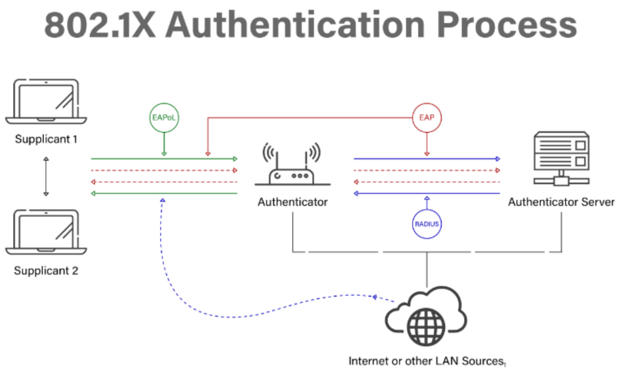
Security+ Notes

#

802.1x

IEEE standard that defines port-based network access control. Centralized wireless authentication. Extensible Authentication Protocol (EAP) integrates with 802.1x.

Port-based Network Access Control (NAC). No access to the network until the user is authenticated. Used in conjunction with an access database i.e. RADIUS, LDAP, TACACS+, Kerberos.



802.11

WLAN standard. Allow you to apply a security control that ties physical ports to end-device MAC addresses. One of the most popular communication methods today. Does not imply full connectivity between nodes.

A

AAA: Authentication, Authorization, Accounting

Authentication: confirms a user's identify using some kind of authentication scheme.

Authorization: controls the authenticated user's access rights and permissions to certain objects.

Accounting: tracks data usage and network resources for auditing purposes.

ABAC: Attribute-based Access Control

Access control model that defines permission based on attributes associated with entities. Uses statements that closely resemble natural language.

Properties used to define access policies in ABAC:

- Subject (i.e. user or process requesting access)

- Type of action (“read”, “write”, “execute”)
- Resource type (medical record, back account etc.)
- Environment (contextual data, such as time of day or geolocation)

Acquisition

The process of extracting all the digital contents from seized evidence for analysis. Important to extract the contents without making any changes to the original copies. When performing an acquisition, the investigator must prepare the destination media, prevent changes to the original media, hash the evidence, copy the evidence, verify the copy, and finally keep the original evidence in a safe and secure location.

ACL: Access Control List

A list of rules used to control access to network resources. Implemented on routers, switches, and firewalls.

AES: Advanced Encryption Standard

AES-CCMP: Advanced Encryption Standard – Galois / Counter Mode with Pipeline

AES-GCMP: Advanced Encryption Standard – Counter with Cipher Block Chaining Message Authentication Code Protocol

AH: Authentication Header

Protocol used in IPsec. Provides data integrity, data origin authentication, and anti-replay service for IP packets.

AIS: Automated Indicator Sharing

U.S. Government initiative for real-time sharing of cyber threat indicators.

ALE: Annualized Loss Expectancy

Refers to the estimated financial loss that an organization can expect to incur in a year due to a specific risk event. Calculated by multiplying the Annualized Rate of Occurrence (ARO) by the Single Loss Expectancy (SLE). ALE = ARO * SLE.

ARO: Annualized Rate of Occurrence

Represents the estimated frequency with which a specific risk event is expected to occur within a given time limit, typically on an annual basis. Key factor in calculation of risk metrics such as Annualized Loss Expectancy (ALE).

ARP: Address Resolution Protocol

ARP Poisoning:

Happens when an attacker changes the ARP cache to change the mappings of IP address to MAC address. This could redirect a victim’s traffic to the attacker’s computer, enabling an on-path or man-in-the-middle (MitM) attack.

Autopsy

Open-source forensic platform that allows one to examine the contents of a hard drive or mobile device and recover evidence from it. Can be used to find evidence in an image collected by dd or FTK Imager.

B

Backups

Refers to the process of creating and maintaining copies of data to ensure its availability and recoverability in the event of data loss, corruption, accidental deletion, or other unforeseen events. The three types of backups:

- Full: Makes a backup of everything and clears the archive bit on all files.
- Incremental: Backs up only the files that have been changed since the last incremental or full backup (i.e. only those with archive bits set) and clears the archive bits.
- Differential: backs up only the files that have been changed since the last full backup. Does not change the archive bits.

Blue Jacking

Sending unsolicited messages to another device via Bluetooth.

Blue Snarfing

Refers to accessing a Bluetooth enabled device and transferring data without the user's consent.

BPDU: Bridge Protocol Data Units

Used by switches running Spanning Tree Protocol (STP) to communicate with each other and determine the topology of the network.

BYOD: Bring Your Own Device

Allows employees to use private mobile devices for accessing company's restricted data and applications.

C

CA: Certificate Authority

Trusted third party that issues digital certificates used for creating digital signatures and public-private key pairs.

Captive Portal

Allows administrators to block network access for users until they perform the required action. Used in hotels to provide Wi-Fi access.

CASB: Cloud Access Security Broker

Provides clients working on an organizations network to access cloud services. Acts as a intermediary between users and cloud service providers. Can be used to apply security policies to cloud-based implementations. Two common functions of a CASB are visibility into application use and data security policy use. Other common CASB functions are the verification of compliance with formal standards and the monitoring and identification of threats.

CER: Crossover Error Rate

Performance metric that is used to assess the accuracy and effectiveness of a biometric system. Calculated at the point where FAR & FRR intersect on a receiver operating characteristic.

Certificate changing:

Refers to the process of verifying authenticity of a newly received digital certificate. Such a process involves checking all the certificates in the chain of certificates from a trusted root CA, through any intermediate CAs, down to the certificate issued to the end user. A new certificate can only be trusted if each certificate in that certificate's chain is properly issued and valid.

Channel Overlapping

A situation where multiple channels share the frequency band causing interference and performance degradation for devices operating on channels that are too close to each other.

CHAP: Challenge Handshake Authentication Protocol

Remote access authentication protocol that periodically re-authenticates client at random intervals to prevent session hijacking. Can be used to create secure tunnels for unsecure environments.

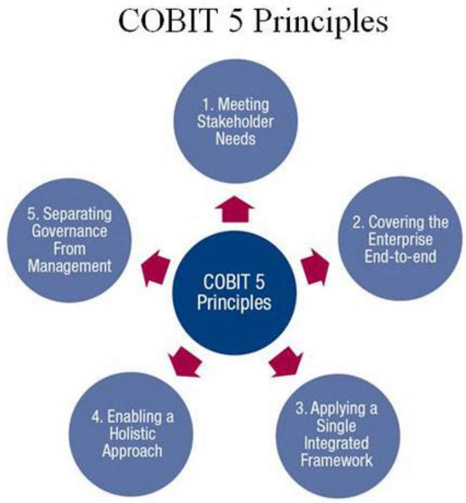
CIS: Center for Internet Security

Client-to-Site

Virtual Private Network (VPN) that enables connectivity between computers and networks.

COBIT: Control Objectives for IT

Business-focused control framework


COBIT 5 Principles
1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Code-signing certificates

Used to verify the authenticity and integrity of software. Self-signed certificates have a lower level of trustworthiness, because they are not signed by a Certificate Authority (CA). Computer certificates (a.k.a. machine certificates) are used to prove the identity of devices. S/MIME certificates are used to encrypt and digitally sign email messages. User digital certificates provide improved security during authentication and authorization of individuals. Root certificates are self-signed certificates that identify a root Certificate Authority (CA). Domain validation certificates prove a user's ownership rights to a domain. Extended Validation (EV) certificates provide the highest level of trust and protection.

COOP: Continuity of Operations

Refers to a U.S. government initiative that provides the details on how to ensure continued performance of essential functions during unexpected events.

Confusion

Means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two. The data that is encrypted looks drastically different than the plaintext from the start. One of the two important characteristics that encryption relies on.

CMMI: Capability Maturity Model Integration

Assess organizations process maturity. The following are the maturity levels different organizations might have:

1. Initial
2. Managed
3. Defined
4. Quantitatively Managed
5. Optimizing

CN: Common Name

In a digital certificate as a field. Describes a device, an individual, an organization, or any other entity the certificate has been issued for. In an SSL certificate, CN refers to the Fully Qualified Domain Name (FQDN), which is the domain name of the server protected by the SSL certificate.

COPE: Corporate-Owned, Personally Enabled

Mobile device management strategy that allows organizations to provide employees with company owned devices while allowing some level of personal use.

CRL: Certificate Revocation List

Provides a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date. Used in the context of Public Key Infrastructure (PKI) to verify the status of digital certificates and ensure the security of online communications.

CSR: Certificate Signing Request

Refers to a method for requesting a digital certificate. In the context of public key cryptography and SSL/TLS certificates, a CSR is a message sent from an applicant to a Certificate Authority (CA) to apply for a digital certificate.

Cuckoo

Open-source automated malware analysis system sandboxing tool. Designed to analyze the behavior of suspicious files and executables in a controlled environment to determine whether they exhibit malicious behavior. Enables analysis of suspicious files in a sandbox environment.

CVE: Common Vulnerabilities and Exposure

CVSS: Common Vulnerability Scoring System

Cyber Kill Chain

A series of steps that outline and trace the stages of a cyber-attack adopted by Lockheed Martin. The following are the steps:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

CYOD: Choose Your Own Device

D

DAC: Discretionary Access Control

Access control model based on user identify. In DAC every object has an owner who uses their own discretion to determine what kind of permissions other users can have for that object.

Data Masking

Involves replacing sensitive data with non-sensitive characters. For example, receipts commonly have all, but the last four digits of a credit card number masked with asterisks/dots.

Data Minimization

Involves collecting and storing only sensitive data that the organization needs. This is the most effective method of protecting sensitive data because an organization can't breach/leak data it doesn't have.

DER: Distinguished Encoding Rules

Digital certificate. Has the following format:

- Encoded in binary format.
- .der and .cer file extensions.
- Generally used for Java servers.

DHCP: Dynamic Host Configuration Protocol

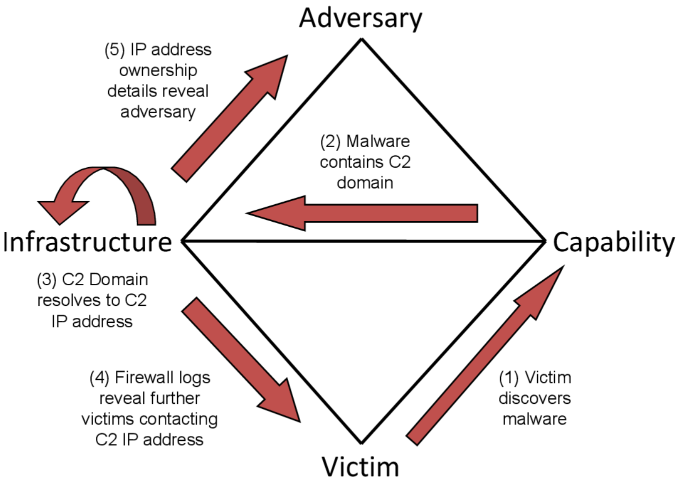
Network management protocol used to assign local IP addresses to devices on a network. It is used to create multiple private IP addresses from one public IPv4 address. Can automatically assign and manage IP addresses and other configuration information. Used on TCP/IP networks.

Port 67/68

DHCP Snooping

Security feature of a network switch that provides counter measures against rogue DHCP servers. Mitigates the risk of unauthorized or malicious DHCP servers on a network.

Diamond Attack Model


Adversary
(5) IP address ownership details reveal adversary
(2) Malware contains C2 domain
Infrastructure
Capability
(3) C2 Domain resolves to C2 IP address
(4) Firewall logs reveal further victims contacting C2 IP address
(1) Victim discovers malware
Victim

Diffusion

Means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change. Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state. One of the two important characteristics that encryption relies on.

Digital certificates

Governed by the X.509 standard. Used in the Public Key Infrastructure (PKI). Allow the secure exchange of public keys.

Digital Signature

A certificate authority will digitally sign a certificate to add trust. If you trust the certificate authority, you can then trust the certificate.

DLL: Dynamically Linked Libraries

DLL Injection

Tricks application into loading malicious code.

DLP: Data Loss Prevention

Software or hardware-based security solutions designed to detect and prevent unauthorized use and transmission of confidential information. Set of tools, processes, and policies designed to prevent unauthorized access, use, and transmission confidential information.

DNSEnum:

Best suited for gathering information about a domain.

DNSSEC

Suit of security extensions for an internet service that translates domain name into IP addresses. Can be used to add digital signatures to DNS.

DPI: Deep Packet Inspection

Used in next-generation firewalls (NGFW) to perform deep packet inspection.

Driver Refactoring

Refers to modifying driver to carry out malicious activities. Requires access to the driver source code.

Driver Shimming

Wraps legitimate driver with a malicious shim. Does not require access to the legitimate driver's source code.

E

EAP: Extensible Authentication Protocol

Authentication protocol introduced with Wi-Fi Protected Access (WPA). Provides standards for the transport and usage of authentication protocols.

EAP-FAST

EAP variant developed by Cisco as a replacement for LEAP. Authentication server and supplicate share a protected access credential (PAC) shared secret. Authenticate over TLS.

EAP-TLS

Uses Transport Layer Security (TLS) tunnels to secure EAP traffic and often relies on digital certificates for authentication. Highest level of security. Does not provide a mechanism for using multiple authentication types within a TLS tunnel.

EAP-TTLS

Tunneled Transport Layer Security: Uses a server-side certificate for authentication and to create a secure tunnel. Clients can be authenticated via a certificate or via a secure tunnel. Requires digital certificate of the Authentication Server (AS). Does not require digital certificates on every device. Allows the use of any authentication while maintaining confidentiality with TLS.

East-West Traffic

Refers to the communication or data flow that occurs horizontally within a network or data center.

ECB: Electronic Codebook

Block cipher mode of operation simple mode where each block of plaintext is independently encrypted using the same key.

ECC: Elliptic Curve Cryptography

Used in asymmetric encryption, secure communication protocols, digital signatures, and encryption. Suitable for small wireless devices.

EDR: Endpoint Detection and Response

Endpoint security solution that provides the capability for detection, analysis, response, and real-time monitoring. Can be used on host computers.

Egress

Refers to the movement of data leaving a network.

Elliptic Curve

Elliptic Curve Cryptography (ECC) uses smaller keys than non-ECC encryption and has smaller storage and transmission requirements. These characteristics make it an efficient option for mobile devices.

Ephemeral Key

Uses Asymmetric keys used for single session or transaction.

Entropy

Refers to the unpredictability of a random number or cryptographic key.

ESP: Encapsulating Security Payload

Provides security services for IP traffic. Provides confidentiality and integrity protection for packet payloads.

F

FACL: File Access Control List

List of permissions or rules associated with a file or directory. Provides file-grained control over access than traditional Unix/Linux file permissions. Uses rule-based access control mechanism associated with files and/or directories.

FAR: False Acceptance Rate

Faraday cage

Protects servers against any unwanted electromagnetic fields. Mesh of conductive material that will cancel electromagnetic fields.

FDE: Full Disk Encryption

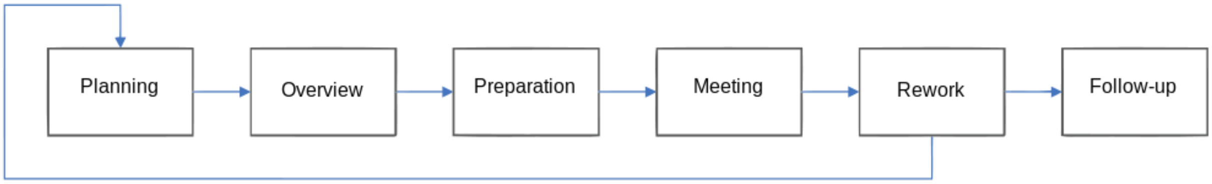
Data protection method that encrypts an entire storage device.

Forward Proxy

Hides the identity of a client and acts on the client's behalf.

FRR: False Rejection Rate

Fagan Inspection Code Review



FTK Imager

An AccessData tool used to create drive images for analysis in FTK or Autopsy.

Fuzzing

Fuzz testing, a software testing technique that feeds software many different input values in an attempt to cause an unpredictable state or unauthorized access. The follow are two types of fuzzing methods:

- Generation Fuzzing: Uses random values.

- Mutation Fuzzing: Modifying real input.

G

Galt Analysis

Study and Evaluation of a person's body movement

GCM: Galois Counter Mode

Authenticated encryption block cipher mode widely used for security network communications.

H

Heat-Map

Can help with identifying areas of low signal strength. Can help with placement of multiple Access Points (APs).

HOTP: HMAC-based One-time Password

Commonly used in two factor authentication based on HMAC-SHA algorithm.

HSM: Hardware Security Module

Dedicated hardware device or appliance designed to provide secure key storage, cryptographic operations, and other security services.

HSTS: HTTP Strict Transport Security

Response header that will block communication via HTTP and force the browser to use only HTTPS.

I

IAM: Identity and Access Management

Controls wo gets access and what they get access to. Provides access to cloud resources.

ICMP: Internet Control Message Protocol

Housekeeping protocol of the internet. Used in ping commands to identify live systems.

ICS: Industrial Control System

IdP: Identifying Provider

A trusted entity that manages and authenticates user identities. Plays crucial role in Single-Sign On (SSO).

Ifconfig

Linux command-line utility for network interface configuration.

IoC: Indicator of Compromise

Forensic evidence that can be used to detect unauthorized access attempts or other malicious activities.

IMAP: Internet Message Access Protocol

E-mail protocol used by e-mail clients to communicate with e-mail servers. Provides two-way communication unlike POP. Email retrieval and storage protocol. Secured IMAP uses TLS to encrypt communications.

Port 143, 993 (secured)

Incident Response Process

Six-step incident response process

1. Preparation: Before an incident occurs, the organization should prepare by creating an incident response team (IRT) and defining the processes and procedures that they will follow when managing an incident.
2. Identification: At some point, a user may notice that a potential incident has occurred and alert the incident response team. A first responder will validate that an incident has occurred and either handle or escalate it.
3. Containment: After verifying the issue, the first responder should isolate it to manage the scope and impact of the incident.
4. Eradication: When the incident is contained, the IRT will investigate and develop and implement a remediation strategy.
5. Recovery: After the incident is over, the IRT can restore the system to normal operation based on predefined procedures.
6. Lessons Learned: After the recovery is complete, the IRT should perform a retrospective to determine what did and didn't go well. This might help with identifying inefficient IR processes or the root cause of the incident that can be corrected to prevent future, similar incidents from occurring.

Ingress

Refers to the management of data entering a network.

Ipconfig

Windows command-line utility that can be used to display TCP/IP configuration settings.

IPFIX: Internet Protocol Flow Information Export

Standard for collecting and exporting network flow information. It is defined by the Internet Engineering Task Force (IETF) in RFC 7011 and is an evolution of the earlier NetFlow protocol.

IR: Infrared

ISO: International Organization for Standardization

ISO/IEC 27001

Standard defining requirements for information security management system objectives.

ISO/IEC 27002

Code of practice for information security control complementation.

ISO/IEC 27707

Privacy data management.

ISO/IEC 3100

Principles and guidelines for risk management.

J

journalctl

Refers to a Linux utility for querying and displaying logs that are stored in binary form.

Jump Server

Best suited to act as an intermediary between an intranet and a screened subnet. Hardened server used as a secure gateway for remote administration of devices placed in a different security zone.

K

KBA: Knowledge-based Authentication

Uses specific pieces of information known by the user.

Kerberos:

Relies on Network Time Protocol (NTP). Can be used to enable SSO in Windows-based network environments. Assigns a unique encrypted key, called a ticket, to each user that logs on to the network. The client's timestamp is used to provide a counter measure against Replay attacks and eavesdropping. The drawback is that it relies on a centralized server such as a domain controller. If the domain controller fails, clients and servers can no longer authenticate. Allows for communication over a non-secure network. Only need to authenticate once with Kerberos to gain access to multiple resources.

Port 88

Key escrow

A trusted third-party storage solution providing backup source for cryptographic keys. Copies of lost private encryption keys can be retrieved from a key escrow by recovery agents. A recovery agent is an individual with access to a key database and permission level allowing them to extract keys from escrow.

L

L2TP: Layer 2 Tunneling Protocol

Used in Virtual Private Networks (VPN).

LDAP: Lightweight Directory Access Protocol

Used to manage and communicate with directories. A directory is like a database that stores and organizes information in a hierarchical structure. Used in network environments to manage user identities, access, permissions, and other directory-related information.

LDAP comes into play in the context of 802.1X in the following ways:

- User Authentication: When a device, like a computer or a smartphone, wants to connect to a secured network using 802.1X, it needs to prove its identity. LDAP is often used for checking the username and password during the authentication process.
- Access Control: LDAP can store information about which users or devices are allowed to connect to the network. The directory can contain details about group memberships, permissions, and other access control information.
- User Management: LDAP can be a central place to manage user identities, making it easier to add, remove, or modify user accounts. When a user's information changes, it's updated in the LDAP directory, influencing how 802.1X processes authentication and access.

Port 389

LDAPS: Lightweight Directory Access Protocol over Secure Socket Layer

Secure directory protocol. Uses TLS.

Port 636

Least Connection Method

A load balancing algorithm used in networking to distribute incoming network traffic across multiple servers based on the number of active connections. The server with the least number of active connections receives the new incoming connection.

M

MAC: Mandatory Access Control

Access control module that enforces the strictest set of access rules. Assigns clearance levels.

Characteristic features:

- Users are not allowed to change access policies at their own discretion.
- Labels and clearance levels can only be applied and changed by an administrator.
- Every resource has a sensitivity label matching a clearance level assigned to a user.

MAC Filtering

Refers to the process of controlling access to a network based on the Media Access Control (MAC) addresses of individual devices. A unique identifier assigned to the Network Interface Card (NIC) of each networked device. 48-bit physical address.

MAM: Mobile Application Management

Type of security management solution that focuses specifically on controlling and securing access to mobile applications used in enterprise environment.

MDM: Mobile Device Management

Type of security software used by organizations to monitor, manage, and secure employees mobile devices.

MFD: Multifunction Device

An all-in-one printer that can print, scan, and fax is often categorized as an MFD.

MIME: Multipurpose Internet Mail Extensions

MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge

Knowledge base and framework that is widely used in the field of cybersecurity. Provides comprehensive and up-to-date understanding of the tactics, techniques, and procedures (TTPs) employed by cyber adversaries during various stages of the cyber kill chain.

Mobile Hotspot:

Refers to a type of WLAN that enables network access through a mobile device that acts as a portable WAP.

MTBF: Mean time between failures

The average time between failures of a system or component. MTBF is the time between repairable failures, while MTTR is the time until a component might be replaced.

MTTF: Mean Time To Failure

The average amount of time a system or component can operate before it fails.

MTTR: Mean Time To Repair/Recovery

The average time it takes to recover a system from a failure.

Multipath I/O

Framework that improves fault tolerance and performance by enabling additional alternate routes for data that is being transferred to and from storage devices.

N

NAC: Network Access Control

Security technology that restricts access to a network based on policies and the security status of the devices trying to connect to the network.

NAT: Network Access Translation

Networking technique used to modify network address information in packet headers while in transit, typically in routers or firewalls. The primary purpose of NAT is to conserve IP addresses and enable multiple devices within a private network to share public IP addresses when communicating with external networks.

Netcat

Network debugging and exploration tool that can read and write data across TCP or UDP connections.

Netstat

Command-line utility used for displaying active TCP/IP connections and network protocol statistics. Can be used to monitor open ports on a computer.

netstat -na: shows all open ports.

netstat -r: displays routing table contents

NFC: Near Field Communication

Refers to communication that is used by devices to communicate in proximity. Usually used with mobile devices.

NIC Teaming

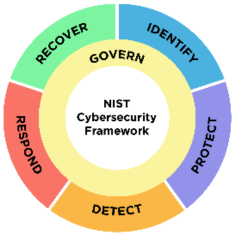
Process of combining multiple physical network adapters into a single logical interface for increased throughput and redundancy.

NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

Security controls mandatory for federal agencies.

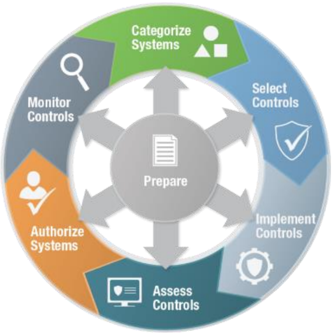
NIST CSF: Cybersecurity Framework

Framework outlining best practices for computer security.



NIST RMF: Risk Management Framework

IT security and risk management framework.



Nmap

Command-line tools used for discovering hosts and service on a network.

Non-Repudiation

A concept in information security and cryptography that refers to the assurance that a party involved in a communication or transaction cannot deny the authenticity or origin of the message or action.

Nontransparent proxy

Modifies client's requests and responses. Requires client-side configuration.

North-South Traffic

Refers to the communication or data flow that occurs vertically between different layers of the network. Involves interactions between client and servers.

NTP: Network Time Protocol

Used for synchronizing clocks of computer systems over a network.

NVD: National Vulnerability Database

NXLog

Cross-platform log-managing tool. Designed to collect, process, and forward log data in various formats from different sources. Commonly used in enterprise environments and Security Information and Event Management (SIEM) solutions to facilitate efficient log management and analysis.

O

OAuth

Authorization

OCSP: Online Certificate Status Protocol

Fastest way to check the validity of a digital certificate. Protocol used to check the revocation status of digital certificates in real-time. Alternative to using Certificate Revocation Lists (CRLs) for verifying the validity of certificates in a Public Key Infrastructure (PKI). Can be checked to see whether a digital certificate has been revoked.

Omnidirectional Antenna

Refers to a common antenna type used as a standard equipment on most Access Points (Aps) for indoor Wireless Local Area Networks (WLAN) deployments. Provides 360-degreee horizontal signal coverage. Sends signals in all directions donut shaped pattern.

OPAL: Open-source Security Service

Set of specifications for implementing Self-Encrypting Drives (SEDs). Defined standardized way for manufacturers for managing SEDs.

OpenID

Authentication

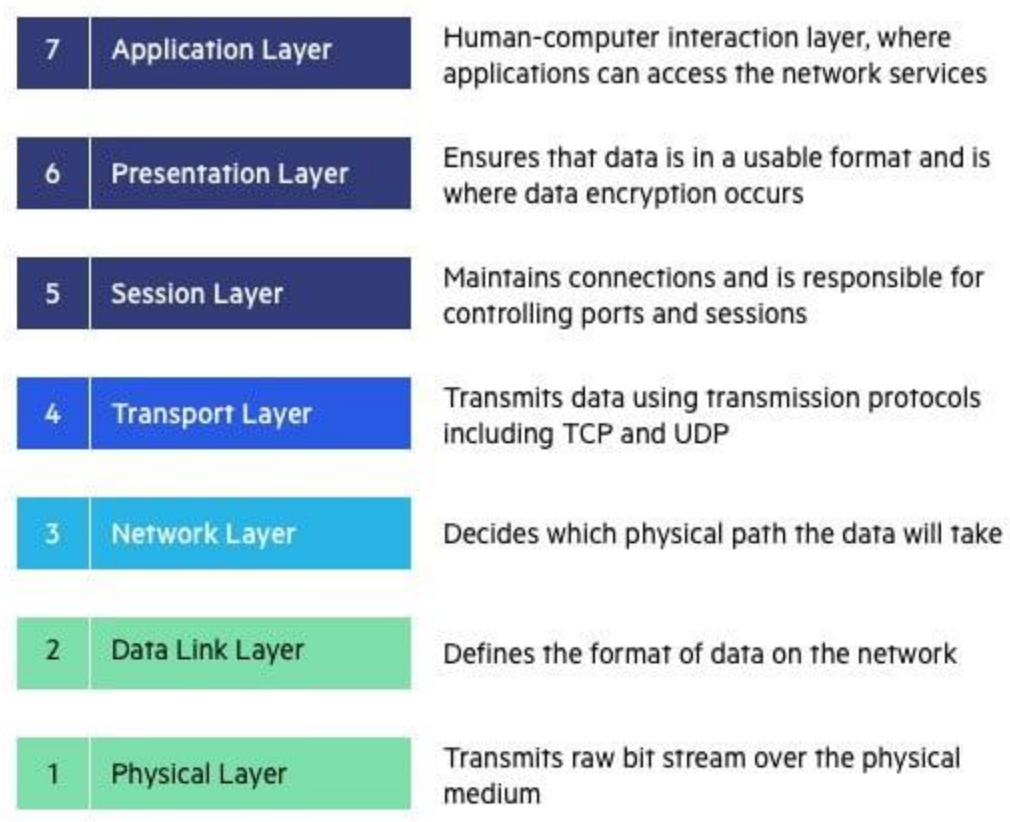
Order of volatility

In forensic procedures, a sequence of steps in which different types of evidence should be collected. The order of volatility for a typical computer system:

Cache memory -> RAM -> Swap/Pagefile -> Temporary files -> Disk files -> Archival media

OSI: Open Systems Interconnection

OSI Model



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

OTA: Over the Air

Wireless transmission of data, updates, or applications directly to electronic devices. Such as smartphones, tablets, or IoT devices.

OTG: USB On the Go

Specification that allows USB devices like smartphones and tablets to act as a host. Enabling them to connect to and communicate with other USB peripherals directly without the need of a computer.

P

P7B:

Digital certificate. Has the following format:

- Encoded in text (ASCII Base64) format.
- .p7b file extension.
- Generally used for Microsoft windows and Java Tomcat servers.

PAM: Privileged Access Management

Security solution that provides control over elevated accounts.

PAP: Password Authentication Protocol

Deprecated and obsolete authentication protocol that sends passwords in cleartext.

Pathping:

The network command-line utility in MS Windows combines the features of ping and tracert.

PBX: Private Branch Exchange

Make an internal phone connection and provide connectivity to the public switch telephone network.

PEM: Privacy Enhanced Email

Digital certificate. Has the following format:

- Encoded in text (ASCII Base64) format.
- .pem, .crt, .cer and .key file extensions.
- Generally used for Apache servers or similar configurations.

PFS: Perfect Forward Secrecy

Property that ensures that even if a long-term secret key is compromised past communication remains secure. Designed to strengthen the security of session keys.

PFX: Personal Information Exchange

P12 digital certificate. Has the following format:

- .pfx and .p12 file extensions.

- Generally used for Microsoft windows servers.
- Encoded in binary format.

Ping

Command-line utility used for checking the reachability of a remote network host.

Pinning:

Refers to a deprecated security mechanism designed to defend HTTPS websites against impersonation attacks performed with the use of fraudulent digital certificates.

PKI: Public Key Infrastructure

Comprehensive system designed to manage digital keys and certificates. PKI facilitates secure communication and helps establish the identify of users, devices, and entities in a networked environment. Uses hierarchical system for the creation, management, storage, distribution, and revocation of digital certificates.

PKI role of Registration Authority (RA):

- Accepting request for digital certificates
- Authenticating the entity making the request

PKI Trust Models:

- Single CA Model
- Hierarchical model (root CA + intermediate CAs)
- Mesh model (cross-certifying CAs)
- Web of trust model (all CAs act as root CAs)
- Client-server mutual authentication model

POP: Post Office Protocol

E-mail protocol that allows e-mail clients to communicate with e-mail server. POP provides only one-way communication.

Port 110

POP3: Post Office Protocol Version 3

Secured standard TLS email protocol email retrieval.

Port 995

Port Mirroring

Allows administrators to inspect traffic passing through a network switch.

PPTP: Point-to-Point Tunneling Protocol

Network protocol that enables creation of Virtual Private Networks (VPN). Deprecated.

PSK: Pre-Shared Key

Passphrase or shared secret that is used to authenticate and establish a secure connection between devices in a network. Used in Wi-Fi Protected Access (WPA) and WPA2.

Q

QoS: Quality of Service

Refers to a set of technologies and techniques used in computer networks to manage the quality and reliability of communication services. QoS prioritizes and controls the delivery of network traffic.

R

RADIUS: Remote Authentication Dial-In User Service

Provides centralized authentication, Authorization, and Accounting (AAA). Primarily used for network access. Combines authentication and authorization. Encrypts only the password in the access-request packet.

RAID: Redundant Array of Independent Disks

Technology that combines multiple physical disk drives into a single logical unit for the purpose of data storage and performance improvement.

RAID 0 (Striping):

Data is divided into blocks, and each block is written to a different disk drive. This provides increased performance but no redundancies. Requires 2 drives.

- Advantages: Improved performance due to parallel read and write operations.
- Disadvantages: No fault tolerance; if one drive fails, all data is lost.

RAID 1 (Mirroring):

Data is duplicated across two drives (mirrored). Reads and writes can occur on both drives simultaneously. Designed for data redundancy and fault tolerance. Requires 2 drives.

- Advantages: Redundancy; if one drive fails, the other contains an exact copy of the data.
- Disadvantages: Cost efficiency is lower as it requires twice the storage capacity for mirroring.

RAID 5 (Striping with Parity):

Data is stripped across multiple drives, and parity information is distributed across all drives. If one drive fails, data can be reconstructed using parity information. Provides a good balance between performance, capacity, and fault tolerance. Requires minimum of 3 drives.

- Advantages: Good balance of performance and fault tolerance.
- Disadvantages: Slower write performance due to parity calculations.

RAID 6 (Striping with Dual Parity):

Similar to RAID 5, but with dual parity. Can withstand the failure of two drives without data loss. Requires minimum of 4 drives.

- Advantages: Higher fault tolerance than RAID 5.
- Disadvantages: Slower write performance than RAID 5 due to dual parity calculations.

RAID 10 (Combination of RAID 1 and RAID 0):

Data is mirrored (RAID 1) and then striped (RAID 0). Combines the advantages of mirroring and striping. Requires minimum of 4 drives.

- Advantages: High performance and fault tolerance.
- Disadvantages: Requires a minimum of four drives; cost efficiency is lower.

RAID 50 (Combination of RAID 5 and RAID 0):

Combines the striping of RAID 0 with the distributed parity of RAID 5. Requires at least 6 drives.

- Advantages: Balances performance and fault tolerance.
- Disadvantages: Requires more drives and has increased complexity.

RBAC: Rule-Based Access Control

Access control model in which access to resources is granted or denied depending on the contents of Access Control List (ACL) entries. Implemented network devices such as firewalls to control inbound and outbound traffic based on filtering rules. Group based access control.

RCS: Rich Communication Services

Protocol for enhancing the capabilities of SMS and MMS. Allows for more feature-rich and interactive messaging experience.

Remote Access

Refers to the ability to connect to a network from outside.

RFC: Request for Comments

A formal document that describes the specifications for a particular technology.

Reverse Proxy

Hides the identity of a server and acts on it’s behalf.

Risk register

Refers to a document containing detailed information on potential cybersecurity risks.

ROM: Read Only Memory

Where the mobile device’s operating system is located.

Rooting

Refers to the capability of gaining administrative access to the operating system and system applications on android devices.

RPO: Recovery Point Objective

Critical metric in disaster recovery and business continuity planning. RPO defines the maximum acceptable amount of data loss, measured in time, in the event of a disaster or system failure.

RSTP: Rapid Spanning Tree Protocol

Provides faster convergence in ethernet networks while maintaining loop prevention capabilities.

RTO: Recovery Time Objective

Crucial metric in disaster recovery and business continuity planning, representing the maximum allowable downtime for a system, service, or business process after a disruption.

S

SAE: Simplified Authentication and Encryption

Key exchange protocol. Client authentication method used in Wi-Fi protected Access 3 (WPA3).

SAE: Simultaneous Authentication of Equals

Introduced by WPA3. Performs mutual authentication between the access point and the client. SAE means that all WPA3-capable devices will have an encrypted connection to the AP even if no password or authentication server is configured.

SAN: Subject Alternative Name

Digital certificate. Allows multiple domains to be protected by a single certificate.

SAN: Storage Area Network

Dedicated local network of devices providing data.

SCADA: Supervisory control and data acquisition

Refers to a control system architecture used in industrial settings to monitor and control processes, infrastructure, and facilities. The primary purpose of SCADA is to gather real-time data from various sensors and devices in the field, process this data, and provide control commands to remote equipment.

Scannless

Can be used to hide an attacker's identity by utilizing a proxy for port scanning.

SCP: Secure Copy

Provides secure command-line file transfer over SSH.

Port 22

SDN: Software-Defined Network

Programmable network that can consolidate multiple series into one infrastructure.

SDV: Software-Defined Visibility

Visibility infrastructure that combines automation with visibility. Centralized compute and software stacks to control most of their functionality.

SEDs: Self-Encrypting Drives

Type of storage that includes hardware-based encryption capabilities to secure data stored on the drive.

Session Affinity

Refers to a method that ignores the load balancing algorithm by consistently passing requests from a given client to the same server.

Session Key: Uses symmetric key single session.

sFlow: sampled Flow

Refers to a cross-platform IP traffic collection method that takes advantage of packet sampling to optimize bandwidth and hardware resource usage.

SIP: Session Initiation Protocol

Signaling protocol widely used for initiating, maintaining, modifying, and terminating real-time sessions that involve video, voice, messaging, and other communications applications and services between two or more endpoints on IP networks.

Site-to-Site

Virtual Private Network (VPN) that enables connectivity between two networks.

Smishing: SMS Phishing

A social engineering attack that asks for personal information using SMS or text messages.

SMTPS: Simple Mail Transferred Protocol Secure

Deprecated

Port 465

Sn1per

Advanced network exploration and penetration testing tool integrating functionalities from multiple other tools, such as ping, whois, or namp.

SNMP: Simple Network Management Protocol

Used to monitor and manage network devices. Agents are installed on and monitor managed devices, which include computer and network-attached devices such as routers and switches. Many routers and switches support SNMP to manage and organize the information about the network devices. Can be used to aggregate logs in a single location.

SNMP v1 & v2 – Community strings sent unencrypted.

SNMP v3 - protects CIA triad. Confidentiality – encrypted data, Integrity – No tampering of data, Authentication – Verifies the source.

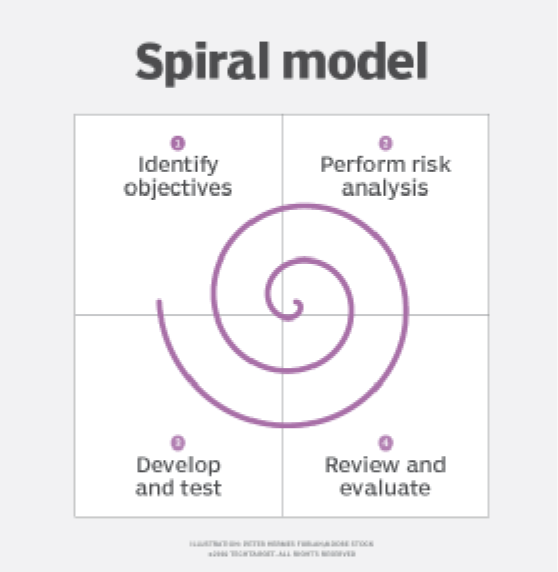
SPIM: Spam Over Internet Messaging

Text-based communication spam.

Split Tunneling

Type of Virtual Private Network (VPN) that alleviates the bottlenecks and conserves bandwidth by enabling utilization of both the VPN and public network links.

Spiral Model



SRTP: Secure Real-time Transport Protocol

Enables secure, real-time delivery of audio and video over the IP network.

Port 5004 UDP

SSH: Secure Shell

Non-proprietary cryptographic network protocol for secure data communication, remote command-line login, remote command execution and other secure network services.

Stapling

Allows for checking digital certificate revocation status without contacting Certificate Authority (CA).

Stateful Inspection

Referred to as dynamic packet filtering. Firewall technology that monitors the state of active connections. Non static packet filtering.

Stateless Inspection

Referred to as static packet filtering. Firewall technology that filters network traffic based solely on the individual packets without considering the context of state of the communication.

Steganography

The practice of concealing one piece of information within another in such a way that it is difficult or even impossible to detect the presence of the hidden information.

STP: Spanning Tree Protocol

Network protocol used to prevent loops in ethernet networks by dynamically discovering and eliminating redundant paths in switches.

STP Frame

Refers to ethernet frames that are used in the context of the Spanning Tree Protocol (STP). Protocol exchanges special frames called Bridge Protocol Data Units (BPDU).

SWG: Secure Web Gateway

A software component or a hardware device designed to prevent unauthorized traffic from entering an internal network of an organization. An SWG implementation may include various security services, such as packet filtering, URL/content filtering, malware inspection, application controls, Acceptable Use Policy (AUP) enforcement, or Data Loss Prevention (DLP).

Syslog

Standardized protocol used for sending log and event messages within a computer network.

Port 514 over UDP

Port 6514 secure TLS

T

TACACS+: Terminal Access Controller Access Control System Plus

Provides Centralized Authentication. Encrypts the entire payload of the access-request packet. Primarily used for device administration. Separates authentication and authorization. Cisco proprietary protocol used for authentication, authorization, and accounting (AAA) services.

Port 49

TCP: Transmission Control Protocol

Tcpdump

Linux utility that can capture network traffic and write it to a packet capture file via the command line.

Tcpreplay

Linux command that can replay traffic captured using tcpdump or similar tools over a network. Converts packet capture files to live traffic. Enables sending custom packets that can be used to evaluate the security of a network device. Packet-crafting tool.

Tethering

A mobile device capability to share its internet connection with other devices.

theHarvester

Python-based tool used for open-source intelligence gathering (OSINT). Can be used to gather email, subdomains, hosts, employee names, open ports, and banners from different public sources like search engines and the SHODAN computer database. Used for information gathering.

TLS: Transport Layer Security

Used to encrypt information like web traffic.

ToCToU: Time of Check to Time of Use

Relates to preventing race conditions.

TOTP: Time-based One-time Password

Commonly used in two factor authentication. Useful authentication control when used in conjunction with other authentication factors.

TPM: Trusted Platform Module

Hardware-based security feature that is part of computers motherboard. Provides a secure and tamper-resistant environment for storing cryptographic keys. Embedded crypto processor. Uses burned-in cryptographic keys and includes built-in protections against brute-force attacks. Specifically designed to assist and protect with cryptographic functions.

Traceroute

Linux command-line utility for displaying intermediary point (routers) the IPv4 packet is passed through on its way to another network node.

Tracert

Network command-line utility in MS Windows that tracks and displays the route taken by IPv4 packets on their way to another host.

Transparent Proxy

Doesn't require client-side configuration, redirects client's requests and responses without modifying them. Clients might be unaware of the proxy server.

TTPs: Tactics, Techniques, and Procedures

Can be used to help security teams understand the behavior of a threat actor.

U

UDP: User Datagram Protocol

UEFI: Unified Extensible Firmware Interface

Modern standard for firmware that replaces the traditional Basic Input/Output System (BIOS) boot process.

UEM: Unified Endpoint Management

Comprehensive approach to managing and securing various types of computing devices within an organization. Single management interface for mobile devices, PC's, printers, IoT devices, and wearables.

UPS: Uninterruptible Power Supply

UTM: Unified Threat Management / Web security gateway

Refers to network security solution that combines functionality of firewall, anti-virus, intrusion detection and prevention, VPN, content-filtering, etc.

V

VDI/VMI: Virtual Desktop Infrastructure / Virtual Mobile Infrastructure

Applications are separated from mobile devices. The data is separated from the mobile device. Allows a mobile device to control a remote server. Technology that allows desktop operating systems, applications, and associated data to be centralized and hosted on servers in a data center. Allows mobile device to act as a terminal for accessing data and applications hosted on a remote server. Virtual desktops access by thin client devices. Allows field teams to access their applications from many different types of devices without the requirement of a mobile device management or concern about corporate data on the devices.

VIP/VIPA

IP address that doesn't correspond to any actual physical network interface.

VLAN: Virtual Local Area Network

Allows for the segmentation of a physical network into multiple logical networks. Allows computer hosts to act as if they were attached to the same broadcast domain.

VM Sprawl

Occurs when an administrator can't manage all the virtual machines in a network.

VM Escape

Vulnerability that allows an attacker to break out of a virtual machine and interact with the host operating system.

VPC: Virtual Private Cloud

W

WAF: Web Application Firewall

Security solution designed to protect web applications from various cyber threats.

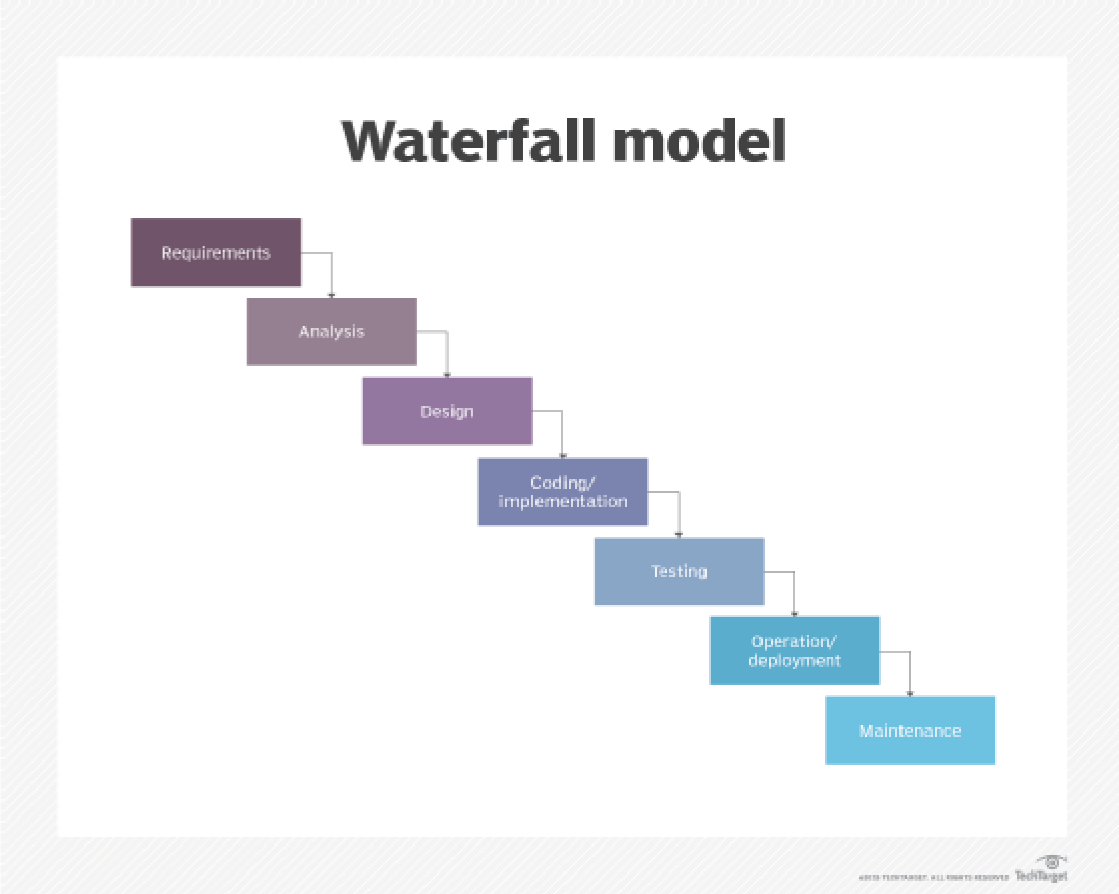
WAP: Wireless Access Point

Network device that allows Wi-Fi.

War driving

Hacking method used to search for wireless networks with vulnerabilities while moving around an area.

Waterfall Model



WEP: Wired Equivalent Privacy

Not secure Wi-Fi protocol. Security Protocol designed to secure wireless computer networks. WEP was part of the original IEEE 802.11 standard. Early wireless protocol. Deprecated.

Wi-Fi Direct

Enables establishing direct communication links between two wireless devices without an intermediary Wireless Access Point (WAP).

Wildcard Certificate

Digital certificate. Allows multiple subdomains to be protected by a single certificate.

WinHex

Hexadecimal editor, disk editor, and a computer forensics tool. A powerful and versatile tool that is used for various purposes in the field of computer forensics, data recovery, and low-level data editing.

WLAN: Wireless Local Area Network

Uses wireless communication to connect devices within a limited geographic area.

WPA: Wi-Fi Protected Access

Deprecated. Not able to change pin numbers. Easy to guess pin numbers. If you can guess the pin numbers you will get the encryption key.

WPS: Wi-Fi Protected Setup

Designed to make it easier for users to set up a secure wireless home network without setting up a long passphrase. Deprecated.

X

X.509

Standard the defines the structure of a certificate. This standard format makes it easy for everyone to view the contents of a certificate, but it doesn't provide any additional trust.

X.609

Standard that defines data structures in a platform independent way. ASN.1 standard. Distinguished Encoding Rules (DER) is a subset of BER defined in X.609. DER imposes additional constraints on encoding, such as a unique canonical encoding, making it more suitable for applications where a unique encoding is critical.

Y

Z

Certificate Formats

Binary Version	**Binary File Extentions**	**Text Version**	**Text File Extensions**
DER	.der, .crt, .cer	**PEM**	.pem, crt
PFX	.pfx, .p12	**P7B**	.p7b

Layer 7 Application	**Port Number**	**Use**
File Transfer Protocol (FTP)	20/21	Port 21 is the control port while port 20 is used to transfer files.
Secure Shell (SSH)	22	Designed to transmit data through a remote connection.
SSH File Transfer Protocol (SFTP)	22	A completely separate protocol from FTP (it is not compliant with FTP servers) that uses SSH to encrypt file transfers.
Simple Mail Transfer Protocol (SMTP)	25	Used to exchange email between servers.
TACACS+	49	Cisco proprietary protocol used for authentication, authorization, and accounting (AAA) services
Domain Name System (DNS)	53	Used to associate IP addresses with domain names

Dynamic Host Configuration Protocol (DHCP)	67/68	This network management protocol is used to assign local IP addresses to devices on a network. It is used to create multiple private IP addresses from one public IPv4 address.
Hypertext Transfer Protocol (HTTP)	80	Protocol used for websites and most internet traffic.
Kerberos	88	Network authentication protocol that allows for communication over a non-secure network.
Post Office Protocol (POP)	110	E-mail protocol that allows e-mail clients to communicate with e-mail servers. POP provides only one-way communication.
Internet Message Access Protocol (IMAP)	143, 993	E-mail protocol used by e-mail clients to communicate with e-mail servers. Provides two way communication unlike POP.
Simple Network Management Protocol (SNMP)	161/162	Protocol used to monitor and manage network devices on IP networks.
Lightweight Directory Access Protocol (LDAP)	389	Used to manage and communicate with directories.
Hypertext Transfer Protocol Secure (HTTPS)	443	Secure version of HTTP that used TLS for encryption. Most websites use HTTPS instead of HTTP.
Lightweight Directory Access Protocol Secure (LDAPS)	636	Secure version of LDAP that uses TLS for encryption.
File Transfer Protocol Secure (FTPS)	989/990	FTPS uses TLS for encryption. It can run on ports 20/21 but is sometimes allocated to ports 989/990.
Internet Message Access Protocol Secure (IMAPS)	993	Secure version of IMAP that uses TLS for encryption.
Post Office Protocol 3 Secure (POP3S)	995	Secure version of POP that uses TLS for encryption.
Remote Authentication Dial-In User Service (RADIUS)	1812, 1813	Used to provide AAA for network services
Diameter	3868	Developed as an upgrade to Radius
Secure Real Time Protocol (SRTP)	5004	SRTP replaced RTP and is a protocol used to stream audio and video communication using UDP.

Layer 5 Session Layer	**Port Number**	**Use**
Layer 2 Tunneling Protocol (L2TP)	1701	Used to create point to point connections, like VPNs over a UDP connection. Needs IPSec for encryption. Designed as an extension to PPTP. Operates at the

		data link layer but encapsulates packets at the session layer.
Network Basic Input/Output System (NetBIOS)	137, 138, 139	Provides session establishment, maintenance, and termination services. Allows communication sessions to be established between devices on a network.

Layer 4 Transport	**Port Number**	**Use**
Transmission Control Protocol (TCP)	N/A	One of two main protocols of the Internet Protocol (IP) suite is used to transmit data over an IP network. TCP provides error checking to ensure packets are not lost in transit.
User Datagram Protocol (UDP)	N/A	The second main protocol in the IP suite transmits datagrams in a best effort method. UDP does not include error checking.
Point to Point Tunneling Protocol (PPTP)	1723	Based on PPP. Deprecated protocol for VPNs.
Remote Desktop Protocol	3389	Windows proprietary protocol that provides a remote connection between two computers.

Layer 2 Data Link Layer	**Port Number**	**Use**
Point to Point Tunneling Protocol	1723	Based on PPP. Deprecated protocol for VPNs.