Cyber Explore

GLOSSARY

Antivirus: Software that prevents, detects, and removes malicious content.

Application (or App): A type of software that allows you to perform specific tasks. Applications for desktop or laptop computers are sometimes called desktop applications, and those for mobile devices are called mobile apps.

Backdoor: An undocumented way of gaining remote access to a program, online service, or an entire computer system.

Basic Input/Output System (BIOS): The most basic software run on a computer which provides the computer with simple instructions about how to start (or "boot") the operating system and crucial applications.

Bluetooth: A technology that allows devices to wirelessly link to each other through pre-shared key authentication and encryption algorithms. These algorithms are widely considered strong when implemented and used correctly. Bluetooth's strength lies within the randomness of the passkey used for pairing with other devices. However, due to the lack of centralized administration and security infrastructure and the pure complexity of the technology, it has vulnerabilities. For example, researchers have shown that Bluetooth headsets can compromise devices in multiple ways. This vulnerability is due to the very common and weak fixed passkeys associated with this device (typically "0000").

Brute Force Attack: A trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software generates a large number of consecutive guesses in an attempt to determine the desired data.

Central Processing Unit (CPU): The physical hardware component that performs all of the instructions that an operating system, application, or user gives to the computer.

Cloud Computing: A type of computing in which shared computing resources, software, or data are delivered as an on-demand service through the internet.

Cloud Types: There are three types of clouds: private, public, and hybrid. See separate entries for definitions. Cloud types should not be confused with the three types of services offered through the cloud (IaaS, SaaS or PaaS).

Cloud Service Provider (**CSP) Lock-in**: The ease (or lack thereof) of moving data between providers or services. Many cloud platforms and services are proprietary, making it difficult to migrate to another provider.

Cookie: A small text file (up to 4KB) created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the website to recognize you and keep track of your preferences.

Cryptography: The practice and study of techniques for securing communication and data in the presence of adversaries.

Data Portability: The ability to transfer data between providers or services. Similar to cloud service provider (CSP) lock-in, when opting to change CSP vendors, the lack of data interchange standards and the sluggish speed of bulk data transfers make data portability between clouds difficult.

Data Protection: The tools and techniques used to ensure data is not lost or corrupted. When selecting a cloud service provider (CSP), consider their services or protocols for backup, recovery, business continuity, and disaster recovery.

Encryption: A technology that codes data into an unreadable form so it can only be decoded by a computer that has the correct key. Encryption prevents unauthorized users from reading data that is transmitted over a network.

File Transfer Protocol (FTP): A standard internet protocol for transmitting files between computers on the internet over Transmission Control Protocol/Internet Protocol (TCP/IP) connections.

Firewall: A software program or piece of hardware that acts as a barrier between a trusted network and other networks such as the internet. A firewall controls access to the resources of a network through a positive control model. The only traffic allowed onto the network is defined in the firewall policy; all other traffic is denied. Before firewalls emerged in the late 1980s, the only real form of network security was performed by Access Control Lists (ACLs) residing on routers. ACLs determined which IP addresses were granted or denied access to the network. The growth of the internet and the resulting increased connectivity of networks meant that this type of filtering was no longer enough to keep out malicious traffic, as only basic information about network traffic is contained in the packet headers. Digital Equipment Corp. shipped the first commercial firewall, DEC SEAL, in 1992, and firewall technology has since evolved to combat the increasing sophistication of cyberattacks.

Hardware: Any part of a computer that has a physical structure, such as the keyboard or mouse. It also includes all of the computer's internal parts, such as its hard disk drive, graphic card, or motherboard.

Hybrid Cloud: A cloud computing environment that uses a mix of on-premises private cloud and public cloud services with orchestration between the two platforms. By allowing workloads to move between private and public clouds as computing needs and costs change, a hybrid cloud gives businesses greater flexibility and more data deployment options.

Hypertext Transfer Protocol (HTTP): The set of communication rules used for transferring files (e.g., text, graphic images, sound, video, and other multimedia files) over the internet.

Hypertext Transfer Protocol Secure (HTTPS): The set of communication rules for securely transferring files (e.g., text, graphic images, sound, video, and other multimedia files) over the internet. The use of HTTPS protects against hackers intercepting data being transmitted.

Hypervisor: A software program that runs and manages virtual machines. By using this program, users can run several different operating systems or other system configurations on a single piece of computer hardware.

Infrastructure as a Service (IaaS): A form of cloud computing that provides virtualized computing resources over the internet, simulating the hardware component of a server.

Insider Threat: A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, vendors, or business associates who have inside information concerning the organization's security practices, data, and computer systems.

Internet Dependency: A reliance on the internet to access data and run software when using cloud services. If the internet temporarily fails due to a lightning strike or internet service provider (ISP) maintenance, the users will not be able to connect to the cloud services and therefore will lose access to their data.

Internet Protocol (IP) Address: An identifier unique to each computer on the internet. This IP address is used to route commands and data from one networked item to the next. IP addresses are not permanently assigned to each machine but can change each time the user logs on to the network.

Kernel: The "middleman" (aka communication) component. It represents the central module of the operating system.

Local Area Network (LAN): A network of devices located and managed within a small geographical area such as a home, school, office building, or group of buildings.

Man-in-the-Middle Attack (MitM): A type of cyberattack where a malicious actor inserts him/herself into the communication between two parties, intercepts online traffic for his own use, and then sends it on to the recipient.

Motherboard: The main printed circuit board within a computer which enables communication between other electronic parts of a computer. It contains the BIOS, and the CPU (microprocessor) fits into a socket on the motherboard.

Network Address Translation or Network Address Translator (NAT): The virtualization of Internet Protocol (IP) addresses. NAT helps improve security and decrease the number of IP addresses an organization needs.

Operating System (O/S): The most important software that runs on a computer. It manages the computer's memory, processes, and all of its software and hardware. It also allows the user to communicate with the computer without knowing how to speak the computer's language. Without an O/S, a computer is useless. Popular operating systems include Microsoft's Windows, Apple's macOS, and Linux.

Packet: A unit of data that has been "wrapped" with instructions regarding transmission and use. Most data sent across networks, especially the internet, is sent in the form of packets.

Packet Filter: A program that uses a set of instructions to allow or block packets being sent or received over a network.

Patch: A small software update to mitigate a vulnerability or fix a bug.

Platform as a Service (PaaS): A cloud computing model that provides a development and hosting platform over the internet, simulating the operating system level of a server. In a PaaS model, a cloud provider delivers hardware and software tools (usually those needed for application development) to its users as a service, allowing users to develop applications without the need to build or maintain the infrastructure of a server.

Port: In computer networking, refers to the digital conduit through which network devices process information from the internet or other devices. Each port is assigned a number and is used to determine what kinds of information are being sent or received. Ports are not a physical plug-in but a representative number.

Private Cloud: A type of cloud computing in which a service provider makes resources, such as applications and storage, available through a proprietary architecture and dedicated to a single organization.

Proxy Server: A server that sits between a client application, such as a web browser, and the server itself. It intercepts all requests sent to the server to see if it can fulfill the request itself. If not, it forwards the request to the real server. It helps protect the real server from being overloaded by requests.

Public Cloud: A type of cloud computing in which a service provider makes resources, such as applications and storage, available to the general public over the internet. Public cloud services may be free or offered on a pay-per-usage model.

Rakshasa Backdoor: Named after a demonic being from Hindu mythology, Rakshasa backdoors attack the BIOS, which boots a computer and helps the O/S. This core software is not typically scanned by antivirus software or other security products, which allows spies to plant malware that remains live and undetected even if the computer's O/S is wiped and re-installed.

Router: A hardware device that forwards data packets between computer networks or from one network to another network like the internet. Routers can operate on either a wired or wireless basis. Based on the address of the destination network in the incoming packet and an internal routing table, the router determines to which port to send out the packet. In the home or small office, a "wireless router" is commonly used to manage internet traffic. It is a combination device that houses a router, network switch, and Wi-Fi in one box.

Secure Shell (SSH) or Secure Socket Shell (SSH): A UNIX-based command interface and set of protocols for securely getting access to a remote computer. It is widely used by network administrators to control servers remotely without having to access the physical server.

Server: A computer program or device that provides services to other programs or computers.

Session Riding: An attack in which a hacker steals a user's cookie in order to use an application in the name of the user. An attacker might also use a cross-site request forgery attack in order to trick the user into sending authenticated requests to arbitrary websites in order to achieve various objectives.

Software as a Service (SaaS): A cloud computing model in which applications are hosted by a vendor or service provider and made available to customers over the internet.

Supply Chain: The system of organizations, people, activities, information, and resources involved in creating, building, and moving a product or service from supplier to customer.

Transmission Control Protocol/Internet Protocol (TCP/IP): A standard that defines how to establish and maintain communication and reliable data transmission between multiple computers or applications simultaneously.

Transport Layer Security (TLS): A protocol that ensures privacy between communicating applications and their users on the internet. When a server and application communicate, TLS ensures that no third party can eavesdrop or tamper with any message. Secure Sockets Layer (SSL) was the prior protocol, and TLS is often still referred to as SSL.

Trojan or Trojan Horse: A type of malware that is often disguised as legitimate software which is used to hack into a computer by misleading users of its true intent. The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy by stealth.

Virtual Machine (VM): An emulation of a computer in a virtualized environment. A VM operates as though it is a physical computer, but in reality all hardware and software components are virtualized in specialized software. This technology enables one physical server to support multiple virtual computers, maximizing computing power and hardware.

Virtual Machine Escape: A cloud vulnerability that exploits a hypervisor remotely by using a vulnerability present in the hypervisor itself. Such vulnerabilities are quite rare, but they do exist. Additionally, a virtual machine can escape from the virtualized sandbox environment and gain access to the hypervisor, and consequentially all the virtual machines running on it.

Virtual Private Network (VPN): A technology that creates an encrypted connection over a less secure network.

Virtualization: The process of creating a software-based (virtual) representation of a device or resource. It allows multiple operating system instances to run concurrently on a single computer and is a means of separating hardware from a single operating system.

Wi-Fi: The standard wireless local area network (WLAN) technology for connecting computers and a myriad of electronic devices to each other and to the internet. Wi-Fi is the common name for the IEEE 802.11 standard, part of a series of wireless standards established by the Institute of Electrical and Electronics Engineers, an international non-profit organization involved with setting standards for computers and communications.

Zero Day: A security vulnerability in software that was previously unknown to the software maker or to antivirus vendors. Because zero-day vulnerabilities are unknown, patches are unavailable. If the vulnerability is discovered by hackers, it can be quietly exploited.