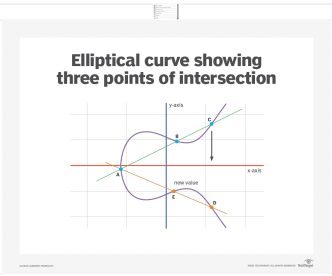
SEC+ 701 TERMS (A-TO-Z)

ACRONYM	FULL NAME	DESCRIPTION	IMAGE
802.11	-	Collection of Wireless LAN & Mesh Wi-Fi	
802.11	-	Collection of Wireless LAN & Mesh Wi-Fi	
SRTP	[Secure] Real-time Transport Protocol	The Secure Real-time Transport Protocol (SRTP) is a profile for Real-time Transport Protocol (RTP) intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.	
AUP	Acceptable Use Policy		
ACL	Access Control List	Allow or deny lists (time-based, dynamic)	
ARP	Address Resolution Protocol	Links MAC addresses with IP addresses	
ASLR	Address Space Layout Randomization	memory protection process for OSes that guards against buffer-overflow attacks by randomizing location for executables	
AES	Advanced Encryption Standards	For symmetric keys. It can have one of three key sizes: 128, 192, or 256 bits. Current version is 256 bit	
AFF	Advanced Forensics Format	The Advanced Forensic Format (AFF) is on-disk format for storing computer forensic information. Critical features of AFF include: AFF allows you to store both computer forensic data and associated metadata in one or more files.	
AFF	Advanced Forensics Format		
APT	Advanced Persistent Threat	Usually, nations state attackers	
ARPANET	Advanced Research Projects Agency Network	Started in 1966, the first wide-area packet-switched network with distributed control and one of the first computer networks to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet.	
ATT&CK	Adverbial Tactics, Techniques, and Common Knowledge	Developed MITRE, Modern way of looking at cyberattacks	
TCP 548	AFP (Apple Filing Protocol)	AppleShare, Personal File Sharing, File services via a networked connection, unsecured - no UN or PWs	
TCP 548	AFP (Apple Filing Protocol)	AppleShare, Personal File Sharing, File services via a networked connection, unsecured - no UN or PWs	
DLP	Agentless DLP	Dedicated devices on a network that blocks traffic and auto-applies encryption	
RAID 10	AKA RAID 1+0	Minimum of four disks, both mirrored and stripped. Pros: good performance, fault tolerance, and fast rebuild times. Cons: large # of drives, reduced useable capacity & scalability	
	Alteration	Unauthorized modification of data. Opposite of integrity	
EFS (Amazon)	Amazon Elastic File System	provides flexible storage capacity that scales to accommodate workloads that run on AWS Elastic Compute Cloud (EC2) instances and access files through application programming interface (API) requests.	
Amplified DoS	Amplified DoS Attacks	taking advantage of small query —> large result (ex: DNS query)	
ALE	Annualized Loss Expectancy	SLE * ARO, amount of damage expected each year	
ARO	Annualized Rate of Occurance	ARO 2.0 means 2X per year	
XaaS	Anything as a service		
TCP 5223	Apple's Push Notification Service	Officially listed as "HP Virtual Machine Group Management"	
TCP 5223	Apple's Push Notification Service	Officially listed as "HP Virtual Machine Group Management"	
API	Application Programmable Interface	Relies on rate limiting, inputting filtering, appropriate monitoring	
ASV	Approved Scanning Vendor	Examples: Nessus, Qualys, Rapid7's Expose, OpenVAS	
	Artifacts	Pieces of evidence that point to an activity on a system	
AV	Asset Value	Expressed in dollars	
	Asymmetric Key Algorithms	Public and private key algorithms. Number of keys needed is always 2X the number of users	
ABAC	Attribute-based Access Control	Policies that are driven by the attributes of the users. Complex to manage	
	Attributes	Can be changeable things, like title or address	
AH	Authentication Header	hashing + shared secret key = IP payload is secured	
AAA	Authentication, Authorization, and Accounting	Device authentication methods: digital certificate, IP addresses, and MAC addresses. People authentication methods: UN/PW, Biometrics, MFA. TACACS+ and RADIUS also provide AAA functionality	
AIS	Automated Indicator Sharing	Automated Indicator Sharing (AIS) is a service the Cybersecurity and Infrastructure Security Agency (CISA) provides to enable real-time exchange of machine-readable cyber threat indicators and defensive measures between public and private-sector organizations. AIS helps to protect the participants of the service and ultimately reduce the prevalence of cyberattacks.	
	Automation	Achieving outcomes without humans	
	Availability	Data/systems are readily available	
	Availability zone	One or more data centers with independent power & cooling	
EBS	AWS Elastic Block Store	Amazon Elastic Block Store (EBS) provides raw block-level storage that can be attached to Amazon EC2 instances and is used by Amazon Relational Database Service (RDS).[1] It is one of the two block-storage options offered by AWS, with the other being the EC2 Instance Store.[2]	
EC2	AWS Elastic Computer Cloud	Amazon Elastic Compute Cloud is a part of Amazon.com's cloud-computing platform, Amazon Web Services, that allows users to rent virtual computers on which to	
S3	AWS Simple Storage Service	Amazon S3 or Amazon Simple Storage Service is a service offered by Amazon Web Services that provides object storage through a web service interface. Amazon S3 uses the same scalable storage infrastructure that Amazon.com uses to run its e-commerce network.	
BIOS	Basic Input/Output System	also known as the System BIOS, ROM BIOS, BIOS ROM or PC BIOS) is firmware used to provide runtime services for operating systems and programs and to perform hardware initialization during the booting process (power-on startup).	
	Biometrics	something you are (physiology) like fingerprints, retina scans, facial recognition, voice recognition, vein recognition, gait analysis (how a person walks)	
	Black Hat	Unauthorized	
	Black Hat Briefings	Black Hat Briefings is a computer security conference that provides security consulting, training, and briefings to hackers, corporations, and government agencies around the world.	
	Blacklists	Application deny lists	
	Blind Cross-site Scripting	A form of persistent XSS, sending a hidden payload that collect victims info like cookies, credentials. Hard to confirm but can be done via XSS Hunter	
	Blind SQL Attacks	Asking data database true or false questions	
	Bloatware	Not necessarily harmful, more applications than you need	
	Block ciphers	Apply encryption algorithm	
BIAS	Bluetooth Impersonation AttackS	Exploiting mutual authentication	
BGP	Border Gateway Protocol	Enables the internet exchange routing information between autonomous systems (insecure). Susceptible to BGP hijacking	
	Botnet	Network of computer that are infected with malware and controlled by an attacker. Usually for DDoS attacks. Utilizes routers, C&C, HTTP or IRC	
BASH	Bourne-Again Shell	a Unix shell and command language written by Brian Fox for the GNU Project as a free software replacement for the Bourne shell.[15][16] The shell's name is an acronym for Bourne-Again SHell, a pun on the name of the Bourne shell that it replaces[17] and the notion of being "born again".	
BPDU	Bridge Protocol Data Unit	Protects STP from sending messages it should not, prevents looping	
BYOD	Bring your own device		
	Buffer Overflows	Placing more data into memory are than it can handle	
BC	Business Continuity	making sure business can continue despite the incident, important for larger incidents	
BEC	Business Email Compromise	Compromised accounts, spoofed email, typo squatting domain, malware	
BIA	Business Impact Analysis		
BPA	Business partner agreements	when two organizations agree to do business together, could potentially specify responsibilities and division of profits	
CIS	Center for Internet Security	US 501 nonprofit organization, formed in October 2000. Its mission statement professes that the function of CIS is to " help people, businesses, and governments protect themselves against pervasive cyber threats	
CA	Certificate Authority	Issues digital certificates to provide assurance people are who they claim to be	
CSR	Certificate Signing Request	Providing CA with your public key to initiate the CSR	
CRL	Certification Revocation Lists	Newly revoked certificates	
CHAP	Challenge Handshake Authentication Protocol	Encrypted challenge + 3-way handshake	
CSU/DSU	Channel Service Unit/Data Service Unit	A router can function as a CSU/DSU A CSU/DSU (Channel Service Unit/Data Service Unit) is a hardware device about the size of a modem. It converts a digital data frame from local area network	
	Checksum	Small-sized block of data derived from another block of data to detect errors	
CIO	Chief Information Officer		
CISO	Chief Information Security Officer		
CSO	Chief Security Officer		
CYOD	Choose your own device		
CYOD	Choose your own device		
CBC	Cipher Block Chaining	Cipher block chaining (CBC) is a mode of operation for a block cipher -- one in which a sequence of bits are encrypted as a single unit, or block, with a cipher key applied to the entire block. Cipher block chaining uses what is known as an initialization vector (IV) of a certain length. By using this along with a single encryption key, organizations and individuals can safely encrypt and decrypt large amounts of plaintext.	

SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
CFB	Cipher Feeback	The cipher feedback (CFB) mode, in its simplest form uses the entire output of the block cipher. In this variation, it is very similar to CBC, turning a block cipher into a self-synchronizing stream cipher	
	Cipher suites	Sets of ciphers and key lengths to support a system	
C	Cipher Text		
CTAP	Client to Authenticator Protocol	Client To Authenticator Protocol (CTAP) is a specification describing how an application (i.e. browser) and operating system establish communications with a compliant authentication device over USB, NFC or BLE communication mediums. The specification is part of the FIDO2 project and W3C WebAuthN specification.	
CCTV	Closed-Circuit Television		
CASB	Cloud Access Security Brokers	software tools in-between cloud users and providers	
	Cloud Bursting	On-demand and temporary use of public cloud when demand exceeds resources	
CCM	Cloud Controls Matrix	Determines appropriate use of cloud security controls	
	Cloud Instance	Virtual server	
CSA	Cloud Security Alliance	Defines best practices for securing cloud computing. Made the CCM & STAR system	
CSP	Cloud Service Provider	a company that offers components of cloud computing -- typically, infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS).	
	Cold Site	Only bare metal infrastructure	
C2	Command & Control Servers	C2 servers facilitate data exfiltration by instructing the compromised device to send specific data to the server. This data can include stolen credentials, sensitive documents, or other valuable information.	
CCE	Common Configuration Enumeration	Systems and configurations issues	
CPE	Common Platform Enumeration	Product names and versions	
CVE	Common Vulnerability & Exposures	Security flaws	
CVSS	Common Vulnerability Scoring System	Measuring and describing severity. 0.1-3.9 (low), 4.0-6.9 (medium), 7.0-8.9 (high), 9.0-10.0 (critical)	
CAPTCHA	Completely Automated Turing Test to Tell Computers and Humans Apart	a type of challenge–response test used in computing to determine whether the user is human in order to deter bot attacks and spam.	
CBT	Computer Based Training	part of a diversity of a strong security training program	
CERT	Computer Emergency Response Team		
	Computer Forensics	Subfield of Digital Forensics	
CIRT	Computer Incident Response Team		
CSIRT	Computer Security Incident Response Team		
	Confidentiality	Unauthorized individuals are not able to gain access to sensitive info	
CIA Triad	Confidentiality, Integrity, Availability (and nonrepudiation)	Describes what cybersecurity professionals seek to continuously protect	
	Containers	Application-level virtualization (ex: Docker), each instance is the same hardware/OS and share the same Kernel	
	Containment	Leaves system in place but prevents further actions	
	Content Filtering	use of hardware or software to screen and/or restrict access to resources	
CMS	Content Management System	A content management system (CMS) is a software application that enables users to create, edit, collaborate on, publish and store digital content. A CMS has two components: a content management application (CMA) and a content delivery application (CDA). The CMA is a graphical user interface that enables users to design, create, modify and remove content from a website without HTML knowledge.	
CAM	Content-addressable memory	AKA associative memory or associative storage, computer memory used in very high-speed searching applications	
CP	Contigency Planning	A contingency plan helps an organization recover from an unexpected event. Find out the seven steps involved in creating one and minimizing disruptions	
COOP	Continuity of Operations Planning	A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.	
CI/CD	Continuous Integration/Continuous Deployment (or Delivery)	Consistently checking code, monitoring	
	Control objectives	Desired security state	
COBIT	Control Objectives for Information and related Technologies	Auditing standards. Used to develop, implement, monitor, and improve IT structures. Maintained by ISACA	
	Control Plane	Controls data plane, adaptive identity, leverages context, may request additional info, policy driven	
	Cookies Theft (AKA cookie hijacking, stealing)	Stealing user's cookie data to access user's accounts	
COBO	Corporate Owned Business Only		
COPE	Corporate-owned, personally enabled		
CAR	Corrective Action Report	an official document issued when an element of a plan hasn't been implemented or executed properly	
CTM/CTR	Counter Mode	converts a block cipher into a stream cipher. It combines an IV with a counter and uses the result to encrypt each plaintext block. Each block uses the same IV, but CTM combines it with the counter value, resulting in a different encryption key for each block. Multiprocessor systems can encrypt or decrypt multiple blocks at the same time, allowing the algorithm to be quicker on multiprocessor or multicore systems. CTM is widely used and respected as a secure mode of operation.	
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol	uses AES to provide confidentiality. Provides authentication for user and access control capabilities	
CSRF/XSRF	Cross-Site Request Forgery (AKA Sea Surf, Session Riding)	Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website or web application where unauthorized commands are submitted from a user that the web application trusts	
XSS	Cross-Site Scripting	Web injection attack which malicious scripts are injected into a website. Executes when the victim loads the website	
	Cryptoanalysis	The study of methods to defeat codes and ciphers	
	Cryptography	Creating and implementing secret codes and ciphers	
	Cryptology	Cryptoanalysis + cryptography	
	Cryptosystems	Specific implementation of code or cipher in software	
	Cryptovariables	Another term for cryptographic keys	
CISA	Cybersecurity and infrastructure security agency	Founded 2018, "We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people"	
CSF	Cybersecurity Framework	Broad structure for cybersecurity controls in private sector	
CRC	Cyclical Redundancy Check	Error-detecting code used in digital networks to detect accidental changes to digital data	
DBAN	Darik's Boot and Nuke	Performs multiple passes over a disk to completely sanitize it	
DES	Data Encryption Standard	developed by IBM in the early 1970s and published in 1976. DES is a block cipher, which divides the plain text into 64-bit blocks and encrypts each block (unsecure)	
DEP	Data Execution Prevention	Data Execution Prevention (DEP) is a technology built into Windows that helps protect you from executable code launching from places it's not supposed to	
DLP	Data loss prevention	Via pattern matching, watermarking, or DRM	
	Data Plane	Implicit trust zones, subject, policy enforcement points	
DPO	Data Protection Officer	Official role required by GDPR (Chief Privacy Officer in US)	
DRA	Data Recovery Agent	Microsoft Windows user account with the ability to decrypt data that was encrypted by other users	
DBA	Database Administrator	the information technician responsible for directing and performing all activities related to maintaining a successful database environment. A DBA makes sure an organization's databases and related applications operate functionally and efficiently.	
DBMS	Database Management System	A database management system (DBMS) is system software for creating and managing databases. A DBMS makes it possible for end users to create, protect, read, update and delete data in a database. The most prevalent type of data management platform, the DBMS essentially serves as an interface between databases and users or application programs, ensuring that data is consistently organized and remains easily accessible.	
	Decryption	Cipher text → plaintext via decryption key	
DID	Defense-in-depth	Multiple controls to prevent SPOF	
	Deidentification	Removing the ability to link data back to an identity	

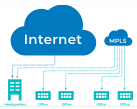
SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
DMZ	Demilitarized Zone	AKA Permieter zone, no-mans-land in network designed to add security layer by isolating networks (like N/S Korea)	
	Denial	Disruption of authorized users to access data. Opposite of availability	
DoS	Denial of Service	A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.	
DNAT	Destination Network Address Translation	is a technique that translates destination IP address generally when connecting from public IP address to private IP address. It is generally used to redirect packets destined for specific IP address or specific port on IP address, on one host simply to a different address mostly on different host.	
	DevOps	Software development + IT operations	
	DevSecOps	Software development + security + IT operations	
	DHCP Snooping	Prevents rogue DHCP server from handing out IP addresses	
	Dictionary attacks	A form of brute force attacks, using list of words for attacks (ex: tool name John The Ripper does this)	
	Differential Backup	All the data that has changed since the last FULL BACKUP	
DH	Diffie-Hellman (Symmetric Key Encryption algorithims)	Developed in 1976, Diffie-Hellman key exchange is a method of digital encryption that securely exchanges cryptographic keys between two parties over a public channel without their conversation being transmitted over the internet. The two parties use symmetric cryptography to encrypt and decrypt their messages. Diffie-Hellman key exchange raises numbers to a selected power to produce decryption keys. Two or more users have a common shared private key. Public key can be transmitted or intercepted by an attacker, but they wouldn't be able to glean the shared private password DH uses PFS: meaning easy to compute one way, but extremely difficult to undo. The components of the keys are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming. Diffie-Hellman key exchange is commonly found in security protocols, such as Transport Layer Security (TLS), Secure Shell (SSH) and IP Security (IPsec). Strengthened by 2048-bit blocks/key lengths	
DFIR	Digital Forensics and Incident Response	Finding evidence, removing attacker, assessing damage, lessons learned Eric Zimmerman's Tools KAPE (Knoll Artifact Parser and Extractor): automates artifact collection, creates timeline Autopsy: open source forensic platform Volatility: memory analysis Redline: collecting forensic information Velociraptor: open-source advanced endpoint-monitoring, forensics, and response platform	
DRM	Digital Rights Management	Enforce copyright and data ownership	
DSA	Digital Signature Algorithm	a public-key cryptosystem and Federal Information Processing Standard for digital signatures, based on the mathematical concept of modular exponentiation and the discrete logarithm problem	
	Digital Signatures	Enforce non-repudiation & integrity	
DSL	Digital Subscriber Line	DSL (Digital Subscriber Line) is a modem technology that uses existing telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. DSL provides dedicated, point-to-point, public network access	
	Directory Traversal (AKA path traversal)	Navigating somewhere else on directory paths (ex: using the "../" In header	
DRP	Disaster Recovery Planning	A disaster recovery plan (DRP) is a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident	
	Disclosure	Data loss or data exfiltration. The opposite of confidentiality	
DAD Triad	Disclosure, alteration, denial	Describes what threat actors seek	
DAC	Discretionary Access Control	More common, access control scheme to control home PCs (ex: Linux file permissions)	
DER	Distinguished encoding rules	Binary file stored in .der, .crt, .cer	
DDoS	Distributed Denial of Service	A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.	
UDP/TCP 53	DNS	Unsecure, succumbs to DDoS	
TCP/UDP 53	DNS	Unsecure, succumbs to DDoS	
	DNS filtering	blocks malicious domains via lists	
DNSSEC	DNS System Security Extensions	provides authentications of DNS data	
UDP/TCP 53	DNSSEC	Provides integrity not confidentiality via digital signatures	
TCP/UDP 53	DNSSEC	Provides integrity not confidentiality via digital signatures	
DOM	Document object model	connects web pages to scripts or programming languages by representing the structure of the document	
	DOM-based XSS	Attacker injects a script into a response, written deep in JS code, look for eval() method	
DV	Domain Validation Certificate	CA verifies use subject has control over the domain name	
DMARC	Domain-based Message Authentication Reporting and Conformance	determine whether you should refuse or accept email message	
DNS	Domain-name system	only tells WHERE to send traffic —> not inherently secure	
DKIM	DomainKeys Identified Mail	Signature header to verify email sender and prevent email spoofing	
802.1Q	Dot1Q	Supports VLAN on IEEE 802.3 Ethernet network	
802.1Q	Dot1Q	Supports VLAN on IEEE 802.3 Ethernet network	
49152-65535	Dynamic and/or Private Ports		
49152-65535	Dynamic and/or Private Ports		
DHCP	Dynamic Host Configuration Protocol	Network protocol that automatically assigns IP address to devices, currently using IPv6 called DHCPv6	
	Dynamic Testing	Executes code as part of test	
DLL	Dynamic-link library	A DLL is a library that contains code and data that can be used by more than one program at the same time in Windows OS	

SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
	E-discovery	Electronic discovery	
	Edge Computing	IoT devices that preprocess data before shipping it back to the cloud	
	Elasticity	Provision/deprovision resources automatically	
ECB	Electronic Code Book	Simplest encryption methods, The message is divided into blocks, and each block is encrypted separately. The problem is that if you submit the same plain text more than once, you always get the same cipher text. This gives attackers a place to begin analyzing the cipher to attempt to derive the key.	
EDRM	Electronic Discovery Reference Model	Framework for outlining activities for recovering and discovering digital data	
ECC	Elliptic Curve Cryptography	Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller and more efficient cryptographic keys. ECC is an alternative to the Rivest-Shamir-Adleman (RSA) cryptographic algorithm and is most often used for digital signatures in cryptocurrencies, such as Bitcoin and Ethereum, as well as one-way encryption of emails, data and software. An elliptic curve is not an ellipse, or oval shape, but it is represented as a looping line intersecting two axes, which are lines on a graph used to indicate the position of a point. The curve is completely symmetric, or mirrored, along the x-axis of the graph. Public key cryptography systems, like ECC, use a mathematical process to merge two distinct keys and then use the output to encrypt and decrypt data. One is a public key that is known to anyone, and the other is a private key that is only known by the sender and receiver of the data. ECC generates keys through the properties of an elliptic curve equation instead of the traditional method of generation as the product of large prime numbers. From a cryptographic perspective, the points along the graph can be formulated using the following equation: $y^2=x^2 + ax + b$ ECC is like most other public key encryption methods, such as the RSA algorithm and Diffie-Hellman. Each of these cryptography mechanisms uses the concept of a one-way, or trapdoor, function. This means that a mathematical equation with a public and private key can be used to easily get from point A to point B. But, without knowing the private key and depending on the key size used, getting from B to A is difficult, if not impossible, to achieve.	
ECDHE	Elliptic Curve Diffie-Hellman Key Exchange	a key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel	
ECDSA	Elliptic Curve Digital Signature Algorithm	offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic-curve cryptography.	
	Embedded Systems	electronic product that contains a microprocessors and software design to perform a specific task	
ESP	Encapsulating Security Payload	tunnel mode - entire packet secured, transport mode - only payload secured	
E01	Encase Image File Format	Developed by ASR Data, the Expert Witness file format (aka E01 format aka EnCase file format) is an industry standard format for storing “forensic” images. The format allows a user to access arbitrary offsets in the uncompressed data without requiring decompression of the entire data stream.	
	Encryption	Plaintext → cipher text via encryption key	
EFS	Encryption File System	provides an added layer of protection by encrypting files or folders on various versions of the Microsoft Windows OS	
EOL	End of life	AKA End of sales	
EOSL	End of service life	End of technical support, legacy	
EDR	Endpoint detection and response	Behavioral monitor endpoint devices & detect/respond to threats	
ERP	Enterprise Resource Planning	ERP software can integrate all of the processes needed to run a company. ERP solutions have evolved over the years, and many are now typically web-based applications that users can access remotely. Some benefits of ERP include the free flow of communication between business areas, a single source of information, and accurate, real-time data reporting. There are hundreds of ERP applications a company can choose from, and most can be customized. An ERP system can be ineffective if a company doesn't implement it carefully.	
ERM	Enterprise Risk Management	formal org approach to risk analysis. Identify risks, determine severity	
	Ephemeral accounts	one-time accounts created on the fly, which are immediately deprovisioned or deleted after use	
DHE	Ephemeral Diffie-Hellman	When a key exchange uses Ephemeral Diffie-Hellman a temporary DH key is generated for every connection and thus the same key is never used twice. This enables Forward Secrecy (FS), which means that if the long-term private key of the server gets leaked, past communication is still secure.	
	Ephemeral Keys	perfect forward key secrecy —> even if key exchange is compromised, communication will not	
	Events	observable occurrence	
	Evil Twin	malicious access point trying to appear legitimate	
XOR	Exclusive Or		
1	Execute	- - x	
3	Execute + Write	-wx	
EF	Exposure Value	Percentage of expected damage (ex: EF 90%)	
XDR	Extended detection and response	Holistic approach using AI to monitor and response to threats across the entire enterprise	
EV	Extended Validation	Higher level of assurance, more security steps for CA	
EAP	Extensible Authentication Protocol	Evolution of PPP, framework that allows for the use of different authentication methods for secure network access technologies	
EAPoL	Extensible Authentication Protocol over LAN	EAPOL (Extensible Authentication Protocol over Local Area Network) encapsulates EAP packets within Ethernet frames.	
EAPOL-Key	Extensible Authentication Protocol over Local Area Network Key	This packet is used to transport encryption keys and related data. You’ll see it when you use EAP methods that use encryption or in the Wi-Fi Protected Access (WPA) four-way handshake.	
XCCDF	Extensible Configuration Checklist Description Format	Reporting checklist results	
XML	Extensible Markup Language	Allows different apps to exchange and store data in a universal way	
FAR	False Acceptance Rate	FIDO sets their standards at 0.01% for FAR	
FRR	False Rejection Rate	FIDO sets their standard for 3% of attempts	
FERPA	Family Educational Rights and Privacy Act	US student education records privacy	
FIDO (1.0)	Fast Identity Online	FIDO Alliance, promoting passkeys instead of passwords	
FIDO2	Fast Identity Online 2.0	FIDO vs FIDO2 FIDO2 is a more comprehensive and standardized protocol that is supported by all leading browsers and operating systems, including Android, IOS, MacOS and Windows.	
FIPS	Federal Information Processing Standard	The Federal Information Processing Standards (FIPS) of the United States are a set of publicly announced standards that the National Institute of Standards and Technology (NIST) has developed for use in computer systems of non-military United States government agencies and contractors	
	Federation	Group of trusted IdPs relaying information. Many CSPs use this	
FPGA	Field-programmable gate array	A field-programmable gate array (FPGA) is a type of configurable integrated circuit that can be programmed or reprogrammed after manufacturing.	
FEK	File Encryption Key		
FIM	File Integrity Monitoring	Detects changes made to system/app/files by creating a baseline creation (hash)	
FACL	File System Access Control List	the list of additional users/groups and their respective permissions to the file	
FTP	File Transfer Protocol	FTP is one of the oldest network communication protocols available today, and it predates the global internet. The first version of FTP was drafted in the 1970s for scientific and research use within the U.S. government’s ARPANET. FTP is the network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.	
FTPS	File Transfer Protocol Secure	FTPS vs SFTP FTPS Uses Two Links and the Encryption Tunnel or Layer is Separate, nor Inherent. It is being phased out. Faster, but less secure SFTP Uses a Single Connection and is Inherently Encrypted	
	File-level encryption	Individual files are encrypted	
EAP-FAST	Flexible Authentication via Secure Tunneling	Replacement for LEAP. FAST provides faster authentication while roaming	
	Fog Computing	IoT sensors in between edge computing and server	
	Four-way Handshake	Message 1: The wireless access point (WAP) sends an EAPOL-Key frame with nonce value (a random number that can only be used once in a given cryptographic exchange) and connection information to the client. The WAP’s nonce value is called ANonce. With this information, the client is able to derive the pairwise transient key (PTK), which is required to encrypt traffic between the	
FTK	FTK Imager	FTK Imager: A Comprehensive Guide to Forensic Imaging and ... FTK Imager allows forensic investigators to create forensic images of hard drives, partitions, and logical files	
TCP 21	FTP - Control Channel	Unsecure	
TCP 21	FTP - Control Channel	Unsecure	
TCP 20	FTP (File Transfer Protocol) - Data Channel	Unsecure	
TCP 20	FTP (File Transfer Protocol) - Data Channel	Unsecure	
TCP 21	FTPS	Using TLS (TCP 21 in explicit mode and 990 in implicit mode)	
TCP 21	FTPS	Using TLS (TCP 21 in explicit mode and 990 in implicit mode)	
TCP 990	FTPS (Implicit) - Control Channel		

SEC+ 701 TERMS (A-TO-Z)

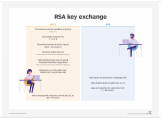
ACRONYM	FULL NAME	DESCRIPTION	IMAGE
TCP 990	FTPS (Implicit) - Control Channel		
TCP 989	FTPS (Implicit) - Data Channel		
TCP 989	FTPS (Implicit) - Data Channel		
	Full Backup	Copies the entire device or storage system	
FDE	Full disk encryption	All files on a hard drive are automatically encrypted, except the MBR	
FaaS	Function as a service		
	Fuzz testing (AKA fuzzing)	Testing codes ability to handle random data	
GCM	Galois Counter Mode	Galois Counter Mode (GCM) combines counter mode (CTR) with Galois authentication. The added benefit of that is we can not only encrypt data, but we can authenticate where the data came from. We get both data integrity and confidentiality	
	Gap analysis	Examining security controls VS control objectives	
GDPR	General Data Protection Regulation	Security and privacy requirements for PII in the EU	
GRE	Generic Routing Encapsulation	Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route various protocols over Internet Protocol (IP) networks. In essence,	
	Geography	Area of the world containing at least one region —> fault tolerance	
GPS	Global Positioning System	uses satellite network (ex: U.S. GPS system, Russian GLONASS) —> used for Geolocation authentication, geofencing	
GPG	GNU Privacy Guard	GnuPG is a hybrid-encryption software program because it uses a combination of conventional symmetric-key cryptography for speed, and public-key cryptography for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is used only once.	
GPG	Gnu Privacy Guard	a free-software replacement for Symantec's PGP cryptographic software suite	
GNU	GNU Project	a free software, mass collaboration project announced by Richard Stallman on September 27, 1983. Its goal is to give computer users freedom and control in their use of their computers and computing devices by collaboratively developing and publishing software that gives everyone the rights to freely run the software, copy and distribute it, study it, and modify it. GNU software grants these rights in its license.	
	Gnu Project	a free software, mass collaboration project announced by Richard Stallman on September 27, 1983. Its goal is to give computer users freedom and control in their use of their computers and computing devices by collaboratively developing and publishing software that gives everyone the rights to freely run the software, copy and distribute it, study it, and modify it	
	Gold Master Image	Best and final version of a VDI (virtual desktop infrastructure)	
	Governance programs	set of procedures and controls put in place to allow an organization to effectively direct its work	
GRC	Governance, risk, and compliance	GRC (governance, risk and compliance) is an organizational strategy for framework for managing governance, risk management and compliance with industry and government regulations.	
GLBA	Gramm-Leach-Bliley Act	US financial institutions must have security programs	
GPU	Graphics Processing Unit	A graphics processing unit (GPU) is a specialized electronic circuit initially designed to accelerate computer graphics and image processing (either on a video card or embedded on motherboards, mobile phones, personal computers, workstations, and game consoles).	
	Gray Hat	Semi-authorized	
GPO	Group Policy Objects	Hardening system and domain controls via policy	
GTK	group temporal key	The Group Temporal Key (GTK) used in the network may need to be updated due to the expiration of a preset timer. When a device leaves the network, the GTK also needs to be updated. This is to prevent the device from receiving any more multicast or broadcast messages from the AP.	
	Hacktivist	Ex: Anonymous	
HDD	Hard Disk Drives		
HSM	Hardware Security Modules	Physical computing devices that are tamper-resistant and hardened. Protect and manage cryptographic keys, digital signatures, perform encryption/decryption, create & verify digital signatures	
HMAC	Hash-Based Message Authentication Code	Hash-based Message Authentication Code (HMAC) is a message encryption method that uses a cryptographic key in conjunction with a hash function, more secure means of encrypting data than a simple Message Authentication Code (MAC), HMAC is a technique for cryptographic authentication	
HIPAA	Health Insurance Portability and Accountability Act	Privacy rules for medical industry in the US	
HA	High availability		
HTOP	HMAC One Time Passwords	generate code token from last known token (ex: SMS code. Susceptible to SIM cloning)	
	Honeyfile	Trap file, prevents ransomeware	
	Honeynet	A honeynet is a network set up with intentional vulnerabilities hosted on a decoy server to attract hackers	
	Honeypot	a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems	
	Honeytoken	fictitious words or records that are added to legitimate databases. They allow administrators to track data in situations they wouldn't normally be able to track, such as cloud-based networks. If data is stolen, honey tokens allow administrators to identify who it was stolen from or how it was leaked	
HIDS	Host-based intrusion detection system	Cannot block, only detect	
HIPS	Host-based intrusion prevention system	Monitors a single host ffor malicious activity, analyzes traffic before host can process it. Con: can block legitimate traffic	
	Hot site	Operated full-time	
TCP 80	HTTP	Unsecure, unencrypted	
TCP 80	HTTP	Unsecure, unencrypted	
TCP 443	HTTPS (Hypertext Transfer Protocol Secure)	Secure and encrypts data between the user's browser and website via TLS	
TCP 443	HTTPS (Hypertext Transfer Protocol Secure)	Secure and encrypts data between the user's browser and website via TLS	
HTML	Hypertext Markup Language (current is 5)	Language of the web for displaying content	
HTTPS	Hypertext Transport Protocol Secure	Normal HTTP over TLS. Most secure and widely adopted method today	
	Hypervisors	Isolates virtual machines. Type 1: bare-metal hypervisors, operate on the hardware. Type 2: runs on top of OS. They do not share the same kernel	
	ICMP Floods	AKA ping floods	
IAM	Identity and Access Management	dentity and access management is for making sure that only the right people can access an organization's data and resources	
IEEE 802	IEEE 802	Collection of networking standards that cover physical and data link layer specifications for technologies such as Ethernet and wireless	
IEEE 802	IEEE 802	Collection of networking standards that cover physical and data link layer specifications for technologies such as Ethernet and wireless	
802.1X	IEEE Standard for NAC	The IEEE 802.1X standard provides a network access framework for managing wireless LAN usage. But 802.1X is merely an envelope that carries some type of Extensible Authentication Protocol.	
	Images	Complete copy of a server or drive down to the bit. Backup method of choice for complex servers	
TCP 143	IMAP (Internet Message Access Protocol)	Send email and more features than POP3 but still unencrypted and unsecured. Use Port 993 instead	
TCP 143	IMAP (Internet Message Access Protocol)	Send email and more features than POP3 but still unencrypted and unsecured. Use Port 993 instead	
IAMPR	Imposter Attacker Presentation Match Rate	a metric used in a full-system evaluation	
	Incident	violation of organizations policies	
IR	Incident Response	plan, process, team, technology, skills, and training to respond appropriately (ongoing process)	
IRP	Incident Response Plan	set of instructions to detect, respond to and limit the effects of an information security event.	
	Incremental Backup	Captures changes since last incremental backup. Pro: fast to recover. Con: slow to backup	
IoC	Indicators of Compromise	Red flags: file signatures, log patterns, file and code repositories	
ICS	Industrial Control Systems	Network and software used to control industrial systems (ex: power plant, water plant, manufacturing)	
ISAC	Information Sharing and Analysis Center		
ISACA	Information Systems Audit and Control Association	Global non-profit to help IT professional audit, cybersecurity, and emerging tech (via certs, publications, etc)	
ISSO	Information Systems Secutity Officer	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.	
	Infrared	only work in line-of-sight (speeds from 115 Kbit/s to 1 Gbit/s)	
IaaS	Infrastructure as a Service	Responsible for Hardware and datacenter	
IaC	Infrastructure as Code	Using code to manage & provide	
IV	Initialization Vector	An initialization vector (IV) is an arbitrary number that can be used with a secret key for data encryption to foil cyber attacks. This number, also called a nonce (number used once), is employed only one time in any session to prevent unauthorized decryption of the message by a suspicious or malicious actor.	
	Injection Vulnerabilities	Primary attack for web applications	
	Inline CASB	Physically inline between users and providers	
IDOR	Insecure Direct Object Reference	When a web app provides direct access to something by modifying the URL (ex: changing the end to 123, 124, 125)	
IEEE	Institute of Electrical and Electronics Engineers	The Institute of Electrical and Electronics Engineers is an American 501 professional association for electronics engineering, electrical engineering, and other related disciplines. The IEEE has a corporate office in New York City and an operations center in Piscataway, New Jersey.	

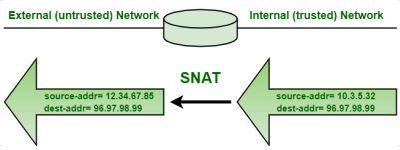
SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
UDP/TCP 1443	Integrated Engineering Software		
TCP/UDP 1443	Integrated Engineering Software		
	Integrity	Ensuring no unauthorized modifications of data	
IKE	Intenet Key Exchanges	setup using X.509 certificates, standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network	
	Interactive Testing	Combines static and dynamic testing	
IC	Intergrated Circuit	An integrated circuit (IC), sometimes called a chip, microchip or microelectronic circuit, is a semiconductor wafer on which thousands or millions of tiny resistors, capacitors, diodes and transistors are fabricated A logic gate is a device that acts as a building block for digital circuits. There are seven basic logic gates: AND, OR, XOR, NOT, NAND, NOR and XNOR.	
IDF	Intermediate Distribution Frame	An intermediate distribution frame (IDF) is a free-standing or wall-mounted rack for managing and interconnecting a telecommunications cable between end-user devices and the main distribution frame (MDF).	
IDEA	International Data Encryption Algorithm	The International Data Encryption Algorithm (IDEA) is a symmetric key block cipher encryption algorithm designed to encrypt text to an unreadable format for transmission via the internet	
ISO	International Organization for Standardizations		
ICMP	Internet Control Message Protocol	The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. **ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.**	
IETF	Internet Engineering Task Force	The Internet Engineering Task Force is a standards organization for the Internet and is responsible for the technical standards that make up the Internet protocol suite. It has no formal membership roster or requirements and all its participants are volunteers	
IMAP	Internet Message Access Protocol	a standard email retrieval (incoming) protocol. It stores email messages on a mail server and enables the recipient to view and manipulate them as though they were stored locally on their device(s).	
IoT	Internet of Things	AKA Embedded Devices	
IP	Internet Protocol	The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.	
IPFIX	Internet Protocol Flow Information Export	The IPFIX protocol provides network administrators with access to IP Flow information	
IPSec	Internet Protocol Security	Entire suite of security protocols, used for VPNs	
IPv4	Internet Protocol version 4	Most common version of IP, uses 32-bit address space	
IPv6	Internet Protocol version 6	hosts automatically generate IP addresses internally using stateless address autoconfiguration (SLAAC)	
IRC	Internet Relay Chat	Internet Relay Chat (IRC) is a text-based chat system for instant messaging. IRC is designed for group communication in discussion forums, called channels, but also allows one-on-one communication via private messages as well as chat and data transfer, including file sharing. Current version is IRCv3	
ISAKMP	Internet Security Association and Key Management Protocol	for establishing security association (SA) and cryptographic keys in an Internet environment	
ISP	Internet Service Provider	An internet service provider is a company that provides internet access for homes and businesses.	
	Intranet	Internal network	
IDS	Intrusion Detection System	Won't shutdown the whole system	
IPS	Intrusion Prevention System	Could shutdown the whole system	
ISO 27001	ISO 27001	Information security management systems	
ISO 27002	ISO 27002	Controls implemented to meet cybersecurity objectives	
ISO 27701	ISO 27701	Standard guidance for managing privacy controls	
ISO 31000	ISO 31000	Guidelines for risk management	
	Isolate	Cutting systems off from access	
	Jailbreaking	the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device	
	Jamf Pro	MDM solution for apple devices	
JSON	JavaScript Object Notation	is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and arrays (or other serializable values)	
JtR	John The Ripper	Helps crack passwords	
	Journaling	Creates a log of changes that can reply if an issue occurs → restoring to a fixed snapshot. Con: The journal also needs to be stored somewhere	
	Jump Servers	(AKA jump boxes) securely operates in two different security zones via SSH or RDP	
JIT	Just-in-time permissions	Permissions granted and revoked when needed	
	Kerberos	Authentication service ticketing request system for between hosts and untrusted networks	
	Kerckhoff's Principle/assumption	the enemy knows the system (not security through obscurity)	
KDC	Key Distribution Center	A key distribution center (KDC) in cryptography is a system that is responsible for providing keys to the users in a network that shares sensitive or private data. Each time a connection is established between two computers in a network, they both request the KDC to generate a unique password which can be used by the end	
KEM	Key Encapsulation Mechanism	used to secure symmetric key material for transmission using asymmetric (public-key) algorithms. It is commonly used in hybrid cryptosystems	
KEK	Key Encryption Key	Key that encrypts another key	
	Key Escrow	a mechanism that allows authorized parties to access the encryption keys of a system or device in the event that the owner is unable to do so	
	Key Length	number of binary bits in the key	
KPI	Key Performance Indicators		
KRACK	Key Reinstallation Attack	KRACK ("Key Reinstallation Attack") is a replay attack (a type of exploitable flaw) on the Wi-Fi Protected Access protocol that secures Wi-Fi connections. It was discovered in 2016[1] by the Belgian researchers Mathy Vanhoef and Frank Piessens of the University of Leuven.[2] Vanhoef's research group published details of	
KRA	Key Results Area		
KRI	Key Risk Indicators		
	Key Space	range of values that are valid for the key to use for an algorithm AKA all the possibilities	
	Key Stretching	Housing of iterations of salting and hashing	
	Keylogger	Keeps track of keystrokes and send it to an attacker via C&C (command-and-control) server	
L2TP	Layer 2 Tunneling Protocol	The Layer 2 Tunneling Protocol (L2TP) is used to transfer information securely and rapidly across public networks. L2TP creates a connection between a device and a VPN server without encrypting the content. It is often used in remote-access scenarios that use the internet to provide intranet-type services.	
TCP 636	LDAPS (Secure Lightweight Directory Access Protocol)	TLS-protected version of LDAP (Lightweight Directory Access Protocol, previously Port 389)	
TCP 636	LDAPS (Secure Lightweight Directory Access Protocol)	TLS-protected version of LDAP (Lightweight Directory Access Protocol, previously Port 389)	
	Legal Hold		
LDAP	Lightweight directory access protocol	Vendor-netural software protocol used to lookup information or devices within a network, supports C and C++	
LEAP	Lightweight EAP	Developed by Cisco prior to IEEE ratification of 802.11i security standard (outdated)	
	Load Balancing	Distribute network traffic to equally across a pool of resources to support an application	
LAN	Local Area Network	A local area network (LAN) is a group of computers and peripheral devices that share a common communications line or wireless link to a server within a distinct geographic area	
	Logic bomb	Malicious code that activates when conditions are met	
LTE	Long-Term Evolution	(ex: 4G) wireless broadband communication for mobile devices	
UDP/TCP 515	LPD (Line Printer Daemon)	Printing port, unsecured	
TCP/UDP 515	LPD (Line Printer Daemon)	Printing port, unsecured	
ML	Machine Learning	Machine learning (ML) is a field of study in artificial intelligence concerned with the development and study of statistical algorithms that can learn from data and generalize to unseen data, and thus perform tasks without explicit instructions. Recently, artificial neural networks have been able to surpass many previous approaches in performance.	
MDF	Main Distribution Frame	Main Distribution Frame (MDF) is a signal distribution frame or cable rack used in telephony to interconnect and manage telecommunication wiring between itself and any number of intermediate distribution frames and cabling from the telephony network it supports.	
MITB/MIB	Man In The Browser		
MITM	Man In The Middle	On-path attacks	

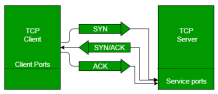
SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
PDU	Managed Power Distribution Units	Intelligent & remote power management	
MSSP	Managed Security Service Provider	Security monitoring, vulnerability management, incident response, and firewall management	
MSP	Managed Service Provider	Capable of working customer's total environment, on-premises and cloud	
MIB	management information base	where a MIB is listed	
	Managerial control (AKA risk management)	Risk assessments, securing planning exercises, change management	
MAC	Mandatory access controls	OS sets security policy, users cannot change security settings (rare setting, ex: SELinux)	
MIC	Mandatory Integrity Control	Mandatory Integrity Control is a system-enforced method of restricting access to and modification of objects based on the integrity of the object and the clearance of the user. While MAC is concerned with the sensitivity of an object, MIC is concerned with the object's trustworthiness.	
MBR	Master boot record	contains executable code to function as a loader for the installed operating system	
MSA	Master Service Agreements	umbrella contract for the work that a vendor does	
MTU	Maximum Transmission Unit	a measurement in bytes of the largest data packets that an Internet-connected device can accept.	
MTBF	Mean time between failure	Expected time between failures, measures reliability of a system	
MTTF	Mean time to failure		
MTTR	Mean time to recover	Average amount of time to restore	
MAC Address	Media Access Control	12-character code that identifies a device or network	
MOA	memorandum of agreement	formal document outlining the terms between parties, establishing roles and responsibilities. More detailed than MOUs	
MOU	Memorandum of Understanding	informal document laying out relationship with vendor	
MAC	message authentication code (AKA authentication tag)	short piece of information used for authenticating and integrity-checking a message. In other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed (its integrity). The MAC value allows verifiers (who also possess a secret key) to detect any changes to the message content.	
MIC	Message Integrity Code	The Message Integrity Code (MIC) is a security feature in the APS frame that is used to detect any unauthorized change in the content of the message. The term message integrity code (MIC) is frequently substituted for the term MAC, especially in communications[1] to distinguish it from the use of the latter as media access control address (MAC address)	
MD5	Message-Digest Algorithm	public key	
MAN	Metropolitan Area Network	a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings.	
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol		
RAID 1	Mirroring	When one drive fails, the other recovers. High reliability, easy setup, fast read performance. But reduced capacity, higher cost	
MAM	Mobile Application Management	software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business	
MCM	Mobile Content Management	Mananing and distributing enterprise files on mobile systems	
MDM	Mobile Device Management	Mobile device management is the administration of mobile devices, such as smartphones, tablet computers, and laptops. MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices.	
MaaS	Monitoring as a Service		
	Monolithic Applications	One app for everything	
	Moore's Law	Moore's law is the observation that the number of transistors in an integrated circuit (IC) doubles about every two years. Moore's law is an observation and projection of a historical trend. Rather than a law of physics, it is an empirical relationship linked to gains from experience in production.	
	Multi-cloud	Business will continue even if one cloud vendor has a problem	
MFA	Multi-Factor Authentication	Something you have, something you are, something you know	
MPLS	Multi-protocol label switching	SD-WAN, 4G, 5G. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. MPLS can encapsulate packets of various network protocols, hence the multiprotocol component of the name	
MFD	Multifunction Device		
MFP	Multifunction peripheral	A device that performs a variety of functions that would be otherwise carried out by seperate devices (ex: printer, scanner, copier, fax machine). Con: can act as reflectors, amplifiers, and pivot points for attackers	
TCP 777	multiling-http	Trojans use this port	
TCP 777	multiling-http	Trojans use this port	
MMS	Multimedia Message Service	standard way to send messages that include multimedia content to and from a mobile phone over a cellular network	
MIME	Multipurpose Internet Mail Extensions	It lets users exchange different kinds of data files, including audio, video, images and application programs, over email	
NIST	National Institute of Standards and Technology	Provides standards for many products and standards, makes the NVD	
NSA	National Security Agency		
NVD	National Vulnerability Database	Lists all of the CVEs	
NFC	Near-field communication	very short-range communication (4 inches) between devices (ex: Apply Pay, Google Pay)	
	Nearline Backups	Not immediately available but can be retrieved. Pro: faster than offsite. Con: slower than onsite. (ex: Amazon's S3, Google's Coldline storage)	
Nessus	Nessus Vulnerability Scanner	Nessus is a proprietary vulnerability scanner developed by Tenable, Inc	
NetFlow v9	NetFlow Version 9	NetFlow services provide network administrators with access to information concerning IP flows within their data networks	
NAC	Network Access Control	the process of restricting unauthorized users and devices from gaining access to a corporate or private network.	
NAT	Network Address Translation	A Network Address Translation (NAT) is the process of mapping an internet protocol (IP) address to another by changing the header of IP packets while in transit via a router. This helps to improve security and decrease the number of IP addresses an organization needs.	
NTP	Network Time Protocol	Synchronizes clocks of computer systems (insecure)	
NAS	Network-Attached Storage		
NIDS	Network-based IDS	A network-based intrusion detection system (NIDS) detects malicious traffic on a network. NIDS usually require promiscuous network access in order to analyze all traffic, including all unicast traffic	
NIPS	Network-based IPS	Network-based IPS —> monitors the entire network	
NTFS	New Technology File System	the file system that the Windows NT operating system (OS) uses for storing and retrieving files on hard disk drives (HDDs) and solid-state drives (SSDs)	
NGFW	Next gen firewalls	all-in-one-network security devices (deep packet inspection, IDS/IPS, AV) —> faster than UTMs because focused but more config time	
	Nexus	A connection or link between things, persons, or events in part of a chain of causation	
	NIST Cybersecurity Framework Implementation tiers	Tier 1: Partial Tier 2: Risk Informed Tier 3: Repeatable Tier 4: Adaptive	
	NIST Framework Core	Identify Protect Detect Respond Recover	
0	No permission	- - -	
NDA	Non-disclosure Agreement		
	Non-persistent/Reflected XSS (Type 1 XSS)	Injecting HTML code into error message and the website unknowingly spits it right back	
	Nonpersistance	Ability to have systems or services that are spun up and shut down as needed	
	Nonrepudiation	Digital signature, cannot deny it was sent from you	

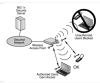
SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
	NTLM pass-the-hash attack	Steals hash and tries to unlock stuff with it, doesn't require the attacker to gain any credentials	
XORed	Numerically combined		
OID	Object Identifier	In computing, object identifiers or OIDs are an identifier mechanism standardized by the International Telecommunication Union (ITU) and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name	
OSCP	Offensive Security Certified Professional	an ethical hacking certification offered by Offensive Security (or OffSec) that teaches penetration testing methodologies and the use of the tools included with the Kali Linux distribution	
OTP	One Time Password	Makes brute force harder, dynamically made	
OCSP	Online Certification Status Protocol	Faster and real-time verification	
OAuth	Open Authorization	Opn standard for authorizing websites via SSO (ex: web conferencing tools using google calendar). Handles authorization of access to protected resources	
OpenID	Open Identity	Open standard for decentralized authentication (ex: sign in with Google)	
OSPF	Open Shortest Path First	Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. OSPF is a link-state routing protocol providing fast convergence and excellent scalability.	
OSINT	Open Source Intelligence		
OSI	Open Systems Interconnection Model	Layer 7: The application layer Layer 6: The presentation layer Layer 5: The session layer Layer 4: The transport layer Layer 3: The network layer Layer 2: The data-link layer Layer 1: The physical layer	
OVAL	Open Vulnerability and Assessment Language	Open Vulnerability and Assessment Language (OVAL) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language. The OVAL community has developed three schemas written in Extensible Markup Language (XML) to serve as the framework and vocabulary of the OVAL Language. Taken over by CIS	
OWASP	Open Worldwide Application Security Project	hosts community-developed standards/best guides	
IdP	OpenID Identity Providers	Google, Facebook, Amazon, etc	
OS	Operating System	An operating system (OS) is system software that manages computer hardware and software resources, and provides common services for computer programs.	
	Operational controls (AKA processes)	Access reviews, log monitoring, vulnerability management	
OT	Operational Technology	Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.	
OWE	Opportunistic wireless encryption	provide encrypted Wi-Fi on open networks when possible	
	Orchestration	Orchestration allows you to share information easily, enabling multiple tools to respond to incidents as a group, even when the data is spread across a large network and multiple systems or devices	
	Order of Volatility	What data is most likely to be lost to due to normal processes: CPU cache and registers Ephemera data: kernel statistics, ARP cache, process table System memory - RAM Temporary files and swap space Data on the disk OS Devices, IoT devices Firmware Snapshots from VMs Remote logs Backups	
OASIS	Organization for the Advancement of Structured Information Protocol	OASIS Cyber Threat Intelligence (CTI) TC, non-profit that maintains XML & HTML	
	Organized Crime	Ransomware, child sexual abuse material, online fraud, dark web	
OSI L1	OSI Layer 1: Physical Layer	Transmits raw bit stream over the physical medium	
OSI L2	OSI Layer 2: Data link layer	Defines the format of the data on the network	
OSI L3	OSI Layer 3: Network Layer	Decides which physical path the data will take. Examples: Firewalls, IPSec	
OSI L4	OSI Layer 4: Transport Layer	Transmits data using the transmission protocols including TCP and UDP	
OSI L5	OSI Layer 5: Session Layer	Maintains connections and is responsible for controlling ports and sessions	
OSI L6	OSI Layer 6: Presentation layer	Ensures that data is in a useable format and is where data encryption occurs	
OSI L7	OSI Layer 7: Application Layer	Human-computer interaction layer, where applicatiosn can access network services	
OOBM	Out of bound management	remotely access and manage devices and infrastructure	
OTA	Over-the-air	wireless delivery of data, software or firmware to mobile devices	
PCAP	Packet Capture	Packet capture is a networking practice involving the interception of data packets travelling over a network. Once the packets are captured, they can be stored by IT teams for further analysis	
PMK	Pairwise Master Key	The pairwise master key (PMK) is a 256-bit key at the top of the key hierarchy and is used indirectly for unicast traffic and the WPA 4-way handshake. The wireless client and AP have the PMK, which should last the entire session, so it should not be exposed. To accomplish this, we use different keys derived from the PMK.	
PTK	pairwise transient key	The Pairwise Transient Key (PTK) is used for encryption and integrity checks in unicast user data. It is also used for protecting the 4-way handshake. Here's how to visualize this:	
PTZ	Pan-tilt-zoom		
	Parameters Queries	Sends parameters and not code to databases to prevent injection	
RAID 5	Parity	Pros: Balance between RAID 0 and RAID 1. Efficient storage capacity can withstand the loss of a single drive. Cons: performance is impacted a bit, may fail during rebuild performance	
PAP	Password Authentication Protocol	Two-way handshake, password-based authentication protocol used by Point-to-Point Protocol to validate users. PAP is specified in RFC 1334. Almost all network operating systems support PPP with PAP, as do most network access servers. PAP is also used in PPPoE, for authenticating DSL users.	
	Password spraying	One password, many accounts	
	Password vaulting	Access privileged accounts without knowing the password	
PBKDF2	Password-based Key Derivation Function 2	In cryptography, PBKDF1 and PBKDF2 (Password-Based Key Derivation Function 1 and 2) are key derivation functions with a sliding computational cost, used to reduce vulnerability to brute-force attacks	
PCI DSS	Payment Card Industry Data Security Standards		
PFI	PCI Forensic Investigator	help determine the occurrence of a cardholder data compromise and when and how it may have occurred.	
P2P	Peer-to-peer	Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers	
	Pen Testing	White hat hacker, first-hand knowledge, constructive feedback, focused information on specific attack targets	
PFS	Perfect Forward Secrecy	also known as Forward Secrecy, is an encryption style known for producing temporary private key exchanges between clients and servers. For every individual session initiated by a user, a unique session key is generated. If one of these session keys is compromised, data from any other session will not be affected. Therefore, past sessions and the information within them are protected from any future attacks.	

SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
PED	Personal Electronic Device	Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders.	
PHI	Personal Health Information	Subject to HIPAA	
PII	Personal Identifiable Information		
PIV	Personal Identity Verification	The logical record containing credentialing information for a given PIV cardholder. This is stored within the issuer's identity management system and includes PIV enrollment data, cardholder identity attributes, and information regarding the cardholder's PIV Card and any derived PIV credentials bound to the account.	
PFX	Personal Information Exchange	password protected file certificate commonly used for code signing your application, Windows systems using .pfx or .p12 file	
	Pharming	Redirects victim to lookalike site by attacking system's host file	
	Phising	Fraudulent acquisition of information	
	Physical controls	Fences, lighting, locks, fire suppression, alarms	
P12	PKCS #12	In cryptography, PKCS #12 defines an archive file format for storing many cryptography objects as a single file In cryptography, PKCS #12 defines an archive file format for storing many cryptography objects as a single file. It is commonly used to bundle a private key with its X.509 certificate or to bundle all the members of a chain of trust.	
POTS	Plain Old Telephone Service	Plain Old Telephone Service (POTS) refers to the traditional, analog voice transmission phone system implemented over physical copper wires (twisted pair). Simply put, POTS is the basic telephone call service that individuals and businesses have been using since the 1880s.	
P	Plaintext		
PaaS	Platform as a service	Responsible for Hardware, Datacenter, and OS	
PAM	Pluggable Authentication Modules	Applications enabled to make use of PAM can be plugged-in to new technologies without modifying the existing applications. This flexibility allows administrators to do the following: Select any authentication service on the system for an application Use multiple authentication mechanisms for a given service Add new authentication service modules without modifying existing applications Use a previously entered password for authentication with multiple modules	
PPP	Point-to-Point Protocol	suite of computer communication protocols that provide a standard way to transport multiprotocol data over point-to-point links (outdated)	
PPTP	Point-to-Point Tunneling Protocol	The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private networks. PPTP has many well known security issues.	
PA	Policy Administrators	Establish or remove communication between subjects and resources	
PDP	Policy Decision Point		
PEP	Policy Enforcement Points	Communicate with policy admins to forward requests between subjects and receive instructions	
PE	Policy Engines	Makes policy decisions	
	Polygraphic Substitution	Shifting letters around even more	
UDP/TCP 110	POP3 (Post Office Protocol Version 3)	First port for sending email. Unsecure, unencrypted, use 995 instead	
TCP/UDP 110	POP3 (Post Office Protocol Version 3)	First port for sending email. Unsecure, unencrypted, use 995 instead	
PAT	Port Address Translation	Port address translation (PAT) is a type of network address translation (NAT) that maps a network's private internal IPv4 addresses to a single public IP address. NAT is a process that routers use to translate internal, nonregistered IP addresses to external, registered IP addresses. PAT differs from other forms of NAT because it uses port numbers when mapping private IP addresses to a public IP address, which is the address seen by external systems.	
POP3	Post Office Protocol 3	Post Office Protocol 3, or POP3, is the most commonly used protocol for receiving email over the internet. This standard protocol, which most email servers and their clients support, is used to receive emails from a remote server and send to a local client.	
PQC	Post Quantum Cryptography	also known as quantum encryption, is the development of cryptographic systems for classical computers that can prevent attacks launched by quantum computers. In the 1980s, scientists speculated that if computers could take advantage of the unique properties of quantum mechanics, they could perform complicated computations faster than classical, binary computers. It quickly became clear that a quantum computer, taking advantage of quantum properties such as superposition and entanglement, could complete certain types of complex calculations in a matter of hours -- something that would take a classical computer several years to complete.	
PQ3	post-quantum cryptographic protocol	On February 21, 2024, Apple announced that they were going to upgrade their iMessage protocol with a new PQC protocol called "PQ3", which will utilize ongoing keying.[81][82][83] Apple stated that, although quantum computers don't exist yet, they wanted to mitigate risks from future quantum computers as well as so-called "Harvest now, decrypt later" attack scenarios. Apple stated that they believe their PQ3 implementation provides protections that "surpass those in all other widely deployed messaging apps, because it utilizes ongoing keying. Apple intends to fully replace the existing iMessage protocol within all supported conversations with PQ3 by the end of 2024. Apple also defined a scale to make it easier to compare the security properties of messaging apps, with a scale represented by levels ranging from 0 to 3.[81]	
PUP	Potentially Unwanted Program	AKA Bloatware	
PSK	Pre-shared Key	a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. PSK is used in Wi-Fi encryption such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), where the method is called WPA-PSK or WPA2-PSK, and also in the Extensible Authentication Protocol (EAP), where it is known as EAP-PSK.	
PICERL	Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned	Incident response process by SANS	
	Pretexting	Made-up scenario to justify	
PGP	Pretty Good Privacy	popular program used to encrypt and decrypt email over the internet, as well as authenticate messages with digital signatures and encrypted stored files	
	Principal	User in federation	
PEM	Privacy Enhanced Mail	Text-version of DER format. Stored in .pem, or .crt extension	
PBX	Private Branch Exchange	A private branch exchange (PBX) is a telephone system within an enterprise that switches calls between users on local lines, while enabling all users to share a certain number of external phone lines. In contrast to a public switched telephone network, the main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.	
	private key	AKA Symmetric key cryptography	
PAM	Privileged Access Management	Tools for ensuring least privilege	
PEAP	Protected EAP	authenticates servers using certificates and wraps EAP using TLS tunnel	
PAC	Proxy Auto Configuration	A proxy auto-config (PAC) file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL.	
	Proxy servers	Accept and forward	
	public key	AKA Asymmetric key cryptography	
PKI	Public Key Infrastructure	the underlying framework that enables entities -- users and servers -- to securely exchange information using digital certificates	
PKCS	Public-Key Cryptography Standards	Public-Key Cryptography Standards (PKCS) are a set of standard protocols, numbered from 1 to 15. These standards were developed to enable secure information exchange on the internet by using a public key infrastructure (PKI).	
QA	Quality Assurance (during manufacturing)	Test environment	
	Quantum Computers	Will break most known cryptographic systems, such as DSA, DH, RSA. ECC is considered more safe	
QC	Quantum Cryptography	Quantum cryptography is a method of encryption that uses the naturally occurring properties of quantum mechanics to secure and transmit data in a way that cannot be hacked.	
QKD	Quantum Key Distribution	Quantum key distribution (QKD) is a secure communication method for exchanging encryption keys only known between shared parties. It uses properties found in quantum physics to exchange cryptographic keys in such a way that is provable and guarantees security. QKD enables two parties to produce and share a key that is used to encrypt and decrypt messages. Specifically, QKD is the method of distributing the key between parties.	
	Quantum Supremacy	the experimental demonstration of a quantum computer's dominance and advantage over classical computers by performing calculations previously impossible at unmatched speeds. To confirm that quantum supremacy has been achieved, computer scientists must be able to show that a classical computer could never have solved the problem while also proving that the quantum computer can perform the calculation quickly	
	Qubit (Quantum Bit)	A qubit (short for quantum bit) is the basic unit of information in quantum computing and counterpart to the bit (binary digit) in classical computing. A qubit plays a similar role as a bit, in terms of storing information, but it behaves much differently because of the quantum properties on which it's based.	
RFID	Radio Frequency ID	Uses a tag and a receiver which includes: active tags, semi-active tags, and passive tags	
RAID 0	RAID 0 - Striping	Pros: Exceptional performance due to parallel data access, cost-effective. Cons: 0 redundancy or fault tolerance.	

SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
RAID 6	RAID 6: double-parity RAID	Pros: offers higher fault tolerance than RAID 5. Cons: write performance is impacted	
	Rainbow table attacks	Creating a hash collision (AKA birthday attack)	
	Ransomware	Holding data for ransom	
RAD	Rapid Application Development	In software development, rapid application development (RAD) is a concept which emphasizes working on software and being more adaptive than older development methods. RAD was born out of frustration with the waterfall software design approach which too often resulted in products that were out of date or	
TCP 3389	RDP (Remote Desktop Protocol)	Microsoft's RDP, officially listed as Windows-Based Terminal (WBT)	
TCP 3389	RDP (Remote Desktop Protocol)	Microsoft's RDP, officially listed as Windows-Based Terminal (WBT)	
4	Read	r--	
5	Read + Execute	r-x	
6	Read + Write	rw-	
7	Read + Write + Execute	rwx	
RTOS	Real-time operating system	Ex: car	
RTP	Real-time Transport Protocol	network standard designed for transmitting audio or video data that is optimized for consistent delivery of live data. It is used in internet telephony, Voice over IP and video telecommunication. It can be used for one-on-one calls (unicast) or in one-to-many conferences (multicast).	
ROC	Receiver Operating Characteristic	The ROC curve can be used to visualize the difference between normal and abnormal test results. It connects points with 1 - specificity (false positive rate) on the x-axis and sensitivity on the y-axis	
RA	Recovery Agent		
RPO	Recovery Point Objective	How much data loss is acceptable	
RTO	Recovery Time Objective	How long the recovery can take	
	Red Hat	Red Hat, Inc. is an American software company that provides open source software products to enterprises and is a subsidiary of IBM. Founded in 1993, Red Hat has its corporate headquarters in Raleigh, North Carolina, with other offices worldwide	
RAID	Redundant Array of Independent Disks		
	Reflected DoS Attack	spoofing IP address to conduct an attack	
	Region	Set of connected data centers	
RA	Registration Authorities	Help CAs verify identities before digital signing	
RP	Relying Parties	Redirect it to the IdPs	
RAS	Remote Access Server	A remote access server (RAS) is a type of server that provides a suite of services to remotely connected users over a network or the Internet	
RADIUS	Remote Authentication Dial-In User Service	Most common AAA systems of networks, system, etc. Sends passwords via shared secret and MD5 hashed passwords	
RDP	Remote Desktop Protocol	a secure network communications protocol developed by Microsoft. It enables network administrators to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers	
RTU	Remote Telemetry Units	Microprocessors collecting data for SCADA	
RTBH	Remotely Triggered Black Hole	Remotely triggered black hole (RTBH) filtering is a technique that provides the ability to drop undesirable traffic before it enters a protected network.	
	Replay Attack	(also known as a repeat attack or playback attack) is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a spoofing attack by IP packet substitution. This is one of the lower-tier versions of a man-in-the-middle attack. Replay attacks are usually passive in nature.	
	Replication	Synchronous (real-time) or asynchronous (after-the-fact) methods of copying data	
RFC	Requests for Comment	Official specification for a technology	
RACE	Research and Development in Advanced Communications Technologies in Europe	Promote competitiveness of the EU's telecommunications industry	
	Responsible Disclosure Programs	Bug bounty programs	
RARP	Reverse Address Resolution Protocol (Obsolete)	Client computer requests its IP address from a network when it has a MAC address, replaced by DHCP	
RCS	Rich Communication Services	new version of SMS, allows for more data connection via text like video, pictures, GIFs, etc	
RMF	Risk Management Framework	formal process for implementing security controls and authorizing system use	
RC4	Rivest Cipher 4	In cryptography, RC4 (Rivest Cipher 4, also known as ARC4 or ARCFOUR, meaning Alleged RC4, see below) is a stream cipher. While it is remarkable for its simplicity and speed in software, multiple vulnerabilities have been discovered in RC4, rendering it insecure.	
RSA	Rivest-Shamir-Adleman (RSA)	A public-key aymmetric key signature algorithm developed in 1977. It the basis of a cryptosystem -- a suite of cryptographic algorithms that are used for specific security services or purposes – which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet. It provides a method to assure the confidentiality, integrity, authenticity, and non-repudiation of electronic communications and data storage. Public key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys -- one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. Strengthened with 2048-bit key lengths SSH, OpenPGP, SSL/TLS rely on RSA	
RSN	Robust Secure Network	RSN (Robust Secure Network) is a protocol for establishing secure communications over an 802.11 wireless network. RSN (Robust Secure Network) is part of the 802.11i standard.	
	Rogue Access Points		
RBAC	ROLE-Based Access Control	Roles are matched with privileges, popular with enterprises, dynamic and good for ZTA	
	Root CAs	Protected by offline CA (like proxy servers)	
RCA	Root Cause Analysis	Ask five why's, event analysis, diagramming cause and effect	
	Rootkit	Infects the MBR	
RuBAC	RULE-Based Access Control	Set of rules that apply to various objects or resources (ex: firewall ruleset). It is not as dynamic as RBAC	
RoE	Rules of Engagement	Defining permitted scope in	
	Salting	Adding random generated values to each password prior to hashing	
sFlow	Sampled Flow	collect IP traffic as it enters or exits interface, developed by Cisco in 1996 —> tracks bandwidth utilization	
	Sandboxing	Controlled test environments	
SANS	SANS Institute	The SANS Institute is a private U.S. for-profit company founded in 1989 that specializes in information security, cybersecurity training, and selling certificates. Topics available for training include cyber and network defenses, penetration testing, incident response, digital forensics, and auditing	
SANS SIFT	SANS SIFT Workstation	The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings	
SOX	Sarbanes-Oxley Act	Strong security for publicly traded companies financial records	
	Scalability	Support demand as needed	
	Script Kiddie	Unskilled attacker	
SASE	Secure Access Service Edge	Private networks + SD-WAN + firewalls + CASBs + ZTA → secure access for devices regardless of location	
	Secure Enclave	Apple's version of a TPM	
SHA	Secure Hash Algorithm	SHA-1, SHA-2, SHA-3 (current)	
SHS	Secure Hash Standard	AKA FIPS 180, created by NIST	
SHTTP	Secure Hypertext Transfer Protocol	Secure Hypertext Transfer Protocol (S-HTTP) is an obsolete alternative to the HTTPS protocol for encrypting web communications carried over the Internet. It was developed by Eric Rescorla and Allan M. Schiffman at EIT in 1994 and published in 1999 as RFC 2660	
SRTP	Secure Real-time Transport Protocol	an extension to RTP (Real-Time Transport Protocol) that incorporates enhanced security features	
SSH	Secure Shell	Protocol for remote console access to devices. Also tunneling protocol	
SFTP	Secure Shell File Transfer Protocol	Secure File Transfer Protocol (SFTP) is a network protocol for securely accessing, transferring and managing large files and sensitive data. Designed by the Internet Engineering Task Force as an extension of Secure Shell (SSH), SFTP enables access, transfer and management of files over a network. Slower than FTPS but more secure, and thus more widely adopted	
SSL	Secure Sockets Layer	It used the same cryptographic keys for message authentication and encryption	
SWG	Secure Web Gateway	A secure web gateway (SWG) is an on-premises or cloud-delivered network security technology that filters internet traffic and enforces corporate and regulatory policy compliance.	
S/MIME	Secure/Multipurpose internet Mail Extensions	widely accepted protocol for sending digitally signed and encrypted messages	
SAML	Security Assertion Markup Languages	XML-based open standard for exchanging authentication and authorizing information, used for identity providers	
	Security Assessments	Comprehensive review of a system's security (internal use only)	
SA	Security Associations	Bulding block where are the secure communications is built	
	Security Attestation Letter	Formal state that proves the safety and security of a system	
	Security Audit	Independent authors (potentially public)	
SCT	Security Compliance Toolkit	Security baseline config	
SCAP	Security Content Automation Protocol	Standardized communication approach for security info (created by NIST)	
	Security controls	Specific measures to achieve control objectives	
SIEM	Security Incident and Event Management	The main dashboard and tool SOC teams use	
SIM	Security Information Management	the practice of collecting, monitoring and analyzing security-related data from computer logs and various other data sources, evolved into SIEM	
	Security Key	Hardware devices	

SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
SOC	Security Operations Center		
SOAR	Security Orchestration, Automation, and Response	Automating responses, learn of emerging threats, scans.	
SPI	Security Paramters Index	an identifier used to uniquely identify both manually and dynamically established IPSec	
SSP	Security Simple Pairing	Security Mode 4 for Bluetooth	
STAR	Security Trust, Assurance, and Risk	Technology-neutral certification. L1: self-assessment. L2: third-party audit. L3: continuous auditing.	
SE Linux	Security-Enhanced Linux	Linux kernel based security module that provides more capabilities than a traditional Linux	
	Segmentation	Placing sensitive systems on separate networks	
SED	Self-Encrypting Drives	type of hard drive that automatically and continuously encrypts the data on the drive without any user interaction	
SMART	Self-Monitoring, Analysis, and Reporting Technology	ASR Data's format for their SMART forensic tool	
SPF	Sender Policy Framework	Allow list for email domains. If not on the list → rejected	
SSRF	Server-side request forgery	Tricking a server to visit a URL based on user-supplied input. Possible when web app accepts URLs as input	
SLA	Service Level Agreement	contracts that specify conditions of service will be provided by vendor	
SP	Service Provider (in Federation)	Provides services to IdPs who have been attested to	
	Session Hijacking	Taking over control of a user's web session	
SIPS	Session Initiation Protocol [Secured]	The Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, and terminating communication sessions that include voice, video and messaging applications	
	Session Replay Attack	Attack replays the website's session as the user	
	Shadow IT	Unapproved IT tech	
	Shor's Algorithm	Shor's algorithm is a quantum algorithm for finding the prime factors of an integer. It was developed in 1994 by the American mathematician Peter Shor.[1][2] It is one of the few known quantum algorithms with compelling potential applications and strong evidence of superpolynomial speedup compared to best known classical (that is, non-quantum) algorithms.[3] On the other hand, factoring numbers of practical significance requires far more qubits than available in the near future.[4] Another concern is that noise in quantum circuits may undermine results,[5] requiring additional qubits for quantum error correction.	
SMS	Short Message Service	commonly referred to as "text messaging," is a service for sending short messages of up to 160 characters (224 character limit if using a 5-bit mode) to mobile devices, including cellular phones and smartphones.	
	Sideloading		
SCEP	Simple Certificate Enrollment Protocol	The protocol has been designed to make the request and issuing of digital certificates as simple as possible for any standard network user. The Simple Certificate Enrollment Protocol still is the most popular and widely available certificate enrollment protocol	
SMTP	Simple Mail Transfer Protocol	an Internet standard communication protocol for electronic mail transmission	
SMTPS	Simple Mail Transfer Protocol Secure	It is a way to secure SMTP at the transport layer, by wrapping SMTP inside Transport Layer Security (TLS). Conceptually, it is similar to how HTTPS wraps HTTP inside TLS.	
SNMP	Simple Network Management Protocol	monitor and manage network devices on a LAN or WAN	
SNMPv3	Simple Network Management Protocol version 3	authenticating message sources, message integrity validation, and confidentiality	
SOAP	Simple Object Access Protocol	SOAP (Simple Object Access Protocol) is a message protocol that enables the distributed elements of an application to communicate. SOAP can be carried over a variety of standard protocols, including the web-related Hypertext Transfer Protocol (HTTP).	
SAE	Simultaneous Authentication of Equals (AKA Dragonfly Key Exchange)	requires client/network to validate both sides	
SLE	Single Loss Expectancy	AV * EF, amount of financial damage expected from each time risk materializes	
SPOF	Single Point of Failure		
SSO	Single sign-on	Authentication protocol	
IPSec VPN	Site-to-site VPN	Tunnel or transport mode. For VPNs that need more than web and app traffic	
TCP 445	SMB (Server Message Block)	Microsoft's networking port. Should not be open to the public. Allows sharing files and printers over the network. Blocking will prevent file and printer sharing	
TCP 445	SMB (Server Message Block)	Microsoft's networking port. Should not be open to the public. Allows sharing files and printers over the network. Blocking will prevent file and printer sharing	
TCP 25	SMTP (Simple Mail Transfer Protocol), sending email	Unsecured, unencrypted. Use Port 587 instead	
TCP 25	SMTP (Simple Mail Transfer Protocol), sending email	Unsecured, unencrypted. Use Port 587 instead	
	Smurf attacks	spoofed sender address via ICMP broadcast messages	
	Snapshot	Captures the full state of a system when the backup is completed (common for VMs). Pro: captured live. Con: consumes a lot of storage	
UDP/TCP 161	SNMP (Simple Network Management Protocol)	Used for network management, unsecured. SNMPv3 is secure but not by much	
TCP/UDP 161	SNMP (Simple Network Management Protocol)	Used for network management, unsecured. SNMPv3 is secure but not by much	
	SNMP Trap	Message when device encounters an error	
SaaS	Software as a service	Responsible for Hardware, Datacenter, OS, and Application	
SDK	Software Development Kits	Set of platform-specific building tools for developers	
SDLC	Software development lifecycle	1-Planning, 2-Requirements, 3-Design, 4-Coding, 5-Testing, 6-Training and Transition, 7-Ongoing Operations, 8-End of Life/Decommissioning	
SDN	Software-Defined Networking	Allows engineers to interact and modify cloud resources via APIs	
SDV	Software-Defined Visibility	Traffic insight on virtual networks	
SD-WAN	Software-defined Wide Area Network	Virtual wide area network design that combines many services for organizations	
SSD	Solid State Drive		
SNAT	Source Network Address Translation	a technique that translates source IP address generally when connecting from private IP address to public IP address. It maps source client IP address in a request to a translation defined on BIG-IP device. It is most common form of NAT that is used when internal host needs to initiate session to an external host or public host.	
802.1D	Spanning Tree Protocol (STP)	Ethernet MAC bridges standard which includes bridging, Spanning Tree Protocol and others. Loop protection mechanism	
802.1D	Spanning Tree Protocol (STP)	Ethernet MAC bridges standard which includes bridging, Spanning Tree Protocol and others. Loop protection mechanism	
	Spear phishing	Targeted phishing	
SPIM	SPIM	SPIM is a MIPS processor simulator, designed to run assembly language code for this architecture. The program simulates R2000 and R3000 processors, and was written by James R. Larus while a professor at the University of Wisconsin–Madison	
	Spyware	Stalkerware, associated with identity fraud	
TCP 1433	SQL	Microsoft's SQL server, needs to be secured	
TCP 1433	SQL	Microsoft's SQL server, needs to be secured	
UDP 5004	SRTP (Secure Real-Time Protocol)	Provides audio and video streams via network. A secure alternative to RTP	
UDP 5004	SRTP (Secure Real-Time Protocol)	Provides audio and video streams via network. A secure alternative to RTP	
TCP 22	SSH	Secure AF (unless you mishandle keys/passwords)	
TCP 22	SSH	Secure AF (unless you mishandle keys/passwords)	
	Staging	Transition environment	
	Stateful Firewalls	(AKA dynamic packet filters) track packets, make smart decisions	
SLAAC	Stateless Address Autoconfiguration	Includes a "privacy address" or "temporary addresses" for IP address privacy	
	Stateless Firewalls	(AKA packet filters) Most basic firewall, filters every packet's header	
SOW	Statement of Work	project-specific details and references to MSAs	
	Static Codes	algorithmically generated, stored in a secure location, but can be compromised	
	Static Testing	Analyzing code without executing it	
STA	Station Nonce	a random number generated by a supplicant, or client, in the 802.11 standard	
	Steganography	Art of using cryptographic techniques to obscure secret messages in another file	
SAN	Storage Area Network	Multiple computers or servers	
SPC	Stored Program Control	Stored program control (SPC) is a telecommunications technology for telephone exchanges. Its characteristic is that the switching system is controlled by a computer program stored in a memory in the switching system. SPC was the enabling technology of electronic switching systems (ESS) developed in the Bell System in the 1950s, and may be considered the third generation of switching technology. Stored program control was invented in 1954 by Bell Labs scientist Erna Schneider Hoover, who reasoned that computer software could control the connection of telephone calls	
	Stored/Persistent XSS (Type 2 XSS)	Waiting for the site to interact with malicious code (ex: leaving malicious HTML code in blog comments)	
	Stream ciphers	One character or a bit at a time (ex: Caesar's cipher)	

SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
SCTP	Stream Control Transmission Protocol (AKA "next gen TCP")	a computer networking Transport Layer protocol, serving in a similar role as the popular TCP/UDP protocols. It provides some of the same service features of both, ensuring reliable, in-sequence transport of messages with connection control	
SEH	Structured Exception Handler	Structured exception handling (SEH) is a Microsoft extension to C and C++ to handle certain exceptional code situations, such as hardware faults, gracefully	
SQL	Structured Query Language	a programming language for storing and processing information in a relational database	
SQLi	Structured Query Language Injection	A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.	
STIX	Structured Threat Information of eXpression	XML language describing the attack in a STIX JSON	
SAN	Subject Alternative Name	A Subject Alternative Name (SAN) is a field in an X.509 certificate that identifies domain names, IP addresses, email addresses, URIs, or UPNs. SANs are used to specify additional hostnames for individual SSL certificates. They are a common practice for SSL certificates and are replacing common names.	
SME	Subject Matter Experts		
	Subjects	Users in ZTA	
SIM	Subscriber Identity Module	Subkect to SIM cloning, physically removing	
	Substitution cipher	Cipher that substitutes one character for another (ex: Julius Caesar's letters)	
SCADA	Supervisory Control and Data Acquisition	Large industrial systems (ex: power plants, manufacturing, water plants)	
SCP	Supply Chain Planning	Supply chain planning (SCP) is the process of anticipating the demand for products and planning their materials and components, production, marketing, distribution and sale. Its overall goal is to balance supply and demand, so sales revenue opportunities are fully exploited in a timely manner and at the lowest possible cost.	
	Symmetric Key Encryption Algorithms	Examples: DES, AES, RC4, DH. Also called secret key cryptography or private key cryptography. The number of keys is calculated by: (n (n-1)) / 2	
SoC	System on a Chip	an integrated circuit that integrates most or all components of a computer or other electronic system	
0-1023	System Ports		
TTP	Tactics, techniques, and procedures		
0-1023	TCP System Ports		
	Technical controls	Firewall rules, access control lists, IPS, and encryption	
SSL VPN	Technically TLS VPN	Portal-based (HTML 5), tunnel mode, no client installation required	
TRUST	Tell your story, ready your team, Understand and assess MDM, Strategize response, track outcomes	CISA's model for countering phishing	
TCP 23	Telnet	Unsecure	
TCP 23	Telnet	Unsecure	
TKIP	Temporal Key Integrity Protocol	security protocol used in the IEEE 802.11 wireless networking standard. TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as an interim solution to replace WEP without requiring the replacement of legacy hardware unlike WEP, TKIP encrypts each data packet with a unique encryption key. Also, TKIP's keys are much stronger than those of its predecessor.	
TACACS+	Terminal Access Controller Access Control System Plus	Provides AAA via TCP, allows for individual commands. Designed by Cisco	
MITRE	The MITRE Corporation	MITRE is a government-funded research organization that provides technical and engineering guidance to the United States Air Force. It was spun off from MIT in 1958, but the name is not an acronym	
	Threat Hunting	Looking for attacks hiding in secret	
	Threat maps	Geographic view of threat intelligence (unreliable)	
	Three-way Handshake (TCP 3-way handshake)	Step 1 (SYN): In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer	
TGT	Ticket Granting Ticket	The ticket for the full ticket-granting service is called a ticket-granting ticket (TGT). When the client asks the KDC for a ticket to a server, it presents credentials in the form of an authenticator message and a ticket — in this case a TGT — just as it would present credentials to any other service. The ticket-granting service opens the TGT with its master key, extracts the logon session key for this client, and uses the logon session key to encrypt the client's copy of a session key for the server.	
TOC/TOU	Time of check to time of use	If someone is logged on already and permission is removed…well too bad. They have that resource forever	
TOE	Time of Evaluation	Being evaluated for potential vulnerabilities	
TOTP	Time-based One Time Password	uses algorithms to derive an OTP and then moves on (ex: Authenticator app)	
TOC	Time-of-Check	Instance when the system verifies permissions	
TOU	Time-of-Use	The moment when system accesses the resource	
TCO	Total Cost of Ownership	The mitigation cost: upfront costs + ongoing costs (nromallly operational)	
	Traits	Inherent to subject (hair, skin, eye color)	
TSIG	Transaction Signature	Primarily it enables the Domain Name System (DNS) to authenticate updates to a DNS database	
TCP/IP	Transmission Control Protocol/Internet Protocol	The suite of communications protocols (the main ones being TCP and IP) used to connect hosts on the Internet. TCP/IP is used by the Internet, making it the de facto most widely spread standard for transmitting data over networks. TCP and IP were developed by a DOD (Department of Defense) research project to connect a number different networks designed by different vendors into a network of networks (the Internet).	
EAP-TLS	Transport Layer Security	Still considered one of thre most secure EAP standards, implements certificate-based authentication as well as mutual authentication	
TLS	Transport Layer Security	cryptographic protocol designed to provide communications security over a computer network	
	Transposition Ciphers	Scrambling letters in a certain manner	
3DES	Triple DES	replacement for DES. It essentially applies DES three times with three different keys, thus the name 3DES.	
	Trojan	Disguised as legitimate software	
TAXII	Trusted Automated eXchange of Intelligence Information protocol	Method of transport for STIX, communication via HTTPS	
TPM	Trusted Platform Module	Dedicated computer chipto perform and store cryptographic information	
EAP-TTLS	Tunneled Transport Layer Security	Extends EAP-TLS, does not require client devices to have a certificate to create a secure session by requiring software	
UEM	Unified Endpoint Management	software that enables IT and security teams to monitor, manage and secure all of an organization's end-user devices, such as desktops and laptops, smartphones, tablets, wearables and more, in a consistent manner with a single tool, regardless of operating system or location.	
UEFI	Unified Extensible Firmware Interface	Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to eventually replace basic input/output system (BIOS) but is compatible with it.	
UTM	Unified Threat Management	firewall, IDS/IPS, AV, URL/email filtering, DLP, analytics —> "out of the box" solution	
URI	Uniform Resource Identifier	A Uniform Resource Identifier (URI) is a character sequence that identifies a logical (abstract) or physical resource -- usually, but not always, connected to the internet. A URI distinguishes one resource from another	
URL	Uniform Resource Locator		
UPS	Uninterruptible Power Supply	Immediate power backup in case of a power outage, not a long-term solution	
USB	Universal Serial Bus		
UAV	Unmanned Aerial Vehicle		
UTP	Unshielded Twisted Pair	Unshielded twisted pair (UTP) is a ubiquitous type of copper cabling used in telephone wiring and local area networks (LANs). The five types of UTP cables are identified with the prefix CAT, as in category, each supporting a different amount of bandwidth.	
TCP 5000	UPnP (Universal Plug-in-Play)	Permits networked devices (Computers, printers, Wi-Fi access points) to discover each other's presence and establish a connection	
TCP 5000	UPnP (Universal Plug-in-Play)	Permits networked devices (Computers, printers, Wi-Fi access points) to discover each other's presence and establish a connection	
USB OTG	USB On-The-Go		
UAT	User acceptance testing (end user)		
UDP	User Datagram Protocol	communications protocol, an alternative to TCP (Transmission Control Protocol), and uses the Internet Protocol (IP) to actually get a data units (datagrams) from one network node to another. UDP does not provide the service of dividing a message into packets (unlike TCP) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. UDP is a stateless protocol, meaning it doesn't acknowledge that packets being sent have been received. For this reason, the UDP protocol is typically used for streaming media, where a lost packet should not stop the transmission of data, or for simple applications where very little processing power is a requirement. TFTP (Trivial File Transfer Protocol) uses UDP as well.	
1024-49151	User Ports		
1024-49151	User Ports		
VLSM	Variable Length Subnet Masking	a computer networking technique to divide an IP network into subnets with different subnet masks	
	Venue	Location where legal case is heard	
VTC	Video Teleconferencing	Video teleconferencing (VTC) is a technology that facilitates the communication and interaction of two or more users through a combination of high-quality audio and video over Internet Protocol (IP) networks.	

SEC+ 701 TERMS (A-TO-Z)			
ACRONYM	**FULL NAME**	**DESCRIPTION**	**IMAGE**
	Vigenere Cipher	Keyword to lookup cipher text	
VDE	Virtual Desktop Environment	a preconfigured image of an operating system and applications that separates the desktop environment from the physical device used to access it	
VDI	Virtual Desktop Infrastructure	a virtualization solution that uses virtual machines to manage virtual desktops	
VLAN	Virtual Local Area Network	Logical overlay network that separates devices that share a physical LAN	
VPN	Virtual Private Network	Virtual network link across a public network	
	Virus	Requires infection mechanisms and host programs to spread themselves	
VM	Virutal Machines		
VPC	Virutal Private Cloud	Virtual segmentation for a multi-tenant model, designates subnets as private or public	
	Vishing, Smishing	Voice and SMS based phishing	
VB	Visual Basic	Visual Basic (VB) is an event-driven programming language and environment from Microsoft that provides a graphical user interface (GUI) which allows programmers to modify code by simply dragging and dropping objects and defining their behavior and appearance. VB is derived from the BASIC programming language and is considered to be event-driven and object-oriented.	
VoIP	Voice over Internet Protocol	Technology that allows users to make phone calls over a broadband internet connection	
	Volume encryption	Volume on a storage device	
	Warm Site	Have systems but no live data	
WAF	Web Application Firewalls	Firewall specific to the application layer (OSI L7), sits in front of web server, performs input validation database queries, APIs, and other web app tools —> firewall + IPS, blocks attacks in real time	
	Whaling	Targeting high-earners/high-rankers	
	White Hat	Authorized	
	Whitelists	Application allow lists	
WHOIS	WHOIS lookup AKA Domain Namelookup	Developed by CISA, DNS lookup gets the IP, WHOIS or Domain Name lookup gets the name	
802.11b	Wi-Fi 1	11 Mbit/s, 2.4 GHz	
802.11b	Wi-Fi 1	11 Mbit/s, 2.4 GHz	
802.11a	Wi-Fi 2	54 Mbit/s, 5 GHz	
802.11a	Wi-Fi 2	54 Mbit/s, 5 GHz	
802.11g	Wi-Fi 3	54 Mbit/s, 2.4 GHz	
802.11i	Wi-Fi 3	Established the four-way handshake 802.11i supersedes the previous security specification, Wired Equivalent Privacy (WEP). TKIP is its encryption protocol The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security Network). 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher.	
802.11g	Wi-Fi 3	54 Mbit/s, 2.4 GHz	
802.11n	Wi-Fi 4	600 Mbit/s, 2.4 GHz and 5 GHz	
802.11n	Wi-Fi 4	600 Mbit/s, 2.4 GHz and 5 GHz	
802.11ac	Wi-Fi 5	6.9 Gbit/s, 5 GHz	
802.11ac	Wi-Fi 5	6.9 Gbit/s, 5 GHz	
802.11ax	Wi-Fi 6 and Wi-Fi 6E	9.6 Gbit/s, 2.4 GHz, 5 GHz, 6 GHz	
802.11ax	Wi-Fi 6 and Wi-Fi 6E	9.6 Gbit/s, 2.4 GHz, 5 GHz, 6 GHz	
802.11be	Wi-Fi 7	Extremely High Throughput (EHT), 40+ Gbit/s, 2.4 GHz, 5 GHz, 6 GHz (adopted 2024)	
802.11be	Wi-Fi 7	Extremely High Throughput (EHT), 40+ Gbit/s, 2.4 GHz, 5 GHz, 6 GHz (adopted 2024)	
802.11bn	Wi-Fi 8	Ultra High Reliability (UHR), 100,000 Mbit/s (adopted 2028)	
802.11bn	Wi-Fi 8	Ultra High Reliability (UHR), 100,000 Mbit/s (adopted 2028)	
WPA-2	Wi-Fi Protected Access 2	Security protocol that encyrpts internet traffic on wireless networks, compatible with CCMP	
WPA-3	Wi-Fi Protected Access 3	Developed in 2018, SAE, perfect forward secrecy, Optional 192-bit security mode, still uses RADIUS, OWE The WPA3 protocol provides new features for personal and enterprise use, such as a harder-to-break 256-bit Galois/Counter Mode Protocol (GCMP-256), 384-bit Hashed-based Message Authentication Code (HMAC) and 256-bit Broadcast/Multicast Integrity Protocol (BIP-GMAC-256). The WPA3 protocol also supports security measures such as perfect forward secrecy, which produces a temporary private key exchange between clients and servers. A unique session key is generated for every individual session a user initiates.	
	Wildcard Certificate	Designated by the "*" sign, applies to only ONE level of subdomain	
WMIC	Windows Management Instrumentation Command-line	The Windows command wmic extends WMI for operation from several command-line interfaces and through batch scripts without having to rely on any other programming language. The command wmic uses class aliases to query related information.	
NTLM	Windows New Technology LAN Manager	Verifies user's identities and protects confidentiality, integrity	
802.3	Wired Ethernet	Collection of standards defining physical layer and data link layer's MAC of wired Ethernet	
802.3	Wired Ethernet	Collection of standards defining physical layer and data link layer's MAC of wired Ethernet	
WAP	Wireless Access Point		
WEP	Wireless Equivalent Privacy	Uses RC4 encryption algorithm, very insecure	
Wi-Fi	Wireless Fidelity		
WIDS	Wireless Intrusion Detection System		
WIPS	Wireless Intrusion Prevention System		
WO	Work Order	A job order is an internal document extensively used by projects-based, manufacturing, building and fabrication businesses.	
	Worm	Self-replicating	
802.1X	WPA-2, Standard for NAC	Port-based NAC for wired/wireless networks, RADIUS validates the user With 802.1X, we have the supplicant, authenticator, and authentication server. With a wireless network, the wireless client is the supplicant, and the Access Point (AP) is the authenticator.	
802.1X	WPA-2, Standard for NAC	Port-based NAC for wired/wireless networks, RADIUS validates the user	
	WPA2-Enterprise	relies on RADIUS as part of 802.1X	
WPA2-PSK	WPA2-Personal	pre-shared key, allows client to authenticate with a server infrastructure	
802.15.1	WPAN/Bluetooth		
802.15.1	WPAN/Bluetooth		
2	Write	-w-	
X.509	X.509 Standard (V3)	The current standard for digital certificates	
	XSS Hunter	Open source service to find XSS	
ZTA	Zero Trust Architecture	Control plane + data plane	
ZTMM 2.0	Zero Trust Maturity Model Version 2.0	The maturity model aims to assist agencies in the development of zero trust strategies and implementation plans and to present ways in which various CISA services can support zero trust solutions across agencies.	
	Zigbee	Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence, Zigbee is a low-power, low-data-rate, and close proximity (i.e., personal area) wireless ad hoc network.	