Definitions

Term **Definition**

acquisition

Process of obtaining a system, software product, or software service. Software products may include commercial, off-the-shelf (COTS) products; modified, off-the-shelf (MOTS) products; open source products; or fully developed products.

The above definition was derived from these references:

[IEEE-CS 2008, IEEE-CS 1998]

active attack

An attack that alters a system or data. [CNSS 2010]

Agile

An iterative and incremental (evolutionary) approach to software development which is performed in a highly collaborative manner by self-organizing teams within an effective governance framework with “just enough” ceremony that produces high quality software in a cost effective and timely manner which meets the changing needs of its stakeholders. [Ambler 2013]

antivirus software

Wikipedia: Software used to prevent, detect and remove malware. http://en.wikipedia.org/wiki/Anti-virus

attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [CNSS 2010]

authentication

1. Authentication is the process of determining whether someone or something is who or what it declares itself to be. Passwords, security cards, and biometric solutions are often employed as methods to provide user authentication. With respect to computer systems, the use of digital certificates, which include a digital signature and are issued and verified by a certificate authority (CA) as part of a public key infrastructure, are a way to perform authentication on the Internet. There are three classic ways to authenticate: something you know, something you have, something you are.
2. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. [CNSS 2010]

authorization

Access privileges granted to a user, program, or process or the act of granting those privileges. [CNSS 2010]

availability

1. Availability refers to assurance that authorized users can access and work with information assets, resources, and systems when needed, with sufficient response and performance. Protecting availability involves measures to sustain accessibility to information in spite of possible sources of interference, including system failures and deliberate attempts to obstruct availability
2. The property of being accessible and useable upon demand by an authorized entity.
NIST 800-53: Ensuring timely and reliable access to and use of information. [CNSS 2010]

back door

Typically unauthorized hidden software or hardware mechanism used to circumvent security controls. [CNSS 2010]

blacklisting

The process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of internet resources. [CNSS 2010]

blended attack

A hostile action to spread malicious code via multiple methods. [CNSS 2010]

blue team

1. The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team). [CNSS 2010]
2. The term Blue Team is also used for defining a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based

on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems. [CNSS 2010]

botnet

Wikipedia: A collection of internet-connected computers whose security defenses have been breached and control ceded to an unknown party. Each such compromised device, known as a "bot", is created when a computer is penetrated by software from a malware distribution.
http://en.wikipedia.org/wiki/Botnet

buffer overflow

A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. [CNSS 2010]

cipher

Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both. [CNSS 2010]

classified information spillage

Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification. [CNSS 2010]

cloud computing

1. Cloud computing is a model for enabling 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. [Mell 2009]
2. Large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet. [Foster 2008]
3. A model for enabling 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 2011a]

compromise

Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [CNSS 2010]

computer abuse

Intentional or reckless misuse, alteration, disruption, or destruction of information processing resources. [CNSS 2010]

computer forensics

The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. [CNSS 2010]

computer incident response team (CIRT)

Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability or Cyber Incident Response Team). [CNSS 2010]

computer network attack

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. [CNSS 2010]

computer security (COMPUSEC)

Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated. [CNSS 2010]

confidentiality

1. Confidentiality refers to assurance that information can be read and interpreted only by persons and processes explicitly authorized to do so. Protecting confidentiality involves implementing procedures and measures to prevent malicious and accidental disclosure of information to unauthorized readers.
2. The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. [CNSS 2010]

contamination

Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category. [CNSS 2010]

control

A safeguard or countermeasure employed to reduce the risk associated with a specific threat or group of threats.

correct functionality

Software assurance seeks to provide a level of confidence that software functions in the intended manner as defined by requirements and specifications. Software should establish a secure computing environment and provide required functionality that is free from errors and known vulnerabilities. Software evolution should maintain these properties.

countermeasure

Actions, devices, procedures, or techniques that meet or oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
NIST SP 800-53: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. [CNSS 2010]

covert channel

An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel. [CNSS 2010]

cryptography

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. [CNSS 2010]

cyber attack

An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [CNSS 2010]

cyber incident

Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident. [CNSS 2010] cybersecurity

The ability to protect or defend the use of cyberspace from cyber attacks. [CNSS 2010]

cyberspace

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [CNSS 2010]

data

A subset of information in an electronic format that allows it to be retrieved or transmitted. [CNSS 2010]

defense-in-depth

Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. [CNSS 2010]

denial of service (DoS)

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) [CNSS 2010]

development models

Include incremental, spiral, evolutionary, and agile methods.

disaster tolerance

Fault tolerant system designed to compute-through flood, fire, earthquake, terrorism, etc.; typically across geographical distances.

disruption

An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). [CNSS 2010]

distributed denial of service (DDoS)

A Denial of Service technique that uses numerous hosts to perform the attack. [CNSS 2010]

diverse systems

Include systems-of-systems, network systems, embedded systems, critical infrastructure systems, service-oriented systems, industrial networks, supervisory control and data acquisition systems

(SCADA), distributed control systems (DCS), COTS, legacy systems, and open source software. Awareness and understanding as applied to diverse systems may include

- analysis of system boundaries, interfaces with service providers, and service level agreement to assure required performance
- evaluation of network system design—throughput, load balancing, backup and recovery, and operational monitoring to assure required availability
- analysis of system-of-systems integration and interoperability to assure preservation of security properties and required functional behavior
- assurance of computational and information asset preservation and continuity of operations through backup and switchover methods
- assurance of security properties—including authentication, authorization, integrity, confidentiality, non-repudiation, and privacy across a variety of system architectures, configurations, and providers

driver

Factor that has a strong influence on the eventual outcome or result.

e-pacts

Contractual terms used to define contractual rights to property and limited rights or remedies.

e-torts

Non-contractual and non-statutory claims for injuries arising from any one or more e-risks.

elevation of privilege

Gain capabilities without proper authorization.

encryption

The process of changing plaintext into ciphertext for the purpose of security or privacy. [CNSS 2010]

event

Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. [CNSS 2010]

exploitation channel

Channel that allows the violation of the security policy governing an information system and is usable or detectable by subjects external to the trusted computing base. See also covert channel. [CNSS 2010]

failover	Automatic recovery from faults by shifting to redundant component; system state not maintained.
failure access	Type of incident in which unauthorized access to data results from hardware or software failure. [CNSS 2010]
fault tolerance	Compute-through faults, transparent to users; system state maintained.
flooding	An attack that attempts to cause a failure in a system by providing more input than the system can process properly. [CNSS 2010]
hacker	Unauthorized user who attempts to or gains access to an information system. [CNSS 2010]
hacktivism	Wikipedia: The use of computers and computer networks as a means of protest to promote political ends. http://en.wikipedia.org/wiki/Hacktivist
hashing	The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. [CNSS 2010]
identity theft	Wikipedia: A form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity. http://en.wikipedia.org/wiki/Identity_theft
inadvertent disclosure	Type of incident involving accidental exposure of information to an individual not authorized access. [CNSS 2010]
incident	An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CNSS 2010]
indicator	Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack. [CNSS 2010]

information

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. [CNSS 2010]

information assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [CNSS 2010]

information disclosure

Exposing information to someone not authorized to see it.

information leakage/spillage

See unauthorized disclosure.

information security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [CNSS 2010]

information system (IS)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [CNSS 2010]

inside(r) threat

An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. [CNSS 2010]

integrity

1. Integrity of information is about assurance that information remains intact, correct, and authentic. Protecting the integrity involves preventing and detecting unauthorized creation, modification, or destruction of information.
2. The property whereby an entity has not been modified in an unauthorized manner.
NIST 800-53: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [CNSS 2010]

internet

The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB and (b) the name and address spaces managed by the Internet

Corporation for Assigned Names and Numbers (ICANN). [CNSS 2010]

intranet

A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency). [CNSS 2010]

intrusion

Unauthorized act of bypassing the security mechanisms of a system [CNSS 2010]

intrusion detection system (IDS)

Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations). [CNSS 2010]

intrusion detection system (IDS) (host-based)

IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks. [CNSS 2010]

intrusion detection system (IDS) (network-based)

IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment. [CNSS 2010]

intrusion prevention system (IPS)

System that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. [CNSS 2010]

issue/problem

A condition that directly produces a loss or adverse consequence.

jamming

An attack that attempts to interfere with the reception of broadcast communications[CNSS 2010] key

A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. [CNSS 2010]

keystroke monitoring

The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. [CNSS 2010]

life-cycle processes

Include new system development, legacy system evolution, and acquisition, both for systems through supply chains, open source, and COTS, and for services through external providers. Also includes process models such as CMMI.
Supervisory Control And Data Acquisition "a computer system for gathering and analyzing real time real data."
http://www.webopedia.com/TERM/S/SCADA.html

macro virus

A virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate. [CNSS 2010]

malicious applets

Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system. [CNSS 2010]

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. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [CNSS 2010]

malicious insider

See inside(r) threat.
CERT Program: a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. [SEI 2013]

malicious logic

Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. [CNSS 2010] malware

See malicious code, malicious applets, and malicious logic. [CNSS 2010]

man-in-the-middle attack (MitM)

A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. [CNSS 2010]

masquerading

A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. [CNSS 2010]

mean time between failures

Expected or observed time between consecutive failures in a system or component. [ISO/IEC/IEEE 2010]

mean time to repair

Expected or observed duration required to return a malfunctioning system or component to normal operations. [ISO/IEC/IEEE 2010]

mission

Fundamental purpose of the system that is being examined.

mission risk

Probability of mission failure (i.e., not achieving key objectives).

mitigation

To address or alleviate a problem.

network resilience

A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands. [CNSS 2010]

non-repudiation

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
NIST 800-53: Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. [CNSS 2010]

objective

Tangible outcome of result that must be achieved when pursuing a mission.

operational controls

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). [CNSS 2010]

operational resilience

CERT Program: The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk. [Allen 2010]

operations security (OPSEC)

Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. [CNSS 2010]

opportunity

The probability of realizing a gain.

outside(r) threat

An unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. [CNSS 2010]

packet sniffer

Software that observes and records network traffic. [CNSS 2010]

passive attack

An attack that does not alter systems or data. [CNSS 2010]

passive wiretapping

The monitoring or recording of data while it is being transmitted over a communications link, without altering or affecting the data. [CNSS 2010]

password

A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data. [CNSS 2010] patch management

The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. [CNSS 2010]

penetration

See intrusion.

penetration testing

A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. [CNSS 2010]

phishing

Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. [CNSS 2010]

port scanning

Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). [CNSS 2010]

potential impact

The loss of confidentiality, integrity, or availability that could be expected to have a limited (low) adverse effect, a serious (moderate) adverse effect, or a severe or catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals. [CNSS 2010]

precursor

A sign that an attacker may be preparing to cause an incident. See indicator. [CNSS 2010]

red team

A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. [CNSS 2010]

redundancy

Multiple “backed-up” components.

reliability

Ability (of a system) to function as intended over time.

replay attacks

An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. [CNSS 2010]

repudiation

Claiming to have not performed an action.

retrospective analysis

CERT Program: Analysis of information and reports from a historical perspective to provide both a comprehensive view of emerging threats and risks and an evaluation of the success of resolution strategies. [Dorofee 2007]

risk

1. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.
Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [CNSS 2010]
2. The possibility of suffering loss, destruction, modification, or denial of availability of an asset.

risk assessment

The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).
NIST SP 800-53: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.
Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [CNSS 2010]

risk management

1. The process of managing risks to organizational operations (including mission, functions, image, or reputation),

organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and 4) documenting the overall risk management program.
NIST SP 800-53: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system, and includes: 1. the conduct of a risk assessment; 2. the implementation of a risk mitigation strategy; and 3. employment of techniques and procedures for the continuous monitoring of the security state of the information system. [CNSS 2010]
2. A process used to identify, analyze, and mitigate the risk (comprised of assets, threats, vulnerabilities, and controls); and provide strategies for sustaining the security requirements of an information asset.

rootkit

A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker’s activities on the host and permit the attacker to maintain root-level access to the host through covert means. [CNSS 2010]

safeguards

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. [CNSS 2010]

security

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach. [CNSS 2010]

security controls

The management, operational, and technical controls (that is, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [CNSS 2010]

security incident

See incident.

security objectives

Confidentiality, integrity, or availability.

security properties

Include authentication, authorization, confidentiality, integrity, non-repudiation, and privacy.

security safeguards

Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [CNSS 2010]

situational awareness

Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future. [CNSS 2010]

sniffer

See packet sniffer or passive wiretapping. [CNSS 2010]

social engineering

An attempt to trick someone into revealing information (e.g., a password) that can be used to attack an enterprise. [CNSS 2010]

software analytics

1. Include reverse-engineering technologies that transform arbitrary control logic into structured form and function abstraction to recover designs and specifications from implementations.
2. Specialized technologies and processes are necessary to analyze and assure functional and security properties of software. Analysis subject matter extends across the life cycle and includes specification, design, code, inspection, and test artifacts. Analytic methods include reverse engineering to transform arbitrary control logic into structured form for improved understanding and function abstraction to recover designs and specifications from implementations.

software assurance(CNSS)

Software assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. [CNSS 2010] software assurance (SEI/CERT)

Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures. [Mead 2010]

software quality

Capability of a software product to satisfy stated and implied needs when used under specified conditions [ISO 2009].

software security

Engineering software so that it is as vulnerability- and defect-free as possible and continues to function correctly in spite of attack or misuse.

software security assurance

Justified confidence that software-reliant systems are adequately planned, acquired, built, and fielded with sufficient security to meet operational needs, even in the presence of attacks, failures, accidents, and unexpected events [SSMA Project].

spam

Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. [CNSS 2010]

spillage

Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level. [CNSS 2010]

spoofing

1. Faking the sending address of a transmission to gain illegal entry into a secure system. [CNSS 2010]
2. The deliberate inducement of a user or resource to take incorrect action.
Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. [CNSS 2010]

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. [CNSS 2010]

steganography

The art, science, and practice of communicating in a way that hides the existence of the communication. [CNSS 2010] strength

A condition that is driving an entity (e.g., project, system) toward a desired outcome.

supply chain

A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. [CNSS 2010]

supply chain attack

Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. [CNSS 2010]

system

Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See also information system. [CNSS 2010]

system defenses

Include filtering, monitoring, and control at network, system, and application levels and specific technologies including encryption and multi-layering.

system integrity

Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. [CNSS 2010]

system vulnerabilities

Include system architecture, design, implementation, operational, and user characteristics that enable attack strategies.

tactical risk

Probability that an event will lead to a negative consequence or loss.

tampering

An intentional event resulting in modification of a system, its intended behavior, or data. [CNSS 2010]

technical security controls

Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [CNSS 2010] technical vulnerability information

Detailed description of a weakness to include the implementable steps (such as code) necessary to exploit that weakness. [CNSS 2010]

threat

1. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSS 2010]
2. Any event that will cause an undesirable impact or loss to an organization if it occurs.

threat assessment

Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. [CNSS 2010]

threat environments

Include attack sources, motivations, technologies, methods, targets, and consequences.

threat monitoring

Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security. [CNSS 2010]

threat source

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. [CNSS 2010]

time bomb

Resident computer program that triggers an unauthorized act at a predefined time. [CNSS 2010]

traffic analysis (TA)

Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence. [CNSS 2010]

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. [CNSS 2010]

unauthorized access

Any access that violates the stated security policy. [CNSS 2010]

unauthorized disclosure

An event involving the exposure of information to entities not authorized access to the information. [CNSS 2010]

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. [CNSS 2010]

vulnerability

1. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [CNSS 2010]
2. The absence or weakness of a safeguard. It can also be described as a weakness in an asset or the methods of ensuring that the asset is survivable.

vulnerability assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [CNSS 2010]

waterfall life-cycle model

A software life-cycle or product life-cycle model, described by W. W. Royce in 1970, in which development is supposed to proceed linearly through the phases of requirements analysis, design, implementation, testing (validation), integration and maintenance [http://www.websters-online-dictionary.org/Wa/Waterfall+Model.html]

white team

1. The group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of their enterprise’s use of information systems. In an exercise, the White Team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. The White Team helps to establish the rules of engagement, the metrics for assessing

results and the procedures for providing operational security for the engagement. The White Team normally has responsibility for deriving lessons-learned, conducting the post engagement assessment, and promulgating results. [CNSS 2010]
2. Can also refer to a small group of people who have prior knowledge of unannounced Red Team activities. The White Team acts as observers during the Red Team activity and ensures the scope of testing does not exceed a pre-defined threshold. [CNSS 2010]

worm

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See malicious code. [CNSS 2010]