make a change in the scope of any particular item. In the realm of project management, a change document is a formal document requiring many signatures before key elements of the project can be modified.

**Checksum**

A hexadecimal value computed from transmitted data that is used in error checking routines.

**Clear Text**

Unencrypted text that can be read with any editor.

**Client**

The part of a client/server network where the computing is usually performed. In a typical setting, a client uses the server for remote storage, backups, or security (such as a firewall).

**Client/Server Network**

A server-centric network in which all resources are stored on a file server and processing power is distributed among workstations and the file server.

**Clustering**

A method of balancing loads and providing fault tolerance.

**Coax (coaxial cable)**

A type of cabling used in computer networks.

**Code Escrow**

The storage and conditions for release of source code provided by a vendor, partner, or other party.

**Collusion**

An agreement between individuals to commit fraud or deceit.

**Common Criteria (CC)**

A document of specifications detailing security evaluation methods for IT products and systems.

**Common Gateway Interface (CGI)**

An older form of scripting that was used extensively in early web systems.

**Companion Virus**

A virus that creates a new program that runs in place of an expected program of the same name.

**Confidentiality**

Assurance that data remains private and no one sees it except for those expected to see it.

**Configuration Management**

The administration of setup and changes to configurations.

**Cookie**

A plain-text file stored on your machine that contains information about you (and your preferences) and is used by a database server.

**Cryptanalysis**

The study and practice of finding weaknesses in ciphers.

**Cryptographic Algorithm**

A symmetric algorithm, also known as a cipher, used to encrypt and decrypt data.

**Cryptography**

The field of mathematics focused on encrypting and decrypting data.

**Custodian**

An individual responsible for maintaining the data, and the integrity of it, within their area.

**D****Data Link layer**

The second layer of the Open Systems Interconnection (OSI) model. It describes the physical topology of a network.

**Data Packet**

A unit of data sent over a network. A packet includes a header, addressing information, and the data itself.

**Data Repository**

A centralized storage location for data, such as a database.

**Datagram**

A Layer 3, User Datagram Protocol (UDP) packet descriptor.

**Decryption**

The process of converting encrypted data back into its original form.

**Demilitarized Zone (DMZ)**

An area for placing web and other servers that serve the general public outside the firewall, therefore, isolating them from internal network access.

**Denial of Service (DoS) attack**

A type of attack that prevents any users, even legitimate ones, from using a system.

**Dictionary Attack**

The act of attempting to crack passwords by testing them against a list of dictionary words.

### **Differential Backup**

A type of backup that includes only new files or files that have changed since the last full backup. Differential backups differ from incremental backups in that they do not clear the archive bit upon their completion.

### **Diffie-Hellman**

An asymmetric standard for exchanging keys. This cryptographic algorithm is used primarily to send secret keys across public networks. The process isn't used to encrypt or decrypt messages; it's used merely for the transmission of keys in a secure manner.

### **Digital Signature**

An asymmetrically encrypted signature whose sole purpose is to authenticate the sender.

### **Directory Service**

A network service that provides access to a central database of information, which contains detailed information about the resources available on a network.

### **Direct-Sequence Spread Spectrum (DSSS)**

A communications technology that is used to communicate in the 802.11 standard.

### **Disaster Recovery Plan**

A plan outlining the procedure by which data is recovered after a disaster.

### **Discretionary Access Control (DAC)**

A method of restricting access to objects based on the identity of the subjects or the groups to which they belong.

### **Disk Mirroring**

Technology that keeps identical copies of data on two disks to prevent the loss of data if one disk faults.

### **Disk Striping**

Technology that enables writing data to multiple disks simultaneously in small portions called stripes. These stripes maximize use by having all the read/write heads working constantly. Different data is stored on each disk and isn't automatically duplicated (this means disk striping in and of itself doesn't provide fault tolerance).

### **Distributed Denial of Service (DDoS) Attack**

A derivative of a DoS attack in which multiple hosts in multiple locations all focus on one target to reduce its availability to the public. See denial of service (DoS) attack.

### **DNS Server**

Any server that performs address resolution from a DNS fully qualified domain name (FQDN) to an IP address. See *also* Domain Name Service (DNS), Internet Protocol (IP).

### **DNS Zone**

An area in the DNS hierarchy that is managed as a single unit. See *also* Domain Name Service (DNS).

### **DoD Networking Model**

A four-layer conceptual model describing how communications should take place between computer systems. The four layers are Process/Application, Host-to-Host, Internet, and Network Access.

### **Domain Name Service (DNS)**

The network service used in TCP/IP networks that translates hostnames to IP addresses. See *also* Transmission Control Protocol/Internet Protocol (TCP/IP).

### **Dumpster Diving**

Looking through trash for clues, often in the form of paper scraps, to find users' passwords and other pertinent information.

### **Dynamic Host Configuration Protocol (DHCP)**

A protocol used on a TCP/IP network to send client configuration data, including IP address, default gateway, subnet mask, and DNS configuration, to clients. DHCP uses a four-step process: Discover, Offer, Request, and Acknowledgement.

### **Dynamic Packet Filtering**

A type of firewall used to accept or reject packets based on their contents.

## **E**

### **Eavesdropping**

Any type of passive attack that intercepts data in an unauthorized manner, usually in order to find passwords.

### **Electromagnetic Interference (EMI)**

The interference that can occur during transmissions over copper cable because of electromagnetic energy outside the cable. The result is degradation of the signal.

### **Elliptic Curve Cryptosystem (ECC)**

A type of public key cryptosystem that requires a shorter key length than many other cryptosystems (including the de facto industry standard, RSA).

### **Encapsulating Security Payload (ESP)**

A header used to provide a mix of security services in IPv4 and IPv6. ESP can be used alone or in combination with the IP Authentication Header (AH).

### **Encryption**

The process of converting data into a form that makes it less likely to be usable to anyone intercepting it if they can't decrypt it.

**Enticement**

The process of luring someone.

**Entrapment**

The process of encouraging an attacker to perform an act, even if they don't want to do it.

**Escalation**

The act of moving something up in priority. Often, when an incident is escalated, it's brought to the attention of the next highest supervisor. See *also* privilege escalation.

**Evaluation Assurance Level (EAL)**

A level of assurance, expressed as a numeric value, based on standards set by the Common Criteria Recognition Agreement (CCRA).

**Exposure factor (EF)**

A calculation of how much data (or other assets) could be lost from a single occurrence. If all the data on the network could be jeopardized by a single attack, the exposure factor is 100 percent.

**Extranet**

Web (or similar) services set up in a private network to be accessed internally and by select external entities, such as vendors and suppliers.

**F**

**Fail-over (Failover)**

The process of reconstructing a system or switching over to other systems when a failure is detected.

**False Positive**

A flagged event that isn't really an event and has been falsely triggered.

**Faraday Cage**

An electrically conductive wire mesh or other conductor woven into a "cage" that surrounds a room and prevents electromagnetic signals from entering or leaving the room through the walls.

**Fault Tolerance**

The ability to withstand a fault (failure) without losing data.

**Federal Information Processing Standard (FIPS)**

An agreed-upon standard published under the Information Technology Management Reform Act. The secretary of commerce approves the standards after they're developed by the National Institute of Standards and Technology (NIST) for federal computer systems.

### **File Transfer Protocol (FTP)**

TCP/IP and software that permit transferring files between computer systems and utilize clear-text passwords. Because FTP has been implemented on numerous types of computer systems, files can be transferred between disparate computer systems

### **Firewall**

A combination of hardware and software that protects a network from attack by hackers who could gain access through public networks, including the Internet.

### **Footprinting**

The process of systematically identifying the network and its security posture.

### **Forensics**

In terms of security, the act of looking at all the data at your disposal to try to figure out who gained unauthorized access and the extent of that access.

### **Frequency-hopping spread spectrum (FHSS)**

A communications technology used to communicate in the 802.11 standard. FHSS accomplishes communication by hopping the transmission over a range of predefined frequencies.

### **Full Backup**

A backup that copies all data to the archive medium.

## **G**

### **Gramm-Leach-Bliley Act**

A government act containing rules on privacy of consumer finance information.

## **H**

### **Hacker**

Generally used to refer to someone who gains access to a system, software, or hardware without permission. Also can be called a cracker.

### **Handshake**

The process of agreeing to communicate and share data. TCP uses a three-way handshake to establish connections, and part of this process can be exploited by certain types of attacks.

### **Hash/Hashing**

The process of transforming characters into other characters that represent (but are not) the originals. Traditionally, the results are smaller and more secure than the original.

### **Hash Value**

A single number used to represent an original piece of data.

**Health Insurance Portability and Accountability Act (HIPAA)**

An act that addresses security and privacy of health-related data. Provide resource reliability and availability.

**Hoax**

Typically an e-mail message warning of something that isn't true, such as the outbreak of a new virus. The hoax can send users into a panic and cause more harm than the virus.

**Honeypot (Honey Pot)**

A bogus system set up to attract and slow down a hacker. A honeypot can also be used to learn of the hacking techniques and methods that hackers employ.

**Host-based IDS (HIDS)**

An intrusion detection system that is host based. The alternative is network based.

**Host-based IPS (HIPS)**

An intrusion prevention system that is host based. To prevent the intrusion, it must first detect it (thus making it a superset of H-IDS) and then act accordingly.

**Hot Fix (Hotfix)**

Another word for a patch. When Microsoft rolls a bunch of hotfixes together, they become known as a service pack.

**HVAC**

A common acronym used for *heating, ventilation, and air conditioning*.

**Hypertext Markup Language (HTML)**

A set of codes used to format text and graphics that will be displayed in a browser. The codes define how data will be displayed.

**Hypertext Transfer Protocol (HTTP)**

The protocol used for communication between a web server and a web browser.

**Hypertext Transfer Protocol (Secure)**

Also known as HTTPS. A combination of HTTP with Secure Sockets Layer (SSL) to make for a secure connection. It uses port 443 by default

**ICMP Attack**

An attack that occurs by triggering a response from the Internet Control Message Protocol (ICMP) when it responds to a seemingly legitimate maintenance request.

**Incident**

An attempt to violate a security policy, a successful penetration, a compromise of a system, or unauthorized access to information.

**Incident Response**

How an organization responds to an incident.

**Incremental Backup**

A type of backup in which only new files or files that have changed since the last full backup or the last incremental backup are included. Incremental backups clear the archive bit on files upon their completion.

**Instant Messaging (IM)**

Immediate communication that can be sent back and forth between users who are currently logged on. From a security standpoint, there are risks associated with giving out information via IM that can be used in social engineering attacks; in addition, attachments sent can contain viruses.

**International Data Encryption Algorithm (IDEA)**

An algorithm that uses a 128-bit key. This product is similar in speed and capability to Digital Encryption Standard (DES), but it's more secure. IDEA is used in Pretty Good Privacy (PGP).

**International Telecommunications Union (ITU)**

Organization responsible for communications standards, spectrum management, and the development of communications infrastructures in underdeveloped nations.

**Internet Architecture Board (IAB)**

The committee that oversees management of the Internet. It's made up of two subcommittees: the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF).

**Internet Assigned Numbers Authority (IANA)**

The organization responsible for governing IP addresses.

**Internet Control Message Protocol (ICMP)**

A message and management protocol for TCP/IP. The Ping utility uses ICMP.

**Internet Engineering Task Force (IETF)**

An international organization that works under the Internet Architecture Board to establish standards and protocols relating to the Internet.

**Internet Group Management Protocol (IGMP)**

A protocol used for multicasting operations across the Internet.

**Internet Layer**

The network layer responsible for routing, IP addressing, and packaging.

### **Internet Message Access Protocol (IMAP)**

A protocol with a store-and-forward capability. It can also allow messages to be stored on an e-mail server instead of downloaded to the client.

### **Internet Protocol (IP)**

The protocol in the TCP/IP suite responsible for network addressing.

### **Internetwork Packet Exchange (IPX)**

A connectionless, routable network protocol based on the Xerox XNS architecture. It's the default protocol for versions of NetWare before NetWare 5. It operates at the Network layer of the Open Systems Interconnection (OSI) model and is responsible for addressing and routing packets to workstations or servers on other networks.

### **Intranet**

Web (or similar) services set up in a private network to be accessed internally only.

### **Intrusion**

The act of entering a system without authorization to do so.

### **Intrusion Detection System (IDS)**

Tools that identify and respond to attacks using defined rules or logic. An IDS can be network based or host based.

### **IP Security (IPSec)**

A set of protocols that enable encryption, authentication, and integrity over IP. IPSec is commonly used with virtual private networks (VPNs) and operates at Layer 3.

### **IP Spoofing**

An attack during which a hacker tries to gain access to a network by pretending their interface has the same network address as the internal network.

## **J**

### **JavaScript**

A programming language that allows access to system resources of the system running the script. These scripts can interface with all aspects of an operating system just like programming languages, such as the C language.

## **K**

### **Kerberos**

An authentication scheme that uses tickets (unique keys) embedded within messages. Named after the three-headed guard dog that stood at the gates of Hades in Greek mythology.

**Key Distribution Center (KDC)**

An organization/facility that generates keys for users.

**Key Exchange Algorithm (KEA)**

A method of offering mutual authentication and establishing data encryption keys.

**Key Suspension**

The temporary deferment of a key for a period of time (such as for a leave of absence).

**Hash Message Authentication Code (HMAC)**

“A mechanism for message authentication using cryptographic hash functions” per the draft of the Federal Information Processing Standard (FIPS) publication. Addressed in RFC 2104.

**L**

**LANMAN**

An old authentication method used with early Windows-based systems.

**Lattice**

The concept that access differs at different levels. Often used in discussion with the Biba and Bell La-Padula models as well as with cryptography to differentiate between security levels based upon user/group labels.

**Layer 2 Forwarding (L2F)**

A tunneling protocol often used with virtual private networks (VPNs). L2F was developed by Cisco.

**Layer 2 Tunneling Protocol (L2TP)**

A tunneling protocol that adds functionality to Point-to-Point Protocol (PPP). This protocol was created by Microsoft and Cisco and is often used with virtual private networks (VPNs).

**Lightweight Directory Access Protocol (LDAP)**

A set of protocols that was derived from X.500 and operates at port 389.

**Local Area Network (LAN)**

A network that is restricted to a single building, group of buildings, or even a single room. A LAN can have one or more servers.

**Local Registration Authority (LRA)**

An authority used to identify or establish the identity of an individual for certificate issuance.

### **Logic Bomb**

Any code that is hidden within an application and causes something unexpected to happen based on some criteria being met. For example, a programmer could create a program that always makes sure his name appears on the payroll roster; if it doesn't, then key files begin to be erased.

## **M**

### **MAC Address**

The address that is either assigned to a network card or burned into the network interface card (NIC). PCs use MAC addresses to keep track of one another and keep each other separate.

### **Macro Virus**

A software exploitation virus that works by using the macro feature included in many applications.

### **Malicious Code**

Any code that is meant to do harm.

### **Mandatory Access Control (MAC)**

A security policy wherein labels are used to identify the sensitivity of objects. When a user attempts to access an object, the label is checked to see if access should be allowed (that is, whether the user is operating at the same sensitivity level). This policy is "mandatory," because labels are automatically applied to all data (and can be changed only by administrative action), as opposed to "discretionary" policies that leave it up to the user to decide whether to apply a label.

### **Man-in-the-Middle (MITM) attack**

An attack that occurs when someone/-thing that is trusted intercepts packets and retransmits them to another party. Man-in-the-middle attacks have also been called TCP/IP hijacking in the past.

### **Mantrap**

A device, such as a small room, that limits access to one or a few individuals. Mantraps typically use electronic locks and other methods to control access.

### **Mean-Time-Between-Failures (MTBF)**

The measure of the anticipated incidence of failure of a system or component.

### **Mean-Time-To-Repair (MTTR)**

The measurement of how long it takes to repair a system or component once a failure occurs.

**Media Access Control (MAC)**

A sublayer of the Data Link layer of the Open Systems Interconnection (OSI) model that controls the way multiple devices use the same media channel. It controls which devices can transmit and when they can transmit.

**Message Authentication Code (MAC)**

A common method of verifying integrity. The MAC is derived from the message and a secret key.

**Message Digest Algorithm**

An algorithm that creates a hash value. The hash value is also used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

**Microsoft Challenge Handshake Authentication Protocol (MSCHAP)**

An implementation of the Challenge Handshake Authentication Protocol (CHAP) common in Microsoft's Windows-based operating systems. The latest version, and the only one supported in Windows Vista, is MSCHAPv2.

**Misuse-Detection IDS (MD-IDS)**

A method of evaluating attacks based on attack signatures and audit trails.

**Modem**

A communications device that converts digital computer signals into analog tones for transmission over the Public Switched Telephone Network (PSTN) and converts them back to digital upon reception. The word *modem* is an acronym for *modulator/demodulator*.

**Modification Attack**

An attack that modifies information on your system.

**Multi-factor**

The term employed anytime more than one factor must be considered.

**Multipartite Virus**

A virus that attacks a system in more than one way.

**N**

**National Institute of Standards and Technology (NIST)**

An agency (formerly known as the National Bureau of Standards [NBS]) that has been involved in developing and supporting standards for the U.S. government for over 100 years. NIST has become involved in cryptography standards, systems, and technology in a variety of areas. It's primarily concerned with governmental systems, where it exercises a great deal of influence.

**National Security Agency (NSA)**

The U.S. government agency responsible for protecting U.S. communications and producing foreign intelligence information. It was established by presidential directive in 1952 as a separately organized agency within the Department of Defense (DoD).

**NetBIOS Extended User Interface (NetBEUI)**

A protocol used to transport Network Basic Input Output System (NetBIOS) traffic in a LAN.

**NetWare Directory Services (NDS)**

A directory management service used to manage all of the resources in a network. In later versions, the acronym was changed to Novell Directory Services, and the service is now known as eDirectory. NDS provides a database of all of the network objects or resources.

**Network Attached Storage (NAS)**

Storage, such as hard drives, attached to a network for the purpose of storing data for clients on the network. Network attached storage is commonly used for backing up data.

**Network-Based IDS (N-IDS)**

An approach to an intrusion detection system (IDS), it attaches the system to a point in the network where it can monitor and report on all network traffic.

**Network Basic Input Output System (NetBIOS)**

The native protocol of Windows PCs. It provides a 15-character naming convention for resources on the network. NetBIOS is a broadcast-oriented network protocol in that all traffic is available to all devices in a LAN. The protocol can be transported over NetBIOS Extended User Interface (NetBEUI), TCP/IP, or Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

**Network File System (NFS)**

A protocol that enables users to access files on remote computers as if the files were local.

**Network Interface Card (NIC)**

A physical device that connects computers and other network equipment to the transmission medium.

**Network Layer**

The third layer of the OSI model, it is responsible for logical addressing and translating logical names into physical addresses. This layer also controls the routing of data from source to destination as well as the building and dismantling of packets.

**Network Operations Center (NOC)**

A single, centralized area for network monitoring and administrative control of systems.

**Network Operating System (NOS)**

The software enabling networking; NOS can be on a LAN or WAN.

**Network Sniffer**

A device that has access to the signaling on the network cable.

**New Technology LAN Manager (NTLM)**

The protocol that Microsoft Windows-based operating systems use for authentication with remote access protocols.

**Non-Repudiation**

Verifying (by whatever means) that data was seen by an intended party. It makes sure they received the data and can't repudiate (dispute) that it arrived.

**Notification**

The act of being alerted to an event.

**O**

**One-Time Pad (OTP)**

Words added to values during authentication. The message to be encrypted is added to this random text before hashing.

**Open Shortest Path First (OSPF)**

A link-state routing protocol used in IP networks.

**Open Systems Interconnect (OSI)**

A model defined by the ISO to categorize the process of communication between computers in terms of seven layers. The seven layers are Application, Presentation, Session, Transport, Network, Data Link, and Physical.

**OVAL**

An acronym for Open Vulnerability and Assessment Language, it is a community standard for system analysis that focuses on testing, analyzing, and reporting.

**P**

**Packet Filtering**

A firewall technology that accepts or rejects packets based on their content.

**Packet Switching**

The process of breaking messages into packets at the sending router for easier transmission over a WAN.

### **Partitioning**

The process of breaking a network into smaller components that can be individually protected.

### **Password Authentication Protocol (PAP)**

One of the simplest forms of authentication. Authentication is accomplished by sending the username and password to the server and having them verified. Passwords are sent as clear text and, therefore, can be easily seen if intercepted.

### **Patch**

A fix for a known software problem.

### **Perimeter Security**

Security set up on the outside of the network or server to protect it.

### **Phage Virus**

A virus that modifies and alters other programs and databases.

### **Phishing**

A form of social engineering in which you simply ask someone for a piece of information that you are missing by making it look as if it is a legitimate request. Commonly sent via e-mail.

### **Phreaker**

Someone who abuses phone systems, as opposed to data systems.

### **Physical Layer**

The first layer of the OSI model; controls the functional interface.

### **Physical Port**

On a computer, an interface where you can connect a device.

### **Ping**

A TCP/IP utility used to test whether another host is reachable. An Internet Control Message Protocol (ICMP) request is sent to the host, which responds with a reply if it's reachable. The request times out if the host isn't reachable.

### **Ping-of-Death**

A large Internet Control Message Protocol (ICMP) packet sent to overflow the remote host's buffer. A ping of death usually causes the remote host to reboot or hang.

### **Point-to-Point**

Network communication in which two devices have exclusive access to a network medium. For example, a printer connected to only one workstation is using a point-to-point connection.

### **Point-to-Point Protocol (PPP)**

A full-duplex line protocol that supersedes Serial Line Internet Protocol (SLIP). It's part of the standard TCP/IP suite and is often used in dial-up connections.

### **Point-to-Point Tunneling Protocol (PPTP)**

An extension to Point-to-Point Protocol (PPP) that is used in virtual private networks (VPNs). An alternative to PPTP is L2TP.

### **Polymorphic Virus**

An attribute of some viruses that allows them to mutate and appear differently each time they crop up. The mutations make it harder for virus scanners to detect (and react) to the viruses.

### **Port**

Some kind of opening that allows network data to pass through.

### **Port Address Translation (PAT)**

A means of translating between ports on a public and private network. Similar to Network Address Translation (NAT), which translates addresses between public and private.

### **Port Scanner**

The item (physical or software) that scans a server for open ports that can be taken advantage of. Port scanning is the process of sending messages to ports to see which ones are available and which ones aren't.

### **Post Office Protocol (POP)**

An email access program that can be used to retrieve email from an email server.

### **Post Office Protocol Version 3 (POP3)**

The protocol used to download email from a SMTP email server to a network client.

### **Power Conditioner**

A device that "conditions" the electrical supply to take out spikes and surges.

### **Presentation Layer**

The sixth layer of the OSI model; responsible for formatting data exchange, such as graphic commands, and converting character sets. This layer is also responsible for data compression, data encryption, and data stream redirection.

### **Privacy**

A state of security in which information isn't seen by unauthorized parties without the express permission of the party involved.

### **Private Branch Exchange (PBX)**

A system that allows users to connect voice, data, pagers, networks, and almost any other application into a single telecommunications system. A PBX system allows an organization to be its own phone company.

### **Privilege Audit**

An audit performed to verify that no user is accessing information, or able to access information, beyond the security level at which they should be operating.

### **Privilege Escalation**

The result when a user obtains access to a resource they wouldn't normally be able to access.

### **Promiscuous Mode**

A mode wherein a network interface card (NIC) intercepts all traffic crossing the network wire and not just the traffic intended for it.

### **Protocol Analyzer**

A software and hardware troubleshooting tool that is used to decode protocol information to try to determine the source of a network problem and to establish baselines.

### **Proxy**

A type of firewall that prevents direct communication between a client and a host by acting as an intermediary.

### **Proxy Firewall**

A proxy server that also acts as a firewall, blocking network access from external networks.

### **Proxy Server**

A type of server that makes a single Internet connection and services requests on behalf of many users.

### **Public Key Cryptography**

(a.k.a. asymmetric cryptography) A technology that uses two keys, a public key and a private key, to facilitate communication. The public key is used to encrypt a message to a receiver.

### **Public Key Cryptography Standards (PKCS)**

A set of voluntary standards created by RSA security and industry security leaders.

### **Public Key Infrastructure (PKI)**

A two-key encryption system wherein messages are encrypted with a private key and decrypted with a public key.

**Public Key Infrastructure X.509 (PKIX)**

The Internet Engineering Task Force (IETF) working group developing standards and models for the Public Key Infrastructure (PKI) environment.

**Q**

**Quantum Cryptography**

Cryptography based on changing the polarity of a photon. Quantum cryptography makes the process of interception difficult because any attempt to intercept the message changes the value of the message.

**R**

**Radio Frequency Interference (RFI)**

The byproduct of electrical processes, similar to electromagnetic interference. The major difference is that RFI is usually projected across a radio spectrum.

**Redundant Array of Independent (or Inexpensive) Disks (RAID)**

A configuration of multiple hard disks used to provide fault tolerance, should a disk fail, or gains in efficiency. Different levels of RAID exist.

**Registration Authority (RA)**

An organization that offloads some of the work from a certificate authority (CA). An RA system operates as a middleman in the process. The RA can distribute keys, accept registrations for the CA, and validate identities. The RA doesn't issue certificates; that responsibility remains with the CA.

**Remote Access Server (RAS)**

A computer that has one or more modems installed to enable remote connections to the network.

**Remote Authentication Dial-In User Service (RADIUS)**

A mechanism that allows authentication of dial-in and other network connections. RADIUS is commonly used by Internet service providers (ISPs) and in the implementation of virtual private networks (VPNs).

**Replay Attack**

Any attack where the data is retransmitted repeatedly (often fraudulently or maliciously). In one such possibility, a user can replay a web session and visit sites intended only for the original user.

**Replication**

The process of copying directory information to other servers to keep them all synchronized.

### **Repository**

A database or database server where the certificates are stored.

### **Repudiation Attack**

An attack in which the intruder modifies information in a system.

### **Request for Comments (RFC)**

A document creation process and a set of practices that originated in 1969 and is used for proposed changes to Internet standards.

### **Retrovirus**

A virus that attacks or bypasses the antivirus software installed on a computer.

### **Reverse DNS**

Using an IP address to find a domain name rather than using a domain name to find an IP address (normal DNS). Pointer (PTR) records are used for the reverse lookup, and often reverse DNS is used to authenticate incoming connections.

### **Revocation**

The process of canceling credentials that have been lost or stolen (or are no longer valid). With certificates, revocation is accomplished with a Certificate Revocation List (CRL).

### **Risk Analysis**

An evaluation of each risk that can be identified. Each risk should be outlined, described, and evaluated on the likelihood of it occurring.

### **Risk Assessment**

An evaluation of how much risk you and your organization are willing to take. An assessment must be performed before any other actions, such as how much to spend on security in terms of dollars and manpower, can be decided.

### **Rivest Cipher 5 (RC5)**

A cipher algorithm created by Ronald Rivest (for RSA) and known for its speed. It works through blocks of variable sizes using three phases: key expansion, encryption, and decryption.

### **Role-Based Access Control (RBAC)**

A type of control wherein the levels of security closely follow the structure of an organization. The role the person plays in the organization (accountant, salesman, and so on) corresponds to the level of security access they have to data.

### **Rootkit**

Software program that has the ability to obtain root-level access and hide certain things from the operating system.

### **Router**

A device that connects two or more networks and allows packets to be transmitted and received between them. A router determines the best path for data packets from source to destination.

### **Routing**

A function of the Network layer that involves moving data throughout a network. Data passes through several network subnetworks using routers that can select the path the data takes.

### **Routing Information Protocol (RIP)**

A distance-vector route discovery protocol used by Internetwork Packet Exchange (IPX) and Internet Protocol (IP). IPX uses hops and ticks to determine the cost for a particular route. See *also* Internetwork Packet Exchange (IPX).

### **Routing Table**

A table that contains information about the locations of other routers on the network and their distance from the current router.

### **RSA**

One of the providers of cryptography systems to industry and government. RSA stands for the initials of the three founders of RSA Security Inc.: Rivest, Shamir, and Adleman. RSA maintains a list of standards for Public Key Cryptography Standards (PKCS).

## **S**

### **Sandbox**

A set of rules used when creating a Java applet that prevents certain functions when the applet is sent as part of a web page.

### **Scanning**

The process that attackers use to gather information about how a network is configured.

### **Screened Host**

A router that is in front of a server on the private network. Typically, this server does packet filtering before reaching the firewall/proxy server that services the internal network.

### **Secure Electronic Transaction (SET)**

A protocol developed by Visa and MasterCard for secure credit card transactions. The protocol is becoming an accepted standard by many companies. SET provides encrypted credit card numbers over the Internet, and it's most suited to small amounts of data transmission.

### **Secure Hash Algorithm (SHA)**

A one-way hash algorithm designed to ensure the integrity of a message.

**Secure Hypertext Transfer Protocol (S-HTTP)**

A protocol used for secure communications between a web server and a web browser.

**Secure Shell (SSH)**

A replacement for rlogin in Unix/Linux that includes security. rlogin allowed one host to establish a connection with another with no real security being employed; SSH replaces it with slogin and digital certificates.

**Secure Sockets Layer (SSL)**

A protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.

**Security Token**

A piece of data that contains the rights and access privileges of the token bearer as part of the token.

**Security Zone**

A method of isolating a system from other systems or networks.

**Segment**

A unit of data transmission found at the Transport layer of the Open Systems Interconnection (OSI) model and used by TCP.

**Separation of Duties**

A set of policies designed to reduce the risk of fraud and prevent other losses in an organization.

**Sequence Number**

A number used to determine the order in which parts of a packet are to be reassembled after the packet has been split into sections.

**Server**

A computer that provides resources to the clients on the network.

**Service Account**

An account created on a server for a user to perform special services, such as a backup operator, an account operator, and a server operator.

**Service-Level Agreement (SLA)**

An agreement that specifies performance requirements for a vendor. This agreement may use mean time before failure (MTBF) and mean time to repair (MTTR) as performance measures in the SLA.

**Session Key**

The agreed-upon (during connection) key used between a client and a server during a session. This key is generated by encrypting the server's digital ID (after validity has

been established). The asymmetric key pair is then used to encrypt and verify the session key that is passed back and forth between client and server during the length of the connection.

### **Session Layer**

The fifth layer of the OSI model. It determines how two computers establish, use, and end a session. Security authentication and network naming functions required for applications occur here. The Session layer establishes, maintains, and breaks dialogs between two stations.

### **Shielded Twisted Pair (STP)**

Network cabling media that has a shield, similar to coax, wrapped over the wires.

### **Shoulder Surfing**

Watching someone when they enter their username/password/ sensitive data.

### **Signed Applet**

An applet that doesn't run in the Java sandbox and has higher system access capabilities. Signed applets aren't usually downloaded from the Internet but are provided by in-house or custom programming efforts.

### **Simple Mail Transfer Protocol (SMTP)**

A protocol for sending e-mail between SMTP servers.

### **Simple Network Management Protocol (SNMP)**

The management protocol created for sending information about the health of the network-to-network management consoles.

### **Single Loss Expectancy (SLE)**

The cost of a single loss when it occurs. This loss can be a critical failure, or it can be the result of an attack.

### **Single Sign-On (SSO)**

A relationship between the client and the network wherein the client is allowed to log on one time, and all resource access is based on that logon (as opposed to needing to log on to each individual server to access the resources there).

### **Site Survey**

A generic site survey involves listening in on an existing wireless network using commercially available technologies. A wireless site survey, or wireless survey, is the process of planning and designing a wireless network, in particular a 802.11.

### **SMTP Relay**

A feature designed into many email servers that allows them to forward email to other email servers. While the ability to act as a relay exists to allow networks to grow, the possibility exists for rogue servers to also participate.

### **Smurf Attack**

An attack in which large volumes of ICMP echo requests (pings) are broadcast to all other machines on the network and in which the source address of the broadcast system has been spoofed to appear as though it came from the target computer. When all the machines that received the broadcast respond, they flood the target with more data than it can handle.

### **Sniffer**

A physical device that listens in (sniffs) on network traffic and looks for items it can make sense of. There is a legitimate purpose for these devices: Administrators use them to analyze traffic. However, when they're used by sources other than the administrator, they become security risks.

### **Social Engineering**

An attack that uses others by deceiving them.

### **Socket**

The primary method used to communicate with services and applications such as the Web and Telnet. The socket is a programming construct that enables communication by mapping between ports and addresses.

### **Spam**

Unwanted, unsolicited email sent in bulk.

### **Spoofing Attack**

An attempt by someone or something to masquerade as someone else.

### **Spyware**

Software programs that work—often actively—on behalf of a third party.

### **State Table**

A firewall security method that monitors the status of all the connections through the firewall.

### **Stateful Packet Filtering**

Inspections that occur at all levels of the network and provide additional security using a state table that tracks every communications channel.

### **Stealth Virus**

A virus that attempts to avoid detection by masking itself from applications.

### **Steganography**

The science of hiding information within other information, such as a picture.

### **Subscriber**

An individual who is attempting to present a certificate proving authenticity.

### **Surge Protector**

A device that protects electrical components from momentary or instantaneous increases (called spikes) in a power line.

### **SYN Flood**

A denial of service attack in which the hacker sends a barrage of spoofed SYN packets. The receiving station tries to respond to each SYN request for a connection, thereby tying up all the resources. All incoming connections are rejected until all current connections can be established.

### **System Architecture**

Documents that provide you with the blueprint of your organization's software and hardware infrastructure.

## **T**

### **Tap**

A type of connection that directly attaches to a cable.

### **TCP ACK Attack**

An attack that begins as a normal TCP connection and whose purpose is to deny service. It's also known as a TCP SYN flood.

### **TCP Sequence Attack**

An attack wherein the attacker intercepts and then responds with a sequence number similar to the one used in the original session. The attack can either disrupt a session or hijack a valid session.

### **TCP/IP Hijacking**

An attack in which the attacker commandeers a TCP session from a legitimate user after the legitimate user has achieved authentication, thereby removing the need for the attacker to authenticate himself.

### **Teardrop Attack**

A DoS attack that uses large packets and odd offset values to confuse the receiver and help facilitate a crash.

### **Telnet**

A protocol that functions at the Application layer of the OSI model, providing terminal emulation capabilities. See *also* Open Systems Interconnection (OSI) model.

### **Temporal Key Interchange/Integrity Protocol (TKIP)**

A wrapper that works with wireless encryption to strengthen WEP implementations.

### **Terminal Access Controller Access Control System (TACACS)**

An authentication system that allows credentials to be accepted from multiple methods, including Kerberos. The TACACS client/server process occurs in the same manner as the Remote Authentication Dial-In User Service (RADIUS) process.

### **Thin Client**

Systems that don't provide any disk storage or removable media on their workstations.

### **Threat**

Any perceivable risk.

### **Token**

A piece of data holding information about the user. This information can contain group IDs, user IDs, privilege level, and so on.

### **Transmission Control Protocol (TCP)**

The protocol found at the Host-to-Host layer of the Department of Defense (DoD) model. This protocol breaks data packets into segments, numbers them, and sends them in order. The receiving computer reassembles the data so that the information is readable for the user. In the process, the sender and the receiver confirm that all data has been received; if not, it's resent. TCP is a connection-oriented protocol.

### **Transmission Control Protocol/Internet Protocol (TCP/IP)**

The protocol suite developed by the Department of Defense (DoD) in conjunction with the Internet. It was designed as an internetworking protocol suite that could route information around network failures. Today it's the de facto standard for communications on the Internet.

### **Transport Layer**

The fourth layer of the OSI model. It's responsible for checking that the data packet created in the Session layer was received. If necessary, it also changes the length of messages for transport up or down the remaining layers.

### **Transport Layer Security (TLS)**

A protocol whose purpose is to verify that secure communications between a server and a client remain secure. Defined in RFC 2246.

### **Triple-DES (3DES)**

A symmetric block cipher algorithm used for encryption.

### **Trojan Horse**

Any application that masquerades as one thing in order to get past scrutiny and then does something malicious. One of the major differences between Trojan horses and viruses is that Trojan horses tend not to replicate themselves.

**Trusted Platform Module (TPM)**

A method of utilizing encryption and storing the passwords on a chip. The hardware holding the chip is then needed to decrypt the data and make it readable.

**Tunneling**

The act of sending data across a public network by encapsulating it into other packets.

**Two-factor Authentication**

Using two access methods as a part of the authentication process.

**U**

**Uniform Resource Locator (URL)**

A way of identifying a document on the Internet. It consists of the protocol used to access the document and the domain name or IP address of the host that holds the document.

**Uninterruptible Power Supply (UPS)**

A device that can provide short-term power, usually by using batteries.

**Unshielded Twisted Pair (UTP)**

The most common networking cable currently in use; Unshielded Twisted Pair (UTP) is 8-wire cabling used with Ethernet.

**Uptime**

The amount of time a particular computer or network component has been functional.

**User Datagram Protocol (UDP)**

The protocol at the Host-to-Host layer of the TCP/IP Department of Defense (DoD) model, which corresponds to the Transport layer of the OSI model. Packets are divided into datagrams, given numbers, sent, and put back together at the receiving end. UDP is a connectionless protocol.

**V**

**Virtual LAN (VLAN)**

Local area network (LAN) that allows users on different switch ports to participate in their own network separate from, but still connected to, the other stations on the same or a connected switch.

**Virtual Link**

A link created by using a switch to limit network traffic.

**Virtual Private Network (VPN)**

System that uses the public Internet as a backbone for a private interconnection (network) between locations.

**Virus**

A program intended to damage a computer system. Sophisticated viruses are encrypted and hide in a computer, and might not appear until the user performs a certain action or until a certain date.

**W****War Driving**

Driving around with a laptop looking for open wireless access points with which to communicate.

**Weak Key**

A cipher hole that can be exploited.

**Web Proxy**

A type of proxy that is used to act on behalf of a web client or web server.

**Web Server**

A server that holds and delivers web pages and other web content using HTTP.

**Wide Area Network (WAN)**

A network that crosses local, regional, and/or international boundaries.

**Windows Internet Naming Service (WINS)**

A Network Basic Input Output System (NetBIOS) name resolution service employed in Windows networks. Windows Internet Naming Service (WINS) translates hostnames into network addresses.

**Windows Socket**

A Microsoft API used to interact with TCP/IP.

**Wired Equivalent Privacy (WEP)**

A security protocol for 802.11b (wireless) networks that attempts to establish the same security for them as would be present in a wired network.

**Wireless Access Point**

A wireless bridge used in a multipoint radio frequency (RF) network.

**Wireless Bridge**

A bridge that performs all the functions of a regular bridge but uses RF instead of cables to transmit signals.

**Wireless Fidelity (Wi-Fi)**

An 802.11b or 802.11g wireless network operating in the 2.4Ghz or 5Hz frequency range.

**Wireless Local Area Network (WLAN)**

A local area network that employs wireless access points (WAPs) and clients using the 802.11 standards.

**Wireless Transport Layer Security (WTLS)**

The security layer of the Wireless Applications Protocol (WAP). WTLS provides authentication, encryption, and data integrity for wireless devices.

**Work Factor**

An estimate of the amount of time and effort that would be needed to break a system.

**Worm**

A program similar to a virus. Worms, however, propagate themselves over a network.

**X**

**X.500**

The International Telecommunications Union (ITU) standard for directory services in the late 1980s.

**X.509**

The International Telecommunications Union (ITU) standard for defining digital signatures.

**Z**

**Zombie**

Any system taking directions from a master control computer. Zombies are often utilized in distributed denial of service (DDoS) attacks.

**Zone**

An area in a building where access is individually monitored and controlled.

## Appendix F – Acronyms

<b>Acronym</b>	<b>Description</b>
3DES	Triple Data Encryption Standard
ACL	Access Control List
AD-IDS	Anomaly-Detection Intrusion Detection System
AES	Advanced Encryption Standard
AES256	Advanced Encryption Standard 256bit
ALE	Annual Loss Expectancy
AP	Access Point
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
CA	Certificate Authority
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CRL	Certificate Revocation List
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service or Server
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
ECC	Elliptical Curve Cryptography
EAP	Extensible Authentication Protocol
EF	Exposure Factor
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HIDS	Host-based Intrusion Detection
HIPS	Host-based Intrusion Prevention
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol over SSL
HVAC	Heating, Ventilation, Air Conditioning
IANA	Internet Assigned Numbers Authority
IAU	Internet Architecture Board
ICMP	Internet Control Manager
ICMP	Internet Control Manager Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IKMP	Internet Key Management Protocol
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IPSEC	Internet Protocol Security
ISP	Internet Service Provider
ITU	International Telecommunications Union
KDC	Key Distribution Center
KEA	Key Exchange Algorithm
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LANMAN	LAN Manager
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MD5	Message Digest version 5
MD-IDS	Misuse-Detection Intrusion Detection System
MITM	Man-in-the-Middle
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
NAC	Network Access Control
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Detection Prevention
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NOS	Network Operating System
NTLM	New Technology LAN Manager
OCSP	Online Certificate Status Protocol
OS	Operating System

OSI	Open Systems Interconnect
OTP	One-Time Pad
OVAL	Open Vulnerability Assessment Language
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBX	Private Branch Exchange
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Independent (or Inexpensive) Disk
RAS	Remote Access Service
RBAC	Role-based Access Control
RFC	Request for Comments
RFI	Radio Frequency Interference
RSA	Rivest, Shamir, and Adleman
S/MIME	Secure Multipurpose Internet Mail Exchange
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SLA	Service Level Agreement
SLE	Single Loss Expectancy
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
SSO	Single Sign-On
STP	Shielded Twisted Pair
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

WAN	Wide Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WTLS	Wireless Transport Layer Protocol

## Appendix G – Resources

### Recommended Readings

Barrett, D., Hausman, K., Weiss, M. (2009). *CompTIA Security+ Exam, 2nd Edition, Exam SY0-201*. USA: Pearson Education, Inc.

Ciampa, Mark. (2009). *CompTIA Security+ 2008 In Depth*. Boston: Course Technology, Cengage Learning.

Samuelle, T. (2009). *Mike Meyers' CompTIA Security+ Certification Passport, Second Edition*. USA: McGraw-Hill.

White, G, Conklin, W. (2009). *CompTIA Security+ All-in-One Exam Guide, Second Edition*. USA: McGraw-Hill.

### Websites and Organizations

**Several websites actively track security issues. This list provides you with the major providers of security information on the Web. Many of these organizations also provide newsletters and mailings to announce changes or security threats.**

- **Center for Education and Research in Information Assurance and Security (CERIAS):** An industry-sponsored center at Purdue University that is focused on technology and related issues. CERIAS provides news and information on technology threats. The website is <http://www.cerias.purdue.edu>.
- **CERT Coordination Center:** A federally sponsored partnership in conjunction with Carnegie Mellon University that provides Internet security expertise. CERT offers a wide variety of information about current threats and best practices in security. The website is <http://www.cert.org>. One of the most interesting pages you can find there, details the steps to take to recover after your computer has been compromised. This resource is located at [http://www.cert.org/tech\\_tips/win-UNIX-system\\_compromise.html](http://www.cert.org/tech_tips/win-UNIX-system_compromise.html).
- **Computer Security Institute (CSI):** A professional organization that offers national conferences, membership publications, and information on computer security issues. CSI is one of the oldest societies in this area. The website is <http://www.gocsi.com>.
- **CCcure Family of Portals:** A website which provides free security training resources. This website helps people in achieving their goal of becoming certified on some of the leading security certifications such as the CISSP, SSCP, CISM, CISA, or GCFW or simply helping them in learning more about what security is all about. This website is a great resource for practice quizzes. The website is <http://www.cccure.org>.

- **European Institute for Computer Anti-Virus Research (EICAR):** An association of European corporations, schools, and educators that are concerned with information security issues. The website is <http://www.eicar.org>.
- **Information Systems Security Association (ISSA):** A not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. The website is <https://www.issa.org>.
- **Information Systems Audit and Control Association (ISACA):** A global organization for information governance, control, security and audit professionals. It offers certifications such as CISA, CISM, CGEIT, etc. The website is <https://www.isaca.org>.
- **Linux Security:** The latest news and articles related to Linux security issues can be found here. The website is <http://www.linuxsecurity.com>.
- **National Institute of Standards and Technology (NIST):** A governmental agency involved in the creation and use of standards. These standards are generally adopted by governmental agencies, and they are used as the basis for other standards. NIST has an organization specifically addressed to computer issues: the Computer Security Response Center (CSRC). The CSRC/NIST maintains a database of current vulnerabilities and other useful information. The website is <http://www.csrc.nist.gov>.
- **National Security Institute (NSI):** A clearinghouse of information relating to security. This site offers a wealth of information on many aspects of physical and information security, including a free e-newsletter. The website is <http://www.nsi.org>.
- **SANS Institute:** The SysAdmin, Audit, Network, Security (SANS) Institute is a research and educational organization. SANS offers seminars, research, and other information relating to the security field. The website is <http://www.sans.org>.
- **Security Focus:** General news and information on security topics of all sorts are archived here. There is also a weekly newsletter that you can subscribe to. The website is <http://www.securityfocus.com>.

### Trade Publications

Numerous trade publications exist that address issues relating to security at different levels of difficulty. Some of these publications are good sources of overview information and case studies; others go into the theoretical aspects of security.

- **2600: The Hacker Quarterly:** A magazine that provides tips and information on computer security issues. Don't let the name fool you, there is a wealth of

information on current issues about security in this magazine. The website is <http://www.2600.com>.

- **CertCities:** An online magazine that covers the broad field of certification. It also does features on the pros and cons of various certifications, and it contains articles related to the computer profession. The website is <http://www.certcities.com>.
- **CIO:** A monthly publication that specializes in IT management issues and periodically offers security-related articles that tend to be high level. The website is <http://www.cio.com>.
- **CSO Magazine:** A monthly magazine that focuses on issues of interest to security executives. The website is <http://www.csoonline.com>.
- **Hackin9:** A bimonthly publication aimed at those with an interest in “hard core IT security”. The website is <http://www.en.hakin9.org/>.
- **Information Security Magazine Information Security:** A monthly publication that focuses on computer security issues. The website is <http://informationsecurity.techtarget.com>.
- **InformationWeek:** A magazine that addresses management and other IT issues. This magazine provides updates in the field of technology. The website is <http://www.informationweek.com>.
- **InfoWorld:** A magazine that deals with PC issues from an IT management perspective. This magazine offers regular articles on security and related topics. The website is <http://www.infoworld.com>.

## Appendix H – Domain Review Questions

### Domain 1.0 Cryptography

1. All of the following are valid cryptographic hash functions EXCEPT:
  - A. RIPEMD.
  - B. RC4.
  - C. SHA-512.
  - D. MD4.
  
2. Which of the following would be used when a higher level of security is desired for encryption key storage?
  - A. TACACS+
  - B. L2TP
  - C. LDAP
  - D. TPM
  
3. Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?
  - A. Cognitive password
  - B. Password sniffing
  - C. Brute force
  - D. Social engineering
  
4. Certificates are used for: (Select TWO).
  - E. Client authentication.
  - F. WEP encryption.
  - G. Access control lists.
  - H. Code signing.
  - I. Password hashing.
  
5. A certificate authority takes which of the following actions in PKI?
  - A. Signs and verifies all infrastructure messages
  - B. Issues and signs all private keys
  - C. Publishes key escrow lists to CRLs
  - D. Issues and signs all root certificates
  
6. The security administrator wants each user to individually decrypt a message but allow anybody to encrypt it. Which of the following MUST be implemented to allow this type of authorization?
  - A. Use of CA certificate
  - B. Use of public keys only
  - C. Use of private keys only
  - D. Use of public and private keys

7. A CRL is comprised of:
  - A. Malicious IP addresses.
  - B. Trusted CA's.
  - C. Untrusted private keys.
  - D. Public keys.
  
8. Which of the following algorithms has well documented collisions? (Select TWO).
  - A. AES
  - B. MD5
  - C. SHA-256
  - D. RSA
  - E. SHA
  
9. A company is sending out a message to all users informing them that all internal messages need to be digitally signed. This is a form of which of the following concepts?
  - A. Availability
  - B. Non-repudiation
  - C. Authorization
  - D. Cryptography
  
10. Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?
  - A. SSLv2
  - B. SSHv1
  - C. RSA
  - D. TLS
  
11. Which of the following are encryption algorithms that can use a 128-bit key size? (Select TWO).
  - A. AES
  - B. RC4
  - C. Twofish
  - D. DES
  - E. SHA2
  
12. Which of the following would MOST likely ensure that swap space on a hard disk is encrypted?
  - A. Database encryption
  - B. Full disk encryption
  - C. Folder and file encryption
  - D. Removable media encryption

13. Which of the following components MUST be trusted by all parties in PKI?
  - A. Key escrow
  - B. CA
  - C. Private key
  - D. Recovery key
  
14. Elliptic curve cryptography: (Select TWO)
  - A. is used in both symmetric and asymmetric encryption.
  - B. is used mostly in symmetric encryption.
  - C. is mostly used in embedded devices.
  - D. produces higher strength encryption with shorter keys.
  - E. is mostly used in hashing algorithms.
  
15. Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?
  - A. Recovery agent
  - B. Certificate authority
  - C. Trust model
  - D. Key escrow
  
16. All of the following are valid cryptographic hash functions EXCEPT:
  - A. RIPEMD.
  - B. RC4.
  - C. SHA-512.
  - D. MD4.
  
17. When a certificate issuer is not recognized by a web browser, which of the following is the MOST common reason?
  - A. Lack of key escrow
  - B. Self-signed certificate
  - C. Weak certificate pass-phrase
  - D. Weak certificate cipher
  
18. Which of the following PKI components identifies certificates that can no longer be trusted?
  - A. CRL
  - B. CA public key
  - C. Escrow
  - D. Recovery agent
  
19. Which of the following is used to ensure message integrity during a TLS transmission?
  - A. RIPEMD
  - B. RSA
  - C. AES
  - D. HMAC

20. Which of the following uses only a private key?
- A. RSA
  - B. ECC
  - C. AES
  - D. SHA

### Domain 2.0 Network Security

1. In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the following security technologies could be used to provide remote access? (Select TWO).
- A. Subnetting
  - B. NAT
  - C. Firewall
  - D. NAC
  - E. VPN
2. Which of the following MOST interferes with network-based detection techniques?
- A. Mime-encoding
  - B. SSL
  - C. FTP
  - D. Anonymous email accounts
3. Which of the following should be considered to mitigate data theft when using CAT5 wiring?
- A. CCTV
  - B. Environmental monitoring
  - C. Multimode fiber
  - D. EMI shielding
4. Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).
- A. 10.4.4.125
  - B. 10.4.4.158
  - C. 10.4.4.165
  - D. 10.4.4.189
  - E. 10.4.4.199
5. Configuring the mode, encryption methods, and security associations are part of which of the following?
- A. IPSec
  - B. Full disk encryption
  - C. 802.1x
  - D. PKI

6. Which of the following network architecture concepts is used to securely isolate at the boundary between networks?
  - A. VLAN
  - B. Subnetting
  - C. DMZ
  - D. NAT
  
7. Which of the following protocols allows for secure transfer of files? (Select TWO).
  - A. ICMP
  - B. SNMP
  - C. SFTP
  - D. SCP
  - E. TFTP
  
8. Which of the following is true concerning WEP security?
  - A. WEP keys are transmitted in plain text.
  - B. The WEP key initialization process is flawed.
  - C. The pre-shared WEP keys can be cracked with rainbow tables.
  - D. WEP uses the weak RC4 cipher.
  
9. Which of the following BEST describes a common security concern for cloud computing?
  - A. Data may be accessed by third parties who have compromised the cloud platform
  - B. Antivirus signatures are not compatible with virtualized environments
  - C. Network connections are too slow
  - D. CPU and memory resources may be consumed by other servers in the same cloud
  
10. Jane, an administrator, needs to transfer DNS zone files from outside of the corporate network. Which of the following protocols must be used?
  - A. TCP
  - B. ICMP
  - C. UDP
  - D. IP
  
11. Which of the following technologies would allow for a secure tunneled connection from one site to another? (Select TWO).
  - A. SFTP
  - B. IPSec
  - C. HTTPS
  - D. ICMP
  - E. SSH

12. Which of the following must Jane, a security administrator, implement to ensure all wired ports are authenticated before a user is allowed onto the network?
- A. Intrusion prevention system
  - B. Web security gateway
  - C. Network access control
  - D. IP access control lists
13. Pete, the security administrator, wants to ensure that traffic to the corporate intranet is secure using HTTPS. He configures the firewall to deny traffic to port 80. Now users cannot connect to the intranet even through HTTPS. Which of the following is MOST likely causing the issue?
- A. The web server is configured on the firewall's DMZ interface.
  - B. The VLAN is improperly configured.
  - C. The firewall's MAC address has not been entered into the filtering list.
  - D. The firewall executes an implicit deny.
14. Which wireless security protocol provides the highest level of security?
- A. WPA
  - B. SSID
  - C. WPA2
  - D. WEP
15. Which of the following should a security administrator implement to prevent users from disrupting network connectivity, if a user connects both ends of a network cable to different switch ports?
- A. VLAN separation
  - B. Access control
  - C. Loop protection
  - D. DMZ
16. A small company needs to invest in a new expensive database. The company's budget does not include the purchase of additional servers or personnel. Which of the following solutions would allow the small company to save money on hiring additional personnel and minimize the footprint in their current datacenter?
- A. Allow users to telecommute
  - B. Setup a load balancer
  - C. Infrastructure as a Service
  - D. Software as a Service
17. Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?
- A. Man-in-the-middle
  - B. Bluejacking
  - C. Bluesnarfing
  - D. Packet sniffing

18. Jane, an administrator, hears reports of circles being drawn in the parking lot. Because the symbols fall within range of the company's wireless AP, the MOST likely concern is:
- A. that someone has used war chalking to help others access the company's network.
  - B. that the symbols indicate the presence of an evil twin of a legitimate AP.
  - C. that someone is planning to install an AP where the symbols are, to cause interference.
  - D. that a rogue access point has been installed within range of the symbols.
19. While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?
- A. EAP-TLS
  - B. PEAP
  - C. WEP
  - D. WPA
20. Matt, the security administrator, notices a large number of alerts on the NIDS. Upon further inspection, it is determined that no attack has really taken place. This is an example of a:
- A. False negative.
  - B. True negative.
  - C. False positive.
  - D. True positive.

### **Domain 3.0 Access Control and Identity Management**

1. Which of the following is a valid server-role in a Kerberos authentication system?
- A. Token issuing system
  - B. Ticket granting server
  - C. Security assertion server
  - D. Authentication agent
2. Sara, the IT Manager, would like to ensure that the router and switches are only available from the network administrator's workstation. Which of the following would be the MOST cost effective solution to ensure that only the network administrator can access these devices?
- A. Restrict console ports
  - B. Time of day restrictions
  - C. Implement ACLs
  - D. Implement an out-of-band administrative network

3. Which of the following combinations represents multifactor authentication?
  - A. Smart card and hard token
  - B. Cipher lock combination and proximity badge
  - C. Voice print analysis and facial recognition
  - D. Username and PIN
  
4. Which of the following should Sara, a security administrator, perform periodically to reduce an organization's risk exposure by verifying employee access?
  - A. Incident management
  - B. Account revalidation
  - C. Qualitative analysis
  - D. Quantitative analysis
  
5. Which of the following encrypts the body of a packet, rather than just the password, while sending information?
  - A. LDAP
  - B. TACACS+
  - C. ACLs
  - D. RADIUS
  
6. Which of the following risk related concepts BEST supports the identification of fraud?
  - A. Risk avoidance
  - B. Job rotation
  - C. ALE calculation
  - D. Clean desk policy
  
7. Which of the following authentication services uses a ticket granting system to provide access?
  - A. RADIUS
  - B. LDAP
  - C. TACACS+
  - D. Kerberos
  
8. Jane, the security administrator for a company, needs to assign permissions for users on her network. Which of the following would allow Jane to give ONLY the appropriate permissions necessary?
  - A. Separation of duties
  - B. Job rotation
  - C. Privilege escalation
  - D. Least privilege

9. Users in the marketing department are given a different level of access to files than users in the accounting department. Which of the following types of access control does this BEST describe?
- A. Standard access control
  - B. Role based access control
  - C. Mandatory access control
  - D. Discretionary access control
10. Which of the following authentication services uses the AAA architecture and runs on TCP?
- A. LDAP
  - B. Kerberos
  - C. RADIUS
  - D. TACACS+
11. Pete, a system administrator, is using a packet sniffer to troubleshoot remote authentication. Pete detects a device trying to communicate to UDP ports 1812 and 1813. Which of the following authentication methods is MOST likely being attempted?
- A. TACACS+
  - B. LDAP
  - C. Kerberos
  - D. RADIUS
12. Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee's credential?
- A. Account expiration
  - B. Password complexity
  - C. Account lockout
  - D. Dual factor authentication
13. Biometrics includes the use of which of the following authentication methods?
- A. Single sign-on
  - B. Retinal scan
  - C. Common access card
  - D. ACLs
14. Which of the following provides authentication, authorization, and accounting services?
- A. PKI
  - B. WPA2
  - C. NTLMv2
  - D. RADIUS

15. Role-based access control is BEST defined as an authorization system by which:
- A. Privileges are granted to persons based on membership in one or more functional groups.
  - B. A separate user account is created for each functional role a person has.
  - C. Access is limited to the time of day a person is expected to work.
  - D. Privileges are assigned to each person based upon authorized requests.
16. Matt, a server administrator, sets up database forms based on security rating levels. If a user has the lowest security rating then the database automatically determines what access that user has. Which of the following access control methods does this describe?
- A. Mandatory access control
  - B. Role based access control
  - C. Rule based access control
  - D. Discretionary access control
17. Which of the following authentication services would be used to authenticate users trying to access a network device?
- A. SSH
  - B. SNMPv3
  - C. TACACS+
  - D. TELNET
18. Which of the following access control technologies provides a rolling password for one-time use?
- A. RSA tokens
  - B. ACL
  - C. Multifactor authentication
  - D. PIV card
19. Which of the following is the BEST approach to perform risk mitigation of user access control rights?
- A. Conduct surveys and rank the results.
  - B. Perform routine user permission reviews.
  - C. Implement periodic vulnerability scanning.
  - D. Disable user accounts that have not been used within the last two weeks.
20. Which of the following MOST likely has its access controlled by TACACS+? (Select TWO).
- A. Mobile devices
  - B. Active directory
  - C. Router
  - D. Switch
  - E. Kerberos

**Domain 4.0 Threats and Vulnerabilities**

1. Which of the following malware types uses stealth techniques to conceal itself, cannot install itself without user interaction, and cannot automatically propagate?
  - A. Rootkit
  - B. Logic bomb
  - C. Adware
  - D. Virus
  
2. Which of the following is BEST utilized to actively test security controls on a particular system?
  - A. Port scanning
  - B. Penetration test
  - C. Vulnerability scanning
  - D. Grey/Gray box
  
3. Which of the following is Jane, a security administrator, MOST likely implementing when deleting all the unneeded files and modules of a newly installed application?
  - A. Exception handling
  - B. Patch management
  - C. System file clean up
  - D. Application hardening
  
4. A user downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?
  - A. Logic bomb
  - B. Worm
  - C. Trojan
  - D. Adware
  
5. Matt, the Chief Information Officer (CIO), wants to protect laptop users from zero day attacks. Which of the following would BEST achieve Matt's goal?
  - A. Host based firewall
  - B. Host based IDS
  - C. Anti-virus
  - D. Anti-spyware
  
6. Matt, an administrator, captures malicious DNS traffic on the network. Which of the following tools would be used to analyze the nature of this traffic?
  - A. Sniffer
  - B. Zone transfer
  - C. Network tap
  - D. Application firewall

7. The IT administrator wants to make sure that only certain devices can connect to the wireless network. Which of the following can she implement to accomplish this task?
- A. MAC filtering
  - B. Increase the power levels of the WAP
  - C. Dynamic DHCP
  - D. Disable SSID broadcast
8. A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?
- A. Fencing
  - B. Mantrap
  - C. A guard
  - D. Video surveillance
9. Which of the following should Sara, a technician, apply to prevent guests from plugging in their laptops and accessing the company network?
- A. Secure router configuration
  - B. Port security
  - C. Sniffers
  - D. Implicit deny
10. Sara, a student, is interested in learning about distributed denial of service attacks. Which of the following types of malware is MOST likely the primary focus of her study?
- A. Botnets
  - B. Logic bombs
  - C. Spyware
  - D. Trojans
11. Which of the following tools provides the ability to determine if an application is transmitting a password in clear-text?
- A. Protocol analyzer
  - B. Port scanner
  - C. Vulnerability scanner
  - D. Honeypot
12. Large, partially self-governing, collection of hosts executing instructions for a specific purpose is an example of which type of malware?
- A. Virus
  - B. Worm
  - C. Trojan
  - D. Botnet

13. Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?
- A. Rootkit
  - B. Logic bomb
  - C. Worm
  - D. Botnet
14. Which of the following utilizes the ECHO function of Internet Control Message Protocol (ICMP) to overwhelm a victim's system?
- A. Logic bomb
  - B. Whaling
  - C. Man-in-the-middle
  - D. Smurf attack
15. A web application has been found to be vulnerable to a SQL injection attack. Which of the following BEST describes the required remediation action?
- A. Change the server's SSL key and add the previous key to the CRL.
  - B. Install a host-based firewall.
  - C. Install missing security updates for the operating system.
  - D. Add input validation to forms.
16. Several staff members working in a datacenter have reported instances of tailgating. Which of the following could be implemented to prevent this security concern?
- A. Proximity readers
  - B. Mantraps
  - C. Video surveillance
  - D. Biometric keypad
17. Which of the following would Sara, a security administrator, implement to divert and analyze attacks?
- A. Protocol analyzer
  - B. DMZ
  - C. Port scanner
  - D. Honeypot
18. Which of the following describes a passive attempt to identify weaknesses?
- A. Vulnerability scanning
  - B. Zero day attack
  - C. Port scanning
  - D. Penetration testing

19. When an attack using a publicly known vulnerability compromises a system, it is considered to be which of the following?

- A. IV attack
- B. Zero day attack
- C. Buffer overflow
- D. Malicious insider threat

20. A targeted email attack sent to Sara, the company's Chief Executive Officer (CEO), is known as which of the following??

- A. Bluesnarfing
- B. Vishing
- C. Whaling
- D. Dumpster diving

### Domain 5.0 Compliance and Operational Security

1. Performing routine security audits is a form of which of the following controls?

- A. Preventive
- B. Detective
- C. Protective
- D. Proactive

2. Which of the following environmental controls would BEST be used to regulate cooling within a datacenter?

- A. Fire suppression
- B. Video monitoring
- C. EMI shielding
- D. Hot and cold aisles

3. Which of the following is a detective security control?

- A. CCTV
- B. Firewall
- C. Design reviews
- D. Bollards

4. Select the formula you would need to calculate SLE.

- A.  $AV * EF$
- B.  $ARO * ALE$
- C.  $AV * ARO$
- D.  $EF * ARO$

5. Which of the following is a preventative physical security control?
  - A. CCTV
  - B. Armed guard
  - C. Proper lighting
  - D. Access list
  
6. Which of the following should Matt, a security technician, integrate into the fire alarm systems to help prevent a fire from spreading?
  - A. HVAC
  - B. Humidity controls
  - C. Video monitoring
  - D. Thermostats
  
7. Which of the following will help Matt, an administrator; mitigate the risk of static electricity?
  - A. Lightning rods
  - B. EMI shielding
  - C. Humidity controls
  - D. Temperature controls
  
8. Which of the following policies is implemented in order to minimize data loss or theft?
  - A. PII handling
  - B. Password policy
  - C. Chain of custody
  - D. Zero day exploits
  
9. Which of the following is a policy that would force all users to organize their areas as well as help in reducing the risk of possible data theft?
  - A. Password behaviors
  - B. Clean desk policy
  - C. Data handling
  - D. Data disposal
  
10. A security administrator wants to determine what data is allowed to be collected from users of the corporate Internet-facing web application. Which of the following should be referenced?
  - A. Privacy policy
  - B. Human Resources policy
  - C. Appropriate use policy
  - D. Security policy

11. Risk can be managed in the following ways EXCEPT?
  - A. Mitigation
  - B. Acceptance
  - C. Elimination
  - D. Transference
  
12. Which of the following is the technical implementation of a security policy?
  - A. VLAN
  - B. Flood guards
  - C. Cloud computing
  - D. Firewall rules
  
13. Which of the following BEST defines risk?
  - A. A threat will have a larger impact than anticipated
  - B. Remediation of a known vulnerability is cost prohibitive
  - C. A degree of probability of loss
  - D. A user leaves a system unsecure
  
14. A company that purchases insurance to reduce risk is an example of which of the following?
  - A. Risk deterrence
  - B. Risk acceptance
  - C. Risk avoidance
  - D. Risk transference
  
15. Which of the following is a reason to perform user awareness and training?
  - A. To enforce physical security requirements by staff
  - B. To minimize the organizational risk posed by users
  - C. To comply with law and vendor software best practices
  - D. To identify the staff's personally owned electronic devices
  
16. Which of the following is used when performing a quantitative risk analysis?
  - A. Focus groups
  - B. Asset value
  - C. Surveys
  - D. Best practice
  
17. Which of the following describes the purpose of chain of custody as applied to forensic image retention?
  - A. To provide proof the evidence has not been tampered with or modified
  - B. To provide verification that the forensic examiner is qualified
  - C. To provide documentation as to who has handled the evidence
  - D. To provide a baseline reference

18. Which of the following is used when performing a qualitative risk analysis?
- A. Exploit probability
  - B. Asset value
  - C. Threat frequency
  - D. Judgment
19. During incident response, which of the following procedures would identify evidence tampering by outside entities?
- A. Hard drive hashing
  - B. Annualized loss expectancy
  - C. Developing audit logs
  - D. Tracking man hours and incident expenses
20. A company wants to have a backup site that is a good balance between cost and recovery time objectives. Which of the following is the BEST solution?
- A. Hot site
  - B. Remote site
  - C. Cold site
  - D. Warm site

### Domain 6.0 Application, Data, and Host Security

1. \_\_\_\_\_ is used to test for or find odd oversights and defects missed by human testers.
- A. Snooping
  - B. Hunting
  - C. Tracking
  - D. Fuzzing
2. Which of the following mitigation techniques is Pete, a security administrator, MOST likely to implement after the software has been released to the public?
- A. Error and exception handling
  - B. Fuzzing
  - C. Secure coding
  - D. Patch management
3. Which of the following has a programmer MOST likely failed to consider if a user entering improper input is able to crash a program?
- A. SDLM
  - B. CRC
  - C. Data formatting
  - D. Error handling

4. Which of the following can cause data loss from web based applications?
  - A. Device encryption
  - B. Poor error handling
  - C. Application hardening
  - D. XML
  
5. An SQL injection vulnerability can be caused by which of the following?
  - A. Password complexity
  - B. Improper input validation
  - C. Discretionary access controls
  - D. Cross-site request forgery
  
6. Which of the following would an administrator do to ensure that an application is secure and all necessary services are disabled?
  - A. Base lining
  - B. Application hardening
  - C. Secure application coding
  - D. Patch management
  
7. A vulnerability has been found in a service that is unnecessary for the corporate environment. Which of the following is the BEST way to mitigate this vulnerability?
  - A. Issue a hotfix to lower the vulnerability risk on the network
  - B. Issue a group policy to disable the service on the network.
  - C. Issue a service pack to ensure the service is current with all available patches
  - D. Issue a patch to ensure the service has a lower level of risk if compromised
  
8. Which of the following allows a company to correct security issues within their software?
  - A. Application fuzzing
  - B. Cross-site scripting
  - C. Configuration baseline
  - D. Patch management
  
9. Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?
  - A. Error and exception handling
  - B. Application hardening
  - C. Application patch management
  - D. Cross-site script prevention

10. Which of the following should be performed if a smart phone is lost to ensure no data can be retrieved from it?

- A. Device encryption
- B. GPS tracking
- C. Screen lock
- D. Remote wipe

11. Which of the following should be used to help prevent device theft of unused assets?

- E. HSM device
- F. Locking cabinet
- G. Device encryption
- H. GPS tracking

12. Which of the following is true about hardware encryption? (Select TWO).

- A. It must use elliptical curve encryption.
- B. It requires a HSM file system.
- C. It only works when data is not highly fragmented.
- D. It is faster than software encryption.
- E. It is available on computers using TPM.

13. Which of the following is a security vulnerability that can be disabled for mobile device users?

- A. Group policy
- B. Remote wipe
- C. GPS tracking
- D. Pop-up blockers

14. Which of the following BEST describes the function of TPM?

- A. High speed secure removable storage device
- B. Third party certificate trust authority
- C. Hardware chip that stores encryption keys
- D. A trusted OS model

15. A security administrator is implementing a solution that can integrate with an existing server and provide encryption capabilities. Which of the following would meet this requirement?

- A. Mobile device encryption
- B. Full disk encryption
- C. TPM
- D. HSM

16. Which of the following is a security best practice that Jane, a security technician, would implement before placing a new server online?
- A. On-demand computing
  - B. Host software base lining
  - C. Virtualization
  - D. Code review
17. Which of the following software types can Sara, a security technician, use to protect against no malicious but irritating malware?
- A. Pop-up blockers
  - B. Antivirus
  - C. Host-based firewalls
  - D. Anti-spy ware
18. Which of the following is the MOST thorough way to discover software vulnerabilities after its release?
- A. Baseline reporting
  - B. Design review
  - C. Code review
  - D. Fuzzing
19. Which of the following BEST explains the security benefit of a standardized server image?
- A. All current security updates for the operating system will have already been applied.
  - B. Mandated security configurations have been made to the operating system.
  - C. Anti-virus software will be installed and current.
  - D. Operating system license use is easier to track.
20. Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?
- A. Warm site
  - B. Load balancing
  - C. Clustering
  - D. RAID

## References

- Ciampa, Mark. (2009). *CompTIA Security+ 2008 In Depth*. Boston: Course Technology, Cengage Learning.
- Dulaney, Emmett. (2009). *CompTIA Security+ Deluxe Student Guide (Exam SY0-201)*. Indianapolis: Wiley Publishing, Inc. *Note: Verbiage from this text was extensively used in this student guide.*
- Harris, Shon. (2007). *CISSP Certification All-in-One Exam Guide, Fourth Edition*. New York: McGraw-Hill Osborne Media.
- Houser, T., O'Boyle, H., Kayne, I., Hebert, A. (2003). *InsideScoop to CompTIA Security+ Certification, Examination SY0-101, Second Edition*. Friendswood, Tx.: TotalRecall Publications, Inc.
- NETg. (2006) *Security+ Certification Student Manual, CompTIA Press Edition*. Boston: NETg, Thomas Learning.
- NIST. (November 26, 2001) *FIPS Publication 197, Announcing the Advanced Encryption Standard*. Retrieved from <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.