UNIT 22: Common Hardware Vulnerabilities

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 7 Risk 2 Establishing Trust		- Research, identify, and categorize common hardware vulnerabilities. - Research tactics for securing hardware vulnerabilities and supply chain threats. - Develop a physical security plan for vulnerable hardware.

Guiding Questions:

- How does a hardware vulnerability differ from a software vulnerability?
- What are some methods used by adversaries exploiting hardware?
- What is the Meltdown vulnerability and how many computers does it affect?
- What are the types of side channel attacks and how do they differ?
- How do hardware vulnerabilities sometimes involve software?
- How can physical security help protect potentially vulnerable hardware?
- How does resource encapsulation benefit hardware?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.2.2 LO: Students will know some common hardware-related vulnerabilities.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Spectre & Meltdown review: "Why are Spectre and Meltdown So Dangerous?" *YouTube*, uploaded by Techquickie, 1 May 2018,	• Review hardware vulnerabilities covered so far (Spectre, Meltdown, physical security vulnerabilities, etc.) • Watch the Spectre & Meltdown review YouTube video. Is there any drawback to mitigating a processor against Meltdown? • Ask students if they think hardware vulnerabilities are easier for adversaries to exploit than software vulnerabilities? Are they easier to detect?

	https://youtu.be/NArwG6yaWJ8 • Common hardware vulnerabilities: Biryukov, Vladislav. "Deep Dive: 5 Threats Affecting Hardware." Kaspersky Daily, *Kaspersky.com*, 1 Apr 2015, https://www.kaspersky.com/blog/hardware-malware/8169/	• Challenge students with researching common hardware vulnerabilities and listing their name, vulnerability, method of exploitation, and any mitigations or fixes. An example link is provided.
5.2.2a EK: A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device (e.g. a home router) to secure remote access. 5.2.2b EK: Manufacturing backdoors are used for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory.	• Cold boot attack demo: "The Chilling Reality of Cold Boot Attacks." *YouTube*, uploaded by F-Secure, 13 Sep 2018, https://youtu.be/E6gzVVjW4yY • Cold boot attack explanation: "Cold Boot Attack | University of South Wales VeraCrypt Research Group." *YouTube*, uploaded by Luke Clarke, https://youtu.be/XfUlRsE3ymQ	• Explain how many hardware vulnerabilities require backdoor access, many of which are obscure. Provide examples. • Show the linked YouTube video of the cold boot attack. Is this an example of a backdoor? What does the adversary need access to in order to do this attack? • Ask students why adversaries would adversaries be interested in gaining access to the content of memory or RFID cards.

7.2.3d EK: Hardware itself may act in unintended ways and an adversary is seeking to find and exploit these unintended behaviors.		• As demonstrated, adversaries can find unique methods for exploiting unintended hardware behaviors. What is the skill level of hackers who do this? • Ask students to summarize how the cold boot attack works.
5.2.2c EK: A side channel attack is based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs)	• Mobile device side channel leakage: "Side-Channel Analysis Demo: Mobile Device." *YouTube*, uploaded by Rambus Inc., 25 june 2013, https://youtu.be/cPDDNVKo43w • Side Channel Timing Attack demo (technical): "Side Channel Timing Attack Demonstration." *YouTube*, uploaded by Joe Grand, 26 Sep 2017, https://youtu.be/2-zQp26nbY8	• Define the term side channel attack/analysis. Ask students what is the meaning of side channel? • Show the linked YouTube video about the Side Channel Timing Attack. Use a video viewing guide if necessary. What is the purpose of measuring the time of button presses?
5.2.2d EK: General classes of side channel attacks include attacks such as: timing attacks, power-monitoring attacks, electromagnetic attacks, data remanence attacks.		• Define and categorize the types of side channel attacks with examples. • Emphasize that timing attacks are only one type of side channel attack. What type is the cold boot attack shown earlier?

		• Ask students why an understanding of low level hardware, binary, and programming languages is important for side channel analysis.
5.2.2e EK: Hardware vulnerabilities can also be due to weaknesses in the implementation of algorithms.		• Explain that sometimes hardware is expected to be used one way, but software may attempt to use it in another way. This muddies the water between whether the vulnerability is a software or hardware vulnerability. For example, the Meltdown vulnerability is achieved through its branch prediction feature designed to speed up processing; however, the algorithm used is exploitable by adversaries.
5.2.3 LO: Students will describe the process of developing secure hardware and validating that it is secure through its lifecycle. 5.2.3a EK: Hardware itself consists of many components and supply chain management attempts to ensure each component as well as the composition of these components meets an overall security policy. 5.2.3b EK: The hardware design, manufacturing and supply chain can be attacked by malicious actors, nation states,	• Supply chain introduction: "What is Supply Chain Management?" *YouTube*, uploaded by BYU Supply Chain, 5 Jan 2014, https://youtu.be/AwemFfdD6VI • Huawei national security concern: "Why The US Thinks Huawei Is A National Security Threat." *YouTube*, uploaded by CNBC, 24 Dec 2018, https://youtu.be/3l20G4OfGk0	• Hardware and software should be tested together to help prevent exploitation; however, hardware isn't always so simple to protect. • Define the term supply chain and show the introductory YouTube video on the left. The Huawei espionage allegations video can also be shown to promote supply chain discussion. • Ask students how they can trust the origin of hardware. Does the origin of all hardware need to be scrutinized? How can the supply chain be secured?

competitors, and organized crime.		
5.2.4 LO: Students will identify hardware security addresses issues related to an adversary physically gaining access to a device. 5.2.3c EK: Physical security measures can be used to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm.	• Securing supply chain resource: Saleh, Emile and Rizvi, Sarah. "10 ways to secure supply chains." *ITP.net*, 2 May 2020, https://www.itp.net/news/92310-10-ways-to-secure-supply-chains	• Sometimes hardware vulnerabilities cannot be eliminated, but physical security can prevent adversaries from getting their hands on your hardware in the first place. • Review physical security practices from Unit 9. • Task students with developing a physical security plan for vulnerable hardware.
5.2.4a EK: The hardware design can require the device disable itself if physically tampered. 5.2.4b EK: Students will identify examples of fail-safe in cybersecurity, i.e., a design feature or practice that in the event of a specific type of failure, inherently responds in a way that will cause no or minimal harm to other equipment, the environment or to people and provide recovery opportunities.		• Review the concept of failing securely. Does this promote the confidentiality or availability portion of CIA Triad? Which is more important when only information is involved? • It's important to note that in mechanisms and systems which impact people, protection of life should be considered priority in fail-safe design.
2.3.3 LO: Students will explain the importance of encapsulating		• Review the principle of resource encapsulation.

resources, i.e., creating well-defined interfaces around resources to set rules for how the resources should interact. 2.3.3a EK: Examples of resources are the memory, disk drive, network bandwidth, battery power, and a monitor. It can also be system objects such as shared memory or a linked list data structure. 2.3.3b EK: Encapsulation allows access or manipulation of the class data in only the ways the designer intended.		• Ask students to explain how hardware security can benefit from resource encapsulation. • Does the Meltdown vulnerability benefit from a breach in encapsulation? How?
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.		• Explore a relevant career, such as system testing and evaluation specialist.