Security Taxonomy

Rev 1/22/2013

Item	Term	Definitions	Source: NISTIR 7298	Source: NIST 800-63	Source: Other	Notes	Proposed changes
1	Authenticate (v)	1. To confirm the identity of an entity when that identity is presented.	X		SP8000-32 CNSSI-4009		
		2. To verify the identity of a user, user device, or other entity			CNSSI-4009		
2	Authentication (adj)	1. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.	X		SP800-53 SP800-53A SP800-27, FIPS 200, SP800-30		
		2. The process of establishing confidence of authenticity			FIPS 201		
		3. Encompasses identity verification, message origin authentication and message content authentication.			FIPS 190		
3	Authenticator (n)	1. The means used to confirm the identity of a user, process, or device (i.e., user password or token).	X				
4	Anti-spoof (n)	1. Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker.	X		CNSSI-4009		
5	Attribute (n)	1. An inherent characteristic; *also* **:** an accidental quality. an object closely associated with or belonging to a specific person, thing, or office <a scepter is the attribute of power>; especially : such an object used for identification in painting or sculpture. a word ascribing a quality.			Merriam Webster Free Dictionary	Attributes can be "credentials"	
6	Credential (n)	1. An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.	X			Credentials can be "attributes". If attributes are consided as credentials, then establishing "Identity" is an authentication process. This allows re-using the probability calculation framework already established for authentication. Propose that any authentication with a probability of error less than 1e-10 is an identity establishing process	
		2. Evidence attesting to one's right to credit or authority.			FIPS 201		
		3. Evidence or testimonials that support a claim of identiy or assertion of an attrtibute and usually are intended to be used more than once.			CNSSI-4009		

Security Taxonomy

Rev 1/22/2013

Item	Term	Definitions	Source: NISTIR 7298	Source: NIST 800-63	Source: Other	Notes	Proposed changes
7	Entity (n)	1. Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.		X	SP 800-27		
		2. Any participant in an authentication exchange; such a participant may be human or non-human, and may take the role of a claimant and/or verifier.			FIPS 196		
8	Identity (n)	1. A unique name for an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include suficient information (for exampole and address, or some unique identifier such as an employee number or account number) to make the complete name unique.	X		SP 800-48		
		2. A set of attributes that uniquely describe a person within a given context.		X			
		3. The set of physical and behavioral characteristics by which an individual is uniquely recognizable.	X		FIPS 201		
		4. The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.	X		CNSSI-4009		
9	Spoofing (v)	1. "IP spoofing" refers to sending a network packet that appears to come from a source other than its original source	X		SP 800-48		
		2. The ability to receive a message by masquerading as the legitimate destination.			FIPS 191		
		3. Masquerading as the sending machine and sending a message to a destination.					
		4. Faking the sending address of a transmission to gain illegal entry into a secure system. Impersonating, masquerading, piggy backing, and mimicking are forms of spoofing			CNSSI-4009		
		5. The deliberate inducement of a user or resource to take incorrect action.					
10	Malicious Applets (n)	1. Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system.		X	CNSSI-4009		
11	Malicious Code (n)	1. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Spyware and some forms of adware are also examples of malicious code.	X		SP800-53, CNSSI-4009		
12	Malicious Logic (n)	1. Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.		X	CNSSI-4009		

Security Taxonomy

Rev 1/22/2013

Item	Term	Definitions	Source: NISTIR 7298	Source: NIST 800-63	Source: Other	Notes	Proposed changes
13	Malware (n)	1. A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.		X	SP 800-61		
		2. A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.		X			
14	Multifactor Authentication (n)	1. Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. passsword/PIN; (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator.					
15	Taxonomy (n)	1. Corporate taxonomy is the hierarchical classification of entities of interest of an enterprise, organization or administration, used to classify documents, digital assets and other information. Taxonomies can cover virtually any type of physical or conceptual entities (products, processes, knowledge fields, human groups, etc.) at any level of granularity.			Wikipedia http://en.wikipedia.org/wiki/Enterprise_taxonomy		