UNIT 9: SECURITY AND VULNERABILITIES

Estimated Time in Hours: 23 - 30

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 3 Ubiquitous Connectivity 4 Data Security 5 System Security 6 Adversarial Thinking 7 Risk	2.1, 2.2, 2.3, 3.1, 3.2 ,4.2, 5.2, 5.3, 6.1, 6.2, 7.1, 7.2,	- Cyber Real Card Game - Create a Threat, Vulnerability, Attack Game - Attack Tree Poster - Create an Authentication Game - Security Vulnerability Table - Physical Controls Diagram - DoD Cyber Awareness Challenge - NIST Poster

Guiding Questions:

- How are simplicity and restriction overarching ideas for cybersecurity principles?
- What are security flaws/vulnerabilities in hardware and software?
- What is the difference between a risk, vulnerability, and a threat?
- How is cybersecurity risk modeled?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.2.1 LO: Students will explore the principle of simplicity, which is about how users can easily translate their general protection goals to appropriate system security configurations. EK: 2.2.1a,b,c 2.2.2 LO: Students will use the principle of abstraction to represent complicated concepts more simply and to allow	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Introduction to Cybersecurity First Principles Lesson: Hale, Ghandi, Morrison, and Rausch.	**Fundamental Security Design Principles: (2-3-day lesson)** In this lesson students learn the fundamental security design principles. • Day 1 of the lesson: The lesson begins with students responding to the following question in their notebook: “What do you need to think about when designing a secure system?” Students then read section 1.4 - Fundamental Security Design Principles (p.17 - 21) in the textbook. Students take window notes as they are reading and update key vocabulary from this section in their notebook.

solutions to be transferred to other contexts. EK: 2.2.2a,b 2.2.3 LO: Students will apply the principle of minimization by decreasing the number of ways in which attackers can exploit a program or device. EK: 2.2.3a,b,c,d 2.3.1 LO: Students will explore the principle of domain separation, which allows for the enforcement of rules governing the entry and use of domains by entities outside the domain. EK: 2.3.1a,b 2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes. EK: 2.3.2a,b,c 2.3.3 LO: Students will know that the principle of resource encapsulation allows access or manipulation of the resource only in intended ways.	"Introduction to Cybersecurity First Principles." *GitHub*, uploaded by mlhale, https://mlhale.github.io/nebraska-gencyber-modules/intro_to_first_principles/README/#cybersecurity-first-principles • Cyber Realm Card Game: https://gencybercards.com/ • GenCyber First Principles: https://users.cs.jmu.edu/tjadenbc/Bootcamp/0-GenCyber-First-Principles.pdf • First Principles using pictures: https://spark.adobe.com/page/DbZGSqJ12Q82A/ • First Principles Hand Gestures: https://gencyber.utulsa.edu/wp-content/uploads/2016/10/10-Principles-	• Day 2+ of the lesson: This lesson uses the Introduction to Cybersecurity First Principles Lesson. Students read the First Principles, followed by the CIA Triad Expectations, and then students play the Cyber Realm Card Game. The lesson is wrapped up with a quiz.

EK: 2.3.3a,b 2.3.4 LO: Students will explore the principle of least privilege, which is about differentiating among types of access control (mandatory, role-based, discretionary, and rule-based access controls) and analyzing which to use for selective restriction of access to a place or other resource. EK: 2.3.4a,b,c 2.3.5 LO: Students will explore 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. EK: 2.3.5a,b 2.3.6 LO: Students will know that the principle of data hiding is about allowing only necessary aspects of a data structure or a record to be observed or accessed. EK: 2.3.6a	GenCyber-Card-Game.pdf	

2.3.7 LO: Students will recognize that the principle of modularity is a design technique that separates the functionality of a program into independent components. Each component is self-sufficient and capable of executing a unique part of the desired functionality through well-designed interfaces. EK: 2.3.7a,b 2.3.8 LO: Students will explore the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created. EK: 2.3.8a,b,c 5.2.4 LO: Students will identify hardware security addresses issues related to an adversary physically gaining access to a device. EK: 5.2.4a,b		
7.1.1 LO: Students will be able to differentiate between threats, vulnerabilities, and attacks. EK:7.1.1a,b,c	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015.	**Understanding Threats, Vulnerabilities, and Attacks: (2-day lesson)** In this lesson students learn the difference between threats, vulnerabilities, and attacks. • The lesson begins with a quick write. Students answer the following question: "What is the difference between

	• Notebook	an attack, a threat, and a vulnerability?" Students then read section 1.2 - Threats, Attacks, and Assets (p.9-15) and A Model for Computer Security (p.7-8) in the textbook. Students update the vocabulary in their notebook. In small groups students create a game that will help others to practice identifying threats, vulnerabilities and attacks.
4.2.3 LO: Students will evaluate and recommend technical controls that can be used to secure data. EK: 4.2.3a,b,c,d,e,j	• Notebook • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015.	**Authentication / Securing Data: (5-6-day lesson)** In this lesson students learn about all of the different ways to secure data with authentication. • Day 1: Students read section 3.1 - Digital User Authentication Principles (p.64-70) in the textbook. Students update the key vocabulary in their notebook. Students answer Review Question 3.1. • Day 2: Students read section 3.2 - Password-Based Authentication (p.70-82) in the textbook. Students update the key vocabulary in their notebook. Students answer Review Questions 3.2,3.3 & 3.4. Students complete Problems: 3.1 & 3.3. • Day 3: Students read section 3.3 - Token-Based Authentication (p.82-87) in the textbook. Students update the key vocabulary in their notebook. Students answer Review Question 3.5. • Day 4: Students read section 3.4 - Biometric Authentication (p. 87 - 92) in the textbook. Students update the key vocabulary in their notebook. Students answer Review Questions 3.6 & 3.7. • Day 5+: Student read section 3.5 - Remote User Authentication, and 3.6 - Security Issues for User Authentication (p.92-97) in the textbook. In pairs

		students create a game to review the types of authentication.
3.2.2 LO: Students will identify and predict the outcomes of security vulnerabilities at the physical/link layer, the network layer, the transport layer, and the application layer. EK: 3.2.2a,b,c,d	- Holl, Kim. "SANS Security Essentials | GSEC Practical Assignment Version 1.4b | OSI Defense in Depth to Increase Application Security." Global Information Assurance Certification, *GIAC.org*, https://www.giac.org/paper/gsec/2868/osi-defense-in-depth-increase-application-security/104841#:~:text=Many%20of%20the%20threats%20to,flooding%20and%20spanning%20tree%20attacks. - Notebook	**OSI Vulnerabilities: (1-day lesson)** In this lesson students identify and predict outcomes of security vulnerabilities at the different layers of the OSI Model. - The lesson begins with students reviewing and diagramming the layers of the OSI model in their notebook. Students then read the OSI Defense in Depth paper. While reading the document students fill out a table that includes the following: vulnerability, layer, outcome.
2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. EK: 2.1.3d	- "Beta – Hotspot Game." Living Security | Resources | Intelligence Center | Games, https://hotspot.livingsecurity.com/	**Physical Security: (3-4-day lesson)** In this lesson students identify physical controls that are used to secure data. - The lesson begins with students completing the Hot Spot Hunt for the Violations simulation. After students complete the simulation the class discusses what violation(s) is/are physical security violation(s). Students

4.2.2 LO: Students will identify physical controls that are used to secure data. EK: 4.2.2a,b,c,d,e,f 6.1.3 LO: Students will understand how different system components impact the cybersecurity of a system design. EK: 6.1.3a,b,c,d 6.2.1 LO: Students will know how natural events and unintentional errors can cause a system to fail. EK: 6.2.1a,b,c,d	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • "Cyber-Physical Systems." UC Berkeley Electrical Engineering and Computer Sciences Dept. Ptolemy Project, https://ptolemy.berkeley.edu/projects/cps/#:~:text=Cyber%2DPhysical%20Systems%20(CPS),affect%20computations%20and%20vice%20versa.	then read section 16.1- Overview, 16.2- Physical Security Threats, 16.3 - Physical Security Prevention and Mitigation Measures, and 16.4 - Recovery From Physical Security Breaches (p.508-519) & 16.6 - Integration of Physical and Logical Security (p. 520 - 526) in the textbook. Students take Cornell notes as they are reading. Students add key vocabulary to their notebooks. Students answer Review Questions 16.8. Then, students read Cyber-Physical Systems. The lesson is wrapped up with students creating a diagram explaining physical controls used to secure data.
5.2.2 LO: Students will know some common hardware-related vulnerabilities. EK: 5.2.2c,d,e	• Bhunia, Swarup and Tehranipoor, Mark. "Side-Channel Attacks." *Hardware Security: A*	**Side Channel Attacks: (1-day lesson)** In this lesson students learn how hardware may act in unintended ways due to side channel attacks.

7.2.3 LO: Students will be able to explain how the logical malleability of software and hardware can allow an adversary to change a system to meet the adversary's goals rather than the systems original objective. EK: 7.2.3c,d	*Hands-On Learning Approach*, Morgan Kaufmann, 2 Nov 2018, pp. 193-218. • Notebook	• In this lesson students read about side channel attacks. They take notes on the reading. The lesson is wrapped up with students discussing the vulnerabilities of hardware and how to secure the hardware.
5.3.3 LO: Students will describe the process of validating that software remains secure through its lifecycle. EK: 5.3.3a,b,c,d,e 7.1.4 LO: Students will be able to conduct standard security testing and assessments. EK: 7.1.4a,c,d,e	• Gonzalez, Kenneth. "A Step-By-Step Guide to Vulnerability Assessment." Security Intelligence, *SecurityIntelligence.com*, 8 June 2018, https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/ • "What is a Zero-Day Exploit?" Fire Eye, *FireEye.com*, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html • Notebook	**Testing & Security:(3-4-day lesson)** In this lesson students learn how to validate that software remains secure through its lifecycle. • The lesson begins with a quick write answering the question: "What is a Zero Day Exploit?". Students respond in their notebooks. The lesson is then introduced and students read about zero-day exploits and the step by step guide to vulnerability assessment. The class then discusses the process of validating software through its lifecycle. Students create a poster representing the process for validating the software. In the next part of the lesson, students learn what is necessary to conduct standard security testing and assessment. • Begin with a discussion about vulnerability assessments and how they play a part in standard security testing. Students then read Application Security Best Practices - Top 10 Checklist. The class then discusses each of the topics on the checklist. Students then apply what they

	• Poster Paper • Markers • Avner, Gabriel. “Application Security Best Practices Top 10 Checklist.” White Source | Resources | Blog, 1 Aug 2019, https://resources.whitesourcesoftware.com/blog-whitesource/application-security-best-practices • Control-Alt-Hack, by Steven Jackson Games (available for purchase on Amazon or at controlalthack.com)	know about standard security testing and assessments through the game Control-Alt-Hack.
6.2.2 LO: Students will know how intentional attacks can adapt to defenses and cause a system to fail. EK: 6.2.2a,b,c,d 7.1.2 LO: Students will be able to identify and prioritize the	• “The Cybersecurity Framework Version 1.1 Downloadable Presentation.” National Institute of Standards & Technology, *NIST.gov*, Oct 2019, https://www.nist.gov/document/cybersecuri	**NIST: (3-4-day lesson)** In this lesson students learn about the NIST Framework and how to apply the NIST Framework to a situation. • The lesson begins with students reading section 1.6 - Computer Security Strategy (p.24-26) in the text. Students take Cornell notes while reading. The teacher then introduces the NIST Framework with the NIST Framework PowerPoint. Students then read the NIST Framework documentation and take notes in their

protection of information assets. EK: 7.1.2a,b,c	tyframeworkv1-1presentationpptx • “Framework Version 1.1 (PDF)- Framework for Improving Critical Infrastructure Cybersecurity.” National Institute of Standards & Technology, *NIST.gov*, 16 Apr 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Poster Paper • Markers	notebook. The class discusses how the NIST Framework works and they walk through a model NIST Framework together. Students will then work in groups to create their own NIST Framework poster to protect a set of assets.

3.1.2 LO: Students will explain how network standards and protocols allow different types of devices to communicate. EK: 3.1.2e,f,g 7.1.3 LO: Students will create a threat model and evaluate the trade-offs associated with defending against different threat sources. EK: 7.1.3a,b,c 7.1.5 LO: Students will understand the trade-offs between cybersecurity benefits and the total cost of cybersecurity protections. EK: 7.1.5a,b,c 7.2.2 LO: Students will be able to describe how the presence of an adversary necessitates that cybersecurity risk is emergent and complex. EK: 7.2.2a,b,c 7.2.4 LO: Students will be able to explain how the decentralized and dynamic nature of networked systems create the	• Notebook • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Schneier, Bruce. “Attack Trees.” Schneier on Security, *Schneier.com*, https://www.schneier.com/academic/archives/1999/12/attack_trees.html • Poster Paper • Markers	**Attack Trees: (1-2-day lesson)** In this lesson students learn about attack trees and identify a possible asset and create an attack tree for the asset. • The lesson begins with a class brainstorming session about attack trees. “Attack trees” is written in the center of the board and students list all of the things they know about attack trees. Each idea is connected to the word. Students then read section 1.5 - Attack Surfaces and Attack Trees (p.21-24) in the textbook. Students then read the Attack Tree Examples. The class then goes back to the attack trees brainstorming list. They cross out any misconceptions that are listed and add the brainstorm to their notebook. Students are then put in small groups. Each group receives a poster paper. The group picks a target and creates an attack tree for the target.

potential for a system to fail or behave incorrectly due a component the designer didn't even know existed. EK: 7.2.4i		
3.2.1 LO: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices. EK: 3.2.1a,b,c,d 6.2.3 LO: Students will analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking. EK: 6.2.3a,b,c,d,e,f,g,h	- Hospelhorn, Sarah. "What is The Cyber Kill Chain and How to Use it Effectively." Varonis Blog, *Varonis.com*, 29 Mar 2020, https://www.varonis.com/blog/cyber-kill-chain/ - "Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform." Lockheed Martin, 2015, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf - Degonia, Tony. "Explaining the Cyber Kill	**Kill Chain: (2-3-day lesson)** In this lesson students will analyze how the cybersecurity attack lifecycle / kill chain is essential to adversarial thinking. - A diagram of the Cyber Kill Chain is introduced to the students at the beginning of the lesson. Students read about the Cyber Kill Chain. Students create a diagram of the Kill Chain that labels each part of the kill chain and explains how each part works. Students are then given a scenario where they analyze how the connected nature of the internet allows an adversary to reach a large number of devices and they apply the kill chain to the scenario. The lesson is wrapped up with students applying what they have learned about the kill chain to stop a breach in the DoD Cyber Awareness Challenge 2020.

	Chain Model.” AT&T Business | AT&T Cybersecurity, 3 Jan 2019, https://cybersecurity.att.com/blogs/security-essentials/the-internal-cyber-kill-chain-model • “Cyber Awareness Challenge 2020”, sponsored by the Department of Defense Chief Information Office (DoD CIO), https://dl.dod.cyber.mil/wp-content/uploads/trn/online/cyber-awareness-challenge/launchPage.htm	