THE ABCs OF CYBERSECURITY TERMS

SANS

Whether you are looking to start a career in cybersecurity or actively wanting to protect your personal information, you will need to know and understand cybersecurity terminology. Keith Palmgren, SANS Senior Instructor, Author of *SEC301: Introduction to Cyber Security* and *Cybersecurity Consultant* has compiled a comprehensive glossary of cybersecurity terminology that will quickly get you up to speed on the industry's terms and meanings.

Authorization

Once we know who a user is via authentication, *Authorization* determines what we let that user do? Which files will we allow them to access? Which servers can they utilize? 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 cybersecurity, an *Algorithm* is the public-knowledge set of rules behind cryptography. Older methods of encryption (turning information into a non-human readable form to protect the meaning) used simple methods to obfuscate the meaning of data. Modern ciphers utilize highly complex mathematical algorithms to accomplish data encryption.

Blue Team

A *Blue Team* are the people who 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.

Botnet

Botnets are a group of private computers in homes and businesses around the internet infected with malware. The most common name for the individual machines that make up Botnets is "Bots," You may also hear the term *Zombie* for the systems and *Zombie-Army* for the collection of computers. Botnets have several "Bot-Herders" or "Zombie-Masters" that attackers use to pass instructions on to the other members. Botnets can perform massive Distributed Denial of Service (DDoS) attacks, massive SPAM campaigns, and more recently, generate large amounts of digital currency.

Countermeasure

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 of these actions lead to reducing the risk to an organization by either preventing the attack or limiting the damage when outright prevention is impossible.

Cloud Computing

To understand *Cloud Computing*, you first have to understand this simple concept: There is no cloud; it is just someone else's computer. When you use the cloud, you utilize remote servers in the data-center of a cloud provider to store, manage, and process your data instead of using local computer systems.

THE ABCs OF CYBERSECURITY TERMS (CONTINUED)

Data Integrity

Data Integrity, the primary goal of cybersecurity, is to ensure that data remains in a pristine state. Meaning the data is only edited by the correct people, in the right way, and with accurate information.

Dark Web

Dark Web is a secretive, semi-hidden area of the Internet. You cannot discover information located on the dark web via search engines such as Google.com or Bing.com. You have to be "in the know" by visiting clandestine chat rooms, being accepted as worthy, and then receiving information on how to access dark web sites. Once there, you can purchase anything you can possibly imagine, including drugs, weapons, uranium, malware, identities, and yes, unfortunately, even people.

Exploit

To *exploit* something is to make full and complete use of it. In computing, this results in several ways the word is applied:

- Software used to compromise a computer is often called exploit software, or sometimes merely a "sploit."
- When you perform the act of compromising a computer, you are said to be exploiting the computer.
- The method and/or flaw that allows a computer to be compromised is often called an exploit.

External Insider

External Insider is a form of an insider attack performed by someone physically located outside a network. 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.

Firewall

A *network firewall* keeps people off your network who do not belong there. A *personal firewall* keeps people off your computer who do not belong there. In both cases, a set of rules define 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.

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 apparent, so the protocol has no encryption capability. It is possible to configure FTP to utilize 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) utilizing TLS encryption.

Gap Analysis

Gap Analysis is a term used in business, marketing, information technology, and cybersecurity. In all of these disciplines, the terms simplest definition is the gap between where we are now and where we would like to be. In cybersecurity, this means determining 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 reason is that the original GNU operating system created in the 1980s was a UNIX-like operating system but contained no code from the Unix operating system. Today, the term primarily applies to free, open-source software. Software licensed under the GNU General Public License is free. You can copy, use, modify, and redistribute GNU software without paying any fee. The only restriction is that you cannot remove the original author's names. When discussing open-source software, you might also hear the terms Copyleft or Attribution Licensing.

HTTPS (Hyper-Text Transfer Protocol Secure)

The Hyper-Text Transfer Protocol or HTTP is the protocol used by the world-wide-web to distribute web pages. When you request a web page from a website, HTTP is what takes care of delivering that web page to you. Unfortunately, HTTP does not provide any security since that webpage passes plaintext across the Internet. *HTTPS* adds encryption to the the process so that when you do things like eCommerce or online banking, your information is encrypted and not easily visible to attackers.

THE ABCs OF CYBERSECURITY TERMS (CONTINUED)

Hash (or Cryptographic Hash)

A *Hash* is a mathematical formula (algorithm) run against an input file. It is used in cryptography to check the integrity of a message or a file. When you "hash a file", you run the hashing algorithm against a computer file and receive a fixed-length output called a hash or fingerprint of the file. A good hash algorithm provides all of the following:

- When you use the same algorithm, you always get the same length output, regardless of the size of input
- Every time you hash the exact same input, you get the exact same output
- If you make even a tiny change to the input your output is completely different (called widely divergent)
- It is extremely fast to calculate a hash regardless of the size of the input
- It is mathematically impossible to use the output to recreate the input
- It is extremely unlikely that two different inputs will create the same output
- The hash algorithm does not modify the input in any way

Insider Threat

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

- **Disgruntled insider** occurs when someone you grant access to becomes unhappy and decides to cause harm.
- **Accidental insider** occurs when someone you 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 you have NOT granted access gains that access. The individual or group's location is physically outside your network, but they have access of someone inside your environment.

Insider Threat is and has always been, one of the primary cybersecurity concerns. It is also one of the most challenging problems to counter.

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
- Returning to normal operation as quickly as possible
- Lessons we can learn from the incident

JavaScript

Websites utilize 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 instead of pure JavaScript. However, since JavaScript is an inherent part of HTML5, those sites still use JavaScript's functionality.)

John the Ripper

John the Ripper or JtR is a robust password cracking software created in 1991, but maintained by a group of open-source developers. JtR can perform a variety of methods when cracking passwords, including dictionary, hybrid dictionary, and brute-force modes. You can find John the Ripper at the site: www.openwall.com/john

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, the Data Encryption Standard or DES algorithm requires that you insert a key of 56 bits in order to use that algorithm. The Advanced Encryption Standard utulizes varying key sizes, specifically 128 bits, 192 bits, and 256 bits.

THE ABCs OF CYBERSECURITY TERMS (CONTINUED)

Keyspace

Keyspace is the range of values that can construct a cryptographic key. In other words, take a key of a specific number of bits and figure out how many combinations you 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 you add a bit to the length of the key. From the examples for the term "Key" above:

- DES utilizes a key of 56 binary bits, which creates a keyspace of 72,000,000,000,000,000 or 72 Quadrillion possibilities.
- 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 or 110 quattuorvigintillion

Least Privilege

Least Privilege 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.

Logic Bomb

Logic Bomb is a type of malware that waits for a preconfigured event or date before executing (or detonating in this case). A famous example includes software containing instructions saying that if my name disappears from the employee database, delete the employee database. Or software that will format the computer's hard drive at one minute after midnight on New Year's.

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 malware released on the Internet is staggering. In 2018, Symantec (a leading anti-malware company) states it identified 10.52 billion unique pieces of malware. That means 333.5 new pieces of malware hit the Internet every second during that year. Windows is the most targeted operating system, while Android is the second most targeted.

Man-in-the-Middle (MitM) Attacks

This type of attack occurs when an attacker can position themselves so that all of your network traffic passes through the attacker. They become a "Man-in-the-Middle." The attacker now has incredible power over your network traffic. They can manipulate it in any way they choose. The limitation of a MitM 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 you. The best defense against this attack is to establish an IPSec based VPN tunnel.

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 above. Where Least Privilege covers all capability, Need to Know is specific to read access. If you need to be able to read something to do your job, you should be able to read it. Permission settings must, therefore, allow for that read access.

Number 1 Goal of Cybersecurity

While not a term to define, it is certainly a concept to understand. In all cases, the number 1 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 remember it at all times. The protection of data and other assets are always secondary concerns.

Owner

In cybersecurity, the Owner of the data (or 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 regarding security mechanisms placed around that data.

Obfuscate

When you ***obfuscate*** something, you render it unintelligible. In computing, the term occurs most frequently in cryptography where we obfuscate the letters of a message (or transpose the letters or permute the letters). The term ***obfuscate*** also shows up elsewhere when attackers attempt to obfuscate their attacks by hiding them inside innocent-looking computer code etc.

THE ABCs OF CYBERSECURITY TERMS (CONTINUED)

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.

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. Traditional phishing messages try to get you to click on a link purportedly taking you to your PayPal account, but taking you to a site that only looks like PayPal (called an Evil Twin site). 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.)

Qualitative Risk

Qualitative Risk is a risk-assessment approach that utilizes a team of subject-matter experts (SMEs) and questionnaires to rank each threat according to likelihood and impact. The answers from the SMEs go into a severity scale that helps the cybersecurity team to prioritize concerns and assign resources effectively. The method is difficult to communicate the results to management, but it is very straightforward to perform.

Quantitative Risk

Quantitative Risk is a risk-assessment approach that assigns hard costs to each risk. The approach utilizes mathematical formulas to calculate single-loss expectancy, annual-loss expectancy, etc. The method lends itself to communicating risk to management and cost justification, but it is impossible to predict the true cost of future events accurately.

Quantitative and Qualitative Risk Assessment

Quantitative = the Quantity of Money

Qualitative = The Quality of the Risk

Ransomware

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

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 my stuff
- **A Vulnerability—**Anything that allows the threat to happen

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

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 used for centuries. Spear phishing is a form of social engineering used for decades. As such, social engineering now accounts for tens and even hundreds of billions of dollars per year in corporate and personal losses.

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 literally hundreds of tools available for free download that will perform steganographic techniques. Many of those techniques are difficult or impossible to discover. These tools are therefore used by attackers 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 or tampering.

Trojan Horse

The *Trojan Horse* is the most common form of malware. It is how most other malware gets delivered. A Trojan Horse occurs anytime you have something with a known, desired function as well as an unknown, undesired function. For example, think of a login screen you use to login to a computer. Say that in addition to logging you in, it also sends your username and password to an attacker. The login function is the known and desired action. Sending your credentials to an attacker is the unknown and undesired action.

Two-Factor Authentication

The three most common authentication factors are:

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

Two-Factor Authentication or (2FA) occurs anytime you employ two or more of these three factors. For example, to log into a computer, you have to provide a PIN (Personal Identification Number) and also provide a specific fingerprint. Assuming proper implementation, this is far better authentication than simple passwords, and you should use 2FA everywhere you can.

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 they are plugged into a computer. (Note: Windows supports autorun scripts, though the feature can be disabled. Mac does not support autorun at all.)

Unified Threat Management

Unified Threat Management is also an all-in-one security appliance. A perfect example of these devices is the "wireless router" we buy for our homes. While this device is indeed a router, it may also be a firewall, intrusion detection system (IDS), gateway anti-virus, dynamic host control protocol (DHCP) server, content filter, and many other security mechanisms all inside one box.

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 where all data is encrypted.

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 you receive a call "from the IRS" telling you that you owe back-taxes and there is a warrant for your arrest and all you have to do is send thousands of dollar's worth of gift cards, and the arrest warrant will go away. Hint: The IRS does not call you and does not accept gift cards as payment of taxes—ever!!!

THE ABCs OF CYBERSECURITY TERMS (CONTINUED)

Work Factor

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

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

The standard used for the creation of digital certificates. An *X.509* certificate consists of two files containing linked information. The private file contains an individual's private key and should be passphrase protected. The public file contains 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 1's or both 0's), 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 utilized by almost all cryptographic algorithms.

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 exploits has not notified the vendor, so they do not know to work on a solution. Since the public (including you) do not know about the attack, you do not know to protect yourself 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.

Zero Knowledge

A *Zero-Knowledge* implementation is when you place your data on a cloud provider's systems in such a way that they have "zero knowledge of your data." To do this locally, you enter a very complex passphrase. That passphrase runs through a process to create an encryption key. The encryption key encrypts your data, and your encrypted data then uploads to the cloud provider. The cloud provider never has access to the passphrase or the encryption key the passphrase creates – hence they have zero knowledge of your data. At any time, you can enter the passphrase, download your data, and decrypt your data.