Sec+ Study Guide Glossary

A

Accounting

Accounting means keeping records/logs of actions performed and which user took each action

Account Lockout and Disablement

Once an account has been locked out, login capabilities for the account are prevented for a certain amount of time

Accept

Acceptance refers both to the accepting of risk responsibility and to the accepting of the fact that some risk will always remain, no matter how small

Access Control Models

Controlling access means regulating who is authorized to take a particular action, whether viewing/modifying files or accessing certain physical locations.

ACL

A mechanism that implements access control for a system resource by enumerating the identi-ties of the system entities that are permitted to access the resources

Acceptable Use Policy

A policy that defines the rules for how a resource can be used

Violation of this policy can lead to punishment, up to and including termination

For example, a policy may state that personal social media is not allowed on work systems

Access Point

A hardware device that allows wireless devices to connect to a wired network using Wi-Fi or re-lated standards

Access violations

Access violations such as unsuccessful login attempts or accounts which have been locked due to repeated login attempts may indicate that someone is trying to gain access in an unauthorized way

Account Maintenance

Involves following onboarding, offboarding, auditing and configuration to ensure users have least-privilege permissions and that user accounts are removed when no longer in use

This is an ongoing process that can help keep user accounts working as expected and keep access levels correct

Active-Active

In an active-active configuration, all load-balancing servers are active and used to process re-sponses. If a server fails, its workload gets pushed onto the remaining servers, resulting in each server having a higher workload

Active-Passive

An active-passive configuration uses a redundant inactive (passive) server in addition to those which are active. If one of the active servers fails, its workload is pushed onto the passive server and the performance of the other servers is not affected

More costly, as it requires an unused system to be standing by in case of failure

Active Reconnaissance

When an attacker gathers information by actively engaging the target service, person, property or network

Traditionally, this term was used to describe actively going into enemy territory to gather intel-ligence

Administrative Controls

Controls that are established through administration to describe how members of an organization should act

Typically refers to a company's security polices and procedures

Advanced Encryption Standard (AES)

The AES algorithm is a symmetric block cipher that was adopted by NIST as the successor to 3DES

AES uses 128-bit blocks and allows for a variety of key sizes, supporting 128-, 192- and 256-bit keys

Adverse Actions

An adverse action happens when an organization discriminates against an employee when disciplining them

In order to prevent accusation of an adverse action, ensure all disciplinary actions are accompanied by evidence of a policy violation or wrongdoing

Adware

Software that displays commercial advertising to generate revenue

Ad Hoc

A wireless network that dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station

Advanced Persistent Threat

An attack in which a person or group gains access to a system or network for an extended period of time

The intent of this attack is usually to steal data and is often associated with nation-state actors who are able to compromise network security with many different tools and techniques

Administrative

Controls which govern policies and procedures (e.g., a list of things to be done before data is released)

Affinity

If using affinity, once a client is matched with a server it will remain with that same server for the remainder of its communication session

Clients are "stuck" with their server

Can be accomplished by caching client IP addresses and/or by using a session identifier

After-Action Reports (AAR)

A document containing findings and recommendations from an exercise or a test of the disaster recovery procedures

Agent

An agent is software that runs on a system and then reports back with the results of the NAC policy compliance check. Determines whether or not a system is allowed network access

Agentless

Agentless means no agent is installed on systems. Instead, a domain controller scans devices directly for NAC compliance as they request to join the domain

Aggregation

Is the process of collecting data from many different sources to a common location. This data can than be parsed to assess the health of an environment

Allows for a SIEM to be a “one-stop shop” for looking at log information, as it will contain the es-sential log data from all applicable machines

Aggregation Switches

Used to combine (aggregate) multiple switch connections into a single source to be connected to a router

Help the flow of traffic in a multi-tier network by reducing the number of connections to a router

Agile

This implementation of the SDLC solves problems in parallel, running multiple different phases at once on separate areas of code. Code is released even if it does not completely solve the problem, with the idea that it will be improved as the project takes form.

Air Gaps

An air-gapped system is not physically connected to another system in any way, which is a specific form of isolation

The air gap prevents malware that utilizes a network from being able to find the system

As with any system, a human can still introduce malware

Alarms

Alarms can be placed on doors, windows, gates and perimeters. They assist security personnel by notifying them of a possible intrusion

Alarms can be human-activated. For example, a hold alarm that a bank teller can activate in case of a robbery

Always-on VPN

A VPN that is configured to be always connected to network resources

Uses cached user credentials to ensure the VPN connection is always established when connect-ing to the Internet over a trusted network

Improves the user experience, as users do not have to manage the connection or repeatedly en-ter their credentials to use the VPN

Alternate Business Practices

Alternate business practices are techniques used to keep an organization’s work flowing in the event of a system failure

Amplification Attack

When an attacker spoofs lookup requests to DNS servers and redirects the response towards a target

The response is larger than the request, allowing the attacker to amplify their efforts

Analytics

Data gathered about a network’s behavior

This data can be used to make rules for the network, which an intrusion detection system can use to stop or prevent malicious activity

Annual Loss Expectancy (ALE)

The total amount of loss over the course of a year due to a risk event

ALE is calculated by multiplying SLE with ARO (ALE = SLE x ARO), as the amount of annual loss is equal to the loss due to an event multiplied by the number of times it occurs in a year

If we expect to break two windows a year (ARO) and the windows cost $500 (SLE), the ALE would be $1,000 for this risk ($500 x 2)

Annual Rate of Occurrence (ARO)

This is a calculation of the number of times a given risk will occur within a year

A company in California may have a high ARO for earthquakes, while an organization in New York would have a low ARO for earthquakes

Anomaly-Based Detection

The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations

A model of trustworthy behavior can be created using machine learning

May suffer from false positives

ANT Connection

ANT is another wireless connection using the 802.11 protocol

Similar to Bluetooth technology, though more often used by devices which track health and fitness data

Like every other wireless connection, the potential exists for attack. Data sniffing, man-in-the-middle, jamming, etc.

Antenna Types

Antenna type and placement can effect signal strength and quality

Distance/objects in the way

Directional antennas

Omni-directional antennas

Anti-Spoofing

Anti-spoofing measures are countermeasures taken to prevent the unauthorized use of legiti-mate identification and authentication (I&A) data — however it was obtained — to mimic a subject different from the attacker

In the world of routers, the above generally refers to defeating IP spoofing, where an attacker modifies the IP header of a packet

IPsec tunnels are a good method of anti-spoofing

Antivirus

A program specifically designed to detect many forms of malware and prevent them from infecting computers, as well as cleaning computers which have already been infected

The output of a specific antivirus program will vary. But if malicious software is detected, steps should be taken to investigate and mitigate as needed

Appliances

Built to work on an appliance which provides a specific function (e.g., storage, virtual machines, backups)

Application-Based Firewall

Software which runs on a machine (often a server) and is designed to protect a specific applica-tion (e.g., a firewall which protects a SQL database)

Sometimes called a host-based firewall, this type of firewall is typically deployed alongside a network-based firewall

Application Cells/Containers

Application virtualization involves encapsulating an application in

such a way that it is able to behave normally but is isolated from the host operating system in some way (virtualizing a single application rather than having an entire virtual machine)

Application Management

Determining what applications and application installation sources will be allowed, often using an application whitelist

Application and Service Attacks

There are a number of way in which attackers can target the applications and services running on a computer

While social engineering threats are important to consider, it is also good to be aware of attacks on technology rather than just on the human element of a system

Application proxy

One that translates a user's request into a format usable with a specific application

Application Whitelist

A list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline

When used correctly, any applications which are not on the whitelist will not be allowed to run server itself

arp

The arp command allows a user to view the Address Resolution Protocol (ARP) cache and potentially modify entries. The ARP cache contains a listing of which MAC address is associated with different IP addresses

ARP Poisoning

When an attacker changes Address Resolution Protocol (ARP) records in a way that resolves the attacker's MAC address to a legitimate IP address

Asset Management

Managing the life cycle of assets in a network can help assess risk and mitigate cost

Knowing the age of machines and having criteria for when to "retire" them helps prevent the use of vulnerable or unsupported operating systems

Asymmetric Algorithms

An encryption method that uses a two-part key: a public key and a private key

Attribute-Based Access Control (ABAC)

An access-control approach in which access is given based on attributes associated with requesters and the objects to be accessed

Authentication

Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in a system

Authentication Header

Authenticates the origin of IP packets and guarantees the integrity of the data. Confirms that both the header and the data have not been changed

Authentication Issues

Authentication issues can occur for many reasons. One of the more common examples is a user not remembering a username or password

Password policies should require passwords to be secure, but if a password policy is too complex, it can lead to users doing things to simplify authentication engineering techniques

Authentication Protocols

There are a number of different methods of providing authentication information when one is attempting to prove their identity through a wireless connection

Authority

Using the appearance of authority to gain access to information, locations or people otherwise not allowed

Types of authority include legal, organizational and social

Authorization

Authorization governs what access privileges are granted to a user, program or process and the act of granting/revoking those privileges

Automated Actions

Environments using automation have the advantage of flexibility. The environment can change rapidly to match an number of needs

Using scripting languages (Python, Bash, PowerShell), many actions can be automated. Security updates can also be automated

Automated Alerts/Triggers

The ability to be alerted or have an action taken based on certain events

Generally, alerts will be sent to system administrators and security team members to notify them that a potential security threat has occurred

Triggers are the specific events which set off (trigger) an automated alert

Avoid

Simply stop participating in risky activities or avoid taking unnecessary actions which cause risk. Not always possible

B

Backdoors

A way to circumvent security features (e.g., encryption) surreptitiously built into software or systems.

Background Checks

Background checks can help an employer determine if a potential employee has any criminal or civil history that would exclude them from employment

This is also an opportunity for an employer to confirm the information provided by an applicant

Backup Utilities

Software/hardware that aids in the automated backup of systems

Used to ensure that data can be recovered in the event of a theft, outage or other loss of data

Band Selection

Band selection can be used to help clear congestion or reach across longer distances by using different signal wavelengths

Banner Grabbing

Banner-grabbing tools use captured banner information that is transmitted by a remote port when a connection is initiated

This information is used to identify version information about a system's software

Passive banner-grabbing tools simply listen

Active banner-grabbing tools interact with target systems

Barricades and Bollards

Barricades and bollards are both large physical barriers which can

be used to direct foot and vehicle traffic by physically preventing someone from entering a certain area.
Used to prevent "smash and grabs" where a vehicle is crashed into a building to disrupt service or open an entrance for an attacker
You often see these types of barriers around high-value targets like government buildings or data centers

Baselining
The process of creating and maintaining a set of basic requirements/ configurations a development environment must meet in order to be considered secure
Once a baseline has been created, it allows for automation when building secure development environments

Baseline Deviation
A baseline defines the minimum security controls required for safeguarding an IT system, based on its identified needs for confidentiality, integrity and/or availability protection
If this baseline is deviated from, this an indication of risk is legitimate

BCRYPT
Password hashing function that is resistant to brute force because the iteration count can be increased

Biometrics
Typically include fingerprint or face scanning
Generally more secure than a password- or PIN-based lock, though false positives can occur

Birthday Attack
An attack that exploits weak cryptographic hash functions. It works by finding separate input values that produce the same hashed value. A birthday attack relies on chance to do this
A birthday attack is a subset of a collision attack. A collision attack is simply when a process is found that can produce the same value. These are associated with cryptographic hashing

Black Box
A test that is conducted without any prior knowledge of how the system, network or target is designed or implemented

Blacklisting
allows you to specify applications that will never be allowed to run

Block Cipher
Encrypts data by first breaking it into blocks of a predetermined size. Each block of data is then encrypted and information from prior blocks is often used to encrypt the following blocks, adding confusion. If the input data does not meet a block-sized length requirement, it will be padded by adding data (typically 0s) to the end until it meets the correct size

Blowfish
Created by Bruce Schneier and left unpatented and open to combat the proprietary nature of other algorithms
Blowfish provides speed and security, using 64-bit blocks and supporting key sizes from 32 to 448 bits
Twofish is similar to Blowfish, but doubles Blowfish's block size from 64 to 128 bits. Twofish supports keys of up to 256 bits

Bluejacking
Sending unsolicited data over Bluetooth
This can be used in guerrilla marketing schemes

Bluesnarfing
The use of a Bluetooth connection to steal data
This attack uses vulnerabilities in the implementation of Bluetooth to access data on a device

Bluetooth Connection
A wireless protocol that allows two Bluetooth-enabled devices to communicate with each other within a short distance (e.g., 30 feet)

Bots
Computers or software that are infected and taken control of by an attacker and used to com-plete some task autonomously

Bridge
A device that creates one network from two by directly connecting one local network to another at at the data-link layer (Layer 2)
A multiport bridge can connect more than two networks and serves as the basis for switching

Bring-Your-Own-Device (BYOD)
A policy where employees are allowed or encouraged to use their personal devices for business purposes. Poses the most security issues

Brute-Force Attack
When an attacker tries to guess a password by trying every possible character combination
An online brute-force attack is when communication with the target system is needed
An offline brute-force attack is when the attacker has a copy of the password hash and can per-form everything locally

Buffer Overflow
When a program overruns a buffer's boundary as a result of a too-large input and overwrites ad-jacent memory locations
Memory locations are often well-defined, allowing an attacker to write the overflow code into an executable area of memory

Buffer Vulnerabilities
When a program overruns a buffer's boundary and overwrites adjacent memory locations. Memory locations are often well-defined, allowing an attacker to write the overflow code into an executable area of memory.

Business Impact Analysis (BIA)
A method of gathering data to predict how a loss of a system or service will affect a business
Identify mission-essential functions and critical systems and determine how quickly and fully they can be recovered in the event of a failure

Business Partners Agreement (BPA)
An agreement between two business partners. These are generally longer-term and broad in nature, and include information such as how to allocate profits/losses, what percent of the business is owned by each partner and how disagreements between partners can be settled

C

Cable Locks
Cables used to lock down hardware
Typically used to temporarily secure mobile devices like laptops
Most laptops have a standard cable lock adapter built in, making it easy to lock them to a table or desk

Cameras
Cameras offer a way to add visibility to areas without actually placing a security guard.

Camera Use

The camera on a device can present a multitude of challenges:

Pictures of sensitive data or areas

Personal or private pictures on devices

Captive Portals

A user often authenticates through a Web browser via a captive portal

This portal can require users to enter credentials or to simply agree to some terms before allowing access to the network

Carrier Unlocking

The ability to unlock a device so that it can be used on another phone service carrier's network

Cellular Connection

The cellular connection offers unique challenges in that it is almost always connected and is coupled with location information

Certificate

A set of data that uniquely identifies a key pair and an owner that is authorized to use the key pair

Certificates are used to provide authentication which is validated by a trusted source

Certificate-based Authentication

Authentication can also be granted through the use of certificates

A certificate is a (usually small) digital file containing authentication information

These certificates can be built into smart devices, removing the requirement of a user having to remember a password or authenticate using a biometric

Certificate Authority (CA)

A trusted entity that issues and revokes public key certificates

The CA is who/what establishes trust in the certificate. If the CA is not trustworthy, neither is the certificate

Certificate Formats

The information contained in certificates can be represented in various ways, and different formats should be used depending on how the certificate will be implemented

Certificate Revocation List (CRL)

Certificates typically have an expiration date after which they are no longer considered valid. However, it is vsometimes necessary to revoke certificates prior to their expiration (typically due to the leaking of a private key or the compromise of a CA)

Certificate Types

Certificates are versatile and are use in many different types of authentication schemes

Different types of certificates have different configuration options which allow the inclusion of information relevant to their purpose, whether that information is an email address, a wildcard or an extra for validation for the certificate

Chain of Custody

A process that tracks the movement of evidence through its collection, safeguarding and analysis life cycle by documenting each person who handled the evidence, the date/time it was collected or transferred and the purpose for the transfer

A legal hold is the concept of retaining evidence which may be relevant in a legal battle, and any lapse in the chain of custody can cause evidence to be rendered useless in a court of law

Change Management

Change management is a formal process for reviewing and approving any changes in an environment or organization

CHAP

Challenge Handshake Authentication Protocol (CHAP) provides authentication by using an encrypted handshake. Components of this three-way handshake are as follows:

Challenge: Server sends a message consisting of random data to the client

Respond: Client computes a hash using its password and the data from the server's challenge message

Verify: Server compares a combination of the stored hash of client's password and the hash of the challenge message to the hash received from the client

Choose-Your-Own-Device (CYOD)

A policy where an organization offers a selection of devices for an employee to choose from

Very similar to COPE, with all the same issues involved physical connection

Cipher Block Chaining (CBC)

Improves upon ECB by XORing an IV with the first block and then XORing each plaintext block with the previously-output ciphertext block

This method introduces randomness via the IV to ensure no block of plain text produces the same ciphertext

Cipher Modes of Operation

Cryptographic block ciphers are used to encrypt data in chunks or blocks, and the mode of operation simply refers to the type of block cipher being used

Clean Desk

A policy that dictates that computers are turned off and nothing is accessible on a desk before an employee can leave

Prevents employees from leaving sensitive information in plain view to be seen/stolen by an attacker. Includes not leaving written passwords in non-secure areas

Clickjacking

When an attacker puts a UI layer over or around a clickable element, tricking the victim into clicking the attacker's element

Client-Side Execution

Client-side execution means the code is executing on the client machine which is interacting with an application. Validation on the client side saves time, as it removes the need to communicate back and forth with the application server, but it can be easily bypassed by a malicious user.

Cloud

Storage is provided somewhere else, usually by an outside organization. Software and platform management can also be provided separate

Cloud Access Security Broker (CASB)

Integrates your organization's security-related polices to applications running in the cloud

Can detect high-risk applications/users and enforce encryption

Cloud Storage

The storing of data across separate physical servers, typically managed by a hosting company (cloud service provider)

Code Quality and Testing

As code moves through the phases of the development process, it needs to be tested for both functionality and security issues.

There are a variety of testing methods, including static versus dynamic analysis and general stress-testing

Testing should be done in non-production environments (e.g., sandboxes or other testing-specific environments)

Code Reuse and Dead Code

Every line of code opens up the potential for a problem or security vulnerability

Any lines of code which are not serving a purpose are referred to as dead code and should be removed

Code Signing

Code signing allows a user to be sure that an application has not been modified and also confirms the author of an application.

Accomplished through hashing file and signing this hash with the developer's private key (asymmetric encryption) to provide a certificate-based digital signature

Code Signing Certificate

A developer can use a code-signing certificate to sign their code executables/libraries so that their software can be verified before installation

If something has changed in the code or the wrong certificate is present, installation can be stopped and the source of the code can be verified

Cold Site

A cold site is a backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place

A cold site is not ready for immediate operation and typically takes a few days to get up and running. However, it is the least expensive type of recovery site to maintain

Counter Mode (CTR)

Also referred to as CTM. This mode acts similarly to a stream cipher, adding a counter value to make each block unique and allowing blocks to be encrypted/decrypted in parallel

The counter value is unique and ensures no two identical plaintexts encrypt to be the same ciphertext

Collectors

In general, collectors are appliances or software that collects logs from disparate sources for later review and data analysis

Collision

Occurs when two or more distinct inputs produce the same output

This can be used to fool hash functions, signifying that the hash function is not ideal

Command Line Tools

Used from a command line interface, these tools provide a user with a variety of differing func-tionalities.

Commands often have a set of sub-commands which can be used by modifying the original com-mand. Commands may vary depending on the host OS

Common Access Card (CAC)

Used by the U.S. DoD to provide an additional authentication factor, these cards contain certificate data and display an photo of the user

Community cloud

is a private cloud that is shared with multiple organizations

Compensating Controls

A control designed as a backup to another control, to be used in the event that the main control is unable to provide sufficient levels of protection on its own

Compensating controls can also involve the recovery of data if lost due to an attack/disaster

For example, an alarm that sounds after a locked door is left open for a period of time

Competitors

The competition looking for an advantage

This could involve stealing information, disrupting service or damaging reputation

Compiled Code

Code that does not need interpretation during execution but must first be converted to executable form by a compiler in order to run

Compilers check code for syntax errors during the compiling process

Common languages: C, C++, Visual Basic, COBOL

Confidentiality

Cryptography allows for confidentiality among data communications and storage

Only those who have the appropriate decryption key can view encrypted data

Configuration Compliance Scanner

Software that scans a host to see if the configuration of the host falls within a set policy which details an ideal setting configuration

Can be done to comply with regulations or simply to follow best practices

Configuration Validation

Scripts can be run against configuration baselines to check for compliance with security policies

Can be bolstered by the idea of templating virtualization. This allows an admin to have a pre-approved framework for building virtual environments that match a specific need and meet configuration requirements

Confusion

The concept that data will look very different after encryption/hashing

There should be no clues in the encrypted or hashed text (e.g., patterns) and no discernible connection to the key

Consensus

Using a sense of popular opinion to convince a victim to do something they would otherwise not be convinced to do

For example, an attacker could convince a target to install a virus by having the virus appear to be highly-valued and well-reviewed by others

Containerization

Containerization refers to running a separate virtual environment on a mobile device

A container can have its own security policies which are separate from those of the user's actual device

Containment

In this stage, you want to prevent further damage to the environment and save as much data as possible by using the information gained in the Identification step

Content Filter

Often fail when they are not a network position to intercept traffic in the clear. Encrypted or obfuscated traffic may not trigger the filters

Content Management

A content management system ensures mobile devices and environments use company data securely

Context-Aware Authentication

Using data such as the user's location, time and type of data being accessed to make a decision if the user trying to authenticate is actually the user

Context rules can be simple or complex to incorporate multiple data points to make a decision

Continuing Education

When an employer encourages, supports or pays for the education of the employee, typically in a role- or security-related way

Continuous Integration

In this model, developers integrate code into the development life cycle often

When paired with security automation and automated testing, this gives the developer confidence in the code when it is initially deployed

Continuous Monitoring

To trigger the automation based on certain events, continuous monitoring is also needed

The monitoring can also be scripted by having the scripts interact with APIs, checking logs, etc.

This concept can be expanded out into looking at security issues as well (e.g., collecting and monitoring security logs with a SIEM)

Corporate-Owned, Personally-Enabled (COPE)

A policy in which an organization buys and owns a device. The employee is allowed to use it for both personal and professional activities

Corrective Controls

Controls that mitigate a materialized risk and possibly prevent the risk from happening in the future

For example, restoring lost data from backups or an employee getting reprimanded for violating a security policy

Correlation

The process of separating out specific data points that are associated with a security event. This can help find patterns that can help identify security threats

A SIEM can be configured to send out alerts notifying of a possible security threat whenever a threat had been identified through correlated patterns

Correlation Engines

Software that can look at events, generally from logs, and provide feedback based on these events

Assists you in determining when seemingly separate events are indicative of a larger attack

Counterintelligence Gathering

Gathering counterintelligence information involves using active logging to record and analyze everything an attacker does, which helps an organization to more effectively detect, log and thwart attack attempts

Crackers

After a network is identified, certain wireless protocols can be cracked using a cracking tool

Credentialed Scans

Credentialed scans are completed with the privileges of an authorized user. Because an author-ized user has more access, this can be more intrusive and can better demonstrate what an attacker with insider access could exploit

CRL

A CRL is a list, maintained and signed by a CA, of the certificates which the CA has issued that have been revoked/invalidated prior to their stated expiration date

Crossover Error Rate (CER)

CER refers to the point where the False Rejection Rate equals the False Acceptance Rate and is the ideal balance between the sensitivity of a biometric sensor and the rate at which it makes errors.

Cross-Site Request Forgery (CSRF)

An attack against a user who is authenticated to a Web application

The attacker takes advantage of the authentication to force the user to take an unwanted action by convincing the user to submit a malicious request accompanied by their credentials

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a type of injection attack

The attack involves injecting malicious scripts into trusted websites

If an attacker's input is not properly sanitized and is reflected in the website's code, the attacker can modify the code and content of the website

Crypto-Malware

Malware that gains access to a system and encrypts system data so that the owner is unable to access it.

Cryptographic Algorithms

A cryptographic algorithm is a set of mathematical functions which uses a (often secret) string of data, known as a key, to encrypt/decrypt other data

Custom Firmware

A user may load custom firmware to have more control over the mobile device's operating system

Custom firmware an also be used to circumvent device authentication (rooting/jailbreaking)

Custodian

Is responsible for implementing the controls provided by the steward

Cyber-Incident Response Team (CIRT)

Depending on the size of an organization, it may be able to allocate enough resources to create a Cyber-Incident Response Team

D

Data Acquisition

There are a variety of data types which are useful to recover and examine during the forensic process, including network logs and system images

Data Encryption Standard (DES)

A now-defunct protocol created by IBM and standardized by the National Bureau of Standards in 1975

Data Exfiltration

The unauthorized transfer of data or the theft of data. This can come from internal or external actors

Data Execution Prevention (DEP)

Technology that can prevent malicious code from running on a system by preventing execution of data in memory regions

Data Exposure

Data exposure happens when an application or procedure contains

an issue which allows unauthorized parties to access sensitive information (SSN, password, credit card info, login token)
Encrypting data can help reduce exposure, providing an extra layer of protection when access controls fail

Data Destruction/Sanitization
When data is no longer is use (or needed as a backup), it should be destroyed.

Data Owner
The data owner is the person that is responsible for the data and data compliance

Data Retention
Before destroying data, consider any legal implications as there may be laws regarding retention (e.g., a regulation may require a company to retain the past three months' worth of data)

Data Sensitivity
Proper labelling of data helps to ensure its information remains accessible only by authorized parties (DLP solutions can also make use of data labels to block access/communication of sensitive data).

Data States
Data-in-Transit: Any data sent across the network
Data-at-Rest: Any data currently located in memory, including databases and backups
Data-in-Use: Any data being actively used by a process

Database Security
In database security, access control lists have a wider range of options
Regulate access to the database (including its tables and entries)
Control a user's ability to run various database commands

DDoS Mitigator
DDoS mitigation is used to help get a service back up during an attack. There are multiple approaches, including cloud solutions

Denial-of-Service (DoS)
Where an attacker attempts to make a networked resource unavailable to others by disrupting the host's connection to the network

Default Configuration
When a system component is left with the configuration that is provided
Think of a home router with the default credentials

Defense-in-Depth and Layered Security
When designing an environment, you want to avoid having a single point of failure. An attacker should not be able to have complete access just by passing one level of security.
This can be addressed by taking a layered approach, where sensitive information is placed behind multiple security controls.

Demilitarized Zone (DMZ)
A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet

Deprovisioning
Removing applications from a package or an environment is known as deprovisioning

Detective Controls
Controls which notify and record when attack attempts are made, but do not prevent attacks from occurring

Deterrent Controls
Deterrent controls communicate, either directly or indirectly, to an attacker that they should not attack

Development
Where all the initial work is being done. This environment focuses more on creating functionality than testing for flaws

Design Weaknesses
Usually associated with the architecture or design of networks
A network with improper design can lead to security holes. Automated tools can make it easy for an attacker to find these holes

Dictionary Attack
A form of brute-force attack which tries to guess a password by trying every word or combination of words within a predefined list (or dictionary)

Differential Backup
A differential backup only backs up data which has changed since the last full backup

Diffie-Hellman (D-H)
A method used to securely exchange or establish secret keys across an insecure network by using the properties of a group and/or trapdoor function, which is easy to compute in one direction but difficult to find the inverse of

Diffusion
The idea that even if the input (plaintext) changes only slightly, the output (ciphertext) will be very different then the ciphertext before the change
A good baseline for diffusion is that changing one bit of the plaintext should cause approximately half of all bits in the ciphertext to change

Digital Cameras and Camera Systems
Can be used to capture sensitive data and act as a USB storage device, giving them similar security concerns. Can also be used to spy on members of an organization if compromised

Digital Signatures
Digital signatures are a method of cryptographically signing a message to authenticate the sender and provide assurance that the message data has not been modified (authentication and data integrity)

Digital Signature Algorithm (DSA)
DSA is an algorithm created as an adaption of Diffie-Hellman, allowing for digital signing of data
The main improvement DSA has over RSA is that it can make use of elliptic curve cryptography to speed up key generation

Disabling Default Accounts and Passwords
Default accounts are often created automatically during installation and are configured with simple passwords

Disassociation
When an attacker de-authenticates a user from a wireless access point. This attack is usually combined with a rogue or evil-twin access point

Displays
Displays also have firmware or even full-blown operating systems. These need to be researched and kept up-to-date to protect against

malware

Directory Services

Directory services includes services (such as Active Directory) which allow for management of users and systems in an environment

Can be used to manage security controls/groups, email configuration and access control

Discretionary Access Control (DAC)

A means of restricting access to objects where the owner of the object has full control and is able to change the permissions of other users as they pertain to the object and its data.

Dissolvable NAC

Dissolvable NAC uses an agent which is downloaded by a client upon requesting access. The agent runs the appropriate NAC checks and allows access if the client passes. Provides one-time authentication, as a new agent will need to be downloaded each time the network is accessed

Distributive Allocation

Switching between different systems for processing and data handling in order to meet service requirements

DLP

Using a system or application to identify, monitor and protect confidential data within a central-ized management framework

DNS Poisoning

An attack against a domain name system (DNS) that resolves a request away from legitimate servers and towards malicious servers

DNSSEC

Domain Name System Security Extensions (DNSSEC) are a set of extensions that secure a subset of information from DNS

Domain Hijacking

When an attacker changes the registration of a domain (example.com) without the owner's per-mission

Domain Name Resolution

Resolves a given domain name into its corresponding IP address by querying DNS servers

Security consideration needs to be given to DNS poisoning and spoofing, as these attacks can redirect a valid URL to a malicious one

Domain Validation

Domain validation is a method of proving to a CA, often via email, that the holder of a certificate owns the respective domain

Downgrade

When an attacker forces a victim to use a less-secure protocol

This is usually possible due to support for backwards compatibility

Dumpster-Diving

When an attacker goes through the trash of a target, looking for sensitive information

Dynamic Code Analysis

Dynamic analysis involves testing the code by simulating a real-world environment and attempting to provide it with all possible inputs to determine if there are any undesirable outcomes.

E

EAP-FAST

Lightweight EAP (LEAP) allows a client and server to mutually authenticate and agree on a key to be used for their encrypted communication tunnel

EAP-TLS

EAP-TLS is similar to PEAP, except it uses a certificate on both the client and server to establish a secure TLS connection tunnel

EAP-Tunneled TLS

Also reminiscent of PEAP, EAP-Tunneled TLS (EAP-TTLS) creates a secure tunnel between client and server by authenticating a server with its certificate. The client then authenticates by sending credentials via secure tunnel

EAP-TTLS can use a wider range of client authentication protocols than PEAP

Elasticity

Refers to how well a system can respond to changes in demand as they happen in real time

High elasticity means there will be no loss of service/performance due to any increase in demand for the service

Electronic Codebook (ECB)

In this mode, each block of plaintext is encrypted with the same key

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography generates public/private key pairs using the properties of elliptic curves

Email Certificate

PKI is good way to secure email communications and email certificates allow for messages to be signed/encrypted

Embedded Systems

A special-purpose computing system that is embedded to add control and/or connectivity. These systems are found in automobiles, medical devices, industrial equipment and much more

EMI

Electromagnetic Interference (EMI) results from one electronic machine's electromagnetic signals interfering with the signals from another machine

EMP

Electromagnetic Pulses (EMP) are powerful waves of electromagnetic energy which are often meant to disrupt or destroy electronics

Encapsulating Security Payload (ESP) Header

Can be used alone or in combination with AH. Using ESP provides confidentiality, authentication and integrity

Encryption

Encryption can be used to protect code both in production and development environments

The data the application uses and produces can also be encrypted

Environmental Threats

Threats that are often called natural disasters. For example: flooding, fires and earthquakes

EOL System

Hardware or software that is no longer maintained by the vendor

Ephemeral Key

A cryptographic key that is newly generated each time it needs to be established for a communication, rather than reusing the same key

Eradication
Once the problem is contained, you can work on removing it completely. This may require internal or external experts to examine and clean/remove all systems and files which were affected during the incident

Escalation of Privilege
Using an attack or exploit to increase the privilege granted to a legitimate user or from an ini-tial exploitation

Event Deduplication
Some errors or events can cause up to thousands of similar or identical error messages to be logged and sent to the SIEM

Evil Twin
A rogue wireless access point made to look the same as a legitimate access point
Used to trick victims into connecting to the fake access point while thinking they are connecting to the original

Exclusive OR (XOR)
A simple binary operation, an XOR compares each bit of two data strings, outputting a 0 if two bits match and outputting a 1 otherwise

Executive User
An executive user is a user that likely has a high level of access across the environment, including privileges to authorize payments and purchases. May be a target of whaling/phishing

Exercises
Performing regular classroom and realistic incident-response exercises allows staff to become familiar with incident response procedures

Exit Interviews
Gives an employer a chance to get review of the organization through the eyes of a former employee (things they like/don't like about the organization and why they left)

Exploitation Frameworks
Software that aids in finding and taking advantage of exploits in various systems, networks and devices. Often used to aid in penetration testing

Extended Validation
Extended validation is similar to domain validation, but the CA completes additional checks to confirm the identity of the holder

Extensible Authentication Protocol (EAP)
An authentication framework designed to protocol-support different authentication methods.

External Media
External media can be used to expand the memory of some mobile devices. This can be done through a USB connection or wirelessly

External Storage
External storage is often easier to steal/lose. This makes data encryption a priority on external devices

External Threats
External threats refer to attackers outside the company who may attempt to infiltrate the company and damage/steal information or assets (DoS attack)

Extranet
A computer network that an organization uses for application data traffic between the organization and its business partners

F

Facial Recognition
Uses the size and shape of a face as a method of authentication

Failover
The capability to switch over automatically to a redundant system, known as an alternate processing site, upon the failure of the regularly active system

False Acceptance Rate (FAR)
The opposite of False Rejection Rate, False Acceptance Rate is the likelihood of a biometric sensor accepting a request for access from a user who is not authorized to access a resource
Also known as a Type 2 error

False Negative
An instance in which an intrusion detection and prevention technology fails to identify malicious activity as being such

False Positive
When a malicious anomaly is detected, but the anomaly actually doesn't exist or is non-malicious

False Rejection Rate (FRR)
The likelihood that a biometric sensor rejects a request for access from someone who is authorized to access a resource
Also known as a Type 1 error

Familiarity
Using the trust gained through knowing someone to further an attack
For example, a phishing email pretending to be a grandson in need of money

Faraday Cage
A Faraday cage uses material, generally metal mesh, to contain and block out radio signals
Faraday cages can be a small (a bag for a cell phone) or big (a whole room or even a building) and are typically used to protect sensitive communications or to remove interference from outside signals

Fat Access Point
A fat access point is one that has everything needed to manage clients. It is able to function without the assistance of a wireless controller (standalone)

Fault Tolerance
This is the ability to keep running after a failure. The higher the fault tolerance, the better the system is at handling failure

Federation
A collection of domains (sometimes separate companies) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.

Fencing
Fencing can keep people out of specific areas. A fence line can be easily monitored for intruders
A fence can also act as a way to obstruct vision to a certain area (e.g., having a privacy fence in your back yard)

File Integrity Checking
Software that generates, stores and compares message digests for files to detect changes made to the files

File Transfer
The most common method for transferring files is by using the File Transfer Protocol (FTP)
FTP is completely insecure by default. Security can be added by using a protocol such as SFTP or FTPS

File System Security
Every file/folder in a file system uses an ACL to determine which users are allowed access to its contents, whether for reading or writing

Filters
Filters can take many forms, including event filtering, packet filtering and content filtering, and are often used by proxies and firewalls

Finance
Another important consideration is the financial impact of a disaster/failure

Fingerprint Scanner
Uses your fingerprint as an authentication factor by comparing stored fingerprint information against the fingerprint provided during access request

Firewall
May allow traffic which was intended to be blocked, both inbound and outbound

Firmware Updates
Firmware updates can be critical to security and should be enforced. A problem in the firmware will often leave sensitive data exposed

Flooding
Flooding is an attempt to overload a switch's MAC caching table by sending it lots of traffic asso-ciated with many different MAC addresses. This is done to cause the switch to fail and act as a hub, forwarding all traffic to all connections and causing a DoS

Flood Guard
A flood guard is a mechanism to help mitigate network floods by placing restrictions on the rate of traffic allowed or specifying which MAC addresses can send traffic on the switch

Forward Proxy
A forward proxy is usually referred to simply as a proxy. A forward proxy proxies for clients, meaning that the proxy makes requests and receives responses on behalf of internal clients

FTPS
File Transfer Protocol over SSL (FTPS) is an extension of FTP that allows the encrypted transfer of data using SSL/TLS

Full Backup
A full backup involves backing up all data in a chosen set, no matter if/when that data has been backed up prior to the full backup

Full Disk Encryption (FDE)
The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product

Full Device Encryption
Everything on the device is encrypted except for the master boot record, resulting in the need for authentication before accessing any data on the device

Full Tunnel
In a full tunnel, all the traffic goes through the VPN tunnel

G

Galois Counter Mode (GCM)
Adds authentication to CBC with relatively low latency and overhead. CBC requires a 256-bit key to be secure, while GCM needs only a 128-bit key

Geofencing
Using a device's geolocation to enable or disable software and hardware on the device. It can also be used to trigger events or alerts

GPS Tagging
The process of placing coordinates in the metadata of images or other media
This is often done automatically by mobile devices and can lead to accidentally revealing sensitive location information

Gray Box
A test conducted with partial knowledge of how the system, network or target is designed or implemented

Group-Based Access Control
Assigning permissions can be done through groups. Users inherit permissions which are given to the groups that they belong to
Allows administrators to easily monitor and modify a user's permissions by moving them from one group into another

Group Policies
Group policies allow an administrator to preconfigure system and user settings based on groups
Windows uses this concept in Active Directory

Guests
It's sometimes necessary to allow guests to connect to the network so they can access the Internet or a specific resource

H

Hacktivist
A person who hacks to further a social or political cause
Generally target political, media or financial groups

Hardware Root of Trust
The main concept behind using hardware to secure a system, a hardware root of trust is the object which establishes a base level of trust. All other trusted security components build off of it

Hardware Security Module
A hardware-based device used to securely generate, store and manage encryption keys

Hashing Algorithms
Hashing algorithms are a method of using a mathematical algorithm against data to produce a numeric value that is representative of that data

Hash Message Authentication Code (HMAC)

A message authentication code that uses a cryptographic key in conjunction with a hash function

This combination of a secret key and a hash provides data integrity and authenticity

HMAC-MD5, HMAC-SHA1 and HMAC-SHA2 all create an HMAC with the corresponding hashing algorithm

Heuristic (Behavioral) Detection

The method of examining a program's interactions within its operating environment, including file systems, the registry (if on Windows) and the network, as well as other processes and operating system components

HIDS

A host-based intrusion detection system (HIDS) monitors the characteristics of a single host and the events occurring within that host to identify and analyze suspicious activity. It does not actively stop threats as they happen

HIPS

A host-based intrusion prevention system (HIPS) is similar to a HIDS, but is able actively prevent threats as they occur upon parameters

High Availability

A system with high availability is one that maintains a high level of uptime and is thus more reliable in terms of providing service

High Resiliency

When a system is set up to ensure a high reliability of communications, where a compromise of some portion of a system does not lead to the entire system being rendered insecure

HMAC-Based One-Time Password (HOTP)

Leverages HMAC to ensure integrity and authentication

Password/code does not expire until used!

Hoax

A trick to make a victim believe something that is not true and then use this belief to coax the victim into taking a malicious action (e.g., your version of Windows is outdated, please install this [malicious] update)

Honeynets

A honeynet is a network that is purposely left vulnerable to attract potential attackers (think honeypot but on a larger scale)

Honeypot

A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears

Hosted

The servers will be off-site and likely owned by another organization, but you manage the software and certain hardware components

Host-Based Firewall

A software firewall installed on a single host to monitor and control its incoming and outgoing network traffic

Host Health

Checking the health of the client to ensure compliance with NAC policies before allowing to access a resource

Hot Site

A hot recovery site is a fully operational facility equipped with all standard hardware and software used by the organization

HSM

Hardware Security Module (HSM): Hardware device that handles the provisioning and storage of cryptographic keys

HTTPS

Hyper Text Transfer Protocol over SSL/TLS (HTTPS) uses SSL/TLS to securely send and receive HTTP data over the Internet

HVAC

Modern Heating, Ventilation and Air Conditioning (HVAC) systems are controlled with centralized software and are used to control the climate in buildings, often being used to ensure server rooms do not overheat.

Hybrid cloud

is one that mixes public and private access, combining multiple cloud deployment models into one

Hypervisor

The virtualization component that manages the virtual guest operating systems on a host and controls the flow of instructions between each virtual OS and the physical hardware of the host.

Hypervisors are implemented either as a standalone product (Type I) or as a part of a host OS (Type II)

I

Identification

Identification is a way to give names/labels to users, allowing a system to map actions to specific users

Identity and Access Management (IAM)

There are different methods for managing an identification and authentication scheme, and organizations can even work together to allow mutual access to resources to authenticated users.

IEEE 802.1x

IEEE 802.1x is an official standard for providing authentication mechanisms on a network

Defines the usage of EAP-based protocols

ifconfig

ifconfig provides similar information to ipconfig, but is used in Linux environments

Immutable Systems

Systems which are unable to be changed once they are deployed. If an update is needed, the entire system is recreated start to finish, replacing systems rather than changing them

Impact

Impact refers to the effect a risk or threat can have on an organization and is an important factor in determining the significance of various risks

Impersonation

When an attacker pretends to be someone that a target is likely to trust or believe to be an au-thority

This trust is used to solicit information from the target that they would not otherwise divulge

Implicit Deny
Implicit deny is a rule that denies traffic unless a rule explicitly allows it

Improper Account Configuration
The mishandling of account creation and maintenance within a system

Improper Certificate and Key Management
When encryption keys or certificates are not handled properly, an attacker can capture them and use them for decryption

Improper Error Handling
If an error divulges too much information to the end user, an attacker can use this to learn about the underlying code

Improper Input Handling
When a program incorrectly handles the validation, sanitization or handling of input
This results in common exploits such as SQL injection and cross-site scripting (XSS)

In-Band
In-band refers to looking at or communicating with network components from within the same network as the device being monitored

In-band exchange
Typically refers to when public/private keys are exchanged and is more secure. The public key can simply be given out, as only the owner of the private key can decrypt messages sent using the public key

Incident Response Plan
An incident response plan involves having policies in place to describe procedures to take in the event of a security incident

Incremental Backup
Incremental backups save all data which has changed since the last backup of any kind

Industry-Specific Frameworks
Apply only to companies in a certain industry or that make use of specific technologies
Many include certifications which can be earned to prove knowledge of the framework's methodologies

Infrared Connection
A wireless connection often found in TV remotes. Now implemented to allow mobile devices to act as a TV remote or control other devices

Infrared Detection
Infrared gives the ability to see in the dark, based on heat signatures.
Another use of infrared is to monitor the temperature of a piece of hardware to ensure a HVAC system is working properly

Initial Exploitation
The first action by a pentester or attacker that gives a foothold into a system, network or infra-structure
May be accomplished via phishing or other social engineering techniques

Initialization Vector (IV)
An initialization vector is used to change an encryption key every time data is sent
A weak implementation, as in WEP, can allow an attacker to decrypt data

Injection
When an attacker takes advantage of a bug which allows them to inject arbitrary code that is subsequently executed
A well-known injection is SQL injection

Inline Detection
Inline detection is done by having the packets pass through the detection system. This allows for prevention of an attack as it occurs (e.g., NIPS)

Insider
A threat actor that comes from inside the organization
Threats can be due to malicious action or simply incompetence
Examples include disgruntled or uneducated employees

Integrity Measurements
Code with high integrity will generally have unit and functional tests that cover most if not all of the code base. Systems with high integrity measurements are generally more secure

Intranet
A computer network that an organization uses for its own internal (and usually private) purposes, which is closed to outsiders
Used only by trusted hosts within the organization

Integrity
Encrypted data cannot be intelligently modified without first being decrypted, so cryptography allows data to be tamper-resistant/ tamper-evident

Interconnection Security Agreement (ISA)
An agreement that defines security controls which need to be in place when a government connects their IT systems to those of an outside entity

Intermediate CA
PKI is a hierarchy, and as a result there are different levels of CAs which must be certified by a separate CA with more authority. These are known as intermediate CAs, and the CA with the highest level of trust/authority is known as the root CA

Internal Threats
Internal threats are those posed by the potential misuse of company information or applications by an employee of the company. These may occur as a result of malicious intent or simply incompetence/bad procedures (user downloading malicious Internet content)

International
International regulations are used to govern standards in two or more nations:
GDPR (EU)

Infrastructure-as-a-Service (IaaS)
Cloud service model which gives the greatest amount of responsibility to the consumer. The provider supplies only cloud infrastructure components, such as servers and storage/networking hardware

Intimidation
Using aggressive tactics to pressure someone to do something or allow access not otherwise allowed
This technique may be combined with impersonation (e.g., an attacker pretending to be the vic-tim's boss)

Insider Threat

Someone who works for the company typically has more access and thus can cause more damage than an outsider

Instrusive Testing

Intrusive testing not only identifies vulnerabilities, but also attempts to exploit them. This can slow performance and has the potential to cause actual damage.

Penetration testing is an intrusive method of testing

IOT

The Internet of Things (IoT) includes things like smart lights and other home automation. These devices have a connection to the Internet and often have no automatic updates, making them the perfect target for attackers making botnets

ip

ip was created to replace ifconfig for Linux and provides additional options such as routing management

ipconfig

ipconfig is a Windows-specific command which displays information about the current network configuration

IPsec

An OSI network-layer security protocol that provides authentication and encryption over IP networks

Provides authentication and integrity by signing packets

Provides confidentiality by encrypting packets

Able to be used with multiple different cryptographic algorithms

Iris Scanner

Scans the color and texture of an iris for authentication. This technology is now found in certain cellphones as a method of authentication

J

Jamming

Interfering with an authorized wireless signal in a way that prevents its use

Job Rotation

Provides everyone with a better view on the job functions as a whole. This may result in better performance, as everyone will understand the other positions' hardships/responsibilities

K

Kerberos

Kerberos is an authentication system designed to enable two parties to exchange private information across a public network by providing mutual authentication, where both the client and server authenticate to each other.

Keyloggers

Hardware or software that covertly records the keystrokes of a user

Key Escrow

A method of allowing a third party to use a private decryption key during certain situations

The private key used to encrypt data is placed in escrow, and the third party is only allowed to access this key for decryption if the terms of the escrow are met

Key Exchange

Securely exchanging keys for an encryption method is a vital part of ensuring the encryption remains secure

Key Management (physical)

The way physical keys are handled within an organization is important, as loss of these keys can lead to unauthorized access/theft

Key Strength

Key strength is a measure of how resistant an encryption key is to brute force and other key-discovery techniques

Key-Stretching Algorithms

Certain algorithms perform key-stretching, which is the process of generating a strong encryption key from a weak password by repeatedly modifying/hashing the password before key generation

Kiosk

Designed to function in a public environment and provide a service, such as an ATM, informational map or flight check-in

Known Plaintext Attack

When an attacker has access to both the plaintext and ciphertext of an encryption method

The attacker can use this to look for weaknesses in the encryption method and easily decipher future encrypted messages

In a Known Ciphertext Attack, the attacker knows the ciphertext but has no access to the plaintext. This can make finding weaknesses more difficult

L

Layer 2 Switch

A Layer 2 switch directs traffic based on MAC address. It does not see IP addresses

Layer 3 Switch

A Layer 3 switch adds the ability to do static and dynamic routing. This can be done using IP addresses. It can also handle VLANs

LDAPS

Use of SSL/TLS allows traditional LDAP to mutually authenticate servers and clients to each other

The protocol is used in many services, including Microsoft's Active Directory

Least Privilege

A security principle that says each entity should be granted only the minimum system resources and authorizations needed to perform its function.

Legal and Compliance

When storing, using, deleting or otherwise managing data, an organization must be aware of and follow all relevant legal and compliance policies and procedures

Least Functionality

The concept of giving users the lowest amount of privilege needed while still allowing them to be productive

Legal Implications

When storing data in a country/state you need to follow the local laws and respond to legal requests

This is true for both backup and recovery sites, and is known data sovereignty (e.g., data stored anywhere in the EU may be subject to GDPR compliance)

License Compliance Violation

Software and hardware solutions are usually paired with a licensing agreement

Not complying with licensing terms may have financial consequences, along with the associated risk of operating outside of the agreed-upon parameters

Life and Safety

Safety of employees and those who use any products produced by a business is obviously the most important consideration when assessing the potential impact of risks. People need to be safe at work and a loss of life is extremely traumatic

Lighting

Lighting can act as a deterrent to an attacker. A well-lit area will reveal an attacker to people and cameras in the area. It also conveys a sense of safety to people who are authorized to be in area

Lightweight Directory Access Protocol (LDAP)

A commonly used protocol for querying and making updates to directories which follow the X.500 standard.

Likelihood of Occurrence

The probability of a given event occurring

Load Balancer

Uses a scheduling algorithm to distribute client requests among a pool of available servers, ensuring individual servers don't receive too much traffic

Location-Based Policies

If your environment can determine the physical (GPS) or network (IP) location of a user, different security policies and permissions can be enforced based on this location data

Lock Types

There are numerous types of locks. Here are a few examples:

- Traditional keys
- Electronic PIN code
- Electronic card
- Deadbolts
- Biometric

Logic bomb

Code that is secretly incorporated into legitimate software and is set to execute when a specific condition is met in the program

Logical Separation

The network can be segmented in a non-physical way using a Virtual Local Area Network (VLAN)

VLANs can help segment network traffic on physical routers

Logs

Logs can be automatically or manually created. For example, a sign in/out sheet or a keycard system which automatically logs whose card was swiped

Logs and Event Anomalies

Having sound logging practices opens the possibility of finding anomalies that can be an indication of security issues

The logs can be monitored in a different ways, either manually or automatically using machine learning

Loop Protection

Loops cause packets to repeatedly traverse the network as fast as possible and will likely cause network outages

IEEE 802.1D (spanning-tree protection) is often used to prevent loops

Low Latency

If speed is the most important factor, symmetric encryption with a smaller key size might be a good option

Low Power Devices

To save power, fewer resources need to be consumed during processing

M

MAC Filtering

Deciding which devices are allowed on a network by using MAC addresses

Some switches allow for MAC filtering, based on which port is being used (port security)

MAC/IP Spoofing

When an attacker changes the Media Access Control (MAC) or Internet Protocol (IP) address of their network interface

This is usually done to help hide their identity or masquerade as another identity

Machine/Computer Certificate

A certificate which is issued to an individual machine to authenticate to a network

Mail Gateway

A server which allows a network to send/receive email communications from other networks. Generally used to receive email from outside the organization

Mandatory Access Control (MAC)

Users are given an access level and are only allowed to view objects at (and sometimes below) their access level

Mandatory Vacations

Mandatory vacations require individuals to take time off and let someone else temporarily take over the responsibilities of their role

Man-in-the-Browser

An attacker infects a Web browser, allowing them to see the browser content as the user and/or modify the content the user sees

Man-in-the-Middle

A man-in-the-middle attack (MITM) is when an attacker is in the middle of two targets' communi-cations, intercepting and/or forwarding messages

The attacker can passively watch (spy) on the communication or actively alter it. This attack is associated with defeating encryption

Man-made Threats

These threats are created by people, both inside and outside the organization

Mantrap

A mantrap is a room, usually small, that you enter before entering a secure area. A mantrap has two doors: an entrance and an exit, and must be entered/exited by one person at a time

Master Image

This is an image of your server/workstation that is specifically configured for what you need. All baseline servers/workstations will be built from this image

Mean Time Between Failures (MTBF)
An estimate of the time it will take for a system to fail, calculated with averages
This is a measurement of reliability and life expectancy for a system

Mean Time to Repair (MTTR)
The estimated time it will take to repair a system to be fully operational following a failure
Measures the maintainability of a system or component

Media Gateway
Software or hardware that converts media streams from one communication format to the other across networks

Memory Management
How and where your application executes is important. You want to confirm that the application allocates and deallocates memory correctly, and that it does not allow malicious code to overwrite/execute in memory

A Memorandum of Agreement (MOA)
Similar to an MOU but is considered a formal contract. An MOA will describe the responsibilities of each party and if these terms are violated, the violating party can be taken to court

Memorandum of Understanding (MOU)
An agreement that two or more parties agree with which is meant to be a precursor to an official contract. This a less formal than a signed contract and is typically non-binding

Message Digest 5 (MD5)
Also created by Ron Rivest, MD5 is a hashing algorithm that converts data into a 128-bit hash
Originally designed to be used as a true cryptographic hash, but collision vulnerabilities have been found

MFDs
Printers and other multi-function devices (MFDs) have proven themselves to be an effective beachhead for attackers, as they can have complex firmware which provides printing, copying, scanning and faxing capabilities

Misconfiguration
When a system or component of a system is configured in a way that causes a vulnerability
Examples included default accounts, error handling and unnecessary components

Mission-Essential Functions
Identifying the functions that are critical to business operations is one of the most important steps when developing a business impact analysis

Mitigate
Implement processes to reduce and respond to risk. For example, role-based training, penetration testing, using the principle of least privilege, etc.

Mobile
Built to be used on the go, typically providing phone and texting capabilities

Mobile Device Management
Just like all other devices, mobile devices have the potential to contain sensitive information and this information needs to be protected in case of loss/theft

Model Validation
Validation is the process of ensuring the design of the developed application allows it to meet all user/consumer requirements.

Model Verification
Verification is the process of making sure the application complies with all design goals.

Motion Detection
Motion detection can alert you to the present of movement in a given area
This can be used to trigger events such as lights, alarms or cameras

MS-CHAP
Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a Microsoft-created version of CHAP and the newer version, MS-CHAPv2, allows for mutual authentication between clients and servers

Multifactor Authentication
Authentication using two or more factors to achieve authentication.
Using multiple forms of authentication from only one factor is NOT multifactor authentication!

Multipurpose proxy
One which has filters for multiple different protocol types, like FTP, HTTP or SMTP

N

NAC
A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the client device

NAT
Network Address Translation (NAT) allows for the changing of one IP address into another, separate IP address

National
National regulations are put in place by a single nation:
HIPAA (U.S.)
SOX (U.S.)
PIPEDA (Canada)
If your organization is doing business in another nation, that nation's regulations will likely need to be followed

Netcat
Netcat is a tool which uses TCP or UDP to read and write data across network connections
The Netcat command is actually run by entering nc on the command line

Network
Created specifically for a router, switch, firewall or other networking component

Network Address Allocation
The way IP addresses are assigned on a network
Dynamic Host Configuration Protocol (DHCP) allows for dynamically assigning IP addresses to devices as they connect to a network and access control

Network-Based Firewall
Controls traffic between two or more networks. Controls traffic into a network (Internet) based on rules that apply to the entire network

Network Scanner
Network vulnerability scanners are utilized to detect vulnerabilities on remote hosts by performing scans across networks

netstat
netstat is used to view ports locally on a machine, displaying which ports have active connections and which process (if any) is running on each port

NFC
Near Field Communications, built from RFID technologies.
Often used in mobile payment systems. One potential vulnerability could be a man-in-the-middle attack

NIDS
Monitors network traffic, looking for malicious activity
If malicious activity is found, a NIDS logs and reports the activity without taking direct action (passive detection)

NIPS
Monitors network traffic looking for malicious activity and is connected inline, so that traffic must flow through the NIPS device

Nmap
Nmap is used to perform host and service discovery on a network or system

Nonce
A random, non-repeating value that is included in data exchanged by a protocol for the purpose of protecting against replay attacks

Non-Credentialed Scans
Non-credentialed scans are performed with the privilege level of an outsider. This means that it is likely to be less intrusive; however, this type of scan may not be able to check all the areas which a credentialed scan is able to

Non-Persistence
Non-persistent systems do not save data; the system boots into the same initial state each time
Does not matter what state the system was in previously before being shut down

Nondisclosure Agreement (NDA)
The signer of an NDA is prohibited from releasing information described within the agreement
NDAs are used to prevent employees or contractors from leaking confidential company information

Non-Intrusive Testing
Non-intrusive tests are done in a way that attempts to make a minimal impact on the network or system. This is accomplished by identifying vulnerabilities without actually exploiting them.
Vulnerability scanning is a non-intrusive method of testing

Non-Regulatory Framework
Beyond the regulatory problems, you may also face consequences internally from your organization
Sometimes an organization will also choose to follow best-practices laid out by a non-governing body (e.g., OWASP)

Non-Repudiation
Non-repudiation is provided when a specific encryption key and/or digital signature is used to identify the sender of a message

Normalization
Typically a precursor to input validation, normalization is the process by which illegal characters are removed from input or modified so they fit the set of accepted characters

NTLM
An updated version of LAN Manager (LM) used by Windows NT
Uses a challenge and response for authentication and only provides client authentication
This protocol is vulnerable to Pass-the-Hash and Man-in-the-Middle attacks

O

OAuth
Token-Based: An OAuth consumer uses a token to access user information stored on provider's website to control what a user is authorized to do on the consumer site

Obfuscation
This is the process of making data harder to read, but does not involve using encryption
Object Identifiers (OID)
Certificates can include additional information through the use of extensions
An extension is identified by an OID number extensions. Besides the number of standardized extensions already created, organizations can create custom extensions to meet their specific use cases

Offboarding
The offboarding process is used when an employee leaves the company and is used to make sure all hardware is returned, all relevant data is saved and all employee access to company resources is revoked

Off-Site Backups
Backups should be stored off-site, as they need to be protected from any attacks/disasters which may affect data on the main site

Onboarding
This occurs when an employee is hired or switches roles. The onboarding process lays out the responsibility of the employer and employee during the transition

Online Certificate Status Protocol (OCSP)
An online protocol used to determine the validity of a certificate by checking the status of a single certificate with an OSCP server, rather than receiving an entire CRL

On-Premise
The organization has full control of everything, including software installation and the physical location of the servers

Open ID Connect
A layer on top of the OAuth protocol which simplifies the process of developing a single sign-on mechanism

Open Network
The network is open for anyone and does not require a password/ credentials

Order of Restoration
Assigning priority to things that need to be restored in the event of an outage is good practice. It is better if these priorities are defined before a disaster rather than during one

Order of Volatility

The more volatile data is, the more likely it is to change or be otherwise overwritten. When performing forensic analysis, it is important to collect volatile data while it still exists before moving onto less volatile data

Organized Crime

Organized criminals that use hacking to further their criminal enterprise

Cybercrime is gaining popularity due to the ability to operate from different countries, making prosecution more complex

Examples include data theft, extortion, blackmail and identity theft

OSINT

Open-source intelligence is data that is publicly available and can be used to further an attack

Information found via email harvesting and social media profiling

Things that can be found using Google, Facebook, etc.

Out-of-band exchange

Means the key(s) are sent over an unrelated channel, such as relaying a key verbally or sending it in the mail. These methods can be easily infiltrated/compromised

Owner

The person who exercises control over the data. For example, the Chief Financial Officer may own all the accounting data

P

PAP

Password Authentication Protocol (PAP) is an authentication method which works with Point-to-Point Protocol (PPP).

Passive Detection

Passive detection inspects traffic from an outside view. This results in any action taken by the detection system being reactive, as it must happen after rather than during the detection (e.g., NIDS)

Passive Reconnaissance

When an attacker gathers information without actively engaging the target service, person, property or network

Passive Test

Passive scanning is designed not to interfere with the network or system being scanned. At a high level, this is accomplished by not actually exploiting any vulnerabilities.

Passwords and Pins

Passwords and PINs rely on complexity to be effective. A short or non-complex PIN may be easily brute-forced

Password Complexity

Attackers can use automated tools to guess thousands of passwords in an extremely short amount of time!

Establishing minimal complexity rules for user passwords can help prevent against these types of brute-force attacks

Use of multiple types of characters, including letters, numbers and special characters (!@#$) makes passwords much more difficult to brute-force than those which use only one type of character

Password Cracker

Software that aids in recovering secret passwords stored in a computer system or transmitted over a network

Patch Management

The systematic notification, identification, deployment, installation and verification of software updates. These updates/revisions are known as patches, hot fixes and service packs

Password Length

Passwords should be long enough to make things difficult for an attacker, but if they are too long users will end up simply writing their password down (not secure)

Password Recovery

This process should be well-defined and secure to prevent unauthorized persons from impersonating users to reset passwords and gain access

Payment Methods

Modern mobile devices come with mobile wallets. This allows the phone to be used as a payment method like a credit card, often using RFID and NFC technologies

PBKDF2

Stretches a key by adding a salt value and hashing the resulting data

Repeats the above process until the newly-created cryptographic key is hardened against brute-force attacks

Penetration Testing

Penetration testing is simulating an attack with the goal of finding both weaknesses and strengths. It involves actively exploiting vulnerabilities as they are discovered, to penetrate as far as possible into the target system.

Look for common (known) exploits as well as unknown exploits

Permanent NAC

Permanent NAC uses an agent which is installed onto the client system and is persistently running in the background, performing a NAC check each time network access is requested

Permission Auditing and Review

Permission Auditing and Review refers to a system of monitoring a user's privileges and ensuring that no user has access which is unnecessary to perform the functions of their role.

Permission Issues

If files on a system have relaxed permissions, it is easier for someone to view/modify information they are not supposed to access

Persistence

An attack that creates and maintains remote access into a system

Gives the attacker the ability to maintain access/control on a machine

Personal Email

Polices need to be in place regarding the use of personal email or using work email for personal communication

Personal Identity Verification (PIV) card

An identity card issued to a U.S. government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation)

Personally Identifiable Information (PII)

Data which identifies an individual and is often required to be protected under guidelines such as PCI DSS. Protecting the PII of those in the organization also helps to mitigate social engineering threats

Personnel Management

Personnel management is a concept which involves creating policies to manage personnel in a way that increases the security of an environment

Phishing
Phishing is a method of sending digital correspondences that appears legitimate but is actually meant to lure a potential victim into providingw personal information for malicious purposes

Physical Controls
Controls which provide physical barriers to prevent access to information. Includes alarms, locks, fencing and security guards

Physical Separation
A physical separation may be the ideal way to provide protection for extremely sensitive data
This could mean that the data is stored in a separate place and/or that the network to access it is physically separated from the rest of the topology

ping
The ping command uses ICMP packets to quickly determine if a machine with a chosen IP address or host name is online and responsive in a network

Pinning
Pinning is an additional control to ensure a certificate is legitimate and is used to prevent man-in-the-middle attacks

Pivot
The method of using an instance (also known as a foothold) to be able to move from place to place inside the compromised network
Essentially using the initially-exploited machine to further compromise other machines on the network

PKI Concepts
Proper implementation of a PKI involves understanding and use of certain concepts, such as whether it is appropriate to use a single-tier or hierarchical trust model or how to use key escrow to allow a third party to securely use a private key which they do not own

Platform-as-a-Service (PaaS)
Cloud service model which lies between SaaS and IaaS, where the provider manages all hardware components of the cloud infrastructure (network, servers, storage) and provides a basic Web application or database platform

Platform and Vendor-Specific Guides
Having secure configurations will depend heavily on the specific technology being used. It is important to remember that although the technology may work, it does not mean that it is secure!

Policy Violations
When users do not to comply with policy guidelines (either maliciously or accidentally), security issues can arise

Port Security
Switches have the ability to control who will be able to communicate over a port (MAC filtering)
Using extensible authentication protocol (EAP), the switch requires devices to provide correct authentication data before activating a port

Preservation
Investigation can take a long time to conclude. This is especially true in the court systems, where cases may span years. It is critical that a strategy is in place to preserve the data and evidence you collected and to ensure proper chain of custody remains in place to prevent tampering
Pretty Good Privacy (PGP)
A standard for encrypting email messages and creating certificates for public key cryptography

Pre-Shared Key (PSK)
A secret key that is established before connecting to an access point

Preventive Controls
Preventive controls serve to prevent an attack from happening in the first place

Privacy Impact Assessment (PIA)
An analysis of how information is handled to determine the current level of risk as it relates to a company's handling of PII

Privacy Officer
Responsible for the data across the organization meets requirements set in relevant polices and procedures

Privacy Threshold Analysis (PTA)
An analysis which is done to determine what privacy concerns an organization may have
Involves examining the types (and amount) of PII collected and stored by an organization. If this PII reaches a certain threshold, a PIA is performed

Private cloud
is one where an organization owns the entire cloud infrastructure and uses it internally. Hosted private means a third party provides the organization with the cloud infrastructure

Private Key
A private key is the counterpart to a public key when using an asymmetric cryptographic algorithm
A private key is kept secret and is used to compute a digital signature that may be verified using the corresponding public key
Information encrypted with a public key can only be decrypted with the corresponding private key

Privileged Accounts
Privileged accounts have a higher permission level than regular user accounts and are thus more powerful.

Privilege Escalation
When an attacker elevates his privileges to gain access to resources that he would not other-wise have
The ability to elevate the privileges can be caused by a bug or simple oversight

Privileged User
A privileged user is one that has greater access to sensitive data than a normal user
A privileged user might receive more in-depth security training, with an emphasis on keeping data secure

Production
The final code that is in use

Proper Error Handling
Even with thorough QA testing, errors are bound to be arise at some point when code is run. Attackers will actively try to produce errors in the hope that the error and its resulting message will provide them with information leading to a possible attack vector.

Property
The capital goods that will need to be replaced if lost or damaged and typically will only be lost/damaged due to a natural disaster

Proprietary
Data involving the intellectual property or inner workings of a company. This data must be protected against theft by competitors

Protected Distribution/Cabling
A wire line or fiber optic system that includes adequate safeguards to prevent an attacker from cutting or eavesdropping on connections. Uses electronic shielding and metal casing or alarms

Protected Extensible Authentication Protocol (PEAP)
Uses an encryption certificate server-side to create a secure tunnel to encapsulate EAP

Protected Health Information (PHI)
Data which contains information about someone's medical health (medical records or health insurance information). PHI can be used to commit fraud using insurance information or to blackmail someone based on a health condition, and is protected by the federal act known as HIPAA

Protocol Analyzer
A device or software application that enables the user to analyze the performance of network data so as to ensure that the network and its associated hardware/software are operating within network specifications

Provisioning
The process of making an application available in an environment. During provisioning, applications are sometimes packaged so they can all be installed in one step

Proximity Cards
A proximity card is a smart card which uses the contactless method to transmit data to a reader wirelessly

Proxy
An application that "breaks" the connection between client and server
Communications are processed by the proxy when entering or leaving a network and are then forwarded to the recipient if accepted by the proxy

Public cloud
is hosted by a third party and anyone with an Internet connection can access and subscribe to it

Public Key
A key that is used with an asymmetric cryptographic algorithm and is associated with a private key
A public key is associated with a single owner and is typically publicly-available information
In the case of digital signatures, the public key is used to verify a digital signature that was signed using the corresponding private key

Public Key Infrastructure (PKI)
A public key infrastructure is a system of components which allows for secure communication through the use of certificate authentication

Push Notification Services
Notifications sent by applications on a device to the user, usually to notify/remind them of something application-specific

Q

Qualitative risk assessments
Less complex than their quantitative counterparts and focus on evaluating risks based on general significance. Rankings include high, medium and low-risk categories rather than assigning numerical values

Quantitative risk assessments
Use numerical values when determining cost and assigning levels of risk, and include concepts such as SLE and ALE

R

Race Condition
A logic problem that can occur when actions are dependent on the timing of outside events
When the timing of actual events does not match the program's expectations, problems can occur

RACE Integrity Primitives Evaluation Message Digest (RIPEMD)
Developed in Europe for use in broadband networks
Designed as an alternate hash function and is similar to SHA-1 when using 160 bits (RIPEMD-160)

RAID-0 (striping)
RAID-0 provides faster read/write times, but does not actually provide any redundancy or fault tolerance. When using two disks, half of the stored file is allocated to each disk, so if one disk fails the file is corrupted.

RAID-1 (mirroring)
RAID-1 uses two disks, placing an exact copy of the stored file on each disk. If one disk fails, the file is still usable from the other disk. Only able to use 50% of storage capacity due to file mirroring.

RAID-5 (striping with parity)
RAID-5 requires three or more disks, with the stored file being striped across all but one of the disks as in RAID-0. However, the remaining disk is set aside to contain parity information, which allows for the recovery of the file if only one drive fails. RAID-5 cannot recover data in the event of two or more failures.

RAID-6 (striping with double parity)
RAID-6 requires four or more disks and is similar to RAID-5, except it uses two disks for parity rather than one. This decreases total storage capabilities but allows for the failure of up to two disks.

RAID-10 (striping with mirroring)
RAID-10 combines the models of RAID-0 and RAID-1 to attain faster read and write capability along with fault tolerance. Raid-10 requires four or more disks, and essentially splits the disks into striped sets of mirrored data. Data is recoverable as long as there is a disk remaining in each mirrored set.

RADIUS
Remote Authentication Dial-In User Service (RADIUS) uses a centralized server to provide Authentication, Authorization and Accounting (AAA) to remote users in a scalable way.

RADIUS Federation
Refers to when multiple organizations share their centralized AAA platform, allowing one organization's users to authenticate to a separate organization's RADIUS server

Rainbow Tables
A table of previously-computed values for reversing hashing functions
Often used to crack password hashes

Random and Pseudo-Random Number Generation

Random number generators are used in cryptographic schemes to provide strength, as random numbers cannot easily be guessed/spoofed

Recertification

A permission auditing scheme can require users to recertify at a repeating interval. At this time, permissions are audited to ensure that users do not have unneeded permissions

Recording Microphone

Many mobile devices have sensitive microphones which can be used to record things surreptitiously

Malware may be able to record conversations without the user's knowledge

Recovery

Data evidence (whether before initial collection or during preservation) can become corrupted

In the event of corruption, tools can be used to recover data by examining hard disks

Recovery is not always possible and data can be lost!

Recovery Point Objective (RPO)

The point in time to which data must be recovered after an outage (i.e., how much data can be lost?). Having an RPO of 12 hours means all data created outside of the past 12 hours can be recovered from backups

Recovery Sites

A recovery site is a location which provides an organization with the capability to continue operations in the event of an attack or natural disaster shutting down their main site.

Recovery Time Objective (RTO)

The overall length of time an information system's components can be in the recovery phase (after an attack/disaster) before negatively impacting the organization's mission or business processes

Redundancy

Having excess hardware, software and automation in place to handle failures

Failures will always happen eventually, so having the systems in place to handle this is key to securing uptime

Redundant Array of Independent Disks (RAID)

RAID is a model which uses multiple disks to store parts of the same data, allowing the remaining disks to serve as backups in the event of a failure.

Refactoring

The practice of changing the way something is coded without changing the end user experience. The lack of refactoring may provide the time for an attacker to find an exploit. Alternatively, bad refactoring may create exploits

Regulatory Framework

Regulatory issues regarding data security and the responsibilities of data owners are becoming more and more relevant

Remote Access

Remote access can be handled by a concentrator. This refers to the ability of a remote user to access the VPN gateway through their local network. Allows people working from home to connect to the company's corporate network

Remote Access Trojan (RAT)

A RAT is a specific type of Trojan which is used to install a backdoor on a system.

Remote Wipe

The ability to remotely and securely remove all data from a mobile device

This can be used in the event a device is stolen or a source of data theft/leakage is found

Removable Media Control

Removable media can be a transmission source for malware or cause data loss

Examining log events related to removable media can help detect attempted attacks or data exfiltration

Replay Attack

When an attacker retransmits valid data with malicious intent

Similar to an application replay attack, but in this context an attacker may capture and replay any wireless traffic sent by a user

Reporting Requirements

Recording events and steps taken during an incident is important so the incident can be later reviewed and learned from

Reputation

The way an organization handles a disaster can impact their reputation. This can have a positive impact if things are handled well. If things are handled poorly, they might have a PR disaster

Resource Exhaustion

Usually associated with a denial-of-service attack

Occurs when a resource is completely consumed, preventing a system from taking a specific action and potentially causing a loss of revenue

Retinal Scanner

Used your retina as a factor of authentication by scanning the relatively unique pattern of blood vessels

Reverse Proxy

A reverse proxy does the opposite. It proxies on behalf of a server, receiving requests and forwarding responses on behalf of internal servers

RFID

Radio frequency identification, used in technologies such as access badges or tracking systems

Susceptible to replay attacks or data sniffing

Risk Assessments

Used to determine the potential costs and likelihood of various threats and to rank them in terms of severity

Risk Register

This is a document that outlines possible risks and risk mitigation by categorizing and ranking each risk faced by an organization

Rivest Cipher 4 (RC4)

RC4 is a stream cipher created by Ron Rivest. It uses a key length of anywhere from 40 to 128 bits

Known for originally being used with WEP and SSL. Found to be weak and has been deprecated

Rivest-Shamir-Adelman (RSA)

One of the first and still widely-used asymmetric encryption schemes. Uses a variety of block/key sizes

Considered to be slow, so it is commonly used to encrypt symmetric keys which are then used to continue the encrypted communication

Roles and Responsibilities
Incident response plans assign roles to employees during an ongoing incident, delegating mitigation and recovery responsibilities among these roles

Role-Based Access Control (RBAC/role-BAC)
A model for controlling access to resources where actions are permitted on resources based on requestor roles rather than individual identities
Different from Rule-Based Access Control!

Root Certificate
A public certificate associated with the root of a CA
This is the most trusted certificate and is where the certificate chain of the hierarchy of intermediate CAs begins

Rootkits
A rootkit is a type of backdoor which embeds itself into core system processes, making it difficult to detect and remove

Rogue AP
An unauthorized wireless access point installed on a network
Can be done maliciously or benevolently

Rotate by 13 (ROT13)
In a substitution cipher, letters or units of data get replaced with different data to create a ciphertext
ROT13 is an implementation of a substitution cipher where each letter is rotated by 13 places in the alphabet

Round Robin
A method of scheduling where the server nodes are set into a certain order and each incoming request is simply passed on to the next server in the list. Once the end of the list is reached, loop back to the beginning of the order

Router
On a network, a router is a device that determines the best path for forwarding a data packet toward its destination. The router is connected to at least two networks and is located at the gateway where one network meets another

Routing and Switching
Being able to control what traffic can go where on a network is vital for both the performance and security of the network
Can be used to segment pieces of the network

RTOS
Real-Time Operating Systems (RTOS) are used to control devices that need to respond in real time and minimize reboots/crashes

Runtime Code
Code which is run as-is and is compiled during runtime by an interpreter, which compiles each line of the code as it executes

S

Safes
Safes can be used to protect objects from fire, water, theft or tampering
Having important equipment or documents in a safe increases the security and safety of these items

Salt
A value that is used in a cryptographic process to modify the regular result of a data hash

SAML
Security Assertions Markup Language (SAML) is a framework for exchanging authentication and authorization information, typically used by federated networks.

Sandboxing
A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized

SATCOM Connection
A device that can utilize satellite communications. These devices are best suited for communications in remote areas

SCADA
Supervisory Control and Data Acquisition (SCADA) systems or Industrial Control Systems (ICS) are used to connect and control large industrial equipment.
Scalability
The ability to ramp up and down based on load or need

Scarcity
Using the idea of a limited amount to make someone take action
For example, a phishing attack that has a link to claim one of five free laptops

Screen Filters
Modern screens are high-resolution, making them easier to read and providing an attacker with an opportunity for shoulder-surfing

Screen Locks
A password, PIN, pattern or biometric that needs to be entered before a mobile device can be unlocked

Script Kiddie
Someone who successfully completes a hack by using scripts (code) that they do not have the ability to create themselves

Secret Algorithms
People sometimes hide parts of an encryption algorithm with the belief that this will make the encryption more secure

Secure Baseline
A defined way that the software should behave in its initial state, including the requirements needed to run the software securely

Secure Boot and Attestation
Secure Boot is built into UEFI and checks the booting system's certificate signature against known certificates from reputable OS vendors. It prevents booting if the signature isn't matched

Secure Cabinets
Secure cabinets can be used in much the same way as a safe, but are less out-of-place in a typical office environment

Secure Coding Techniques
The best way to develop secure code is by being aware of proper secure coding techniques and to constantly implement them during the development process.

Secure Configurations
Best practices should be followed while configuring the operating system to ensure that it begins from a state of maximum security

while still being able to perform its intended purpose

Secure DevOps

Developing a secure product requires a continuous focus on security throughout the development life cycle.

Secure Hash Algorithm (SHA)

SHA was adopted by NIST as a replacement hashing standard over MD5

SHA-1 was created as a quick fix to the original SHA algorithm and in turn was found to have collision weakness, though it is generally considered more secure than MD5

SHA-2 was created to solve the issues found in SHA-1, and has a longer output (digest). SHA1- outputs 160 bits whereas SHA-2 supports output lengths of 224, 256, 384 and 512 bits

Secure Logs

To ensure logs are protected from tampering, only system processes and secure, non-administrative accounts should be able to write to them and only by appending data to the end of the log.

Secure IMAP

Secure IMAP (IMAPS) is the secured version of Internet Message Access Protocol v4 (IMAP4)

Addresses issues in POP3 by allowing permanent connections to servers and letting multiple clients connect to one mailbox

Secure POP

Secure POP is an implementation of Post Office Protocol v3 (POP3), which adds the ability to secure mail communications.

POP3 allows users to download mail onto an email client from the server where the email data is stored

Secure Staging and Deployment

When developing code, it is important to consider security from the beginning rather than as an afterthought

Secure Token

Tokens can provide authentication that is stored client-side

Security-as-a-Service (SECaaS)

Having all (or some) of your security appliances and software live in the cloud is referred to as SECaaS

Processes such as antivirus scanning and SIEM data collecting/ aggregation are offloaded to the cloud

Security Automation

Good practice dictates that software should be tested before it is released. Much of this testing can be automated. Automated tests can check for functionality and known security threats

Security Guards

Security guards can be used to confirm identification, patrol physical locations and respond to emergencies

Security Through Obscurity

The concept where an attacker not knowing how a system works makes this system more secure

Self-Signed Certificate

Self-signed certificates are typically created for use with Web servers or developed applications

Self-Encrypting Drive (SED)

A disk that uses built-in hardware to encrypt/decrypt data stored on the drive

Sensors

Sensors include things like proximity badges, motion sensors and perimeter sensors

Thought has to be given to where and how these sensors are used

Separation of Duties

Splitting job responsibilities so that no one person can take critical actions on their own

Often, payroll departments will require checks to be co-signed to prevent a single person from having the power to (maliciously) distribute checks

Server

Created to serve requests from client computers and to potentially host applications and databases

Server-Side Execution

Server-side execution refers to code from an application that is run directly on the hosting server, and validation on the server side protects against any attempt by a program/user to bypass validation on the client side. Server-side validation acts as a failsafe in case client-side validation is bypassed

Service Accounts

Accounts used by the OS to access and run specific processes and assist with automation.

Service-Level Agreement (SLA)

Agreement that specifies the minimum level of service that needs to be provided between parties

Defines items such as the responsibilities of the service provider and the lowest levels of quality and availability that the client will tolerate when using their service

Service Set Identifier (SSID)

The SSID is a name associated with a WLAN

Allows devices to distinguish between and connect to different wireless networks

Session Hijacking

When an attacker uses a victim's valid session (key, cookie) to validate with a service

Session Key

A cryptographic key established for use for a relatively short period of time. The session key is used to encrypt/decrypt all communications until the end of the current communication session

Also known as a symmetric key

SFTP

Secure File Transfer Protocol (SFTP), aka "Secure FTP," is designed to send files over FTP in a reliable and secure way

Uses Secure Shell (SSH) to establish secure (encrypted) FTP communication between a client and server on TCP port 22

Shared and Generic Accounts

Accounts that multiple people can log into are known as shared accounts

Shimming

A shim is commonly used as a way to support legacy software. Code is used to allow the old sys-tems to speak with the new one. An attacker can use this concept to build their own shims that can result in malicious activities

Shoulder-Surfing

When an attacker looks over a victim's shoulder to steal sensitive data (e.g., ATM PIN code)

Sideloading
Is the process of installing applications directly by using developer tools rather than going through an app store

SIEM
A SIEM is an application that provides the ability to gather security log data from multiple information system components

Signal Strength
The distance an antenna can receive the transmission is directly related to the strength of the signal
Stronger signals can be received at further distances and through a greater number of obstacles
There are multiple ways to boost signal strength (changing wavelengths or antenna type)

Signature-Based Detection
The process of comparing signatures defining known malicious activity against observed events to identify possible incidents

Signs
Signs are important to communicate who and what is allowed in a specific area

Single Loss Expectancy (SLE)
Is the projected loss in the event that a single risk event takes place

Single Point of Failure
Having a single point of failure means that there is a single system entirely controlling an application or functionality. If this system fails, there is no way to keep operations running smoothly

Single Sign-On
Single sign-on (SSO) employs a central authorization server to enable a user to authenticate once yet access all applications or machines which they are permitted to use

Site-to-Site
A site-to-site VPN connects two or more local networks together through the VPN. This is not same function as a concentrator

Smart Cards
A smart card contains a chip which is scanned by a smart card reader to provide authentication data

Smart Devices
Used to enhance a regular object by connecting it to the Internet (e.g., smart TVs, refrigerators, washer/dryers)

S/MIME
Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard used to secure email communications
S/MIME uses a classic, hierarchical design based on certificate authorities for its key management

SMS/MMS
Short Message Service (SMS) and Multimedia Message Service (MMS) allow for sending text messages and transferring files within an environment, but come with challenges:
» Spreading of malware
» Phishing
» Data exfiltration
» DoS attacks

SNMPv3
Simple Network Management Protocol is used to monitor and manage a network
To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB)

SoC
System-on-a-Chip (SoC) devices are computing devices that have all their functionality handled with one chip, saving space and providing power efficiency.

Social Engineering Techniques
Use deceptive tactics to trick individual into providing information they otherwise would not

Social Media
Policies need to be in place about how social media can be used on and off work systems to help prevent sensitive company information from being exposed and to protect against social engineering attacks

Something You Are
Using a physical aspect of a person for authentication
This generally involves collecting biometric information by performing fingerprinting, iris scans or facial recognition. The recorded information is then compared to input given when users request access to determine if there is a biometric match

Something You Do
Using a unique action as a method of authentication
Makes use of biometric information that is collected by analyzing behaviors rather than physical aspects
Examples include signature writing, typing and speaking patterns

Something You Have
This refers to authenticating with a physical object that can be carried
Using keys, key cards, cell phone, etc. as a factor of authentication

Something You Know
Using a secret such as a password or a PIN as a factor of authentication
Also includes Personally identifiable information (PII) like your name, address or birthday, though this information may be more well-known and thus less secure

Software-as-a-Service (SaaS)
Cloud service model where the provider manages the entire cloud infrastructure, including network, servers, operating systems, storage and application capabilities

Software-Defined Network (SDN)
Using software to manage a network by separating control and traffic forwarding. This approach generally utilizes cloud computing

Software Tokens
Software tokens are generated by an application (such as Google Authenticator) and generally consist of a string of letters/numbers which must be used as input to authenticate

Spearphishing
Phishing designed for and conducted towards a specific person or persons

Special Purpose Device
Medical devices, vehicles and unmanned aerial vehicles (UAVs) are all special-purpose device
Like any other device they have firmware/operating systems that could

be compromised.
The level of data sensitivity that is compromised can prove disastrous

Split Tunnel
In a split tunnel, a portion of the traffic does not go through the tunnel
For example, a remote connection to a corporate server would go through the VPN tunnel, but a general Internet connection would not

Spyware
Software that collects information about the user, system or organization by monitoring user activity without their knowledge or consent

SRTP
Secure Real-time Transport Protocol (SRTP) provides encryption (default AES), authentication, integrity
Securely enables streaming of media data and is intended for use in VoIP communications

SSH
Allows for secure remote connection to a machine and is often used for remote administration tasks
Uses TCP port 22

SSL Decryptor
Dedicated proxy used to decode and inspect encrypted traffic as it enters or leaves a network
Used to prevent attackers from passing maliciously encrypted data onto a network

SSL/TLS
Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a protocol designed to provide secure communications and data integrity over the network
Uses a client-server handshake to establish an initial connection and generate encryption certificates

SSL/TLS Accelerator
A hardware device that speeds up the processing of SSL/TLS encryption
The accelerator handles the processor-intensive parts of the encryption process by using a specialized chip for the calculations

Staging
Production-level area where the code can be tested and used against data similar to that found in production

Standard Naming Convention
Names should be memorable and avoid using information that could change frequently

Standard Operating Procedures
A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event

Statefull Firewall
Makes decisions on whether to allow or deny packets based on the status of the communication session between hosts

Stateless Firewall
Control traffic based on static values such as source/destination address and protocol type (ICMP, TCP, UDP etc.)
Inspects the values of individual packets to make determinations. This process is often referred to as packet inspection

Static Code Analysis
Tool can be used to analyze code before it is packaged into your application
Static analysis involves scanning code using signatures of known issues, and does not actually execute the code itself

Steganography Tools
Tools that help hide or extract data from within another file
Steganography is the art of hiding data within other data. It is a form of hiding data “in plain sight” and is not as secure as actually encrypting data

Steward
Manages the accuracy and privacy of data, along with confirming data security

Storage Segmentation
Separating out segments of storage to be used for specific purposes by designating different areas of memory for each data type

Stored Procedures
A stored procedure is a database query in which the database receives an input key and returns the matching pre-defined value as an output

Strategic Intelligence
Forensic information provides strategic intelligence information on the who, what, why and how of an attack. Knowing this information allows organizations to modify systems and procedures to better protect themselves against future attacks

Stream Cipher
Encrypts a stream of data one byte at a time, beginning with an IV. Stream ciphers are best used when the amount of data to be encrypted is not initially known and/or data needs to be processed and encrypted continually. RC4 is an example of a stream cipher

Stress-Testing
Putting a heavy load on an application may cause it to fail in unexpected ways.
These failures can be examined, so that they are handled gracefully if they occur in the real world. You do not want failures to give an attacker a foothold or an opportunity for a DoS attack

Subject Alternative Name (SAN)
A type of certificate extension which allows different alternate name values (email/IP addresses, general names) to be linked to the certificate

Subscription Services
Employees often need to access various kinds of subscription services to perform their duties. Content to/from these services needs to be delivered securely and generally comes with a method of authentication

Supply Chain
The supply chain can be a weak point in security. If a device is compromised intentionally during manufacturing, it is going to be hard to diagnose or remedy.

Supply Chain Assessment
Looking at the supply chain from start to finish and looking for risk and improvements
This includes looking for improvements in efficiency and security but can prove difficult, as a full assessment can require obtaining confidential information from multiple companies

Switch

A network device that filters and forwards packets between LAN segments

Essentially a multiport bridge which can process and forward data on either the data-link layer

Symmetric Algorithms

A cryptographic algorithm that uses the same secret key for both encryption and decryption

System Administrator

Is the person who controls who can access resources, applications and data in the environment

Generally has total control over a particular system and can assign user roles/permissions and make critical changes to the system

System Owner

System owners decide the layout of a network and its associated systems

System Sprawl

When a system grows and components are added without full knowledge of impact or incomplete documentation

T

TACACS+

The Terminal Access Controller Access-Control System (TACACS+) was created to improve upon the security of RADIUS.

Tailgating

When an unauthorized person follow an authorized person into a restricted area

Piggybacking — Same technique, but requires consent/knowing cooperation from an authorized person (while tailgating is just sliding in behind while the door is still open)

Taking Backups

Taking backups, either by simply duplicating data or taking snapshots of the total current state of a device, allows for the quick recovery of data during an outage

Taps and Port Mirroring

Taps and port mirrors are used to capture packets on the network. This would generally be done for analysis

tcpdump

tcpdump is a command for Linux whose function is to capture (sniff) packets on a network

A basic usage would be running tcpdump -i eth0, which will cause tcpdump to display all packets captured on the eth0 interface until the program is halted

Technical Controls

Controls dictated through technology and used to determine what types of applications/traffic are allowed. Example: application white/blacklisting

Templates

Templating can make scripting easier because the script can just reference a template for its specific need

Simply modify a few variables and the script is complete with a new template

Test

It is important to put code to the test before deploying to the production environment. A place where developers can perform initial tests of code and solutions

Tethering

A mobile device can be tethered to other devices, allowing these other devices to make use of the original mobile device's data connection

Can be done via Wi-Fi, Bluetooth or physical connection

Thin Access Point

A thin access point can be thought of as a switch with an antenna. It does not have features that would help manage clients and thus requires management by a wireless controller (controller-based)

Third-Party Libraries and SDKs

Software which provides built-in functionality to a developer

Third-party libraries speed up the development process, allowing developers to make use of functions without having to build them from scratch (complex math libraries)

Threat Assessment

Performing a threat assessment involves identifying possible risks to the safety/productivity of an organization and classifying these threats based on severity and likelihood of occurrence

Time-Based One-Time Password (TOTP) algorithm

Adds time-based expiration to generated passwords

Time-of-Day Restrictions

If you know that a resource is not going to be used during a certain timeframe, it can have time restrictions put on it

Time Synchronization

A SIEM must be able to normalize the timing of events from all sources into one time zone

If the timing is off, reconstructing a security event can impossible, as knowing the correct chronological order of events is essential to figuring out when and how an attack happened

Tokens and Cards

Tokens can be hardware- or software-based and are used to aid in providing authentication before access is given.

TPM

Trusted Platform Module (TPM): A tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation)

Tracking Man-Hours

It is important to track all man-hours which are spent collecting and analyzing evidence during a forensic process. Be sure to include hours used by third-party resources as well!

Transfer

Moving risk responsibility from one party to another. An example is using insurance to transfer the risk of loss to the insurance company

Transitive Trust

When trusting domains, a system can be configured to trust domains transitively

Allows the system to trust networks which are trusted by the original domain without explicitly creating this trust

Transparent Proxy

A proxy that receives and forwards traffic without modifying it (similar to how looking through a clear window does not modify a view)

Transport Layer Security (TLS)

A cryptographic protocol which provides privacy and data integrity

between communicating applications

Transport Mode
Encrypts only the packet data and does not encrypt the packet's IP header
Generally used on private networks for end-to-end communications

Trojans
Malware that is disguised or hidden in seemingly legitimate software.

Trust
Similar to familiarity, except that the attacker takes time to build a relationship
The trust gained in the relationship is then used to further the attack

Trust Model
PKIs can make use of different trust models, either using a single CA or creating a hierarchy of CAs with the root CA granting authority to intermediate CAs through certificate chaining

Trusted Operating System
An operating system in which there exists a level of confidence (based on rigorous analysis and testing) that the security principles and mechanisms are correctly implemented and operate as intended even in the presence of an attacker

Tunneling
VPN tunneling allows for multiple devices/networks to connect securely even if they are physically separated, often using one of the two methods below:
Site-to-SiteVPN gateways tunnel traffic for entire networks
Remote Access Clients use their local network to connect to the VPN, typically by authenticating at a VPN gateway (work-from-home model)

Tunnel Mode
Encrypts the entire packet and appends a new IP header
Used to used to send communications on non-secure networks

Type I Hypervisor
Type I hypervisors run directly on the system hardware and manage the hardware without utilizing a host OS
They may be referred to as: native, bare-metal or embedded hypervisors

Type II Hypervisor
Type II hypervisors run within the operating system of the host. Act as a manager for virtual machines on the host
Must support the OS of the host machine

U

Unauthorized Software
Software that is untested may contain malicious elements such as spyware or malware

Unencrypted credentials
Storing credentials in plaintext is dangerous. It is recommended to encrypt login credentials and other sensitive information when storing or transmitting them
Unified Extensible Firmware Interface (UEFI)
A possible replacement for the conventional BIOS that is becoming widely deployed in new x86-based computer systems. The UEFI specifications were preceded by the EFI specifications

Unified Threat Management (UTM)
A UTM solution is a service or appliance that offers protection against a wide variety of threats through a single platform, rather than having separate products for different security functions

Untrained Users
A system with theoretically-perfect technical security still relies on a user, and users are often the weakest link!

Urgency
Using the lack of time to make people take action that they would not otherwise take
For example: a ransom that gives you 24 hours to pay the ransom or lose the data

URL Hijacking
When an attacker relies on a mistake to get a victim to their site. Often referred to as Typo squatting. For example: google.com vs. goolge.com

Usage Auditing and Review
Similar in value to a permission audit, usage auditing and review ensures that users are making appropriate use of their permissions and are not attempting to exploit them.

USB Blocking
A DLP solution can block USB writes in an environment when the data being written is determined to be confidential

USB Connection
USB has the advantage of needing physical access to the device to make a connection. The flip side of this is that if it is possible to get this connection, it is more likely that the attack will work

USB On-the-Go (USB OTG)
A feature on certain mobile devices that allows the device to act as a host for peripherals (drives, mouse, keyboard) via a USB connection

User
This is the everyday consumer of the environment
A user might receive generalized role-based training and standard security-awareness training. The training would likely cover topics such as phishing

User Accounts
A user account has limited privileges and will be used for general tasks, such as reading email and surfing the Web.

User Certificate
These are commonly used as another factor for a user to authenticate to a computer or an application

User Training
User training can be one of the most critical layers of defense-in-depth, as users are often the "weakest link" in the security chain

V

VDE
VDE refers to the user's virtualized desktop environment, and all processing done in this environment is actually handled by the hosting server. The user's machine is used simply to connect to and display the virtual desktop

VDI
VDI is when an organization configures machines to run using a VM. The user boots the machine, and a basic OS then authenticates the user and connects remotely to the VM pool to provide the user with

their virtual desktop

Vendor Diversity

Relying on a single vendor for security can be problematic. If a zero-day is found that affects that specific vendor, your entire security implementation could be compromised

Version Control and Change Management

When making changes to a program, having version control helps to keep track of changes as they happen over time. In the event an issue/bug occurs in the code, the problem can either be tracked down and eliminated or the code can be rolled back to an earlier version before the issue arose

Virus

A malicious computer program that attaches to applications or executable components.

Virtual Desktop Infrastructure (VDI)

This allows administrators to develop for a single virtual environment in lieu of administering multiple devices

Virtual Private Network (VPN)

Using a VPN allows you to connect to a private network remotely without having to go through a public network

Virtual IPs

Offer a virtual IP to advertise a service without publicly exposing the IP addresses of the internal servers used by the load balancer

Able to force clients to go through the load balancer to communicate with the servers

Virtualization

The use of an abstraction layer to simulate computing hardware so that multiple operating systems can run on a single computer

Vishing

Using phishing techniques over voice calls

VM Escape

Attackers will attempt to escape their virtual environment and interact with the host environment

This can be hard a problem to solve. Layered security and good logging practices can go a long way toward mitigating these threats. Be sure to keep VM software up to date!

VM Sprawl

Making virtual machines has become relatively easy and is certainly easier than setting up a physical server. This makes it more likely that the VMs will become unwieldy. The excessive deployment of VMs is known as VM sprawl

Voice and Video

Used by businesses to allow for Voice over IP (VOIP) and Web/video conferencing capabilities

Data must be sent/received in real time, as in video and audio streams

Voice Recognition

A person trying to authenticate provides a sample of their voice.

VPN Concentrator

A device that handles multiple VPN tunnels

Acts as a router for VPN connections, allowing multiple VPN connections into one network

Vulnerable Business Processes

When the processes that run a business are compromised or used to advantage the attacker

Consider a shipping company that relies on an automated process to determine delivery routes. An attacker could use this to alter delivery routes, causing a slowdown or facilitating the movement of illegal substances

Vulnerability Scanner

Software that aids in identifying hosts/host attributes and associated vulnerabilities

Scans a system by comparing its settings with a predefined set of known-vulnerable settings and software types

Vulnerability Scanning

Vulnerability scanning uses software to check for known vulnerabilities.

Generally uses passive techniques and does not exploit any vulnerabilities which are found in the scan

Vulnerability scanning would likely be part of a penetration test

Vulnerability Testing

Involves scanning systems/networks with automated tools to discover any configurations which match known vulnerability signatures. Vulnerability scans are non-intrusive and do not exploit vulnerabilities as they are found

W

Warm Site

A warm site lies somewhere between a hot site and a cold site in terms of operational readiness (as the name suggests)

Waterfall

Waterfall is a software development life cycle (SDLC) method in which development is done in distinct phases.

Watering Hole Attack

When an attacker targets websites that are popular with a specific person or group

The attacker can leverage the trust people have in this website to compromise the victim or vic-tim group

Web Application Firewall

A specific type of application firewall with the purpose of protecting Web servers by filtering traffic and blocking attacks using signatures and pattern-matching

Weak Cipher Suites

Using a cipher suite with known vulnerabilities or implementing a secure cipher incorrectly can cause encryption to become useless

Weak Implementation

When a victim configures things in such a way that makes a system insecure

For example: using a weak encryption key

Weak or Deprecated Algorithms

When an encryption algorithm has been broken or otherwise has known weaknesses (e.g., key length is too short), the algorithm is weak and its use will bring about a certain level of risk

Weak Security Configuration

A general term describing software or hardware misconfigurations that may result in a foothold for an attacker

Whaling

Spearphishing designed and conducted towards a high-value target, such as a CEO

White Box
A test conducted with full knowledge of how the system, network or target is designed or implemented

Whitelisting
allows you to specify the applications allowed to run on your operating system. All others will be blocked

Wi-Fi Connection
Mobile devices have similar challenges to any other devices that are on a wireless network
Challenges may include data encryption, evil twin or denial-of-service attacks
The biggest risks with using Wi-Fi are associated with connecting to insecure access points

Wi-Fi Direct and Ad Hoc
Mobile devices can often connect directly with each other (Wi-Fi Direct) or with a network of mobile devices, creating what is known as an “ad hoc” network
This type of connection has all the challenges of similar wireless protocols and offers another potential foothold for attackers

Wi-Fi MicroSD
The convenience of being able to transfer media from a device wirelessly is counter-balanced with security concerns

Wi-Fi Protected Setup (WPS)
A solution to make it easier to connect to a wireless access point
WPS uses an 8-digit PIN system to allow access
Because the last number in the PIN is actually a checksum value, it is easily brute-forcible with 10,000,000 possible PIN combinations

Wildcard
A wildcard certificate includes the “*” symbol and is valid for all subdomains up to one level away from the main domain

Wireless
Wireless technology can be used to connect clients to a network

Wireless Keyboards and Mice
Wireless keyboards and wireless mice send their input data wirelessly to the machine they are connected to

Wireless Scanners
Wireless scanners aid in identifying wireless networks and their type, also allowing for the capture of packets being sent across the network (sniffing)

Wireless Security Using Wi-Fi Protected Access (WPA and WPA2)
WPA was created to replace Wired Equivalent Privacy (WEP) when WEP was found to be insecure. WPA uses RC4 with the inclusion of Temporal Key Integrity Protocol (TKIP), which uses an encrypted hash with a sequence counter and a 48-bit IV to avoid the problems inherent in WEP. WPA2 is a stronger version of WPA, using AES in conjunction with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

Witnesses
Witnesses and involved parties should be interviewed to gather information on what each person was doing at the crime scene and what the function of the computer system in question is

Workstation
Functions as the typical PC, allowing users to access personal files and use the Internet

Worm
Malware that spreads from computer to computer with little or no interaction from a user.

WORM
Write Once, Read Many (WORM) media is another option for secure logging. Once data is written to WORM media, it cannot be rewritten, though data can be appended to that which was previously recorded

WPA-Enterprise
Allows users to authenticate to the network using their organizational credentials

X

Y

Z

Zero-Day
A vulnerability (in a software or system) that the creators or responsible parties are not aware of
If exploited by an attacker, no users will have had this vulnerability fixed. Thus, the attack will always succeed