Unit 4: Securing Devices

Content Area: **Business**
Course(s): **Generic Course**
Time Period: **Semester 2**
Length: **5 weeks**
Status: **Published**

Standards

8.1.12.CS.1	Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
8.1.12.CS.2	Model interactions between application software, system software, and hardware.
8.1.12.CS.3	Compare the functions of application software, system software, and hardware.
8.1.12.NI.2	Evaluate security measures to address various common security threats.
8.1.12.DA.2	Describe the trade-offs in how and where data is organized and stored.
8.2.12.ED.2	Create scaled engineering drawings for a new product or system and make modification to increase optimization based on feedback.
8.2.12.ED.5	Evaluate the effectiveness of a product or system based on factors that are related to its requirements, specifications, and constraints (e.g., safety, reliability, economic considerations, quality control, environmental concerns, manufacturability, maintenance and repair, ergonomics).
CAEP.9.2.12.C.3	Identify transferable career skills and design alternate career plans.
CAEP.9.2.12.C.7	Examine the professional, legal, and ethical responsibilities for both employers and employees in the global workplace.

Enduring Understandings

EU 4.1: Diversity of the Endpoint Attack Surface
Every connected device—from a massive enterprise server to a smart lightbulb—carries a unique set of hardware and software vulnerabilities that require specialized threat models. Adversaries weaponize distinct categories of malware (such as ransomware, Trojans, or fileless scripts) to exploit these variations, with low-power embedded/IoT devices often presenting the greatest challenge due to their lack of built-in security controls.

EU 4.2: Cryptographic Identity Enforcement
True authentication security requires mathematically obscuring credentials and combining multiple, distinct types of proof. Storing passwords safely relies on irreversible cryptographic hash functions and random "salts" to render leaked data useless, while robust access control demands Multi-Factor Authentication (MFA) that spans what you know, what you have, what you are, or where you are located.

EU 4.3: Continuous Proactive Device Hardening
Securing a device is an ongoing race against time that requires strict software hygiene, granular local boundaries, and clear operational rules. Because the release of a software patch signals a race where attackers actively reverse-engineer the vulnerability to target unpatched systems, devices must be continuously hardened using automated updates, host-based firewalls, and active endpoint defenses.

EU 4.4: Behavioral and Contextual Evidence Digital Footprints
An attacker operating on a device always leaves a trail of physical or behavioral evidence, but discovering that trail depends entirely on capturing the right context. Defenders must look for specific Indicators of Compromise (IoCs) across system logs, distinguishing between highly visible online attacks and silent, offline cryptographic cracking that leaves no log footprint at all.

Essential Questions

Topic 4.1: Device Vulnerabilities and Attacks
How do the structural differences between device types (servers, PCs, mobile, and IoT) change their risk profile and determine how they are targeted by specific malware mechanisms or exploitation vectors?

Topic 4.2: Authentication
How do cryptographic hash functions and multi-factor authentication (MFA) technically secure user identities, and what logic dictates how configurable policies mitigate both online and offline credential attacks?

Topic 4.3: Protecting Devices
How do defenders leverage host-based firewalls, signature scanning, software patching, and managerial policies to systematically shrink a device's attack surface?

Topic 4.4: Detecting Attacks on Devices
How do security teams analyze host, file, and behavior-based indicators of compromise (IoCs) to distinguish active endpoint attacks from normal system noise without creating operational bottlenecks?

Knowledge and Skills

Topic 4.1: Device Vulnerabilities and Attacks

- Identify and classify the four CED device types: server, personal computer, handheld/mobile, and embedded/IoT (4.1.A)
- Identify all eight malware types by name and mechanism, including fileless malware (4.1.B)
- Explain the seven device exploitation vectors and which vulnerability each adversary technique targets (4.1.C)
- Apply the High/Moderate/Low risk framework to device vulnerabilities using CED criteria and illustrative examples (4.1.D)
- Explain why embedded/IoT devices present unique security challenges compared to general-purpose computers

Topic 4.2: Authentication

- Explain why passwords are stored as hashes and describe the four properties of cryptographic hash functions (4.2.A)
- Explain how salting prevents rainbow table attacks and why identical stored hashes are a vulnerability (4.2.A.6)
- Distinguish online vs. offline password attacks and identify all seven attack types by mechanism (4.2.B)
- Classify authentication factors as knowledge, possession, biometric, or location, and explain MFA (4.2.C)
- Apply the five configurable login policy settings to reduce password attack risk (4.2.D)

Topic 4.3: Protecting Devices

- Identify and distinguish the three CED managerial policies for device security (4.3.A)
- Explain how anti-malware signature scanning works and its limitation against fileless malware (4.3.B)
- Explain why patching closes the exploitation window and why the patch release moment creates immediate risk for unpatched devices (4.3.C)
- Configure host-based firewall ACL rules and distinguish host-based from network-based firewalls (4.3.D)
- Map each protective control from this lesson to the exploitation vectors from Topic 4.1 it addresses

Topic 4.4: Detecting Attacks on Devices

- Explain what system logs record and define an indicator of compromise (IoC) (4.4.A.1–A.3)
- Classify IoCs as host-based, file-based, or behavior-based and identify examples of each (4.4.A.4–A.6)
- Apply the three detection method criteria (performance, cost, sensitivity/criticality) to choose between signature-based, anomaly-based, and hybrid detection for a given device (4.4.B)
- Evaluate detection methods using the three CED factors: speed, phase of attack, and false positive vs. bypass rate (4.4.C)
- Identify IoCs for online attacks, compromised passwords, password spraying, and credential stuffing in auth logs — and explain why offline attacks produce no detectable log evidence (4.4.D)

Transfer Goals

Students will be able to recognize the distinct warning signs of different types of malware and device exploits, allowing them to adjust their browsing habits and software downloads to avoid infecting their personal electronics.

Students will be able to effortlessly secure their digital identities by combining multiple layers of authentication (like biometrics, hardware keys, and passphrases) and recognizing the fundamental flaws of

relying entirely on simple passwords.

Students will be able to take ownership of their personal device security by proactively managing software patches, host firewalls, and application permissions, treating tech maintenance as a vital shield against active exploits.

Students will be able to spot unusual device behavior, unexpected background activity, or strange login notifications, knowing how to interpret these clues to determine if an account or device has been breached.

Resources

AP Cybersecurity Course and Exam Description, Effective Fall 2026, College Board

AP Cybersecurity Course Framework, Effective 2026-2027 School Year, College Board

AP Cybersecurity Curriculum, by APCSExamPrep.com

Cybersecurity Curriculum Materials, by Cyber.org

Cyber Range, provided by Cyber.org