4.3 3 Knowledge Area: Component Security

The Component Security knowledge area focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems.

The security of a system depends, in part, on the security of its components. The security of a component depends on how it is designed, fabricated, procured, tested, connected to other components, used and maintained. This knowledge area is primarily concerned with the security aspects of the design, fabrication, procurement, testing and analysis of components. Together with the Connection Security and System Security KAs, the Component Security KA addresses the security issues of connecting components and using them within larger systems.

4.3.1 Knowledge Units and Topics

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

COMPONENT SECURITY		
Essentials - Vulnerabilities of system components, - Component lifecycle, - Secure component design principles, - Supply chain management security, - Security testing, and - Reverse engineering.		
Knowledge Units	**Topics**	**Description/Curricula Guidance**
Component Design [*See also Software Security KA for related content.*]		This knowledge unit introduces design principles and techniques which increase the security of components.
	Component design security	This topic covers threats to the security of component design artifacts (e.g., schematics, netlists, and masks) such as hardware Trojans, intellectual property piracy, reverse engineering, tampering, side-channel analysis and counterfeiting. It also introduces techniques for protecting components from unauthorized access and use.
	Principles of secure component design	This topic covers principles such as establishing a sound security policy, treating security as an integral part of system design, trusted computing platforms, chain of trust, reducing risk, layered security, simplicity of design, minimizing system elements to be trusted, and avoiding unnecessary security mechanisms.

	Component identification	This topic covers techniques such as watermarking, fingerprinting, metering, encrypted IDs, and physical unclonable functions for protecting components against intellectual property theft and ensuring component authenticity.
	Anti-reverse engineering techniques	This topic covers techniques such as design obfuscation and camouflaging for making component designs and implementations difficult to reverse engineer.
	Side-channel attack mitigation	This topic covers techniques for defending against side-channel attacks primarily targeted at cryptographic algorithms. Defensive techniques include leakage reduction, noise injection, frequent key updates, physical random functions, and secure scan chains.
	Anti-tamper technologies	This topic covers techniques for making components resistant to physical and electronic attacks including physical protection techniques, tamper evident systems and tamper responding systems.
	Component Procurement	This knowledge unit describes techniques for ensuring that the security of system components is maintained throughout the procurement process.
	Supply chain risks	This topic describes security threats and risks to both hardware and software in component procurement.
	Supply chain security	This topic describes strategies such as physical security, split manufacturing, traceability, cargo screening and validation, and inspections to detect and prevent compromises of component security during the procurement process.
	Supplier vetting	This topic includes strategies such as supplier credentialing to establish trusted suppliers and transporters of components.
Component Testing [*See also Software Security KA for related content*]		This knowledge unit introduces unit testing techniques and describes tools and techniques used to test the security properties of a component.
	Principles of unit testing	This topic describes unit testing tools and techniques as distinguished from system-level testing.
	Security testing	This topic describes tools and techniques such as fuzz testing for testing the security properties of a component beyond its functional correctness.
	Component Reverse Engineering	This knowledge unit describes techniques for discovering the design and functionality of a component with incomplete information.

	Design reverse engineering	This topic describes tools and techniques for discovering the design of a component at some level of abstraction.
	Hardware reverse engineering	This topic describes tools and techniques for discovering the functionality and other properties of a component's hardware, such as the functions of an integrated circuit.
	Software reverse engineering	This topic describes tools and techniques such as static and dynamic analysis for discovering the functionality and properties of a component's software.

4.3.2 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
Vulnerabilities of system components	
	Explain how the security of a system's components might impact the security of the system.
	Describe ways in which the confidentiality of a component's design may be compromised.
	Describe ways to learn information about component's functionality with limited information about its design and implementation.
Component lifecycle	
	List the phases of a component's lifecycle.
Secure component design principles	List component design artifacts which may require protection.
	Give examples of several secure component design principles and explain how each protects the security of components.
	Describe several techniques for protecting the design elements of an integrated circuit.
Supply chain management	
	List common points of vulnerability in a component's supply
	Describe security risks in a component supply chain.
	Describe ways to mitigate supply chain risks.
Security testing	
	Differentiate between unit and system testing.
	List several techniques for testing security properties of a component.
Reverse engineering	
	List reasons why someone would reverse engineer a component.
	Explain the difference between static and dynamic analysis in reverse engineering software.
	Describe a technique for reverse engineering the functionality of an integrated circuit.