Privacy and Cybersecurity Study Glossary

LWVOR.org

(APPENDIX A: Glossary)

Definition Sources

The study committee collected a broad spectrum of current information. Please understand that term interpretations are a moving target because privacy and cybersecurity Issues evolve and expand daily.

The following glossary definitions are directly quoted from various sources, including individuals and corporate authors identified by these acronyms:

- CNSS: Committee on National Security Systems Instruction, combining terms from the Dept. of Defense, Intelligence Community, and NIST, (CNSSI Glossary)
- HSS: the mission of the U.S. Department of Health & Human Services (HHS) to enhance and protect the health and well-being of all Americans. We fulfill that mission by providing for effective health and human services and fostering advances in medicine, public health, and social services. (HSS)
- NIST: Computer Security Resource Center (CSRC), Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST), (NIST Glossary)
- NICCS: National Initiative for Cybersecurity Careers and Studies (NICCS), Department of Homeland Security. Glossary of Common Cybersecurity Terminology, (NICCS Glossary)
- SANS: SANS Technology Institute, part of Escal Institute of Advanced Technologies; offers specialized training and education for information security professionals. SANS Glossary.

Definitions

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (NIST Glossary)

Multi-Factor Authentication (MFA): An authentication system requiring more than one distinct factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators to provide different factors. Three authentication factors can be something you know, something you have, and something you are. (NIST Glossary)

NOTE: 'Two-factor' authentication is commonly used to add one extra layer of security to consumer devices.

Big data: Large volumes of high velocity, complex and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information. (Big Data Commission, TechAmerica Foundation)

Biometrics: Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. (CNSSI Glossary)

Bot: A computer connected to the Internet that has been surreptitiously/secretly compromised with malicious logic to perform activities under command and control by a remote administrator. (NICCS Glossary)

Botnet: A collection of computers compromised by malicious code and controlled across a network. (NICCS Glossary)

Breach: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. (NICCS Glossary)

Cloud computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST Glossary)

Cookie: A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.(CNSSI Glossary)

Cyber Hygiene: a set of practices for managing the most common and pervasive cybersecurity risks faced by individuals and organizations. Software Engineering Institute, Carnegie Mellon University (2017)

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (CNSSI Glossary)

De-identification: general term for any process of removing the association between a set of identifying data and the data subject. (NIST Glossary)

Denial of Service (DoS): The prevention of authorized access to a system resource or the delaying of system operations and functions. (NIST Glossary)

Disinformation: The deliberate creation and/or sharing of false information in order to mislead (Bellemare, 2019).

Distributed Denial of Service (DDoS): A denial of service technique that uses numerous hosts to perform the attack. (NIST Glossary)

Domain: A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network. SANS Glossary

Domain name: A domain name locates an organization or other entity on the Internet. SANS Glossary

Exploit: A technique to breach the security of a network or information system in violation of security policy. (NICCS Glossary)

Facial recognition: (see biometrics) measurable, physical characteristics or personal behavioral traits used to recognize the identity or verify an individual's claimed identity. Facial images, fingerprints, and iris scan samples are all examples of biometrics. (NIST Glossary)

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. (NIST Glossary)

Hacker: Unauthorized user who attempts to or gains access to an information system. (NIST Glossary)

Internet of Things (IoT): The network of physical objects, machines, people, and other devices that enable connectivity and communications to exchange data for intelligent applications and services. Source: Medium, 2016.

Intranet: A computer network, especially one based on Internet technology, that an organization uses for its internal (and usually private) purposes, closed to outsiders. (NIST Glossary)

Internet Protocol (IP): The method or protocol by which data is sent from one computer to another on the Internet. SANS Glossary

Local-area network (LAN): A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network. (NIST Glossary)

Malware (malicious code): Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. These include ransomware, spyware, Trojan horses, viruses, worms, and other code-based entities that infect hosts. (NIST Glossary) ⏎

[See malware example definitions ransomware, spyware, Trojan horse, virus, and worm.]

Misinformation: the act of sharing information without realizing it's wrong. (Bellamare, 2019).

Network: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (NIST Glossary)

Penetration testing: A test process intended to circumvent system security functions. Note: Penetration testing may leverage system documentation (e.g., system design, source code, manuals) and is conducted within specific constraints. Some penetration test methods use brute force techniques. Also known as "pen testing". (NIST Glossary). This has been described to us as trying the doorknob, to see if it is locked.

Personally identifiable information (PII): Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). NIST Glossary)

Protected Health Information (PHI): The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. (HHS.gov)

Phishing: A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent email or website solicitation, with an imposter masquerading as a legitimate business or reputable person. "Spear-phishing" is a targeted attack for particular data. (CNSSI Glossary)

Privacy (Informational): The control or protection of personal information (Acquisti, Taylor, & Wagman, 2016).

Ransomware: A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again. SANS Glossary.

Spyware: Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. (NIST Glossary)

Trojan horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (CNSSI Glossary)

Ubiquitous Computing: "…small, networked portable computer products in the form of smart phones, personal digital assistants (PDAs), and embedded computers built into many…devices (Want, pg. 2)

Virus: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See malicious code. (CNSSI Glossary)

Virtual Private Network (VPN): A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them. (NIST Glossary)

Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. (NIST Glossary)

Wide area network (WAN): A physical or logical network providing data communications to a larger number of independent users than are usually served by a local area network (LAN). WANs usually spread over a larger geographic area. (NIST Glossary)

Contact information:

Mary Sinclair	cksinclair@gmail.com
Sheila McGinnis	skmcginnis1967@gmail.com
Becky Gladstone	rebecca.gladstone@gmail.com