Introduction to Software Security

Glossary of terminology

Loren Kohnfelder
loren.kohnfelder@gmail.com

Elisa Heymann
elisa@cs.wisc.edu

Barton P. Miller
bart@cs.wisc.edu

Revision 0.3, July 2020.

- AUTHOR NOTE: NIST glossary for reference — http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Access Control List (ACL): Configuration defining access privileges for resources consisting of a list of user or groups, and the type of access permitted.

Adversary – Individual(s) conducting or planning activities harmful to protected systems. [1]

Allowlist: A list of entities or code determined to be non-malicious used to preemptively exclude all others as potentially malicious until they are analyzed. [1]

Asset: Data, or the systems and applications that manage it, as target of a potential threat. [1]

Attack: An attempt to gain unauthorized access to systems, resources, information, or to compromise their availability or integrity. [1]

Attack Surface: The point of entry available to an Adversary to make an Attack. [2]

Authentication: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to data or resources. [1]

Authorization: The decision to permit access to resources or data, often defined by policy or an Access Control List. [1]

Availability: Assurance of timely and reliable access to data or resources. [1]

Backup: A copy of data maintained to facilitate recovery in case of harmful damage or loss.

Blacklist: A deprecated term due to its racial insensitivity. See “Blocklist” for a preferred and acceptable alternative.

Blocklist: A list of entities or code determined to be malicious used to preemptively exclude them.

Bot Net: The collection of exploited hosts used in a DDoS attack

Buffer Overflow: A bug that permits accessing locations of a buffer (typically an array or string) outside of its allocated boundaries. [4.1]

CERT: The common name of the Computer Emergency Readiness Team, a group that responds to computer security incidents in an organization. The first CERT, the CERT Coordination Center (CERT-CC) was founded at Carnegie Mellon University in response to the first Internet worm (www.cert.org).

Confidentiality: Assurance against the disclosure of non-public information. [1]

Cookie: – State information supplied by a server to be maintained on the client side as context for subsequent server use. Commonly, Web servers exchange HTTP Cookies with browsers.

Credential: Evidence (such as a password) used to demonstrate identity or right to privileges.

Cross Site Scripting (CSS or XSS): A Web vulnerability allowing the injection of malicious code into the context of the host website. [4.9.1]

Defense in Depth: Multiple redundant defensive measures. Since an Attack must penetrate all layers of defense, so long as at least one blocks a given Attack the combination is more effective as a whole. [1]

Denial of Service (DoS): Prevention or delay of access by overloading a computer, service, application or network. [1]

Direct attacks: Attacks where input at the attack surface leads to triggering a vulnerability. [1.3]

Directory traversal attack: Manipulating the construction of a path name resulting in access to an unintended file. [3.3]

Distributed Denial of Service (DDoS): A DOS attack that involved the coordinated use of many computers, often many thousands, from around the network.

Exfiltrate: The exporting (downloading) of data from a system by an attacker or implant. [1]

Exploit: A successful Attack that is able to compromise a protected asset. [1]

Impact Surface: The set of all ultimate actions the attacker can cause to happen via these various attack paths. [1.3]

Implant: The name used by the intelligence community for the code that is inserted into a computer system by an attacker. [1]

Incident: An instance of attacker(s) exploiting a vulnerability and causing harm. [1]

Indirect attacks: Attacks where a series of actions cause state changes, and a series of vulnerabilities eventually causing harm (something like a Rube Goldberg apparatus). [1.3]

Insider threat: The threat of a person violating trust and abusing their authorized access. [1.3]

Integrity: Assurance against harmful modification of data or system behavior. [1]

Key: A key is a shared secret, basically a secret number, that is use with a cryptographic algorithm to ensure communication between parties remains private. Symmetric key (or one key) algorithms share a common key between the sender and receive. Public key algorithms uses two keys, a private one for encrypting a message from a party and a public key for decrypting messages from that party. [2.1]

Least Privilege: Best practice that no more privileges than strictly necessary should be granted. [1]

Man-in-the-middle Attack (MitM): An attack on a communication channel in which the Attacker is positioned between the communicants.

Mitigation: A corrective action to fix or reduce the adverse effects of a vulnerability. [1]

Non-repudiation: Assurance that the entity initiating an action is securely documented such that they cannot later deny responsibility. [1]

Offline Attack: An attack that can be analyzed and tested on a system of the attacker's choosing. [1]

Open source software: Software for which the source code is made public. Such software contains a copyright notice that defines the terms of its use. Licenses such as the GNU General Public License (GPL) require anyone that modifies and distributes the software, must also distribute the modified source code. Others, such as the Apache License, allow the user to modify the software and keep the changes private. [1.2]

Persistence: The characteristic of an implant that allows it to survive across reboots and perhaps even across reinstallation of the operating system. [1]

Privilege: Rights to access data or resources in a system. [1]

Sandbox: A restricted, controlled execution environment that prevents potentially malicious software from accessing any system resources except in by limited authorized means.

Security by Obscurity: The dangerous assumption that simply keeping the details of a system hidden from public knowledge provides any real protection.

Software Security: The art and science of improving protection against Attacks, by understanding potential Threats to Assets, detecting and fixing or Mitigating Vulnerabilities. [1]

Stealth: The characteristic of an implant that makes it difficult to detect, causing no visible change to system behavior. A stealthy implant should be invisible to virus scanners and intrusion detection systems. [1]

Threat: A potential harm to Asset(s) that must be protected against. [1]

Vulnerability: A software bug that enables an Exploit. [1]

US-CERT: The Computer Emergency Readiness Team (https://www.us-cert.gov/) is an agency of the US government that coordinates software security vulnerability and best practice information. For a more general discussion, see the entry on "CERT".

Whitelist: A deprecated term due to its racial insensitivity. See "Allowlist" for a preferred and acceptable alternative.

XML Bomb: A malicious XML fragment that causes the XML parser, or the application processing its output, to hang or crash executing. [4.8.4]

XML External Entity (XXE) Attack: An attack based on the External Entity feature of XML that causes the parser to reference a private resource resulting in information disclosure. [4.8.4]