Cyber Security Branch

Security+ Review Course

SY0-501v6

This page is left intentionally blank for printing purposes

Overview

The skills and knowledge measured by the CompTIA Security+ examination was 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 milestone 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+ (2014 Edition) exams are based on these objectives.

CompTIA Security+ Certification Domains % of Exam*

CompTIA SY0-501 Domain	% 0f Examination
Threats, Attacks and Vulnerabilities	21%
Technologies and Tools	22%
Architecture and Design	15%
Identity and Access Management	16%
Risk Management	14%
Cryptography and PKI	12%
Total	100%

* 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

Overview 3
Domain – Cryptography 7
General Concepts 7
Key Management 8
Cryptographic Security Goals 9
Security by obscurity 9
Ciphers 10
Key Exchange 11
Hashing Algorithms 13
Symmetric Cryptography 15
Cipher Modes 16
Asymmetric Cryptography 18
Digital Signatures 21
Public Key Infrastructure (PKI) 22
Key Recovery 25
Certificate Types 27
Certificate Encodings 29
Domain – Identity and Access Management 30
Access Control Concepts 30
Identification 30
Authentication 31
Mutual Authentication 35
Strong Authentication 35
Multifactor Authentication 35
Single Sign-On (SSO) 36
Transitive Trust 36
Federations 37
Access Control Models 37
File System Access Control 39
Authentication Protocols 40
Remote Access Control Authentication Protocols 42
Enterprise Access Control Protocols 44
Web-based Access Control Protocols 46
Account Management 48
Account Types 49
Domain – Technology and Tools 51
Network Security Zones 51
Network Frame Management 53
Network Gateway Management 56
Wireless Architecture 59
Wireless Authentication 62

Wireless Encryption 63
Mobile Devices 65
Resolving Network Resources 70
Network Filtering 73
Tunneling 77
Remote Administration 85
Transport Encryption 86
Email 88
Telephony 89
Domain – Threats, Attacks, and Vulnerabilities 92
Threat Actors 92
Social Engineering 93
Malware 97
Network Attacks 101
Password Attacks 108
Wireless Attacks 110
Application Attacks 112
Domain – Architecture and Design 118
IT Governance Frameworks 118
Security Model 122
Security Control Categories 122
Security Control Types 123
Software Development 125
Secure System Design 130
Implementation Environments 136
Resiliency 137
Data Backups 138
RAID 139
Host Architecture 140
Provisioning 142
Virtualization 143
Cloud Computing 146
Physical Security 149
Domain – Risk Management 152
Risk Management 152
Business Continuity 156
Data Handling 158
Security Monitoring 161
Vulnerability Assessment 168
Command Line 173
Incident Response 175
Computer Forensics 176
Appendix A – Networking Models 178
OSI Model 178

Comparison of OSI model and TCP/IP model 178
Appendix B – IPv4 179
Public classes 179
Private classes 179
Appendix C – IPv6 180
Appendix D – Subnetting Example 181
Appendix E – Common Port Numbers 182
Appendix F – Algorithms 184
Index 186

Domain – Cryptography

CompTIA SY0-501 domain objectives covered:

- CompTIA domain 6.1: Compare and contrast basic concepts of cryptography
- CompTIA domain 6.2: Explain cryptography algorithms and their basic characteristics
- CompTIA domain 6.4: Given a scenario, implement public key infrastructure

---

General Concepts

Algorithm:
An algorithm is defined as a series of steps/processes/formulas that are followed to transform data from one state to another state (such as from a state of plaintext to a state of ciphertext).

Algorithms can be proprietary or open-source. Proprietary algorithms are developed internally within the organization and used only by the organization. They are considered secret algorithms. Open-source algorithms are built upon international standards such as RFCs or ISOs and are considered to be more thoroughly vetted.

Choosing legacy algorithms (known to be weak or have been deprecated) increases the risk to data. Weak or deprecated algorithms increase the likelihood the confidentiality, integrity, or availability of the data will be compromised. The compromise can occur at any of the three data states: data-at-rest, data-in-transit, or data-in-use. Examples of legacy cryptographic algorithms are: MD5 (hashing) and DES (symmetric).

Plaintext or clear text:
Information that is transferred or stored without cryptographic protections

Ciphertext:
The result when encryption is performed on plaintext data using an algorithm.

Pseudo-random number generator (PRNG)
A PRNG is a program or function that can produce an arbitrary number used for a myriad of purposes such as strengthening encryption or authentication.

Initialization Vector (IV):
An arbitrary value created by a random/pseudo-random number generator that is used with plaintext data, encryption keys, or ciphertext before the encryption process is finalized. They are not encrypted when being sent to the destination network node.

Randomization is crucial for encryption schemes to achieve security and to prevent repetition in the encryption process. The IV helps remove the patterns in the ciphertext that would have been created if multiple instances of the same word were encrypted with the same key. They are used in both stream and block ciphers to remove patterns that would otherwise be created by continuously encrypting packets with the same encryption key.

Other terms that are similar, or sometimes used interchangeably, are nonce and salt:

- An IV is used in cryptographic block and stream ciphers. Ideally, it is random and non-predictable.
- A nonce is a "number used once" and is often used with network-based authentication protocols. A nonce could be a sequentially generated number.
- Salt is an arbitrary number that is commonly appended to a password before it is encrypted to create the password hash. This could also be used for key stretching.

Key Management

Ephemeral key:
A temporary key used for the current conversation and is discarded when the conversation is completed. It is implied that an ephemeral key has a short life-span. Ideally, a session key is an example of an ephemeral key.

Key space:
Key space is the range of values that can be used to create a crypto variable.

- AES can use a key size of 128 bits, which means the cryptosystem has up to 2^{128} ways to rearrange the binary bits to create a session key from.
- A password can be chosen from upper-case letters, lower-case letters, numbers, and certain special characters.

Key strength:
Generically speaking, the size of an encryption key is directly proportional to its ability to resist a brute-force attack. For example, a key size of 128 bits would require a brute-force attack to iterate through 2^{128} possibilities in order to have a 100% chance of discovering the key.

A larger key size provides a more effective deterrent solution against attack because it would present a greater work factor to the attacker.

Key stretching:
Key stretching protocols lengthen a security variable such as an encryption key or a password to make it more resistant to attack.

- PBKDF2 (Password-Based Key Derivation Function 2): used in Cisco devices to protect the password
- bcrypt(): a key stretching protocol used by Linux and UNIX to "salt" the password before encrypting it with Blowfish. It is then stored in the "shadow" file.

Key stretching techniques can be helpful when trying to harden legacy systems.

Cryptographic Security Goals

Cryptography can provide up to four security services:

1. **Confidentiality**
   Ensuring only authorized parties can read the data. Encryption is used to protect the secrecy of information from unauthorized individuals.
2. **Integrity**
   Verifying the data has not been altered in some undesirable way. Hashing algorithms can be used to ensure information has not been modified in transit or while stored on the hard drive.
3. **Authentication**
   Process of verifying that the source is who they say they are. The digital signature, encrypted tokens, and password hashes can provide authentication.
4. **Non-repudiation**
   Prevents one party from denying actions they carried out. Encrypting with the asymmetric private key supports non-repudiation. Symmetric encryption is not capable of supporting non-repudiation.

Security by obscurity

Steganography

Steganography is the technique of hiding, concealing, or embedding a message within some other data object. Besides the sender and the intended recipient, no one else *suspects* the existence of the message.

In the case of graphics, steganography would use the least significant bit(s) of a pixel to hide data without the difference being detectable to the human eye. The Greek word *steganos* means *"covered, or hidden"*; *graphein*, "to write". It provides a weaker form of confidentiality when compared to capabilities of cryptography.

- Also known as Least Significant Bit (LSB) software
- Cryptography could be used before steganography in support of defense in depth.

Where is it used?

- Covert Channel (File Forking, Alternate Data Streams)
- Digital Rights Management (DRM)
  - Electronic Watermarking or Digital Watermarking
- Metadata (digital camera pictures)

Common steganography tools: S-Tools, Steghide, StegoShare

Obfuscation

Obfuscation is a technique that camouflages the computer code or data in such a way so that its meaning isn't obvious to the casual observer. It is an example of security by obscurity.

Examples of obfuscation:

- Encoding human readable ASCII characters displayed in the web browser's address bar as Base64 or Base16 (Hexadecimal) characters instead.
- Using Exclusive-OR (XOR) logic on data to help disguise the data.
- Encoding data with the ROT13 shift cipher

Exclusive-OR (XOR) Operation

XOR is a binary mathematical operation that compares two bits to produce a binary output. It is commonly used in cryptography and parity checking.

- Plaintext is XORed with a random keystream to generate ciphertext
  - If values are same, result is 0
  - If values are different, result is 1

  Truth Table:

Converted Plaintext	0101 0001
Keystream	0111 0011
Output of XOR	0010 0010

Ciphers

Substitution Cipher

A substitution cipher changes one character or symbol into another character or symbol throughout the entire message. Each character keeps its position in the message but cryptographically changes its identity.

- Substitution ciphers support the cryptographic goal of confusion: masking the relationship between a plaintext character and the encryption key.
- Substitution ciphers include shift ciphers, mono-alphabetic ciphers, or polyalphabetic ciphers.
  - A shift cipher merely shifts the alphabet so that the message is disguised.
  - ROT13 shift cipher example:

Plain text:	`the time to attack is now`
Cipher:	`GUR GVZR GB NGGNPX VF ABJ`

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	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Transposition

A transposition cipher changes the positions of plaintext letters within a sentence. 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.

- Transpositions ciphers support the cryptographic goal of diffusion: breaking up patterns in the plaintext so they won't be noticeable in the ciphertext.
- Example:

  Plain-text: the time to attack is now
  Cipher-text: wonsikcattaotemiteht

Stream Cipher
A stream cipher is a method of encrypting data with a cryptographic key and an algorithm to each binary digit in a data stream, either one bit at a time or one byte at a time. Stream ciphers are often used for their speed and simplicity or in applications where plaintext comes in quantities of unknowable length (for example, a secure wireless connection).

- Requires little to no resources:
  - Minimal processing needs
  - Minimal memory needs
  - Less power consumption
  - Lower latency issues: uses fast mathematical operations
- More aptly suited to support smaller devices.
- Example: RC4

Block Cipher
A block cipher is a method of encrypting data with a cryptographic key and an algorithm to a block of data at once as a group, rather than to one bit at a time. The block of data might be 64 bits (as in DES) or 128 bits (as in AES).

- Considered to be naturally stronger than stream ciphers
- Requires more resources than stream ciphers
- More aptly suited for operating systems and large devices with sufficient memory capacity, processing power, and abundant electrical power.
- Example: AES

Key Exchange

In-band exchange
In-band key exchange performs the exchange within the same communication channel. This method is more susceptible to eavesdropping and other man-in-the-middle issues because the data, exchanged parameters, and keys are all captured from one source.

Out-of-band exchange
Out-of-band key exchange performs the exchange of parameters or keys in a separate communication channel or with an alternative technology. This is generally considered to be a more secure method to exchange secrets because the alternate method is less likely to be monitored by the attacker. This method borrows from the concept of security by obscurity.

Examples:

- Sending a PIN via text message or email that is then typed into a web browser text field
- Asymmetric encrypion exchanging a symmetric session key (hybrid cryptography)
- Physical means (trusted courier, United States Postal System)

Rivest, Shamir, Adleman (RSA) key exchange method
The RSA key exchange method uses the same server RSA public key not only for identifying the website, but also for encrypting and then exchanging the session key between the client and the server. This method keeps reusing the same public key which becomes a static key security issue. This method does not support the concept of Perfect Forward Secrecy.

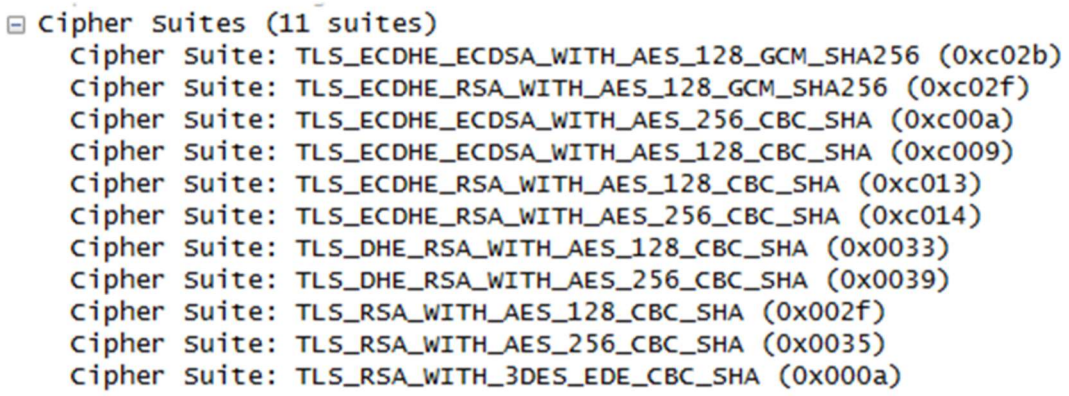
Diffie-Hellman Ephemeral (DHE) key exchange method
The DHE key exchange method uses Diffie-Hellman for key agreement between a client and a server by exchanging parameters used within discrete logarithms. This protocol supports Perfect Forward Secrecy because the key agreement parameters aren't linked to the server's asymmetric keys and are destroyed when the session has ended.

DHE needs to use larger bit sizes (greater than 2048 bits) in order to be considered secure enough in today's computing world. The larger bit sizes can overwhelm the processor of a busy server making the server sluggish.

Elliptical Curve Diffie-Hellman Ephemeral (ECDHE) key exchange method
The ECDHE key exchange method uses Diffie-Hellman for agreeing upon a key by exchanging points along an agreed upon elliptical curve. This protocol typically uses ECC asymmetric public and private keys that can be generated within the session and can't be used independently from the server's asymmetric key that was used for website identification.

Of the three key exchange protocols, the ECDHE key exchange protocol does the best job of supporting Perfect Forward Secrecy. The key agreement parameters aren't linked to the server's public key and ECC keys are more processor friendly because of their smaller key sizes without losing key strength.

Cipher Suite
A cipher suite is a named combination of authentication, encryption, message authentication code (MAC) and key exchange algorithms used to negotiate the security settings for a network connection using Transport Layer Security (TLS), Secure Sockets Layer (SSL), Secure Shell (SSH), or some other secure networking protocol.



Hashing Algorithms

Hashing refers to performing a calculation on a message and converting it into a numeric hash value. Its primary goal is to establish integrity of a message.

- Algorithm that takes a variable-length input and generates fixed-length ciphertext
- The algorithm is public domain
- One-way encryption function
    - Encryption is performed to create the ciphertext that becomes the baseline, but decryption does not occur
    - There aren't any keys used with hashing algorithms, so decryption is not possible
- Cryptographic services supported:
    - Ensures data integrity
        - Used to create cryptographic checksums or message digests
    - Authentication
        - Password hashes

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 message. If they do not match, the data has been altered and is discarded.

A hashing collision occurs when two different sets of plaintext data, ran through the same hash function, create the same hash value. Once a collision has been discovered in a hashing algorithm, the algorithm should no longer be used. MD4, MD5, and SHA-1 are good examples of hashing algorithms with documented collisions.

MD5 Hashing 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

Common Hashing Functions

Name	Digets Size(s)	Known Collisions
MD5	**128 bits**	**Yes**
SHA (SHA-1)	**160 bits**	**Yes**
SHA-2		
SHA-224	**224 bits**	**No**
SHA-256	**256 bits**	**No**
SHA-384	**384 bits**	**No**
SHA-512	**512 bits**	**No**
SHA-3		
SHA-224	**224 bits**	**No**
SHA-256	**256 bits**	**No**
SHA-384	**384 bits**	**No**
SHA-512	**512 bits**	**No**
RIPEMD-160	**128, 160, 256, and 320 bits**	**Yes (128 bits)**
HAVAL	**128, 160, 192, 224, and 256 bits**	**Yes (128 bits)**
Whirlpool	**512 bits**	**No**

Message Authentication Code (MAC)
The purpose of a MAC is to authenticate both the source of a message and the integrity of a message without the use of any additional mechanisms. Unlike digital signatures, MACs are computed and verified with the same secret key, so they can only be verified by the intended recipient.

Cryptographic services provided:

- Data Integrity
- Data Origin

Hashed MAC (HMAC)
HMAC is a type of message authentication code (MAC) calculated using a specific 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 origin of a message.

Any 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 accordingly.

- 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, TLS, and SSH

Symmetric Cryptography

Symmetric algorithms require both ends of an encrypted message to have the same key and same 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.

- Uses the same key to encrypt and also decrypt the data
- Both parties share a copy of the same key
- Must use "out-of-band" key distribution
- Best suited for bulk encryption; much faster (smaller key size) than asymmetric cryptography
- a.k.a. Session Key, Secret Key, Shared Key, Same Key, Single Key, Conventional Key, Master Key

The disclosure of a symmetric key breaches the security of the encryption system. If a key is lost or stolen, the entire cryptosystem is breached.

Advantages:

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

Disadvantages

- Key distribution issue: how to exchange the keys to all necessary parties securely
- 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
- Is there trust between parties sharing the key?
- Lacks "non-repudiation"

Symmetric Algorithms:

Algorithm	**Key Size(s)**	**Block Size**
Data Encryption Standard (DES) Triple Data Encryption Standard (3DES)	*56 bits *168 bits	64 bits
International Data Encryption Algorithm (IDEA)	128 bits	64 bits
Blowfish	32 – 448 bits	64 bits
Carlisle Adams and Stafford Tavares (CAST) CAST-128 CAST-256	 40 – 128 bits 128, 160, 192, 224, 256 bits	 64 bits 128 bits
Advanced Encryption Standard (AES)	128, 192, 256 bits	128 bits
Twofish	128, 192, 256 bits	128 bits
Serpent	128, 192, 256 bits	128 bits
Rivest Cipher 6 (RC6)	8 – 2048 bits	128 bits
Rivest Cipher 4 (RC4)	8 – 2048 bits	stream

*Note: DES and 3DES create a 64-bit key, however only 56 bits are used for encryption. The remaining 8 bits were to be used for parity bits. At any single iteration of encryption, the algorithms are working with a 56-bit key. NIST has determined that 3DES has an overall, effective key strength of approximately 80 bits. Both algorithms are considered weak by today's standards and should be avoided if possible.

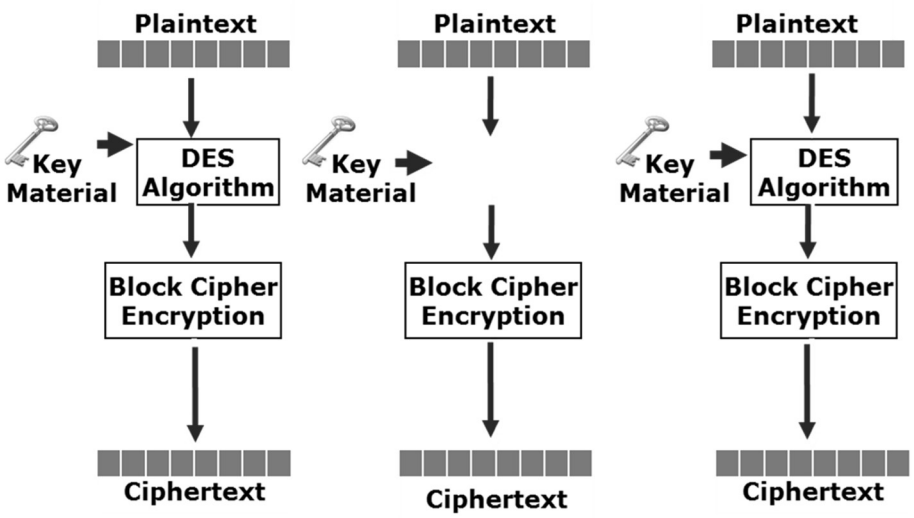
Cipher Modes

Cipher modes of operation provide an organized means of managing encryption keys, IVs, and the plaintext data as the block cipher performs multiple rounds of encryption.

Cipher Mode	Behavior	Errors	IV Used
Electronic Code Book (ECB)	block	N	N
Cipher Block Chaining (CBC)	block	Y	Y
Counter Mode (CTM)	stream	N	Y
Galois Counter Mode (GCM)	stream	N	Y

Electronic Code Book (ECB)

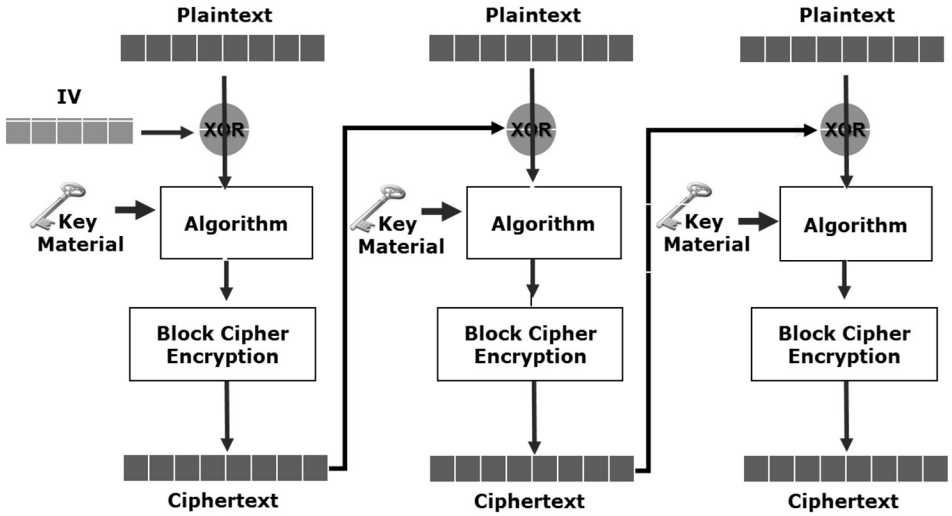
ECB mode is fast and simple, but there isn't an IV used so large messages would have patterns in the ciphertext. Identical plaintext messages would be encrypted with the identical encryption key causing identical ciphertext to be created. It behaves as a traditional block cipher.



ECB should only be used on very small plaintext data such as PINs, encryption keys, or within challenge-response authentication systems.

Cipher Block Chaining (CBC)

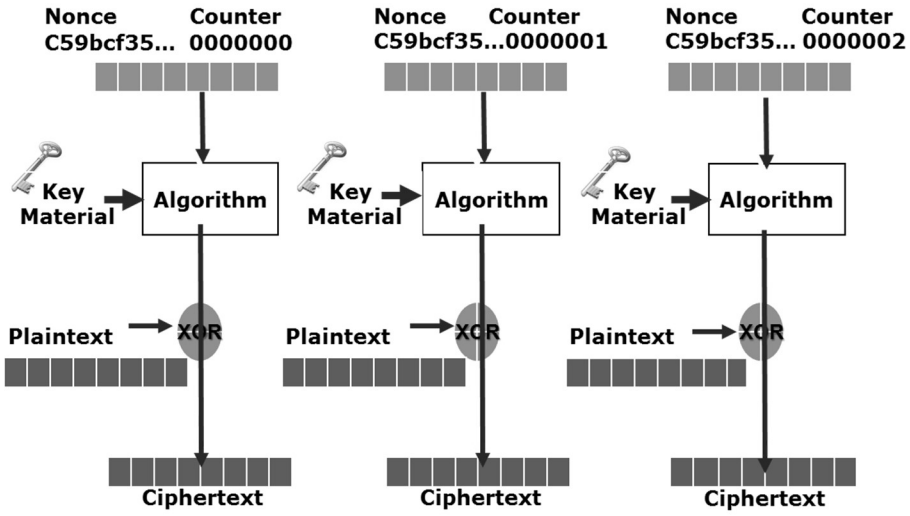
CBC is the most common cipher mode implanted in today's cryptosystems. It is used to encrypt anything from files to wireless frames to hard drives.



An IV is applied to the block of plaintext data so that when the key is used over again, the same ciphertext would not be created. After the initial round of encryption, the previous round's ciphertext becomes the IV for the next round of encryption. CBC requires that the sender and receiver both know the IV so it becomes exchanged during the handshaking process of the cryptosystem.

Counter Mode (CTM)

CTM does not using any kind of chaining technique so the recipient can begin decrypting the received packets without having to wait for the entire message be encrypted by the sender. It is commonly used with streaming communication transmissions such as with IEEE 802.11i, IPsec, and Asynchronous Transfer Mode (ATM) network links. Also, the blocks of plaintext can be encrypted in parallel so that throughput can be increased.



CTM uses an IV called a nonce, but each iteration has a counter incremented to the IV.

Galois Counter Mode (GCM)

GCM is based upon Counter Mode but specifies a 128-bit block cipher is to be used. It is specifically designed to be used with AES. The minimum encryption key size is 128 bits.

GCM can be used to create a Galois Message Authentication Code (GMAC). Besides supporting packet proof of origin and packet integrity, it can provide confidentiality as well. It is used by the IPsec protocol, ESP, and later versions of TLS.

Asymmetric Cryptography

Asymmetric cryptography is also called Public Key Cryptography (PKC). It uses two keys; one to encrypt with and then the other to decrypt with. These asymmetric keys are referred to as the

public key and the private key. 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 its owner.

- Based on mathematical number theory
    - Uses either large prime numbers, discrete logarithms, or elliptical curve mathematics
- 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

The Receiver's public key can be used by the sender to encrypt a message, and the Receiver's private key can be used by the receiver to decrypt the message. This supports confidentiality of the message. If someone wants to send you an encrypted message, they can use your public key to encrypt the message and then send you the encrypted message. You can use your private key to decrypt the message. If both keys become available to a third party, the encryption system will not protect the privacy of the message.

Alternatively, you can encrypt the message with your private key and the receiver can decrypt the message using your public key. Though encryption is being used, confidentiality is not supported because anyone can have access to the public key and decrypt the message. This method is used for digitally signing an object, such as an email. Encrypting with your asymmetric private key supports authentication, integrity, and non-repudiation.

Advantages

- More simplified key management (n*2)
- Public key can be freely distributed
- Offers: Digital signatures, integrity checks, secure key exchange, and non-repudiation

Disadvantages

- Typically, 100 to 1000 times slower than symmetric key algorithms
- The encrypted message increases in size which can affect availability of resources such as processing throughput, network throughput, and storage capacity

---

Asymmetric Algorithms

Diffie-Hellman

Dr. Whitfield Diffie and Dr. Martin Hellman designed the Diffie-Hellman key exchange algorithm in 1976. It provides a means to share a secret over an unsecured communication channel. The various cryptographic technologies traditionally use Diffie-Hellman during the early stages of creating a session, called the handshake phase.

- First public domain asymmetric algorithm
- Provides secure Key Exchange
    - Based on the difficulty of computing discrete logarithms
- Works with variable key lengths
    - 512-bit to arbitrarily long
    - Exchange of keys that are 2048 bits or greater are considered secure

This algorithm is used primarily for two parties to clandestinely agree on what key (secret) will be used between the two of them. The algorithm does not create any keys itself, but moreover provides the means to agree upon a key.

1. Alice and Robert agree on a Prime Number, p = 7 and a Base Number, b = 5
2. Alice chooses a secret number, a = 14
3. Robert chooses a secret number, r = 6
4. Alice sends Robert: $(b^a \bmod p) = (5^{14} \bmod 7) = (6103515625 \bmod 7) = 4$
5. Robert sends Alice: $(b^r \bmod p) = (5^6 \bmod 7) = (15625 \bmod 7) = 1$
6. Alice computes: $(1^a \bmod p) = 1^{14} \bmod 7) = (1 \bmod 7) = 1$
7. Robert computes: $(4^r \bmod p) = (4^6 \bmod 7) = (4096 \bmod 7) = 1$

Alice and Robert clandestinely agree on a secret ("1").

It is commonly used by hybrid encryption protocols such as IPsec, TLS, and SSH during the handshake phase. ECDHE uses Diffie-Hellman with ECC and is considered to be a more secure way of exchanging keys because of its ability to properly support perfect forward secrecy.

Diffie-Hellman Groups

DH groups are agreement packages that set the size of the secret number chosen during the Diffie-Hellman process. It also determines whether ECC will be used. A larger key size would need to be supported by a DH Group with a higher bit size. Generally speaking, the higher the group number, the more secure it is considered to be.

Example DH Groups:

- Diffie-Hellman Group 2: 1024-bit group
- Diffie-Hellman Group 5: 1536-bit group
- Diffie-Hellman Group 14: 2048-bit group
- Diffie-Hellman Group 15: 3072-bit group
- Diffie-Hellman Group 19: 256-bit elliptic curve group
- Diffie-Hellman Group 20: 384-bit elliptic curve group
- Diffie-Hellman Group 21: 521-bit elliptic curve group
- Diffie-Hellman Group 24: 2048-bit, 256-bit subgroup

Rivest, Shamir, Adleman (RSA)

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 prime numbers that are computationally difficult to factor as the basis of its structure. It is widely implemented, and it had become a de facto standard. RSA is used in the vast majority of cryptographic environments, such as SSL and TLS.

- Provides encryption, digital signature, and key exchange services
- The most common asymmetric algorithm used on the internet
    - Used by various technologies (HTTPS, SSH, PGP, etc.) to handle asymmetric confidentiality
- Based on the difficulty of factoring N, a product of two large prime numbers
- Variable Block and Key length
    - Key sizes range from 512 – 4096 bits (greater than 2048 bits considered secure)

RSA was the first algorithm known to be suitable for signing as well as encryption. It is strong when using large key sizes, 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.

Elliptic Curve Cryptography (ECC)

Elliptical Curve Cryptography (ECC) provides similar functionality to RSA. ECC was originally implemented in smaller, less-intelligent devices such as cell phones and wireless devices but has become more and more common. It uses smaller keys than RSA (yet retains the same level of strength) and requires less computing power.

- Provides encryption, digital signature, and key exchange services
- Based on the idea of using points on a curve to define the public/private key
    - 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

The digital signature is the electronic version of a person's paycheck signature. Its presence indicates a person's acknowledgement and approval of an act carried out by that person (such as sending an email).

Three items are used to create the digital signature and the cryptographic service supported:

- Data (such as an e-mail message)
- Hashing Algorithm [supports integrity]
- Asymmetric Private Key [supports authentication and nonrepudiation]

Digital Signature Standard (DSS)
DSS is the NIST standard that defines how DSA is to be used. It is defined by FIPS 186-4.

Digital Signature Algorithm (DSA)
DSA was created by NIST. It uses a SHA or SHA-2 hashing algorithm in conjunction with an asymmetric private key to create a digital signature of a message. It can use RSA or ECC asymmetric keys (ECDSA specifically uses ECC keys).

- Provides integrity, authentication, and non-repudiation
- Does not provide confidentiality
- Faster at verifying signatures than RSA alone

DSA has two goals:

1. Assures the recipient that the message truly came from the claimed sender
2. Assures the recipient that the message was not tampered with

Digital signature process example:

The Sender:

1. Creates the message
2. Hashes the message to create the hash / message digest
3. Uses the sender's asymmetric private key to encrypt the hash
4. The encrypted hash becomes the digital signature and is sent with the message to the recipient (message itself is in plaintext)

Note: 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:

1. Hashes the received message
2. Uses the sender's public key to decrypt the encrypted hash that was sent with the message
3. The two hashes are compared. If the hashes match, then the received message is valid and the sender is verified

---

Public Key Infrastructure (PKI)

PKI is a centralized system for provisioning, storing and deprovisioning asymmetric keys. It comprises one or more Certificate Authority (CA) servers that create asymmetric private and public keys. The CA server also digitally signs the asymmetric public key, transforming it into an X.509 digital certificate. The need for universal systems to support e-commerce, secure transactions, and information privacy are some of the issues addressed by PKI.

- A framework for creating, managing, issuing, distributing, and storing asymmetric private keys and X.509 Digital Certificates

- Utilizes the hierarchical trust model amongst the CA servers
- PKI is designed to be scalable so the infrastructure can be expanded without added complexity
- Establishes who is responsible for authenticating the identity of the owners of the digital certificates
- Establishes a means for key destruction and certificate revocation

PKI allows two separate parties that are foreign to each other to securely exchange a message. It is the core infrastructure of ecommerce. The Public Key is used for encryption and the Private Key is used for decryption in order to support confidentiality.

Certificate Authority (CA)
The CA is responsible for issuing, revoking, and distributing certificates. Each user of a PKI system has a certificate that can be used to verify their authenticity.

- Manages certificate store
    - Creates, signs, distributes, stores, and/or revokes keys
- Authenticates the certificates it issues by signing them with their asymmetric private key
- CA server architecture is typically deployed within a Single Authority trust model or a hierarchical trust model

The CA server is a critical component of PKI and must always maintain its trustworthiness. A CA might be kept offline to help minimize the chances of it becoming compromised. However, when high availability is needed, then the CA server would be kept online.

Trusted Root Certificate Authority (CA)
A trusted root CA is a CA server that creates its own asymmetric keys and digitally signs its own public keys. It uses self-signed certificates. There is only one root CA in a single PKI domain.

The root CA also creates keys for the intermediate CA server(s) and digitally signs their public keys. The intermediate CA creates keys and digitally signs the public key for the lower leaf objects. This establishes a certificate chain of trust between the digital certificates of the CA servers and the leaf objects.

- The root CA is the "root" of the hierarchical trust model
    - Creates and signs keys for **itself**
    - Creates and signs keys for **intermediate CA(s)**
    - Intermediate CA signs for leaf objects (end users, production servers, etc)
    - Example certificate chain of trust:
        - Root CA-1 ← intermediate CA-14 ← web server
          (trust) (trust)

The root CA may or may not be kept offline. However, it would be very rare for the intermediate CA to be kept offline.

Digital Certificates
Standardizing the certificate format is important to assure system interoperability in a certificate-oriented environment. Without standardization cross-certification would not be possible.

- Defines the formats and fields for public keys
- Defines procedures for distributing public keys

Pretty Good Privacy (PGP) / GNU Privacy Guard (GPG)
PGP / GPG cryptosystem software has its own digital certificate format that is incompatible with X.509. Asymmetric keys are created by the client's software and the asymmetric public key is digitally signed by one or more peers. PGP is popular for encrypting email.

- More likely to use a web-of-trust or a Peer-to-Peer (P2P) trust model
- Decentralized key management
- Asymmetric public key is digitally signed by many peers

X.509
The most popular certificate used is X.509 version 3. The X.509 standard is a certificate format developed by the International Telecommunications Union (ITU) and supported by many other standards bodies (such as ANSI, IETF, and multiple RFCs).

- Hierarchical trust model
- Centralized key management

A typical X.509 digital certificate contains the following:

- The Distinguished Name (DN) of the owner (subject) of the certificate
- The subject's public key
- The CA's Distinguished Name (DN)
- The CA's digital signature
- Periodicity: valid from when to when
- Certificate policy: how the certificate can be used
    - Object Identifiers (OID): numerical extensions that define the purpose(s) of the digital certificate

        Examples:

Smart card logon	1.3.6.1.4.1.311.20.2.2
Encrypting File System	1.3.6.1.4.1.311.10.3.4
Client authentication	1.3.6.1.5.5.7.3.2
Secure email	1.3.6.1.5.5.7.3.4
- Serial number

Certificate Signing Request (CSR)
The formal request sent from a client to a CA asking for a certificate to be generated.

- Identifying information about the client must be included, such as:
    - Driver's License
    - Social Security Number

    - Phone number
- The CSR would include:
    - Client's digital signature
    - Public Key to be signed
    - Distinguished Name
    - Business Name
    - Email Address
    - Location information

Key Recovery

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.

Key Escrow

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.

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

Recovery Agent

Someone within the organization with the authority to interact with keys stored within a key repository

M of N Control

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 single individual could compromise the security system.

- 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

---

Certificate Revocation List (CRL)

The CRL is maintained by the CA that created the digital certificate. It is a .crl file stored by the CA and can be queried manually (very time consuming) or queried using Online Certificate Status Protocol (OCSP).

Certificate revocation is the process of revoking a certificate before it expires. Examples why a certificate would be revoked:

- Key theft or loss

- Personnel termination due to illegal activity or company policy infringement
- Significant changes to the organizational business structure such as selling portions of the company (business splintering) or company mergers

Digital certificates are not revoked due to normal expiration. Once a certificate has been revoked, it is permanent and can never be used again.

Different from revocation, a digital certificate can also be suspended, or put "on hold". Usually this would be done because personnel will be away from the company for an extended period of time, such as a mandatory vacation or maternity / paternity leave. A suspended certificate is temporary and can be unsuspended.

Online Certificate Status Protocol (OCSP)
OCSP allows a client to query the CA server that issued the server's digital certificate. Using OCSP, the CA server would check its CRL for the digital certificate's serial number and then send an OCSP response to the requesting entity.

There are three specific OCSP response types:
- "Good": the digital certificate has not been revoked
- "Revoked": the digital certificate has been revoked
- "Unknown": the digital certificate has been suspended or placed "on hold"

OCSP is traditionally used between a web client and an intermediate CA to check the web server's digital certificate's revocation status.

OCSP Stapling
OCSP stapling helps offload some of the burden that a CA server might experience as clients navigate to a high traffic web server. With stapling, instead of the web client sending an OCSP query to the CA server, the web server in advance queries the CA server and caches the digitally-signed OCSP response with its own server-side digital certificate.

With each client receiving the "stapled" OCSP response from the web server instead of the CA server, the CA server isn't overwhelmed with OCSP queries.

Key Pinning
Key pinning is an administrative technique that forces the client to accept the server's certificate as valid. OCSP queries are not performed.
- Static pinning: high traffic sites or internal sites have their digital certificates administratively cached inside the client software so that the certificate being delivered to the client naturally matches and is deemed valid

- Dynamic pinning: client stores the server's public key the first time they interact. Any sessions in the future, the server public key cached inside the client is used to validate that session. This technique mitigates forged certificate attacks.
    - If the public keys match then domain validation is successful
    - Uses the concept of "Trust on First Use"
    - HTTP Public Key Pinning (HPKP) protocol

Key pinning could be as simple as creating an exception within the web browser to accept the certificate as valid no matter what. This technique is not recommended, however.

Certificate Types

Certificates can serve specific niches:

Root certificate
A root certificate is a public key that the root CA created for itself and digitally signed itself. Its purpose is to validate certificates belonging to itself and its intermediate CAs. They are usually preloaded inside of web browsers and operating systems.

- Self-signed certificate
- The "root" of a certificate chain
- Usually created with a longer key lifetime
- Usually created with a bigger key length

User certificate
The user certificate has been created and mapped to a specific user account. It can be used to validate digital signatures that have been created by the user. They are commonly stored on smart cards and can be used for certificate-based authentication.

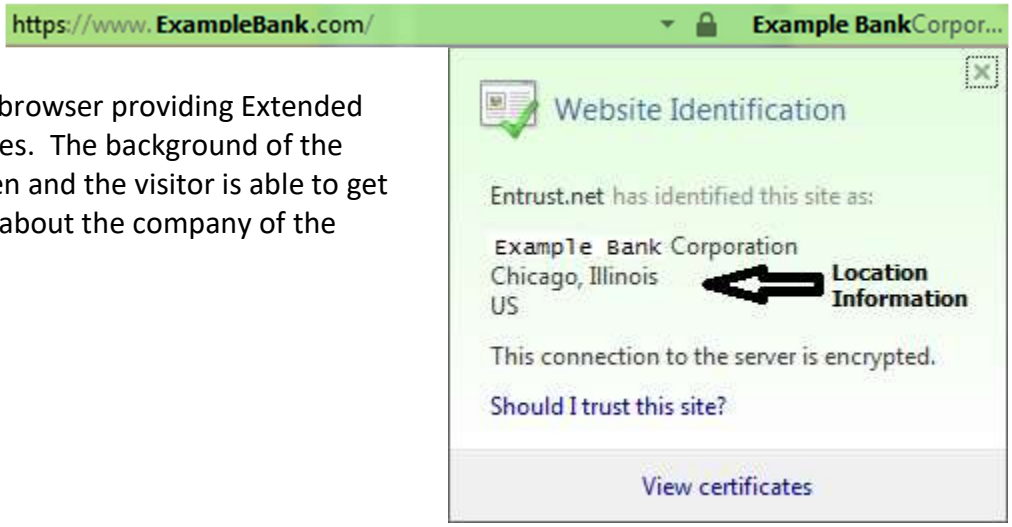
Machine certificate
The machine certificate is created and mapped to a specific computer, especially servers. In the case of a web server, it is used for domain validation. The Distinguished Name (DN) recorded in the certificate must match the website name.

Limited purpose certificate
The limited purpose certificate is created to serve a single purpose or a minimal few purposes by setting specific Object Identifiers to "critical". This method is often used within a multiple key pair environment, in which each individual set of asymmetric public and private keys serve specific niches. For example, one set of asymmetric public and private key pair is used for digitally signing documents but a different set of asymmetric public and private keys are used for encryption in support of confidentiality. This helps limit the damage that is caused by a compromised key.

Extended Validation (EV) certificate

The Extended Validation (EV) certificate has gone through a much more rigorous identity vetting process before the CA created the digital certificate. EV certificates are commonly used by the websites of financial firms, such as banks. Typically, a web browser signifies the website is using an EV certificate by having a color-coded differentiated (usually green) address bar. Also, the visitor of the website can view more information about the attributes of the company, such as location information.

Example of a web browser providing Extended Validation attributes. The background of the address bar is green and the visitor is able to get more information about the company of the website.



Multi-domain certificate

- Subject Alternative Name (SAN) extension
  - One certificate that can be used to validate the identity of all domain names owned by a single organization. It contains an extension field that lists the other Fully Qualified Distinguished Names (FQDN).
  - Hypothetical example:
    Certificate Subject Alt Name
    www.usa.gov
    www.DOD.mil
    www.DOT.gov
    www.DOJ.gov
    www.HHS.gov
- Wildcard certificate
  - One certificate that can be used to validate the identity of the parent domain website and any child domain websites. It contains an entry preceded by "*."
  - Hypothetical example: "*.DISA.mil"

  The following child domains could use the certificate:
  army.DISA.mil, af.DISA.mil, navy.DISA.mil, etc

Certificate Encodings

The following are common file extensions associated with digital certificates, asymmetric public and private keys. Each dictate where, how, and what kinds of cryptographic elements can be used.

Canonical Encoding Rules (CER)
CER is defined by ASN.1 and defines the structure of a digital certificate. It requires the digital certificate fields to be encoded as Base64 ASCII strings. These types of certificates are often used by web servers in HTTPS exchanges.

- Base64 ASCII encoded digital certificate
- Popular with web traffic

Distinguished Encoding Rules (DER)
DER is defined by ASN.1 and defines the structure of a digital certificate. It requires the digital certificate fields to be binary encoded. This file extension is commonly used for storing X.509 digital certificates in a data store. Though it can be used for storing and archiving digital certificates, it is not used for storing and archiving asymmetric private keys.

- Binary encoded digital certificate
- Popular with X.509 key storage

Privacy Enhanced Mail (PEM)
PEM is highly associated with the digital certificate format used in email traffic. It requires the digital certificates fields to be Base64 ASCII encoded.

- Base64 ASCII encoded digital certificates

Public Key Cryptography Standard #7 (PKCS #7)
P7B files are digital certificate archives. It is the standard used for validating a digital signature in the email encryption protocol called S/MIME. It is not used for archiving the asymmetric private key however.

- PKCS #7: Cryptographic Message Syntax Standard

Public Key Cryptography Standard #12 (PKCS #12)
P12 files are archive files that contain one or more digital certificates (certificate chain) and the asymmetric private key. The file is password protected using a symmetric algorithm ("conventional encryption"). This standard would be used for transferring asymmetric keys belonging to leaf objects within a PKI environment.

- Archive file that includes the asymmetric private key
- Could include the digital certificate chain (root and intermediate CA digital certificates)

Personal Information Exchange (PFX)
PFX is the file format created by Microsoft and is considered to be the precursor to the P12 format. It still remains popular with Microsoft-based platforms and could be used by Microsoft Office technologies and Microsoft's Encrypting File System (EFS).

- Archive file that includes the asymmetric private key
- Microsoft specific

Domain – Identity and Access Management

CompTIA SY0-501 domain objectives covered:

- CompTIA domain 4.1: Compare and contrast identity and access management concepts
- CompTIA domain 4.2: Given a scenario, install and configure identity and access services
- CompTIA domain 4.3: Given a scenario, implement identity and access management controls
- CompTIA domain 4.4: Given a scenario, differentiate common account management practices

---

Access Control Concepts

Securing system resources begins with identification and then generally follows a three-step process of authentication, authorization, and accounting (AAA). It is commonly referred to as the AAA model.

- Authentication: positive identification of the person or system seeking access
- Authorization: a predetermined, granted level of access to the resource
- Accounting: the use of each resource is monitored, tracked, and/or logged

Identification is often mistakenly forgotten or confused with authentication. It is the claim of who the person is and is represented as the user ID, or something similar. Without established positive identification, other security goals quickly deteriorate.

Identification

Identification is the claim of who we are. However, it is tied to other functions as well. It is the initial security step before authentication can be established.

- Provides group membership association
- Means for tracking in accounting, such as log entries
- Determines resource allocation

User Identification Guidelines

- Uniqueness: must be unique to provide unambiguous identification
- Non-descriptive: should not infer the associated role or job function of the account
- Issuance: must be provisioned in a controlled and documented manner

Most common forms:

- Username, User ID, account number, email address

Authentication

Authentication is the proving of a subject's claim of identification. Authentication must maintain a one-to-one (1:1) relationship between the subject and the authentication component. If the authentication component is shared with another subject, nonrepudiation is lost because the security system would not be able to ascertain which subject had performed the (possibly harmful) action.

Authentication systems utilize one or more authentication factors:

Authentication Types	Examples
Something you know	Password or PIN
Something you have	Smart Card, Token, or Device
Something you are	Fingerprints or Retinal Pattern
Something you do**Error! Bookmark not defined.**	Keystroke Authentication
Somewhere you are**Error! Bookmark not defined.**	Location

Something you know

Authentication based upon "something you know" is also known as "Type 1" authentication. It is the most common, cheapest, and easiest authentication system to implement. And likewise, it is the usually the easiest to compromise.

Authentication examples:

- PIN
- Passphrase
- Password
    - One-time Password (OTP)
        - Password that is good for only one login
        - Dynamic password that changes with each session
    - Strong password: entropy attributes
        - Mixture of upper-case, lower-case, numbers, and special characters in no apparent order

---

Something you have

Authentication based upon "something you have" is also known as "Type 2" authentication. It requires the subject to be in possession of something unique. It is the authentication factor used by token-based authentication systems.

Authentication examples:

- Certificate-based authentication
- Secure token authentication
- Physical access token

Token-based authentication

Some kind of token must be in the possession of the subject for authentication to be established.

Hardware-based versus software-based tokens:

- Hardware-based tokens implement a physical mechanism that can be held and used for authentication
    - Examples: USB dongle, ID card, OTP secure token device
- Software-based tokens implement a chunk of computer bits that can be used for authentication
    - Examples: certificate-based authentication, Kerberos tickets, SAML cookies

Static versus dynamic tokens:

- Static tokens don't change and are provided to the authentication interface as is
    - Vulnerable to rogue interfaces
    - Examples: swipe cards such as ATM cards or proximity cards
- Dynamic tokens provide a modified form of the token with each iteration to the authentication interface
    - Involves encryption and/or salt
    - Effective countermeasure against rogue interfaces
    - Examples: smart cards such as CAC, PIV and other "chip" cards

Synchronous versus asynchronous tokens:

- Synchronous tokens are synchronized with the authentication server so the token being used is already known by the authentication server
    - Examples: Time-based One Time Password (TOTP) devices
- Asynchronous tokens use an algorithm to create the next token
    - Often delivered by an out-of-band communication channel such as email or text
    - Example: Hashed Message Authentication Code One Time Password (HOTP)

Hardware-based token
Dynamic token
Synchronous token (TOTP)

Hardware-based token
Dynamic token
Asynchronous token (HOTP)

Figure 1 Comparing Security Token Attributes

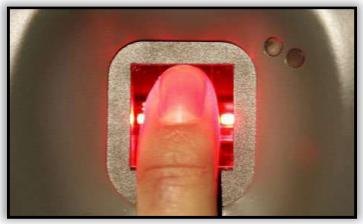
Something you are

Authentication based upon "something you are" is also known as "Type 3" authentication. It uses biometrics and authentication systems that use biometrics are often very expensive.

Biometric-based authentication naturally supports non-repudiation because it is based upon who the individual is. However, Biometric-based authentication suffers from revocation complications. For instance, how would an organization revoke someone's thumbprint if an intruder was able to create or steal the thumbprint? How would the organization create a new, unique thumbprint of the individual?

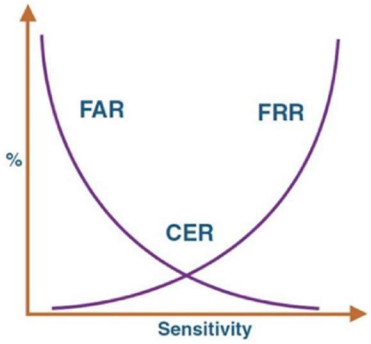
Biometric examples:

- Fingerprint scanner
- Retinal scanner
- Iris scanner
- Facial recognition
- Hand Geometry
- Voice recognition
- Signature analysis
- Gait recognition
- Keystroke recognition



Biometric Error Rates

- Type I Error: False Rejection Rate (FRR)
  - Likelihood that someone legitimate will be denied access
- Type II Error: False Acceptance Rate (FAR)
  - Likelihood an imposter is granted access



- 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

Something you do

Authentication based upon “something you do” is action-based authentication. The subject must perform some act to complete the authentication process.

- Mobile devices can utilize “unlock patterns” such as connecting the dots on a computer display
- Keystroke authentication uses pattern analysis to examine how the person is typing and compares that to a recorded baseline

---

Somewhere you are

Authentication based upon “somewhere you are” is location-based authentication that evaluates geolocation attributes. Geolocation is a term used in information systems security to extrapolate the geographical location of a subject, based on available information. Location-based polices would be implemented to support this form of authentication.

- GPS tagging
- RFID tags
- Reverse IP lookups
- Geofencing

“Somewhere you are” can support anomaly detection, especially within the sphere of remote access. For example, if a person is trying to log into their bank’s website and they live in Chicago they would have been allocated a public IP address from their ISP operating in Chicago. However, if an attacker from Morocco was trying to impersonate the customer in Chicago, the Moroccan attacker would have been allocated a public IP address from the public IP address space belonging to Morocco. Alternatively, the bank could do a reverse IP lookup.

From an IDS and IPS perspective, the ability to restrict or block traffic based on geolocation can greatly simplify a security administrator's job. If a network attack originates from a particular country, packets originating from IP addresses physically located in that country could be summarily dropped for a period in time. Packets originating from "friendlier" areas would continue to be accepted. Furthermore, organizations that only do business in certain parts of the world could configure their perimeter to always drop traffic coming from areas outside of their zones of interest, thereby limiting their potential risk.

Mutual Authentication

Mutual authentication is when both subjects involved in a session authenticate to each other before messages are exchanged. Once again, the authentication components must not be shared.

- Mitigation technique for an Evil Twin attack
- Ensures client is not unwittingly connecting and providing credentials to a rogue server

Protocols that provide mutual authentication:

- Certain types of EAP: LEAP, EAP-FAST, EAP-TTLS, EAP-TLS, PEAP
    - Diameter
    - TACACS+
- Any protocol that uses SSL or TLS
- Kerberos
- IPsec
- MS-CHAPv2

Strong Authentication

Strong authentication uses multiple instances of authentication. It commonly uses multiple instances of the same factor, especially knowledge-based forms of authentication. It is commonly used in online banking.

- Provides layered defense to the authentication process
- Examples
    - ImageMark™, PassMark™ banking systems
    - Answering multiple security questions such as “What is your billing zip code” or “What is your favorite food”

Multifactor Authentication

Multifactor authentication is when a subject is required to provide authentication material that satisfies two or more *factors* of authentication. While strong authentication may use multiple instances of Type 1 authentication, multi-factor authentication would use Type 1 authentication in conjunction with Type 2 or Type 3 authentication.

Two-factor authentication specifically uses only two factors of authentication. Three-factor authentication would specifically use three types of authentication. For example, CAC would be two-factor authentication:

- Type 1: must *know* the PIN
- Type 2: must *have* the card

Authentication Scenario	Strong	Two Factor	Multi-factor
password			
Password + "What is your mother's maiden name?"	✓		
Password + PIN	✓		
PIN + smart card	✓	✓	✓
PIN + smart card + iris scan	✓		✓
Iris scan + fingerprint	✓		
Iris scan + fingerprint + X.509 Digital Certificate + RFID card	✓	✓	✓

Single Sign-On (SSO)

Single Sign-On provides access to all authorized resources within a single instance of authentication (authenticate only once). Once authenticated, subjects can use the network/resources without being challenged again. The key purpose of SSO is to reduce the burden of repetitive authentication to disparate services.

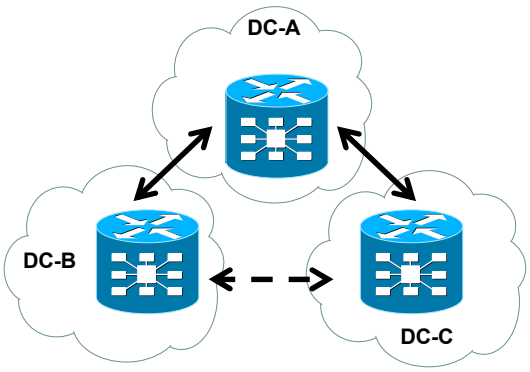
- Potential single point of failure
- If the account is compromised by an intruder then the intruder has access to everything the compromised account was granted access to
- Examples of SSO services:
  - Kerberos
  - LDAP
  - RADIUS
  - SAML
  - Shibboleth
  - TACACS+

Transitive Trust

A transitive trust is an implied access control relationship that exists between two entities, such as between domains. The two entities have the potential of gaining access to each other's resources because of the established trust relationship they both have with an intermediary entity.

For example:

1. The domain controller in Domain A has an explicit bidirectional trust with the domain controller in Domain B, and



2. The domain controller in Domain A has an explicit bidirectional trust with the domain controller in Domain C.
3. B and C have a transitive trust.

Federations

A federation is a collection of autonomous, possibly nonhomogeneous, computer networks that agree on common standards (especially security standards) for conducting business operations, especially among various business partners.

- A federated identity is a user ID with privileges that can be used across business boundaries. Separate user accounts would not be created for each business domain the user will be interacting with; instead the same account is used across all the business domains.
    - Example: RADIUS federations

Access Control Models

Mandatory Access Control (MAC)

MAC is an access control model that restricts a subject's access to objects based on the security clearance of the subject in relation to the security classification level of the object. A reference monitor makes the access decisions. The system enforces the security policy and users cannot share their files with other users. It is commonly used by governments and militaries because it is the ideal model for environments requiring high security.

- Primarily used in high security environments
- Follows the Lattice Model
    - Reference Monitor
    - Access to objects based on clearance and need to know
- Objects are assigned security labels
- Subjects are assigned clearance levels

Discretionary Access Control (DAC)

DAC is an access control model that restricts access to objects based on the identity of the subjects or the groups to which those subjects belong. The creator or the owner of the resource decides which subject's will be granted access to the object. It is the most common access control model used and heavily used by operating systems.

- Owner establishes privileges to the information they own
    - Each object (like a file) has an owner (user)
- Allows information to be shared easily between users
- Decision to grant or deny access is usually aided by an ACL (Access Control List)
- Highly susceptible to Social Engineering attacks

Rule-Based Access Control (RBAC)
Rule-BAC is an access control model that grants or denies access based upon the satisfying of specified rules. It is a nondiscretionary model.

- 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.

Role-Based Access Control (RBAC)
Role-BAC is an access control 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. This model manages access rights more on a group-based access control level instead of a user account micro level. The model is ideal for managing access rights in large organizations or when there is high employee turnover.

- Based on responsibilities that an individual user or process has within an organization
    - Schedule audit checks to avoid privilege creep issues
- Group-based access control
- Task-based access control

Instead of thinking "Denise needs to be able to edit files," Role-BAC uses the logic "Editors need to be able to edit files." Denise is able to edit the file not so much because she has been granted that permission but because she is a member of the Editors group and the group has been granted permission.

Attribute-Based Access Control (ABAC)
ABAC is an access control model that provides access to resources by the satisfactorily matching of the subject's attributes and object attributes within environmental conditions. ABAC is policy driven and enforced through a designated access control mechanism. ABAC requires certain conditions to be met:

- Subject attributes
- Object attributes
- Environmental conditions or context is known
- Policy established

Previous models had to have rules or permissions explicitly set before access was requested. However, the ABAC model can look at the current attributes and make an access decision for that moment.

Examples of environment conditions:

- Threat level
- Subject / object location
- Time of day the access request is being made

From NIST SP 800-162:
"Attribute Based Access Control (ABAC): An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions."

File System Access Control

Accessing files and folders within an operating system's file structure is different between a Unix-based operating system and a Microsoft-based operating system.

UNIX / Linux privileges: Read | Write | Execute
UNIX / Linux principals: Owner | Group | Others (within the operating system's domain)
Resource marker:

- Directory marker ("d")
- File marker ("-")

Example as seen from the command line:

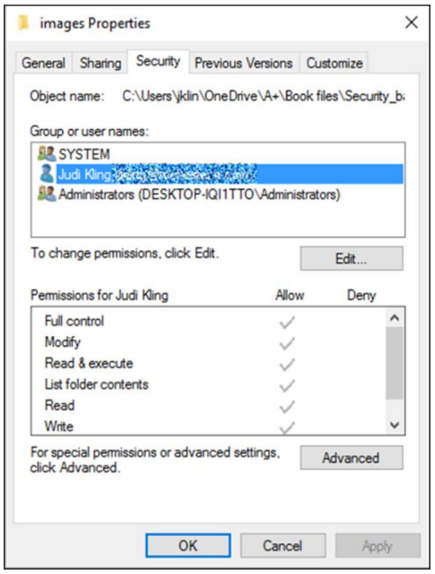
```
drwxr-xr--   6 waffle waffle    4096    Apr 21 16:18  proto
-rw-r-----   1 waffle sales     822     Apr 21 15:34  sales.txt
-rw-r-----   1 waffle sales     10      Apr 21 15:33  sales.txt~
```

Examining the second entry, the permission set (`-rw-r-----`) for sales.txt:

- First character "`-`" is the resource marker and denotes it is a file
- Characters 2-4 "`rw-`": permissions set for the resource owner
    - Allowed Read and Write, but denied Execute
- Characters 5-7 "`r--`": permissions set for the group
    - Allowed Read, but denied Write and Execute
- Characters 8-10 "`---`": permissions set for all others
    - Denied Read, Write, and Exectute

Microsoft privileges

- Security Identifier (SID)
  - Subject's user ID
- Discretionary Access Control List (DACL)
  - Access Control Entry (ACE): permissions for a SID (Full Control, Modify, etc)
  - Inheritance of permissions



Authentication Protocols

New Technology LANMAN (NTLM)
NTLM is a Challenge-Response authentication replacement for the older LM authentication protocol and is primarily used with Microsoft operating systems when Kerberos is not available.

There are two versions of NTLM and neither provides mutual authentication.
NTLM version 1: available to NT operating systems before NT4 Service Pack 4 and is obsolete

- Uses DES for enciphering

NTLM version 2: available to NT operating systems since NT4 Service Pack 4 and is used today

- Uses MD5 for enciphering

Within Microsoft operating systems, the NTLM password hash is stored in the Security Account Manager (SAM) database. NTLM is vulnerable to the Pass the Hash replay attack.

Password Authentication Protocol (PAP)
PAP is a network-based authentication protocol that requires a username and password. However, they are passed across a network in plaintext. It was a popular protocol with the earliest dial-up modems.

- Weakest network-based authentication protocol
- Maintained primarily for interfacing with legacy systems

If PAP must be used in today's production environment, it should be wrapped within a more secure protocol such as TLS or a VPN tunnel.

Challenge Handshake Authentication Protocol (CHAP)
CHAP is a challenge-response authentication protocol that uses MD5 to hash the password and a nonce. The nonce is an IV that modifies the password before it is hashed. The computer being logged onto is called the authenticator; the user's computer is called the peer.

- Decentralized, used in peer-to-peer (P2P) architecture
- Credentials are hashed using MD5
- Uses a nonce as part of the challenge in the 3-way handshake challenge

Not only does CHAP perform the 3-way handshake challenge during the initial session construction but also intermittently throughout the session to protect against man-in-the middle attacks.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
MS-CHAP uses the same handshake process as CHAP but uses MD4 instead of MD5. There are two versions of MS-CHAP.

- MS-CHAPv1: identical to CHAP, except uses MD4
- MS-CHAPv2: provides MD4 mutual authentication
    - Each endpoint creates and exchanges their own nonce
    - Used in LEAP and EAP-FAST

While both versions provide intermittent challenges, MS-CHAPv2 provides mutual authentication.

Extensible Authentication Protocol (EAP)
EAP was developed in response to an increasing demand for authentication methods that use security devices, such as smart cards, token cards, and crypto calculators. It extends 802-type network protocols so that authentication can be supported with various authentication options.

Lightweight EAP (LEAP)
Cisco proprietary authentication protocol designed to be used with WEP.

- Uses MS-CHAPv2 to support mutual authentication between the AP and wireless client
    - Password-based authentication
- Purposely created to mitigate evil twin attacks against WEP

EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
EAP-FAST is an appropriate solution when password-based authentication is desired and certificate-based authentication is to be avoided.

- Cisco proprietary improvement and replacement for LEAP

Protected EAP (PEAP)
Secures EAP authentication within a TLS tunnel
Uses X.509 digital certificates for authentication
Commonly used with WPA/WPA2 Enterprise Mode

EAP Transport Layer Security (EAP-TLS)
EAP-TLS uses X.509 digital certificates for authentication and secure session key exchange

- Requires certificates on both endpoints
- PKI needs to be established

EAP Tunneled Transport Layer Security (EAP-TTLS)
EAP-TTLS (Tunneled Transport Layer Security) clients use server-side certificates for authentication so the server-side digital certificate must be deployed to all devices.

- Client-side digital certificate is not required

Remote Access Control Authentication Protocols

Remote access is when an authorized user is trying to get access to an internal private network from a foreign network (from home or a hotel room). While the connection may be protected with confidentiality and integrity by using TLS or a VPN tunnel, AAA must also be established.

IEEE 802.1X
802.1X provides port-based network access control. It supports EAP-based authentication protocols but not PAP or CHAP.

- Supplicant
  - The device requesting network access such as a user's laptop or mobile device
- Client
  - Typically a network backbone access device such as a WAP, switch or a VPN concentrator
- Server
  - Stores all user authentication and network service access information
  - Ability to implement auditing and accounting

Remote Authentication Dial-In User Service (RADIUS)
RADIUS authenticates remote users, authorizes their access, and provides logging for user to resource interactions. Authentication requests from multiple RAS servers are forwarded to a single RADIUS server.

In RADIUS, the Authentication and Authorization services are bundled together and collectively listen on UDP port 1812. When the client requests authentication, the server replies with the authentication status and any applicable authorization attributes.

- Centralized system for authentication, authorization, and accounting (AAA)
    - Uses IEEE 802.1X
    - Only the password field is protected, everything else is plaintext
    - Supports PAP, CHAP, and EAP

The IANA assigned ports for RADIUS are:

- UDP port 1812: Authentication and Authorization (combined)
- UDP port 1813: Accounting

Terminal Access Controller Access Control System (TACACS+)
TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting.

- Alternative to RADIUS
- AAA performed separately
    - Supports PAP, CHAP, and EAP
    - Allows use of multi-factor authentication
    - Protects the entire message between the TACACS+ client and TACACS+ server
- Allows a RAS to forward user credentials to a separate authentication server
- Uses TCP port 49

For example, it is possible to use Kerberos for authentication and TACACS+ for 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.

Diameter
Diameter is the latest AAA server designed to be the replacement for RADIUS. It is much more versatile than RADIUS because it can handle various LAN and WAN technologies. Internet Service Providers use it because it understands 3G and 4G wireless WANs, Frame Relay, Ethernet, and other networking technologies. Unlike RADIUS, Diameter can provide end-to-end encryption.

- Challenge/Response user authentication

- Supports end-to-end encryption through IPsec, TLS, or both
    - HMACs
    - Endpoints are protected within VPN tunnels
    - Message tampering can be detected
- Supports mutual authentication
- Versatile: handles various WAN technologies
    - Ethernet
    - 3G and 4G WANs
    - Frame Relay
    - ATM
- Uses TCP port 3868

Enterprise Access Control Protocols

Enterprise architecture is a centralized way of managing network-based resources. The enterprise security perimeter is abstract; it is not always clearly defined and may change moment by moment. Enterprise architectures will use directory service protocols within a trusted LAN with the assumption that physical security has been established. Single Sign On (SSO) authentication is used.

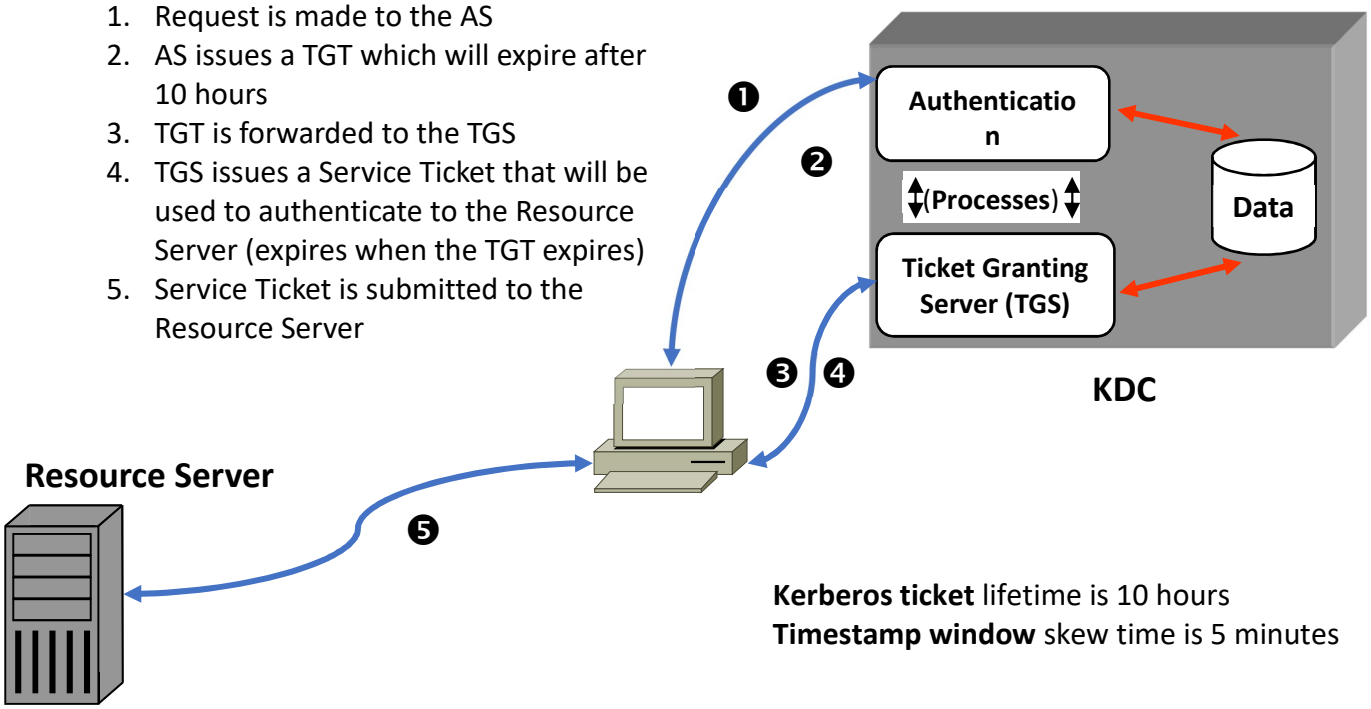
Kerberos

Kerberos is a centralized SSO enterprise authentication protocol developed by MIT that operates within a trusted realm (domain). It uses symmetric tickets with encrypted timestamps for authentication. Kerberos doesn't protect network traffic, only the subject's authentication token.

The latest standard is Kerberos version 5, which can use AES. It is the most common authentication protocol used in directory service architectures such as Microsoft's Active Directory, Apple's Open directory, and Novell's eDirectory.

- Security Principal: the subject or end user
- Realm: area of Kerberos coverage (some vendors call it a domain)
- Centralized SSO server is called the Key Distribution Center (KDC) that works on port 88
    - Authentication Service (AS): issues the Ticket Granting Ticket (TGT) that authenticates the security principal to the realm
    - Ticket Granting Service (TGS): issues the Service Ticket that authenticates the security principal to a service/server
- Kerberos symmetric tickets have a default lifetime of 10 hours and uses encrypted timestamps (authenticators) that have 5 minute windows
    - Tickets provide mutual authentication between the client and the server
    - Packets contain an HMAC-based timestamp that help mitigate replay attacks

1. Request is made to the AS
2. AS issues a TGT which will expire after 10 hours
3. TGT is forwarded to the TGS
4. TGS issues a Service Ticket that will be used to authenticate to the Resource Server (expires when the TGT expires)
5. Service Ticket is submitted to the Resource Server



Kerberos ticket lifetime is 10 hours
Timestamp window skew time is 5 minutes

Kerberos weaknesses:

- KDC is a single point of failure
  - Vulnerable to DoS and DDoS attacks
  - KDC must be able to handle lots of requests in a timely manner
  - All credentials stored in one place
- Tickets are temporarily stored on the user's workstation and could be compromised by malware or spyware
- Network traffic is not protected by Kerberos
- Computer clocks must be synchronized because of the encrypted timestamps

---

Lightweight Directory Access Protocol (LDAP)

LDAP is the most common directory service protocol used in today's enterprise architectures. It provides an object-oriented naming schema and a means to query the network-based resources. Authorization is supported through OU group membership.

- Uses a hierarchical design with a root object at the top followed by Organization and OU containers for logical organization
  - Follows the X.500 standard
- Port 389 (plaintext), Port 636 LDAP over TLS/SSL

Distinguished Names (DN) exists for every object in LDAP. There cannot be duplicates and it must be unique within the realm / domain. It is the full path of the object, including any containers.

- DN = “Relative Path” + “Common Name”

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.

LDAP authentication options:

- Anonymous authentication
  - Only a username is required to authenticate
- Simple authentication
  - 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

- Man-in-the-middle issues
  - Compromise of username/password
  - Deploy simple authentication with TLS or SASL
  - Employ strong passwords and educate users
- Evil Twin and poisoning issues
  - Employ SASL for mutual authentication
  - Implement Secure LDAP (LDAPS) over port 636
- Improper directory security settings
  - Tightly manage ACLs
  - Use auditing and privilege testing to identify users with too many rights

---

Web-based Access Control Protocols

Access control protocols designed to be used on the internet are implemented between a web browser and web server within a SSL/TLS secured session. Sensitive data is transported across untrusted networks (the internet) using trustworthy protocols. Physical security of the communication lines cannot be assumed. Confidentiality, integrity, authentication, and non-repudiation must be primarily handled through cryptography.

Security Assertion Markup Language (SAML)

SAML is an open SSO authentication standard based on XML that provides identification, authentication and authorization services across internet business boundaries. It provides scalability to web-based, federated architecture.

- Identification: cloud-based identity management
- Authentication: centralized SSO is handled by the Identity Provider (IdP)
- Authorization: XML-based cookie serves as the access token

SAML defines three primary roles:

- Principal: the user requesting access to the service provider's resources
- Identity Provider (IdP): a centralized, outside agency that houses credentials for various unrelated, nonhomogeneous, foreign subjects.
    - Example: Google, Facebook, Twitter, or LinkedIn IDs
- Service Provider: an organization that has the service or services a principal (customer) desires.

SAML relies on a trusted 3rd party, called an Identity Provider to validate a principal's authentication and authorization. The federated Service Providers use the Identity Provider relationship in a manner similar to a hybrid single-authority / horizontal trust model. An XML-based cookie is used as a token to record the credentials and capabilities of the user and travels with the user wherever the user goes within the system.

1. Principal sends their cloud-based credentials to the service provider
2. Service provider forwards credentials to the identity provider
3. Identity provider authenticates the Principal's credentials and issues an XML-based authorization cookie
4. Authentication and authorization is granted to the principal through the XML-based cookie

Online service providers often use SAML to prove the identity of someone connecting to the service provider (accessing their website). A customer can log into the Service Provider's website using the credentials they had created at an Identity Provider. The burden of account management is shifted from the Service Provider to the Identity Provider.

Open Authorization (OAUTH)

OAUTH is an open web-based standard created by IETF that provides delegated authorization so that a 3rd party internet client can get approved access to a desired resource belonging to a customer. An access token is generated that allows certain customer resources to be retrieved by someone other than the customer. OAUTH is about authorization, not authentication.

OAUTH Infrastructure components:

1. OAUTH Client: the 3rd party app requesting access to some resource that belongs to the Resource owner.
2. Resource owner: the subject (customer) that owns the resource(s) that the business app want may find desirable
3. Resource Server: the system that is the steward of the resources and will need an API service (GPS interface, credit card interface, etc.) to interact with the OATH client.

4. Authorization Server: the entity that provides the allow/deny interface to the Resource Owner

---

OpenID Connect
OpenID Connect is the combining of SAML with OAUTH. It is the most popular eCommerce protocol used on the web for customer information sharing amongst business advertisers.

Shibboleth
Shibboleth is an open web-based standard similar to SAML. Both Shibboleth and SAML were developed around the same time with similar design goals. However, Shibboleth was designed to be more flexible and more federation driven.

- Identification: cloud-based identity management
- Authentication: decentralized SSO is handled by a federation of Identity Providers (IdP)
- Authorization: cookie-based access token

Shibboleth is managed by the Shibboleth Consortium and came from the Internet 2.0 web project. It was idealized to support a multi-organization collaboration environment.

Account Management

Before an account is created it is important to have the various overriding polices such as the security policy, acceptable use policy, and password policy already established.

Credential management
The credentials used will later lead to which resources are available to the subject.

- Onboarding: allocation of resources to an account
- Offboarding: retrieval of resources that were issued to a subject

Account lockout features are necessary to mitigate security incidents.

- Establish logon clipping levels: a subject typically has three tries to log into their account, afterwards it is locked
- Time-of-day restrictions: temporary account lockout that's designed to mitigate accounts from being compromised during hours the account is typically not used

Password policy
Establish an organization-wide password policy and enforce it within all systems. It should address various topics such as:

- Password complexity: use strong but manageable passwords built upon entropy attributes (upper and lowercase, numbers, and special characters without any patterns)
    - Avoid password obfuscation (example: "p@ssw0rd")
- Password length: at least 8 characters long

- Password lifetime parameters:
    - Minimum password lifetime: determines how soon the password can be changed
    - Maximum password lifetime: determines when the password expires
    - Password history should be kept track of to determine when a password can be used again

Account maintenance
Each account should follow a lifecycle that includes:

- Permission auditing verifies that a subject continues to need certain permissions that have been assigned to the account
    - Mitigates privilege creep
- Usage auditing reviews the interactions the subject has had with various resources
- Set the account to expire at some predetermined, future date so that the account becomes disabled even if an administrator forgets to disable the account after the account user leaves the organization
- Inactivate accounts when they are no longer needed by disabling the account
    - Deleting an account might violate regulatory requirements for data retention
- Establish procedures that must be followed to recover disabled accounts

---

Account Types

Operating systems use various accounts types to represent a subject. The account is assigned a user ID, username, and some form of authentication requirement. The account type implies the scope of access the account might generically possess.

User account
The basic user account is allowed to have use of basic system resources such as programs. It should not be allowed to make system changes.

- Enforce with least privilege management
- Enforce with separation of duties
- Group-based access control: exercise Role-BAC to manage user rights

---

Privileged account
A privileged account is an account that has escalated privileges and can make changes to the settings assigned to the operating system, its services, and installed applications. This account is used to for both system management and account management.

- Requires enhanced auditing
- Enforce separation of duties

Examples of privileged accounts would be administrator accounts and root.

Guest account
A guest account is designed to provide temporary system usage. Typically, once the user of the account is logged off, the user state is not saved. It is highly restrictive with the bare minimum capabilities.

- Enforce with least privilege management

Shared account
A shared account is an account used by a collection of people. The authentication component is shared amongst the collection of people, which violates non-repudiation. This account type should be avoided.

Service account
A service account is created and used by the operating system itself. Typically, each major function of the operating system would have its own service account. These accounts would interact with the operating system's kernel. No person should be allowed access to this type of account.

- Inherently contains escalated privileges

Domain – Technology and Tools

CompTIA SY0-501 domain objectives covered:

- CompTIA domain 3.2: Given a scenario, implement secure network architecture concepts
- CompTIA domain 2.1: Install and configure network components, both hardware- and software-based, to support organizational security
- CompTIA domain 6.3: Given a scenario, install and configure wireless security settings
- CompTIA domain 2.5: Given a scenario, deploy mobile devices securely
- CompTIA domain 2.6: Given a scenario, implement secure protocols
- CompTIA domain 2.4: Given a scenario, analyze and interpret output from security technologies

---

Network Security Zones

Network security zones are compartmentalization models that help isolate systems and networks from other systems or other networks. Network-based resources can be isolated from each other using physical or logical means.

Security zone design is an important aspect of computer security. You can use many different approaches to accomplish a good solid design. 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.

Physical separation

Networks have collision domains and/or broadcast domains that are managed through network segmentation and the network devices used for creating the segments.

- Collision domains are separated by layer 2 devices such as switches and bridges
    - Carrier Sense Multiple Access / Collision Detection (CSMA/CD): a decentralized collision management scheme used on wired networks such as IEEE 802.3 Ethernet networks
    - Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA): a collision management scheme used on wireless networks such as IEEE 802.11 WLANs
- Broadcast domains are separated by layer 3 devices such as routers and Layer 3 switches
    - IPv6-based networks do not broadcast message traffic
- Air gapping is a network isolation technique that removes all wired and wireless interface connections to other networks.
    - Network devices would be updated or patched using "sneakernet" (manually updated by walking over to the network device)

Logical separation

Systems should be grouped together based upon their purpose, level of sensitivity, or level of

criticalness. Grouping systems together strengthens access control and proffers more judicious management of the finite pool of security controls.

- Virtual Local Area Network (VLAN) architecture allows network resources to be compartmentalized through the use of software running inside managed switches
- Virtualization allows resources to be compartmentalized through the use of a hypervisor that enforces the sandbox security model
- Sandboxing is an isolation technique used within a processing environment that quarantines questionable hardware, firmware, or software components until the threat level can be evaluated as safe

---

Internet
WAN interfaces provide internet connections, which is the least trustworthy network. If sensitive data must traverse the internet, it needs to be protected with confidentiality, integrity, authentication, and non-repudiation by using secure protocols, secure channels or VPN tunnels.

Intranet
The trusted, private network includes systems and workstations that typically must not receive directly initiated connections from the internet. The intranet must be protected by a firewall filtering device.

- Compartmentalize further using subnetting and/or VLAN architecture
- Also known as: Local Area Network (LAN), Campus Area Network (CAN), Corporate Area Network (CAN)

De-militarized Zone (DMZ)
The DMZ is the portion of the network owned by the organization but is accessible from the internet. It contains public facing servers such as the web server, email server, VPN concentrator, proxies, etc. The DMZ is not a network security zone that should house a sensitive database server.

- Bastion hosts: any hardened system located in the DMZ

Extranet
A network segment set aside for the storage and sharing of information that is exchanged with a trusted business partner is called an extranet. The business partner's IP address must be known and access to the extranet would likely require a VPN connection.

Honeynet
An entire network segment used as a decoy for researching attack methods is called a honeynet. It is designed to simulate an actual network environment but with a collection of honeypots. An entire honeynet could be virtualized inside one physical machine but it still has to be housed on its own network segment.

Wireless
Wireless network zones rely heavily upon logical separation measures due to the ease of reception of RF signals.

- Wireless Local Area Network (WLAN) uses the 802.11 protocol family to connect network devices within a production environment instead of twisted pair cables
- WLAN guest network is a separate wireless network segment that is ideally implemented to visitors to an organization
    - Guests are sandboxed and unable to reach production systems on the organization's main WLAN
- Ad Hoc networking is a method of connecting two network devices without a centralized network controller such as a gateway or Wireless Access Point (WAP). Examples:
    - Wireless computer connected wirelessly to a wireless printer
    - Two computers connected by a cross-over cable

Network Frame Management

The block of bits that are used within a local link is referred to as a network frame. They are confined to the broadcast domain. Other than NICs, the switch is the main network device that places frames onto a cable, and the Wireless Access Point (WAP) is the main network device that delivers IEEE 802.11 frames into a wireless network.

Switch
The switch conjoins multiple network segments together, but each connection is given its own collision domain. The switch works at layer 2 of the OSI model, the Data Link layer (though more advanced switches covered later can work at even higher layers).

The switch contains memory so it is able to record MAC addresses in its MAC table. When a frame is delivered to a switch, the table is searched for the address to determine which physical port the frame should be sent to.

- Access port: the physical ports on a switch that have been configured to accept traffic from end-point devices such as printers, client computers, and servers
- Trunk port: the physical ports on a switch that have been configured to accept traffic from network backbone devices such as other switches

Switches can be categorized as being either managed or unmanaged. Managed switches have the ability to be logged into and configured. Unmanaged switches can't be logged into.

Bridge
The bridge is the precursor to the switch and is limited to two physical port connections. It works at layer 2, the Data Link Layer.

They were popular when hubs were the primary means to connect an endpoint device to the

network. Today, a switch can be thought of as multiple bridges combined.

Switching loops

A switching loop can occur when there is more than one active pathway between two endpoints on a LAN. The frame could be passed around within the loop and never reach its intended target. Ultimately a switching loop can affect network availability.

IEEE 802.1D Spanning Tree Protocol (STP) organizes switches hierarchically by exchanging Bridge Protocol Data Unit (BPDU) frames amongst the switches. The BPDUs help speed up network convergence on a LAN.

- Manages switch port states automatically through BPDUs exchanges
- Provides loop detection and protection
- Provides faster convergence
    - Selects the fastest network links
    - STP will failover to an alternate link if there is a failed link on the network

---

Broadcast storm

A broadcast storm occurs when broadcast frames are sent, received, and then rebroadcasted by each switch within the LAN. Ultimately, the frame is never delivered because the switches are preoccupied with the broadcast traffic.

- Network congestion: network bandwidth is exhausted
- Switch degradation: memory and processing cycles are exhausted

Broadcast storms can be mitigated:

- Implement IEEE 802.1D STP
- Minimize the broadcast domain:
    - Subnetting
    - VLANs

Virtual LAN (VLAN)

A VLAN allows you to create groups of users and systems and segment them on the network. This segmentation lets you hide segments of the physical 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.

Instead of breaking up a network with multiple, expensive, physical routers, the switch's operating system logically breaks up the network into multiple virtual networks by using IEEE 802.1Q. 802.1Q enables VLAN tagging so each frame can be delivered to the proper VLAN.

- Devices on the same physical network are divided into multiple logical networks
- Created using VLAN-capable switches that understand IEEE 802.1Q

A VLAN is a good way to contain network traffic to a certain area in a network. Network nodes can be isolated from others.

- Segments users or groups of users on a network

Shrinking the size of the LAN by segmenting it into smaller groups (VLANs) reduces the size of the broadcast domains. This will help in reducing the scope of the broadcasts, improving performance and manageability, and decreasing dependence on the physical topology

- Benefits:
    - Improves network throughput by decreasing unnecessary broadcast traffic
    - Mitigates eavesdropping through compartmentalization

A multilayer switch has VLAN capabilities and routing capabilities. It is basically a switch with the ability to route packets.

- Works at layers 2 and 3

Multiple VLANs can be created with a single network switch. A VLAN can logically group several different systems together, or logically separate systems from each other, without the need for extra, costly physical equipment. It does this even without regard to the system's physical location.

VLANs don't require any rewiring of the wiring closet, server rooms, or patch panels. The administrator can place a user in one VLAN or the next, simply by logging into the switch and setting the user's physical Ethernet port to the desired VLAN.

Quarantine portals and padded cells are implementations of VLAN architecture.

VLAN Trunking Protocol (VTP)

When multiple switches (multiple trunks) are used to manage multiple VLANs that coexist amongst those switches, VTP is used to get a "bird's eye" view of all the VLANs. It allows all switches to be privy of all existing VLANs on the whole network.

- Provides bird's eye view of nested VLANs
- Susceptible to **QinQ attacks**: a malicious frame is encapsulated within a benign frame to gain unauthorized access to a VLAN

Switch architecture

Large organizations usually implement a three-layer model that uses the hierarchical trust model when designing switch architecture. STP is an important protocol to manage pathways.

- Network clients connect to edge switches, also known as access switches
    - Most of their physical ports are configured as access ports
- Aggregation switches connect other edge switches to backbone switches, or in smaller

organizations, connect the clients as well
    - Appropriate to have port mirroring configured
    - Stronger need for redundancy
- Backbone switches may serve as gateways to connect the LAN to the WAN, and ultimately to the ISP
    - Typically layer 3 switches with routing capabilities
    - Cisco calls these switches "core" switches.

Network Gateway Management

Recall the following address ranges have been reserved for use on private networks:

Class A	**10.0.0.0 – 10.255.255.255** (10.0.0.0/8)
Class B	**172.16.0.0 – 172.31.255.255** (172.16.0.0/12)
Class C	**192.168.0.0 – 192.168.255.255** (192.168.0.0/16)

Network Address Translation (NAT)

NAT creates a unique opportunity to assist in the security of a network. Originally, NAT extended the number of usable Internet addresses. However, it provides an unintended means to mask the internal private IP address and present a single public IP address to the Internet for all computer connections.

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

- 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

Most NAT implementations operate with the internal hosts already assigned a private IP address but will be lent a public IP address when communicating to the outside world. The NAT table records which IP address is lent to whom.

- Types of NATs:
    - Static NAT (SNAT)
    - Dynamic NAT (DNAT)
    - Port Address Translation (PAT) or NAT overloading
- NAT-T is needed if IPsec's Authentication Header (AH) is going to be used across a network gateway that implements NAT.

Static NAT
When static NAT is implemented, each external IP address is pre-configured for an internal client. There is a one-to-one mapping between the client and the external IP address.

- Provides a more accurate audit trail

Dynamic NAT
When dynamic NAT is implemented, each external IP address is pooled together and allocated on a first come, first serve basis. If more clients attempt to reach the WAN interface, and there aren't enough external IP addresses, then the client will not be able to proceed. There is a one-to-one mapping between the client and the external IP address.

- Also known as "pooled NAT"

Port Address Translation (PAT)
When PAT is implemented, each external IP address is multiplexed with a listening port so the gateway's WAN IP address is reused for many internal clients. In previous versions of NAT, the NAT table would record the rewriting of the IP addresses. However, in PAT not only is the IP address recorded but also the gateway's listening port is recorded as well. There is a many-to-one mapping between the internal clients and the external IP address.

- Also known as "NAT overloading"

Router
Routers are intelligent devices that store pathway configuration and status information about the networks they join together. Routing tables keep track of this information and are updated by routing protocols. A route contains information about the systems connected to it and where to send requests if the destination is not known.

- Provides connectivity between two or more networks
- Routes packets based upon IP addressing

Standard routing protocols:

- Routing Information Protocol (RIP)
- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)

RIP: Private Networks
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
BGP allows groups of routers to share routing information to ensure effective and efficient routing.

Most routers can be configured to operate as a packet filtering firewall if need be. However, they are ideally used as a gateway that routes LAN traffic to the WAN interface and vice versa (as a border router).

Layer 3 switch
A layer 3 switch is a multilayer switch that operates not only at the data link layer, but also the network layer. An L3 switch can operate as a gateway because it understands routing and routing protocols. It is best placed in the role of a network perimeter backbone switch serving as a gateway.

Besides routing services, the multilayer switch typically provides other services such as:

- Network Address Translation (NAT)
- VLAN Trunking Protocol (VTP)
- Quality of Service (QoS)

By their very nature, they are managed switches.

Wireless Access Point (WAP)
The WAP serves as the gateway for a Wireless LAN (WLAN). It can be used to connect a WLAN to a LAN or a WLAN to another WLAN. It rarer cases, it might be called a brouter: combination of a bridge (switch) plus a router. It can bridge the network's wireless and wired segments together as one seamless network and then route traffic through its WAN interface.

Besides serving as a gateway appliance, there are other services often provided:

- Network Address Translation (NAT)
- Dynamic Host Configuration Protocol (DHCP)
- Wireless encryption services
- IEEE 802.1X
- MAC address filtering

Standalone AP is commonly used for smaller WLANs such as within homes. It is typically loaded with very services such as those mentioned in the bullets within the previous paragraph. In this sense it is sometimes referred to as a "fat" AP.

- Single Authority trust model
- May or may not be used with PKI

Controller-based AP is a collection of Access Points used by larger WLANs. A root AP controls all other subordinate “thin” APs.

- Hierarchical trust model
- Used with PKI

Wireless Architecture

Wireless Personal Area Network (WPAN)
An IEEE 802.15 WPAN pertains to peripheral devices that communicate to the computer through some wireless means, usually Bluetooth.

- IEEE 802.15.1 Bluetooth
- Wireless keyboards and wireless mice

Wireless Local Area Network (WLAN)
IEEE 802.11 pertains to WLANs. Each wireless node is assigned an IP address and uses one of the 802.11 protocols to communicate within the WLAN.

- IEEE 802.11a/b/g/n/ac

The WiFi alliance is a group of organizations that certify devices that comply with the 802.11 standards.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
CSMA/CA is the method that wireless transceivers use to avoid transmission collisions within a busy RF environment. A station wishing to transmit has to first listen to the channel 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.

- Wireless is uses half-duplex communications: it is not possible to listen while sending

---

Infrastructure mode
Infrastructure mode is the traditional WLAN implemented in a star topology design with the WAP as the gateway.

- Basic Service Set (BSS)
- WAP provides centralized management of the WLAN

Ad Hoc mode
Wireless Ad Hoc mode lacks a gateway service. It is used in peer-to-peer (P2P) environments in which no one wireless device is in charge of the wireless network. For example, wireless can be used between two wireless computers to exchange a file, or between a wireless computer and a wireless printer.

- Independent Basic Service Set (IBSS)
- Decentralized network management

Association
Association frames are sent from the wireless client to the WAP as a request to join the wireless realm managed by the WAP. It is not authentication. However, during the association phase, MAC filtering is likely to occur.

1. Association of the device
2. Identification of the subject
3. Authentication of the subject
4. Authorization of the resource access request
5. Accounting of the interaction

Disassociation frames release wireless devices from the wireless realm.

Beacon frame
A beacon frame is a management frame that promulgates the SSID of the WAP. By default, the WAP repeatedly broadcasts its SSID name into the air waves through beacon frames.

- Disable SSID broadcasting in the WAP's settings

Service Set ID (SSID)
The SSID is the name given to the WAP. The WLAN adopts the SSID as the name of the network. Wireless devices must agree on, and exchange, the correct SSID name during the association phase. By default, it is usually something to do with the vendor's name.

- Change the default SSID name
- Disable SSID broadcasting

Use a separate "Guest" network for transient visitors.

Basic Service Set ID (BSSID)
The BSSID is the ID of the WLAN and used as an addressing scheme for 802.11 frames. It indicates which frames belong to which WLANs. There is no requirement as to what the BSSID must contain, but it is an ad hoc industry standard to make it the WAP's MAC address.

Extended Service Set ID (ESSID)
The ESSID is the collective name of all the WLANs spread out over a large area. It is used with wireless roaming.

The various WAPs are either set to bridge mode or managed within a hierarchical controller-based AP architecture. In either case, all the APs are set to the same SSID, thus "extending" the area in which the SSID is used.

The wireless client associates to the generalized ESSID, however the AP that provides the greatest signal strength becomes the AP in which the client communicates with. If at some point later, one of the other APs provide the stronger signal then the two APs handshake the wireless client from one AP to the other.

IEEE 802.11 protocol specifications:

Protocol	Frequency	Bandwidth	Modulation
802.11a	5 GHz	54 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	OFDM / DSSS
802.11n	2.4 GHz / 5 GHz	*600 Mbps	OFDM / DSSS
802.11ac	5 GHz	*1.69 Gbps	OFDM / DSSS
*supports Multiple In Multiple Out (MIMO)			

Channel bonding is the technique of combining two or more communication channels into one large communication channel. MIMO is used in wireless to support channel bonding. Each antenna is assigned a channel so that the bandwidth of the channels is combined within one communication channel.

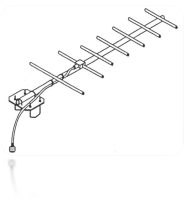
For two 802.11 devices to communicate, the following must match:

- Frequency (i.e. 2.4 GHz, channel 1)
- SSID information
- Modulation type (i.e. OFDM)
- Encryption standard (i.e. WPA2)

Antennae

Antennae placement needs to be strategically planned. Avoid placing the antennae on exterior walls to better contain the signal within the building. Antenna types:

- Omnidirectional: provides 360-degree coverage and is commonly used by wireless clients.
- Directional antenna: used for point-to-point scenarios, especially between two WAPs.



Yagi Antenna

Parabolic Antenna

Flat Panel Antenna

Signal quality effects distance and the transmission rate.

- Signal strength: the wireless client associates with the AP with the greater signal strength when there are two or more equally named APs.
- Attenuation issues will cause signal loss:
    - Distance from the transmitter
    - RF absorbed by water molecules
    - Barriers in the RF pathway
- Radio Frequency Interference (RFI): is produced from competing devices.

Wi-Fi Protected Setup (WPS)

WPS was created to make setting up wireless encryption within a WLAN as easy as pressing a button. WPS uses a PIN scheme to agree and configure wireless encryption in PSK mode. However, WPS has many flaws that are easily exploited. It is highly advisable to not use WPS, but disable it.

MAC Filtering

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.

- 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

Guest mode

Guest mode is also called "AP isolation" mode. Guest mode is not a synonym for "Guest network" but a type of sandboxing technique. Enabling guest mode / AP isolation mode places each wireless device within their own sandbox. Though the wireless clients are in the same WLAN, they will not be able to communicate to each other but only to the AP. This is beneficial if there are devices from questionable origins allowed to connect to the WLAN and may pose an increased risk to the others.

Wireless Authentication

Open authentication

Open system authentication is an option in WEP.

- Nothing is used for authenticating to the WLAN

Pre-shared Key (PSK) authentication
PSK is password-based authentication. The password is used for authentication and as part of the encryption key. PSK is poorly implemented in WEP causing a static key issue.

- Credentials and keys are managed manually
- Commonly used in residential-grade WLANs: Keys are manually distributed

---

Enterprise authentication
Enterprise authentication is available in WPA and WPA2. It uses one of the EAP variants along with an IEEE 802.1X server.

- Can be used with PKI environments: X.509 digital certificates
- Credentials and keys are centrally managed and distributed dynamically
- Appropriate for corporate WLANs

RADIUS federation
RADIUS is a AAA server that uses IEEE 802.1X to help decide access decisions. A federation is a collection of organizations that share a common business or security goal. A RADIUS federation allows a wireless user in one domain access to a domain of another organization. The credentials are stored centrally but can be used across multiple WLANs.

- Supports wireless roaming

Wireless Encryption

Wired Equivalent Privacy (WEP)
WEP was the original encryption standard for wireless communications. It is outdated and should be avoided unless WEP is the only choice available. WEP was designed to give the equivalent security provided by a twisted pair cable.

WEP uses the symmetric stream cipher algorithm RC4 limited to one of two key sizes, either 64-bits or 128-bits. The first 24 bits are used for IV parity bits, so the effective key strength is a weak 40-bits or 104-bits.

WEP understands two different password-based authentication modes:

- Open System authentication: no authentication
- Pre-shared Key (PSK) authentication: the WEP key is used for encrypting data and as a password for authentication

Open authentication is considered more secure then 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 does not have mutual authentication capabilities in itself so it is recommended to implement LEAP or EAP-FAST.

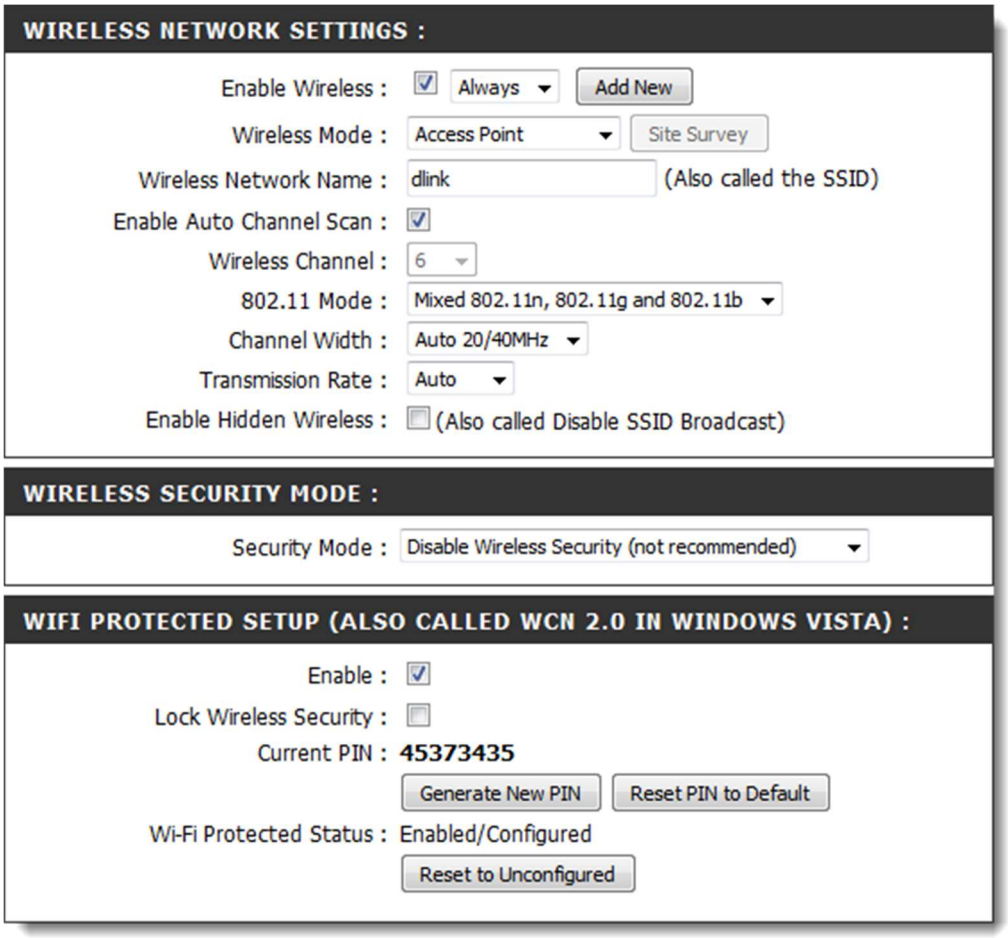
WiFi Protected Access (WPA)

WPA was created to fix some of the problems that exist in WEP. Though WPA still uses RC4 it adds Temporal Key Integrity Protocol (TKIP) to better manage the encryption key lifecycle.

TKIP provides:

- A larger 48-bit IV space
- Message Integrity Code (MIC) tag that provides authenticity of the wireless frame
- Per-frame sequence counter to mitigate replay attacks

WPA can be used with protocols that provide mutual authentication such as PEAP, EAP-TTLS, EAP-TLS, or EAP-FAST.



Example: wireless settings and options

WiFi Protected Access version 2 (WPA2)
WPA2 fulfills the requirements of IEEE 802.11i (wireless encryption) and is mandatory for a product to be "WiFi" certified or NIST FIPS 140-2 compliant. WPA2 is backwards compatible to WPA. It uses CCMP instead of TKIP, by default.

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

- Uses AES encryption
- Uses CBC-MAC for packet authenticity

CCMP uses multiple rounds of encryption. Instead of adding an IV to the encryption key and then encrypting the data like TKIP, CCMP uses an IV and multiple rounds of encryption. Within each round of encryption CCMP uses the previous round's ciphertext as an ad hoc IV for the next round's encryption so that the IVs don't get exhausted.

WPA2 can be used with protocols that provide mutual authentication such as PEAP, EAP-TTLS, EAP-TLS, or EAP-FAST.

Mobile Devices

Strategy
Controlling mobile devices and their usage has to be policy driven.

- Organizational security policy: declares the overall arching security goals for the company.
- Acceptable Use Policy (AUP): defines the acceptable use of company resources. This policy applies to mobile devices used within the company.
    - The primary focus is on authorization
- Privacy policy: defines what will be monitored within the company.
    - The primary focus is on accounting

Deployment models
There are varying mobile device deployment models, each with their own sets of advantages and disadvantages.

- Bring Your Own Device (BYOD): the employee chooses, purchases, and controls the mobile device.
    - Cost overhead is transferred to the employee, and the device can be used for both personal and business functions
    - Most flexible model, but provides the weakest security posture
    - Security awareness training is critical if this model is implemented
- Choose Your Own Device (CYOD): employees choose from a list of company provided mobile devices.
    - Device whitelisting
    - Company makes the purchase so they are the legal owner

- Corporate Owned, Personally Enabled (COPE): company chooses, purchases, and controls the mobile device.
    - Employees can use the corporate device for personal functions
- Corporate Owned, Business Only (COBO): the mobile device is completely locked down for business functions only.
    - The device is issued to the employee and completely managed by the company
    - Security is centrally managed and enforced
    - Most restrictive use
- Virtual Desktop Infrastructure (VDI): mobile device is merely used as an interface to a remote server that houses the corporate data and applications
    - Only the desktop is deployed to the device
    - Data is never stored on the device
    - If the device is lost or stolen, the data is still safe on the remote server

---

Mobile Device Management (MDM)

An MDM is a centralized enterprise solution to provision, configure, manage, restrict, and de-provision mobile devices from smartphones to laptops. It enforces policy, supports troubleshooting, and monitors enrolled enterprise resources.

- Examples: Cisco Meraki, Apple Business Manager, Citrix XenMobile

MDM software manages mobile devices through various features:

- Application management
    - Application white-listing: an exclusive allow list of apps that will be executed within the mobile device to ensure compatibility within the enterprise
        - Baseline of enterprise compatible apps
    - Application black-listing: an exclusive deny list of apps known to be harmful and are actively prevented from being installed
- Storage management
    - Storage segmentation: separate storage areas within the device based upon security level, personal versus corporate data storage, etc.
    - Implement full device encryption to overall protect the contents of the device if it is lost or stolen
- Content management: separate work storage from personal data storage
- Containerization: sandboxing technique in which an app is virtualized and ran from a server but accessed by can be accessed from a mobile device

---

Mobile device authentication

Various authentication methods can be used to authenticate to the mobile device.

- Passwords or PINs: authentication based upon something you know
- Pattern matching: authentication based upon something you do
    - Drawing a pattern on the screen to unlock the device

- Biometrics: authentication based upon something you are
    - Fingerprint, iris scan, facial profile, voice recognition, etc.
- Screen locks: provide device-side session time outs that requires authentication to unlock the device.

Mobile device security options

- Remote wipe: sanitizes the mobile device if lost or stolen
    - Sanitize data, credentials, and cryptographic keys
    - Data Loss Prevention (DLP): goal of enforcing data sanitation and limiting sensitive data spillage
    - Backups must be performed on a regular basis to prevent complete loss
- Geofencing: restricts device usage or app usage when in certain areas
    - Proximity control
    - Can be used in conjunction with TEMPEST controls
- Geolocation: asset tracking
- Push notifications: MDM can send messages and alerts

Mobile device connection methods

- WIFI (2.4 / 5 GHz): using one of the IEEE 802.11 protocols
- Cellular: using a cellular carrier's 3G or 4G network
- Bluetooth (2.4 GHz): using IEEE 802.15.1 to connect wirelessly to another device
- ANT (2.4 GHz): popular with sensor devices used in the medical and fitness industries
    - Proprietary owned by ANT Wireless, Inc
- Near Field Communication (NFC): uses a wireless signal between two devices that are touching or nearly touching
- SATCOM: communication with a satellite when it is within the satellite's footprint
- Infrared: uses point-to-point IR
- Tethered via USB: two devices communicate through a USB cable

---

Mobile device code delivery

Firmware OTA updates

Patches can be deployed wirelessly to the mobile devices. Firmware Over the Air (OTA) updates can be applied when the device is turned on.

- Updates are deployed over wireless communications such as cellular, satellite, or Wi-Fi
- Digitally signed by the operating system vendor

Custom firmware
The device firmware pertains to the operating system and supporting services. The firmware could be custom built but may contain bugs or untrusted code that may compromise the overall security of the mobile device.

By default, a mobile device's operating system doesn't accept unsigned code. In order to accept custom firmware, the security settings of the device need to be changed in one or more ways:

- The device's security settings need to be set to accept unsigned code (which also opens the door wider for malware proliferation)
- The mobile device might need to be jailbreaked or rooted
- Create a PKI environment and embed the organization's digital certificates into the mobile device

Sideloading
Sideloading is the process of transferring firmware, an app, or a file between two local devices, such as from a workstation to a mobile device via a USB cable. Instead of downloading the app from the app store, it's transferred from another system.

- Can be used legitimately to install custom company apps without having to publish the app to a vendor's app store
- Can be used maliciously to bypass network filters

Wired data-in-transit
Mobile devices can be used to transport malware and steal sensitive company data from company systems, including air-gapped systems.

- Tethering: using a cable to connect a mobile device to another system
    - NAT can be used to hide an attacker's mobile device behind a legitimate network device
- USB On The Go (OTG): using the mobile device as a USB storage device
    - Implement Public Key Infrastructure (PKI): exercise digital certificates and digital signatures
    - Map the device's identifying marks (serial number) to the user's profile
    - Implement Full Disk Encryption (FDE)
- External media: could be used for data exfiltration
    - MicroSD card: can be used for sneakernet malicious code transfers and data exfiltration
    - SIM card: SIM cards can be cloned and spoofed

Mobile device privilege escalation
By default, a user of a mobile device is limited in their ability to configure the device. Gaining system-level access of the mobile device is referred to as rooting or jailbreaking. Once

escalation is successful, the user has control over the trusted computing base of the device. Rooting or jailbreaking voids the warranty of the mobile device.

- Rooting: Android operating systems
- Jailbreaking: Apple iOS

Carrier unlocking
In order to use a mobile device in a different vendor's network it has to be unlocked from the previous vendor's network. A code is provided from the old vendor that releases the mobile device so it can be reallocated in the new network.

Payment method
Mobile devices can be used as an authentication device within a payment system. Cached credentials can be unknowingly disclosed to unauthorized parties.

Mobile device app stores
When an app is downloaded to a smartphone or tablet, the operating system is required to grant all of the access permissions required by the app or the app can't be installed.

Open source app development
Anyone can develop and distribute the app so there is an inherent lesser degree of trustworthiness.

- Examples: android apps from Google Play, Amazon Appstore, or from the vendor directly

Closed source app development
Software is tested, reviewed, and certified by the operating system vendor before being made available for download.

- Examples: Apple store Microsoft store

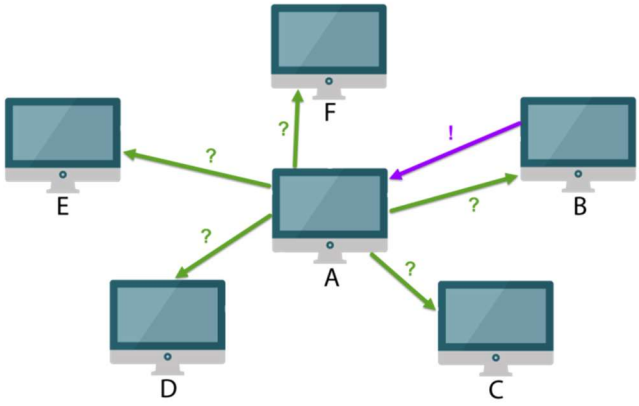
Privilege abuse
Mobile device apps use a capability list for access control. In order for the app to be installed, the various requested permissions must be granted. The list of permissions granted may violate the concept of least privilege management. The permissions aren't selectively granted but are presented as an all or nothing decision. Granting an app access to the components of a system does not require the app to ask for access permission in the future.

Common system components sought by mobile apps:

- Camera access
- Microphone access
- Wi-Fi access
- SMS/MMS access
- Access to device information
- GPS service
- File storage access
- Access to contacts list

Resolving Network Resources

Address Resolution Protocol (ARP)
ARP provides the means for a network device to discover the MAC addresses of neighboring LAN devices. A message is broadcasted to all LAN nodes asking for the MAC address of a node given its IPv4 address. The node in question responds back with its MAC address which is then recorded in the ARP table.



Broadcast message: who has address for node B, tell node A

ARP entries can be configured statically as well by using the "arp –s" command. A static entry has to be manually removed.

Dynamic Host Configuration Protocol (DHCP)
DHCP provides a means to dynamically lease an IP address to a network node. The device's entire IP stack can be configured through DHCP so the network administrator doesn't have to manually configure the network devices with static IP addresses. Typically, DHCP dynamically configures the machine's IP address, subnet mask, gateway IP address, DNS IP address, and the lease time of the IP address.

- DHCP scope: the range of IP addresses that are allocable by the DHCP server
- DHCP reservation: a configuration table within DHCP that allows an administrator to assign a specific IP address to a specific MAC address
    - Alternative to assigning static IP addresses
- DHCP options: a configuration table within DHCP that allows an administrator to select IP-capable servers and assign the IP address of that server
    - Examples of servers or services that can be configured through DHCP options:
        - Default gateway (listed as "router" in the options listings)
        - DNS server(s) address(es)
        - Email server
        - FTP server
        - Time server

DHCP uses a four way handshake (Discover, Offer, Request, and Acknowledge). The configuration settings are listed in the DHCP offer packet. The DHCP server listens on port 67, and the client listens on port 68.

Automatic Private IP Address (APIPA)

A computer may assign itself an IP address if a DHCP server could not be found or if a static IP address had not been assigned. A machine with this kind of address may talk to machines with similar IP addresses within the LAN. Routers will filter this address because they are not allowed to be used on the internet.

- 169.254.000.000/16
- Suitable for local peer-to-peer communications
- Part of the "zero configuration" suite of protocols

Domain Name Service (DNS)

Domain Name Service (DNS) resolves Fully Qualified Domain Names (FQDN) to IPv4 or IPv6 addresses. DNS servers can be used internally for private functions as well as externally for public lookups.

- An IETF standard
    - Hierarchical unique naming schema of resources on the network
    - Distributed, object-oriented database

Example: mail.corporate.acme.com
(host).(subdomain).(domain).(TLD)

Local Hosts File

The hosts file is stored locally on the client and is the first place a system looks for name resolution. Its entries are cached by the operating system at boot time.

- Maps hostnames to IP addresses
    - The hosts file supplements the DNS server
- Stores name and address information about nodes in a network
- Located at /etc/hosts on Unix Systems
- Can be poisoned

DNS Zones

The portion of the DNS domain name space over which a DNS server has authority. A DNS server's zone can contain a single domain, a domain along with some or all of its subdomains, or even multiple separate domains.

Ultimately, a zone is the DNS server's area of DNS namespace it has authority over.

- A portion of a namespace, not a domain
- Can contain one or more contiguous domains

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.

- Publishes information about the domain and the name servers of any domains subordinate
- Port 53 TCP

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.

Ports of interest:

- DNS queries: UDP port 53
- Zone transfers: TCP port 53

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
    - **AAAA** – Returns the IPv6 address
    - **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 indicates that the IP Address for the domain *example.com* is 69.9.64.11

DNS Security (**DNSSEC)**

DNSSEC provides tamper protection to DNS zone table updates sent across the network. It was created by IETF and is not turned on by default inside a DNS server. It helps defeat man-in-the-middle attacks and DNS poisoning attempts. PKI must be established before DNSSEC can be implemented.

- Resource Record Signature (RRSIG): before a DNS server sends a packet containing a DNS update, it digitally signs the update and stores the digital signature in the RRSIG field
- DNSKey: the receiving DNS server retrieves the asymmetric public key from the DNSKey field and validates the digital signature.

Through the DNSSEC digital signature the cryptographic goals of authentication, integrity, and non-repudiation are satisfied.

Transaction Signature (TSIG)

TSIG provides tamper protection to DNS zone table updates that occur within a LAN. It helps defeat man-in-the-middle attacks and DNS poisoning attempts. The protocol uses secret keys and HMAC to sign the updates.

- Requires secure key distribution
- Requires clocks be updated (use NTP)
- TSIG Resource Record: stores the HMAC signature

TSIG is a common solution on a LAN when PKI isn't available.

Network Filtering

Port Security

Controlling access to the physical ports of a network backbone device is important to help keep intruders off the network. Disabling the unused ports of a network switch, bridge, or access point, and then applying MAC filtering to the legitimate ports greatly mitigates various LAN attacks. Managed switches are switches that can be logged into so that their ports can be administratively shut down.

- Disable unnecessary connection ports
- Implement IEEE 802.1X
- Implement MAC filtering

Each physical port can be set to only accept a specific MAC address which is useful if mobility is not required. Another approach is to create a sticky port for a port and the first MAC address that is delivered to the port is recorded and then becomes the only MAC that can be used on that specific port.

Access Control List (ACL)

The ACL is a rule-based access control that is configured on an interface to restrict access to resources. It is a preventative, technical control that can be applied to inbound traffic or outbound traffic. Starting at the top of the list, the list would be traversed until a match was found, the allow or deny would be performed, and then the list would be escaped out of so further potential matches aren't explored.

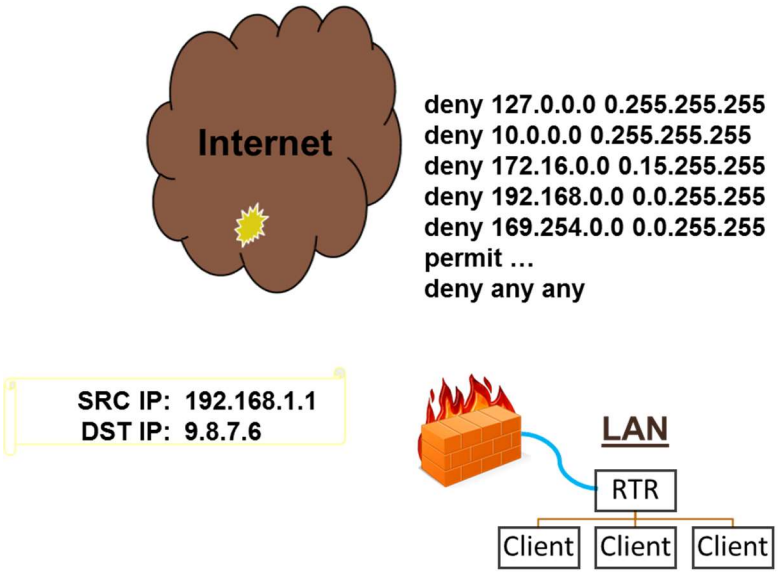
Anti-spoofing filter

At the very top of an ACL is a list of entries that should be exclusively denied because they should logically never be delivered to the interface. For example, a list of private IP address ranges on a network perimeter firewall's ingress filter should be denied because private IP addresses should never be delivered from the internet.

Implicit deny statement

The very last line of an ACL should be set to deny everything as a catch all. If something in the list is not exclusively allowed, then the last line of an ACL will deny it. The implicit deny statement at the end of an ACL supports the concept of least privilege management.

Source IP of 192.168.1.1 would be denied access:



Access-List #	Action	Protocol	SRC IP	Mask	DST IP
access-list 10	permit	IP	192.168.10.0	255.255.255.0	any
access-list 10	permit	IP	192.168.20.0	255.255.255.0	any
access-list 10	permit	IP	192.168.30.0	255.255.255.0	any
access-list 10	deny	IP	any		any

Example: standard ACL

Access-List #	Action	Protocol	SRC IP	Mask	DST IP	Mask	Port
Access-list 101	permit	IP	192.168.10.45	/32	192.168.10.12	/32	eq 1433
Access-list 101	deny	IP	192.168.10.0	/24	192.168.10.12	/32	eq 1433
Access-list 101	permit	TCP	192.168.10.0	/24	192.168.10.100	/32	eq FTP
Access-list 101	deny	IP	any		any		

Example: extended ACL

Firewalls

Firewalls are the primary security guardians of a network. They use ACLs to filter activity.

Network-based and software-based firewalls serve different responsibilities. Network-based firewalls must be multi-homed and installed in-line with the network traffic. Software-based firewalls are installed on a host and are limited to the activity of the host.

Network-based firewalls: filter or restrict network traffic to and from networked resources and focus on what's happening within the communication line

- Screened subnetwork: can be used to restrict access to a subnetwork or a VLAN
- Screened host: can be used to restrict access to a network host
- Port restrictions: can be used to disable services by blocking know operating ports
- Content and protocol filtering

Software-based firewalls: reside on a single host and block access to ports on that host

- Mitigates malware attacks such as worms, backdoors, and RATs
- AKA Personal Firewall (PFW) or host-based firewall

Stateless Packet Firewall

A packet filtering firewall is a *stateless* firewall that 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 ACL setting.

- Uses a standard ACL
- Can see the IP information at Layer 3 and some of Layer 4 (protocol and ports)
    - Would not examine Layer 4 status flags
    - Does not analyze the content (data payload)
- Ideal for network perimeter guardianship duties
- Considered a first-generation firewall

Stateful Packet Inspection (SPI) Firewall
Stateful firewalls use a state table to track the ongoing status changes of a conversation. It filters not only on rules but also on the context of prior packets. For example, it is able distinguish between TCP status flags.

- Uses an extended ACL
- Analyzes all of layer 3 and all of layer 4 of the OSI model
- Requires significant amounts of memory for its state table
- Considered a second-generation firewall

The SPI firewall was initially designed to thwart SYN flood attacks.

Application Proxy Firewall
Application proxy firewalls perform deep packet inspection that allows it to examine the entire packet including the data payload. Due to the deeper analysis, the firewall takes longer to examine the packet.

- Uses an extended ACL
- Multilayer and multipurpose
    - Analyzes up to layer 7 of the OSI model
- Context-aware: analyses the current packet and its relationship to previous packets
- Content-aware: examines the data payload and its meta data
- AKA Application gateway firewall

Proxy Server
A proxy is simply an intermediary between a client and a server and is the middle-man in 3-tier architecture. It serves as a front-end appliance to a back-end service.

- Forward proxy: facilitates a connection from a LAN client to an internet server
- Reverse proxy: facilitates a connection from an internet client to a LAN server
- Transparent proxy: a forward proxy whose settings need not be configured on the clients

---

Internet Content Filter
The internet content filter allows or blocks web traffic based upon the category the content matches. The filter examines the IP address, the URL, and the meta data of the content. An administrator creates allowed and denied categories of content.

- Designed to enforce the security policy
- Prone to false positives

Content filters may block legitimate websites so a means to contact the administrator is advisable so that explicit allows can be implemented.

Flood Guard
The flood guard is a network security device that mitigates various types of network flood attacks. It can work down to layer 2 so that it can be used with switches and thwart ARP floods.

Examples of attacks the flood guard mitigates:

- ARP flood attacks
- SYN flood attacks
- ICMP flood attacks
- HTTP flood attacks

The flood guard can be embedded inside a firewall, network-based IPS, or a multilayer switch.

Web Application Firewall (WAF)
A WAF solely protects the web server from malicious web traffic such as XSS, SQL injection, XML injection, forged HTTP requests, SYN flood attacks, and more. It helps filter the data being submitted to a web server's interface when proper input validation wasn't applied by the web programmer's code.

The WAF could be, software-based and installed on the web server, or more preferably a separate security device that is placed in-line with the web server. The hardware-based WAF would need to be multi-homed.

Tunneling

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 routable protocol for transmission. The data passed through the tunnel appears at the other side as part of the organization's network.

- Virtual dedicated connection between two systems or networks
- Sends private data across a public network by encapsulating data into other packets
- May or *may not* include data protection mechanisms such as encryption

Tunneling might be performed because:

- A non-routable protocol needs to be made routable
- Make a physically distant computer logically near
- Make a foreign protocol routable through an inflexible network
- Make a non-internet routable protocol, routable across the internet

---

Virtual Private Network (VPN)
A Virtual Private Network uses virtual circuits that begin from one trusted network, tunnels through an untrusted network (such as the internet), back to a trusted network. To the user, it

looks like they never even left the network, though the system they are connecting to could be on the other side of the world.

- Established via tunneling protocols that perform encapsulation
    - PPTP (MPPE provides the encryption)
    - L2TP (IPsec provides the encryption)
    - SSH
    - SSL VPNs such as OpenVPN and SSTP (TLS provides the encryption)
    - IPsec
- VPN tunnels may apply security mechanisms such as authentication and encryption services to protect the communication line
- Remote Access is best protected using a VPN Tunnel

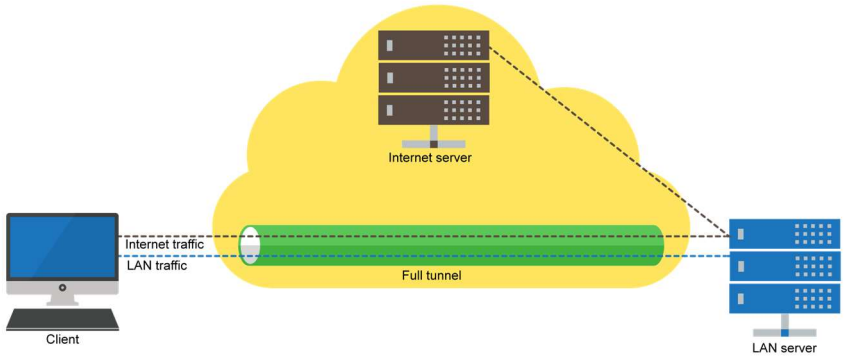
VPN Topology

- Host-to-host: two machines on the same network establish a VPN tunnel
    - Example: front-end webserver to a back-end SQL database server
- Host-to-site: a machine on one LAN traverses through a WAN to gain remote access to another LAN
    - Example: a company employee remotes into the corporate network from home
- Site-to-site: two LANs communicate by traversing a WAN but the two LANs are one autonomous system
    - Example: one branch of the corporate network is able to communicate to another branch of the corporate network but with the internet between the two branches

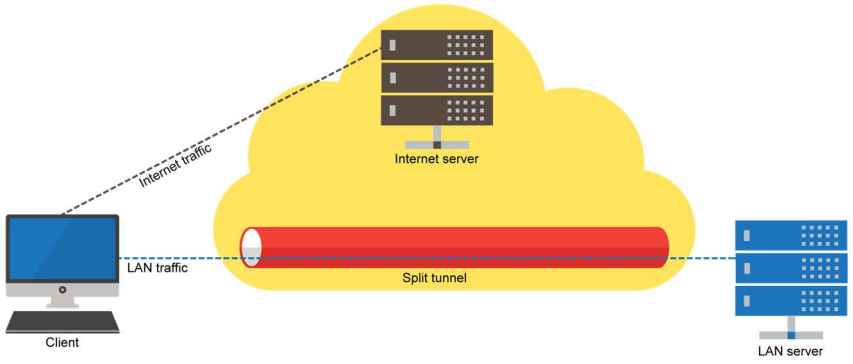
---

VPN Tunnel Methods

- Full tunnel
    - All network is passed through the tunnel
    - Can cause extra processing burden on the corporate infrastructure



- Split tunnel
    - Only network traffic destined to the corporate network is passed through the tunnel, all other traffic goes directly to the internet



- Always-on VPN tunnel
    - VPN client solution that uses a VPN tunnel whenever a client is connecting to an untrusted network

---

VPN Concentrator

A VPN concentrator terminates the influx of VPN tunnels coming from the internet. It is most likely to be placed in the DMZ because of tunnels are originating from the internet.

- Primarily used for remote access VPN's
- Commonly used with either IPsec or TLS VPN tunnels

A VPN concentrator is the first checkpoint into a corporate LAN so it is going to be tasked with Network Access Control (NAC) duties. The VPN concentrator must enforce the security policy.

Network Access Control (NAC)

NAC devices examine 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. The foreign computer needs to still be in compliance with ruling policies and standards.

For example, an employee wants to remote in from home and they are using their personal computer. The NAC service would conduct a host health check before allowing the connection to proceed. NAC is a policy enforcement mechanism.

Some of the items commonly reviewed:

- Anti-virus status
- System update level
- Configuration settings
- Software firewall enabled

NAC attributes
There are various NAC methods:

- Agent-based: a small program is deployed to the prospective system and reports back to a centralized console
    - Example: Windows Action Center
- Agentless: the prospective system is scanned by an external, centralized security device
    - Example: a website's browser compatibility check
- Dissolvable NAC: the health check is performed only in the beginning of the session
    - Interrogation occurs at connection request time or during the session's handshake phase
    - Vulnerable to Time of Check / Time of Use (TOC/TOU) attacks
- Permanent NAC: persistent, continuous monitoring throughout the session
    - Alert is generated as soon as the system becomes non-compliant with the security or configuration baseline

---

Quarantine Portal
A quarantine portal redirects the user to a transient area while their system has not been verified to be compliant with the security policy or configuration requirements.

A quarantine portal is an example of sandboxing. The user may be redirected to a webpage with hyperlinks to the fixes. Once the identified deficiencies have been remedied the system may then access other resources.

- Isolated VLAN
- Wireless guest network

Examples of policy or configuration deficiencies that may need remedy:

- Features needing to be enabled or disabled (i.e. popup blocker)
- Missing or necessary device drivers
- Missing patches for the operating system or specific application
- Antivirus menu to choose a missing antivirus engine
    - Antivirus updates for a specific antivirus engine
- Absent software needed for communication or transactions
    - Media player codec
    - Adobe Flash or Microsoft Silverlight
    - Microsoft .Net architecture
    - Acrobat Reader

Captive Portal
A captive portal "captures" or redirects the user's initial traffic because something more is needed from the user, such as a credit card, or user name and password.

Hotels and coffee shops use them to ensure only their customers are using the business's resources. Once the required information is provided, the user is allowed to continue onto their destination.

- Hotel network requires the visitor to provide credentials
- Coffee shop or airport charges for internet access so the user is redirected to a login page that asks for a credit card number

---

TLS VPN Tunnel

SSL/TLS VPN tunnels are web-based VPN solutions that utilize PKI and X.509 digital certificates from a trusted CA. The client's web browser is used as the client-side VPN interface. The encryption security settings are easier to setup and maintain on the client because the cipher suite is used for settings negotiation.

- Ease of client-side configuration
- Supports certificate-based mutual authentication
- Web browser: no need for additional client-side software

The VPN tunnel communicates over TCP port 443. Examples are OpenVPN and Secure Socket Tunneling Protocol (SSTP).

Layer 2 Tunneling Protocol (L2TP)

L2TP is a hybrid of Cisco's L2F and Microsoft's PPTP being combined at the Data Link Layer. It is defined as a standard, RFC 2661. L2TP does not provide data encryption by itself so is usually teamed up with IPsec.

- 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

L2TP has two message types:

- Control messages manage the tunnel
- Data messages are encapsulated PPP frames

The frames can then be tunneled inside of IP, Frame Relay, X.25, or ATM cells, making L2TP more versatile than PPTP. L2TP is commonly used for remote administration of network backbone devices, such as routers and switches.

IP Security (IPsec)

IPsec is the most popular VPN tunneling protocol used across the internet. It provides authentication and encryption services to anything that is IP-based and is built into IPv6.

Most widely deployed VPN technology:

- Works down to layer 3 to protect either IPv4 or IPv6 network traffic
- Security goals provided:
    - Authentication
        - IKE: X.509 digital certificates
        - Pre-shared keys (passwords)
        - Kerberos
    - Confidentiality: AES, 3DES, DES
        - Possible only with the ESP protocol
    - Anti-tamper protections
        - Integrity: MAC/HMAC (either SHA or MD5)
    - Anti-replay services

IPsec can be implemented by itself or complement other protocols such as L2TP.

IPsec Modes

IPsec needs to be configured to run in one of two modes:
"Transport on the LAN and Tunnel on the WAN"

Transport Mode
Used for end-to-end encryption of data. Packet data is protected, but the header is left intact

- Host to host, host to network communications

Tunnel Mode
Uses encapsulation for the header information and is used in link-to-link network communications. Both the packet contents and the header are protected

- Site to site, network to network, gateway to gateway communications

---

IPsec Protocols

The two primary protocols used by IPsec to provide security services at the IPsec bottom layer are Authentication Header (AH) and Encapsulating Security Payload (ESP). They can be applied individually or, through encapsulation, they can be applied in combination with each other. Both can operate in either the transport or tunnel mode.

Though it is rare to see a lack of choice between ESP and AH, ESP is the only one of the two that is required to be supported by IPsec. AH may or may not be supported. Besides providing confidentiality, ESP has a "null" encryption option which purposely does not provide confidentiality of the packet but moreover provides a way to mimic most of the functionality found in AH. The "null" encryption setting allows the NIDS to analyze traffic in the absence of AH.

Authentication Header (AH)

AH is normally used in Transport mode to protect address information as it's delivered within a LAN. AH does not provide confidentiality so a NIDS would be capable of analyzing the network traffic. It offers authentication and integrity security services.

- HMAC
- SHA or MD5
- IP Protocol #51

AH provides tamper protections to the data payload and the IP headers. Thus, NAT-T is needed if AH is used across a NAT gateway because a NAT interface would exchange the internal network's private IP address for a public IP address. Otherwise, the receiving endpoint's computed hash would never match the original computed hash.

Encapsulating Security Payload (ESP)

ESP is normally used in Tunnel mode to protect network data as it goes across the internet. It offers authentication, integrity, and confidentiality security services. It is required to be supported in IPsec (AH is not required).

- Uses AES, 3DES, or DES
- IP protocol # 50

ESP uses Counter Mode (CTM) with AES, 3DES, or DES to symmetrically protect the data payload. It doesn't protect the IP header though (IP addresses).

Internet Key Exchange (IKE)

IKE is the standard automated method for encryption key negotiation, agreement, and exchange in IPsec. IKE works closely with ISAKMP and Diffie-Hellman over UDP 500.

- Negotiates the key to be used for protecting IPsec traffic
- Supports pre-shared keys and X.509 certificates for authenticating VPN endpoints
- Supports mutual authentication
- Uses UDP port 500
    - NAT-T UDP port 4500
- Uses DHE (IKEv1) or ECDHE (IKEv2)

IKE negotiates the keys between two IPsec endpoints. The current standard is IKEv2.

Internet Security Association and Key Management Protocol (ISAKMP)

ISAKMP defines procedures and packet formats to establish, negotiate, modify, and delete Security Associations. While ISAKMP provides the framework for key exchange, it typically uses IKE to negotiate the key exchange.

- Defines payloads for exchanging key generation and authentication data
- UDP port 500

ISAKMP manages the Security Parameter Index (SPI) which is the list of security associations that ISAKMP oversees.

IPsec Security Association (SA)

All IPsec connections must have a security association defining the parameters of security services such as confidentiality, integrity, and authentication. The security association is tied to only one connection, in one direction. This means that in an encrypted session, there are two security associations - one for each direction.

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. Each SA is recorded in the Security Parameter Index (SPI).

Security services are performed by either the Authentication Header (AH) or the Encapsulating Security Payload (ESP) protocols.

- Negotiated either by IKE or by manual user configuration
- Unidirectional

Secure Shell (SSH)

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

- Secures remote terminal communications
- Secure replacement for Telnet and FTP
    - Protects against sniffing, spoofing, and man-in-the-middle attacks
    - SSH suite (SSH, SCP, SFTP, Slogin)
    - Uses TCP port 22
    - Examples: OpenSSH, Putty
- Uses Hybrid Cryptography:
    - Symmetric cryptography for confidentiality
        - Usually either 3DES or Blowfish
    - Establishes connection and authentication using public key cryptography

Though SSH is a VPN tunneling protocol, it isn't ideal for end users. SSH is most likely to be used as a VPN tunnel for remotely administering network backbone devices such as routers, switches, and firewalls. SSH is not found natively on Windows operating systems.

Remote Administration

Telnet
Telnet is a protocol that provides remote administration through the command line. All major operating systems have Telnet capability. Due to its various security issues, Telnet is usually disabled within the operating system. Network switches and routers may have the Telnet service turned on by default.

- Application Layer protocol
- Provides command-line remote administration
- Passes data in plaintext (including the password) across the network
- Works on TCP port 23

If Telnet must be used across a network, it needs to be protected by encryption. Though Telnet can be used with TLS, the more favorable solution is using SSH instead.

Remote Desktop Protocol (RDP)
RDP provides a means to remotely administer another system, but unlike Telnet, RDP provides a Graphical User Interface (GUI).

- Often used to remotely administer a Microsoft-based server
- 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

RDP is Microsoft proprietary so it should be looked upon as a Microsoft solution for remote administration of their 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.

Simple Network Management Protocol (SNMP)
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. SNMPv3 provides authentication and encryption.

- Application Layer Protocol
- Manages and monitors devices on a network that understand the MIB querying format.
- No authentication capabilities prior to version 3
- Change the default “community strings”:
    - “public” provides read access

    - "private" provides modify access
- Ports of interest:
    - Uses port 161 for SNMP queries
    - Uses port 162 as a "trap channel" that delivers alerts

SNMP allows network administrators to manage network devices, evaluate and monitor network performance, find and solve network problems, and plan for network growth.

Transport Encryption

Secure Socket Layer (SSL)
SSL was proprietary to Netscape, Inc and is now considered obsolete. The last version created was SSL 3.0. Legacy systems may still use SSL, however. It is the precursor to TLS.

SSL provides a secure communication channel between two TCP-based endpoints. It uses hybrid cryptography:

- Asymmetric cryptography provides secure key distribution of the session key
    - Uses X.509 digital certificates
- Symmetric cryptography provides data confidentiality
- Uses a MAC for packet origin and data integrity

SSL 3.0 supported mutual authentication, prior versions did not. The web client delivers a cipher suite to the server from which the server picks the security settings for the session.

Transport Layer Security (TLS)
TLS was designed by IETF to be an open standard that would replace SSL. There are a lot of similarities between SSL and TLS but they are not compatible with each other. Like SSL, TLS provides a secure communication channel between two TCP-based endpoints from layer 7 to layer 4 of the OSI model and uses hybrid cryptography. All major web browsers support TLS.

- Official web standard created by the Internet Engineering Task Force (IETF)
- Though TLS has similar functionality to SSL, they are incompatible with each other
    - TLS 1.0 is sometimes referred to as SSL 3.1
    - TLS 1.1 is sometimes referred to as SSL 3.2
    - TLS 1.2 is sometimes referred to as SSL 3.3
- WTLS is the wireless version of TLS used in WAP 1.x; TLS is used in WAP 2.x
    - WTLS are incompatible with each other

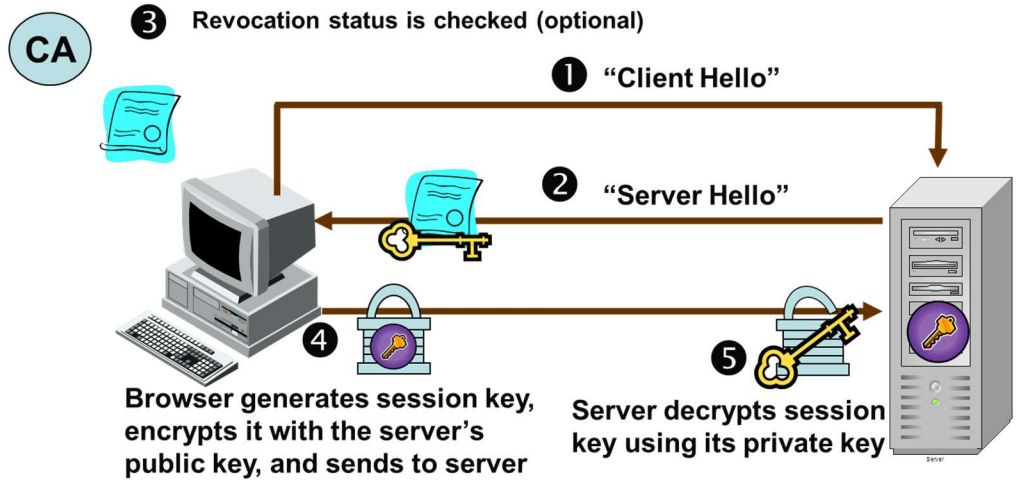
TLS uses hybrid cryptography:

- Asymmetric cryptography provides secure key distribution of the session key
    - Uses PKI and X.509 digital certificates
- Symmetric cryptography provides data confidentiality

- Uses an HMAC for more secure hashing than SSL
- All versions of TLS can support mutual authentication
- Supports Perfect Forward Secrecy (PFS)

The web client delivers a cipher suite to the server from which the server picks the security settings for the session. The TLS 1.0 protocol is purposely designed to be capable of downgrading to SSL 3.0 if both endpoints agree. This makes it susceptible to a downgrade attack such as the POODLE attack.

Refer to appendix E for a list of noteworthy ports.



HTTPS process

File Transfer Protocol (FTP)

FTP transfers files between systems on a network, or to a centralized FTP server. It 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.

- Ports TCP 20 (data) and TCP 21(control)
- Active FTP: FTP server attempts to initiate the data channel
- Passive FTP: FTP client initiates the control channel and the data channel
    - Necessary method if trying to pass through a firewall

Vulnerabilities:

- Plaintext issues:
    - Man-in-the-middle attacks
    - Username, password, data

- Bounce attacks: an attacker uses the FTP server to attack or explore other locations on the network

---

FTP Alternatives

- FTP Secure (FTPS): session is encrypted using TLS or SSL cryptographic protocols
  - Operating system independent
  - Requires PKI
  - TCP ports 989 and 990
- Secure FTP (SFTP): uses SSH to communicate to an FTP server
  - Used with UNIX and Linux operating systems
  - TCP port 22
- Secure Copy Protocol (SCP): uses SSH to securely transfer a file between two endpoints
  - Used with UNIX and Linux operating systems
  - Replacement for RCP or FTP
  - TCP port 22

Email

Mail Gateway

The mail gateway is the central network device that inspects and protects email traffic coming into or out of the corporate network. It scans emails for malicious code such as viruses, spyware, or adware.

- Vendor diversity: use an antivirus vendor different from the antivirus vendor used on the email clients
- Supports DLP: sanitizes email of sensitive data so it is not spilled onto the internet
- Can encrypt the email communication lines with a VPN tunnel
- Uses a spam filter to mitigate spam

Email Cryptography

Email technology uses three standard network protocols:

- SMTP: TCP port 25 (plaintext)
  - Sends email from the email client to the email server
  - Email server to email server
  - Encrypt with SMTPS: TCP port 465
- IMAP: TCP port 143 (plaintext)
  - Downloads email from the email server to the email client
  - Encrypt with IMAPS: TCP port 993

- POP3: TCP port 110 (plaintext)
    - Downloads email from the email server to the email client
    - Encrypt with POPS: TCP port 995

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

- Provides centralized key management
    - Follows the PKI X.509 standard
    - Uses the hierarchical trust model
- Provides authentication, integrity, confidentiality, and non-repudiation:
    - Asymmetric: Diffie-Hellman with DSS or RSA
    - Symmetric: AES, 3DES, DES, or RC2
    - Hashing: SHA-1 or MD5

Pretty Good Privacy (PGP) / GNU Privacy Guard (GPG)
PGP was initially published in 1991 by Phil Zimmermann as a response to the FBI to demanding 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. Public keys are stored in a "key ring".

- Provides decentralized key management
    - Keys created locally through the installed PGP software
    - Uses a web of trust model and PGP-based digital certificates (not X.509)
- Considered a cryptosystem
    - Asymmetric: RSA, DSS, Diffie-Hellman
    - Symmetric: AES, CAST-128, IDEA, Twofish, or 3DES
    - Hash Coding: SHA-2, SHA-1, MD5, RIPEMD-160

S/MIME and PGP/GPG use hybrid encryption to protect the email and email attachment. Though they use similar encryption algorithms, they are not compatible with each other.

GPG is the GNU project's complete and free implementation of the OpenPGP standard. PGP and GPG can be used interchangeably.

Telephony

Media Gateway
The media gateway is a network server that delivers streaming video and audio across a network. Due to the need to minimize latency issues in the media stream, Quality of Service (QoS) must be an available feature.

- Implements IEEE 802.1p QoS

The media gateway is designed to support various collaboration endeavors:

- Closed Circuit Television (CCTV)
- Web conferencing
- Video chat
- Voice over IP (VoIP)

Telephony Protocols

Session Initial Protocol (SIP)
SIP is the decentralized management protocol for telephony multimedia communication sessions. It was based on HTTP and so works at Layer 7, the Application layer. It utilizes ports 5060 (plaintext) and 5061(TLS).

- Establishes, manages, and tears down the telephony session

Real-time Transport Protocol (RTP)
RTP is what transfers the streaming media (audio or video) over networks

- Transports real-time data over unicast or multicast network services
- Real-time Control Protocol (RTCP) would provide IEEE 802.1p Quality of Service (QoS)

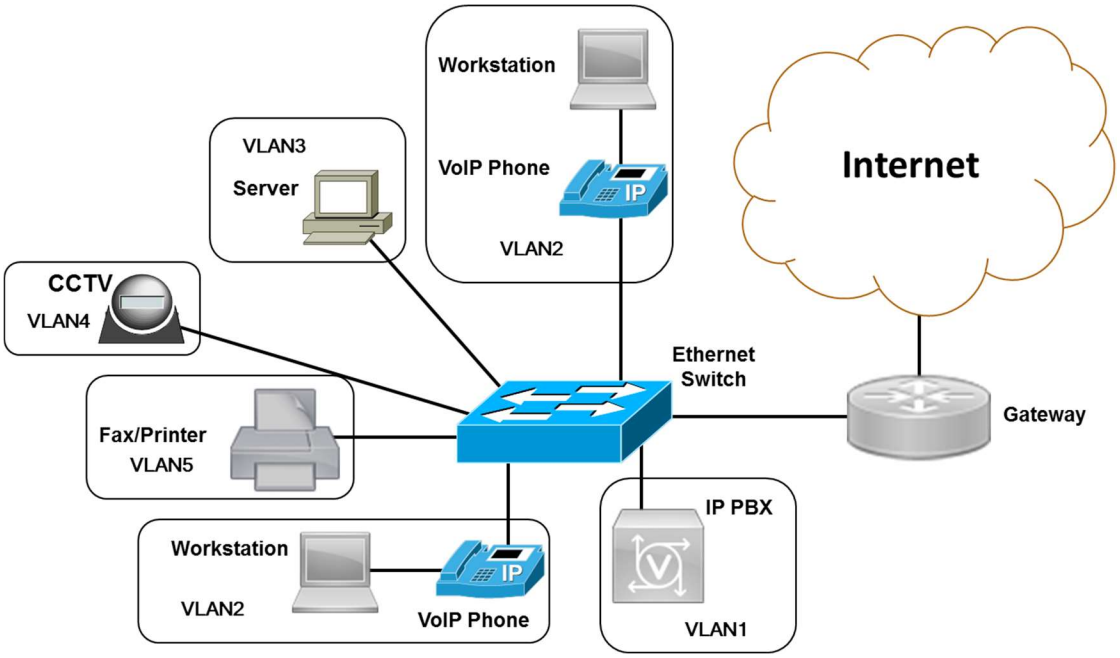
Secure Real-time Transport Protocol (SRTP)
SRTP provides message authentication, message integrity, confidentiality, and replay protection to the streaming media.

- Uses its own encryption security solution, it does not use SSL/TLS
- Uses AES with HMAC-SHA

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

Eavesdropping is the greatest concern of VoIP. Spam over Internet Telephony (SPIT) is a modern twist on spam being used in VoIP networks. Protect VoIP traffic through Defense in Depth:

- Implement IEEE 802.1p QoS: assures timely packet delivery
- Implement IEEE 802.q VLAN architecture: segregates VoIP traffic to ensure compartmentalization
- Implement IPsec: use ESP to provide confidentiality of the conversation and AH to ensure the IP addresses don't get tampered with
- Implement voice firewalls: provides network access restrictions



VoIP architecture example

Domain – Threats, Attacks, and Vulnerabilities

CompTIA SY0-501 domain objectives covered:

- CompTIA domain 1.3: Explain threat actor types and attributes
- CompTIA domain 1.1: Given a scenario, analyze indicators of compromise and determine the type of malware
- CompTIA domain 1.2: Compare and contrast types of attacks
- CompTIA domain 1.6: Explain the impact associated with types of vulnerabilities

---

Threat Actors

Script kiddies

- Attackers who lack the knowledge of how the various protocols work
- They lack the skill to build their own attack tools

Hacktivists

- Attackers with a political or ideological agenda

Organized crime

- Attackers with the primary goal of financial gain at the expense of others
- Often involves extortion

Business competitors

- A business adversary trying to gain a competitive advantage
- Corporate espionage

Insiders

- Attackers within the employ of the organization
- Often viewed as trustworthy and possess basic information about the organization

Nation states

- Government-supported attackers
- Afforded more finances and training
- Possesses an advanced skillset

Advanced Persistent Threat (APT)

- Attackers who exercise prolonged, stealthy, and ongoing sophisticated attacks
- Usually involves diddling attack methods and redundant attack vectors
- Goal is to gain subtle and long-term control without being discovered
- Possesses an advanced skillset

Threat actor attributes
Not all attackers attack for the same reason.

- Location
    - Internal threats are already past most of the layers of security and can more easily hide their attacks
    - External threats usually begin from the internet
- Level of sophistication
    - Script kiddies have very low levels of sophistication
    - Advanced Persistent Threat (APT) has a very high level of sophistication
- Availability of resources and funding
    - Nation-state attackers have more tools, resources, and money at their disposal
- Intent or motivations
    - Different attackers are motivated differently which may affect what they intend to attack
    - Political, ideological, or financial motivations

Social Engineering

Social engineering is the exploitation of the human psyche so that data can be stolen or an act can be performed to the benefit of the attacker. The manipulation is sometimes referred to as "people hacking".

Social engineering uses social tactics to trick users into giving up information or performing actions they wouldn't normally take. Social engineering attacks can occur in person, over the phone, while surfing the internet, through email, or through instant messaging.

Social engineering principle techniques:

- Authority: plays on a person's willingness to please someone perceived to be in authority
- Intimidation: coercion
- Consensus: implied group approval
- Scarcity: limited supply of a resource
- Urgency: limited time
- Familiarity: been done in the past
- Trust: looking out for someone's best interests

Dumpster Diving
Looking in the trash for sensitive information

Countermeasures:

- Physical destruction
    - Pulverizing equipment and devices

    - Shredding documents before throwing them out
- Physical security of the dumpster
    - Fence, cage, locks
- Clean desk policy

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

Countermeasures:

- Screen protectors
- Limiting the viewing angle (keep your back against a wall)

Impersonation
Impersonation is pretending to be someone you are not in an attempt to gain access to an area you should not. The intruder would have the same access as the person being impersonated.

- Type of masquerading attack
- Can lead to a data disclosure attack

An individual pretends to be support staff over the telephone or someone who uses a maintenance uniform to gain access to a facility as a maintenance person.

Tailgating or Piggybacking
Entering a secured building/area by following an authorized employee
Countermeasures:

- Security awareness training
- Mantrap
- Security guards
- Turnstiles

Phishing Attacks
Phishing attacks are traditionally delivered through email but can be delivered through other means as well, such as social media websites.

- Target is anyone

Countermeasure:

- Security awareness training

Spear Phishing Attack
Spear Phishing is the sending of email to a group of people or a specific person within an organization. Some inside information about the organization or individual is needed to make it more effective. Often impersonation of someone with authority is used.

- Target is a person, group, or organization

Countermeasures:

- Security awareness training
- Digitally signed email messages prove authenticity and nonrepudiation

---

Whaling
Whaling targets upper management personnel. Though the goal may include stealing personal information from the senior executive, moreover the attacker wants to steal sensitive, proprietary, or strategic merger and acquisition information about the company. The message is tailored to the individual.

- AKA harpooning

Countermeasures: security awareness training, DLP

Vishing
Vishing uses phone calls to steal personal identity data and financial account credentials. It could be used in conjunction with caller ID spoofing to more effectively scam people.
Countermeasure: security awareness training

Hoax
Hoaxes are false virus warnings that circulate over email and are designed to cause self-inflicted 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, the damage is almost always the result of hoax recipients being tricked into harming their own PCs by following a set of persuasive instructions that promise to "fix" or "disinfect" a perfectly healthy machine.

Countermeasures: security awareness training and least privilege management

Watering Hole Attack
The attacker uses a site that is visited by those they are targeting, poisoning that site, and then waits for the results. The victims would be familiar with the site and trust it. The attacker may use a drive by download attack, Trojan horse, or malicious scripts to compromise the victim's machine.

Spam
Spam is defined as any unwanted, unsolicited e-mail. From a business perspective, the problem with spam is that when it is delivered in bulk, system resources are lost. The spam has to be stored, processed, and delivered which means legitimate email suffers.

- Can be infected with viruses and worms
- Web beaconing
- Spam over Instant Messaging (SPIM)
- Spam over Internet Telephony (SPIT)

There is no one technique that will be a complete solution to the spam problem. Filtering the messages out and preventing them from ever entering the network is the most effective method of dealing with the problem.

- Implement a network spam filter
- Configure SMTP relay
    - Blacklisting
        - Track down spammer by recording the email's SMTP ID number and IP address
        - Place the IP address on the blacklist if it's the confirmed spammer and not merely an intermediate server
    - Whitelisting
- Block HTML formatted emails

URL Hijacking
URL hijacking is wen an unethical actor registers a web domain with a name very similar to a legitimate organization.

- Similar sounding

Example:

- Real website: comptia.org
- URL hijack: comptia.biz

Typo Squatting
Typo squatting is when an unethical actor registers a web domain that is similar to a legitimate web domain but slightly misspelled.

- Slight misspelling

Example:
- Real website: google.com
- Typo squatting: gooogle.com

Clickjacking
Clickjacking employs a maliciously crafted webpage that hides clickable content under normal content. A portion of the clickjacking content is visible and when clicked, causes a click event at some other website.
- Often is used to fraudulently increase an advertisement's click count at some other website

---

Malware

Virus
Malicious software designed to infect a computer file by delivering a damaging payload. It's intent is to render the system inoperable and then spread to other systems.

Indications or warning of infection:
- Programs on your system start to load more slowly
- Unusual files or appear or disappear
- File icons change to some other icon
- Program sizes change from the installed versions

Countermeasures:
- Updated anti-virus software
- Enforce least privilege management

Worms
A worm is different from a virus, as worms can self-reproduce without a host application and are self-contained programs. Worms can propagate by using email, website downloads, etc.
- Computer program that propagates on its own
- Does not need a host application to be transported
- Self-contained
- Typically exploits a flaw (such as a buffer overflow) on the host

Countermeasures:
- System hardening: remove unnecessary services to reduce potential attack vectors
- Patch management: the majority of worms exploit buffer overflows
- Maintain the anti-virus software

Logic Bomb
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.

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

Countermeasures:

- Enforce least privilege management
- Implement strong audit controls
    - Code review

Trojan horse
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.

- Social engineering attack
    - A program that is disguised as another program and tricks the person into installing it
- Might be included as an email attachment or as part of an installation program

Countermeasures:

- Enforce least privilege management
- Security awareness training

Backdoor
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 without having to authenticate. A backdoor's goal is to remove the evidence of initial entry from the systems log. A port on the victim's machine is commonly opened for the attacker to backdoor through.

- AKA maintenance hook or programming hook

Mitigation techniques:

- Install and maintain anti-virus software
- Install and enable the host-based firewall
- Enforce least privilege management
- Implement an IDS/IPS

Remote Access Trojan (RAT)
A RAT provides unauthorized remote control of another system. It typically employs a backdoor communication channel by opening a communication port on the victim's machine.

- Privilege escalation attack
- Provides the attacker with communication persistence
- AKA Illicit server
- Detectable with anti-virus software

Examples: NetBus, Back Orifice, Loki

Countermeasures:

- Enforce least privilege management
- Install and maintain anti-virus software
- Install and enable a host-based firewall
- Implement an IDS/IPS

Rootkits
"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 very high system level that the user can't see with normal software utilities. A rootkit could potentially hide from anti-virus software.

- Malware that has the ability to hide from spyware blockers, the anti-virus program, and system utilities
- Runs at the root level or with administrator level access
- Provides the attacker with communication persistence
- Uses privilege escalation to subvert the operating system's security kernel

Countermeasures:

- System hardening: reduce possible attack vectors
- System auditing: establish system file baselines
- Install and maintain anti-rootkit software

Spyware
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, passwords stored in cookies, system information, or install a backdoor.

- Software that collects information about the system, including cookies
- Spreads to machines by users who inadvertently ask for it

Countermeasures:

- Updated anti-spyware software

- Enforce least privilege management
- Security awareness training
- IDS/IPS

Adware
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.

- Frequently refers to any software which displays advertisements

Countermeasures: enforce least privilege management, security awareness training

---

Ransomware
Ransomware is malicious software that takes "control" of a system (usually through encryption) and then demands payment to a third party.

- Often delivered through a Trojan horse technique
- Often employs encryption to gain control of the system

Countermeasures:

- Enforce least privilege management
- Security awareness training
- Adopt an effective data backup schedule

Keystroke Logger
A keystroke logger is malicious software that captures and stores keys pressed on the keyboard and stores them in a file for later retrieval by the attacker.

Countermeasures: Least privilege management, IDS/IPS

Man-in-the-browser (MITB)
MITB uses a malicious browser plug-in to view or altar web page interactions. It could be used later to support a Cross-site Request Forgery (XSRF). An example would be a malicious toolbar.

Countermeasures: least privilege management, security awareness training

---

Shimming
Shimming is snippets of software code that acts as a man-in-the-middle between two system processes.

- Can redirect the system call to another location
- Can change system call parameters

Refactoring
Refactoring involves rearranging code modules or snippets of code without changing the program's functionality. Though this technique can be used for legitimate purposes, an attacker might use refactoring in their malware to make it difficult to reverse engineer the malware. Tracing through the code is purposely made to be confusing and hard to follow.

Overall countermeasures to malware:

- Security awareness training: train personnel in the issues
- Enforce least privilege management
    - Restrict a user's ability to install software or make system changes
    - Restrict the use of mobile media such as USB-based storage devices
- Adopt an effective system security posture
    - System hardening: disable unnecessary ports and services to reduce the attack surface available to attackers
    - Patch management: fix the discovered flaws
    - Install and maintain antivirus software: use a defense-in-depth approach in conjunction with vendor diversity
    - Install and enable host-based firewalls

Network Attacks

Spoofing Attack
Spoofing is a situation in which one person or program successfully masquerades as another by falsifying credentials. Spoofing is an impersonation attack.

Examples:

- MAC spoofing: forging the source address of a network frame
- IP address spoofing: forging the source IP address of a TCP/IP packet
- Email spoofing: forging the "From" field of an email
- Caller ID spoofing: forging the phone number of the caller
- Web spoofing: creating a convincing but false copy of a website
- Biometric spoofing: obtaining a biometric sample of a legitimate person to bypass a biometric device

---

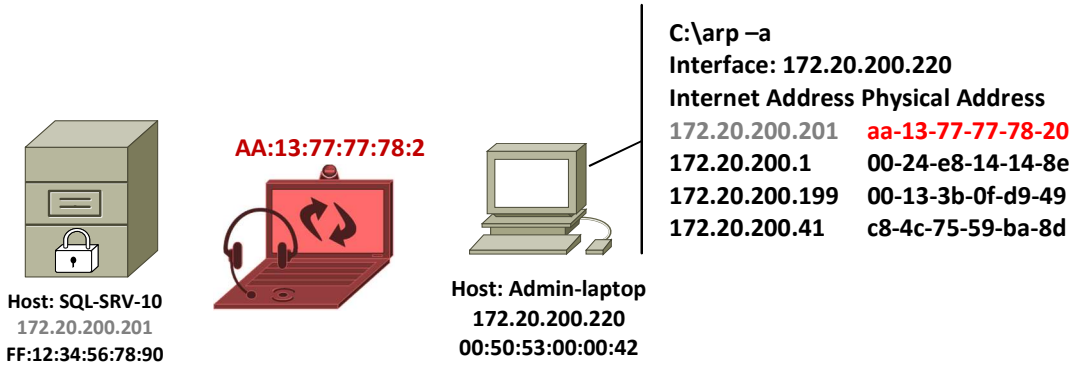
Man-in-the-Middle Attack

The attacker sits between two communicating systems and sniffs the conversation. This can allow the attacker to steal files or glean sensitive information from the network. The attacker could modify the information and then forward the tampered message to the other endpoint. A Man-in-the-Middle attack could be something simple as sniffing the network or it could escalate into modifying or stealing data.

Countermeasures: SSL, TLS, VPN tunneling protocols (IPsec)

ARP Poisoning Attack

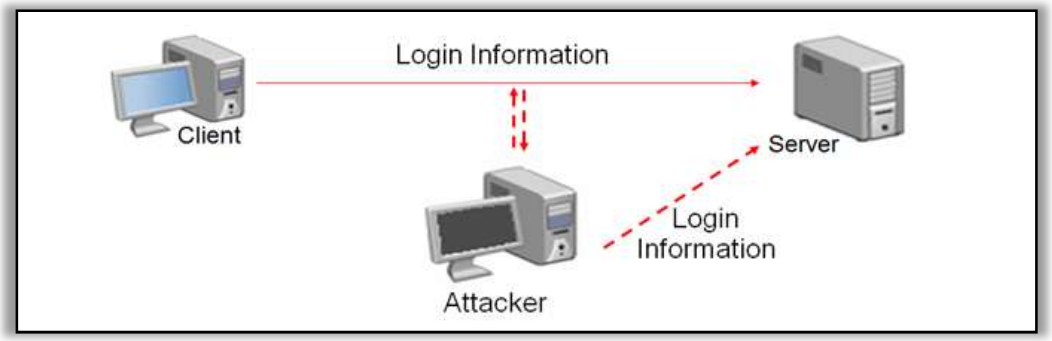
An ARP Poisoning attack is when the attacker is able to respond to a victim's ARP request before the legitimate machine can respond. The victim's ARP table has a MAC address entry belonging to the attacker. When the victim wants to communicate to a server or a gateway, they actually communicate to the attacker instead.



Replay Attack

A replay attack is 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 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: multifactor authentication, encrypted timestamps, OTP

Downgrade Attack
An attacker manipulates the security negotiation phase between two endpoints so that a weaker encryption package is chosen.

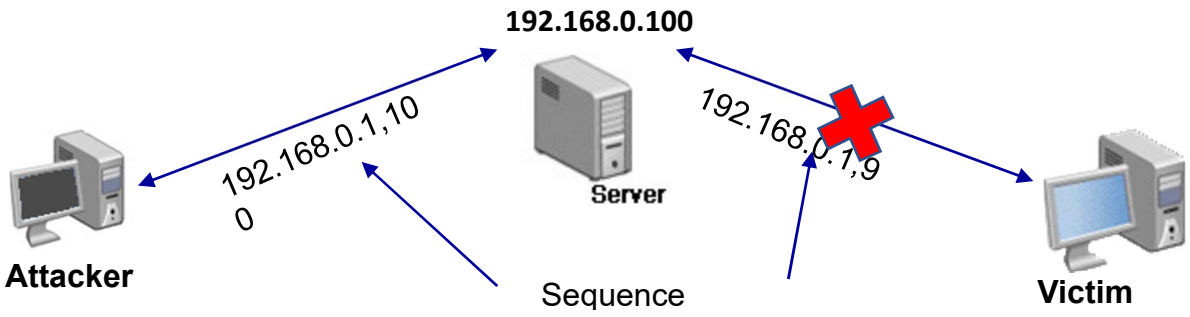
Examples:

- Implementing DES instead of AES
- POODLE attack tricks a web server and web browser to downgrade from TLS 1.0 to SSL 3.0 and then exploits the flaws in SSL to gain access to the session key

---

Session Hijacking
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.

- Takes control of an active TCP session by using sequence number guessing



Countermeasures: “Random” sequence numbers, encryption, MAC/HMAC/CBC-MAC

Denial of Service (DoS)
A system is attacked in a way so that it is no longer available to be used by an authenticated and authorized user. The goal in DoS is not to destroy anything but to compromise availability. Often the attack method is designed to exhaust a victim’s resources so that it is too busy to respond to legitimate traffic.

Examples:

- Domain hijacking
- DNS poisoning
- Zero day attack

Domain Hijacking
Domain hijacking is when an unethical actor registers the domain name of an organization as soon as it expires. The once trusted domain can now be used for phishing attacks and credential stealing

- Form of web spoofing

Countermeasure:

- ICANN sets a 60-day grace period for ownership transfers of domain names
- Develop a more cognizant auditing cycle

DNS Poisoning
DNS is poisoned when false address information is recorded in the Domain Name System either at the local machine’s host file or the DNS server’s DNS table.

- DNS cache poisoning specifically relates to the DNS server
- Exploitation of TCP port 53 traffic

Countermeasures:

- Enable DNSSEC in the DNS server to produce and accept only digitally signed updates
- Enable TSIG within an enterprise LAN
- Enforce least privilege management

Zero Day Attack
A zero day attack is when malicious code exploits a flaw (such as a buffer overflow) to which a fix for the flaw does not exist.

- Vendor doesn't know about the flaw, so the fix doesn't exist
- Vendor knows about the flaw, but hasn't created a fix yet

Countermeasures:

- Code review
- Patch management
- Anomaly detection

Distributed Denial of Service (DDoS)

DDoS is a general attack method that uses multiple attackers to prevent access to resources that authenticated and authorized users should be able to get access to.

- It often uses resource exhaustion techniques
  - Network bandwidth
  - Processor bandwidth
  - Memory race conditions
- Amplification: a neutral system is used to broadcast the attack

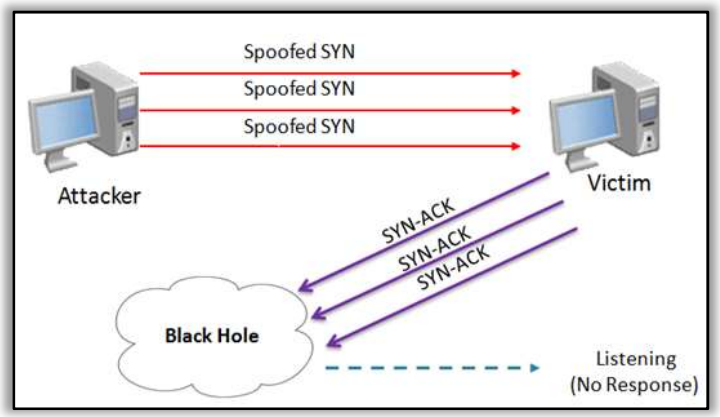
Examples of DDoS attacks:

- SYN Flood attack
- Smurf attack
- Fraggle attack
- Botnet attack

TCP SYN Flood

Multiple attackers send a succession of SYN requests to a target but never let the TCP 3 way handshake complete. The victim is left with a barrage of half open TCP connections.

- Can be mitigated by using Stateful Packet Inspection (SPI) firewalls
- Does not work with SCTP's 4-way handshake



TCP needs to synchronize the sequence numbers exchanged between two communicating systems. A normal TCP 3-way handshake connection process:

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.

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

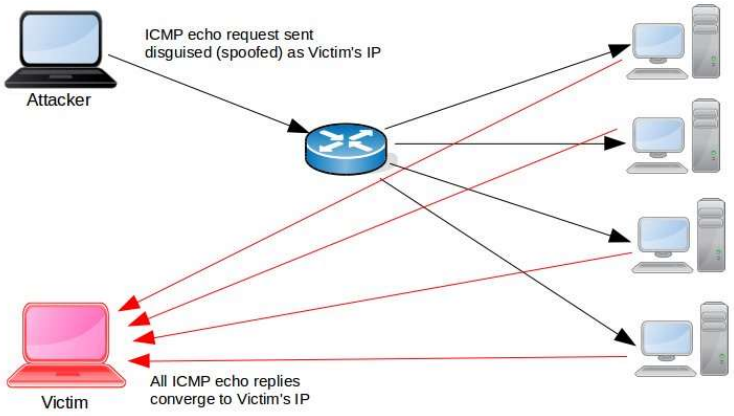
- A malicious client can skip sending this last ACK message
- Attacker can spoof the source IP address in the SYN
    - The victim sends the SYN-ACK to the falsified IP address, and thus never receives the ACK.

In both cases, the server will patiently wait for the acknowledgement (simple network congestion could also be the cause of the missing ACK). The more half open connections on the victim machine, the less memory available to the rest of the operating system. The victim will either experience significant delays or experience a system failure - Blue Screen of Death (BSoD).

Smurf Attack

In a smurf attack, an attacker sends a large amount of ICMP echo requests (ping) traffic to a network's broadcast address, 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.

- ICMP is used in the attack
- Source IP address is spoofed to the victim's IP address
- Amplification: router amplifies the attack by delivering the ICMP Echo Request to the broadcast address



Countermeasures:

- Apply an anti-spoofing filter at the network perimeter
- Network Intrusion Prevention System (NIPS)

Fraggle Attack

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.

- UDP is used in the attack
- Source IP address is spoofed to the victim's IP address
- Amplification: router amplifies the attack by broadcasting the UDP datagrams

Countermeasures:

- Apply an anti-spoofing filter at the network perimeter
- Network Intrusion Prevention System (NIPS)
- Disable unnecessary UDP ports

Botnet Attack

A malicious architecture of compromised systems used for delivering malware, Spam or DDoS attacks.

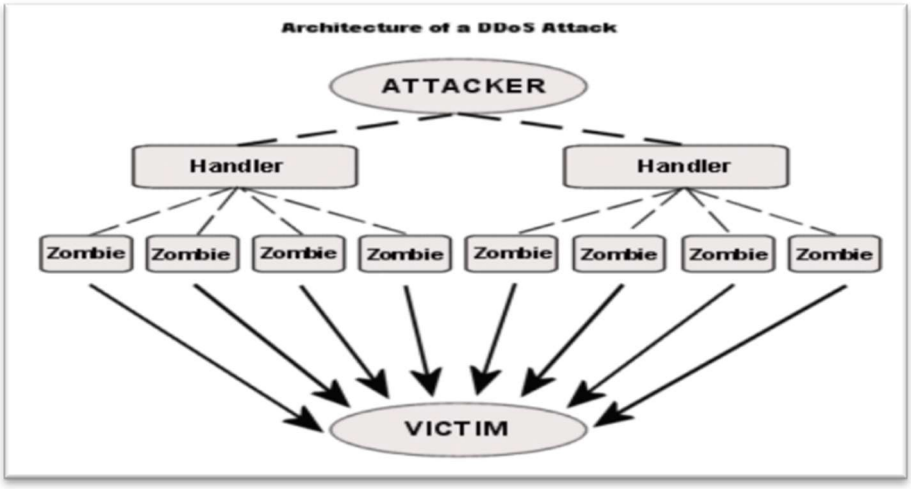
- Internet Relay Chat (IRC): common protocol used for the attack orders
- Handlers: compromised intermediary machines that communicate to the zombies
- Zombie: Compromised machine that attacks the victim
- Bots: Small programs that run automated tasks
    - Compromised systems obey a master or author of the code
- Botnets: the collection of zombies that adhere to a hierarchical command and control architecture

These attacks exploit the inherent weaknesses of dedicated networks such as cell phone, DSL, and cable service providers. 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 master controller is the attacker's computer. The systems taking direction from the master control computer are referred to as handlers. Handlers will forward the attack instructions to the zombies. Zombies merely carry out the instruction they've been given indirectly 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 return to its dormant state.



Botnet army illustrated

Password Attacks

Password Cracker

A password cracker is a computer program that attempts to discover the plaintext password from a password hash. It's a cryptanalytical attack using one of three techniques: brute force, dictionary, or rainbow tables.

Examples:

- Cain and Abel: windows-based cracker
- John the Ripper: Linux-based command-line cracker
- Ophcrack: Linux-based rainbow table cracker
- RainbowCrack: rainbow table cracker

Brute Force Attack

A brute force is accomplished by applying every possible combination of characters that could possibly be used. This tends to be the most time-consuming manner to attack passwords.

- Online brute force attack: the attack is performed within the session
    - More easily identified by detection sensors
- Offline brute force attack: the encrypted password has been obtained and is attacked within the attacker's zoo
    - More challenging to detect but the attacker must have a copy of the encrypted password

Countermeasures:

- Establish clipping levels: lockout controls
- Establish a password lifecycle

Dictionary Attack

Using a dictionary of common words to reveal the user's password

- Footprinting can be used to make the dictionary attack more effective

Countermeasures:

- Use strong passwords
- Entropy: password complexity

Rainbow Tables

A rainbow table is a hash lookup table used to recover an unknown password using its known cryptographic hash. It allows recovering the plaintext password from a password hash generated by a hash function.

- AKA Rainbow cracking
- A list of hashes

Countermeasure:

- Salt: a random value is calculated into the hashing process which adds more complexity to the hash digest

---

Birthday Attack

The Birthday Attack is derived from the birthday paradox: 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 within hash algorithms.

Countermeasure:

- Salt: a random value is calculated into the hashing process which adds more complexity to the hash digest

---

Pass the Hash

Pass the Hash is a replay attack used against an operating system that uses the NTLM authentication service within a network. Microsoft operating systems are vulnerable to this type of attack.

- Authentication packet containing the NTLM password hash is captured and then replayed by the attacker
- Provides an impersonation attack

Wireless Attacks

Rogue Access Point
A rogue access point is an unauthorized wireless access point that has been installed on a company network. It can be used to bypass the organization's security appliances, especially firewalls and content filters

- Ad hoc in nature (someone's cell phone with hotspot capability)
- Unauthorized SSID, Unauthorized BSSID(MAC)

A Wireless Intrusion Prevention System (WIPS) can be used to disassociate the wireless client from the rogue AP so that an effective connection is never established

- WIPS supports sandboxing

Evil Twin
An attacker can use their wireless device to masquerade as one of the wireless network's Access Points. This effectively turns the attacker's laptop into a false gateway.

- 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
- Authorized SSID, Unauthorized BSSID(MAC)

Evil Twins can be used as part of a Man-in-the-Middle attack.

- Attacker can eavesdrop; possibly collect usernames and passwords, etc.

Countermeasures:

- WIPS can sandbox by issuing disassociation frames
- Mutual authentication

Disassociation Attack
Attack spoofs the Access Point and sends a disassociation management frame to the victim causing the victim to disassociate from the WLANs Access Point.

- Victim gets kicked off the WLAN

Countermeasure: WIPS

Interference
Unintentional conflicting signals that cause degradation to the wireless architecture

Common sources of interference:

- Cordless phones
- Baby monitors
- Microwave ovens
- Competing 802.11 devices
- Bluetooth devices (2.4 GHz)

Jamming
Intentional conflicting signals that cause degradation to the wireless architecture

- Caused by attackers

Bluetooth Attacks
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. In order to properly target a phone, a directional antenna should be used.

Bluebugging
In a Bluebugging attack, the target phone is taken over by the attacker. The attacker can have incoming calls forwarded to their phone so they can eavesdrop on the conversation. Also, the attacker would be able to make calls through the compromised phone, using up the victim's minutes instead of their own.

Bluejacking
Bluejacking is the sending of unsolicited messages to Bluetooth- enabled devices such as mobile phones, PDAs or laptop computers. A barrage of messages could degrade performance of the device. The unsolicited messages can be customized leading to social engineering opportunities

Bluesnarfing
Bluesnarfing is the unauthorized access of information on a Bluetooth-enabled, wireless device. This allows access to the calendar, contact list, emails, private files such as pictures and videos, or text messages stored on the device.

- Data loss

Near Field Communication (NFC)
NFC is a wireless communication standard used with mobile devices to provide easy communications between two devices. It performs device-to-device automatic synchronization and association just by touching the devices together. Data can be easily exchanged.

NFC does not provide encryption or any kind of security services. The data can easily be captured, manipulated, or replayed at a later time.

- Could be classified as a compromising emanation

Radio Frequency Identification (RFID)
RFID is an IC chip technology that can transmit a weak signal within a few meters. It can be used in Electronic Access Control (EAC) such as proximity cards or for asset tracking such as RFID tags.

RFID does not have encryption service capabilities. It is prone to eavesdropping and a wide gamut of man-in-the-middle attacks.

Countermeasures:

- Faraday cage
- Faraday sleeve

Application Attacks

Privilege Escalation
Privilege escalation occurs when a subject is able to modify their access restrictions to gain more or different capabilities. It is a violation of least privilege management. The most common method used to escalate privileges is through social engineering.

- Vertical privilege escalation
    - Lower privileged subject (end user) accesses functions or content reserved for higher privilege subjects (administrator)
    - Maintenance hooks left in software
    - Rootkits
- Horizontal Privilege Escalation
    - Normal user accesses functions or content reserved for other users at the same security level
    - Can be a form of impersonation attack

Countermeasures: strong access controls

Buffer Overflow
More information is placed in a buffer (memory stack) than it can hold, which then overflows into the next buffer.

- Writes data beyond the allocated memory space
    - Attacker can create a DoS issue
        - Application service can be terminated

        - System crash
    - Attacker can run code with elevated privileges

Countermeasures:

- Code review
- Input validation
- Patch management
- Fuzzing

Integer Overflow

Like a buffer overflow, involves putting too much information into too small of a space.

- Example: Using 8 bits, it is possible to express any number in binary from 0-255. If only 8 bits are set aside and the user enters a value of 256 to be converted to binary, it exceeds what can be stored and results in an integer overflow
- Can lead to data corruption or DoS

Countermeasure: bounds checking

Pointer Dereference

The attacker manages to arbitrarily move the logical memory pointer to a different location in memory. This allows access to the data in that memory location (data disclosure).

Countermeasures:

- Input validation
- Use local variables instead of global variables in software code to maintain stricter control of the memory variables

---

Race Condition

A race condition is a situation where the attacker is able to successfully manipulate multiple processes in a way that accomplishes the attacker's goal. It could simply be for the purpose of resource exhaustion.

Example: an attacker is able to skip to the authorization step before the authentication step has been completed.

Countermeasure:

- Secure software design: don't split up critical tasks (such as access control steps) into separate asynchronous processes

---

Memory Leak
A program requests memory to be allocated from the memory heap but never releases the memory when it is no longer needed. Either the offending software is malicious (logic bomb) or the software is poorly written. When the host machine runs out of memory it will cause a system crash.

- Blue Screen of Death (BSOD)

Countermeasures:

- Code review
- Reboot the operating system
- Implement a garbage collector

DLL Injection Attack
An attacker can use a malicious dll file to gain system-level privileges. The dll file gets loaded at boot time. Ultimately, this can lead to a data disclosure attack later.

- Dynamic Link Library (DLL)

Countermeasure:

- Implement secure boot and attestation services: verifiably trusted modules get loaded at boot up time
- Whitelisting

SQL Injection
SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.

As long as injected SQL code is syntactically correct, tampering cannot be detected programmatically. Therefore, you must validate all user input and carefully review code that executes constructed SQL commands in the server that you are using.

Code injected into a database via a web form allows an attacker to query data from the database.

- User ID = ‘ ‘ or 1=1;

Example 1: If this command was executed remotely by the attacker, what would happen?

```
SELECT email, passwd, login_id, full_name
  FROM members
 WHERE email = 'x'; DROP TABLE members; --';  -- Boom!
```

Answer: it would delete all of the member information from the member's field.

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).

```
SELECT email, passwd, login_id, full_name
  FROM members
 WHERE email = 'x';
       UPDATE members
       SET email = 'steve@unixwiz.net'
       WHERE email = 'bob@example.com';
```

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

LDAP injection is a specific form of attack that can be employed to compromise Web sites that construct LDAP 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.

- 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

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 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.

When a user has the ability to add structured XML as input, they 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.

Here is an example:

1. The price of the widget is 500.00 for 1.

```
<item>
        <description>Widget</description>
        <price>500.00</price>
        <quantity>1</quantity>
</item>
```

2. Malicious individual inserts a string to line 4, with this input.

```
1</quantity><price>1.00</price><quantity>1
```

3. A parser interprets the input and resolves the second price, overriding the first. The widget now costs 1.00 for 1.

```
<item>
        <description>Widget</description>
        <price>500.00</price>
        <quantity>1</quantity><price>1.00</price><quantity>1</quantity>
</item>
```

Cross-Site Scripting (XSS)

XSS is a type of injection attack typically used against web applications that fail to filter malicious code before it is submitted to the service's interface. Users' web browsers are manipulated when they render the injected malicious code within the web page.

- Vulnerability where an attacker can add comments/code to web pages which allows code injection
- Code could redirect valid user data to the attacker
- Code could redirect the user to a malicious website owned by the attacker

Safeguards:

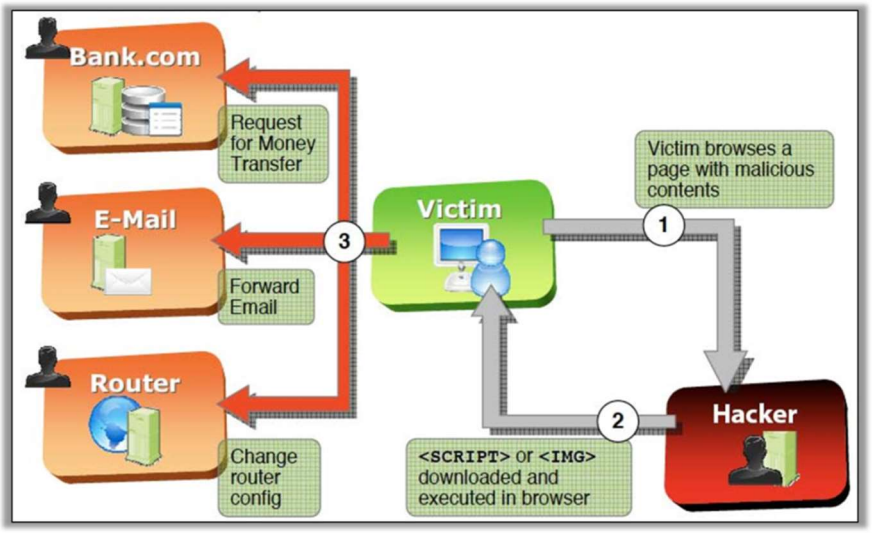
- Input validation (phone number – server side routine could remove all character other than digits).
- Install a Web Application Firewall (WAF)
- Set web apps to tie session cookies to the IP address of the original user and only permit that IP to use the cookie.

Cross-site Request Forgery (XSRF)

An XSRF attack is where a user is tricked into interacting with something malformed within a legitimate web page that then performs a malicious act on another website. Usually the website that receives the action request is a website the user had previously viewed and had logged into. A cookie with the user's credentials still exists and is used to automatically provide the authentication steps in the background.

Countermeasures:

- Strong authentication
- Code review
- Verifiably correct web server pages
- Proper cookie destruction



XSRF Illustrated

Domain – Architecture and Design

CompTIA SY0-501 domain objectives covered:

- CompTIA domain 3.1: Explain use cases and purpose for frameworks, best practices, and secure configuration guides
- CompTIA domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security
- CompTIA domain 5.7: Compare and contrast types of controls
- CompTIA domain 3.4: Explain the importance of secure staging deployment concepts
- CompTIA domain 3.6: Summarize secure application development and deployment concepts
- CompTIA domain 3.3: Given a scenario, implement secure systems design
- CompTIA domain 3.7: Summarize cloud and virtualization concepts
- CompTIA domain 3.8: Explain how resiliency and automation strategies reduce risk
- CompTIA domain 3.5: Explain the security implications of embedded systems
- CompTIA domain 3.9: Explain the importance of physical security controls

---

IT Governance Frameworks

Regulatory frameworks

Regulatory frameworks are compulsory because they relate to governmental law.

- Penalized if not adhered to

Examples: HIPPA, SOX, FERPA

Non-regulatory frameworks

Non-regulatory frameworks are non-compulsory so they serve more as guidelines.

- Organizational guides

Example: COBIT

National frameworks

National frameworks are created with a specific country in mind and begin to lose their relevance during offshoring situations.

- Country-centric

Examples: FISMA and NIST SP-800 series pertain to the U.S. government

International frameworks

International frameworks are developed without bias towards a specific country. They are developed with global situations in mind.

- Recognized globally

Example: ISO 27000 series

Industry-specific frameworks
Industry-specific frameworks are created with a specific industry as its focus. They can be either government or industry enforced.
Examples:

- SOX is government enforced and pertains solely SEC financial reporting regulations
- PCI-DSS is industry enforced and pertains to the handling and processing of credit card data

---

Service Level Agreement (SLA)
The SLA is essentially a business contract between a client and a service provider, such as an Internet Service Provider (ISP). Of all the IT-related legal documents, it holds the greatest legal weight. Often non-compliance of the requirements may lead to a lawsuit.

- Establishes minimum required performance baselines such as network throughput, processing thresholds, RTO/RPO, and other contract deliverables

---

Interconnection Security Agreement (ISA)
The ISA is a legal document that specifies the technical security requirements for the data being exchanged between two organizations. It may specify certain encryption standards or VPN tunneling protocols to be used.

- Focus is on protecting data-in-transit

Memorandum of Understanding (MOU)
An MOU is an informal agreement on paper that states the goals and responsibilities between two or more organizations. The purpose of the document is not to penalize but to minimize misunderstandings of responsibilities. It may also be referred to as a Memorandum of Agreement (MOA).

Business Partnership Agreement (BPA)
A BPA is a formal agreement between business partners that defines each party's responsibilities within the partnership. It typically defines the allocation of certain responsibilities and profits.

- Defines profit sharing parameters

Non-Disclosure Agreement (NDA)
The NDA is a formally signed document that establishes confidentiality of proprietary information and sensitive interactions between two entities. It is in essence an agreed gag order.

An NDA must be signed before a person gains access to sensitive information. It is also a best business practice to have the person sign the NDA again during their exit interview.

Change Management
Change management needs to be policy driven. A formal policy defining the change control process should be established.

Change Control includes three basic stages:

1. Request stage: cost-benefit analysis is done
2. Change stage: version control is established and the new product begins development
3. Release stage: product is implemented and documented

Changes may affect certification and accreditation. It may also introduce new risk so a risk assessment needs to be performed.

Privacy Policy
The privacy policy defines the reasonable levels of privacy that employees can expect. It focuses on what the subject is doing. For example, will the company be listening to the telephone when an employee dials a phone number belonging to a personal contact, not a business contact? The privacy policy establishes the founding security goals of accounting.

- Subject-centric

The privacy policy must be formally acknowledged by those being monitored through some form of non-repudiation:

- Paycheck signature on a hardcopy privacy policy
- Digital signature on a softcopy privacy policy

Acceptable Use Policy (AUP)
The AUP defines the conditions in which company resources may be used. It focuses on the authorization of company-owned objects. For example, can an employee use a company-owned telephone to make personal phone calls? The AUP establishes the ground rules of behavior for interacting with company resources.

- Object-centric

The AUP must be formally acknowledged by company employees through some form of non-repudiation:

- Paycheck signature on a hardcopy AUP
- Digital signature on a softcopy AUP

Policy elements:

Establish an overall clean desk policy

- Ensure company resources are positively controlled by locking items in physical security containers

Enforce least privilege management

A subject should only have enough permissions to do their job, no more, no less.

- Auditing must support the monitoring for privilege escalation attacks

Mandatory vacations

Personnel in sensitive positions can be selectively required to go on vacation in an attempt to discover the perpetrator of fraud. While the person is on vacation, suspend their right.

- Detective control

Rotation of duties

Personnel should rotate their duties over a period of time. This can aid in detecting adverse actions, but also deter employees from committing adverse actions.

Separation of duties

Tasks and roles within a company need to be partitioned to help mitigate the effectiveness of adverse actions by company employees. By not allowing one person to fulfill multiple duties, damage control can be enhanced if that employee chooses to turn rogue.

- Auditing must support the monitoring for privilege creep

Hiring

During the hiring process background checks should be conducted. Excessive debt and felony activity would be serious warning flags.

Training

The organization should include in their policies the topic of on-going training. Certain professional fields require a license or certification to remain active for the employee to participate in their vocational field. Continuing education might be required to support the quickly changing skillsets in Information Technology.

Policy violations

State the penalties for policy violations within the policies themselves. At one point might someone's rights be suspended or the employee terminated due to adverse actions?

Employee termination
When an employee's time with the company has been terminated (whether they quit or are fired) certain steps need to be performed.

- An exit interview should be conducted and during the exit interview the employee's permissions should be disabled
- Have the employee re-acknowledge the NDA

Security Model

CIA Triad Model

- Confidentiality: achieving and maintaining secrecy
  - Deny read
- Integrity: achieving and maintaining trust
  - Deny write
- Availability: maintaining timely access
  - High availability (99.999% uptime)
  - Implementing redundancy and fault tolerance solutions

Data States

- Data-in-transit: data being passed through a network
  - Protect with physical security, ACLs, TLS, VPN tunnels
- Data-at-rest: stored data
  - Protect with access control permissions, data backups, whole disk encryption, and file-level encryption
- Data-in-use: data being processed
  - Protect with system hardening, secure baselines, application whitelisting and blacklisting

Implement the CIA triad within each data state.

Security Control Categories

Administrative controls
Administrative controls are designed to shape human behavior. They are used as an overarching starting point for security. Administrative controls are sometimes called management controls.

Examples:

- Organizational security policy
- Privacy policy
- AUP policy
- Password policy

Technical controls
Technical controls work at the individual bit level. They are sometimes called logical controls.

Examples:
- Encryption protocols
- Firewall ACLs
- Authentication protocols
- File system permission bits

Operational controls
Operational controls focus more on the day-to-day activities of the organization. They help ensure that equipment continues to work as specified.

Examples:
- Data backups
- Security assessments
- Incident response
- Computer forensics

Physical controls
Physical controls focus on physical security and the safety of personnel.

Examples:
- Security guards, mantraps, and turnstiles
- Fences, gates, and cages
- Cable locks, padlocks, and keys
- Lighting

Security Control Types

Preventative controls
A preventative control is designed to neutralize an attack and keep it from proceeding. To get past a preventative control, an attacker would have to exploit some flaw in the control.

Examples:
- Proximity card
- Mantrap
- ACLs
- Encryption

Detective controls
A detective control aids in the monitoring of attacks. The monitoring could be real-time or a historical recording of events that can later be reviewed.

Examples:

- Closed Circuit Television (CCTV)
- System log files
- Intrusion Detection System (IDS)
- Keystroke monitoring

Corrective controls
A corrective control is designed to re-establish the compromised baseline of the resource.

Examples:

- Anti-virus software
- Portable CO2 bottle
- Halon
- Uninterruptible Power Supply (UPS)

Deterrent controls
A deterrent control is designed to discourage an attacker from attacking. The attacker would still have a choice to proceed or not though.

Examples:

- Lighting
- Barking dog
- Speeding ticket
- Privacy policy

Recovery controls
A recovery control will re-establish a failed process or bring controls back to regular operations.

Examples:

- Alternate processing site
- Data backups
- Snapshots
- Continuity of Operations Plan (COOP)

Compensating controls
A compensating control is a control implemented solely to give additional support to another control in which some gap exists. It reinforces other controls and is usually temporary in nature due to some recent heightened threat.

Examples:

- Defense in depth
- Sandboxing
- Temporary port blocking
- Temporarily disabling a service

Defense in depth
The concept that one control by itself is not sufficient, but multiple, linearly layered security controls provide a more effective security posture.

- Practice security control diversity: deterrent, preventative, detective, corrective, recovery, and compensating controls
- Practice vendor diversity: one universal flaw won't compromise everything

---

Software Development

Software Development Models
Project management development models used in software engineering cover areas from conceptual design to software coding to end-of-lifecycle phases.

Popular development models:

- Waterfall model
- Agile model

Waterfall model
The waterfall model is a highly structured model that uses rigid linear stages for development. All requirements of the current phase must be completed before graduating to the next phase of development. If an issue was discovered in the previous phase, there is no going back to that phase.

Stages of development:

1. Requirements phase
2. Analysis phase
3. Design phase
4. Development phase
5. Testing phase
6. Maintenance phase

The waterfall model maps well to legal stages in the court room or construction stages in the construction industry, but not so well for software development.

Agile model
The agile model is the model more appropriate for software development projects. It allows the software requirements and the solutions to those requirements to evolve as the project progresses. Collaboration between the developers and the customer occur throughout the project.

- Embraces adaptive planning
- Supports continual improvement
- More flexible to mid-development change requests

Development and Operations (DevOps)
DevOps is a set of practices designed to minimize the time to make changes and the time to implement those changes. DevOps uses the agile model to synthesize collaboration between the software development team, the quality assurance team, and the operations team.

- DevOps mantra: do it quickly, do it well, and do it right the first time

Establish software module baselines
Use version control to incrementally move a software project forward. Rollback to a previous module version to tweak the software or answer what if questions.

Automate security testing
Use controlled repeatable security tests to compare the actual test results to predicted test results to help discover undesirable behavior.

Continuous integration
Establish scheduled checkpoints (scrums) so modularized code segments from various teams can be merged with the main overall code.

Source code

- Code written and readable by a computer programmer
- May include comment information from the programmer

Compiled code

- Code that has been compiled by a compiler and is readable by a computer
- AKA machine code

Runtime code

- Code that is ready to be ran by a computer and runs within its own process space
- Compiled code or script code

Software Development Kit (SDK)

- Package of code libraries, debugging tools, coding environment, and compiler designed for a specific kind of architecture
- Code libraries could have flaws that causes flaws in the developed code
- Must remain proactively aware of potentially needed patch deployments
- Examples: Microsoft Visual Studio, Java SDK

Code reuse

- Reusing snippets of code from previously developed software
- Helps speed up the software development process
- Flaws in the old software is ported over to the new software
- Could lead to dead code if not properly pruned

Using third-party code

- May contain undesirable unknowns
- Must remain proactively aware of possible future patch downloads
- May be restricted by copyright limitations

Cryptographic modules

- Subsystem that provides encryption services to an application
- Example: Microsoft CryptoAPI (CAPI)
- Package includes algorithms that the application can specify and key management

Cryptographic Service Provider (CSP)

The cryptographic module being used must remain verifiably trustworthy.

- Digitally signed

A cryptographic service provider (CSP) contains implementations of cryptographic standards and algorithms. At a minimum, a CSP consists of a dynamic-link library (DLL) that implements the functions of a cryptosystem.

Exception handling

Exception handling ensures that the code can handle alternate behaviors so the program doesn't crash. It is necessary to present the code with a wide spectrum of invalid or unexpected inputs by using software fault injection and mutation testing techniques (fuzz testing).

- A mechanism designed to handle the occurrence of exceptions that change the normal flow of program execution

- Try{} catch() {} statements
    Try{} catch() {} analogy:
    Try {Ringing the doorbell}
    Catch(error message of “no doorbell”) {Knock loudly}

Error handling

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.

- Error handling
    - Takes place during the execution of a program
    - Adverse system parameters or invalid input data are often the cause

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.

When an error occurs, a generic message should be presented to the user, but a detailed message should be written to the logs.

Memory management

- Check the size of the data before allowing it to enter a memory buffer to mitigate the chance of a buffer overflow
    - Bounds checking
- Computer code scope:
    - Computer code comprises of methods and variables

Methods and variables declared as “public” are available for access outside of the program

- Example: public char[] SSN; declares a string of characters labeled SSN as a memory variable that would be accessible from an external computer program.

Methods and variables declared with “private” can only be used within the program

- Example: private char[] SSN; declares a string of characters labeled SSN as a memory variable that would be accessible only within the computer program that declared it.

Input validation checks

Input validation is the programmatic means of sanitizing data before it is offered to an interface so that harm doesn't occur.

- Improper length checking could lead to buffer overflows
- Improper values can lead to poor quality of data
    - Example: non-email formatted characters in an email address field
- Improper characters can lead to injection attacks
    - Various special characters (%, ‘, “, =, <, >, *, ?, etc) should not be allowed into an input field

---

Client-side vs. server-side input validation checks

Input validation must be performed as close to the data store as possible so it has to be done at the very least at the server's interface (server-side).

- Client-side can be used for pre-sanitization
- Client-side input validation can be disabled by the client
- Successful client-side validation checks can be maliciously modified during a man-in-the-middle attack
    - Mitigate with SSL/TLS encryption

Fuzzing

The software application is subjected to an unusually large number of requests with varying data types and data sizes which can help discover buffer overflow issues.

- Stress testing: performance testing that verifies expected throughput and capacity rates are met
- Model verification testing: Tests every possible state of the application
    - Helps determine unexpected fail-state conditions

Static code analysis

- Reviewing the source code looking for logic and syntax errors
- Code review usually performed by an alternate computer programming team, such as a debugging team

Dynamic code analysis

- Runtime analysis that includes normal and abnormal data inputs and analyzing the output
- Helps discover run-time errors

Secure System Design

Baselines
Baselines are critical to anomaly detection because they are something that can be compared or measured against to help recognize undesirable behavior. Anomaly detection helps discover zero-day attacks.

Security baselines
Security baselines implement security controls such as technical controls (hashing), corrective controls (antivirus software), etc.

- Minimal level of security
- Implement layered security controls

Performance baselines
Performance baselines help discover latency issues, normal protocol activity during certain parts of the day (2pm versus 2am), or expected performance capabilities based upon certain specifications, etc.

- Utilizes benchmarking and statistics

Configuration baselines
Configuration baselines help mitigate misconfigurations, attack vectors, etc.

- Remove default configurations
- Implement whitelisting and blacklisting techniques

Trusted operating system

1. Install trustworthy hardware
2. Utilize verifiably correct firmware and software
3. Perform system hardening
    - Remove unnecessary ports and services
    - Disable default accounts and configuration settings
    - Implement patch management
    - Enforce least privilege management

Maintain trustworthiness

- Conduct periodic vulnerability assessments
- File integrity checker: helps discover zero-day attacks (though the name and location of the file might be correct, it still could be malware)

Root of trust
The concept of software relying on trustworthy firmware to stay trustworthy, and firmware relies on trustworthy hardware, so the baseline of trust has to start with trustworthy hardware.

- Hardware can't be modified by software

Use a secure design approach

- Secure validation
- Tamper resistance
- Secure initial program load
- Secure storage
- Key management

Implement trusted firmware
Trusted firmware uses cryptographic checksums to ensure the firmware architecture hasn't been compromised. File integrity checks help discover zero-day attacks. Though the name and location of the file might be correct, it still could be malware.

- Process of verifying the firmware is trustworthy through the use of cryptographic checksums
- Software will not be secure if the underlying firmware has been compromised
- Needs to be performed at load time to maintain a trusted operating system
- Part of the root of trust concept

Secure boot process
Ensuring the Initial Program Load (IPL), the operating system bootloader, and the accompanying operating system software is trustworthy.

- Non-Volatile RAM (NVRAM) or Read Only Memory (ROM) chips store a trusted root digital certificate that is used to validate signed code and also houses the signature database of firmware signatures
- Unified Extensible Firmware Interface (UEFI) is required
    - Digitally signed motherboard firmware that replaces the obsolete BIOS firmware
    - Secure boot must be enabled in UEFI before the operating system is installed
- Attestation: validating the firmware

Though it's not required, TPM is often used with the secure boot process.

Code signing
Software code that has been digitally signed by the software vendor.

- Appropriate for installable programs and device drivers downloaded from trusted websites to verify their integrity and proof of origin
- Must have the vendor's digital certificate to perform the validation

Code signing doesn't protect a user from poorly written software code. Furthermore, if the software is malware on the website, then it is malware that is being downloaded but with a correct cryptographic checksum.

A slip stream attack is when malware is inserted into the downloaded program during the download process.

Application hardening

Implement the concept of least functionality
Remove or disable any unnecessary modules or features from the installed software.

- Example: remove support for SSL within the browser and web server, use TLS only.

Application whitelisting
Application whitelisting is the term used for designating the software applications that are necessary to carry out the business tasks of the organization. Unlisted software might still be able to be installed but won't be allowed to execute.

- Exclusive allow list of specific applications authorized to be executed within an organization

Application blacklisting
Blacklisting prevents the installation of software based upon its name or a known signature of the executable. Organizations need to be proactive to keep the list updated.

- Exclusive deny list of applications specifically deemed unauthorized for use within an organization
- Example: anti-virus software blocking a list of malware

Patch management
Patch management is the methodical way of updating the security baseline of firmware, applications, or operating systems in order to eliminate known bugs or flaws, or to add new features and capabilities.

- Patches, hotfixes, or maintenance releases
- Service Packs
- Over The Air (OTA) updates

Patch management tools
Use patch management tools to aid in deploying and tracking patches. Use a test server to verify the patch won't cause any conflicts with the enterprise software. Roll out the patch in groups or stages in case something goes wrong not everyone is affected.

- Decentralized patch management
    - Client pulls patches from the vendor housing the patches through an installed update service
- Centralized patch management
    - Patch management server pushes patches to the endpoint devices
- Examples: WSUS, SCCM

Use a vulnerability scanner to verify that patch has been applied and the vulnerability it was designed to fix has been neutralized.

Group Policy

Group policy provides a centralized means of creating, applying, and managing system and account security restrictions across the network enterprise.

- Allows administrators to have more control over the system settings
- Hierarchical control spans from across the entire site down to an individual Organizational Unit (OU) within the company.

Site	All domains in a site replicate data with each other
Domain	Used to group objects together to make management easier and more efficient All objects share a common domain name
Organizational Unit (OU)	Grouping objects within a domain into containers Allows for finer control of objects Usually setup by departments within the company

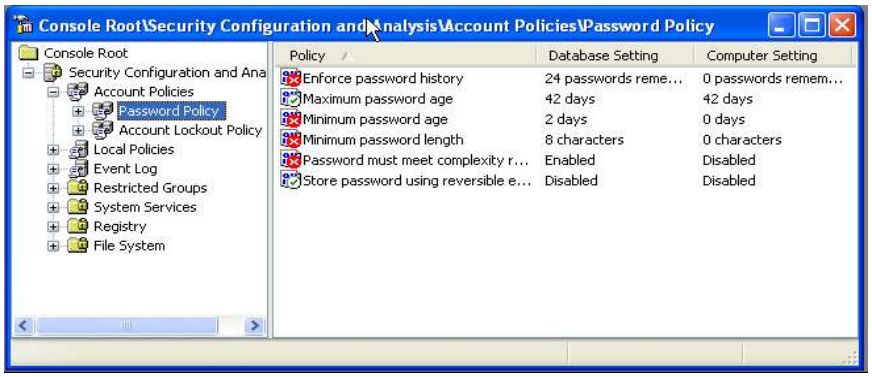
GPO inheritance:

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

Security templates enhance the security baseline on a per-machine basis.

- Decentralized deployment



Database normalization

Process of refining a relational database to reduce data redundancy and improve the integrity of the data

Example normalization levels:

- First Normal Form (1NF)
- Second Normal Form (2NF)
- Third Normal Form (3NF)

Database stored procedures

Database stored procedures can offer a performance boost over prepared statements sent from external applications.

- Prewritten functions stored within the database data dictionary
- SQL commands written to the data placeholders are treated as data instead of as SQL commands
    - Helps mitigate SQL injection attacks

Database encryption solutions

When it comes to encrypting a database, it comes down to a choice between cell-level encryption and Full Disk Encryption (FDE).

- Transparent Data Encryption (TDE) provides encryption for data without user awareness
- TDE programs account for the added overhead of encryption and key management
    - Does not encrypt data in transit

Drive encryption solutions

Encrypting a storage device is important for mobile media. The encrypted drive can help support DLP.

Full Disk Encryption (FDE)

- Software that encrypts the disk drive so it can't be read unless the decryption key is known
- Some implementations due not encrypt the boot sector of the disk

- Keys should be stored within a TPM chip

Self-Encrypting Drive (SED)

- A drive with a built-in cryptosystem within the drive controller

---

Hardware Security Module (HSM)

An HSM is a self-contained cryptosystem that can be added or removed from a system

- Provides key storage and cryptographic functions
- A removal card or external device

Examples: TPM, smart cards, SIM cards, SSL accelerator cards

SSL/TLS Accelerator

Security module card that works with servers to offload the demands of encrypting and decrypting SSL/TLS traffic from the server's CPU.

Trusted Platform Module (TPM)

TPM is a microcontroller chip typically found on the motherboard that stores keys, passwords, and digital certificates. It provides key generation, key storage and cryptographic functions commonly used by FDE.

- Contains root keys provided by the manufacturer that can be used to encrypt stored passwords and drive encryption keys
- Stores hashes that can be used with attestation services

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.

USB Security solutions

- Map the USB device to the user's profile
- USB On The Go (OTG) encryption
    - Extends FDE/SED solutions to removable media
    - Example: Microsoft's Bitlocker To Go
- Disable autoplay functionality as part of operating system hardening

Implement sanitization techniques appropriate for solid state devices when the drive's data is no longer needed. Degaussing does not work on solid state devices.

Securing peripheral devices

- Disable unused external ports
- Mobile storage devices
    - External storage devices
    - SD cards
- Digital cameras
    - Metadata embedded into the media may need to be sanitized
- Wireless keyboards and mice
- Display monitors
    - Shoulder-surfing
    - Screen savers and screen locks

Implementation Environments

Sandbox environment

- A containment environment where a potential unstable process is prevented from causing harm to surrounding processes
- Emphasis is on controlling I/O activity

Development environment

- An environment in which product concepts are turned into written code

Test environment

- An environment in which the compiled code is functionally tested

Staging environment

- An environment where a full mock-up of the projected real-world environment is used
    - Could be virtualized
- Includes testing security controls: includes stress testing and fuzzing
- Appropriate for testing patches before they are deployed to the production environment
- Alpha-stage versus beta-stage testing

Production environment

- The environment that the product interacts with live systems

While the production environment involves live data, the other environments should use dummy data or placeholder data.

Resiliency

High Availability
High availability is the goal of keeping services and systems operational even during an outage.

- Goal: Five nines availability (99.999%)
- Need to implement:
    - Fault tolerant systems: the overall system continues to operate even if it experiences a negative event
    - Hot swappable devices: devices can be replaced without having to power down the system
    - Redundant technology
    - Backup communication channels

Load Balancer
A load balancer is either a hardware device or a software program that listens for client requests. It serves as the frontend to a pool of backend systems. The load balancer forwards the client request to one of the "backend" systems that have the service the client wants so that no one single system is overloaded.

- Used to distribute workloads across multiple computers or network links
- In the event of server or application failure, load balancers can facilitate automatic failover to ensure continuous availability
- Supports high availability, elasticity, and scalability

The backend architecture is transparent to the client. The separation of functions prevents clients from contacting backend servers directly and attacking the kernel's network stack or unrelated services running on other ports.

Load balancer attributes:

Active-active load balancing

- All components are online
- Maximizes capacity

Active-passive load balancing

- Necessary components are online, the remaining are on standby
- Supports failover and elasticity

Priority Queuing

- Prioritization of one traffic type or another

Example: Quality of Service (QoS)

Server clustering

- Aggregate servers act as one server system
- Each server takes turns responding to requests

Example: Round robin DNS

Channel bonding

- Multiple physical interfaces collectively become one virtual communication line

---

Scheduling and session management

Virtual IP address

- Like services share the IP address seen by the client, but individually have their own address
- Usually involves NAT

IP affinity

- Client and load balancer session is tracked by the source IP address

Persistence

- Client and load balancer session state is tracked by a cookie

---

Data Backups

Onsite storage

- Location on site at the computer center
- Containers designed and rated for fire, moisture, and pressure resistance

Offsite storage

- Prevents the same disaster from affecting the network and the backup media

---

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 Newly created or modified files since	Yes
Differential	Backs up files which the archive bit is set to 1 Newly created or modified files since last full backup	No

Copy	Backs up all files regardless of the archive bit status Serves as a snapshot	No

Data backup types

Full-incremental backup

- Backup Characteristics
  - Fastest backup method
- Restore Characteristics
  - Restore the last full back-up, then every subsequent incremental backup

Full-differential backup

- Backup Characteristics
  - Takes progressively longer to complete
- Restore Characteristics
  - Restore the last full back-up, then the last differential backup
  - Next to a full backup, this is the fastest restore method

---

RAID

Redundant Array of Independent Disks or Redundant Array of Inexpensive Disks

- Hardware RAID is faster than software RAID

RAID Level	Description	Strengths	Weaknesses	Minimum disks
0	Data striping	Highest performance	No redundancy; 1 fail = all fail	2
0+1 (RAID 01)	"Mirror of Stripes"	Very high performance	No scalability	3
1	Data mirroring	Duplicates data on other disks	Expensive; double cost of storage	2
1+0 (RAID 10)	"Stripe of Mirrors"	Highest performance, highest data protection (can tolerate multiple drive failures)	Expensive; double cost of storage	4 (stripe and mirror to 2 sets)
3	Data striping Dedicated parity drive	Excellent performance; fault tolerance, made obsolete by RAID 5	Write requests suffer from same single parity-drive	3 (2 for striping and one dedicated parity disk)

5	Data striping Parity striping	Best cost/performance for networks. Can handle non-contiguous drive failures	Write performance is slow. Data is lost with 2 sequential bad drives.	3 (data and parity striping)
6	Data striping Double parity striping	Best for high availability systems and large storage capacity. Data survives if 2 sequential drives fail (but not 3!).	Increased cost of additional drives and parity drives	4 (data striping and double parity striping.

RAID Level	Recommended Implementation
0	High end, fast workstations
0+1 (RAID 01)	Mirrored array with high performance but no scalability
1	Used to provide fault tolerance, lower performance databases
1+0 (RAID 10)	Fast databases, application servers, virtualizations
3	Made obsolete by RAID 5 but may be used in very specialized situations
5	Data storage, web servers, web and file archiving
6	Data archives, high availability cloud computing systems

Host Architecture

Kiosks

Kiosks are terminals that provide customer self-service capabilities and are available for interaction from the general public. Untrustworthy users inherently have access to the kiosk.

- Interface may be a touch screen instead of a traditional keyboard
- Enforce the principal of least functionality
- Implement detective controls to monitor for malicious usage (monitor with CCTV)

Embedded devices

Embedded architecture is a small computer system with a dedicated function within a larger system. Due to their micro-architecture and limited resources, embedded systems lack common security features such as firewalls and antivirus software.

- Can be compromised and used within a bot army or for pivot attacks
- Examples of where embedded devices can be found:
    - Heating Ventilation Air Conditioning (HVAC)
    - Printer / Multi-function Devices (MFD)
    - Network attached camera systems such as CCTV
    - Multimedia devices (such as MP3 players, blue-ray players, smart TVs, etc.)

Real-time Operating System (RTOS)
RTOS is an operating system that is specifically designed to run with precise timing and a high degree of reliability.

- Often associated with time critical processes such as safety equipment, medical devices, stock market tracking systems, weapon systems, etc.
- Concerned less about how much work can be done, but instead when will it be completed
    - Focuses on minimal latency
- Jitter: the time variance between various tasks being completed

---

System on a Chip (SoC)
SoC houses all of the traditional subsystems inside of one IC chip, instead of how a motherboard would have separate subsystems with an individual controller chip for each subsystem.

- All-in-one CPU, GPU, RAM, DMA controller, and input/output ports
- A minicomputer inside of one IC chip
- Lower power requirements

A smartphone is a good example of SoC architecture.

Internet of Things (IoT)
IoT devices are smart devices that can connect to each other or to general purpose computers and can perform small tasks or check the status of hardware.

- Computerized versions of ordinary devices often controlled through a smart phone app
- Common usage:
    - Wearable technology
    - Home automation systems

Supervisory Control And Data Acquisition (SCADA)
Industrial Control System (ICS)
SCADA and ICS are embedded microcontrollers within network-attached industrial equipment and are often used by utility service providers such as electrical and oil companies to control power generators or oil pipelines.

- Uses sensors to report on capacity or throughput levels
- If compromised, could lead to environmental disaster

Implement network segmentation, isolation, or compartmentalization:

- Implement a firewall to restrict access
- Place SCADA / ICS on a separate network or VLAN
- Use sandboxing techniques

Legacy systems

Legacy architecture is a system or application that has out lived its end-of-lifecycle (EOL) but still serves a necessary function within the organization.

- Lacks vendor support from the manufacturer
    - Lacks patch management
- May implement weaker cipher suites
- May implement weak/deprecated algorithms
- May implement inadequate encryption key sizes

Often legacy systems remain utilized due to financial constraints or lack of skill with newer, more complex systems.

Provisioning

Network provisioning

- Ensures network resources are available and accessible

Server provisioning

- Setting up and allocating a server to house data, host applications, or host services

User provisioning

- Creation, allocation, and maintenance of user accounts, credentials, media, and user profiles

Deprovisioning

- Orderly recovering of resources
- Address data remanence issues

Immutable systems

Systems provisioned as a whole and then deleted and replaced by the next version.

- Immutable systems aren’t modified, but instead replaced outright

Infrastructure as code

- Code that provisions infrastructure components such as virtualized servers, routers, and switches.

- Used within Infrastructure as a Service data centers

Live CD
The operating system is installed on a CD-ROM and the computer is booted from the CD-ROM

- Non-persistent O/S: can't be altered because it resides on read only media
- Persistent user file storage: files could be stored to the local hard drive

Bootable USB drive
The operating system is installed on a USB flash drive.

- Highly portable
- Persistent: O/S and user's files

Virtualization

Virtualization allows multiple virtualized systems to share the resources of one physical system. An administrator can host multiple virtual machines (VMs) on one physical machine. Today's computer servers are built with more than adequate resources such as memory capacity, storage capacity, and processing capabilities. Virtualizing helps a business maximize the usage of those resources so that more physical machines don't have to be purchased. The cost to do business can be reduced.

With virtualization technology, an application, an operating system, an entire computer, or even an entire network can be virtualized. Virtualized machines tend to be platform independent, so they can be moved to different hosts with differing host operating systems.

- Examples: Hyper-V, Virtual PC, VMware

Sandbox security model
Sandboxing is the concept of isolating something from the rest of the environment. It is a form of compartmentalization.

When sandboxing is used with virtualization, each virtual machine is isolated from each other, and each virtual machine is isolated from the host machine. If sandboxing isn't implemented, a compromised VM could be used to compromise other VMs or even the physical host machine. Breaking out of the sandbox is an attack referred to as VM Escape.

If a virus were to infect one of the VMs, the virus could be contained and not allowed to spread to the other virtual and physical machines.

Sandboxing is also used for research, reverse-engineering malware, or analyzing recreated, compromised enterprises. Instead of the malware being in the "wild", it is being analyzed in the "zoo".

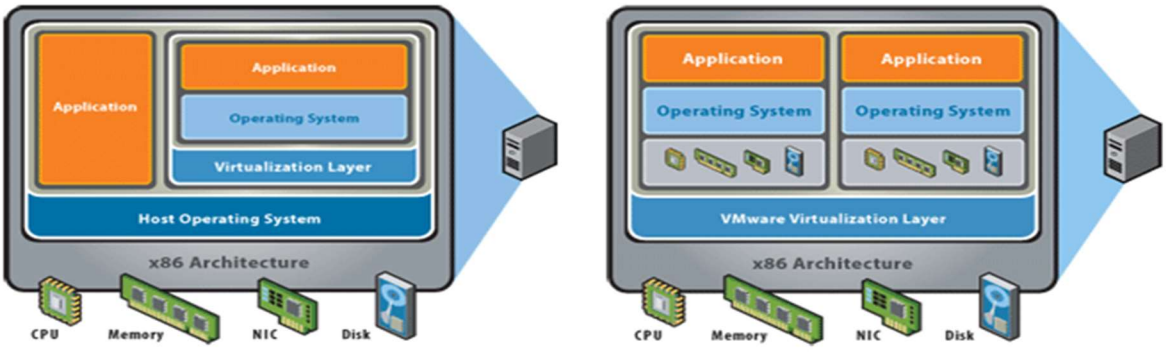
Hypervisor
The hypervisor is the software that manages the VM and interfaces with the host operating system on the VM's behalf. The hypervisor acts out the sandbox security model and serves as a proxy to the other machines.

Type 1 hypervisor
Type 1 hypervisors are software systems that run directly on the host's hardware to control the hardware and to monitor guest operating-systems. It is sometimes referred to as "native" or bare-metal hypervisor because there is no host operating system to interact with, just the hypervisor and the VMs.

Type 1 hypervisors are typically found in large data centers.
Examples: VMWare's ESX or Microsoft's HyperV

Type 2 hypervisor
Hypervisors are software applications running within a conventional host operating system environment. It runs as one application within all the other applications installed on the host operating system.

- Examples: VirtualPC, VMware player



Virtual Desktop Infrastructure (VDI)
The user's desktop does not reside on the local device but on a centralized virtual server when implementing VDI. The user's desktop is provisioned within a session and can be saved during and/or at the end of the session.

- Applications are virtualized
- Platform-independent solution
- Requires a network connection

Persistent VDI
The user's desktop is provisioned from a master image and saved on a centralized server.

- Saved snapshots
- Server could suffer from VM sprawl

Non-persistent VDI
The user's desktop is provisioned as a temporary image from the master image and deleted at the end of the session.

- Each provisioning instance is reverted to a known state
- Server does not experience VM sprawl

Virtualization benefits:

Computing elasticity
Virtual machines can be loaded or unloaded on a whim to satisfy dynamically changing computing processing needs

Compartmentalization
The overall span of data can be partitioned amongst multiple virtual machines so that if one machine gets compromised the entire database hasn't been lost

Containment
If one of the machines becomes compromised, they can't be used to attack other machines

- A virtualized clone can receive patches to verify there won't be any conflicts before rolling the patch out to the production server

Snapshots
Snapshots are complete backups of the VM at a specific moment in time

- Misbehaving VMs can be rolled back to a previous snapshot when everything was OK with the VM
- System Recovery is more expedient

Reduction of costs
Instead of multiple physical computers requiring excessive electrical demands from the HVAC, it is merely a few servers with multiple VMs instead

- Less hardware needs to be purchased

Virtualization issues
Though virtualization has many benefits, it has issues that need to be addresses just like any other technology:

- Single point of failure
    - Multiple Virtual Machines running on one physical host machine
    - Implement server clustering of the physical machines

    - Physical security of the host machines needs to be applied
- Third party access: each Virtual Machine is essentially a single file stored on the physical host machine that contains the VM's operating system, applications, and files
    - Insider Access attacker gets it all in one little file
    - Databases need to be partitioned and spread amongst multiple VMs
- Network failure
    - Communication lines can be attacked using Dos/DDoS techniques
- Inadequate encryption
    - VMs transmit and receive data on a network just like any other computer making them vulnerable to sniffing and man-in-the-middle attacks
    - Use secure channels or VPN tunnels amongst systems, both physical machines and virtual machines
- VM Escape
    - Flaws in the hypervisor can be exploited to break out of the sandbox
    - Effective patch management is needed
- VM sprawl: excessive provisioning of unnecessary virtual machines

---

Cloud Computing

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. Company resources are stored, processed, or managed outside of the corporate perimeter.

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.

- Access to the company resources requires traversing the internet
- On-demand self-service
- Cloud provider exercises resource pooling to support multi-tenant hosting
- Cloud provider exercises resource elasticity
- Measured/metered services

Software as a Service (SaaS)
Software as a Service is sometimes referred to as "software on demand" because it 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 streams, such as from advertisements 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.

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

Example: web-based e-mail like Yahoo or Hotmail, ISP's

Platform as a Service (PaaS)

PaaS is 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.

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 often based on a metering or subscription model so users only pay for what they use.

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

---

Infrastructure as a Service (IaaS)

IaaS is 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.

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

Software Defined Networking (SDN)

Network infrastructure functionality is broken into two planes controlled by a network controller

- Control plane
    - Handles the network's logical decision making: makes decisions about overall flow of traffic
    - Manages the routing protocols and routing decisions
    - Manages QoS decisions
- Data plane
    - Handles traditional network frame delivery

Security as a Service
Security protection mechanisms, auditing, and incident response are handled by the cloud provider.

Cloud Access Security Broker (CASB)
CASB is a cloud-based filter that monitors activity between a cloud consumer and cloud resources.

- Enforces the company's security policy within the cloud portal
- Mitigates BYOD security issues

Private cloud
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers.

- Example: Defense Knowledge Online, AKO

Public cloud
The cloud infrastructure is provisioned for open use by the general public (Pay- as-you-go Model).

- Example: Google or Dropbox

Community cloud
The cloud infrastructure shared by several organizations which supports a specific community.

- Example: travel industry (hotels, airlines, and travel reservation sites)

Hybrid cloud
A hybrid cloud is a combination of a private cloud combined with the use of public cloud services where one or several touch points exist between the environments. The goal is to combine services and data from a variety of cloud models to create a unified, automated, and well-managed computing environment.

Cloud computing security concerns:

Single Point of Failure

- If your Cloud Service Provide is having a bad day, you're going to be having a bad day.

Example: you or the cloud provider lose network connectivity

Network failure

- Network communication lines can be disrupted or attacked.

Third party access
Physical security is an important component in any security program. An organization loses control of physical security when it utilizes cloud computing architecture.

Inadequate encryption
- VPN tunnels while communicating with the cloud
- Whole disk encryption
- File level encryption
- Strong authentication

Cloud computing legal concerns

Geographical considerations
- Different countries have different laws and varying severity of law
- Governmental and trans-border snooping

Legal implications
- Data sovereignty rules: applicable laws are based upon the country where the data resides
- Data ownership laws
- Access rights: owner of equipment versus owner of the data

Physical Security

Physical perimeter
- Visibility/accessibility
    - Lighting
    - Posted signs
    - Escape routes / emergency egress
- Barricades / bollards
- Fences / gates / cages

Surveillance
- CCTV cameras
    - Night-vision
    - Motion-sensitive
- Alarms/sensors
    - Motion detection
    - Infrared detection

    - Detect environmental changes
- Security guards
- Manage facility keys

Conventional locks

Electronic locks

- Passcode
- ID badge
- Electronic tokens
- Biometrics
- Fail-secure vs. fail-safe

Mantrap

Entry logging

Securing Equipment

- Network hardware rooms
- Secure cabinets / enclosures
- Locked safes
- Wireless access points
- Protected cable distributions
- Cable locks
- Social engineering

Environment controls

- HVAC settings
- Temperature controls
- Humidity controls
    - Electrostatic discharge (ESD)
- Sudden changes
- Air flow
    - Hot and cold aisles
    - Positive ventilation

Adverse signals

- Electromagnetic interference (EMI)
- Electromagnetic Pulse (EMP)

- Radio Frequency Interference (RFI)
- Protections
    - TEMPEST standards: mitigate compromising emanations
    - Shielded cables
    - Faraday cage
    - Proper frequency channel selection: channels 1, 6, and 11

Fire suppression

- Fixed or portable (CO2 bottle)
- Water-based
- Clean agent-based (Halon, FM-200, CO2)

Domain – Risk Management

CompTIA SY0-501 domain objectives covered:

- CompTIA domain 5.3: Explain risk management processes and concepts
- CompTIA domain 5.2: Summarize business impact analysis concepts
- CompTIA domain 5.6: Explain disaster recovery and continuity of operations concepts
- CompTIA domain 5.8: Given a scenario, carry out data security and privacy practices
- CompTIA domain 1.5: Explain vulnerability scanning concepts
- CompTIA domain 1.4: Explain penetration testing concepts
- CompTIA domain 2.2: Given a scenario, use appropriate software tools to assess the security posture of an organization
- CompTIA domain 2.3: Given a scenario, troubleshoot common security issues
- CompTIA domain 5.4: Given a scenario, follow incident response procedures
- CompTIA domain 5.5: Summarize basic concepts of forensics

Risk Management

Risk Management is the process of identifying, monitoring, and reducing risk to an acceptable level. The greater the risk, the more of the security budget should be applied to mitigate the risk. Risk management isn't about eliminating all risk because that would not be realistic. Risk that has been brought to a manageable level is called residual risk.

- Risk: the potential damage to a resource
- Threat: the potential to cause harm to an asset
- Vulnerability: a flaw or hole in the security posture
- Exploit: a method or technique used to manipulate a flaw
- Safeguard: a mitigation security control

Risk Assessment

1. Conduct an asset inventory: find out what we have
2. Conduct a threat assessment for each asset: find out what kind of threats are applicable to each of the assets
3. Conduct Business Impact Analysis (BIA): find out how much damage the organization will experience from a loss of one or more of the assets
4. Determine likelihood of occurrence: different parts of the business is exposed to different threats
5. Prioritize risks by weighing likelihood vs. potential impact.
6. Create risk mitigation strategy: mitigate the risk to an acceptable level

---

Asset Inventory

- Identify business intangible assets
- Identify business tangible assets

- Identify mission essential business functions and processes
- Identify critical systems
- Determine asset values

Risk Register
Documents discovered risks.

- Unique ID and description
- Category, to help group similar risks
- Likelihood of occurrence
- Business impact assessment
- Priority for mitigation
- Mitigation steps and strategies
- Residual risk remaining after mitigation
- Contingencies if risk can't be prevented
- “Owner" of the risk

Threat assessment
Determine which threats are applicable to the asset.

Examples:

- Internal threats
- Extreme heat / cold
- Equipment failure
- Human error
- Insider access
- External threats
- Supply chain failure
- Hackers
- Natural disasters

Qualitative risk assessment
Qualitative analysis involves someone’s best judgment or opinion instead of hard, measurable facts. The analysis uses a numerical value system (such as 1, 5, and 10) that represents a low, medium, or high grade.

Risk = (Likelihood of occurrence) x (Impact on organization)
Example: Website defacement.
Risk = Likelihood (5) x Impact (2) = 10
Example: Credit card numbers stolen from the SQL database.
Risk = Likelihood (3) x Impact (10) = 30

Analysis: the loss of credit card numbers poses a greater risk to the company.

Quantitative risk assessment
Assigns "real" numbers to the costs of damages and countermeasures.

Cost-benefit analysis
Sometimes the cost to implement a safeguard is more than the damage the risk would cause. When implementing countermeasures, the safeguard must be cost-effective. A cost-benefit analysis and a quantitative analysis would use the same formulas to come to a manageable understanding of monetary needs.

- If the cost of the safeguard is less than the cost of the resource loss spread out over a period of time, then implement the safeguard.
- If the cost of the safeguard costs more than the cost to replace the damaged resource, then accept the risk.

Single Loss Expectancy (SLE)
A measure of how much actual loss either incurred or is anticipated to occur. The SLE is the value of the asset multiplied by how much loss as a percentage.

SLE = (Asset Value) x (Exposure Factor)

Take for example a car that is worth $40,000. Let's say there is a car accident and the back half of the car is damaged because another driver rear-ended the vehicle.
SLE = ($40,000) x (50%)
SLE = $20,000

Annualized Loss Expectancy (ALE)
Managers would like a budgetary number to figure how much loss can be anticipated each year. The ALE is used to figure how much anticipated loss might occur given a specific resource and is instrumental when doing cost-benefit analysis.

- If the safeguard cost is less than the ALE, implement the safeguard
- If the safeguard cost is more than the ALE, accept the risk

ALE = (SLE) x (ARO), where ARO is the Annual Rate of Occurrence

Annual Rate of Occurrence (ARO)
The ARO is the projected number of times the damage will occur each year. It is usually figured by using statistics of prior events. Continuing with the example provided in the SLE previously, let's say that for every 100 vehicles of the same make, model, color, and production year in the example given, one will experience an automobile accident that year.

The ARO would thus be 1 out of 100 per year, or 1% per year.
ALE = ($20,000) x (1%)
ALE = $200

Business Impact Analysis (BIA)
The BIA is a report of the level of degradation to the health of the business or organization

- Regulation and policy compliance
- Privacy concerns
    - Privacy Threshold Analysis (PTA)
    - Privacy Impact Assessment (PIA)
    - Personally Identifiable Information (PII)
    - Personal Health Information (PHI)

Impact on:

- Life
- Safety
- Reputation
- Revenue
- Property

Supply chain and vendors:

- Service providers
- Suppliers
- Business partners

Recovery time objective (RTO)
The maximum expected amount of down time in case of a failure.

- Includes troubleshooting, recovery itself, and testing

Recovery point objective (RPO)
The maximum expected period of time for which data will be lost in the case of a disaster.

- Defined primarily by data backup frequency

Likelihood: probability of occurrence

Mean Time Between Failures (MTBF)
Average time a repairable component operates before it will likely experience failure again.

Mean Time To Repair (MTTR)
Average time it would take to repair a component.

Responses to risk
There are four ways management can responsibly handle risk (notice that "ignoring the risk" is not one of the options).

- 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 Mitigation
    - Reducing either the probability or consequences of a threat. These may range from implementing physical measures (protective fences) to financial measures (stockpiling cash, insurance)

Automation through software or scripts

Configuration validation
Provides consistency in implementing and checking system settings.

- Patch management software
- Group policy

Continuous monitoring
Proactive, automated checking of system state or system security posture.

- Vulnerability scanners
- Intrusion Detection Systems

Automated course of action
Minimizes delay from reacting to a security violation.

- Failsofts

Business Continuity

Business Continuity Plan (BCP)
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.

- Goal is to maintain business operations with reduced or restricted infrastructure due to business disruptions
- Includes risk analysis, controls, and business restoration procedures
- Mitigates single point of failures
- Reinforces the day to day business practices

Continuity of Operations Plan (COOP)
COOP provides a means for a business process to continue operating during times of reduced capabilities.

- Focuses on sustaining business operations
- Implements failover measures per business process that could be local or geographically distant
- Defines under what conditions alternate business practices would be implemented
    - Legal implications
- Addresses alternate processing sites
    - Location selection
    - Distance
    - Data sovereignty issues

Disaster Recovery Plan (DRP)
DRP is a detailed tactical plan for responding to disasters so core essential business processes can be brought back online.

- Focuses on the prioritized restoration of business processes
    - Order of restoration
- Implements failover measures that are geographically distant
- Location / distance specifications

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

Cold site
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.

- No hardware infrastructure
    - Basic facility with wiring, ventilation, plumbing, and flooring
- Not immediately available
- Relatively low cost

Warm site
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.

- 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

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.

Hot site

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. A database can be kept up-to-date using network connections. Hot sites are expensive, and they are primarily suitable for short-term situations.

- A fully configured and functional facility
- Available within hours
    - Necessary when an organization cannot tolerate any downtime
- Requires constant maintenance
- Expensive to maintain

Testing the plan(s)

- Checklist test: giving the plan to one or more people to review and examine item by item
- Tabletop exercise/Structured walkthrough: gathering the team to walk through a theoretical disaster step by step
- Simulation test: small- or large-scale response test under controlled circumstances
- After-action reports

Data Handling

Data owner

- Authoritative person with direct contact with the generation of data
- Assigns the level of classification and security label for the data
- Determines data distribution and who is allowed to have access to the data
- Sets the data retention period (data expiration)

- Signed NDA
- Example: department heads

Privacy officer
A member of the executive management team tasked with overseeing data compliance requirements.

- Ensures privacy policy remains in effect for proprietary and PII/PHI data:
- Customer data
- Employee personal data
- Signed NDA

Data custodian
The person with delegated responsibility for the protection of the data through security controls.

- Responsible for data backups and data recovery
- Exercises data sanitization techniques
- Signed NDA

Examples: system administrator or network administrator

Data steward

- The person responsible for the quality of the data
- Signed NDA

Examples: Quality Control officer or Quality Assurance officer

Data user
Any person who is authorized to interact with the data to fulfill business goals is a data user.

- Most restrictive data role
- Enforce least privilege management
- May or may not require an NDA

Information classification scheme

- Applying security labels to resources based upon its level of sensitivity or criticalness

Generic Schema	Military Schema	Business Schema	Notes
High	Top Secret	Confidential	Highly restricted. Causes severe damage to the organization if disclosed.

Medium	Secret	Proprietary	Internal, limited distribution. Causes significant damage.
Low	Confidential	Private	Internal distribution. Causes damage.
	Unclassified	Public	Releasable outside of the organization.

Personally Identifiable Information (PII)
Any information that is directly linkable to a specific individual

PII Examples:

- Government created identifications
- Financial account numbers
- Biometric information
- Full name and address

Disclosure can lead to identity theft

- Protect with physical security, data retention policy, sanitization techniques, and encryption

---

Protected Health Information (PHI)
PHI is medical or health information that is directly linkable to a specific individual and their health records.

- Requires a higher level of auditing
- Requires compliance checks
- Disclosure can lead to identity theft
- Protect with physical security, data retention policy, sanitization techniques, and encryption

---

Proprietary data
Proprietary data is used, produced, or marketed under exclusive legal right of the owner.

- May or may not be disclosed in the public domain depending upon the type of data
    - Trade secret: data that is extremely sensitive and provides a company a competitive edge
        - Must never be disclosed
    - Patent protection: legal monopoly of an invention for a set period of time (no compete legal mechanism)
    - Copyright protection: legal protection from unauthorized selling, distributing, or reproducing of an artistic product

---

Data Loss Prevention (DLP)
A security control that mitigates the unauthorized disclosure of data, whether accidental or not accidental. DLP measures must be implemented at communication checkpoints such as a gateway service. Some common examples how DLP would be helpful:

- Removing PII/PHI from emails
- Preventing the use of removable media (USB blocking)
- Preventing the uploading of sensitive company information to social media sites or untrusted cloud services

---

Media destruction techniques

- Incineration: Burning the media into unrecognizable ash
- Pulverizing: Smashing the equipment and media so it's no longer usable
- Shredding: Hardcopy documents are thinly sliced and cross-sliced before throwing the media away
- Pulping: Churning the media into a soup so that the printed ink is separated from the media

---

Data sanitization techniques
It might be desirable to reuse the storage media but the old data must be destroyed.

- Purging: altering or removing the data in a way so that it can no longer be accessed
    - Degaussing: using a strong electromagnetic field on magnetic media to make the data unreadable
    - Wiping: overwriting the media with multiple rounds of intermittent bits (zeroization)
    - Encryption: encrypting the data but deleting the decryption key

---

Security Monitoring

In order to properly monitor a network, a NIC must be tricked into storing all data that is brought to its interface, regardless if it is a unicast or multicast destined to some other machine.

- **Promiscuous mode:** sniffer is capable of capturing ALL packets traversing the network. Wireless sniffing focuses on one frequency channel and is considered "associated" with the Access Point
- **Monitor mode:** used in wireless sniffing to see all channels Potential exists to capture and read sensitive plaintext data

---

Protocol Analyzers
Protocol analyzers are sometimes referred to as packet sniffers. However, a protocol analyzer does much more than just "sniff" a network. They allow us to see the various protocols being actively used within a network and capture it into a log for analysis.

Protocol Analyzers are an important troubleshooting utility, allowing a technician to see any issues at the various layers of the OSI model. Protocol Analyzers are also important for determining normalcy on a network, at any given point in time.

- Hardware or software-based
- Can be placed in-line or between devices
- Can be used on wired or wireless networks
- Uses Promiscuous mode
    - Monitor mode sometimes might be used in wireless networks
- Used for:
    - Establishing network traffic baselines
    - Logging real-time network traffic
    - Sniffing network traffic for policy violations
    - Network performance monitoring
    - Network troubleshooting
- Noteworthy tools:
    - Wireshark
    - TCPDump
    - WinDump
    - Ettercap
    - NetStumbler
    - Kismet

Intrusion Detection Methods
How an IDS determines if something is of interest can be one of two ways:

- Signature-based
- Anomaly-based

Signature-based Detection
Signature-based detection uses a database of previously known malicious acts. It is a storage container for the fingerprints of known attacks. When an analyzer examines the raw data and matches one of these fingerprints, it triggers an alert.

- Evaluates attacks based on a database of signatures written by the vendor
- Useless against zero-day attacks
- a.k.a. Knowledge-based, Misuse-Detection MD-IDS, and Rule-based

Signature-based systems must be readily updated to remain effective and minimize false negatives.

Anomaly-based Detection
Anomaly-based detection compares the current activity to a predetermined baseline of normalcy. If the current activity falls outside the scope of what is normal, then the analyzer

triggers an alert.

- Uses a baseline for evaluations
    - Must learn what activities are normal and acceptable
    - Looks for unexpected events
    - More susceptible to False Positives
- a.k.a. Heuristics, Behavior-based and Statistical-based

In-band management interface

- Management and alerts occur on the same interface as the security sensor
- Attackers can snoop the traffic and discover if a network device is a security control and what kind of security control

Out-of-band management interface

- A separate interface that does not connect to the LAN is used for alerts and management communications
- Attacker would not be able to snoop the traffic because it is external of the LAN

Clipping levels

The set security threshold before a security control reacts to an incident

Examples:

- IDS Tuning: configuring IDS rules
- 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

---

Security evaluations:

False Positive

A false positive is when the IDS reports legitimate activity as an intrusion. Too many false positives can condition a human being not to take a real security incident seriously.

- Poor IDS tuning
- Inadequate system or network baselining

False Negative

A false negative is when the IDS failed to detect malicious activity that is occurring. This can ultimately lead to a successful compromise of a system and loss of sensitive data.

- Zero Day attacks
- Poorly written signatures
- Outdated signature files
- Slow / stealth attack

Host-based IDS (HIDS)
A HIDS is installed on a host and monitors all traffic coming into the host (antivirus 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 application 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.

- Installed on a single 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 because it hasn't been encrypted yet
- Is detectable and can be a target of attack

File integrity checks
Process of verifying the correct files or programs are being used through the use of cryptographic checksums.

- Must be exercised to maintain a trusted operating system

Can be done:

- Manually as part of a scheduled audit check
- Automatically through a program or script
- Continuously through a HIDS or HIPS

Network-based Intrusion Detection Systems (NIDS)

- Monitor's network traffic in real time
    - Analyzes protocols and other relevant packet information
    - Sensors are deployed and usually report back to a system running a management console
- Used to Detect:
    - Attacks coming from outside the network (DoS/DDoS)
    - Attacks and misuse from within the network
    - Port scanning
- NIDS cannot analyze encrypted traffic

Passive IDS

- Looks for security breaches, but effectively takes no action
- Logs suspicious activity and generates an alert
- 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

---

Intrusion Prevention System (IPS)

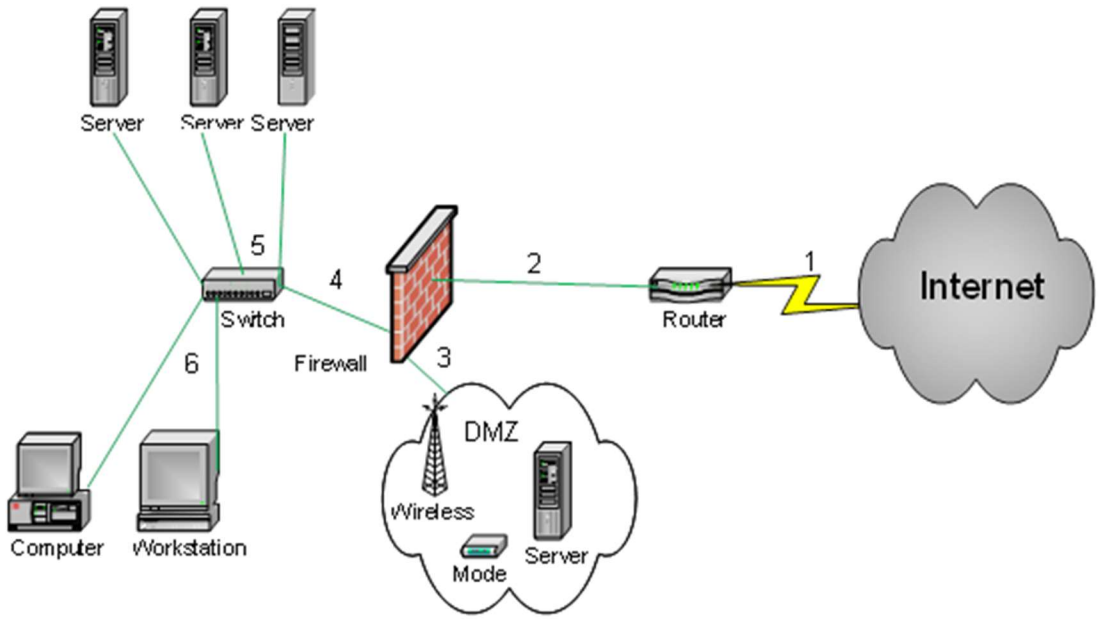
The NIPS monitors network traffic for malicious activity and can block, reject, or redirect traffic in real-time.

- Focuses on prevention as opposed to detection
- Preventative control instead of merely a detective control
- Anticipates the attack before it is successful
- Can adjust security posture on the fly
- Installed in-line: must be dual-homed
- Encrypted traffic is not inspected

Honey Pots

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.

- 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
    - Honeynet
- Enticement versus entrapment



Vampire tap: 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.

Linear tap

A security device is placed in-line with the communication channel.

- Traffic must flow through the security control in order to be delivered to its destination
- Must be dual-homed
- Purposefully designed to be a chokepoint
- More effective at stopping the security incident

Example: firewall or IPS deployment

Parallel tap

A security device is placed alongside the communication channel instead of in the communication channel.

- Traffic is merely snooped by the security control
- Designed to be a detective control, not a preventative control

Example: NIDS connected to the switch's mirroring port

Mirroring Port

Connecting the NIDS to a network switch and hoping to analyze all the network traffic is going to work because a switch forwards frames to the specific port that the receiver is at. In order to monitor across the network switch, one of the switch's physical ports has to be configured as a mirroring port. When a mirroring port is established, a copy of all frames traversing the switch

will be sent to the mirroring port. A security administrator using a protocol analyzer or a connected NIDS then can analyze the traffic.

- Sometimes called a "Spanning" port, after the Cisco protocol SPAN (**S**witched **P**ort **AN**alyzer)
- Causes performance degradation of the switch

SSL Decryptor

An SSL decryptor is an authorized man-in-the-middle proxy that forces the network traffic to enter a decrypted state so the SSL/TLS traffic can be scanned.

- Client must have the proxy's X.509 digital certificate installed to avoid unsecure channel errors

---

System log files

Any information possibly needed to reconstruct pertinent actions should be logged.

- Event: change in system state
- Incident: a violation of the security posture
- Alert: a security event needing evaluation

Define the retention policy

- Control access to logs and do not over audit
- Hash the logs for integrity checking
- Storage media: Write Once Read Many (WORM) storage

Network Time Protocol (NTP)

NTP is a clock synchronization protocol that helps keep TCP/IP-based devices' clocks updated by passing a UTC timestamp to the device over UDP port 123. Some protocols (such as Kerberos) require clocks to be accurate. And, for obvious reasons, so do log entries.

Syslog

Syslog is a structured log event reporting protocol that redirects log entries to a centralized log server commonly called Syslog on UDP port 514. It uses numbered severity level types that can be customized and filtered. For example:

0 = Emergency
1 = Alert
2 = Critical
3 = Error
4 = Warning
5 = Notice
6 = Informational

Security Information and Event Management (SIEM)
SIEM is a centralized auditing system that provides real-time automatic auditing of networked services.

- Aggregation: gathers events from multiple sources by using agents and/or syslog
    - DHCP logs provide a history of IP address to MAC address transactions
    - DNS logs provide a history of web destinations
    - Router and firewall logs provide a history of network traffic events
    - Domain controller logs provide a history of enterprise logon attempts
- Correlation: automated log analysis
- Provides an automated alerting system in which triggers are sent to a reporting console
- Time synchronization: manages time offsets between various system log events
- Event deduplication: multiple instances of an event may occur, but displayed only once
- Supports compliance auditing by providing an auditing bird's eye view

---

Unified Threat Management (UTM)
A centralized network security solution that implements various types of security features to provide security throughout the entire enterprise

- Security management system with centralized reporting

Multiple features:

- Firewall
- IDS / IPS / log monitoring
- Proxy service
- VPN concentrator
- NAC
- Security posture assessment

Vulnerability Assessment

Assessing the effectiveness of security planning, policies, and security controls is the realm of vulnerability assessments. It is the process of identifying, quantifying, and prioritizing vulnerabilities in a system and ultimately tells us how we are doing with our security posture.

- An audit report should give detailed information on tools used, when scans were conducted, and the vulnerabilities discovered, along with their risk levels.
- Verifies compliance with policies and regulations
    - Aids in discovering inadequate security controls
    - Assess baselines
        - Performance baseline
        - Security baseline
        - Configuration baseline
- Senior management approval needed

Banner grabbing
Interacting with a network application service to discover its type of service, version information, and other information.

- Active reconnaissance
- Provides more precise information about the service running on a system
- Tools: Telnet, Netcat, NMAP

Vulnerability scanning
Vulnerability scanning is designed to check for violations to the various policies upheld by an organization, from the security policy to the AUP, and everything in between. A vulnerability scanner's initial report will likely contain false positives that need to be verified. A vulnerability scanner aids the security team in identifying:

- Vulnerabilities in software-based services, network-based communications, and physical security
- Gaps in security where security controls are lacking or non-existent
- Common misconfigurations

Vulnerability scanner evaluations:

- False positive: event was benign but the scanner mistook it for a problem
    - It was a false alarm
- False negative: a real vulnerability was mistaken for something normal
    - The security posture is actually compromised and security personnel are unaware of the problem!!!
- True positive: a vulnerability was properly identified
    - The scanner did what it was designed to do and discovered the vulnerability so it can be mitigated
- True negative: an event was correctly evaluated as benign
    - It was correctly decided to be safe

Common vulnerability scanners:

- Nessus: a proprietary vulnerability and compliance scanner
- SAINT (Security Administrator's Integrated Network Tool): a network vulnerability scanning tool that has the means to also exploit the vulnerabilities that were discovered
- OpenVAS (Open Vulnerability Assessment System): a free open source software framework designed for vulnerability scanning and vulnerability management
- NMAP: the most popular open source software tool that can discover hosts, map out networks, scan ports, detect service and O/S versions, and also deliver exploits

---

Vulnerability scan types:

Non-intrusive scan

- Uses simple, benign requests to identify devices
- Helps discover rogue devices
- Monitors communication lines
- Helps discover rogue protocols that provide covert channels

Intrusive scan

- More aggressive by using malformed packets or more traffic volume
- Stress testing
- Designed more for testing the response of security controls

Non-credentialed scan:

- Scanner is not logged into the target
- Discovers addresses, ports, rogue devices
- Appropriate for sweeping the network

Credentialed scan:

- Tester is scanning with an appropriate username and password
- Discovers unauthorized software, traverses the file system
- Provides more information than a non-credentialed vulnerability scan

---

Penetration testing

The intent of a penetration test is to determine feasibility of an attack and the amount of impact a successful exploit will have on the business. 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. It is a key method to proactively search for zero-day exploits.

This analysis is usually carried out from the position of the 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.

- 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

Penetration testing reveals whether a system can still be breached even though it conforms to policy, while vulnerability scanning focuses more on policy infringement issues. Due to its aggressive nature, penetration testing may cause damage to systems. It helps discover:

- Known or unknown hardware or software flaws
    - Zero-day flaws
- Application weaknesses
- It involves active exploitation of discovered vulnerabilities

---

Stages of pentesting:

Planning stage

- Define scope / Rules of Engagement (RoE)
- Management's approval in writing

Discovery stage

- Active/passive reconnaissance occurs
- Banner grabbing is exercised so that service type and version information can be ascertained

Attack stage

- Initial exploitation: the goal is to be successful on the first try
    - Establish persistence
- Privilege escalation: gaining elevated or broadened access
- Pivot: using a compromised network host to gain further access within the network

Report presented to system owner

- Lists vulnerabilities discovered
- An assessment of impact vs. probability
- A proposal for mitigation or a technical solution

Penetration testing toolkits

Exploitation frameworks

Exploitation frameworks are a suite of tools, usually bundled together within their own deployable operating system. Examples:

- Kali Linux: a Debian Linux distribution pre-loaded with ethical hacking and security assessment tools so that penetration testing and digital forensics can be performed.
- Metasploit: a pre-loaded distribution of tools that can be used to perform security assessments
- Pentoo: an open source Live CD or Live USB distribution that focuses on penetration testing of UNIX-based systems

Fuzzing
Fuzzing is a quality assurance software testing technique of using software tools (called a fuzzer) to check for coding errors in software. Fuzzers apply large amounts of data or varying kinds of data to a software interface to stress test the interface or to discover flaws in the code. It is a proactive way to discover buffer overflow and other significant software issues that could be exploited by an attacker.

Network Mappers
Software that allows a person to map out the network architecture, such as MAC addresses and IP addresses. Network mappers help to determine if an address is currently allocated. Captured addresses can be compared to network documentation to help weed out potential intruders.

- Examples: NMAP, netcat (nc), and hping

Port Scanners
Port scanners help determine which ports are open and which are closed on a system of interest. Various port scanning techniques can also be used to help determine which type of operating system is being used and which type of services are running on that operating system. Most port scanners can also perform banner grabbing.

- Examples: NMAP, SuperScan, and Pscan

Password Crackers
A password cracker is a software program that allows direct testing of a user's logon password strength. It deciphers passwords using one of three main techniques:

- Brute force attack: going through every possible combination until the password is discovered.
- Dictionary attack: using a list of words to discover the password
- Rainbow Tables: compares hashed passwords against pre-computed hash tables to discover the plaintext password

Password cracker examples:

- Cain and Abel: suite of tools with password cracking capabilities against multiple types of authentication systems
- L0phtCrack: password cracker designed to crack Windows-based passwords
- John the Ripper: Linux-based command line password cracker
- Ophcrack: Linux-based rainbow table cracker
- RainbowCrack: rainbow table cracker

Penetration testing methods:

Black Box

Examines a system from a hacker's perspective

- All stages of hacking need to be completed
- Black box testing treats the software as a "black box"—without any knowledge of internal implementation.

Gray Box

Examines a system from the viewpoint of a rogue end user

- Basic organizational information is known
- Footprinting stage is already complete

White Box

Examines the internal logical structures of a program, line by line, for errors

- Viewpoint of a rogue administrator
- Often used for "war gaming"
- White box testing is when the tester has access to the internal data structures and algorithms including the code that implement these.

Command Line

ipconfig utility

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

 Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.25.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.25.1
```

LINUX / UNIX ifconfig utility

```
root@kali:~# ifconfig
eth0   Link encap:Ethernet HWaddr 00:50:53:00:00:13
       inet addr:192.168.1.20 Bcast:192.168.1.255
       Mask:255.255.255.0
       inet6 addr: fe80::20c:29ff:fec8:6fd8/64 Scope:Link   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:89 errors:0 dropped:0 overruns:0 frame:0
       TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:8564 (8.3 KiB) TX bytes:2582 (2.5 KiB)

lo     Link encap:Local Loopback
       inet addr:127.0.0.1 Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING MTU:65536 Metric:1
       RX packets:16 errors:0 dropped:0 overruns:0 frame:0
```

LINUX / UNIX tcpdump sniffer

```
root@kali:~# tcpdump –i eth0
tcpdump version 4.3.0
libpcap version 1.3.0

listening on eth0, link-type Ethernet,
capture size 65535 bytes
23:14:09.171884 IP packetflows.local.47860 > mydomain.com
Flags[S], seq 2046377878, win 29200, options [mss 1460,
sackOK, TS val 9320277 ecr 0, nop, wscale 7], length 0
23:14:09.173117 IP packetflows.local.10745 > mydomain.com
47145+ PTR? 13.33.213.87.in-addr.arpa. (44)
23:14:09.174413 IP packetflows.local > mydomain.com: ICMP
packetflows.local udp port 10745 unreachable, length 118
```

---

netstat utility

```
C:\>netstat -an

Active Connections

Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    10.0.0.12:49139        10.0.0.8:445           ESTABLISHED
TCP    [::]:135               [::]:0                 LISTENING
TCP    [::]:445               [::]:0                 LISTENING
UDP    0.0.0.0:68             *:*
UDP    0.0.0.0:4500           *:*
UDP    10.0.0.12:137          *:*
UDP    10.0.0.12:138          *:*
UDP    [::]:500               *:*
```

---

nslookup utility

```
C:\>nslookup www.army.mil
Server:      UnKnown
Address:     10.10.0.200

Non-authoritative answer:
Name:  33532.dscb.akamaiedge.net
Addresses:   2600:1408:10:18e::dcc
             2600:1408:10:190::dcc
             104.118.209.174
Aliases:     www.army.mil
             www.army.mil.edgekey.net
```

---

ping utility

```
C:\>ping 107.21.1.61

Pinging 107.21.1.61 with 32 bytes of data:
Reply from 107.21.1.61: bytes=32 time=43ms TTL=48
Reply from 107.21.1.61: bytes=32 time=31ms TTL=48
Reply from 107.21.1.61: bytes=32 time=32ms TTL=48
Reply from 107.21.1.61: bytes=32 time=31ms TTL=48
Ping statistics for 107.21.1.61:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 43ms, Average = 34ms
```

---

tracert utility

```
C:\>tracert 107.21.1.61

1     1 ms         1 ms     1 ms      10.10.0.100
2     13 ms        13 ms    13 ms     69.29.181.17
3     12 ms        14 ms    11 ms     207.119.244.129
4     25 ms        14 ms    11 ms     206.51.71.213
5     21 ms        19 ms    18 ms     209.85.254.130
6     32 ms        31 ms    31 ms     72.14.232.141
7     30 ms        32 ms    30 ms     209.85.241.37
8     40 ms        34 ms    36 ms     107.21.1.61

Trace complete.
```

Incident Response

Incident response plan

- Establish the incident response team
- Define incident types / categories
- Define incident response roles and responsibilities
- Establish reporting requirements
- Establish escalation milestones
- Establish incident response training

Steps to Incident Response

- Preparation
    - Identified and trained incident response team
    - Tools: forensic toolkit, hand-held camera, establish baselines
- Identification
    - Detect and identify the incident and severity
- Containment
    - Keep the incident from spreading to other systems

- Eradication
    - Remove the root cause of the incident
- Recovery
    - Re-establish baselines and restore services
- Lessons learned
    - Review history of events and readjust security controls to mitigate future potential occurrences

---

Computer Forensics

Order of volatility
Proceed from the most volatile to the least

1. Register Cache
2. Routing Table, Memory
3. Temporary File System
4. Disks or other storage media
5. Remote logging and monitoring data
6. Hardcopy evidence (contracts, policies, SLAs)

Don't forget surrounding network systems.

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
- Capture video
- Record time offsets
- Take screenshots
- Gather and interview witnesses
- Track labor hours

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
- Form should include:
    - 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

---

Legal hold

Items may have been sequestered as evidence.

- May require documentation due to overriding the item's lifecycle

---

Appendix A – Networking Models

OSI Model

Layer	Purpose	Protocols	Hardware
7 – Application	Main interface between the network and the application	HTTP, FTP, SMTP, POP, IMAP, TELNET, SSH, SIP	Proxy, DPI firewall
6 – Presentation	Syntax and data formatting	HTLM, MIME, ASCII, Unicode, JPG, MP3	
5 – Session	Establish connections between applications	SQL, ASP, ASP.net, NetBIOS, NFS, RPC	
4 – Transport	Error recovery and flow control	TCP, UDP, SCTP, RTP, NetBEUI	SPI firewall
3 – Network	Pathway determination amongst network	IPv4, IPv6, IPsec, ICMP, routing protocols	Router, L3 switch, firewall, WAP
2 – Data Link	Frame delivery	802.3, 802.1X, L2TP, PPTP, PPP, STP	NIC, switch, bridge
1 – Physical	Convert bits into energy	802.11, CAT 5/6, Coax, Fiber, ISDN, Bluetooth	NIC, hub, modem

Notes:
Deep Packet Inspection (DPI)
Layer 3 (L3)
Stateful Packet Inspection (SPI)

Comparison of OSI model and TCP/IP model

OSI model	TCP/IP model
7 – Application	**4 – Application**
6 – Presentation	
5 – Session	
4 – Transport	**3 – Host to Host**
3 – Network	**2 – Internetwork (AKA Internet)**
2 – Data Link	**1 – Network Interface**
1 – Physical	

Notes:
TCP/IP model is also called the DoD model

Appendix B – IPv4

Public classes

Class	First Octet	First Bits	# of Subnets	# of Hosts	Subnet Mask	VLSM
A	0. – 127.	0000	128	16,777,216	255.0.0.0	/8
B	128. – 191.	1000	16,384	65,536	255.255.0.0	/16
C	192. – 223	1100	2,097,152	256	255.255.255.0	/24
D	224. – 239.	1110	n/a	n/a	n/a	n/a
E	240. – 254.	1111	n/a	n/a	n/a	n/a

Notes:
Class A: "0." is not assignable and "127." is loopback.
Class D is used for multicasting.
Class E is used for experimental or scientific purposes.

Private classes

Class	Address Range	Subnet Mask	VLSM
A	10.0.0.0 – 10.255.255.255	255.0.0.0	/8
B	172.16.0.0 – 172.31.255.255	255.240.0.0	/12
C	192.168.0.0 – 192.168.255.255	255.255.0.0	/16

Notes:

APIPA	169.254.0.0 – 169.254.255.255	255.255.0.0	/16

Appendix C – IPv6

IPv6 address space = 2^{128} = 3.4 x 10^{38} possible addresses.

IPv6 example address:	3FFE:0B00:0800:0002:0000:0000:0000:000C
Leading zero rule applied:	3FFE:B00:800:2:0000:0000:0000:C
Zero compression rule applied:	3FFE:B00:800:2::C (notice the double colon)
IPv6 loopback address:	::1/128
IPv6 Link-local address:	FE80::/10
IPv6 Site-local address (deprecated):	FEC0::/10 or (FEC0 – FEF0)
IPv6 Unique Local Address (ULA):	FD
IPv6 Global address:	2000::/3 or (2000 – 3FFF)
IPv6 Multicast address:	FF

IPv6 Anycast address is allocated from the unicast address space when a unicast address is assigned to more than one interface (more than one router interface).

- Sends the message to the closest node within a group of nodes
- Anycast addresses can be used by a device (router), not a host (printer)
- Cannot be used as the source address in an IPv6 packet

Appendix D – Subnetting Example

Subnetting 192.168.10.20/24 network into 192.168.10.20/26 networks:

IP Address:	192	.	168	.	10	.	20
Subnet Mask:	11111111 255		11111111 255		11111111 255		00000000 0
	nnnnnnnn		nnnnnnnn		nnnnnnnn		hhhhhhhh
Network:	192	.	168	.	10	.	0
Host 1	192	.	168	.	10	.	1
Host + 1	192	.	168	.	10	.	h + 1
Host 254	192	.	168	.	10	.	254
Broadcast:	192	.	168	.	10	.	255

Original IP schema (192.168.10.20/24)

IP Address:	192	.	168	.	10	.	20
Subnet Mask:	11111111 255		11111111 255		11111111 255		11000000 192
	nnnnnnnn		nnnnnnnn		nnnnnnnn		nnhhhhhh
Network #1:	192	.	168	.	10	.	0
Broadcast #1:	192	.	168	.	10	.	63
Network #2:	192	.	168	.	10	.	64
Broadcast #2:	192	.	168	.	10	.	127
Network #3:	192	.	168	.	10	.	128
Broadcast #3:	192	.	168	.	10	.	191
Network #4:	192	.	168	.	10	.	192
Broadcast #4:	192	.	168	.	10	.	255

Original network split into 4 subnetworks

Note: All four networks are assigned the same subnet mask of 255.255.255.192 (/26).

Appendix E – Common Port Numbers

Port	TCP	UDP	Other	Description
20	TCP	UDP		File Transfer Protocol (FTP) - data transfer
21	TCP	UDP	SCTP	File Transfer Protocol (FTP) - control channel
22	TCP	UDP	SCTP	Secure Shell (SSH) | Secure Copy (SCP) | Secured FTP (SFTP)
23	TCP	UDP		Telnet
25	TCP	UDP		Simple Mail Transfer Protocol (SMTP)
49	TCP	UDP		Terminal Access Controller Access-Control System (TACACS)
53	TCP	UDP		Domain Name System (DNS)
67	TCP	UDP		Dynamic Host Configuration Protocol (DHCP) – server
68	TCP	UDP		Dynamic Host Configuration Protocol (DHCP) - client
69	TCP	UDP		Trivial File Transfer Protocol (TFTP)
80	TCP	UDP	SCTP	Hypertext Transfer Protocol (HTTP)
88	TCP	UDP		Kerberos
110	TCP			Post Office Protocol v3 (POP3)
118	TCP	UDP		Structured Query Language(SQL) Services
123	TCP	UDP		Network Time Protocol (NTP)
137	TCP	UDP		NetBIOS NetBIOS Name Service
138	TCP	UDP		NetBIOS NetBIOS Datagram Service
139	TCP	UDP		NetBIOS NetBIOS Session Service
143	TCP			Internet Message Access Protocol (IMAP)
161		UDP		Simple Network Management Protocol (SNMP)
162	TCP	UDP		Simple Network Management Protocol Trap (SNMP Trap)
389	TCP	UDP		Lightweight Directory Access Protocol (LDAP)
443	TCP	UDP	SCTP	Hypertext Transfer Protocol over TLS/SSL (HTTPS)
445	TCP			Server Message Block (SMB)

465	TCP			Simple Mail Transfer Protocol over TLS/SSL (SMTPS)
500	TCP	UDP		Internet Security Association and Key Management Protocol (ISAKMP)
514		UDP		SYSLOG
636	TCP	UDP		Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
989	TCP	UDP		File Transfer Protocol Secure (FTPS) Protocol (data): FTP over TLS/SSL
990	TCP	UDP		File Transfer Protocol Secure (FTPS) Protocol (control): FTP over TLS/SSL
993	TCP			Internet Message Access Protocol over TLS/SSL (IMAPS)
995	TCP			Post Office Protocol 3 over TLS/SSL (POP3S)
1701		UDP		Layer 2 Forwarding Protocol (L2F) & Layer 2 Tunneling Protocol (L2TP)
1723	TCP	UDP		Microsoft Point-to-Point Tunneling Protocol (PPTP)
1812	TCP	UDP		RADIUS authentication protocol
1813	TCP	UDP		RADIUS accounting protocol
3389	TCP	UDP		Microsoft Terminal Server – Remote Desktop Protocol (RDP)
3868	TCP	UDP	SCTP	Diameter
4500		UDP		IPSec NAT Traversal
5004	TCP	UDP		Real-time Transport Protocol (RTP) media data (RFC 3551, RFC 4571)
5004			DCCP	Real-time Transport Protocol (RTP) media data (RFC 3551, RFC 4571)
5060	TCP	UDP		Session Initiation Protocol (SIP)
5061	TCP			Session Initiation Protocol (SIP) over TLS

Appendix F – Algorithms

Name	Type	Algorithm	Size	
DES	Symmetric	Block cipher	Block: 64 bits	Key: 56 bits
3DES	Symmetric	Block cipher (used in PGP/GPG)	Block: 64 bits	Key: 168 bits
AES	Symmetric	Rijndael Block cipher (used in PGP/GPG)	Block: 128 bits	Key: 128, 192, 256 bits
Blowfish	Symmetric	Block cipher	Block: 64 bits	Key: variable 32-448 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 40-128 bits
CAST-256	Symmetric	Block cipher (used in PGP/GPG)	Block: 128 bits	Key: variable 128, 160, 192,224, 256 bits
RC4	Symmetric	Stream cipher (used in WEP)	Stream	Key: variable 8-2048 bits
RC6	Symmetric	Block cipher	Block: 128 bits	Key: variable 8-2048 bits
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, 256 bits
SAFER++	Symmetric	Block cipher (bluetooth for key derivation)	Block: 64, 128 bits	Key: 64, 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	Based on discrete logarithms Key: 512-bit to arbitrarily long (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			128 bits
SHA-1	Hash			160 bits
SHA-2	Hash			224, 256, 384, 512 bits
SHA-3	Hash			224, 256, 384, 512 bits
Whirlpool	Hash			512 bits
RIPEMD	Hash			128 bits
RIPEMD-160	Hash			160, 256, 320 bits
HAVAL	Hash			128, 160, 192, 224, 256 bits

Index

3

3DES 16, 84, 89, 184

8

802.11 ..... *See* IEEE 802.11
802.15 ..... *See* IEEE 802.15
802.1D ..... *See* IEEE 802.1D
802.1Q ..... *See* IEEE 802.1Q
802.1X ..... *See* IEEE 802.1X

9

99.999% 137

A

AAA security model 30
ABAC 38
Acceptable Use Policy (AUP) ..... 65, *See* AUP
Access control 30
Access Control List (ACL) 74
  Extended 75, 76
  Standard 75
Access control models 37
  ABAC 38
  DAC 37
  MAC 37
  Role-BAC 38
  Rule-BAC 38
Account types
  Guest account 50
  Privileged account 49
  Service account 50
  Shared account 50
  User account 49
Ad hoc network 53
Address Resolution Protocol (ARP) 70
Administrative controls 122
Advanced Persistent Threat (APT) 92, 93
Adverse policy actions 121
Adware 100
AES 16, 18, 89, 90, 184
Aggregation 168
Aggregation switches 55
Agile model 126
Air gapping 51
ALE 154
Algorithm 7
  deprecated 7
  secret 7
Alternate sites 157
Amplification 105, 106, 107
Annual Rate of Occurrence (ARO) ..... *See* ARO
Annualized Loss Expectancy (ALE) ..... *See* ALE
Anomaly-based detection 162
ANT 67
Antennae 61
Anti-spoofing filter 74, 107
Application gateway firewall . *See* Application proxy firewall
Application proxy firewall 76
ARO 154
ARP poisoning 102
Asset inventory 152
Asymmetric cryptography 18
Attestation 131, 135
Attribute-Based Access Control (ABAC) 38
AUP 120
Authentication 9, 13, 31, 40
  Multifactor authentication 35
  mutual authentication 35
  Something you are 33
  Something you do 34
  Something you have 31
  Something you know 31
  Somewhere you are 34
  Strong authentication 35
Authentication Header (AH) 83
  NAT-T 56
Automatic Private IP Address (APIPA) 71
Avalanche effect 14

B

Back Orifice 99
Backdoor 98
Background checks 121
Banner grabbing 169, 171
Baselines 130
  Configuration 130
  Performance 130
  Security 130
Basic Service Set (BSS) 59
Basic Service Set ID (BSSID) 60
Bastion host 52
BCP 156
bcrypt() 8
BIA 155
Biometric-based authentication 33
  Facial recognition 33
  Fingerprint scanner 33
  Gait recognition 33

Hand Geometry 33
Iris scanner 33
Keystroke recognition 33
Retinal scanner 33
Signature analysis 33
Type I error 33
Type II error 33
Voice recognition 33
Biometrics 67
Birthday attack 109
Black box 173
Blacklisting 96, 132
Block Cipher 11
Blowfish 16, 84, 184
Blue Screen of Death (BSOD) 114
Bluebugging 111
Bluejacking 111
Bluesnarfing 111
Bluetooth 59
Bootable USB drive 143
Border Gateway Protocol (BGP) 57
Botnet attack 107
Bounce attack 88
BPDU 54
Bridge 53
Bring Your Own Device (BYOD) 65
Broadcast storm 54
Brute force attack 108, 172
Buffer overflows 112
Business Continuity Plan (BCP) ..... *See* BCP
Business Impact Analysis (BIA) ..... *See* BIA
Business Partnership Agreement (BPA) 119

C

CAC 32
Cain and Abel 108, 172
Caller ID spoofing 101
Campus Area Network (CAN) ..... *See* Intranet
Canonical Encoding Rules (CER) 29
Captive portal 80
CAST 16, 184
CCTV 90, 149
Certificate
CER 29
DER 29
Exteneded Validation (EV) 28
Limited purpose 27
Machine 27
Multi-domain 28
P12 29
P7B 29
PEM 29
PFX 29
Root 27
SAN 28
Self-signed 23, 27
User 27
Wildcard 28
Certificate Authority 23
Certificate Revocation List (CRL) 25
Certificate Signing Request (CSR) 24
Certificate-based authentication 27, 32
Chain of custody 176
Challenge Handshake Authentication Protocol (CHAP) 41
Change management 120
Channel bonding 61, 138
Choose Your Own Device (CYOD) 65
CIA triad model 122
Cipher Block Chaining (CBC) 17
Cipher modes 16
Cipher suite 13, 81, 86, 87
Cipher text 7
Clean desk policy 94, 121
Clickjacking 97
Clipping level 109, 163
Cloud Access Security Broker (CASB) 148
Cloud computing 146
Legal concerns 149
COBIT 118
Code review 98
Code signing 131
Cold site 157
collision
Hashing 14, 109
Community cloud 148
Community strings 85
Compensating controls 124
Competitor threat 92
Compiled code 126
Confidentiality 9
Configuration baselines 130
Continuing education 121
Continuity of Operations Plan (COOP) ..... *See* COOP
Continuous integration 126
Continuous monitoring 80, 156
Control diversity 125
Conventional key 15
Convergence 54
COOP 157
Copyright 160
Corporate Area Network (CAN) ..... *See* Intranet
Corporate Owned, Business Only (COBO) 66
Corporate Owned, Personally Enabled (COPE) 66
Corrective controls 124
Counter Mode (CTM) 18, 83
Covert Channel 9
Credentialed scan 170
Crossover Error Rate (CER) 34
Cross-site Request Forgery (XSRF) ..... See XSRF
Cross-Site Scripting (XSS) ..... See XSS
Cryptographic Service Provider (CSP) 127
CSMA/CA 51, 59
CSMA/CD 51

D

Data backup types 139
Data backups
  Offsite storage 138
  Onsite storage 138
Data custodian 159
Data Loss Prevention (DLP) 161
Data owner 158
Data steward 159
Data user 159
Deduplication 168
Defense in depth 125
Degaussing 161
Denial of Service (DoS) 104
Deprovisioning 142
DES 16, 89, 184
Detective controls 123
Deterrent controls 124
Development and Operations (DevOps) ..... *See* DevOps
Development environment 136
DevOps 126
DHCP 70
  Options 70
  Reservations 70
  Scope 70
DHE 83
Diameter 35, 43
Dictionary attack 109, 172
Diddling attack 92
Diffie-Hellman 19, 83, 89, 184
  Groups 20
Digital certificate 24
  PGP / GPG 24
  revocaton 25
  X.509 24
Digital Rights Management (DRM) 9
Digital signature 21
  Signed code 131
Digital Signature Algorithm (DSA) 22
Digital Signature Standard (DSS) 22
Directory services
  Kerberos 44
  LDAP 45
Disassociation 110
Disaster Recovery Plan (DRP) ..... *See* DRP
Discretionary Access Control (DAC) 37
Distinguished Encoding Rules (DER) 29
Distinguished Name (DN) 24, 46
Distributed Denial of Service (DDoS) 105
DLL injection 114
DLP 134
DMZ 52
DNS cache poisoning 104
DNS poisoning 104
DNSSEC 73, 104
Domain hijacking 104
Domain Name Service (DNS) 71
  Record types 72
  Zones 71
Downgrade attack 87, 103
DRP 157
Dumpster diving 93
Dynamic Host Configuration Protocol (DHCP) ..... *See* DHCP
Dynamic NAT 57

E

EAP 35, 41, 43
EAP Transport Layer Security (EAP-TLS) 42
EAP Tunneled Transport Layer Security (EAP-TTLS) 42
EAP-FAST 42
ECC 21
ECDHE 83
Elasticity 145
Electromagnetic interference (EMI) 150
Electromagnetic Pulse (EMP) 150
Electronic Code Book (ECB) 17
Electrostatic discharge (ESD) 150
Elliptical Curve Cryptography (ECC) 21
Embedded devices 140
Encapsulating Security Payload (ESP) 83
Enterprise access control
  Kerberos 44
  LDAP 45
Entropy 31, 109
Ephemeral Key 8
Error handling 128
Ettercap 162
Evil Twin 35, 110
Exception handling 127
Exclusive-OR (XOR) 10
Exit interview 122
Extended Service Set ID (ESSID) 60
Extensible Authentication Protocol (EAP) ..... *See* EAP

F

Failsofts 156
False Acceptance Rate (FAR) 33
False negative 163, 169
False positive 76, 163, 169
False Rejection Rate (FRR) 33
Faraday cage 112, 151
Fault tolerance 137
Federations 37
File integrity check 164
File integrity checker 130
File systems 39
  UNIX / Linux 39
File Transfer Protocol (FTP) 87
Firewalls 75
  Multipurpose 76
  Network-based 75
  Software-based 75
Five nines 137

Flat panel antenna 61
Flood Guard 77
Footprinting 109, 173
Fraggle attack 107
FTPS 88
Full Disk Encryption (FDE) 68, 134
Full-differential backup 139
Full-incremental backup 139
Fully Qualified Domain Names (FQDN) 71
Fuzzing 129, 136, 172
  Dynamic code analysis 129
  Static code analysis 129

G

Galois Counter Mode (GCM) 18
Garbage collector 114
Geofencing 34, 67
Geolocation 34, 67
GMAC 18
GNU Privacy Guard (GPG) 24, 89
GPS tagging 34
Gray box 173
Group policy 133
  Inheritance 133
  OU 133
Group-based access control 38

H

Hacktivists 92
Halon 151
Hardware Security Module (HSM) 135
Harpooning ..... *See* Whaling
Hash 22
Hashed MAC 15, 87, 90
Hashing 13
HAVAL 14
Heuristics 163
HIDS 164
High availability 137
HIPPA 118
Hoax 95
Honey pot 165
Honeynet 52, 165
Honeypot 52
Host file 104
host health check 79
Host-based firewall ..... 98, *See* Firewalls
Host-based IDS (HIDS) 164
Hosts File 71
Hot and cold aisles 150
Hot site 158
Hot swappable 137
HOTP 32
Hping 172
HTTPS 87
HVAC 150
Hybrid cloud 148
Hypervisor 144

I

ICANN 104
ICS 141
IDEA 16, 184
Identification 30
Identity Provider (IdP) 47
IDS tuning 163
IEEE 802.11 ..... 59, 111
  Specifications 61
IEEE 802.11i 65
IEEE 802.15 59
IEEE 802.1D 54
IEEE 802.1p 89, 90
IEEE 802.1Q 54
IEEE 802.1X 42, 73
IEEE 802.q 90
ifconfig 173
Illicit server ..... *See* Remote Access Trojan (RAT)
IMAP 88
IMAPS 88
Immutable systems 142
Impersonation 94, 110
Implicit deny 74
Incident Response 175
Incineration 161
Independent Basic Service Set (IBSS) 59
Industrial Control System (ICS) ..... *See* ICS
Information classification 159
Infrared detection 149
Infrastructure as a Service (IaaS) 147
Infrastructure as code 142
Initialization Vector (IV) 7
Input validation 129
Insider threat 92
Integer overflow 113
Integrity 9
Interconnection Security Agreement (ISA) 119
Interference 111
Internet 15, 87
Internet Content Filter 76
Internet Engineering Task Force (IETF) 86
Internet Key Exchange (IKE) 83
Internet of Things (IoT) 141
Internet Relay Chat (IRC) 107
Intrusion Prevention System (IPS) 165
Intrusive scan 170
IP affinity 138
IP spoofing 101
ipconfig 173
IPsec 35, 81
  AH 83
  IKE 83
  ISAKMP 83
  Security association 84

Transport mode 82
Tunnel mode 82
ISAKMP 83

J

Jailbreaking 69
Jamming 111
Jitter 141
John the Ripper 108, 172

K

Kali linux 171
Kerberos 35, 44, 167
authentication 32
Key escrow 25
Key exchange 19, 20
DHE method 12
ECDHE method 12
In-band 11
out-of-band 12
RSA method 12
Key pinning 26
Key recovery 25
Key ring 89
Key space 8
Key strength 8
Key stretching 8
Keystroke logger 100
Kiosk 140
Kismet 162

L

Layer 2 Tunneling Protocol (L2TP) 81
Layer 3 switch 58
LDAP injection 115
Least functionality 132
Least privilege management 101, 121
Legacy 142
Legacy systems
Issues 86
Legal hold 177
Lightweight Directory Access Protocol (LDAP) 45
Lightweight EAP (LEAP) 41
Linear tap 166
Live CD 143
Load balancer 137
Active-active 137
Active-passive 137
Location-based polices 34
Logic bomb 98
Logical controls 123
Loki 99
Loop
Network switching 54

M

M of N control 25
MAC filtering 62, 73
MAC spoofing 101
Mail gateway 88
Management controls 122
Mandatory Access Control (MAC) 37
Mandatory vacation 121
Man-in-the-browser (MITB) 100
Man-in-the-Middle 102
Mantrap 94, 150
Masquerading 94
Master key 15
MD5 ..... 14, 89
Mean Time Between Failures (MTBF) 155
Mean Time To Repair (MTTR) 155
Media gateway 89
Memorandum of Agreement (MOA) 119
Memorandum of Understanding (MOU) 119
Memory leak 114
Memory management 128
Message Authentication Code (MAC) 15, 86
Message digest 22
Metasploit 171
Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) 41
Mirroring port 166
MMS 69
Mobile device
App stores 69
Carrier unlocking 69
Custom firmware 68
Jailbreaking 69
OTA updates 67
Privilege abuse 69
Rooting 69
Sideloading 68
Mobile Device Management (MDM) 66
Model verification testing 129
Monitor mode 161, 162
Motion detection 149
MS-CHAPv2 ..... 35, 41
Multifactor authentication 35
Multi-function Devices (MFD) 140
Mutual authentication 35, 41

N

NAT 56
dynamic 57
static 57
NAT overloading 57
Nation state threats 92
NAT-T 56, 83
NDA 119, 122, 159
Near Field Communication (NFC) 111
Nessus 169

NetBus 99
Netcat 169, 172
netstat 174
NetStumbler 162
Network Access Control (NAC) 79
Agent-based 80
Agentless 80
Dissolvable 80
Permanent 80
Network mapper 172
Network Time Protocol (NTP) 167
Network-based Intrusion Detection Systems (NIDS) ..... See NIDS
New Technology LANMAN (NTLM) 40
NIDS 164
NIPS 165
NMAP 169, 172
Nonce 8
Non-credentialed scan 170
Non-Disclosure Agreement (NDA) ..... *See* NDA
Non-intrusive scan 170
Non-repudiation 9, 19, 120
nslookup 174

O

Obfuscation 9
Object Identifiers (OID) 24
OCSP stapling 26
One-time Password (OTP) 31
Online Certificate Status Protocol (OCSP) 26
Open Authorization (OAUTH) 47
Open Shortest Path First (OSPF) 57
OpenID Connect 48
OpenPGP 89
OpenSSH 84
OpenVAS 169
OpenVPN 78
Operational controls 123
Ophcrack 108, 172
Order of volatility 176
Organized crime 92
Over The Air (OTA) 132

P

Parabolic antenna 61
Parallel tap 166
Pass the Hash 40, 109
Passphrase 31
Password 31
complexity 48
length 48
lifetime 49
Password Authentication Protocol (PAP) 40
Password cracker 108, 172
Password policy 48
PAT 57
Patch management 132
Patent 160
Pattern matching 66
PBKDF2 8
PCI-DSS 119
Penetration testing 170
Pentoo 171
Perfect Forward Secrecy 12, 87
Performance baselines 130
Persistence 99, 138, 171
Personal Firewall (PFW) ..... *See* Firewalls
Personal Information Exchange (PFX) 29
PHI 160
Phishing 95
Physical controls 123
Piggybacking 94
PII 160
PIN 31
ping 175
PIV 32
Pivot 171
Plain text 7
Platform as a Service (PaaS) 147
Pointer dereference 113
POODLE 87, 103
POP3 89
POPS 89
Port scanner 172
Port Security 73
Positive ventilation 150
Preservation of Evidence 176
Pretty Good Privacy (PGP) 24, 89
Preventative controls 123
Principal 47
Priority queuing 137
Privacy Enhanced Mail (PEM) 29
Privacy officer 159
Privacy policy 65, 120
Private cloud 148
Private key 19
Privilege creep 38, 121
Privilege escalation 112, 121, 171
Production environment 136
Promiscuous mode 161, 162
Proprietary data 160
Protected EAP (PEAP) 42
Protected Health Information (PHI) ..... *See* PHI
Protocol analyzer 162
Provisioning 142
Proximity card 32
Proxy server 76
Forward 76
Reverse 76
Transparent 76
Pscan 172
Pseudo-random number generator 7
Public cloud 148
Public key 19

Public Key Cryptography (PKC) 18
Public Key Cryptography Standard #12 (PKCS #12) 29
Public Key Cryptography Standard #7 (PKCS #7) 29
Public Key Infrastructure (PKI) 22
Pulping 161
Pulverizing 161
Purging 161
Push notifications 67
Putty 84

Q

QinQ attacks 55
Qualitative risk 153
Quality of Service (QoS) 89, 137
Quantitative risk 154
Quarantine portal 80

R

Race condition 105, 113
Radio Frequency Identification (RFID) ..... See RFID
Radio Frequency Interference(RFI) 151
RADIUS 43
RADIUS federation 63
Rainbow cracking 109, 172
Rainbow tables 109
RainbowCrack 108, 172
Ransomware 100
RC4 ..... 16, 184
RC6 16
Real-time Control Protocol (RTCP) 90
Real-time Operating System (RTOS) 141
Real-time Transport Protocol (RTP) 90
Recertification 121
Recovery agent 25
Recovery controls 124
Recovery point objective (RPO) 155
Recovery Time Objective 158
Recovery time objective (RTO) 155
Refactoring 101
Remote access control
  authentication 42
  RADIUS 43
  TACACS+ 43
Remote Access Control
  Diameter 43
Remote Access Trojan (RAT) 99
Remote Desktop Protocol (RDP) 85
Remote wipe 67
Replay attack 102, 109
Resource exhaustion 104, 105, 113
Resource Record Signature (RRSIG) 73
Reverse IP lookup 34
RFID 34, 112
RIPEMD 89
RIPEMD-160 14
Risk 155
Risk Acceptance 156
Risk assessment 152
Risk Avoidance 155
Risk Management 152
Risk Mitigation 156
Risk register 153
Risk Transference 156
Rogue Access Point 110
Role-Based Access Control (RBAC) 38
Root of trust 131
Rooting 69
Rootkits 99
ROT13 10
Rotation of duties 121
Round robin 138
Router 57
Routing Information Protocol (RIP) 57
Routing protocols
  BGP 58
  OSPF 57
  RIP57
RSA 20, 89
Rule-Based Access Control (RBAC) 38
Runtime code 126

S

S/MIME 89
SAFER 184
SAINT 169
Salt 8, 109
Same key 15
Sandbox environment 136
Sandbox security model 143
Sandboxing 52, 80, 110, 143
SATCOM 67
SCADA 141
SCP 84, 88
Screen locks 67
Script kiddies 92, 93
Secret key 15
Secure boot 114, 131
Secure Real-time Transport Protocol (SRTP) 90
Secure Shell (SSH) 84
Secure Socket Layer (SSL) 86
Security as a Service 148
Security Assertion Markup Language (SAML) 46
  Token-based authentication 32
Security Association (SA) 84
Security baselines 130
Security by obscurity 9
Security guards 94, 150
Security Information and Event Management (SIEM) ..... *See* SIEM
Security templates 133
Self-Encrypting Drive (SED) 135
Separation of duties 121
Serpent 16

Server clustering 137
Service Level Agreement (SLA) 119
Service Provider 47
Service Set ID (SSID) 60
SSID broadcasting 60
Session hijacking 103
Session Initial Protocol (SIP) 90
Session key 15
SFTP 84, 88
SHA 89
SHA-1 14
SHA-2 ..... 14, 89
SHA-3 14
Shared key 15
Shibboleth 48
Shimming 101
Shoulder surfing 94
Shredding 161
Sideloading 68
SIEM 168
Signature-based detection 162
SIM 68
Simple Network Management Protocol (SNMP) 85
Single key 15
Single Loss Expectancy (SLE) ..... *See* SLE
Single Sign-On (SSO) 36
SLE 154
Slogin 84
Smart card 32, 135
SMS 69
SMTP 88
SMTPS 88
Smurf attack 106
Snapshots 145
Sneakernet 51, 68
SNMPv3 85
Social engineering 93, 98
Software as a Service (SaaS) 146
Software Defined Networking (SDN) 147
Software Development Kit (SDK) 127
Source code 126
SOX 119
Spam 96
Spam over Instant Messaging (SPIM) 96
Spam over Internet Telephony (SPIT) 90, 96
SPAN 167
Spanning Tree Protocol (STP) 54
Spear phishing 95
Spoofing 101
Spyware 99
SQL injection 114
SSH 84
SSL decryptor 167
SSL VPN tunnel 81
SSL/TLS Accelerator 135
SSO 36
Staging environment 136
Stateful firewall 105
Stateful Firewall 76
Stateless Firewall 75
Static NAT 57
Steganography 9
Stream Cipher 11
Stress testing ..... 172, *See* Fuzzing
Strong authentication 35
Strong password 31
Subject Alternative Name (SAN) 28
Substitution Cipher 10
SuperScan 172
Supervisory Control And Data Acquisition (SCADA) ..... *See* SCADA
Switch 53
Access port 53
Multilayer 58
Trunk port 53
Switching loops 54
Symmetric cryptography 15
SYN flood 105
Syslog 167
System on a Chip (SoC) 141

T

TACACS+ 35, 43
Tailgating 94
TCPDump 162, 174
Technical controls 123
Telnet 85, 169
Termination 122
Test environment 136
Tethering 68
Third party access 149
Threat assessment 153
Time-of-day restrictions 39
TLS VPN tunnel 81
TOC/TOU 80
Token-based authentication 32
Asynchronous 32
Dynamic tokens 32
hardware-based 32
software-based 32
Static tokens 32
Synchronous 32
TOTP 32
TPM 131, 135
tracert 175
Trade secret 160
Transaction Signature (TSIG) 73, 104
Transitive trust 36
Transparent Data Encryption (TDE) 134
Transport Layer Security (TLS) 86
Transposition Cipher 10
Trojan horse 98
True negative 169
True positive 169
Trust model

Hierarchical....24
Peer-to-Peer (P2P)....24
Trusted firmware....131
Trusted operating system....130
Trusted Platform Module (TPM)....*See* TPM
Trusted Root Certificate Authority....23
Tunneling....77
Turnstiles....94
Two-factor authentication....35
Twofish....16, 89, 184
Typo squatting....96

U

Unified Extensible Firmware Interface (UEFI)....131
Unified Threat Management (UTM)....168
URL hijacking....96
USB OTG....68, 135
User ID....30

V

Vampire tap....166
VDI....144
Non-persistent....145
Persistent....144
Vendor diversity....88, 125
Virtual Desktop Infrastructure (VDI)....66, *See* VDI
Virtual IP address....138
Virtual LAN (VLAN)....52, 54
Tagging....54
Virtual Private Network (VPN)....77
Virtualization....52, 143
Virtualization Technology....143
Virtualization Vulnerabilities....145
Virus....97
Vishing....95
VLAN Trunking Protocol (VTP)....55
VM sprawl....145
Voice over IP (VoIP)....90
VPN Concentrator....79
VPN tunnel....78
Always-on....79
Full tunnel....78
Host-to-host....78
Host-to-site....78
Site-to-site....78
Split tunnel....79
Vulnerability assessments....168
Vulnerability scanning....169

W

Warm site....157
Waterfall model....125
Watering hole attack....96
Web Application Firewall (WAF)....77
Web conferencing....90
Web spoofing....101, 104
Web-based access control
OAUTH....47
OpenID Connect....48
SAML....46
Shibboleth....48
Whaling....95
Whirlpool....14
White box....173
Whitelisting....96, 114, 132
WiFi....59
WiFi Protected Access (WPA)....64
WiFi Protected Access version 2 (WPA2)....65
Wi-Fi Protected Setup (WPS)....62
WinDump....162
Wiping....161
WIPS....110
Wired Equivalent Privacy (WEP)....63
Wireless Access Point (WAP)....58
Controller-based....59
Guest mode....62
Standalone....58
WPS....62
Wireless Intrusion Prevention System (WIPS)....*See* WIPS
Wireless Local Area Network (WLAN)....59
Wireless Personal Area Network (WPAN)....59
Wireshark....162
WLAN....53
Ad Hoc mode....59
Association....60
Beacon frame....60
Disassociation....60
Enterprise authentication....63
Guest network....53
Infrastructure mode....59
Open authentication....62
PSK authentication....63
Worms....97
Write Once Read Many (WORM)....167
WTLS....86

X

X.509....24
XML Injection....116
XSRF....117
XSS....116

Y

Yagi antenna....61

Z

Zero Day attack....104
Zeroization....161
Zombie....107