INCOSE International Symposium

Security Systems Engineering: Toward a Harmonized Taxonomy

Marcus Thompson, Mike Ryan, Alan McLucas

THE UNIVERSITY OF NEW SOUTH WALES

AUSTRALIAN DEFENCE FORCE ACADEMY

Security Terminology

- Traditionally, there are three types of security: Personnel; Physical; Electronic (incorporating cyber security)
- The specification and design of modern security systems are hampered by:
  - prominent standards bodies have produced definitions that lack commonality in meaning and interpretation
  - overlapping and recursive terminology
  - a strong focus on electronic or cyber security
- Consequently, current security terms and definitions are of little help to stakeholders when establishing their requirements.

Definitions of Security

- Every standards organisation has a different definition of security:
  - ‘measures used to provide physical protection of resources against deliberate and accidental threats’ (ISO).
  - ‘minimising vulnerabilities of assets and resources’ (ITU).
  - ‘information is secure if it cannot be intercepted, understood if intercepted, altered or faked either during or beyond an interaction’ (CSIRO).
  - ‘the protection of the interests of those relying on information systems from harm’ (OECD).
  - ‘measures taken to protect a system’ (IETF)
  - ...

Definitions of Security

- Every standards organisation has a different definition of security:
  - ...
  - ‘the condition of a system that results from the establishment and maintenance of measures to protect the system’ (IETF)
  - ‘the condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss’ (IETF)
  - ‘the security and preservation of confidentiality, integrity and availability of information’ (Standards Australia).

Definitions—Physical Security

- Measures intended to improve protection by means such as fencing, locks, ... , alarms, access controls, vehicle control, and housekeeping. (US Government 2011)
- ... physical measures designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (OSPA 2011)
- Tangible means of preventing unauthorized physical access to a system. (IETF 2010)
- The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information. (National Computer Security Center 1988)

Definitions—Personnel Security

- Procedures to ensure that persons who access a system have proper clearance, authorization, and need-to-know as required by the system's security policy. (IETF 2010)
- The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. (National Computer Security Center 1988)

Definitions—Electronic Security

- ... the security and preservation of confidentiality, integrity and availability of information. (Standards Australia 2004)
- The preservation of confidentiality, integrity and availability of information. (Standards Australia 2006b)
- Information is secure if it cannot be intercepted, understood if intercepted, altered or faked either during or beyond an interaction. (CSIRO 2009)
- A computer is secure if you can depend on it and its software to behave as you expect (Garfinkel and Spafford).
- Ability of a system to protect information and resources with respect to confidentiality and integrity. (Ross 1999)
- ...

Definitions—Electronic Security

- ...
- The protection of the interests of those relying on information systems from harm. (OECD 1992)
- Measures taken to protect a system; the condition of a system that results from the establishment and maintenance of measures to protect the system; and the condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss. (Shirey 2010)
- A system characteristic as well as a set of mechanisms which span the system both logically and physically. (Stoneburner 2001)
- ...

Definitions—Electronic Security

- ...
- The protection of information and control systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide availability, integrity, and confidentiality. (US Government 2011)
- The policies, practices, and procedures that are applied to information systems to ensure that the data and information that is held within or communicated along those systems is not vulnerable to inappropriate or unauthorized use, access, or modification and that the networks that are used to store, process, or transmit information are kept operational and secure against unauthorized access. (Symantec 2011)
- ...

Definitions—Electronic 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)
- The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute. (OSPA 2011)
- unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards. (ICANN 2011)
- ....

Definitions—Electronic Security

- ...
- The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order. (US Government 2006)

Other Security Terms

- A *security service* is:
  - ‘a service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers’ (ISO).
  - ‘a processing or communication service that is provided by a system to give a specific kind of protection to system resources’ (IETF).
- A *security mechanism* is:
  - an activity that, alone or in combination with others, contributes to the provision of a security service (ISO).

Other Security Terms

- In 1989, the ISO defined *security services* as authentication, access control, confidentiality, integrity, and non-repudiation. (then included in Recommendation X.800 by ITU in 1991).
- In 1992, the OECD published their Guidelines for the Security of Information Systems that defined security as the protection of availability, confidentiality and integrity.
- In 1996, the Control Objectives for Information and related Technology (COBIT) Framework defined a list of six *control criteria* of availability, confidentiality, integrity, effectiveness, efficiency, compliance and reliability.
- During the following year, the IETF adopted the original ISO and ITU list of security services, but added authorisation, auditing and back-ups (IETF 1997).

Other Security Terms

- Then in 2001, NIST presented confidentiality, integrity, availability, accountability and assurance as *security objectives* and defined *security services* in three subsets:
  - *supporting security services*: identification, cryptographic key management, security administration and system protection
  - *prevention security services* of protected communications, authentication, authorisation, access control, non-repudiation and transaction privacy
  - *detection and recovery security services* were defined as audit, intrusion detection and containment, proof of wholeness and restore the secure state.

Security Terminology

	ISO	ITU	OECD	COBIT	IETF	NIST	Standards Australia
authorisation					x		
confidentiality	x	x	x	x	x	x	x
integrity	x	x	x	x	x	x	x
non-repudiation	x	x					
access control	x	x			x		
availability			x	x		x	x
authentication	x	x			x		
auditing					x		
assurance						x	
accountability						x	
backups					x		
effectiveness				x			
efficiency				x			
compliance				x			
reliability				x			

Terms that are called variously: *security services*, *security objectives*, or *control criteria*.

Security Terminology

The terms associated with security services and mechanisms are a confusing mix of actions, states, and management functions.

	Action	State	Governance Function
authorisation	x		
non-repudiation	x		
access control	x		
authentication	x		
confidentiality		x	
integrity		x	
availability		x	
auditing			x
assurance			x
accountability			x
backups			x
effectiveness			x
efficiency			x
compliance			x
reliability			x

Other Security Terms

- Other commonly used security terms have recursive definitions.
- For example, NIST defines a threat as:
  - ‘the potential for an actor to exploit or trigger a specific vulnerability’.
- And the Australian Government’s Information Security Manual defines a vulnerability as:
  - ‘a weakness of an asset or group of assets that can be exploited by one or more threats’.

A Better Taxonomy

- The ultimate aim of security is to retain a resource of value at some particular nominated state (whether that is preserving a bank balance, ensuring personal safety, preserving the confidentiality of information in a database, or safeguarding the integrity of a territorial border).
- So:
  - *Security is the maintenance of the nominated state of a designated resource.*
- where the nominated state is a specific condition that is determined through an assessment of the intrinsic value of the resource that is designated as requiring security.

A Better Taxonomy

- So:
  - *Security is being **maintained** when an action has an authorised effect on the **nominated state** of a **designated resource**.*
- Note the state of a particular resource is not preordained—the owner of the resource must make an assessment of what effects are *authorised*, on which particular *nominated* state, of whichever resources are *designated* to be important.
- Security is a state that is desired by stakeholders, not one that is natural and predefined for any system.
- Governance therefore has a significant role to play before any design of a security system can be undertaken.

A Better Taxonomy

- This base definition can be elaborated further—the phrase ‘an action has an authorised effect’ can be decomposed to include the detail of the entity performing the action, the combination of which results in an authorised effect.
- The entity (such as a person, animal, program, or bot) that must be able to be identified to a sufficient degree (commonly called *authentication*). The necessary property of the action is that it is *accessible* (at all entities, to a single authenticated entity, or to a number of entities). So, we could then elaborate:
  - *Security is being **maintained** when an authenticated entity **performs** an accessible action on **the nominated state** of a **designated resource**.*

A Better Taxonomy

- This definition is still not complete, however. Security is not necessarily maintained unless the authorised effect is able to be attributed to a particular entity-action combination.
- This property is known as *attribution* (that is, it is known—to a desired state of certainty— that an entity performed an action) or, in the negative, as *non-repudiation* (that is, the entity cannot deny that the action was performed by them).
- So:
  - *Security is being **maintained** when an **authenticated entity** is known to perform an **accessible action** on **the nominated state** of a **designated resource**.*

Some Examples

- Border security is being maintained when an identified (*authenticated*) individual (*entity*) is recorded as (*known to*) crossing (*perform an accessible action*) a controlled (*nominated state*) border (*designated resource*).
- Physical security of a home is being maintained when a known (*authenticated*) individual (*entity*) is welcomed into (*known to*) the home and respects (*perform an accessible action*) the possession (*nominated state*) of belongings of value (*designated resource*).
- Electronic security is being maintained when a recognised (*authenticated*) person/computer/bot (*entity*) is recorded as (*known to*) accessing/manipulating/transmitting/copying (*accessible action*) controlled (*nominated state*) data (*designated resource*).

A Better Taxonomy

- Our improved definition of security also allows us to provide better definitions of a security service and security mechanisms:
  - *A security service is a process that, alone or in combination with others, maintains the nominated state of a designated resource.*
  - *A security mechanism is an activity that, alone or in combination with others, contributes to the provision of a security service.*

A Better Taxonomy

Definition	*Security is the maintenance of the nominated state of a designated resource.*				
Maintenance	*an authorised action is performed*			*on the nominated state of a designated resource*	
Security Services	Authorisation			Resource Assessment	
	an authenticated entity	*is known to*	*perform an accessible action*	*on the nominated state*	*of a designated resource*
Security Mechanisms	Authentication	Attribution	Access Control	State Nomination	Resource Designation

A Better Taxonomy

authorisation
confidentiality
integrity
availability
access control
non-repudiation
authentication

Definition	*Security is the maintenance of the nominated state of a designated resource.*				
Maintenance	*an authorised action is performed*			*on the nominated state of a designated resource*	
Security Services	Authorisation			Resource Assessment	
	an authenticated entity	*is known to*	*perform an accessible action*	*on the nominated state*	*of a designated resource*
Security Mechanisms	Authentication	Attribution	Access Control	State Nomination	Resource Designation

A Better Taxonomy

- *Threat:* A threat is a *possible action* that may have an *unauthorised effect* on the *nominated state* of a *designated resource*.
- *Vulnerability:* A vulnerability is a *possible undesirable effect* on the *nominated state* of a *designated resource*.
- *Security Event:* A security event occurs when a threat is realised.
- *Security Attack:* A security attack is a combination of security events coordinated to achieve a particular objective.
- *...*

A Better Taxonomy

- ...
- *Security Breach:* A security breach occurs when a vulnerability is realised (that is, a threat successfully exploits a vulnerability).
- *Countermeasure:* A countermeasure is a feature or function of a security system that removes vulnerabilities or counters threats (that is, prevents a breach).

Mechanisms: Conditions and Means

- Setting the required level of each security mechanism is a specific governance function that will be derived from the threat assessment and risk management processes within an organisation.
- Each mechanism should be described in both functional and physical terms:
  - in terms of the *conditions* required by the organisation for that mechanism, and
  - in terms of the possible physical *means* by which the mechanism can be implemented.

Mechanisms: Conditions and Means

- By way of example, consider the security mechanism of *authentication* of a holder of a bank account when accessing that account online.
- *Conditions:* What degree of authentication is required? How certain must the bank be of the identity of the person accessing the account?
- *Means:* Almost 100% certainty can be achieved using DNA analysis, but that is clearly impractical. The bank must then conduct a risk analysis of any other lesser authentication mechanism.

Mechanisms: Conditions and Means

- For example, the bank could use a customer identity number in combination with a password.
- However, it must accept that it cannot guarantee that the combination is not being used by a party other than the intended customer—in which case, for example, it could manage the risk by:
  - the bank accepts responsibility if the account is hacked, and
  - the customer accepts responsibility if the logon details were knowingly or unwittingly exposed by the customer to another person.

Conclusion

- Current security terminology is overlapping, recursive and at times contradictory in nature.
- The terms and associated definitions used by several prominent standards organisations present a confusing mix of actions, states and governance functions that lack commonality in meaning, and tend to be specific to a single problem domain.
- We propose a definition and an associated taxonomy to be:
  - Better harmonized, non-recursive, and hierarchically structured; and
  - applicable across electronic (cyber), physical, and personnel security domains

A Better Taxonomy

Definition	*Security is the maintenance of the nominated state of a designated resource.*				
Maintenance	*an authorised action is performed*			*on the nominated state of a designated resource*	
Security Services	Authorisation			Resource Assessment	
	an authenticated entity	*is known to*	*perform an accessible action*	*on the nominated state*	*of a designated resource*
Security Mechanisms	Authentication	Attribution	Access Control	State Nomination	Resource Designation

Acronyms

- CNSS – Committee on National Security Systems
- COBIT – Control Objectives for Information and related Technology
- CSIRO – Commonwealth Scientific and Industrial Research Organisation
- ISO – International Standards Organisation
- ICANN – Internet Corporation for Assigned Names and Numbers
- IETF – Internet Engineering Task Force
- ITU – International Telecommunications Union
- OECD – Organisation for Economic Co-operation and Development
- OSPA – Operations Security Professional's Association

References

- Australian_Government (2007), 'Australian Government Protective Security Manual', in Attorney General's Department (ed.), (Barton: Commonwealth of Australia).
- CNSS (2010), 'National Information Assurance Glossary', *CNSS Instruction No. 4009*.
- Commonwealth_of_Australia (1979), 'Australian Security Intelligence Organisation Act', in Commonwealth of Australia (ed.), *Act No. 113 of 1979 (as amended)*.
- Garfinkel, Simson and Spafford, Gene (1996), *Practical UNIX and Internet Security* (2 edn.; Sebastopol, CA: O'Reilly).
- ICANN (2012), 'Glossary: Terms Applicable to the Application Process', <http://www.icann.org/en/topics/new-gtlds/glossary-30aug11-en.pdf>, accessed 5 February.
- IETF (2010), 'Internet Security Glossary', in Robert W. Shirey (ed.), *IETF RFC 2828* (Arlington: The Internet Society).
- ISO (1989), 'Information processing Systems - Open Systems Interconnection - Basic Reference Model', *Part 2: Security Architecture* (International Organisation for Standardisation (ISO)).
- --- (1998), 'ISO/IEC 2382-8 Information technology — Vocabulary — Part 8: Security'.
- ITU (1991), 'Security Architecture for Open Systems Interconnection for CCITT Applications', *Recommendation X.800* (Geneva).
- National_Computer_Security_Center (1988), 'Glossary of Computer Security Terms', in National Security Agency (ed.), (NCSC-TG-004).
- OSPA (2011), 'OPSEC Glossary of Terms', <http://www.opsecprofessionals.org/>, accessed 26 November.
- .....

References

- ...
- Ross, Seth T. (1999), *Unix System Security Tools* (McGraw-Hill Companies) 444.
- Standards_Australia (2004), 'Information Security Risk Management Guidelines', (Sydney).
- Standards_Australia (2006a), 'Security Risk Management', (HB 167:2006 Sydney: Standards Australia).
- Standards_Australia (2006b), 'Information technology - Security techniques - Code of practice for information security management', *AS/NZS ISO/IEC 17799:2006* (Sydney: Standards Australia).
- Standards_Australia (2008), 'Lexicon of Key Terms used in Security', (Sydney: Standards Australia).
- Standards_Australia (2010), 'Business Continuity - Managing disruption-related risk', *AS/NZS 5050:2010* (Sydney: Standards Australia).
- Symantec (2011), 'Glossary', < http://www.symantec.com/business/security_response/glossary/define.jsp?letter=a&word=also-known-as>, accessed 11 May
- United_States_Government (2006), 'National Industrial Security Program Operating Manual', in Department of Defense (ed.), (Washington: Department of Defense).
- United_States_Government (2011), 'Catalog of Control Systems Security: Recommendations for Standards Developers', in Department of Homeland Security (ed.), (Washington).