4.4 4 Knowledge Area: Connection Security

The Connection Security knowledge area focuses on the security of the connections between components including both physical and logical connections.

It is critical that every cybersecurity professional have a basic knowledge of digital communications and networking. Connections are how components interact. Much of this material could be introduced through examples, and then abstracting to the essentials and introducing the appropriate vocabulary. Together with the Component Security and System Security KAs, the Connection Security KA addresses the security issues of connecting components and using them within larger systems.

4.4.1 Knowledge Units and Topics

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

CONNECTION SECURITY

Essentials

- Systems, architecture, models, and standards,
- Physical component interfaces,
- Software component interfaces,
- Connection attacks, and
- Transmission attacks.

Knowledge Units	**Topics**	**Description/Curricular Guidance**
Physical Media		This knowledge unit introduces the concepts of physical signaling and transmission. These general concepts could be introduced through presenting the history of Ethernet protocols and 802.11 wireless. Starting with a coax broadcast domain and CSMA/CD, moving to hubs and then switches without changing the addressing and payload. The introduction of switching required simulating broadcast behavior to simulate the coax broadcast behavior. Wireless is a shared medium but physical characteristics of the medium required
	Transmission in a medium	This topic covers signals in coax, twisted pair, optical fiber, and air.
	Shared and point-to-point media	This topic discusses the communication characteristic of the media
	Sharing models	This topic describes the various schemes for sharing media between multiple clients. For example: 802.1 MAC addressing and PPP.
	Common technologies	This topic examines various implementations of the models covered above. IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi), IEEE 802.16 (fixed wireless broadband).

Physical Interfaces and Connectors		This knowledge unit describes the characteristics of connectors, their materials, and standards that define the characteristics of the connectors. Different materials have different characteristics and signal transmission capability. Even non-technical security people need to understand that optical fiber is different than twisted pair and that each has different standards and specific standard
	Hardware characteristics and materials	This topic introduces the connection characteristics of various media and the requirements for physical connections.
	Standards	This topic examines various standards for connectors.
Hardware Architecture		This knowledge unit introduces the advantages and potential vulnerabilities of standard hardware architectures.
	Standard architectures	This topic should introduce the idea of standard architectures and the advantages of standardization. The history of PC motherboards could be used as an example showing the evolution from ISA through PCI and beyond. The ability for cards to add functionality without changing the base architecture is important. Adding Multiport Ethernet ports in a card allows a PC to become a
	Hardware interface standards	This topic introduces various hardware interface standards starting with IC package design, through busses such as ISA and PCI for integration platforms and on to networking standards like IEEE 802.3.
	Common architectures	This topic should examine the current technologies learners will face (CPU chips, PC motherboard, Ethernet standards).
Distributed Systems Architecture		This knowledge unit introduces the general concepts of distributed systems and how they are connected together. The Internet is not the only network and TCP/IP is not the only protocol for system interconnection. Each implementation has specific characteristics and different potential vulnerabilities. The focus of the curriculum should be on similarities, differences, and why design choices are made. Each architecture has advantages and disadvantages for particular use cases and each has particular vulnerabilities and strengths from a security perspective. One cannot assume that a mitigation strategy for the Internet will be appropriate for a supercomputer infrastructure.
	General concepts	This topic should start with the idea of a process in and operating system and then introduce the various architectures for running processes and enabling their communication. Symmetric multiprocessing and shared memory, network based with an interprocess communication model.

	World-wide-web	This topic covers the HTTP/HTTPS protocol and demonstrates how it is an example of a distributed processing standard.
	The Internet	This topic covers the evolution of the Internet as a distributed processing platform. Learners should be clear as to why the world-wide-web and the Internet are not equivalent.
	Protocols and layering	This topic covers the 7 layer OSI model along with the 5 layer Internet model and compares them as an example of encapsulation and layering to enable services that build on each other.
	High performance computing (supercomputers)	This topic introduces HPC and use cases that distinguish HPC from the standard Internet.
	Hypervisors and cloud computing implementation	This topic introduces the concepts of providing infrastructure as a service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS), and all of their relatives relevant to the learners should be covered.
	Vulnerabilities and example exploits	This topic examines the attack surfaces of the various distributed computing models emphasizing the fact that every interface introduces potential vulnerabilities. The hypervisor, virtual networking, physical network, and interprocess communication should all be
Network Architecture		This knowledge unit introduces the concepts typically covered in a computer networking course. It provides the foundation for the more specialized KUs.
	General concepts	This topic should cover the ideas of nodes and edges with the names of the various topologies and the transmission characteristics of the topologies.
	Common architectures	This topic covers the IEEE 802 network architecture and how the various networks are named based on the physical characteristics (LANs, MANs, etc.).
	Forwarding	This topic covers packet forwarding in general. Since similar switching silicone is now used in routers and switches, and SDN treats forwarding separate from building the forwarding table, this is its own topic.
	Routing	This topic covers routing algorithms and explains how forwarding tables are built using graph analysis algorithms such as link-state and distance
	Switching/ Bridging	This topic covers learning algorithms and IEEE 802.1 bridging along with Spanning Tree Protocol and its relationship to routing. It is not currently clear how this topic will evolve with STP being replaced through the emergence of Trill and STP.

	Emerging trends	This topic covers emerging technologies and their impact as they emerge. Currently the impact of SDN and adding routing to layer 2 with enhanced learning bridges would be the content. This is evolving rapidly.
[*See also System Security KA for related content*]	Virtualization and virtual hypervisor architecture	Virtualization has provided ways to design architecture using either native virtualization (type 1) or virtualization under the control of a host operating system (type 2).
Network Implementations		This knowledge unit explores specific technologies that implement the general concepts of networking. Network architecture concepts may be illustrated by specific implementations but it should be made clear that there are other possibilities. It should be emphasized that vulnerabilities are exploited in implementations. Often an architecture can be proven correct theoretically, but implemented in a way that has vulnerabilities. Also seams between technologies often open vulnerabilities. ARP poisoning is a perfect example of how a seam between technologies opens vulnerabilities.
	IEEE 802/ISO networks	This topic is a deep dive into the ISO standards. It is expected that this topic will be introduced other places.
	IETF networks and TCP/IP	This is a deep dive into the basic infrastructure of the Internet and TCP.
	Practical integration and glue protocols	This topic looks at the problem of integrating technologies through the implementation of what could be called interface shims or glue code. ARP is the obvious example. A mechanism was required to map the IP addresses of the IETF internetworking model to the MAC addresses of the underlying networks. ARP is the glue. Similarly, Infiniband needs a shim to carry IP traffic. Other examples abound.
	Vulnerabilities and example exploits	This topic should provide examples from the technologies important to the program. If ARP is chosen as an example, ARP poisoning as a MitM attach works well. USB and other serial connections could also provide examples.

Network Services		This knowledge unit explores different models used to implement connectivity between the consumer of a service and the provider of a service. Each topic can be explored at many levels with many examples (e.g., wireless issues surrounding biomedical devices). This area is broken out because the service models can be implemented in so many ways with so many different architectures. Remote procedure calls (RPC) are implemented over many different connection technologies varying from process-to-process in a single processor to across the Internet. The security concerns are different and the design tradeoffs change based on implementations and requirements.
	Concept of a service	This topic is a network-centric dive into one model of distributed computing. A service is a process that provides something to another process based on a request.
	Service models (client-server, peer-to-peer)	This topic is a network-centric look at how services are modelled. From a network perspective, the client initiates a connection and a server responds. With P2P either side can initiate the request.
	Service protocol concepts (IPC, APIs, IDLs)	This topic describes all of the ways components connect. Procedure calls, IPC requests, Interface Definition Languages with stub code, private protocols over a socket, everything.
	Common service communication architectures	This topic looks at specific services and how their protocols are implemented. Examples are SMTP, HTTP, SNMP, REST, CORBA, etc. Specialty connections such as wireless control of implanted medical devices can also be examined.
	Service virtualization	This topic covers service virtualization as a method to emulate the behavior of specific components such as cloud-based applications and service-oriented architecture.
	Vulnerabilities and example exploits	This topic looks at the vulnerabilities and exploits of client-server, peer-to-peer, and virtualization network services. Common service signatures are often used for vulnerability profiling.
Network Defense		This knowledge unit captures current concepts in network protection. It is likely that the vocabulary and technology will evolve significantly over time. The key ideas should include connection vulnerabilities like inserting a tap into a connector and enabling eavesdropping. All of these provide vulnerabilities that can be exploited for man-in-the- middle attacks. The idea of base-line capture and monitoring for deviations from the base needs to be covered as it applies in several of the specific topics.
	Network hardening	This topic covers ways to help the network defend itself from unauthorized access.

	Implementing IDS/IPS	This topic covers intrusion detection and intrusion prevention services. These services audit the network traffic.
	Implementing firewalls and virtual private networks (VPNs)	This topic covers the installation and use of firewalls and virtual private networks.
	Defense in depth	This topic introduces the idea that defenses must be layered.
	Honeypots and honeynets	This topic introduces the idea of providing intentionally vulnerable networks and devices in isolated networks so that they can be watched and analyzed as they are attacked.
	Network monitoring	This topic covers the tools and techniques for monitoring network devices and their associated logs.
	Network traffic analysis	This topic covers the tools and techniques for capturing and analyzing the packets flowing through the network. Research topic in this area include threat hunting and attack pattern detection.
	Minimizing exposure (attack surface and vectors)	This topic covers the tools and techniques for finding and mitigating vulnerabilities through looking at potential weaknesses.
	Network access control (internal and external)	This topic covers tools and techniques for limiting the flow of packets based upon rules for packet content. Examples include network admission control techniques; machine certificates; machine profiling techniques; probing with SNMP, DHCP, HTTP, DNS, LDAP, and NMAP.
	Perimeter networks (also known as demilitarized zones or DMZs) / Proxy Servers	This topic covers tools and techniques for implementing Defense in Depth using isolated networks and special servers.
	Network policy development and enforcement	This topic covers the creation of policies that provide guidance and requirements for the services provided by the network along with the measures to be used to see that the policies are followed.
	Network operational procedures	This topic discusses the creation of procedures that are used to operate the network.
	Network attacks (e.g., session hijacking, man-in-the-middle)	This topic covers the tools and techniques used to test the network by actually attempting to exploit vulnerabilities.
	Threat hunting and machine learning	This topic covers how proactive threat hunting uses machine learning to detect patterns in attack

4.4.2 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**
Systems, architecture, models, and standards	
	Discuss the need for common models and architectures in order to describe systems.
	Describe a model of systems that consists of components and interfaces for connections.
	Explain why a component requires at least one interface.
	List several standards that define models consisting of systems of components and interfaces.
	Describe the components and interfaces of a networking standard provided.
Physical component interfaces	
	Explain why a hardware device is always modeled a physical component.
	List several examples of physical component interfaces with their associated vulnerabilities.
	Describe an exploit for a vulnerability of a physical interface provided.
Software component interfaces	
	Explain why every physical interface has a corresponding software component to provide a corresponding software interface.
	Explain how software components are organized to represent logical layers in a standard model.
	Discuss how the Internet 5 layer model can be viewed as software components and interfaces that represent levels of services encapsulated by lower-level services.
	Discuss how TCP/IP as a service is represented by different interfaces in different software systems.
Connection attacks	
	Explain how connection attacks can be understood in terms of attacks on software component interfaces.
	Describe how a specified standard interface could expose vulnerabilities in a software component that implements the interface.
	Describe how an implementation could protect itself from a specified vulnerability in a specified standard interface.
Transmission attacks [*See also* *Data Security KA* *for related content*]	
	Explain how transmission attacks are often implemented as attacks on components that provide the service of relaying
	Describe an attack on a specified node in a TCP/IP network given the description of a vulnerability.
	Explain why transmission attacks can often be viewed as connection attacks on network components (physical or