UNIT 19: Network Security Technologies

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
3 Ubiquitous Connectivity 6 Adversarial Thinking 2 Establishing Trust	3.2	- Investigate firewalls, Intrusion Detection Systems, Intrusion Protections Systems, Application Layer Defenses, and IoT Defenses. - Research Types of threat indicators (pyramid of pain). - Provide a defense in depth network model.

Guiding Questions:

- Why are network security technologies needed?
- What are these technologies?
- What are the types/features of these technologies?
- How/why is security a characteristic of a system, not a tool?
- Why is layering (defense in depth) important?
- What happens when the tools fail?
- What is the role of policy?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
3.2.3 LO: Students will identify and distinguish between the purposes of network security devices and technologies. 3.2.3a EK: Most protocols lack a security component but some protocols build in security. For example, http was designed before security was a major concern while extensions like	• Computer, lecture slides, projector, graphic organizers, access to Internet • Timberg, Craig. "Net of Insecurity Part 1 | A Flaw in the Design | The real story of how the Internet became so vulnerable." The Washington Post,	"The Internet is not the setting of most attacks. It is the delivery system."– Craig Timberg • Ask students if they agree or disagree with the quote. Explain how the Internet was originally designed for information sharing; therefore, security was not a concern. It was built for speed and ease. Use http/https as an example here. • Note that the Internet was made with a dumb core that was designed to carry data to intelligent edges (individual computers). Review how packets are carried across the

https explicitly add security to the standard. 3.2.3b EK: A packet can be identified by its source address (sending device), source port (sending application on the device), destination address (receiving device), and destination port (receiving application on the device).	*WasingtonPost.com*, 30 May 2015, https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.ba1761c56b14	dumb core to the intelligent edges. The article linked left can help with these concepts.
3.2.3c EK: Firewalls work primarily at the network and transport layer by blocking packets with addresses and ports that correspond to unwanted traffic.	• "What are Firewalls?" *YouTube*, uploaded by CBT Nuggets, 31 Jan 2019, https://www.youtube.com/watch?v=9JQtyQEpQV8 (7:58 minutes) • "Security in Formation | 5 Generations of Firewall Solutions." CypherShark, *Sharkscale.WordPress.com*, 7 May 2016, https://sharkscale.wordpress.com/2016/05/07/5-generations-of-firewall-solutions/ • Souppaya, Murugiah and Scarfone, Karen, "Guide to Malware Incident	• List types of network security technologies designed to secure a system (the intelligent edges). These should include firewalls, intrusion detections systems, intrusion protection systems, application layer defenses, and IoT defenses • Provide an overview of a firewall. Explain its role in a security system. Show video linked left. • Discuss firewall types. See source linked left. • Discuss firewall placement (host-based, network based, cloud-based). Have students research the pros and cons of each type. • Discuss firewall rules. The NIST publication linked left offers resources for this on page 13. NIST also offers *Guidelines on Firewalls and Firewall Policy*, also linked left.

	Prevention and Handling for Desktops and Laptops." SP 800-83 Rev. 1, *NIST.gov,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf (See page 13) • Scarfone, Karen and Hoffman, Paul. "Guidelines on Firewalls and Firewall Policy." SP 800-41 Rev. 1, *NIST.gov*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf • Sehl, Sibylle and Vaniea, Kami. "Unity WebGL Player | SecondGameDraft." The University of Edinburgh School of Informatics, https://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/	• Use the game linked left to allow students to practice firewall rules.
3.2.3d EK: Intrusion Detection Systems (IDS) work at all layers to identify and raise an alarm when	• "Zero Day Exploit explained under 2 mins." *YouTube*, uploaded by	• Show video linked left. Have students define a zero-day attack in their own words. Explain to students that entities

unexpected message patterns (anomalies) or known bad patterns (signatures) are detected (blacklisting). IDS systems can also be configured to block all packets and only allow a select set of valid packets (whitelisting). 3.2.3e EK: Intrusion Prevention Systems (IPS) are similar to IDS and also can prevent attacks by blocking messages related to anomalies or signatures.	Cyber Security Entertainment, 26 Dec 2017, https://www.youtube.com/watch?v=PNgIJXodwic • Slowik, Joe. "Unraveling Detection Methodologies: Indicators vs. Anomalies vs. Behaviors." *RSA Conference 2019 | San Francisco | March 4-8 2019*, https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13770/AIR-T09-Unraveling-Detection-Methodologies-Indicators-vs.-Anomalies-vs.-Behaviors.pdf • "The Pyramid of Pain." Enterprise Detection & Response, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html	have to worry about all kinds of attacks, especially zero-day attacks. How do they protect against them? • Discuss the definition of an IDS. Discuss whitelisting and blacklisting. Discuss the types of IDSs (signature detection, anomaly detection, behavior-based). The slideshow linked left is a good resource to explain the differences. • Have students research types of indicators using the site linked on the left (Pyramid of Pain). Discuss HIDS versus NIDS. • Introduce IPS and contrast to IDS. Show video linked left.

	• "MicroNugget: IDS vs. ISPs." *YouTube*, uploaded by CBT Nuggets, 16 Jan 2014, https://www.youtube.com/watch?v=rvKQtRklwQ4	
3.2.3f EK: Application layer defenses, such as input validation, check and block potentially harmful message data from getting to the application. 3.2.3g EK: Devices with limited processing power such as Internet of Things (IoT) devices and control systems in industrial settings may rely almost entirely on network security devices such as firewalls and IPS for protection.	• "Input Validation Cheat Sheet." OWASP Cheat Sheet Series, Open Web Application Security Project, *OWASP.org*, https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html • "OWASP Top Ten Proactive Controls 2018 | C5: Validate All Inputs." Open Web Application Security Project, *OWASP.org*, https://owasp.org/www-project-proactive-controls/v3/en/c5-validate-inputs • "Defense-in-Depth. Layered Protection and Data Security." Infosec Institute, *InfosecInstitute.com*, 28 Sep 2014,	• Discuss application layer defenses. The sites linked left can assist with this. The video linked left also show an example of the importance of input validation and has an activity to go with it (see left). WARNING: The video has bleeped language. Please preview before showing. • Discuss how IoT devices have very little built in security. This means they have to depend on the security of the network. The article linked left is useful for teaching this this.

	https://resources.infosecinstitute.com/defense-depth-layered-protection-data-security/#gref • "Hacking Websites With Cross-Site Scripting (XSS Attack Basics)." *YouTube*, uploaded by Chef Secure, 2 Nov 2018, https://www.youtube.com/watch?v=9kaihe5m3Lk • "Hacking Websites With Cross-Site Scripting." *ChefSecure.com*, https://chefsecure.com/courses/xss/recipes/hacking-websites-with-cross-site-scripting • Craven, Connor. "What is Edge Security? Definition." SDxCentral, *SDxCentral.com*, 27 Mar 2020, https://www.sdxcentral.com/edge/definitions/what-is-edge-security-definition/	

6.1.2e EK: Security is a characteristic of systems and not system components. 2.3.5 LO: Students will break down how the principle of layering is a strategy for slowing down an attack because the attacker has to conquer each layer before moving on to the next. 2.3.5a EK: A layer is a separate level that must be conquered by an attacker to breach a system. 2.3.5b EK: Multiple independent layers require integration and independent management to get the full benefits of layered protection.	• "How the Cyber Kill Chain Can Help You Protect Against Attacks." SBS CyberSecurity, *SBSCyber.com*, 23 Aug 2019, https://sbscyber.com/resources/how-the-cyber-kill-chain-can-help-you-protect-against-attacks	• Ask students to explain how security is a characteristic, not a tool. Discuss how the tools have to be properly configured to provide security. • Have students examine the matrix linked left. What weapons are in place to protect a system from each stage of the cyber kill chain? How is layering used? Have students link these strategies with security technologies on a network.
6.1.2 LO: Students will explain how complexity impacts the failure of cybersystems. 6.1.2c EK: Product failure is deceptively difficult to understand given that it depends on the intrinsic properties of each part, what it's made of, how those materials respond to		• Ask if any of these devices could fail. If so, what would happen? • Discuss unified threat management (UTM). Is it a good or bad idea? Have students explain. Discuss redundancy. • Have students research examples of the times system failures have resulted in a breach.

varying and unanticipated conditions, and how customers use a product. 6.1.2a EK: In complex systems, failures are rarely the result of one individual's problem or behavior; catastrophe requires multiple failures. 6.1.2b EK: System failures are characterized by a series of actions or behaviors that are normally isolated or self-contained, but become consequential due to interconnected impact. 6.1.2d EK: Given the complexity of cybersystems, there are limits to how much entities can control their functioning and success of their policies.		• Have students create a network diagram for a fictitious company. They should include network devices to protect against malicious software, phishing, spam, leakage of intellectual property, BYOD, and rogue access points. The technology should not be limited to the ones discussed in this unit. Have students explain their choice and include these items in their network diagram. • Note the importance of user training and auditing.
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.		• Discuss a career. We recommend a career as a warnings analyst.