The ABCs of Cybersecurity Terms

Whether you're just starting a career in cybersecurity or simply trying to protect your personal information, understanding cybersecurity terms is essential. This glossary, compiled by SANS Senior Instructor, author of *SEC301: Introduction to Cyber Security*, and cybersecurity consultant Keith Palmgren, provides easy to understand explanations of key concepts that will help you navigate the complex field of cybersecurity. From *Active Defense* to *Zero Trust*, these terms form the foundation of your knowledge and equip you to defend against cyber threats.

Active Defense

A newer category of cyber defense adds a dose of offense. Active Defense or "offensive countermeasures" typically involves sending attackers misinformation to misdirect their activities. Active Defense also often sets up tripwires to alert us to attacks in real-time. The intent is to make our network a harder target and slow attackers while making us aware of the attack. This provides us more time to respond and prevent their attacks completely.

Authentication

Authentication is the process of verifying the identity of an entity—a user, an application, a system, or anything else trying to gain access. At the most fundamental level, we verify identity before granting access to ensure that only authorized people and processes have access. We also must verify identity to allow us to implement authorization and accountability mechanisms. There are three Authentication "factors" we can use to verify identity:

1. Something we know
2. Something we have
3. Something we are

See the entries ***Biometrics*** and ***MFA and 2FA***.

Authorization

Once we verify identity via authentication, Authorization dictates what we allow them to do, which files will we allow them to access, which servers can they use, and what resources are available to them. Authorization is a primary method of implementing the principle of Least Privilege: "Everyone can do everything they are supposed to be able to do, and nothing more."

Algorithm

Merriam-Webster's dictionary defines the term Algorithm as a "procedure for solving a mathematical problem in a finite number of steps that frequently involves repetition of an operation." In modern cryptography, an Algorithm is the public-knowledge set of mathematical rules that both encrypt and decrypt information.

See the entry ***Encryption***.

All-In-One Security Appliance

An All-In-One Security Appliance or Unified Threat Management Device incorporates many security functions within a single device. A perfect example of these devices is the wireless access point we buy for our homes. This device acts as a wireless access point and router. It is usually also a firewall, it does Network Address Translation, and it serves as our home's Dynamic Host Configuration Protocol (DHCP) server. That wireless access point may also perform as an intrusion detection system (IDS), gateway anti-virus, content filter, and many other security mechanisms all inside one box.

See the entry ***Wireless Access Point (WAP)***.

Application Allowlisting

With Application Allowlisting, we define a list of every legitimate, authorized piece of software on the computer. Then the allowlisting software only allows that authorized software to execute. Because malware is not on the allowlist, it cannot run and therefore it cannot affect our computer. Some argue that with properly tuned allowlisting software, it is no longer necessary to run anti-malware software.

While Application Allowlisting is potentially very effective, allowlisting implementation must be prefect. Incorrect implementation can prevent systems from functioning or even booting up, resulting in self-imposed denial of service.

Artificial Intelligence (AI)

The term Artificial Intelligence is widely misapplied. There is no *true* artificial intelligence today. Applications we refer to as artificial intelligence are really Machine Learning systems. A key distinction between the two is that artificial intelligence requires that a computer system shows true intuitive thinking (meaning it can innovate) while a machine learning system regurgitates preexisting information.

See the entries ***Machine Learning*** and ***ChatGPT***.

Backdoor

Backdoor is a hidden, unauthorized entry point into a network, a computer or an application. Rootkit malware often creates backdoors so that attackers can easily gain access to the system.

Backup

A Backup is a copy of information stored on media such as a tape or hard drive that is separate from the original. Generally speaking, the greater the physical separation between the original and the Backup, the greater the protection the Backup provides.

We do ***not*** create backups just so we can have backups. *We create backups so we can recover data.* If we don't do test recovery to validate a Backup, we don't really have a Backup at all—we just hope we do.

Blue Team

Blue Team members perform defensive cybersecurity tasks. These include placing and configuring firewalls, implementing patching programs, enforcing strong authentication, ensuring physical security measures are adequate and a long list of similar undertakings.

See the entry ***Red Team***.

Biometric Authentication

Biometric Authentication systems use the physical characteristics of a person to authenticate their identity. Common examples include fingerprint readers, facial recognition systems, and iris scanners that scan the iris of a person's eye. These methods use the authentication factor of "something we are."

See the entries ***Authentication*** and ***MFA and 2FA***.

Botnets

Botnets are a group of private computers in homes and businesses around the internet infected with malware. The malware allows attackers to control the members of the botnet (called bots) and have them act in unison. Botnets today routinely have more than thirty-million computers in them and can be rented on the dark web for around $20 per week. Attackers commonly use them in massive Distributed Denial of Service (DDoS) attacks. Botnets also serve as "SPAM Blasters" (sending massive quantities of SPAM email), and Crypto Currency Mints or Mines (creating large amounts of crypto currency).

Brute Force Attack

Brute Force Attacks occur when we guess every possible combination of something until one of those combinations works to achieve our goal. Two common variations on this theme include:

1. **Password brute force attacks—**We use software to guess every possible password—eventually one of them will work and we gain unauthorized access to an account.
2. **Cryptographic key brute force attacks—**We guess every possible combination of a cryptographic key until one of them works to decrypt data.

See the entries ***Password Cracking***, ***Password Spraying***, ***Key***, ***Keyspace***, and ***Workfactor***.

Business Email Compromise (BEC)

Business Email Compromise (BEC) is an attack that leverages social engineering and phishing to impersonate co-workers or, more often, executives of a company. The goal is to cause an unsuspecting employee to transfer company money or trade secrets to the attacker. This is among the fastest growing attacks today and results in several billion U.S. dollars per year in losses.

See the entries ***Social Engineering*** and ***Phishing***.

ChatGPT

The company OpenAI created ChatGPT, and defines it as a "neural network model called GPT (generative pre-trained transformer)." It allows us to post a plain-text query on a very wide range of topics and ChatGPT then generates a plain-text response. OpenAI "pre-trained" ChatGPT by having it "read" hundreds of millions of pages of information including books, articles, and websites. ChatGPT draws on this vast corpus of text to generate its responses.

Many refer to ChatGPT as "artificial intelligence." We would more accurately call it a very advanced form of "machine learning."

See the entries ***Artificial Intelligence*** and ***Machine Learning***.

CIA (Confidentiality, Integrity, Availability)

The CIA Triad is among the most often discussed topics in cybersecurity. The three letters stand for:

- Confidentiality
- Integrity
- Availability

The word Triad implies that we should implement all three of these things in equal measure. unfortunately, doing so is an unattainable ideal. Instead, we should use this as a method of prioritization of our limited cybersecurity resources.

https://youtu.be/BmSZFHQg2zA

Cloud Computing

To understand Cloud Computing, we first must understand this simple concept: There is no cloud; it is just someone else's computer. When we use the cloud, we utilize remote servers in the datacenter of a cloud provider to store our data instead of using local computer systems storage. Less often, we use the cloud provider's computers to process our data as well.

Command and Control (C2)

Command and Control or C2 channels are increasingly common in attacks and in attack detection. If an attacker is going to issue commands to a remote system, they must use a C2 channel to do so. This is how their instructions cross the network to the controlled system. These communication channels are strong Indicators of Compromise (IoC) used by Security Operations Center (SOC) analysts to identify attacks.

See the entries ***Lateral Movement*** and ***Security Operations Center (SOC)***.

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) database is a repository of known cybersecurity attacks. The database aids cybersecurity practitioners in identifying and prioritizing these known attacks.

Countermeasures

Cybersecurity Countermeasures are the culmination of defensive measures taken by the Blue Team. These include implementing technologies such as firewalls, anti-virus, content filtering, and so on. It also includes procedures such as hardening operating systems and applications, ensuring employee security awareness and skills training is effective, and creating and enforcing proper security policies. All these actions help to reduce the risk to an organization by either preventing the attack or limiting the damage when outright prevention is impossible.

See the entry ***Blue Team***.

Cryptography

Cryptography is the art of private communication in a public environment. Any mechanism providing private communication in a public environment falls under this broad definition, whether it involves encryption or not. Steganography is a mechanism that hides the existence of the message without necessarily encrypting it.

See the entries ***Encryption*** and ***Steganography***.

Cyber Kill Chain®

The Cyber Kill Chain® from Lockheed Martin is a well-known and widely referenced "attack model" to help understand the cyber attacker's process. There are seven steps of the Cyber Kill Chain® beginning with initial reconnaissance and ending with data exfiltration. The key point of the Cyber Kill Chain® is that it is indeed a chain—meaning if we stop the attacker at any one of the seven steps, the attack cannot continue. If we break the chain, we thwart the attack.

Data Integrity

Data Integrity, one of the primary goals of cybersecurity, ensures that data stays in a pristine state. Meaning the data is only edited by the correct people, in the right way, and with correct information.

The ABCs of Cybersecurity Terms (CONTINUED)

Dark Web

The Dark Web is a hidden segment of the Internet that isn't indexed by search engines like Google or Bing. While it used to require insider knowledge to access, nowadays information about how to reach Dark Web sites can be easily found through a simple search. On the Dark Web, users can purchase a variety of illicit items, including drugs, weapons, uranium, malware, stolen identities, and regrettably, even people.

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) systems are hardware and/or software solutions that try to detect sensitive data leaving our protected environment. Upon detection, the DLP system alerts us to the exfiltration and, hopefully, prevents the data from leaving.

Deep Packet Inspection

Deep Packet Inspection is a mechanism used by firewalls, gateway anti-malware, intrusion detection and prevention systems, data loss prevention and potentially any other detective technology. It involves delving into the data portion of a packet to find signs of maliciousness. It is more thorough than shallow inspection which only looks at packet headers. In fact, it is often the only way to find malicious traffic. Unfortunately, deep inspection is also much slower than shallow inspection. Because of the potential to slow throughput, we should use deep inspection selectively.

See the entries ***Firewall*** and "***Intrusion Detection System (IDS)***.

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

A Denial of Service (DoS) attack strives to keep a computer or network from doing anything useful. This can come in the form of exploiting system flaws to crash computers. More commonly, attackers send massive amounts of traffic to flood a network's bandwidth so legitimate traffic cannot get through. The traffic flood attacks are often Distributed Denial of Service (DDoS) attacks—meaning the flooding traffic originates from many distributed sources.

Denial of Service is not always malicious in nature. "Popularity DoS" occurs when a website becomes so popular, the web server cannot handle all the traffic and crashes. Similarly, "Accidental DoS" happens when something accidentally causes either system crashes or massive amounts of network traffic. A well-known example of Accidental DoS occurred in 2024 when the CrowdStrike company issued a faulty software patch, crashing over 8.5 million computers worldwide. The event was not malicious but was still very damaging.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is extremely common. In fact, we all use it almost daily even if we don't know it exists. When we turn our computer on in a coffee shop, hotel, airport, at home, or at work, this protocol provides the necessary network configuration to our computer so that we can communicate on that network. At minimum, this includes assigning an IP address to our computer and providing the "default gateway" address and "subnet mask" our computer must know. In many cases, our computer also asks the DHCP for the IP address of a DNS server we can use to resolve internet addresses.

Encryption

Encryption is the act of transforming text from a human readable form called plaintext to a non-human readable form called ciphertext. People have been doing Encryption for centuries using many ingenious methods. Today, cryptographic systems such as the Advanced Encryption Standard (AES) employ extremely complex mathematical formulas to create very random ciphertext.

See the entries ***Cryptography*** and ***Plaintext***.

Endpoint Security

Endpoint Security systems are the software we run on our local computers, phones, and tablets to provide security. Common examples include anti-virus, personal firewalls, and content filters. There are many vendors who provide software of this nature. Increasingly, we have these capabilities built into the operating systems from Microsoft and Apple.

Enumeration

In cybersecurity, enumeration means that we can remotely determine the type of computer and software running on a distant system. An example is a port scanner that can report the operating system version and server software version of a distant web server. This type of enumeration is valuable to an attacker because it allows them to launch highly targeted attacks.

Ethical Hacker

An Ethical Hacker is someone who employs many of the same tools and techniques of an unethical hacker to break into computer systems and networks. The difference is that the ethical hacker does so under contract and with written legal permission to perform the attack. The ethical hacker then works with the customer organization to fix the security problems discovered during the attack.

See the entries ***Penetration Testing*** and ***Red Team***.

Exploit

To Exploit something is to make full and complete use of it. In computing, this results in several applications of the word:

- Exploit software compromises a computer. Another name for software of this nature is "sploit."
- When we "Exploit a computer," we compromise that computer.
- The method and/or flaw that allows a computer compromise is an "Exploit."

External Insider

External Insider is a form of an insider attack performed by someone physically located outside a network, but has the access of an insider. For example, when a computer user opens a malicious email attachment, that attachment may install malware, granting the malware author remote control of that user's computer. The attacker now controls the user's computer as though they were sitting at the keyboard, even though they are physically external to the organization.

Fileless Malware

Historically, malware existed in files on the hard drive. Therefore, anti-malware scanned those files to discover the malware. More recently, a class of malware exists only in the computer's Random Access Memory (RAM) and does not write to the hard drive at all. This makes traditional anti-malware software useless at detection. Some anti-malware software now looks for Fileless Malware.

Firewall

A network Firewall keeps people off our network who do not belong there. A personal Firewall keeps people off our computer who do not belong there. In both cases, a set of rules defines what type of network traffic the Firewall will allow to pass through, and what traffic the Firewall will deny. Firewalls are one of the most ubiquitous security mechanisms in the world today.

See the entry ***Stateful Inspection***.

Firmware

Firmware is software on a computer chip. In other words, instead of software being on a computer's hard drive as we normally think, the software exists on the device's chips. This is common on devices such as a wireless access point, smart televisions, and a long list of similar devices that typically have no hard drive. A "Firmware update" simply means we overwrite all or part of the software on the chip with a newer version of software.

Forensics

Digital Forensics and Incident Response (DFIR) is a specialized area of cybersecurity that involves investigating and recovering from an incident. This can include low-level analysis of data on hard drives to discover and preserve digital evidence. DFIR also deals with containing and eradicating cyber threats causing the incident. A primary goal of DFIR is to return the organization to normal operation promptly through root-cause recovery, while maintaining the integrity of any evidence collected.

FTP (File Transfer Protocol)

Created in 1971, FTP is one of the very first network protocols. FTP allows two computers to exchange files. Unfortunately, in 1971 the need for security was not yet clear, so the protocol has no encryption capability. It is possible to configure FTP to work with or without authentication. However, usernames, passwords, and the files themselves all traverse the network in plaintext. Today, we have much more secure protocols for file transfer, including FTPS (File Transfer Protocol Secured) using TLS encryption.

See the entry ***Transport Layer Security (TLS)***.

Gap Analysis

Gap Analysis is a term used in business, marketing, information technology, and cybersecurity. In all these disciplines, Gap Analysis finds the gap between where we are now and where we would like to be. In cybersecurity, this means figuring out how high the current level of risk is and how much we want to lower that level. Reducing the level of risk involves choosing countermeasures to close the gap in the most effective and cost-effective ways possible.

GNU (GNU Not Unix)

GNU is a recursive acronym and stands for "GNU Not Unix." The term applies to free, open-source software licensed under the GNU General Public License. We can copy, use, change, and redistribute GNU software without paying a fee. The only restriction is that we cannot remove the original author's names. With open-source software, we also see the terms Copyleft and Attribution Licensing.

Google Dorking

Google Dorking uses highly specific and often complex Google search strings called Google Dorks to find systems vulnerable to various attacks, reconnaissance, data exfiltration, etc. The Google Hacking Database is a collection of Google Dorks in several categories including foothold attacks, files having "juicy info," files holding passwords, vulnerable servers, and so on.

www.exploit-db.com/google-hacking-database

GUI (Graphical User Interface)

The GUI (pronounced *gooey*) is the graphical interface of a computer, phone, tablet, etc. For example, when working with a computer, we double-click on the icon for a piece of software and that software begins running. The icon is part of the GUI. Most of our interaction with computing devices today happens via a GUI. By contrast, we can interact with a computer via a Command-Line Interface (CLI). In cybersecurity, knowledge of both the GUI and CLI methods of working with computers is necessary.

Hash (or Cryptographic Hash)

A Hash is a mathematical formula (an algorithm) run against an input of some kind. Cryptography uses hashes to check the integrity of data. When we "hash a file," we run the hashing algorithm against a computer file and receive a fixed-length output string called a hash. Any minor change in that file changes the hash dramatically. Therefore, if two communicating parties both generate the same hash, we know both parties have identical data.

See the entry ***Algorithm***.

HTTPS (Hyper-Text Transfer Protocol Secure)

The Hyper-Text Transfer Protocol or HTTP transfers web pages between our browser and a webserver. Unfortunately, HTTP does not provide any security since the webpage's content passes plaintext across the Internet. HTTPS adds encryption to the process so that when we do things like eCommerce or online banking, our information is not readable to attackers.

See the entry ***Transport Layer Security (TLS)***.

Imposter Vishing

The capability of AI-driven voice generation has grown exponentially. With just a few seconds of someone's voice recorded, we can type words and have AI generate the voice of that person saying those words.

This gives rise to a new form of Social Engineering often called Imposter Vishing. This can take the form of a phone call supposedly from our CEO directing us to transfer funds for example. They can also pretend to be loved ones who have been detained and require urgent financial help.

A similar form of this attack now generates realistic-looking video and voice to make the attack even more believable.

See entries ***Artificial Intelligence***, ***Social Engineering***, and ***Vishing***.

Incident Response

An "incident" means that something occurs which results in harm or the intent to harm. The incident can be intentional, accidental, or natural. Incident Response is the combination of all possible activities taken to respond to an incident. The desired culmination of incident response is to:

- Determine who did it
- Determine what they did
- Repair the damage
- Fix the root cause to prevent recurrence
- Return to normal operation as quickly as possible
- Learn our lessons from the incident

See the entry ***Forensics***.

Insider Threat

Insider Threat occurs when someone with access inside our organization causes damage. The damage may be intentional or accidental and may come from employees, contractors, or even those we do not know. There are three categories of Insider Threat:

- Disgruntled insider occurs when someone we grant access to becomes unhappy and decides to cause harm.
- Accidental insider occurs when someone we grant access to has no intention of causing damage but makes a mistake that leads to harm. Examples include clicking malicious links in emails, opening malicious attachments, plugging in untrusted malicious thumb-drives, etc.
- External insider occurs when someone we have NOT granted access gains that access. The individual or group's location is *physically outside* our network, but they have access of someone *inside* our environment.

Insider Threat is one of the primary cybersecurity concerns. It is also one of the most challenging problems to fix.

See the entry ***External Insider***.

Internet of Things (IoT)

Any device connected to the internet is part of the Internet of Things or IoT. On the consumer side, this includes a rapidly growing number of devices in our "smart home." We can tell our smart speaker, such as Amazon's Echo, to turn on the lights, close the blinds, open the garage door, turn on the coffee maker, start the garden sprinkler, and a host of other things. All of these devices are IoT.

Outside our homes, we also find IoT devices. Municipalities control parking meters, remotely read gas or electric meters, check traffic patterns, etc. Companies use it to control heating, ventilation, and air conditioning (HVAC), lighting, and other services.

IoT falls into two broad categories:

- Internet of Things (IoT) devices manipulate data only and are Information Technology devices. An example is a smart speaker playing music.
- Industrial Internet of Things (IIoT) devices are Operation Technology (OT) devices because they manipulate physical objects. An example is a light switch turning on or off.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is an automated system watching for signs of an attack. Some IDS systems are devices connected to the network and watch network traffic for attacks. Other IDSs run on the host (PC) and watch for signs of attack there making them a form of endpoint security. We respectively refer to these as Network IDS and Host IDS.

See the entries ***Stateful Inspection***, ***Deep Packet Inspection***, and ***Intrusion Prevention System***.

Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is an intrusion detection system capable of stopping attacks. It is not possible for an IPS to stop an attack unless it first detects the attack. Therefore, an IPS must first be an IDS. Once IPS identifies the attack, any one of several mechanisms can cause the attack to fail.

See the entries ***Stateful Inspection***, ***Deep Packet Inspection***, and ***Intrusion Detection System***.

IP Spoofing

IP Spoofing occurs when we send packets having an incorrect source IP address. The recipient computer responds to that incorrect IP address. A common reason for doing this is to have many computers sending enormous quantities of traffic to that incorrect IP address. That IP address becomes the victim of a Distributed Denial of Service attack.

See the entry ***Denial of Services (DoS)***.

Jailbreaking

When we Jailbreak a phone, we extract the phone's operating system, decompile it, edit the software, recompile it and put it back into the phone. The phone now has capabilities the manufacturer never intended. Whoever creates the jailbreak can put any functionality they want into the phone, including sending our personal sensitive data to attackers. The act of Jailbreaking a phone is illegal in most countries. NEVER jailbreak a phone.

JavaScript

Websites use scripting languages to automate their web pages and provide a high degree of interaction between a website and the end-user. The most popular web scripting language by far is JavaScript. It is very lightweight, meaning that it does not require a lot of computing power to provide a ton of functionality. Released in 1997, it powers over 95% of websites. Highly interactive sites such as Gmail, YouTube, Facebook, Amazon, and a long list of others all use JavaScript. (Note: Since 2014, websites including those listed here are migrating to HTML5. JavaScript is an inherent part of HTML5, so those sites still use JavaScript's functionality.)

Juice Jacking

Juice Jacking occurs when we infect our phone or tablet by plugging into a publicly available USB outlet to charge our device (in an airport for example). That public USB port may have a computer connected that holds malware. Because USB can pass both power and data and malware is data, the USB port can infect our device. Plugging our device into an actual power outlet does not provide for data transfer.

Kernel

All operating systems have a Kernel that acts as an interface between the operating system software and the computer's hardware. It is the Kernel that dictates almost everything about how a computer functions including how it stores information on the hard drive or in Random Access Memory (RAM), how it enforces file permissions, how the computer communicates on a network, and so on.

See the entry ***Operating System (OS)***.

Key (or Cryptographic Key)

In modern cryptography, a Key is simply a series of binary 1s and 0s (called bits) that complete an encryption algorithm so it can work. For example, Advanced Encryption Standard uses varying key sizes, specifically 128 bits, 192 bits, and 256 bits.

Key Derivation Function (KDF)

A Key Derivation Function (KDF) gets its name because it *derives a key* from a passphrase. These tend to be extremely complex in how they function, but very easy to use. Zero Knowledge implementations including password managers and cloud data storage use KDF's extensively.

When we use a KDF, we enter a strong passphrase. The KDF software generates a cryptographic key from that passphrase. That key then encrypts our data. That exact passphrase will always generate that exact key.

See the entries ***Zero Knowledge*** and ***Password Manager***.

Keylogger

A Keylogger is either hardware or software that captures our keystrokes and sends them to an attacker. The attacker then uses our keystrokes—such as our username and password or a credit card number—for malicious purposes. Typically, hardware keyloggers only capture keystrokes. Software keyloggers can capture keystrokes, screen captures, camera video, microphone audio, etc.

Keyspace

Keyspace is the range of values that can construct a cryptographic key. In other words, take a key of a specific number of binary bits and figure out how many combinations we can make with that number of bits. The answer to that exercise is the keyspace. It is important to note that the size of the keyspace doubles every time we add a bit to the length of the key. Two common keyspace examples are:

- AES 128-bit key gives a keyspace of 340,000,000,000,000,000,000,000,000,000,000,000,000 or 340 undecillion keys.
- AES 256-bit key provides a keyspace of 110,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 or 110 quattuorvigintillion keys.

Lateral Movement

Lateral Movement occurs when an attacker moves from one computer to another within our network. It is rare for the first system an attacker compromises to hold the data they want to exfiltrate. Therefore, they must move laterally from one computer to another to find that data. They use Command and Control (C2) channels to instruct each computer they compromise to attack the next computer in the chain.

See the entry ***Command and Control (C2)***.

Linux

Linux is a free, open source, "UNIX-like" operating system first created in 1991. It is extremely flexible and customizable. This is why many cybersecurity tools for penetration testing and forensics run on the Linux operating system. People working in cybersecurity must have a rudimentary knowledge of the Linux operating system. Deep Linux knowledge is necessary for most of us.

Living off the Land (LotL) Attacks

Living off the Land (LotL) Attacks occur when an attacker uses the same remote administration software in their attack that legitimate administrators use. A common example is the Remote Desktop Protocol (RDP) commonly used by administrators to remotely administer Windows computers. If an attacker can obtain the administrator's username and password, they can use RDP software to log into that administrator's account . The attacker's network traffic looks normal and is therefore difficult to detect as malicious.

See the entry ***Remote Desktop Protocol (RDP)***.

Logic Bomb

A Logic Bomb is a type of malware that waits for a preconfigured event or date before executing (or detonating in this case). An example includes malware with instructions saying; "If my name disappears from the employee database, delete the employee database." Another example is malicious software put in place by a disgruntled employee that would format all the organization's computer's hard drives at one minute after midnight on New Year's day.

Machine Learning System

A Machine Learning System is a computer that is "trained" by "reading" large amounts of text. The result is a system that can respond in quasi-intelligent fashion to queries. Well-known examples of Machine Learning Systems are ChatGPT, Amazon's Echo (Alexa), and Microsoft's Copilot. This is a rapidly evolving area of the Information Technology (IT) landscape. Great care must be taken during the training of a machine learning system. There is an old saying in the IT world; "Garbage in, garbage out."

See the entries ***Artificial Intelligence*** and ***ChatGPT***.

Machine-in-the-Middle (MitM) Attacks

This type of attack occurs when an attacker can position themselves so that all our network traffic passes through the attacker. Their computer becomes a "Machine-in-the-Middle." The attacker now has incredible power over our network traffic. They can manipulate it in any way they choose. The limitation of a MitM attack is their imagination and their knowledge. If they can think of something to do and know how to do it, they can do it to us. The best defense against this attack is to set up an IPSec based VPN tunnel.

See the entries ***Rogue Access Point*** and ***Virtual Private Network (VPN)***.

Malware

Malware is an umbrella term for any software with malicious intent, including viruses, worms, trojan horses, and a list of other categories. The number of malwares released on the Internet is staggering. Depending on which study we look at, the number of new malwares is at least several hundred thousand per day. Windows is the most targeted operating system, while Android is the second most targeted, but there is also malware that affects Apple's Mac computers, browsers, etc.

See the entries ***Worm*** and ***Application Allowlisting***.

MFA and 2FA

The three most common authentication factors are:

- Something we know (a passphrase)
- Something we have (a token held in our hand)
- Something we are (a biometric such as a fingerprint)

Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) occurs anytime we employ two or more of these three factors.

For example, to log into a computer, we must provide a PIN (Personal Identification Number) and provide a specific fingerprint. Assuming proper implementation, this is far better authentication than simple passwords, and we should use MFA /2FA everywhere we can.

Need to Know

As one of the simplest yet most important security principles, Need to Know has close ties with the Principle of Least Privilege. Where Least Privilege covers all capability, Need to Know is specific to read access. If we need to be able to read something to do our job, we should be able to read it. Permission settings must, therefore, allow for that read access.

See the entry ***Principle of Least Privilege (PoLP)***.

Network Address Translation (NAT)

Network Address Translation (NAT) maps multiple internal IP addresses to a single external IP address. For example, in our home, we might have ten computing devices (personal computers, laptops, phones, tablets, smart televisions, smart speakers, refrigerator, etc.). Each of those devices must have its own IP address on our home network. As those devices send traffic to the internet, those internal IP addresses map (or translate) to a single public IP address assigned to our home by the Internet Service Provider (ISP).

Nmap

Nmap is free, open-source software that can do any type of port scan. Nmap will find active IP addresses and show which network ports are "listening" for connections on those addresses. It can then enumerate the operating system and version on that distant computer as well as the software running on the open ports.

Non-Repudiation

Non-repudiation means that a user or other entity cannot deny or dispute the authenticity and integrity of a message or transaction. To prove non-repudiation of a message for example, we must be able to prove beyond question who sent the message as well as prove that the message was not tampered with (what we received is identical to what they sent).

Number-One Goal of Cybersecurity

While not a term to define, it is certainly a concept to understand. In all cases, the number-one goal of cybersecurity is the preservation of human life—always! While we deal most directly with this issue when working with physical security and disaster response plans, we must always remember it. The protection of data and other assets are always secondary concerns.

One-Time Password (OTP)

Just as the name implies, a One-Time-Password is authentication information that is only good once and never again. In cybersecurity, a "replay attack" occurs when an attacker captures our authentication information and replays it to authenticate as us. A One-Time-Password system defeats that attack.

See the entries ***Authentication*** and ***Replay Attack***.

Operating System (OS)

An Operating System (OS) is the software that makes a computer work. Common examples are Microsoft Windows, Apple's macOS, and Linux—but there are many others. The Operating System, in conjunction with its kernel, dictate everything about how a computer functions.

See the entries ***Kernel*** and ***OS Hardening***.

OS Hardening

Operating System (OS) Hardening—sometimes called System Hardening—is the process of removing everything from a computer that is unnecessary to its function. The goal is to make the computer more secure. Every service and piece of software on a computer is a potential point of attack. By removing all unneeded services and software, we lower the number of potential attack vectors.

Owner

In cybersecurity, the Data Owner is the person with the most direct knowledge of a set of data, its value, and the protection it deserves. This individual makes all decisions about security mechanisms placed around that data. Cybersecurity staff can only advise the Data Owner on what those decisions should be.

Packet

A packet is a formatting construct used to send data across a network. The payload of the packet is the data, and the various headers of the packet take care of various addressing needs. For example, every packet has an IP header that holds the source and destination IP address of the packet.

See the entries ***Deep Packet Inspection***, ***Packet Sniffer***, and ***Wireshark***.

Packet Sniffer

Packet Sniffer is a hardware and/or software tool that captures packets from a network and displays the contents. The tool displays the packet headers as well as the data. This is invaluable in figuring out what is happening on a network. Both IT staff and cybersecurity practitioners use Packet Sniffers for trouble shooting, confirming tools such as firewalls are working correctly, and a very long list of other tasks.

See the entries ***Packet*** and ***Wireshark***.

Passphrase

A passphrase is a longer, stronger, and easier to remember form of a password. Historically, we recommended that users use a "complex password" having upper case, lower case, numbers, and special characters. An example is the eight character ***%y6dGk^Z***—which is extremely hard to remember and type. Further, against a brute force password attack generating one hundred trillion guesses per second, that password only provides about 1.12 minutes of protection.

The passphrase ***ILoveRockAndRoll!81*** still contains all four character sets, is easier to remember (the song came out in 1981), is easier to type, and at 19 characters is far stronger. The brute force attack mentioned above requires about 1.21 hundred trillion centuries to crack it.

To strengthen that passphrase even further, add the spaces: ***I Love Rock And Roll! 81*** has 24 characters. The brute force attack would require about 9.38 hundred billion trillion centuries to crack it! Microsoft Windows, Apple's macOS, Linux, and a growing list of websites allow spaces in passphrases.

See the entries ***Password Cracking*** and ***Brute Force***.

Reference: https://sec301.com/haystack

NOTE: the passphrase above is for illustration purposes only. Do not use that example as your passphrase.

Password Cracking

Password (or passphrase) Cracking is the act of figuring out what someone's password is. Administrators do this to audit passphrase security in their environment. Attackers do this to gain unauthorized access.

Password cracking software often uses some combination of a dictionary attack and brute force. Dictionary attacks use a text file of common words which the software "mangles" into combinations of upper case and lower-case characters, appending and prepending numbers and special characters, etc. Brute force attacks simply try every possible combination of characters.

See the entries ***Passphrase*** and ***Brute Force***.

Password Spraying

Password Spraying attacks are a form of brute force attack against accounts. The attacker uses a software tool and a dictionary (a text file) of common passwords. The software sends attempts to log into a series of accounts using each word in the dictionary sequentially. Any account with a very weak password (e.g. ***123456789*** or ***password123***) will result in a successful login, granting the attacker access. This attack is remarkably successful in many situations.

See the entries ***Password Cracking*** and ***Brute Force***.

Password Manager

A Password Manager is software that remembers our usernames and passphrases needed to log into our various accounts. The Password Manager uses Zero Knowledge with a Key Derivation Function to encrypt our username/passphrase data.

A common feature of password managers is to place our Zero Knowledge encrypted username and passphrase data into their cloud. They then synchronize that data across multiple computers, phones, and tablets running the password manager software.

There are free, open-source password managers available that are very good (e.g. Bitwarden). There are also commercial solutions including Dashlane, OnePassword, and NordPass.

See the entries ***Zero Knowledge***, ***Key Derivation Function (KDF)***, and ***Passphrase***.

Patch

A Patch, or Software Patch, fixes flaws in the software of a computing device (personal computer, laptop, phone, tablet, printer, smart television, etc.). The "flaw" in this case might be a problem with functionality or security.

To take a very simple example, there is a file on every Microsoft Windows computer called ***spoolsv.exe***. This is the "print spooler" of the Windows operating system and handles all printing for all software on the computer. If there is a flaw of some type discovered in that file, Microsoft will create a new version of the ***spoolsv.exe*** file and include it in the next update. When we "Update Windows," that new version downloads and overwrites the old, flawed version of the file.

Penetration Testing

Penetration Testing is when a cybersecurity professional employs the same tools and techniques (except destructive methods) as a hacker in an attempt to gain access to a network, building, etc. Two big differences between criminal hackers and Penetration Testers are:

- **Contracts—**Penetration testers have extensive contracts with their customers that give the penetration tester permission to perform the attacks, list what they can and cannot do, etc.
- **Cleanup—**Good penetration testers always clean up after themselves. Some tests may leave accessible vulnerabilities on a network that require repair.

Criminal hackers do not care about contracts, permission, or cleaning up after themselves. The other significant difference is that a criminal hacker tends to cost an organization a great deal more than penetration testers do.

See the entries ***Ethical Hacker*** and ***Red Team***.

Phishing

A Phishing email is a form of social engineering and is now the single most common attack method in the world. It is also the most successful, resulting in billions of dollars per year in corporate and personal losses. Unfortunately, the sophistication of the hacking community has grown considerably in this area so recognizing a legitimate email from a phishing email is no longer a simple matter. (Note: Spear Phishing is simply a highly targeted phishing email.)

See the entries ***Social Engineering*** and ***Business Email Compromise (BEC)***.

Plaintext

Plaintext is data in a human-readable form as opposed to ciphertext which is the same data encrypted into a non-readable form.

See the entry ***Encryption***.

Principle of Least Privilege (PoLP)

The Principle of Least Privilege (PoLP) states: *everyone can do everything they need to do, and nothing more!* It is the most fundamental principle in cybersecurity. It is the principle we use when we answer questions such as what firewall rules we should have, who should get a user account, what access should that account have, and so on.

Privileged Account

A Privileged Account is an account with a higher level of permissions and capabilities than a normal user account has. Administrators use privileged accounts to configure and maintain computers. On Microsoft Windows, the default name for the privileged account is *Administrator*. On Linux, the default name is *root*.

See the entry ***Privilege Escalation***.

Privilege Escalation

Privilege Escalation happens when someone changes their level of permission from a standard, non-privileged user to that of a privileged account. Administrators do this on a regular basis. They log in with their non-privileged account and only escalate their permissions when necessary for administrative duties.

Attackers do Privilege Escalation as quickly as possible after initially exploiting a computer. It is rare for initial access to a computer to be at the privileged level, but attackers can rarely proceed with the next steps of their attacks until they obtain privileged status.

See the entries ***Privileged Accounts*** and ***Exploit***.

Protocol

In Information Technology (IT), a Protocol is the set of rules governing communication on a network. There are thousands of protocols in use today. Request for Comment (RFC) documents published by the Internet Engineering Taskforce (IETF) define protocols. Each of these documents explain precisely how a particular protocol works.

Quarantine

In cybersecurity, a Quarantine isolates a file, or files suspected of containing malware in a safe place. While in quarantine, the malware is unable to execute and infect other files. This also allows us to send the suspected malware to anti-malware vendors for analysis and possible inclusion in future anti-malware updates.

Quick Response Code (QR code)

A Quick Response Code or QR code is a two-dimensional bar code. We can use a camera, such as that found on a phone or tablet, to scan a QR code. Most often today, doing so will cause our device to open a browser and visit a specific web page. For example, this QR code will take us to https://sans.org/sec301

Ransomware

A type of malware that encrypts our data files, making them inaccessible to us. To obtain our data, we must pay ransom to the author of the malware. We pay the ransom in an untraceable digital currency such as BitCoin.

Red Team

Red Team members perform offensive operations—better known as penetration testing—against customer networks. Penetration testing is a highly specialized field requiring extensive knowledge of computer systems, exploits and exploit software, protocols, etc.

See the entries ***Ethical Hacking***, ***Penetration Testing*** and ***Blue Team***.

Remote Desktop Protocol (RDP)

Microsoft developed the Remote Desktop Protocol (RDP). As the name implies, RDP allows us to access the desktop of a distant computer. Once we set up an RDP session, we can use our mouse and keyboard as though we were sitting in front of that remote computer.

Windows administrators commonly use RDP for remote configuration and maintenance. It is also used by attackers for Living off the Land attacks any time the attacker can obtain the login credentials of an administrator.

See the entry ***Living off the Land (LotL) Attacks***.

Replay Attack

A replay attack occurs anytime someone captures our authentication information and "replays it" to authenticate as us. To defeat this attack, we deploy one-time password systems.

See the entries ***One-Time Password***, ***Passphrase***, and ***Authentication***.

Risk

The term Risk means exposure to danger. In cybersecurity, it means that two things are present:

- **A Threat—**Anything that can do anything bad to our stuff
- **A Vulnerability—**Anything that allows the threat to happen

Once both are present, there is a level of Risk. A Risk assessment will enable us to figure out the level of Risk. Only the senior manager of an organization can decide if the level of obtained Risk is too high.

Rogue Access Point

The term Rogue Access Point has two common uses:

1. An unauthorized wireless access point connected to our organization's network.
2. A "fake" wireless access point in a public area, trying to trick unsuspecting people into connecting. For example, we might see two wireless networks, one named "coffeeshop" and one named "coffeeshopsuperfast." Many people will connect to the second network, not realizing that is a wireless access point controlled by an attacker trying to establish themselves as a Machine-in-the-Middle.

See the entry ***Machine-in-the-Middle (MitM)***.

Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) allow administrators to grant or deny permissions to data based on the role of the employee in the organization. For example, an employee working in Human Resources might have their user account added to a user group named "HR." The permission for anyone belonging to that group allow access to HR specific data.

RBAC is extremely common in enterprise security. Properly configured, they can be very good to use. All too often, improper configuration leads to excess access and potential compromise.

Root User (root)

On a Linux computer, the default privileged account name is "root." More specifically, any account with a user number of zero is the all-powerful privileged user. The user account named root has a user number of zero.

See the entry ***Privileged Account***.

Rubber Ducky

In cybersecurity a Rubber Ducky is a USB device used by attackers that looks very much like a USB thumb drive. When plugged into a computer, it mimics a USB keyboard and begins "typing" a particular and configurable set of keystrokes into the system. The computer trusts those keystrokes just as much as any keystrokes we type on a real keyboard. This opens the door to many potential attacks so long as the attacker can physically plug the Rubber Ducky into a computer.

Script Kiddie

The term Script Kiddie is a derogatory name for an attacker who has little or no knowledge of how their attacks work. They simply download a free attack tool and run it. This has the potential to be extremely dangerous because the Script Kiddie has no idea what attacks might cause harm. Of course, running attack tools without written authorization is often also illegal.

Security Operations Center (SOC)

A Security Operations Center (SOC—pronounced *sock*) is a team of cybersecurity analysts performing continuous, 24/7 monitoring of an organization's network traffic. The analysts continually watch for Indicators of Compromise (IoC) such as the traffic associated with attacker Command and Control (C2) channels. In many organizations, the SOC may also run many of the organization's security tools, perform log analysis, and a variety of other tasks.

See the entries ***Command and Control (C2)*** and ***Threat Hunting***.

Social Engineering

Social Engineering is the use of manipulation, deception, and pretexting (AKA lying) to get an individual to divulge corporate or personal secrets. It is the most common attack category and has been around for centuries. Spear phishing is a form of social engineering used for decades and accounts for hundreds of billions of dollars per year in corporate and personal losses.

See the entries ***Phishing*** and ***Imposter Vishing***.

Stateful Inspection

Stateful Inspection is the most common firewall technology used today. Enterprise firewalls, home firewalls, and even personal firewalls often employ this technology.

With Stateful Inspection, only the first packet of any communication must be checked against the firewall's rules. Once a communication is allowed by those rules, the firewall tracks the state of the communication and continues to allow it so long as it makes sense to do so.

Supply Chain Attack

Supply Chain Attacks occur in several forms. The most common involve malicious updates placed into the legitimate software update channel. As administrators update their software as they ought to do, they unknowingly install the malicious updates and compromise their systems.

There have been several examples of this occurring in recent years. Supply Chain Attacks tend to be highly complex and difficult to understand. Because of this, they are generally under-reported by the press.

The ABCs of Cybersecurity Terms (CONTINUED)

Steganography

In Greek, Steganos means "covered," and Graphy means "writing." Therefore, Steganography is "covered writing." In modern cybersecurity, it deals with hiding data inside of other files such as pictures, movies, word documents, etc. There are dozens of tools available for free download that will perform steganographic techniques. Many of those techniques are difficult or impossible to discover. Attackers use these tools to exfiltrate data off our networks without discovery. Steganography also works for good. These methods allow steganographically hidden "by-partner watermarks" on files to detect unauthorized disclosure on the part of partner organizations.

Threat Hunting

Traditional security is about keeping bad people off our networks. Threat Hunting takes the approach that the bad people are already on our network, we need to find them and remove them. The primary way this happens is via the continuous monitoring conducted by the Security Operations Center (SOC). Typically, "threat feeds" try to provide the SOC analysts with up-to-date information on current attack methods and Indicators of Compromise (IoC).

See the entry *Security Operation Center (SOC)*.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is the security protocol used by HTTPS and several other protocols to encrypt data. While HTTPS is by far the most common implementation of TLS, it can and does encrypt many types of network traffic.

Trojan Horse

The Trojan Horse is the most common form of malware. Trojan Horse malware is the delivery mechanism of most other malware. A Trojan Horse occurs anytime we have something with a known, desired function as well as an unknown, undesired function. For example, think of a login screen used to login to a computer. Say that in addition to logging us in, it also sends our username and password to an attacker. The login function is the known and desired action. Sending our credentials to an attacker is the unknown and undesired action.

Two-Factor Authentication (2FA)

See the entry *MFA and 2FA*.

URL (Uniform Resource Locator)

A URL or Uniform Resource Locator is the web address we type into a browser to access a web site. An example of a URL is https://sans.org/sec301

USB Seeding

USB Seeding is the practice of leaving malicious USBs around and waiting for someone to pick them up and try to use them. These USBs have autorun scripts on them that will automatically install malware on a system the instant we plug them into a computer. (Note: Windows supports autorun scripts, though we can disable the feature. Mac does not support autorun at all.)

Virtual Private Network (VPN)

The term VPN describes a network connection between two sites (such as branch offices of a company) that have an end-to-end encrypted connection. With this in place, no data passing between the branch offices are visible to prying eyes. The term also describes the encrypted link between a laptop and the corporate network.

Virtualization or Virtual Machine

The definition of the word "virtual" is "appearing to exist." Therefore, a Virtual Machine is a computer that appears to exist. We create Virtual Machines with Virtualization software. In the past, this required a third-party application, but operating systems like Microsoft Windows now natively include the capability.

It is possible to run a Virtual Machine on a PC or Laptop. Virtualization is ubiquitous in Cloud Computing since almost all "cloud computers" are virtual machines.

Virus

A computer virus is malware that, to survive and propagate (or spread), must insert itself into other executable code. For example, we have a legitimate software program on our computer. The virus inserts itself into that program. When we execute the legitimate software, we unknowingly also execute the virus. This is why we often say that a virus is "parasitic."

Vishing

Just as phishing attempts to solicit information via email, vishing attempts to solicit information via voice. Most commonly, this comes in the form of a phone call. For example, when we receive a call supposedly from a company telling us we missed a payment and owe money. They instruct us to go purchase large quantities of gift cards and send them to a specific mailing address. This is one example of many Vishing attempts.

See the entries ***Imposter Vishing*** and ***Social Engineering***.

Vulnerability

If a "threat" is anything that can do anything bad to our computer, then a "vulnerability" is anything that allows that threat to happen. A common example might be when a piece of software "has a vulnerability"—meaning that there is a flaw in the software's code that allows someone to exploit that software and gain unauthorized access. We fix that flaw by applying a patch.

See the entries ***Risk***, ***Exploit***, and ***Patch***.

Vulnerability Scanner

A Vulnerability Scanner is software that attempts to automate the discovery of vulnerabilities in our environment. Typically, this software scans for active IP addresses and open ports, then enumerates the operating systems and software running there. The software then compares this information against a database of known vulnerabilities and puts its finding into a report. For example, the report might say something like: This system is running the XYZ software version 1.2.3, so it may be vulnerable to the ABC attack.

Unfortunately, vulnerability scanners tend to err on the side of caution. If there is the slightest possibility the vulnerability exists, they include it in the report. This results in a lot of "false positive" findings.

Watering Hole Attack

Watering Hole Attacks allow attackers to target specific users or organizations. A common example is when an attacker places malicious code on a web site that the employees of a specific organization are likely to visit. In this way, they increase the likelihood of installing their malware on that organization's systems.

WAF (Web Application Firewall)

A Web Application Firewall or WAF is a highly specialized type of firewall placed in front of a web server. All traffic to and from that web server must pass through the WAF, which is very knowledgeable about attacks against web servers. The WAF allows legitimate traffic to pass through to the web server while blocking malicious traffic.

A similar device is a Mail Application Firewall (MAF) which sits in front of an organization's email server.

Wireshark

A free, open-source packet sniffer. Wireshark is by far the most common packet sniffer in use today. Both Information Technology (IT) staff and cybersecurity practitioners need to have knowledge of this important tool.

See the entries ***Packet*** and ***Packet Sniffer***.

Wireless Access Point (WAP)

A Wireless Access Point (WAP)—often called a Wireless Router—is a device that sits between our wireless network and our wired network. When we connect to a wireless network, we set up wireless communication to the WAP. As we send network traffic, the WAP passes that traffic onto the wired network as appropriate. We find WAP devices at home and in the enterprise. Wi-Fi uses several specifications to facilitate communication. The current security specifications are WPA2 and WPA3.

See the entries ***All-In-One Security Appliance***, ***Rogue Access Point***, and ***WPA2 and WPA3***.

WPA2 and WPA3

Wi-Fi Protected Access version 3 or WPA3 is the most recent security specification for Wi-Fi. We will continue to see WPA2 supported by Wireless Access Points for some time to come. Both versions dictate how we authenticate to a wireless access point, how our data encrypts, and a list of other security features. While both specifications are considered good, WPA3 is a distinct improvement over WPA2.

See the entry ***Wireless Access Point***.

Work Factor

In cryptography, the term Work Factor describes the length of time it would take to break our cryptography implementation. In other words, if we encrypt our email today and an adversary cannot decrypt and read it for 20,000 years, will we still care? In that example, the work factor is twenty thousand years. Please note this is not a ridiculously high work factor. Modern cryptographic systems commonly measure work factors in the billions and even trillions of centuries.

Worm (or Network Worm)

Worm is a type of malware that is self-standing and self-executing—meaning it spreads without human intervention. This is important because it means this type of malware can spread very quickly. For example, Wannacry was the first ransomware worm and spread to hundreds of thousands of computers around the world in a matter of hours. The Notpetya malware spread as a worm and, at one company, infected over 28,000 servers on three continents in under 12 seconds.

X.509 Certificate

The standard used for the creation of digital certificates. An X.509 certificate consists of two files having linked information. The private file holds an individual's private key and should be passphrase protected. The public file holds the individual's public key that they share with the world. These certificates are an integral part of creating a Public Key Infrastructure (PKI).

XOR (or Exclusive OR)

XOR is a logical computer function that compares two binary bits:

- If both bits are the same (both 1s or both 0s), the output is always 0.
- If the bits are different (a 1 and a 0), the output is always 1.

XOR is one of the fastest things a computer can do and is used by almost all cryptographic algorithms.

Zenmap

Zenmap is the GUI for the command line port scanner Nmap.

See the entries ***Nmap*** and ***Graphical User Interface (GUI)***.

Zero-Day Exploit

A Zero-Day Exploit is an attack against a computer that is only known by the person who discovered it. The person who discovered the attack or exploit has not notified the vendor, so the vendor does not know to work on a solution. Since the public does not know about the attack, we do not know to protect ourselves from it. Zero-day exploits have now become a commodity bought and sold on the dark web. Google, Microsoft, and other companies also have "bounty programs" that will pay for the disclosure of zero-day exploits.

See the entry ***Exploit***.

Zero Knowledge

An example of a Zero-Knowledge implementation is when we place our data on a cloud provider's systems in such a way that they have "zero knowledge of our data." The most common implementation involves using a Key Derivation Function (KDF) with a very strong passphrase on our local computer. The KDF generates an encryption key to encrypt our data before it uploads to the cloud provider's storage system. Because the cloud provider never knows the passphrase, they cannot regenerate the encryption key. Without that key, they cannot access our data. The cloud provider is simply a storage repository of our encrypted data, but they cannot decrypt that data. Note that not all cloud storage solutions implement zero knowledge. Some cloud providers encrypt our data with a key that they possess.

Password managers routinely use Zero Knowledge and KDF technology to encrypt our data, store it in their cloud, and allow that data to synchronize to multiple computers, phones, and tablets.

See the entries ***Key Derivation Function (KDF)*** and ***Password Manager***.

Zero Trust

In traditional network security models, we authenticate an entity once, and then that entity can access everything they are supposed to have access to for a set period of time. In other words, we deploy a "verify once, then trust" approach.

In a Zero Trust security model, we deploy a "never trust, always verify" approach. Every entity (user, software, process, etc.) that wants to access something on the network must authenticate—every time.

Zero Trust can be difficult to implement, but when combined with continuous monitoring by a SOC it has the potential to greatly increase the security of a network.

See the entries ***Authentication*** and ***Security Operations Center (SOC)***.