4.5 5 Knowledge Area: System Security

The System Security knowledge area focuses on the security aspects of systems that are composed of components and connections, and use software. Understanding the security of a system requires viewing it not only as a set of components and connections, but also as a complete unit in and of itself. This requires a holistic view of the system. Together with the Component Security and Connection Security KAs, the System Security KA addresses the security issues of connecting components and using them within larger systems

4.5.1 Knowledge Units and Topics

The following table lists the essentials, knowledge units, and topics of the System Security knowledge area.

SYSTEM SECURITY		
Essentials - Holistic approach, - Security policy, - Authentication, - Access control, - Monitoring, - Recovery, - Testing, and - Documentation.		
Knowledge Units	**Topics**	**Description/Curricular Guidance**
System Thinking		This knowledge unit introduces the student to thinking of the system as a whole, rather than simply a number of connected components.
	What is a system?	This topic discusses the definition of system and how it depends on context.
	What is systems engineering?	This topic discusses the definition of system and how it depends on context.
	Holistic approaches	This topic covers viewing the system as a whole rather than as simply a collection of interconnected components. For example, viewing the human, organizational and environmental considerations of the whole as opposed to viewing each individual component and connection and how they affect the view of risk.
	Security of general-purpose systems	This topic covers the security considerations of computing and of systems in general.
	Security of special-purposes systems	This topic covers security considerations derived from the purposes to which the system is put.
	Threat models	This topic covers what security problems can arise and how they might be realized, detected, and
	Requirements analysis	This topic presents requirements derivation and validation throughout the system lifecycle, including in various methodologies such as the waterfall and agile development methodologies.

[*See also Software Security KA for related content*]	Fundamental principles	The Software Security knowledge area covers these principles in detail, but they also apply here.
	Development for testing	This topic covers designing systems for ease and effectiveness of testing.
System Management		This knowledge unit describes techniques for including security considerations throughout the management of the system.
	Policy models	This topic includes examples such as Bell- LaPadula, Clark-Wilson, Chinese Wall, and Clinical Information Systems Security.
	Policy composition	This topic covers restrictiveness.
	Use of automation	This topic includes data mining, machine learning and related techniques, and their benefits and limitations.
[*See also Software Security KA for related content*]	Patching and the vulnerability life cycle	This topic includes the security issues patching raises such as whether to patch a system, and patching a running system, as well as how to handle vulnerability reports.
	Operation	This topic includes security in operation, and the importance of usability considerations.
	Commissioning and decommissioning	This topic describes the security considerations when installing and removing a system.
	Insider threat	This topic includes examples of insider threats such as data exfiltration and sabotage, and covers countermeasures.
	Documentation	This topic covers security and assurance documentation as well as installation and user guides focused on the system itself.
	Systems and procedures	This topic discusses procedures that are used to manage systems.
System Access [*See also Human Security KA for related content, p. 44.*]		This knowledge unit introduces security considerations about controlling access to systems. It deals with the identification of entities, and confirmation of that identification to the desired level of granularity. Topics overlap with the Human Security knowledge area, but the focus here is on the system elements and not the human ones.
	Authentication methods	Authentication methods refers to human-to-system or system-to-system authentication; examples include passwords, biometrics, dongles, and single sign-on.
	Identity	How is identity represented to the system? This topic includes roles as well as names, etc.
System Control		This knowledge unit examines the security considerations involved in controlling the system itself. It includes detecting, compensating for, defending against, and preventing attacks.

[*See also Data Security KA for related content*]	Access control	This topic focuses on controlling access to resources, and the integrity of the controls, rather than their controlling access to data, which is covered in the Data Security knowledge area.
	Authorization models	This topic covers the management of authorization across many systems, and the distinction between authentication and authorization.
	Intrusion detection	This topic covers anomaly, misuse (rule-based, signature-based) and specification-based techniques.
	Attacks	This topic covers attack models (such as attack trees and graphs) and specific attacks.
	Defenses	This topic includes examples such as ASLR, IP hopping, and intrusion tolerance.
	Audit	This topic covers logging, log analysis, and relationship to intrusion detection.
	Malware	This topic includes examples such as computer viruses, worms, ransomware, and other forms of malware.
	Vulnerabilities models	This topic includes examples such as RISOS and PA; and enumerations such as CVE and CWE.
	Penetration testing	This topic covers the Flaw Hypothesis Methodology and other forms (ISSAF, OSSTMM, GISTA, PTES,
[*See also Data Security KA for related content*]	Forensics	This topic focuses on the system requirements for forensics.
	Recovery, resilience	This topic includes availability mechanisms.
System Retirement		This knowledge unit examines how retiring a system at or before its end of life may affect the security of other systems, or of the organization that used the system.
	Decommissioning	This topic examines how retiring a system at or before its end of life may affect the security of other systems, or of the organization that used the system. The student should understand the effects of removing a system, or components or connections within a system, upon the security of the system as a whole.
	Disposal	This topic includes wiping media and other forms of destruction to prevent sensitive information (such as PII) from being recovered.
System Testing [*See also Software Security KA, p. 23, and Component Security KA, p. 29, for related content.*]		This knowledge unit covers considerations of testing systems to ensure they meet security requirements.

	Validating requirements	This topic describes methodologies to show that requirements meet objectives.
	Validating composition of components	This topic covers how to test a system as a whole.
	Unit versus system testing	This topic covers how system testing differs from component and connection testing.
	Formal verification of systems	This topic covers languages, theorem provers, and hierarchical decomposition.
Common System Architectures		This knowledge unit applies the topics of this knowledge area to specific architectures that are, or are becoming, more common.
[*See also Connection Security KA for related content, p. 32.*]	Virtual machines	This topic covers hypervisors, virtualization of disks and memory, and the use of virtual machines in security.
	Industrial control systems	This topic includes SCADA.
	Internet of Things (IoT)	This topic includes examples such as refrigerators and sensors.
	Embedded systems	This topic includes examples such as systems in spacecraft, and systems used in other hostile environments.
	Mobile systems	This topic includes examples such as laptops and smartphones.
	Autonomous systems	This topic includes examples such as robots and UAVs that do not require human control.
	General-purpose systems	This topic includes examples such as desktops, laptops, and mainframes.

4.5.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Holistic approach	
	Explain the concepts of trust and trustworthiness.
	Explain what is meant by confidentiality, integrity, and availability.
	Explain what a security policy is, and its role in protecting data and resources.
Security policy [*See also Organizational Security KA for related content.*]	
	Discuss the importance of a security policy.
	Explain why different sites have different security policies.

	Explain the relationship among a security group, system configuration, and procedures to maintain the security of the system.
Authentication	Explain three properties commonly used for authentication.
	Explain the importance of multifactor authentication.
	Explain the advantages of pass phrases over passwords.
Access control	
	Describe an access control list.
	Describe physical and logical access control, and compare and contrast them.
	Distinguish between authorization and authentication.
Monitoring	Discuss how intrusion detection systems contribute to security.
	Describe the limits of anti-malware software such as antivirus programs.
	Discuss uses of system monitoring.
Recovery	
	Explain what resilience is and identify an environment in which it is important.
	Discuss the basics of a disaster recovery plan.
	Explain why backups pose a potential security risk.
Testing	
	Describe what a penetration test is and why it is valuable.
	Discuss how to document a test that reveals a vulnerability.
	Discuss the importance of validating requirements.
Documentation	
	Discuss the importance of documenting proper installation and configuration of a system.
	Be able to write host and network intrusions documentation.
	Be able to explain the security implications of unclear or incomplete documentation of system