CompTIA Security+ Acronym Guide

Exam Number: SY0-701

Chloe Stogsdill

All acronyms are sourced from the CompTIA Security+ Certification Exam Objectives
EXAM NUMBER: SY0-701

A

AAA

Authentication, Authorization, and Accounting

- Authenticating people
    - Authenticating is the process of verifying the identity of people before allowing them access to a system, ensuring they are who they claim to be. This authentication is commonly done using multiple methods of identification, known as a Multi-Factor Authentication (MFA).
- Authorization systems
    - Authorization is the process of verifying the identity of devices before allowing them into a network, ensuring they are trusted. An organization has a dedicated Certificate Authority that maintains digital certificates, signed by the CA, for each device used to authenticate a user.
- Accounting models
    - Accounting is the process of defining permissions and access levels of a user or device. An organization might have Role-Based Access Control, where access is based on the user's role within the organization, or Attribute-Based Access Control, where access is granted based on the attributes of a user such as time or location they are logging in.

ACL

Access Control List

- Define which systems and resources a user is allowed access to, along with the operations that are allowed on those resources.

AES

Advanced Encryption Standard

- A symmetric block cipher algorithm encrypting data in blocks of 128 bits with keys of 128, 192, or 256 bits. AES is widely used to protect sensitive information as it is considered secure against all known attacks.

AES-256

Advanced Encryption Standards 256-bit

- A symmetric block cipher algorithm that uses a 256-bit key to convert plain text into a cipher. It's considered the most secure encryption standard available and it is often used to protect top-secret information.

AH

Authentication Header

- Part of IPSec, the AH provides data authentication and integrity, along with protection from replay attacks. The AH protects the payload of the IP packet.

AI

Artificial Intelligence

- The ability of a computer to perform tasks historically requiring human intelligence, such as reasoning, decision making, and problem-solving.

AIS

Automated Indicator Sharing

- A service provided by the Cybersecurity and Infrastructure Security Agency that enables users to receive and share cyber threat indicators and defensive measures in real time.

ALE

Annualized Loss Expectancy

- An estimate of the yearly financial impact of a risk. It is calculated by multiplying the SLE by the ARO.

AP

Access Point

- A device allowing wireless devices to connect to a wired network, such as the internet, and acts as a central point for communications.

API

Application Programming Interface

- Enables different software components or systems to communicate and interact with each other using a set of definitions and protocols.

APT

Advanced Persistent Threat

- A cyber attack involving gaining unauthorized access to a network and remaining undetected for a long period of time.

ARO

Annualized Rate of Occurrence

- The expected frequency of a risk event occurring within a year. It helps quantify how often a specific risk is likely to happen annually.

ARP

Address Resolution Protocol

- A communication protocol that links IP addresses to MAC addresses on a LAN.

ASLR

Address Space Layout Randomization

- A computer security technique that randomizes the memory addresses where system executables are loaded, effectively guarding against buffer overflow attacks.

ATT&CK

Adversarial Tactics, Techniques, and Common Knowledge

- A knowledge hub of known cyberattack tactics and techniques based on real-world observation, presented in a tabular framework.

AUP

Acceptable Use Policy

- Defines acceptable and unacceptable behaviors when using organizational resources. It aims to protect both the organization and its employees by outlining rules and expectations.

AV

Antivirus

- A software that is designed to detect, prevent, and remove malware using signature-based detection to identify and mitigate threats

B

BASH

Bourne Again SHell

- The command line and shell program for most Linux server computing environments. It is used for system administration and task automation.

BCP

Business Continuity Planning

- A strategy and set of systems to help businesses prevent and rapidly recover from cyber attacks and other threats.

BGP

Border Gateway Protocol

- A set of rules to help determine the best network route for data across the internet. It is the language of routers that finds the best pathway to transmit packets from one to the other.

BIA

Business Impact Analysis

- Evaluates the potential effects of disruptions to critical business operations, prioritizing recovery efforts and resources based on the impact of different scenarios

BIOS

Basic Input/Output System

- Low level software that is run when booting up a system. The BIOS tests the hardware components and then starts and runs the main OS.

BPA

Business Partners Agreement

- Outlines the terms and conditions of a partnership between businesses. It includes details about roles, responsibilities, revenue sharing, and conflict resolution mechanisms.

BPDU

Bridge Protocol Data Unit

- This is a data message that is transmitted across a LANs across spanning tree network configurations to detect loops.

BYOD

Bring Your Own Device

- A policy where employees use their own mobile devices for work, requiring more detailed MDM policies to secure, such as acceptable use policy (AUP) and on/offboarding policies.

C

CA

Certificate Authority

- Trusted entities that create, issue, and verify digital certificates.

CAPTCHA

Completely Automated Public Turing Test to Tell Computers and Humans Apart

- A program written to distinguish human input from machine input in order to deter bot attacks and spam.

CAR

Corrective Action Report

- An official document written when an element of a plan is not implemented or executed correctly, typically used in quality management.

CASB

Cloud Access Security Broker

- These solutions sit between users and cloud platforms and serve as a central enforcement point from which organizations can manage a range of security policies.

CBC

Cipher Block Chaining

- A block mode of DES that XORs the previous encrypted block of ciphertext to the next block of plaintext to be encrypted, creating a chain of encrypted blocks of data.

CCMP

Countermode/CBC-MAC Protocol

- “Counter Mode Cipher Block Chaining Message Authentication Code Protocol” is an encryption protocol designed for Wireless LAN based upon the standards of the IEEE and the CCM mode of the AES. It was created to address the vulnerabilities presented by WEP.

CCTV

Closed-Circuit TeleVision

- A system that uses cameras to transmit a signal to a limited number of monitors, primarily for surveillance and security.

CERT

Computer Emergency Response Team

- An expert group responsible for containing computer security incidents, minimizing their impact on the organization's operations and reputation, and facilitating post-crisis remediation and reconstruction.

CFB

Cipher FeedBack

- A block of cipher from the previous encrypted block is given to the next block to influence output of the next cipher.

CHAP

Challenge Handshake Authentication Protocol

- CHAP is an authentication scheme that was originally utilized by PPP servers to validate the identity of remote clients. CHAP verifies the identity of the client by using a three-way handshake during the establishment of the link. The verification is based on a shared secret, such as the client's password, where both the client and the server must possess each other's credentials, which includes their shared secret, and the server will proceed to authenticate the client if the client's response aligns with the server's expectations.

CIA

Confidentiality, Integrity, Availability

- The CIA triad is a foundational concept in cybersecurity
    - Confidentiality makes sure sensitive information is securely stored and accessible only to those who are authorized to view it. You are the only person that should have access to your information.
    - Integrity makes sure that data remains unaltered and trustworthy. When you send a message, you want it to remain unedited or modified, and any modification to be identified.

- Availability makes sure information and resources are available to users when requested. If you need to access your data, you want the system that accesses it to be operating.

CIO

Chief Information Officer

- A high-ranking executive who manages a company's information and computer technology systems in order to support enterprise goals.

CIRT

Computer Incident Response Team

- A group of experts that respond to a cyber incident so that a company can recover and protect itself from other similar incidents.

CMS

Content Management System

- An application that allows businesses to create and manage websites and other digital content without having to code, such as Squarespace or Wix.

COOP

Continuity Of Operation Planning

- The processes and procedures an organization puts in place to ensure operations can continue during and after a failure or disruption, such as backups

COPE

Corporate Owned, Personally Enabled

- A policy where the employer provides devices for employees to use for both work and personal activities. Organizations have more control over the device, as IT can control security, wipes, and applications.

CP

Contingency Planning

- A risk management document that provides instructions for a company to recover data and services in the event of a disaster.

CRC

Cyclical Redundancy Check

- A method to detect errors in a network transmission through the performance of a binary solution derived from the checksum error detection algorithm.

CRL

Certificate Revocation List

- Lists, maintained by CAs, that store information on the revocation or invalidation status of digital certificates, allowing systems to check if a certificate is no longer valid.

CSO

Chief Security Officer

- A senior executive officer in charge of information security and securing systems and data. Responsibilities include cybersecurity, physical security, risk management and incident response

CSP

Cloud Service Provider

- A third-party organization that offers cloud-based computing platforms, infrastructure, and services to customers.

CSR

Certificate Signing Request

- A request generated to obtain a digital certificate by a CA. The CSR will include the entity's public key and relevant information, allowing the certificate authority to issue a signed certificate.

CSRF

Cross-Site Request Forgery

- These attacks occur when users are tricked into performing malicious actions on a website they are logged into, exploiting the trust the browser has for users.

CSU

Channel Service Unit

- A digital interface device that connects data terminal equipment to digital circuits. In essence, it acts as the bridge between a LAN to a WAN.

CTM

CounTer Mode

- An AES counter-based block cipher encryption mode.

CTO

Chief Technology Officer

- A senior executive responsible for managing the technical needs and operations of an organization, along with research and development.

CVE

Common Vulnerability Enumeration

- A standardized list of publicly known security vulnerabilities where each entry includes an ID, description, and relevant patches.

CVSS

Common Vulnerability Scoring System

- A standardized framework for rating the severity of security vulnerabilities from 0 to 10.

CYOD

Choose Your Own Device

- A policy where employees choose from a select few pre-approved devices that employees can buy and bring to work, allowing IT to manage fewer devices while still offering options.

D

DAC

Discretionary Access Control

- A model that gives the owner of a resource full control over who can access the resource and what permissions they have.

DBA

Database Administrator

- Professionals responsible for managing and maintaining a database to ensure it runs efficiently and securely.

DDoS

Distributed Denial of Service

- DDoS attacks involve compromising multiple computer systems to disrupt services. Reflected DDoS occurs when the attacker reflects their requests off of a third party with a spoofed IP address, so the response goes to the IP of the system the attacker is targeting. Amplified DDoS uses reflection to turn a small request, such as a DNS request, into a much larger amount of data, reflected onto the target system.

DEP

Data Execution Prevention

- A security feature built into Windows that helps protect against executable code running in unauthorized areas of memory by marking certain areas as “data only.”

DES

Digital Encryption Standard

- A block cipher that encrypts data in 64-bit blocks. Its short key length makes it too insecure for modern applications.

DHCP

Dynamic Host Configuration Protocol

- A network protocol that automatically assigns IP addresses and configuration information to devices when they connect to the network using a client-server architecture.

DHE

Diffie-Hellman Ephemeral

- A method for securely exchanging keys across a network through using temporary, public keys for each individual usage of the protocol.

DKIM

Domain Keys Identified Mail

- An email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain. It is designed to detect forged sender addresses in email, a technique often used in phishing and email spam. In essence, DKIM allows the receiver to check that an email that claimed to have come from a specific domain was authorized by the owner of that domain by matching the digital signature the email is signed with to the domain name the email was sent using.

DLL

Dynamic Link Library

- A shared library containing code, data, and resources that can be used by multiple programs at the same time.

DLP

Data Loss Prevention

- Helps protect sensitive information from leaving an organization by identifying and monitoring sensitive data and blocking, encrypting, or alerting administrators of intentional or unintentional transmission.

DMARC

Domain Message Authentication Reporting and Conformance

- Controls how your domain handles emails that fail SPF or DKIM checks, providing instructions to email servers on how to deal with unauthenticated emails. DMARC uses a TXT file stored in your DNS with a tag called ‘p’. Setting p=none alerts the inbox provider to take no action, p=quarantine alerts the provider to move the email to the spam folder, and setting p=reject alerts the provider to block the message entirely.

DNAT

Destination Network Address Translation

- A method used to map the destination address of a packet to another IP, such as when a public destination IP is translated into a private IP.

DNS

Domain Name System

- A system translates human-readable domain names into corresponding IP addresses

DoS

Denial of Service

- A cyber attack that attempts to deny users the service of a specific system or network resource through overwhelming the service with traffic.

DPO

Data Privacy Officer

- An expert officer whose primary role is to ensure the company follows all data related rules and policies when processing sensitive data.

DRP

Disaster Recovery Plan

- These plans focus on restoring IT systems and data after a catastrophic event, including plans for data backups, system restoration, and recovery procedures to resume operations.

DSA

Digital Signature Algorithm

- A FIPS algorithm for digital signatures that provides message authentication, non-repudiation, and integrity verification through the use of public and private keys.

DSL

Digital Subscriber Line

- A broadband internet connection that uses telephone lines to send and receive data.

E

EAP

Extensible Authentication Protocol

- EAP is an authentication framework that allows newer authentication technologies to be compatible with older point-to-point authentication.

ECB

Electronic Code Book

- A block cipher algorithm that uses a symmetric key to encrypt and decrypt data. It was the original mode for DES, but is now considered extremely weak and simple.

ECC

Elliptic Curve Cryptography

- A type of public-key cryptography that uses elliptic curves creates private keys, which are nearly impossible to crack as the math involved is extremely difficult to reverse. It provides fast encryption speeds along with comparable security to RSA.

ECDHE

Elliptic Curve Diffie-Hellman Ephemeral

- A key exchange method that uses two sets of elliptic curve key pairs to allow two parties to create a shared secret over an insecure channel.

ECDSA

Elliptic Curve Digital Signature Algorithm

- A cryptographic algorithm that uses ECC to create digital signatures.

EDR

Endpoint Detection and Response

- EDR is an advanced threat detection and response tool that protects endpoints from suspicious activities and has real-time threat detection. It has automated response capabilities such as isolating infected endpoints, blocking malicious activities, and remediating threats.

EFS

Encrypted File System

- Protects data at rest through the use of FDE built into the OS of Windows devices.

ERP

Enterprise Resource Planning

- A software system that allows companies to manage all essential processes in a single place, allowing for the management of a variety of components in one integrated system.

ESN

Electronic Serial Number

- A unique ID number that is embedded into mobile devices during manufacturing to identify them on a network.

ESP

Encapsulated Security Payload

- A protocol that encrypts and authenticated data packets sent over the network to allow for secure, protected communication with a VPN.

F

FACL

File System Access Control List

- A table that informs an OS system which users have access to which system privileges.

FDE

Full Disk Encryption

- Encrypts an entire storage device at the disk level and makes sure if the device is stolen the data on it remains confidential.

FIM

File Integrity Management

- Tracks changes to files to ensure that unauthorized modifications do not occur, alerting administrators to any unauthorized changes that could indicate a security breach or malicious activity.

FPGA

Field Programmable Gate Array

- An extremely versatile integrated circuit that is designed to be programmable to suit different purposes, from acting as a logic gate to executing more complex operations.

FRR

False Rejection Rate

- A measure of how often a system fails to accept authorized users.

FTP

File Transfer Protocol

- A standard network protocol used for transferring files from one host to another.

FTPS

Secured File Transfer Protocol

- Adds TLS/SSL encryption to the FTP, increasing security.

G

GCM

Galois Counter Mode

- A mode for symmetric-key block ciphers that uses hashing over a binary Galois field to provide encryption in a highly efficient and low-cost manner.

GDPR

General Data Protection Regulation

- An EU law that protects personal data that is collected and processed by companies.

GPG

Gnu Privacy Guard

- A free and open-source software that allows users to encrypt and digitally sign their communications using the command line.

GPO

Group Policy Object

- Provides a policy-based, centralized control of Windows devices, allowing for remote control over all computers' user permissions, security settings, password policies, and software installations.

GPS

Global Positioning System

- A satellite-based positioning, navigation, and timing system.

GPU

Graphics Processing Unit

- A circuit designed initially to accelerate the process of digital images that has progressed on to be used for graphics, video rendering, and AI.

GRE

Generic Routing Encapsulation

- A protocol that encapsulates one packet inside of another packet, allowing for the simplification of connections.

H

HA

High Availability

- High availability systems are systems designed to provide continuous operation and minimal downtime, even in the event of a failure or during maintenance.

HDD

Hard Disk Drive

- A “non-volatile” data storage device.

HIDS

Host-based Intrusion Detection System

- A security system installed on a host that monitors and analyzes the system's behavior to detect malicious activities.

HIPS

Host-based Intrusion Prevention System

- A security system installed on a host that monitors and analyzes the system's behavior to detect and prevent malicious activities. By identifying and blocking suspicious actions in real-time, HIPS protects the host from various threats.

HMAC

Hashed Message Authentication Code

- A hash-based cryptographic technique used for authentication. Each message, using HMAC, is sent with an HMAC hash, which both parties in a communication can use to validate and verify authenticity through the use of shared keys.

HOTP

HMAC-based One-Time Password

- A one time password that uses HMAC to generate a unique code to authenticate users.

HSM

Hardware Security Module

- A dedicated hardware device designed to generate, store, and manage cryptographic keys securely in large environments.

HTML

HyperText Markup Language

- The standard markup language for creating web pages and web applications, defining the structure and presentation of web content.

HTTP

HyperText Transfer Protocol

- Defines how data should be formatted and transmitted between a client and a web server.

HTTPS

HyperText Transfer Protocol Secure

- A more secure version of HTTP that uses TLS/SSL encryption.

HVAC

Heating, Ventilation Air Conditioning

- A physical device that regulates air flow and temperature.

I

IaaS

Infrastructure as a Service

- A cloud computing service model that provides virtualized computing resources over the internet allowing for high levels of control over OS, storage, and deployed applications

IaC

Infrastructure as Code

- Manages and creates infrastructure through coded scripts rather than physical hardware configuration or configuration tools. IaC automates infrastructure setups and makes scaling and consistency easier to maintain.

IAM

Identity and Access Management

- A framework for managing and controlling access to resources and information.

ICMP

Internet Control Message Protocol

- A protocol devices use to communicate errors in data transmissions.

ICS

Industrial Control Systems

- Physical and digital systems that control industrial processes.

IDEA

International Data Encryption Algorithm

- A symmetric block-cipher, intended as a replacement for DES, that encrypts data using a 128 bit key.

IDF

Intermediate Distribution Frame

- A physical frame that acts as a secondary distribution point for a company's wiring. It is connected to a MDF (that controls all of the wires), allowing for simplified and distributed wire management.

IdP

Identity Provider

- Stores, manages, and verifies user identities.

IDS

Intrusion Detection System

- IDS monitors network traffic for malicious or suspicious activities passively, alerting administrators in the event of a potential security incident.

IEEE

Institute of Electrical and Electronics Engineers

- A non-profit organization of professionals that aims to advance technology for the benefit of humanity.

IKE

Internet Key Exchange

- A key management protocol used to set up secure and authenticated communications, ensuring both parties use secure encryption and authentication methods.

IM

Instant Messaging

- A form of real-time messaging hosted by a dedicated service.

IMAP

Internet Message Access Protocol

- Allows users to access their email from multiple devices.

IoC

Indicators of Compromise

- Evidence that an attacker may have attempted to breach or exploit a system.

IoT

Internet of Things

- The class of devices that connect to the internet and exchange data with systems and devices.

IP

Internet Protocol

- Delivers packets from the source host to the destination host based on their IP addresses.

IPS

Intrusion Prevention System

- IPS builds on IDS by actively rejecting the malicious packets.

IPSec

Internet Protocol Security

- A suite of protocols used to secure IP communications. It includes an authentication header (AH) and encapsulating security payloads (ESP) protocols. AH is used to provide authentication and ESP provides confidentiality and integrity through encryption. IPSec has two modes: transport mode and tunnel mode.

IR

Incident Response

- A structured and standardized approach for handling security incidents.

IRC

Internet Relay Chat

- A text-based system for IMing, created for real-time group discussions in rooms called “channels.”

IRP

Incident Response Plan

- A set of instructions to follow in the event of a security incident for companies to detect, respond, and recover.

ISO

International Standards Organization

- A nongovernmental organization that sets proprietary, industrial, and commercial standards.

ISP

Internet Service Provider

- A company that provides customers with internet access.

ISSO

Information Systems Security Officer

- A senior role, responsible for maintaining the appropriate security posture of an organization.

IV

Initialization Vector

- A random value inputted into a cryptographic algorithm to provide the initial state.

K

KDC

Key Distribution Center

- An access control component responsible for providing keys to users.

KEK

Key Encryption Key

- A key used to encrypt another key.

L

L2TP

Layer 2 Tunneling Protocol

- A VPN protocol that aids in the secure transmission of data through creating a direct tunnel for layer 2 traffic.

LAN

Local Area Network

- A network of devices located in a particular area sharing an internet connection.

LDAP

Lightweight Directory Access Protocol

- Used to access and manage directory information over an IP network. LDAP provides a centralized repository for user credentials and access rights. For example, a user might log in to an application using their ID and password. The software sends this information to a security server, which logs into the LDAP server on the user's behalf with their ID and password. If successful, the security server can authorize the user and allow them to access the application.

LEAP

Lightweight Extensible Authentication Protocol

- Also known as lightweight EAP, LEAP is the Cisco alternative to TKIP before 801.2X and WPA became the standard.

M

MaaS

Monitoring as a Service

- A cloud computing service model that provides monitoring functionalities for systems and applications on the cloud.

MAC

Mandatory Access Control

- A model where access rights are strictly regulated by a central authority based on levels of security. Users and resources are assigned classifications, such as “confidential,” and access rights are based on these classifications.

MAC

Media Access Control

- A protocol used to identify devices on a network, determine how devices can access the network, and control how data is transmitted through a network cable.

MAC

Message Authentication Code

- A short token of information used to check the authenticity and integrity of a message using keys.

MAN

Metropolitan Area Network

- A computer network that connects computers in a metropolitan area, such as a city. It is larger than a LAN but smaller than a WAN.

MBR

Master Boot Record

- A program that loads a device’s OS at startup.

MD5

Message Digest 5

- One of the first popular hashing algorithms, considered secure when it was developed. Now easily decoded and unsafe for use.

MDF

Main Distribution Frame

- A centralized hub of all of the wires in a building, used as the main point of infrastructure management.

MDM

Mobile Device Management

- A software solution that solves how organizations can securely manage and monitor mobile devices using passwords, geofencing, app and content management, remote wipe, screen lock, geolocation, and push notifications.

MFA

Multi Factor Authentication

- A security mechanism that requires users to provide two or more forms of identification before accessing a system or application.

MFD

MultiFunction Device

- A device that combines the functionalities of multiple devices into one, singular machine.

MFP

MultiFunction Printer

- A printer that combines multiple functionalities, such as scanning, copying, and faxing.

ML

Machine Learning

- The development of computer systems that are capable of learning and adapting given patterns of data.

MMS

Multimedia Message Service

- A way to send and receive multiple forms of media, such as videos, photos, and files, through text messaging.

MOA

Memorandum of Agreement

- A formally agreed upon document that outlines the terms of an agreement between two or more parties. It specifies the responsibilities, objectives, and commitments of each party involved.

MOU

Memorandum of Understanding

- A non-binding agreement that expresses the intention of two parties to cooperate. It outlines the general terms and conditions of a partnership and serves as a preliminary understanding between groups before a formal contract is established.

MPLS

Multi-Protocol Label Switching

- A routing technique that uses labels instead of network addresses to more efficiently transmit data packets in a WAN.

MSA

Master Service Agreement

- A detailed contract that establishes the general terms and conditions for future transactions between parties, simplifying future agreements by providing a foundational framework for continuing services.

MSCHAP

Microsoft Challenge Handshake Authentication Protocol

- An EAP method for CHAP that is used as an authentication option in Microsoft's implementation of the PPTP protocol for VPNs.

MSP

Managed Service Provider

- Third parties you rely on to manage your service and inform you of any updates or changes you need to make.

MSSP

Managed Security Service Provider

- A third party that manages and monitors devices and systems, offering security services to an organization.

MTBF

Mean Time Between Failures

- The average time between successive failures of a system or component. It provides an indication of the reliability and expected lifespan of the system or component.

MTTF

Mean Time To Failure

- The average amount of time a non-repairable system or component can go until failure.

MTTR

Mean Time To Recover/Repair

- The average time required to repair a system or component and restore it to full functionality. It measures the efficiency and effectiveness of the repair process.

MTU

Maximum Transmission Unit

- The size of the largest data packet, in bytes, that a device can accept.

N

NAC

Network Access Control

- Ensures only authorized and compliant devices have access to a network through authenticating, authorizing, and assessing the security posture of devices before granting network access. NAC allows for network segmentation and access controls based on user roles, device types, and security status.

NAT

Network Address Translation

- A way to map private IPs in a LAN to a public IP before transmission.

NDA

Non-Disclosure Agreement

- A legal contract that protects confidential information that is shared between parties. It ensures that sensitive information is not disclosed to unauthorized individuals.

NFC

Near Field Communication

- A short range wireless technology that enables two devices to communicate when they are located near each other. NFC is a subset of RFID and less powerful than Bluetooth.

NGFW

Next-Generation FireWall

- Advanced firewalls that combine traditional firewalls with WAFs. They offer deep packet inspection with the ability to process traffic from Layers 3, 4, and 7 and use that information to take action before traffic reaches the application.

NIDS

Network-based Intrusion Detection System

- Monitors the network for malicious or suspicious activities passively, alerting administrators in the event of a potential security incident on the network.

NIPS

Network-based Intrusion Prevention System

- Monitors the network for malicious or suspicious activities, actively preventing and denying packets in the event of a potential security incident on the network.

NIST

National Institute of Standards & Technology

- A U.S. agency dedicated to advancing American innovation.

NTFS

New Technology File System

- The system Windows devices use for storing and managing files on a hard disk.

NTLM

New Technology LAN Manager

- A set of Microsoft security measures used to authenticate users as a SSO tool. It relies on CHAP to confirm users without requiring passwords.

NTP

Network Time Protocol

- A protocol used to synchronize computer clocks with time sources in a network.

O

OAUTH

Open AUTHorization

- Allows a website or application to access resources hosted by other web apps on behalf of a user. OAuth is commonly used in SSO scenarios to grant access to user data across different applications without sharing passwords. For example, a web service might ask permission to add or modify files in your Google Drive account.

OCSP

Online Certificate Status Protocol

- Used to check the status of a digital certificate, allowing systems to verify a certificate's validity in real-time.

OID

Object Identifier

- A group of characters that uniquely identifies an object

OS

Operating System

- The software that manages hardware, memory, and processes that run on a computer.

OSINT

Open-Source INTelligence

- Publicly available sources of information such as security blogs, social media, and government advisories, to identify potential threats and vulnerabilities.

OSPF

Open Shortest Path First

- A routing protocol that uses a mathematical algorithm to calculate the shortest path from one place in an IP network to another.

OT

Operational Technology

- Hardware and software that directly monitor and control physical processes or devices, such as an ICS or SCADA.

OTA

Over the Air

- A method of distributing software updates or other data “through the air,” or, through wireless communication channels.

OVAL

Open Vulnerability Assessment Language

- A standardized way to report on the condition of computer systems.

P

P12

PKCS #12

- A binary format for storing file that contains both a private key and a X.509 certificate.

P2P

Peer to Peer

- A network in which computers on the network are equally privileged and the workload is evenly distributed.

PaaS

Platform as a Service

- A cloud computing service model that provides hardware and software tools, creating a platform to develop and manage applications without dealing with underlying infrastructure. Caveat is less control over hardware and OS; but more focus is on the development and deployment of applications.

PAC

Proxy Auto Configuration

- A file that defines whether browser requests go directly to their intended location or if they are routed to a proxy server.

PAM

Privileged Access Management

- Strategies and tools that control and monitor privileged accounts to prevent unauthorized access or compromise.

PAM

Pluggable Authentication Modules

- A framework that allows for the incorporation of many authentication mechanisms into one system using plug-ins.

PAP

Password Authentication Protocol

- A PPP authentication method that uses passwords and a two-way handshake to verify users. It is an extremely popular and widely supported form of authentication; however, PAP is sent in cleartext and can be considered vulnerable on its own as no encryption is used.

PAT

Port Address Translation

- A NAT method that translates a computer's private IPv4 address into a single public address. It gives each computer request a unique port number to communicate through as to differentiate between different computers on a private network communicating using the same public IP.

PBKDF2

Password-Based Key Derivation Function 2

- Adds salt and, occasionally, an HMAC to a password and hashes it repeatedly to produce a derived key that can be used for additional operations. It is a form of key stretching and makes password cracking more difficult.

PBX

Private Branch eXchange

- An internal telephone network for a company that allows for a single phone line to be split into several lines identifiable by extensions.

PCAP

Packet CAPture

- A duplicate copy of a packet that has been transmitted through a network, typically stored and viewed in a packet analyzer program.

PCI DSS

Payment Card Industry Data Security Standard

- The security standard for the storage, transmission, and processing of a credit or debit card to ensure security and user protection.

PDU

Power Distribution Unit

- A device that controls and protects the distribution of power in an industrial setting, such as a data center.

PEAP

Protected Extensible Authentication Protocol

- Also known as protected EAP, encompasses EAP in a TLS tunnel, providing authentication and encrypted/protected data transfers.

PED

Personal Electronic Device

- A small and easily transferable device, such as a smartphone or laptop.

PEM

Privacy Enhanced Mail

- An email security standard that enables email over the internet using digital signatures and encryption.

PFS

Perfect Forward Secrecy

- A way of encrypting where keys used to encrypt and decrypt messages are frequently and automatically changed so that if a key is hacked, only a small portion of messages are decryptable.

PGP

Pretty Good Privacy

- An extremely popular encryption system used to provide an extra layer of email security through encryption using public-key cryptography and symmetric keys.

PHI

Personal Health Information

- Any information in a medical context that can be used to identify an individual and relates to their health.

PII

Personally Identifiable Information

- Any data that can be used to identify a specific individual.

PIV

Personal Identity Verification

- A framework for identity management that can be used for MFA that uses personal information such as a photo, fingerprints, and cryptographic keys, commonly encapsulated in smart cards, to provide identity proofing.

PKCS

Public Key Cryptography Standards

- A set of standards that define how to use PKI to securely exchange information including the hardware, software, procedures, and roles involved.

PKI

Public Key Infrastructure

- A security framework that uses encryption and authentication to communicate over the network using public and private keys. PKI is used to create, store, and manage keys and digital certificates.

POP

Post Office Protocol

- A protocol that allows users to request new messages from the email server.

POTS

Plain Old Telephone Service

- An analog-based phone line that creates a dedicated circuit between two phones (which are attached to the phone line via wire, unlike VoIP which is wireless) allowing for a call.

PPP

Point-to-Point Protocol

- An OSI layer 2 protocol that links two devices directly, typically used to access the internet or connect to remote networks with a WAN.

PPTP

Point-to-Point Tunneling Protocol

- A method used for implementing VPNs that allows for private transference of data by encapsulating packets at the TCP/IP level. It is now considered obsolete.

PSK

Pre-Shared Key

- A shared secret that had been previously established by two parties in a separate communication.

PTZ

Pan-Tilt-Zoom

- Robotic cameras with the capability to pan, tilt, and zoom.

PUP

Potentially Unwanted Program

- Any software that may cause unwanted behavior on a device, often bundled with wanted software or downloaded unintentionally.

R

RA

Recovery Agent

- A person or entity, typically with a “master key,” permitted to decrypt other users’ data in the event of an emergency

RA

Registration Authority

- An entity authorized by a CA to verify and submit information on a user’s behalf to be entered, or registered, into public key certificates.

RACE

Research and development in Advanced Communications technologies in Europe

- A program launched to promote the advancement of communication technology throughout Europe.

RAD

Rapid Application Development

- A development methodology that emphasizes speed and frequent iterations over planning in application development.

RADIUS

Remote Authentication Dial-In User Service

- A network protocol designed to provide AAA. RADIUS is often used to authenticate users connecting to Wi-Fi networks. User’s usernames and passwords are sent to a RADIUS server to be authenticated during log-in. This is often the back-end of the 802.1X authentication.

RAID

Redundant Array of Inexpensive Disks

- A technique that uses multiple physical disks to store data, creating data redundancy and increased performance.

RAS

Remote Access Server

- A server that provides services to remotely connected users, acting as a gateway into a company's internal LAN.

RAT

Remote Access Trojan

- Malware that allows attackers to gain full administrative control and remotely operate a computer.

RBAC

Role-Based Access Control

- A model that assigns permissions to users based on their role within an organization.

RBAC

Rule-Based Access Control

- A model that uses specific organization or administrator rules to determine access permissions. These rules can be based on various conditions such as time of day, location, or type of resource.

RC4

Rivest Cipher version 4

- A symmetric key stream cipher that encrypts messages one byte at a time.

RDP

Remote Desktop Protocol

- A protocol that allows users to use a desktop computer remotely.

RFID

Radio Frequency IDentifier

- A technology that uses radio waves for identification by transmitting and receiving data stored on RFID tags.

RIPEMD

RACE Integrity Primitives Evaluation Message Digest

- A family of hash functions developed in 1992 that produce a fixed sized output.

ROI

Return On Investment

- A measure to determine the profitability of an investment: ROI = (profit - cost) / cost, ROI = net income / cost of investment * 100, or ROI = investment gain / investment base.

RPO

Recovery Point Objective

- The maximum acceptable amount of data loss measured in time. It defines the point in time to which data must be recovered to resume operations, indicating the tolerance for data loss.

RSA

Rivest, Shamir, & Adleman

- Uses the factorization of the product of two prime numbers to deliver encryption of 1024-bits and up to 2048-bit key length. The length of keys make encryption and decryption incredibly slow, but the level of security is extremely high.

RTBH

Remotely Triggered Black Hole

- A filtering technique that allows packets to be blocked at the edge of a network, routing to a null IP which creates a “black hole” for the packet to be discarded at.

RTO

Recovery Time Objective

- The maximum acceptable amount of time to restore a business function or system after a disruption. It defines the target timeframe for resuming normal operations to minimize impact.

RTOS

Real-Time Operating System

- An operating system used for applications that require high reliability and precise timing, like embedded systems in medical devices and industrial automation, where delays can lead to failures or unsafe conditions. These systems are typically self-contained and difficult to access, as installing firewalls and anti-malware is difficult and could result in non-immediate responses or delays.

RTP

Real-Time Transport Protocol

- A network protocol that transmits real-time data, like audio and video, used to enable VoIP.

S

S/MIME

Secure/Multipurpose Internet Mail Extensions

- The most commonly used protocol for sending digitally signed and encrypted emails.

SaaS

Software as a Service

- A cloud computing service model that provides subscription software applications accessed through a web browser, eliminating installation and maintenance. However, there is minimal control; users do not manage underlying infrastructure or platform.

SAE

Simultaneous Authentication of Equals

- Allows for the mutual authentication of devices as part of a handshake process using cryptographic tools to prevent brute force attacks. Authentication hashes a key unique to each authentication, rather than having the same key every time.

SAML

Security Assertions Markup Language

- Allows users to log into multiple applications with one set of credentials through authenticating a user once and then communicating that authentication to multiple applications. It is generally used as an authentication protocol for exchanging authentication and authorization between directories and web applications.

SAN

Storage Area Network

- A network of storage devices providing a shared space for storage that can be accessed by outside servers and computers.

SAN

Subject Alternative Name

- An extension of the X.509 certificate that specifies all of the IPs and domain names that are secured by that certificate.

SASE

Secure Access Service Edge

- Combines networking, WAN, and security, delivering them as a unified cloud service using cloud architecture. It integrates SD-WAN with security functions like secure web gateways, cloud access security brokers, firewall-as-a-service, and zero-trust network access. SASE can automatically connect remote and hybrid users to nearby cloud gateways instead of routing traffic to corporate data centers.

SCADA

Supervisory Control And Data Acquisition

- A system designed to closely monitor, control, and collect data on industrial operations, providing efficient, safe, and reliable operation of critical infrastructure like power plants.

SCAP

Security Content Automation Protocol

- A suite of standards used to automate vulnerability management, security measurement, and compliance evaluation to assess, measure, and report the security posture of systems.

SCEP

Simple Certificate Enrollment Protocol

- A protocol that allows devices to request digital certificates directly from a CA.

SD-WAN

Software-Defined Wide Area Network

- Enables users in remote offices to securely and remotely connect to an organization's network, allowing the usage of many network services, such as LTE, MPLS, and broadband. It uses IPSec, VPNs, and NGFWs to provide secure connections.

SDK

Software Development Kit

- A set of tools to help software developers develop applications, such as APIs or frameworks.

SDLC

Software Development Lifecycle

- A plan for how to continuously develop, test, and maintain a software system.

SDLM

Software Development Lifecycle Methodology

- A process that breaks down software development into a series of repeatable and cycling steps.

SDN

Software-Defined Networking

- A network management approach that directs traffic based on a data, control, and management plane to control networks centrally. The data plane manages forwarding data, processing network packets, and encryption. The control plane manages what actions occur in the data plane such as routing tables and session tables. The management plane manages the configuration of devices, such as the browser and ssh.

SELinux

Security-Enhanced Linux

- For Linux environments, SELinux enforces mandatory access controls (MAC), and can confines user programs and system services to the minimum required privileges.

SED

Self-Encrypting Drives

- An HDD or SSD that is designed to automatically encrypt stored data.

SEH

Structured Exception Handler

- A programming construct that handles errors during execution, separating and handling exceptions outside of the running program.

SFTP

Secured File Transfer Protocol

- An extension of SSH that is fully encrypted and secure.

SHA

Secure Hashing Algorithm

- A family of hash functions. SHA-256 is now the most commonly used hashing algorithm, resulting in a 256-bit hash value from an input message of any length.

SHTTP

Secure HyperText Transfer Protocol

- An extension of HTTP that uses symmetric encryption to provide stronger security.

SIEM

Security Information and Event Management

- These systems collect, aggregate, and analyze log data from various sources within an organization, providing real-time monitoring and alerts on suspicious activities.

SIM

Subscriber Identity Module

- A small smart card that stores ID information for mobile devices.

SLA

Service-Level Agreement

- A contract that specifies the expected level and quality of service that is to be provided between a vendor and a client. It outlines metrics for performance, response times, uptime, and the penalties for failing to meet these standards.

SLE

Single Loss Expectancy

- A calculation of the expected monetary loss each time a risk event occurs. It is determined by multiplying the asset value by the exposure factor (percentage of loss).

SMS

Short Message Service

- A cellular network service that allows users to send short text messages on mobile devices.

SMTP

Simple Mail Transfer Protocol

- The standard protocol for sending email messages across a network.

SMTPS

Simple Mail Transfer Protocol Secure

- Expands the security of SMTP by using TLS/SSL.

SNMP

Simple Network Management Protocol

- Manages and monitors network-connected devices in Internet Protocol networks.

SOAP

Simple Object Access Protocol

- A protocol used to create web APIs using XML to exchange information in a decentralized and distributed application.

SOAR

Security Orchestration, Automation, Response

- A group of tools that allows an organization to immediately respond to security incidents through the streamlining of repetitive tasks and the automation of alert systems.

SoC

System on Chip

- A circuit that combines all or most of a system's components onto a single chip.

SOC

Security Operations Center

- A team of security professionals, either in-house or outsourced, that is responsible for managing the IT infrastructure of a company.

SOW

Statement Of Work

- A detailed document that defines specific tasks, deliverables, timelines, and costs for a particular project or service and operates under the terms of a MSA or other agreement.

SPF

Sender Policy Framework

- An email authentication protocol that helps verify the sender of an email and helps to identify the mail servers that are allowed to send email for a given domain. By using SPF, ISPs can identify email from spoofers, scammers and phishers as they try to send malicious email from a domain that belongs to a company or brand. In essence, SPF allows the receiver to check that an email was not sent using a forged sender address by ensuring the IP address the email was sent from is authorized by the domain owner.

SPIM

SPam over Internet Messaging

- Unsolicited messages sent in bulk over the internet to many recipients using an IM service.

SQL

Structured Query Language

- A standardized programming language used for managing databases, allowing users to perform tasks such as querying, updating, and managing data.

SQLi

SQL Injection

- A web-based vulnerability that occurs when an attacker enters malicious SQL statements into an input field lacking input validation, allowing the attacker access to the underlying database.

SRTP

Secure Real-Time Protocol

- An extension of the RTP that adds encryption, authentication, and replay protection.

SSD

Solid State Drive

- A persistent storage device with no moving parts. It uses flash-based memory, making it faster than traditional HDDs.

SSH

Secure SHell

- Allows users to securely access a computer over an unsecured network.

SSL

Secure Sockets Layer

- Encrypts data sent between a website and a browser.

SSO

Single Sign-On

- Allows a user to log in to multiple applications using a single set of credentials. For example, your Google account allows you to access services like Gmail, Photos, Drive, etc, using the one login.

STIX

Structured Threat Information eXchange

- A standardized, JSON-based language used to share threat intelligence information.

SWG

Secure Web Gateway

- Act as a checkpoint for emails moving in and out of an organization, using filters to prevent spam or other attacks. Additionally, the gateway can prevent sensitive data from leaving an organization by automatically encrypting messages containing sensitive information.

T

TACACS+

Terminal Access Controller Access Control System

- A protocol that authenticates and authorizes users who access a remote network using a centralized server, providing AAA.

TAXII

Trusted Automated eXchange of Indicator Information

- A protocol used to exchange cyber threat information over HTTPS.

TCP/IP

Transmission Control Protocol/Internet Protocol

- A reliable, connection-oriented protocol that ensures data is delivered correctly the source host to the destination host based on their IP addresses

TGT

Ticket Granting Ticket

- A user authentication token granted by a key distribution center that allows users to request tokens for resources or systems without the need to re-authenticate users for every request.

TKIP

Temporal Key Integrity Protocol

- A wireless network standard created to replace WEP, adding a key-mixing function, sequence counter, and a message integrity check. It is now considered insecure

TLS

Transport Layer Security

- A cryptographic protocol that encrypts data sent over the internet for secure and private communications, commonly used in HTTPS.

TOC

Time-of-check

- The time at which an application checks and validates a value or resource.

TOTP

Time-based One-time Password

- A computer algorithm that generates a one-time password. It uses the current time as a source of uniqueness.

TOU

Time-Of-Use

- The time at which an application uses a value or resource.

TPM

Trusted Platform Module

- A chip residing in a device that provides hardware security. It can generate random numbers and keys, can securely store and manage keys, and provides unique keys often burnt into the TPM during manufacturing.

TTP

Tactics, Techniques, and Procedures

- Describes how cybercriminals execute attacks, such as patterns of activities or methods associated with specific actors.

TSIG

Transaction Signature

- Enables the DNS to authorize updates to its database using shared secret keys and one-way hashing to provide secure authentication of a connection, allowing it to update the DNS.

U

UAT

User Acceptance Testing

- The final stage in software development, involving testing the product from the user's perspective to ensure that the software is ready for release.

UAV

Unmanned Aerial Vehicle

- Commonly known as a drone, a UAV is an aircraft without any human pilot, crew, or passengers on board.

UDP

User Datagram Protocol

- A connectionless communication protocol used for fast and efficient data transmission with no error checking or guaranteed delivery.

UEFI

Unified Extensible Firmware Interface

- A computer software that replaces traditional BIOS firmware interfaces with a more advanced platform for interacting with computer hardware.

UEM

Unified Endpoint Management

- Provides a single interface for managing different types of devices, replacing MDM and client management tools.

UPS

Uninterruptible Power Supply

- A standby, battery-powered device that provides immediate, short-term power to critical systems when the primary power source fails.

URI

Uniform Resource Identifier

- A sequence of characters that uniquely identifies a resource, like a website or email address.

URL

Universal Resource Locator

- A website reference that tells a browser its location on a computer network and how to retrieve it.

USB

Universal Serial Bus

- An interface that allows external devices to connect to a computer for power or communication purposes.

USB OTG

USB On The Go

- Allows USB devices to also act as a host so other USB devices can be attached to them.

UTM

Unified Threat Management

- An all–in-one solution to security. It combines firewall, antivirus, IDS/IPS, and filtering, etc. into one application.

UTP

Unshielded Twisted Pair

- A copper cable made of pairs of insulated wires twisted together, surrounded by an outer jacket. These cables are most commonly used for networking as the twisting helps minimize electromagnetic interference and electrical noise.

V

VBA

Visual BAsic

- A programming language that's part of Microsoft Office. It allows users to create macros and customize applications.

VDE

Virtual Desktop Environment

- Allows users to access a desktop remotely from any device using a hypervisor to separate computing resources into virtual instances and a connection broker to link virtual desktops and authenticate users.

VDI

Virtual Desktop Infrastructure

- Allows users to access a company’s computer system through any device using virtualization technology to separate the OS from the physical desktop.

VLAN

Virtual Local Area Network

- The logical grouping of devices on physical LANs, configured to communicate like they are on the same network.

VLSM

Variable Length Subnet Masking

- A computer networking technique that allows for the division of an IP network into subnets with different subnet masks.

VM

Virtual Machine

- A software-based emulation of a computer that provides the functionality of a physical computer and allows multiple OSs to run concurrently on a single platform.

VoIP

Voice over IP

- A technology that allows users to make phone calls and other communications over the internet.

VPC

Virtual Private Cloud

- A private cloud computing environment contained within a public cloud. VPCs are part of the infrastructure as a service (IaaS) category of cloud services. In essence, VPCs are logically isolated sections of a public cloud in order to provide a virtual private environment.

VPN

Virtual Private Network

- Create secure, encrypted tunnels over insecure networks, like the internet. Users can send data that is protected from unauthorized access, allowing for secure access to private networks from remote locations.

VTC

Video TeleConferencing

- A live audio and video conversation between two or more people in different locations over the internet.

W

WAF

Web Application Firewall

- Designed to protect web applications through filtering HTTP/HTTPS traffic between web apps and the internet, protecting from vulnerabilities such as SQLi, XXS, and CSRF. WAF is not a primary firewall, but it is good for protecting web applications exposed to the internet.

WAP

Wireless Access Point

- A device that transmits and receives data over a WLAN, serving as the connection between a WLAN and a wired network.

WEP

Wired Equivalent Privacy

- A wireless encryption method used to secure wireless networks. WEP is flawed and vulnerable to attack, making it obsolete.

WIDS

Wireless Intrusion Detection System

- A device that monitors a WLAN for threats, alerting security administrators or suspicious activity.

WIPS

Wireless Intrusion Prevention System

- A device that monitors a WLAN for threats and actively takes actions to prevent or deny suspicious activity.

WO

Work Order

- A document that outlines specific tasks that have been requested to be done, including the process for completing the task.

WPA

Wi-Fi Protected Access

- A standard for devices with wireless internet connections. WPA3 is the latest security protocol, providing stronger encryption and more secure authentication methods. WPA3 uses SAE to allow for the mutual authentication of devices.

WPS

Wi-Fi Protected Setup

- Allows users to connect devices to a secure wireless network without entering a password, instead though using a PIN. It can be dangerous for malicious attackers to get onto your network without the need for your Wi-Fi password as these PINs can be easily deduced.

WTLS

Wireless TLS

- A security level for applications that use WAP based on TLS. WTLS encrypts messages between the mobile WAP client and the gateway.

X

XDR

eXtended Detection and Response

- Extends EDR by integrating with other security tools and providing a holistic view of threats including networks, servers, and cloud services.

XML

eXtensible Markup Language

- A language that allows users to define and store data in a way that is both human and machine readable.

XOR

eXclusive Or

- A boolean logic operation that outputs 1 if the bits compared are different and outputs 0 if the bits compared are the same.

XSRF

Cross-Site Request Forgery

- Attacks occur when users are tricked into performing malicious actions on a website they are logged into, exploiting the trust the browser has for users.

XSS

Cross-Site Scripting

- Occurs when a malicious script is injected into an otherwise trusted web page viewed by end users. This compromises the trust a user has for the web application.