ESL
SCIENCE
BUSINESS
BILINGUAL
PRESCHOOL
MATHEMATICS
LIBRARY MEDIA
SOCIAL STUDIES
WORLD LANGUAGES
GIFTED & TALENTED
TECHNOLOGY EDUCATION
ENGLISH LANGUAGE ARTS
FINE & PERFORMING ARTS
FAMILY & CONSUMER SCIENCE
HEALTH & PHYSICAL EDUCATION

RAHWAY PUBLIC SCHOOLS

CURRICULUM & INSTRUCTION

Content Area: Technology Education

Course: Advanced Placement Cybersecurity

Grade Level: 10-12

This curriculum is part of the Educational Program of Studies of the Rahway Public Schools.

ACKNOWLEDGMENTS

Jeffery Kurczeski,

Program Supervisor of 7-12 Math & Science and 9-12 Business & Technology Education

The Board acknowledges the following who contributed to the preparation of this curriculum.

Ambika Bhosale, Computer Science Teacher

Mrs. Lee Andrea Garvin, Director of Curriculum and Instruction

Subject/Course Title:
Advanced Placement Cybersecurity
Grades 10-12

Date of Board Adoption:
August 25, 2026

RAHWAY PUBLIC SCHOOLS CURRICULUM

Advanced Placement Cybersecurity: Grades 10-12

PACING GUIDE

Unit	Title	Pacing
1	**Introduction to Security**	**4 weeks**
1A	Understanding Social Engineering	1 week
1B	Suspicious Website Logins & Best Practices for Public Networks	1 week
1C	AI-Based Cybersecurity Attacks	1 week
1D	Leveraging AI in Cyber Defense	1 week
2	**Securing Spaces**	**6 weeks**
2A	Cyber Foundations	1 week
2B	Physical Vulnerabilities and Attacks	1 week
2C	Protecting Physical Spaces	2 weeks
2D	Detecting Physical Attacks	2 weeks
3	**Securing Networks**	**7 weeks**
3A	Network Vulnerabilities and Attacks	1 week
3B	Managerial Controls and Wireless Security	2 weeks
3C	Protecting Networks: Segmentation & Firewalls	2 weeks
3D	Detecting Network Attacks	2 weeks
4	**Securing Devices**	**6 weeks**
4A	Device Vulnerabilities and Attacks	1 week
4B	Authentication	2 weeks
4C	Protecting Devices	1 week
4D	Detecting Attacks on Devices	2 weeks
5	**Securing Applications and Data**	**10 weeks**
5A	Application and Data Vulnerabilities and Attacks	1 week
5B	Protecting Applications and Data: Managerial Controls and Access Controls	2 weeks
5C	Protecting Stored Data with Cryptography	2 weeks
5D	Asymmetric Cryptography	2 weeks
5E	Protecting Applications	2 weeks
5F	Securing Applications and Data - Detecting Attacks on Data and Applications	1 week

ACCOMMODATIONS

504 Accommodations:

- Provide scaffolded vocabulary and vocabulary lists.
- Provide extra visual and verbal cues and prompts.
- Provide adapted/alternate/excerpted versions of the text and/or modified supplementary materials.
- Provide links to audio files and utilize video clips.
- Provide graphic organizers and/or checklists.
- Provide modified rubrics.
- Provide a copy of teaching notes, especially any key terms, in advance.
- Allow additional time to complete assignments and/or assessments.
- Provide shorter writing assignments.
- Provide sentence starters.
- Utilize small group instruction.
- Utilize Think-Pair-Share structure.
- Check for understanding frequently.
- Have student restate information.
- Support auditory presentations with visuals.
- Weekly home-school communication tools (notebook, daily log, phone calls or email messages).
- Provide study sheets and teacher outlines prior to assessments.
- Quiet corner or room to calm down and relax when anxious.
- Reduction of distractions.
- Permit answers to be dictated.
- Hands-on activities.
- Use of manipulatives.
- Assign preferential seating.
- No penalty for spelling errors or sloppy handwriting.
- Follow a routine/schedule.
- Provide student with rest breaks.
- Use verbal and visual cues regarding directions and staying on task.
- Assist in maintaining agenda book.

IEP Accommodations:

- Provide scaffolded vocabulary and vocabulary lists.
- Differentiate reading levels of texts (e.g., Newsela).
- Provide adapted/alternate/excerpted versions of the text and/or modified supplementary materials.
- Provide extra visual and verbal cues and prompts.
- Provide links to audio files and utilize video clips.
- Provide graphic organizers and/or checklists.
- Provide modified rubrics.
- Provide a copy of teaching notes, especially any key terms, in advance.
- Provide students with additional information to supplement notes.
- Modify questioning techniques and provide a reduced number of questions or items on tests.
- Allow additional time to complete assignments and/or assessments.
- Provide shorter writing assignments.
- Provide sentence starters.
- Utilize small group instruction.
- Utilize Think-Pair-Share structure.
- Check for understanding frequently.
- Have student restate information.
- Support auditory presentations with visuals.
- Provide study sheets and teacher outlines prior to assessments.
- Use of manipulatives.
- Have students work with partners or in groups for reading, presentations, assignments, and analyses.
- Assign appropriate roles in collaborative work.
- Assign preferential seating.
- Follow a routine/schedule.

Gifted and Talented Accommodations:

- Differentiate reading levels of texts (e.g., Newsela).
- Offer students additional texts with higher lexile levels.
- Provide more challenging and/or more supplemental readings and/or activities to deepen understanding.
- Allow for independent reading, research, and projects.
- Accelerate or compact the curriculum.
- Offer higher-level thinking questions for deeper analysis.
- Offer more rigorous materials/tasks/prompts.
- Increase number and complexity of sources.
- Assign group research and presentations to teach the class.
- Assign/allow for leadership roles during collaborative work and in other learning activities.

ELL Accommodations:

- Provide extended time.
- Assign preferential seating.
- Assign peer buddy who the student can work with.
- Check for understanding frequently.
- Provide language feedback often (such as grammar errors, tenses, subject-verb agreements, etc…).
- Have student repeat directions.
- Make vocabulary words available during classwork and exams.
- Use study guides/checklists to organize information.
- Repeat directions.
- Increase one-on-one conferencing.
- Allow student to listen to an audio version of the text.
- Give directions in small, distinct steps.
- Allow copying from paper/book.
- Give student a copy of the class notes.

	● Provide written and oral instructions. ● Differentiate reading levels of texts (e.g., Newsela). ● Shorten assignments. ● Read directions aloud to student. ● Give oral clues or prompts. ● Record or type assignments. ● Adapt worksheets/packets. ● Create alternate assignments. ● Have student enter written assignments in criterion, where they can use the planning maps to help get them started and receive feedback after it is submitted. ● Allow student to resubmit assignments. ● Use small group instruction. ● Simplify language. ● Provide scaffolded vocabulary and vocabulary lists. ● Demonstrate concepts possibly through the use of visuals. ● Use manipulatives. ● Emphasize critical information by highlighting it for the student. ● Use graphic organizers. ● Pre-teach or pre-view vocabulary. ● Provide student with a list of prompts or sentence starters that they can use when completing a written assignment. ● Provide audio versions of the textbooks. ● Highlight textbooks/study guides. ● Use supplementary materials. ● Give assistance in note taking ● Use adapted/modified textbooks. ● Allow use of computer/word processor. ● Allow student to answer orally, give extended time (time-and-a-half). ● Allow tests to be given in a separate location (with the ESL teacher). ● Allow additional time to complete assignments and/or assessments. ● Read question to student to clarify. ● Provide a definition or synonym for words on a test that do not impact the validity of the exam. ● Modify the format of assessments. ● Shorten test length or require only selected test items. ● Create alternative assessments. ● On an exam other than a spelling test, don’t take points off for spelling errors.

UNIT 1A OVERVIEW

Content Area: Technology Education

Unit Title: Introduction to Security - Understanding Social Engineering

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit various scenarios are designed to connect the knowledge and skills students gain to relevant, real-world applications. These scenarios are paired with applicable student activities. Students experience three distinct examples of how adversaries try to compromise systems: Students explore how adversaries use social engineering to influence the behavior of targets and the impacts of targets clicking on malicious links or downloading malicious files. Students see how adversaries compromise systems through weak authentication, and they learn how to strengthen authentication to protect themselves. Students learn about the hazards of public Wi-Fi, including how adversaries use it to attack victims, as well as how to protect themselves.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
1.1.A Identify common indicators of social engineering tactics.
1.1.B Explain how social engineering tactics influence victims to perform a desired action
1.1.C Describe possible impacts for victims of social engineering attacks.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.
b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Vulnerabilities in systems cause risk and will learn to identify potential avenues of attack.
- Not to share personal details in response to unexpected emails, texts, DMs, or calls.
- If someone claims to be from a company or school, contact the organization using a trusted method (official website, known phone number, or in-person).
- To be careful what personal details are posted publicly.

Unit Essential Questions:

- What elements of an email might justify that the phishing email is not legitimate?
- What are some potential consequences for someone who clicked a link in a phishing email?
- What makes social engineering such an effective technique for hackers?
- Imagine you are trying to protect your network from social engineering hacks. What would you do?
- What do attackers do with personal information?

Knowledge and Skills:

Students will know...

- Social engineering attacks employ psychological tactics to manipulate users into revealing sensitive information (elicitation), downloading a malicious file, or clicking on a malicious link. Social engineering can be performed in person but is often done by email, by text message, or through social media messages.
- Adversaries often use psychological tactics like intimidation and urgency to achieve their goals. Intimidation is when an adversary threatens a target with negative consequences if they don't comply. Urgency is when an adversary creates reasons why a target should act quickly
- Social engineering tactics rely on common psychological principles that influence human behavior.
- Intimidation leverages a natural human aversion to negative consequences. By drawing attention to possible negative consequences, adversaries use fear to incite targets to act.

- Urgency leverages a natural human response to react quickly to time-sensitive needs. When targets detect a sense of urgency in a message, they feel pressured to respond or act quickly, which can prevent them from taking the time to consider whether an action is reasonable or safe.
- Victims may give an adversary personal information that could lead to impersonation, such as name, phone number, address, workplace, pets' names, or birthdate. These types of information, and information like them, are often used on websites as challenge questions to verify a user's identity.
- Victims may give an adversary secure information like a one-time password (OTP) or authentication login code, which could allow an adversary to log in to a service as the victim
- Victims may download malware or click a link that installs malware on their device, steals information from their web browser, or directs them to a website where their login credentials can be captured by an adversary.

Students will be able to...

- To identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 1B OVERVIEW

Content Area: Technology Education

Unit Title: Introduction to Security - Suspicious Website Logins & Best Practices for Public Networks

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit various scenarios are designed to connect the knowledge and skills students gain to relevant, real-world applications. These scenarios are paired with applicable student activities.This unit will focus on identifying password attacks and analyzing log files to identify signs of suspicious activity. Students will learn to identify the dangers of accessing public Wi-Fi.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
1.2.A Identify common signs of a password attack. .
1.2.B Explain how adversaries take advantage of weak authentication
1.2.C Explain how to make authentication stronger
1.3.A Identify the type of adversary conducting a cyberattack.
1.3.B Identify types of wireless cyberattacks.
1.3.C Describe actions individuals can take to increase protection of sensitive data when using the internet and Wi-Fi.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.
b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Vulnerabilities in systems cause risk and will learn to identify potential avenues of attack.
- By mitigating risks we can identify ways to protect from potential cyberattacks.
- Cyberattacks can be detected by analyzing log files and identifying signs of suspicious activity—often called indicators of compromise (IoCs).
- By analyzing network log files , security teams can spot the warning signs of an online password attack:
    - Many failed attempts over a short duration — Attackers often use automated tools that try hundreds or thousands of passwords in minutes
    - Login attempts at unusual times — Legitimate users typically log in during business hours; attacks often happen late at night or on weekends
    - Login attempts from unknown devices or locations — Unfamiliar IP addresses or devices can indicate an unauthorized access attempt

Unit Essential Questions:

- Does your password follow any predictable patterns?
- Could someone guess it using info from your social media?
- Is MFA enabled?
- Based on the pattern of usernames and passwords attempted, can you identify the type of password attack (brute force, dictionary attack, etc)?
- Why are zero-day vulnerabilities so much more dangerous than known vulnerabilities?
- Which combination (skill + motivation) do you think poses the greatest threat? Why?

Knowledge and Skills:

Students will know...

- In an online password attack, adversaries try logging in to a device or service using common passwords, common password patterns, or stolen passwords.
- Signs of an online password attack include:
    - Many failed attempts to log in over a short duration

    - Login attempts at unusual times
    - Login attempts from unknown devices
- Many people use common patterns when creating passwords, such as:
    - Starting a password with one or two words, adding a two-digit number (often signifying a year), and putting a special character at the end
    - Including the names of family or pets in their passwords
    - Including personally significant dates in their passwords
- Adversaries often construct a dictionary of possible passwords based on personal information gathered about a target (e.g., birthday, anniversary, names of pets and family) and use an automated tool to submit potential passwords.
- Users should create passwords that are long, random, and unique. A password manager can be used to generate and store strong passwords, or a user may create long, unique passphrases for their accounts.
- When creating passwords, users should avoid names, dates, or other personally meaningful words or numbers.
- When available, users should enable multifactor authentication (MFA), which will require the user to provide extra proof of identity—such as a one-time code—in addition to the password as an extra layer of security.
- Adversaries can be classified by their skill levels.
    - Low-skilled adversaries rely on malicious cyber tools created by others that can be purchased online. The tools they use exploit known vulnerabilities.
    - High-skilled adversaries have the capacity to create new malicious cyber tools or modify existing ones to adapt to new defensive techniques and tools. They also have the capacity to discover undocumented vulnerabilities, known as zero days.
- Adversaries have a variety of motivations, including greed, desire for recognition, dedication to a cause, revenge, politics, or beliefs.
- In an evil twin attack, an adversary sets up their own wireless access point (WAP) with a service set identifier (SSID) similar or identical to a target network; the adversary's network is called the evil twin. Victims of this attack could select to unknowingly connect to the evil twin, allowing the adversary to capture their network traffic. The adversary cannot read traffic that uses an encrypted protocol like HTTPS.
- In a jamming attack, an adversary floods an area with a strong electromagnetic (EM) signal in the same frequency range as the wireless network, which prevents legitimate traffic between the access point (AP) and users. This type of attack that prevents users from accessing resources is called a denial of service (DoS) attack.
- In a war driving attack, adversaries try to detect wireless network beacons while driving or walking around a target. If a wireless signal is detected, the adversary can gather information about the type of wireless network used and find areas where the wireless signal extends outside the physical building.
- Individuals should verify that the name of any wireless network they join exactly matches the name of the network they intend to join
- Most internet protocols are encrypted to protect network traffic. However, individuals may consider the sensitivity of their data in choosing whether to join unencrypted Wi-Fi networks to protect vulnerable data such as DNS queries
- Individuals may consider using a virtual private network (VPN), which encrypts all their traffic to the VPN operator's system. Although this action prevents a service provider from viewing traffic, the VPN provider can view the traffic.

Students will be able to...

- Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.

- Identify security controls, and explain how they mitigate risks.
- Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.
- Identify security controls, and explain how they mitigate risks.

EVIDENCE OF LEARNING

Assessment:
What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:
What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 1C OVERVIEW

Content Area: Technology Education

Unit Title: Introduction to Security - AI Based Cybersecurity Attacks

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit various scenarios are designed to connect the knowledge and skills students gain to relevant, real-world applications. These scenarios are paired with applicable student activities. Students will focus on understanding how AI regenerative tools can be used in cybersecurity attacks. This unit will focus on various types of attacks that are created using AI and preventive measures to avoid AI cyberattacks.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:

8.1.12.NI.2 Evaluate security measures to address various common security threats.

8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.

8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.

8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:

1.4.A Explain how adversaries use AI-powered tools to augment cyberattacks.

1.4.B Explain how to protect against some AI-augmented cyberattacks.

Career Readiness, Life Literacies, and Key Skills:

9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.

9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.

9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Large Language Models (LLM) like ChatGPT or Gemini are trained on massive amounts of text.
- Both adversaries and defenders in the realm of cybersecurity can leverage large Language Models (LLM).
- AI can be used to gather intelligence on the target and attack gaps in the defense system
- Multi factor Authentication (MFA) should be enabled to protect data
- Personal data should not be entered into any AI models.
- Output generated from AI tools needs to be reviewed before using it

Unit Essential Questions:

- How could an adversary use AI-generated videos to impersonate a real person?
- What are features of AI-generated content that can be leveraged by adversaries in cyber attacks?
- Why does multifactor authentication provide stronger protection than using a password alone?
- Why should personal data not be used to prompt AI tools?

Knowledge and Skills:

Students will know...

- Adversaries can use AI-powered tools that leverage existing voice and image samples of a person to create a digital avatar of that person. The use of these technologies enables adversaries to impersonate someone over the phone or even on a video call, which can lead to financial loss or the sharing of sensitive or private information. As more organizations adopt voice-based authentication, the impact of voice-impersonation has a larger potential impact. .
- Adversaries can use generative AI tools, like large language models (LLMs), to create convincing phishing messages in any target language. Because traditional phishing messages are sometimes written by nonnative speakers of the target's language, unnatural language is a feature that has been used to distinguish phishing messages from legitimate messages. However, with AI tools, adversaries can now craft phishing messages in any language that read as though they were written by a native speaker.
- Adversaries can craft prompts that extract secure or sensitive information from LLMs. Secure or sensitive information in LLMs can come from user input and the large data sets used to train LLMs.

- Adversaries can publish websites or modify existing websites to contain false information so that the false information will be included in the training sets for LLMs, causing the LLMs to repeat the false information.
- Adversaries can perform reconnaissance on a target using AI-powered tools that scan the internet to gather information posted on social media and public websites.
- Adversaries can use AI-enhanced coding tools to help them write new malware, modify existing application code to perform malicious activities, or to find vulnerabilities in large code bases.
- Shared secrets with close friends and relatives that can be used to verify each other's identities should be established. A secret word or phrase known only to two parties can be used to authenticate identities in high-stakes situations.
- Multifactor authentication (MFA) should be enabled. If an adversary clones a target's voice to access a system with voice authentication, requiring a second authentication factor could prevent an adversary from gaining access to accounts.
- Personal or sensitive data should not be entered into any AI-powered tools, such as chatbots or virtual assistants. Some AIpowered tools feed user input back into the model to provide continuous training. Adversaries could extract data that users have included in prompts.
- Output from AI-powered tools should be carefully evaluated. Verify information from AI-powered tools using reputable, stable, nonAI-based sources.

Students will be able to...

- To identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.
- Identify security controls, and explain how they mitigate risks

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 1D OVERVIEW

Content Area: Technology Education

Unit Title: Introduction to Security - Leveraging AI in Cyber Defense

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit various scenarios are designed to connect the knowledge and skills students gain to relevant, real-world applications. These scenarios are paired with applicable student activities. Students will explore how AI can be leveraged to defend a cyber attack. This unit will focus on how AI powered tools can be used to identify vulnerabilities and recommend mitigations.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
1.5.A Explain how cyber defenders can leverage AI-powered tools to protect networks, applications, and data
1.5.B Explain how AI-powered tools are enabling faster and more accurate threat detection and response.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- AI-powered threat detection can identify attacks in seconds, while manual analysis might take hours or days.
- AI-powered tools can be trained to, analyze massive volumes of digital events, identify patterns that indicate malicious activity and sort events into categories: like malicious vs. harmless
- AI can flag unusual patterns that could indicate attacks or misuse.
- AI can accelerate threat detection but it does not replace human expertise.
- AI is a tool that enhances human decision-making and it doesn't replace it.

Unit Essential Questions:

- What is a key advantage of using AI to review firewall rules and access controls?
- What is the main risk of automatically applying AI-generated security recommendations without a human security technician reviewing them first?
- How do AI-powered tools help cybersecurity teams manage the enormous volume of digital events occurring on networks every day?
- What are the potential benefits and risks of allowing AI systems to automatically take corrective actions when malicious activity is detected?
- How does AI improve the speed and effectiveness of threat detection and incident response compared to relying solely on human analysts?

Knowledge and Skills:

Students will know...

- AI tools can review current security configurations, like firewall rules and access controls, and recommend more secure options. A knowledgeable security technician should always check recommendations before being implemented.
- AI-powered tools can analyze application code to identify vulnerabilities and recommend mitigations. Recommendations should always be reviewed by a knowledgeable programmer before being implemented.
- AI-powered tools can suggest rules for automated detection systems. A knowledgeable detection engineer should always review detection rules before being added to a system.
- Of the millions of digital events that happen on networks daily, some likely represent an adversary conducting malicious activity. Humans cannot carefully examine all those events to identify the malicious activity.
- AI-powered tools can be trained to quickly analyze digital events and sort the events that are likely malicious activity from those that are harmless.

- AI-powered tools can be programmed to alert human cybersecurity personnel when likely malicious activity is detected or to take specific corrective actions based on the type of malicious activity detected.
- AI-powered tools enable threat-detection and response teams to catch malicious activity and intervene quickly to prevent loss, harm, damage, and destruction to digital infrastructure and data.

Students will be able to...

- Identify methods for monitoring systems, and explain how they detect attacks.
- Identify security controls, and explain how they mitigate risks.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- End of Unit Common Assessment
- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 2A OVERVIEW

Content Area: Technology Education

Unit Title: Securing Spaces - Cyber Foundations

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students focus on securing a physical location. Adversaries that can gain physical access to a device are often able to bypass many of the technical controls that protect the device and the data on it. Thus, securing the physical space is a critical first layer of defense and a concrete way for students to develop adversarial thinking skills and begin to identify vulnerabilities, threats, attacks, and mitigations. Students consider how physical spaces might be breached by adversaries, how to detect physical breaches, how to select devices to prevent or deter an adversary, and how to place those devices to maximize their usefulness.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
2.1.A Identify social engineering attacks.
2.1.B Identify types of adversaries.
2.1.C Describe the phases of a cyberattack.
2.1.D Describe the risk assessment process.
2.1.E Identify strategies for managing risk.
2.1.F Identify types of security controls.
2.1.G Explain why a defense-indepth security strategy is necessary to optimally protect an organization.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Adversaries use psychological manipulation (social engineering) and technical exploits to gain initial access, establish command and control (C2), move laterally, and exfiltrate high-value assets while evading detection.
- Cybersecurity controls are designed to protect Confidentiality, Integrity, and Availability from diverse adversaries ranging from low-skilled Script Kiddies to highly motivated Transnational Criminal Organizations and Insider Threats.
- Absolute security is impossible; organizations prioritize assets using qualitative and quantitative risk assessments to balance threat, vulnerability, and impact while managing unavoidable residual risk.
- Because single security controls can fail, layered defensive controls, guided by the appropriate risk treatment strategies (avoid, transfer, mitigate, accept), are required to build resilient systems.

Unit Essential Questions:

- How do adversaries exploit human psychology and technical vulnerabilities to perform a full network breach?
- How do an adversary's motivations, methods, and access level dictate the impact on an organization's Confidentiality, Integrity, and Availability?
- How do organizations evaluate likelihood, impact, and residual risk to make informed security choices?
- Why is a layered defense-in-depth approach necessary to mitigate risk, given that total security is unattainable?

Knowledge and Skills:

Students will know...

- Social engineers use psychological tactics to manipulate targets into taking a desired action.
- Pretexting is when adversaries create a believable reason to contact a target.
- Authority is when adversaries impersonate someone with power over a target or pretend to relay instructions from that person.
- Intimidation is when adversaries state negative consequences if demands aren't met.
- Consensus is when adversaries create social pressure by making a target believe everyone else is doing a desired action.
- Scarcity is when adversaries create a sense of limited availability.
- Familiarity is when adversaries pretend to be or know someone close to a target to establish trust.
- Urgency is when adversaries create a deadline that requires quick action by a target to avert negative consequences.
- Script kiddies are low-skilled adversaries who use tools developed by others without understanding how the tools work. They are often motivated by greed or a desire for recognition.
- Hacktivists are motivated by social, political, or personal causes. They compromise computers and networks to support their cause or stop perceived harm, believing their goals justify their illegal methods.
- Insider adversaries are unique threats because they have legitimate credentials and access to systems and data. Malicious third parties can recruit them and can be motivated by greed or revenge.
- Cyberterrorists are motivated by politics or beliefs and seek to disrupt entire communities, regions, or nations through cyberattacks (e.g., attacking a power grid, water treatment plant, or other civil infrastructure). They can act independently or on behalf of governments or criminal organizations.
- Transnational criminal organizations seek financial gain primarily by deploying ransomware and stealing corporate intellectual property (IP) to sell in illegal markets.
- Cyberattacks aim to disrupt, harm, steal, or destroy devices, networks, or data. Adversaries work in phases, which may not all be used in every attack. The phases are: i. Reconnaissance ii. Initial access iii. Persistence iv. Lateral movement v. Taking action vi. Evading detection
- In the reconnaissance phase of an attack, adversaries gather as much information as possible about their target, often using open source intelligence (OSINT), which is freely available information.
- In the initial-access phase of an attack, adversaries establish a foothold on the target's computer, often through social engineering or compromised or weak credentials.
- After gaining access during an attack, adversaries establish persistence to maintain access without needing to regain it. They may use a command and control (C2) protocol to send commands to the device and receive output, often through malware like a remote access trojan (RAT) or rootkit.
- In the lateral-movement phase of an attack, adversaries try to escalate their privileges by accessing computers and user accounts with elevated permissions to services and data.
- In the taking-action phase of an attack, adversaries act on their objectives by collecting targeted data, exfiltrating it, and disrupting services or destroying data.
- In the final phase of an attack, many adversaries try to evade detection by removing or editing log files and erasing other files they may have planted on devices.
- Risk occurs when a threat can exploit a vulnerability to compromise an asset.
- An asset is anything valuable. Assets include financial resources, intellectual property, data, digital infrastructure, physical property, and reputation.
- The likelihood of a vulnerability being exploited depends on many factors, including:
    - The value of the target: Adversaries are more likely to attack targets they perceive as valuable.
    - The level of skill required to exploit the vulnerability (i.e., the difficulty):

    - Vulnerabilities with well-documented exploits often require less skill and can be carried out by more adversaries.
    - The motivation and capabilities of likely adversaries: Highly motivated and skilled adversaries are more likely to be able to perform more complex exploits.
- Risk assessment considers two factors:
    - The likelihood of an attack against a specific vulnerability.
    - The severity of the projected damage from an attack against a specific vulnerability.
- The severity of an attack is often measured by financial cost, which can also include reputational and operational impacts.
- The result of a risk assessment can be quantitative or qualitative.
- Risk assessment documentation should include:
    - Vulnerable assets and their value.
    - Descriptions of likely threats to the assets.
    - Details of specific vulnerabilities for specific assets and how they would be exploited.
    - An explanation of the severity of damage (financial, operational, reputational, etc.) if a specific asset were compromised, and the likelihood of that compromise occurring.
    - A final rating, quantitative or qualitative, for each risk identified.
- Once a risk has been identified and assessed, an organization has four options for managing that risk: Avoid, Transfer, Mitigate and Accept
- Risk avoidance stops the activity that is generating the risk. If the activity is a critical part of an organization's mission or purpose, then avoidance is not possible.
- Risk transference places the burden of the risk on another entity, such as an insurance company, a government, or consumers.
- Risk mitigation implements security controls to reduce the likelihood or impact of a risk.
- Residual risk is the risk that remains after an organization has gone through avoidance, transference, and mitigation. The residual risk is the level of risk that an organization is willing to accept. Risk acceptance acknowledges the fact that absolute security is unattainable.
- To conserve financial resources and employee capacity, an organization will often favor solutions that are cost effective and easy to implement and maintain. Cost-effective solutions cost less to install and maintain than the expected loss from an attack.
- Security controls address at least one of the following principles:
    - Confidentiality ensures that only authorized individuals, systems, or processes can access data. Systems lacking confidentiality are vulnerable to data theft or destruction.
    - Integrity ensures data are accurate and trustworthy. Systems lacking integrity are vulnerable to data manipulation.
    - Availability ensures data and services are accessible to authorized individuals when needed. Systems lacking availability may experience unexpected downtime.
- Security controls can be classified by type.
    - Physical controls provide security in the physical space and include locks, fences, and cameras, bollards, and security guards.
    - Technical controls provide security in the digital space and include firewalls, antimalware software, and encryption.
    - Managerial controls provide rules, guidelines, policies, and procedures that specify what security should be in place and include password policies, regular access reviews, and incident response plans (IRPs).
- Security controls can be classified by function.
    - Preventative controls address potential vulnerabilities with the goal of stopping an adversary from attacking and include locks and encryption.
    - Detective controls help identify attacks when they occur and include intrusion detection systems (IDSs), cameras, and security incident and event management (SIEM) systems.
    - Corrective controls fix problems and help restore systems to an operational state and

include vulnerability patching, repairing a broken card reader, and intrusion prevention systems (IPSs).
- A defense-in-depth strategy, or layered defense, uses multiple types of security controls to protect sensitive data and systems
- A defense-in-depth strategy allows an organization to address different types of threats, each with a security control most suited to mitigate it.
- A defense-in-depth strategy allows for resilience in data protection so when one security control is bypassed by an adversary, another security control may still prevent access to the data or system or limit the damage done to the data or system.
- Layers in a defense-in-depth strategy can include human, physical, network, device, application, and data.

Students will be able to...
- Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk
- Identify security controls, and explain how they mitigate risks.

EVIDENCE OF LEARNING

Assessment:
What evidence will be collected and deemed acceptable to show that students truly "understand"?
- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:
What differentiated learning experiences and instruction will enable all students to achieve the desired results?
- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:
- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 2B OVERVIEW

Content Area: Technology Education

Unit Title: Securing Spaces - Physical Vulnerabilities and Attacks

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students focus on identifying physical vulnerabilities and attacks. Physical security threats include techniques like piggybacking, tailgating, shoulder surfing, dumpster diving, and card cloning, which allow adversaries to observe, impersonate, or bypass security controls. These threats can lead to serious consequences such as unauthorized access, data theft, system damage, service disruption, and overall organizational risk depending on the value of the asset and likelihood of exploitation.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:

8.1.12.NI.2 Evaluate security measures to address various common security threats.

8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.

8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.

8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:

2.2.A Identify common physical attacks.

2.2.B Explain how threats can exploit common physical vulnerabilities to cause loss, damage, disruption, or destruction to assets.

2.2.C Assess and document risks from physical vulnerabilities.

Career Readiness, Life Literacies, and Key Skills:

9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.

9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.

9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Adversaries bypass digital safeguards by exploiting human psychology (politeness, distraction) and physical security gaps through techniques like piggybacking, tailgating, card cloning, and dumpster diving.
- Direct physical access to devices or infrastructure allows attackers to bypass technical controls, install malicious hardware, alter systems, or disrupt essential power and service availability.
- Security risks originate not only from human adversaries seeking unauthorized entry or theft, but also from natural disasters that threaten the infrastructure supporting digital operations.
- Organizations prioritize physical security controls by evaluating physical vulnerabilities against asset value, likelihood of exploitation, and total business impact.

Unit Essential Questions:

- How do adversaries use physical social engineering and reconnaissance tactics to bypass technical security controls?
- Why does physical access to hardware or infrastructure pose an equal or greater threat to an organization than remote cyberattacks?
- How do non-human threats, such as natural disasters and power disruptions, impact the availability and integrity of digital systems?
- How can organizations evaluate and mitigate physical vulnerabilities to prevent initial footholds that escalate into major breaches?

Knowledge and Skills:

Students will know...

- Adversaries often use social engineering when conducting a physical attack.
- Piggybacking is the name for an attack where an adversary uses social engineering to manipulate an authorized individual to grant the adversary access to a restricted area. Common piggybacking tactics include carrying something large to entice an authorized person to hold the door open, pretending to be an authorized person who has forgotten their access token, or pretending to be a maintenance person who needs to get into a certain area to perform an inspection or repair.

- Tailgating is the name for an attack where an adversary gains unauthorized access to a restricted area by following close behind an authorized individual without that individual's awareness or knowledge.
- Shoulder surfing is the name for an attack where an adversary watches as a user accesses sensitive information so the adversary can use it later. Sometimes adversaries use a camera to record the target accessing the sensitive information for later analysis.
- Dumpster diving is the name for an attack where an adversary goes through a target's physical trash to look for information that could be used to help the adversary reach their goal.
- Card cloning is the name for an attack where an adversary makes a copy of an authorized user's access card so they can gain access to all the resources the user is authorized to access.
- Threats include human adversaries seeking to cause harm or disruption as well as natural disasters. Natural disasters can cause physical damage or destruction to computers and data as well as disruption of digital services provided by computers.
- Vulnerabilities are weaknesses or flaws that could allow an asset to be compromised. Common compromises include:
    - Unauthorized access to sensitive data or restricted physical spaces.
    - Disruption of services.
    - Theft or destruction of digital or physical resources.
    - Unauthorized modification of data.
- When adversaries disrupt power to a device, the device and any services it provides become unavailable. To disrupt power, adversaries may damage fuses or breakers in an electrical box, unplug or cut electrical wiring, or damage power distribution systems like substations and transformers.
- When adversaries gain access to an area with sensitive information, they can steal or copy sensitive information.
- When adversaries gain physical access to a device and its ports, they can plug in a keylogger or external drive containing malware, which could allow them to collect data from a user or possibly even to gain control of the device. With direct physical access adversaries can also physically destroy a device, making the device itself, any data stored on it, and any services it provides unavailable.
- Physical access to devices can allow adversaries to bypass many technical controls and layers of security.
- High risks from physical vulnerabilities arise when sensitive information or systems are exposed in physical spaces without sufficiently restricted and controlled access
- Moderate risks from physical vulnerabilities arise when a noncritical or nonsensitive part of an organization is left unprotected in a way that it could act as a foothold for an adversary to gain initial access to other resources.
- Low risks from physical vulnerabilities arise when a vulnerable asset is of low value and the vulnerability is unlikely to be exploited.

Students will be able to...

- Evaluate, with and without the support of AI, the likelihood and impact of risks.
- Document, with and without the support of AI, the likelihood and impact of risks.

EVIDENCE OF LEARNING

Assessment:
What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:
What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 2C OVERVIEW

Content Area: Technology Education

Unit Title: Securing Spaces - Protecting Physical Spaces

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students focus on the importance of increasing employee security awareness training and workstation security policies to help individuals recognize threats, reduce human error, and protect organizational assets through safe practices like locking devices and maintaining clean workspaces. Cyber defenders choose appropriate physical and technical security controls by analyzing how vulnerabilities may be exploited. Students will understand that organizations prioritize risk mitigation by evaluating both the severity of potential threats and the cost-effectiveness of the controls used to prevent, detect, or respond to attacks.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
2.3.A Identify managerial controls related to physical security.
2.3.B Determine mitigation strategies for risks from physical vulnerabilities.
2.2.C Assess and document risks from physical vulnerabilities.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.
a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Employees act as a primary defensive layer when supported by continuous security awareness training and baseline workstation policies (e.g., clean desk habits, locked screens, privacy filters).
- Cyber defenders implement a mix of preventive, detective, and corrective controls, ranging from physical barriers (bollards, turnstiles) to technical safeguards (disabling USB ports, UPS units), to mitigate exploits and maintain system availability.
- Selecting appropriate controls requires defenders to model potential adversary tactics, map vulnerabilities, and determine where technical versus physical measures are most effective.
- Security decisions balance threat severity against implementation costs, ensuring controls adequately mitigate high-impact risks without incurring prohibitive expense.

Unit Essential Questions:

- How do security awareness training and workstation policies turn employees into active defenders against social engineering and physical theft?
- How do defenders map specific physical and technical controls to adversary attack vectors to prevent, detect, or correct security breaches?
- How do infrastructure controls, such as access barriers and backup power systems, maintain availability and physical perimeter defense?
- How do organizations weigh risk severity against cost-effectiveness to select and prioritize security controls?

Knowledge and Skills:

Students will know...

- Organizations should conduct employee security awareness training to educate employees about how they can contribute to the organization's security by:
    - Detecting social engineering attempts like phishing.
    - Not badging other people into restricted areas.
    - Preventing device theft.
- Organizations should have a workstation security policy that outlines the measures necessary to protect a physical workplace. The policy may have tiers of workstation security based on the type of data handled at a workstation. Workstation policies often require:

    - Locking devices before leaving workstations unattended to prevent unauthorized access.
    - Clearing sensitive documents off workstations before leaving them unattended (sometimes called a clean desk policy).
    - Using a privacy screen filter or other physical barrier to prevent others from viewing information on the screen.
    - Connecting devices to surge protectors or uninterruptible power supplies (UPS).
- To determine a relevant control, a cyber defender considers how an adversary could take advantage of a vulnerability to attack a system and how to prevent, detect, or correct the attack.
- Installing physical controls like fencing, gates, and bollards around a building can deter adversaries from trying to physically access an organization's buildings.
- Locks on doors, server cabinets, and computers can prevent devices from being accessed or stolen.
- Card readers can record which employee badges are being used to access different entries at specific times and deny access to unauthorized badges.
- Access control vestibules and turnstiles can prevent an authorized person from intentionally or accidentally admitting an unauthorized person into a restricted area.
- Organizations can disable USB ports to prevent external drives from loading malware onto a computer.
- An uninterruptible power supply (UPS) provides a backup power source for a device during a power outage. Organizations can also use power generators to provide power at a larger scale to a building or set of critical devices.
- Organizations prioritize risk mitigations based on the severity of the risks and the cost of the recommended mitigations.

Students will be able to...

- Identify security controls, and explain how they mitigate risks.
- Determine layered security controls that address vulnerabilities.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 2D OVERVIEW

Content Area: Technology Education

Unit Title: Securing Spaces - Detecting Physical Attacks

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students focus on securing a physical location. Adversaries that can gain physical access to a device are often able to bypass many of the technical controls that protect the device and the data on it. Students will understand that cameras, motion sensors, locks, and security guards controls are most effective when properly placed and combined, such as using cameras with motion detectors, securing entry points with locks or vestibules, and positioning guards strategically to observe or respond to activity. Together, these measures help organizations identify suspicious behavior, reduce false alarms, and investigate incidents by providing both real-time monitoring and recorded evidence.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
2.4.A Identify ways security controls can detect physical attacks.
2.4.B Determine effective placement of security controls for detecting physical attacks.
2.4.C Apply detection techniques to identify physical attacks.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.
a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Monitoring assets like cameras and motion sensors are most effective when strategically positioned based on coverage angles, tampering risks, and traffic patterns, such as placed at entry/exit points or low-traffic sensitive areas.
- Humans play complementary security roles, where stationary/patrolling guards provide active deterrence and response, while trained employees serve as the first line of defense in recognizing and reporting unauthorized presence.
- Combining access controls (locks, access control vestibules, electronic badge logs) with monitoring tools directly counters unauthorized entry techniques like tailgating and piggybacking.
- Merging diverse physical security measures, such as cameras, motion detectors, door sensors, and guard forces, creates a comprehensive defense system capable of real-time detection, identity verification, active monitoring, and post-incident investigation.

Unit Essential Questions:

- How do organizations strategically deploy surveillance and monitoring tools (cameras, motion sensors) to maximize coverage and minimize blind spots or false alarms?
- How do human defenders, both security personnel and general employees, deter, detect, and respond to physical security breaches differently than automated monitoring systems?
- How do physical access controls and logging mechanisms work together to prevent and detect unauthorized entry techniques like tailgating and piggybacking?
- How does integrating physical detection, verification, and monitoring technologies enhance an organization's overall ability to investigate and respond to security incidents?

Knowledge and Skills:

Students will know...

- Cameras can capture a visual record of an adversary’s malicious activity. The feed from a camera should be recorded and monitored for maximum effect. Recordings can be especially helpful in after-incident investigations.
- Security guards can monitor activity in an area and respond to suspicious activity once detected.
- Motion sensors can alert security to movement in an area.

- Employees that work in a physical space are often the first to notice the presence of an unauthorized person and can alert security.
- When placing cameras, consideration should be given to visual coverage, angle, and the ability to be tampered with by an adversary. Consideration should also be given to what a camera in a specific area could capture an adversary doing and how that information would be helpful. Points of ingress and egress are often monitored by camera.
- Motion sensors should be placed in areas where traffic is unexpected, like server rooms, or areas where sensitive materials are stored and few people have access. Motion sensors in high-traffic areas create many false alarms, making the alarms less likely to be taken seriously when there is a real security event.
- Locks should be placed on all entries to areas containing sensitive information or systems. For areas with particularly sensitive information or systems, an organization could use an access control vestibule at the entry point to prevent piggybacking or tailgating.
- Security guards can be stationary or patrolling. Stationary guards can provide constant protection for a specific area, entrance, or high-value item. Patrolling guards are more difficult for an adversary to plan around and can create time pressure for an adversary. Placing stationary guards at places that funnel traffic (e.g., entry gates, main entrances or lobbies, and entrances to more secure access areas) can be highly effective, while patrolling guards are better suited for perimeters and exterior areas.
- Cameras provide visual monitoring and a visual record of activity within a designated space. Cameras can be paired with facial recognition software that can provide alerts when unauthorized individuals enter controlled areas. Once a physical breach has been detected, defenders can use live and recorded camera footage to track an adversary's path and actions.
- Motion detectors work best when paired with cameras. When a security alert is raised because a motion detector has been activated, defenders can use cameras to check the space visually and verify a physical security breach.
- When employees are required to use an electronic badge to unlock a door to a restricted area, a sensor can record how long the door was open. In reviewing entry logs for the door, potential piggybacking or tailgating can be detected by doors being open for longer than normal lengths of time.

Students will be able to...

- Identify methods for monitoring systems, and explain how they detect attacks. .
- Determine strategies and methods to detect attacks.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- End of Unit Common Assessment
- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 3A OVERVIEW

Content Area: Technology Education

Unit Title: Securing Networks - Network Vulnerabilities and Attacks

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students learn to apply their risk assessment skills in the domain of networking, identifying vulnerabilities and evaluating the likelihood and impact of a vulnerability being exploited to determine the risk. Students learn how to apply security controls to a network to help prevent and deter adversaries, and how to collect and analyze network data to detect attacks. Students also learn how automated tools, including AI, enable faster, more efficient detection of malicious activity on networks.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
3.1.A Identify common network attacks.
3.1.B Explain how adversaries can exploit network vulnerabilities to steal, disrupt, or destroy network communication.
3.1.C Assess and document risks from network vulnerabilities.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.
a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

C. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Adversaries exploit inherent trust in core network protocols (ARP, DNS) and device identifiers (MAC addresses) using techniques like spoofing, ARP poisoning, and DNS poisoning to conduct Man-in-the-Middle (MitM) attacks and harvest credentials.
- Weak physical port security, unsecured wireless networks, and unauthenticated access allow attackers to connect unauthorized devices, launch MAC flooding attacks, laterally move across local networks, or cause Denial-of-Service (DoS/DDoS) conditions.
- Firewalls and strong authentication mechanisms filter malicious traffic, prevent IP/MAC spoofing, and regulate network access, serving as critical barriers against unauthorized entry and lateral movement.
- Network flaws jeopardize Confidentiality, Integrity, and Availability. Organizations must utilize vulnerability scanners to systematically identify, assess, and prioritize remediation based on potential severity and impact.

Unit Essential Questions:

- How do adversaries exploit trust in fundamental network protocols and device identities to execute Man-in-the-Middle and spoofing attacks?
- How do uncontrolled network access points (unsecured switch ports, wireless networks, and lack of authentication) enable initial entry, lateral movement, and Denial-of-Service attacks?
- How do perimeter controls like firewalls defend against unauthorized traffic, spoofing, and reconnaissance attempts?
- How do vulnerability scanners and risk prioritization frameworks help organizations evaluate and defend against threats to network Confidentiality, Integrity, and Availability?

Knowledge and Skills:

Students will know...

- The address resolution protocol (ARP) is used by a default gateway on a network to establish a table that pairs internet protocol (IP) addresses with media access control (MAC) addresses. An ARP poisoning attack is when an adversary sends falsified ARP packets to the default gateway to modify the table so that the adversary's device receives traffic intended for the target by linking the target's IP address to the adversary's MAC address. Faking a MAC address is called MAC

spoofing. This is an example of an on-path attack (or man-in-the-middle attack), which is when an adversary interrupts a data stream between two parties, captures both parties' data, and copies or alters the data before sending them on. Both parties think they are communicating directly with each other, but instead they are each communicating with the adversary who is secretly intercepting their messages.

- A MAC flooding attack is when an adversary sends the target switch many Ethernet frames, each with a different MAC address. This can force the switch into broadcast mode, and the adversary can then collect all of the frames on the network (because they are being broadcast), which could allow the adversary to access sensitive information. This is an example of eavesdropping (or sniffing), which is when an adversary captures data in transit and can record and copy the data.
- A domain name system (DNS) poisoning attack is when an adversary pretends to be an authoritative name server (NS) and plants a fake DNS record on a DNS server to redirect browser traffic to a malicious website designed to steal credentials. This is an example of credential harvesting, which is when adversaries set up a fake login site that looks like a real one. Unsuspecting users enter their real credentials, which the adversaries capture and use.
- A smurf attack attempts to overwhelm a network with Internet Control Message Protocol (ICMP) requests. It is a type of denial of service (DoS) attack, which makes a system or resource unavailable to authorized users. During a smurf attack, an adversary sends many ICMP requests with the victim's address to the network's broadcast address. The network's gateway then sends these requests to all devices on the network. Each device on the network replies to the victim's address, creating a flood of traffic that can block legitimate messages. When multiple devices attack the same target simultaneously, it's called a distributed denial of service (DDoS) attack.
- Adversaries can send malicious traffic into a network to flood it creating a DoS, to map the internal structure of the network, or to spoof a legitimate device. Networks without firewalls, or with improperly configured firewalls, are vulnerable to these types of attacks.
- Adversaries that have compromised a device often attempt to leverage their access to compromise other devices on the local area network (LAN).
- Adversaries that physically plug into a data port can gain access to a LAN through the switch port unless port security is enabled. This allows adversaries to launch DoS attacks or perform MAC flooding or MAC spoofing attacks.
- Adversaries standing outside of physically secure spaces can pick up the signals and beacon frames from a wireless access point that is broadcasting outside the physical space. This allows them to gather information about the wireless network and to attempt eavesdropping and cryptographic attacks on it.
- Adversaries can attempt to join networks to launch attacks from within the networks. Networks that do not authenticate devices and users make it easier for adversaries to join.
- If there is an open network port, an adversary can plug a wireless access point into the port creating a rogue access point. The adversary could use this rogue access point to access the internal network wirelessly (maybe even from outside the physical space). This allows the adversary direct access to the LAN, bypassing any firewalls.
- Adversaries can attempt to break wireless encryption and intercept, steal, or compromise data on a network.
- Vulnerabilities on a network can lead to adversaries being able to intercept and alter data in transit, launch DoS attacks, or move laterally on a network to gain access to more sensitive or critical systems. Network vulnerabilities can constitute a risk to confidentiality, integrity, and availability.
- There are automated vulnerability scanners that can check networks, devices, and applications for known vulnerabilities. These scanners produce a report that often includes the vulnerabilities detected, their severity, and mitigation recommendations.
- Successfully exploiting a network vulnerability often requires advanced technical ability and knowledge. This can impact the likelihood of an exploit.

- High risks from network vulnerabilities allow an adversary to easily have a significant impact by capturing network traffic, spoofing a legitimate device on the network, or launching a DoS attack.
- Moderate risks from network vulnerabilities could include vulnerabilities that might give adversaries the ability to gain information about systems or devices on a network.
- Low risks from network vulnerabilities include vulnerabilities that would be difficult to exploit and would likely have minimal negative impacts on an organization.

Students will be able to...

- Evaluate, with and without the support of AI, the likelihood and impact of risks.
- Document, with and without the support of AI, the likelihood and impact of risks.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 3B OVERVIEW

Content Area: Technology Education

Unit Title: Securing Networks - Protecting Network: Managerial Controls and Wireless Security

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students learn to apply their risk assessment skills in the domain of networking, identifying vulnerabilities and evaluating the likelihood and impact of a vulnerability being exploited to determine the risk. Students learn how to implement network security policies for routers, switches, VPNs, and wireless systems establish configuration standards that improve protection by enforcing authentication, encryption, and access controls. Measures such as disabling unnecessary services, using port security and MAC filtering, restricting VPN access, and prohibiting split tunneling help reduce vulnerabilities and prevent unauthorized access.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
3.2.A Identify managerial controls related to network security.
3.2.B Configure wireless network security features.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.
a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Network infrastructure (routers and switches) requires consistent configuration policies, such as disabling risky legacy services (e.g., Telnet), enforcing centralized authentication, and implementing port security/MAC filtering, to restrict device access and minimize attack surfaces.
- Virtual Private Network (VPN) security relies on strong authentication, strict multi-factor checks, and the prohibition of split tunneling to ensure all remote traffic routes through organizational inspection and encryption controls.
- Deprecated wireless standards (WEP, WPS, WPA) contain fatal flaws; modern networks require WPA3 combined with robust user authentication to protect wireless communications from interception and brute-force attacks.
- Combining access controls (MAC filtering, mutual authentication) with visibility controls (adjusting signal strength, disabling SSID broadcast) reduces exposure while balancing network usability and security.

Unit Essential Questions:

- How do standardized hardening policies for routers and switches, such as central authentication, port security, and service management, prevent unauthorized access?
- How do VPN access rules and tunneling configurations protect remote data traffic and maintain control over network perimeters?
- Why are legacy wireless protocols vulnerable to interception, and how does modern encryption (WPA3) mitigate these weaknesses?
- How can organizations integrate authentication, encryption, and signal management to balance wireless network availability with defensive security?

Knowledge and Skills:

Students will know...

- A router security policy will set forth a minimum configuration standard for routers on an organization’s network and may include:
    - Banning local user accounts (All router logins must use an approved authentication server.).
    - Disabling unnecessary services (e.g., Telnet).

    - Requiring a firewall (An organization may opt for a firewall device separate from the router.).
- A switch security policy will set forth a minimum configuration standard for switches on an organization's network and may include:
    - Banning local user accounts (All switch logins must use an approved authentication server.).
    - Requiring port security to be enabled.
    - Using MAC filtering.
- A virtual private network (VPN) policy will detail the minimum security requirements for employees using a VPN to access an organization's internal network, and it may include:
    - A list of roles within the organization that are allowed to use a VPN to access the organization's internal network.
    - Authentication requirements for employees using a VPN (e.g., public/private key system or MFA).
    - A prohibition against split tunneling (also called dual tunneling).
- A wireless security policy will establish the minimum security requirements for wireless networks within an organization and may include:
    - Requiring users to authenticate to the wireless network through an extensible authentication protocol (EAP) connected to an approved authentication server.
    - Requiring all wireless traffic to be encrypted using AES encryption with a minimum key length.
    - Disabling beacon frames on wireless access points.
- Organizations can disable beacon frame broadcasting on wireless access points (WAPs) to make it harder for adversaries to find their wireless network and learn its basic properties.
- Organizations can control the broadcast direction and signal strength of a WAP so the signal does not extend beyond the physical space the access point is meant to cover.
- Organizations should enable strong wireless encryption protocols to ensure wireless frames are not readable by adversaries who might intercept them.
    - WEP, WPS, and the original WPA wireless encryption protocols have known vulnerabilities and are insecure.
    - WPA3 is currently the strongest wireless encryption algorithm.
- Organizations can enable MAC filtering to prevent unauthorized devices from accessing the network, and they can require users to authenticate when joining a network.

Students will be able to...

- Evaluate, with and without the support of AI, the impact of protective risk-management strategies.
- Implement and log mitigations with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies

- AP College Board Practice Questionnaire

Learning Activities:
What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 3C OVERVIEW

Content Area: Technology Education

Unit Title: Securing Networks - Protecting Network: Segmentation and Firewalls

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students learn to apply their risk assessment skills in the domain of networking, identifying vulnerabilities and evaluating the likelihood and impact of a vulnerability being exploited to determine the risk. Students learn about how network segmentation divides a network into smaller subnets, VLANs, and screened subnets (DMZs) to isolate traffic, contain security breaches, and apply different security controls based on the sensitivity of systems and data. The unit will focus on how firewalls protect these network segments by controlling inbound and outbound traffic through rules known as access control lists (ACLs), which filter traffic based on factors such as IP addresses, ports, protocols, services, and applications.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
3.3.A Identify techniques for segmenting a network.
3.3.B Explain why network segmentation can increase network security.
3.4.A Identify types of network-based firewalls.
3.4.B Explain how a firewall uses an access control list to allow or deny traffic entering or leaving a network.
3.4.C Determine the effective placement of firewalls in a network.
3.4.D Configure a firewall to manage the flow of network traffic.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Dividing networks into subnets, VLANs, and screened subnets (DMZs) isolates high-risk, public-facing services from internal assets, enforcing least privilege and containing adversary lateral movement.
- Strategic placement of firewalls at network boundaries and internal segment intersections establishes customized security zones, applying targeted controls based on data sensitivity and asset criticalness.
- Network traffic filtering relies on a hierarchy of technology, from basic packet headers (stateless) and session tracking (stateful) to advanced application-aware filtering and intrusion prevention in Next-Generation Firewalls (NGFWs).
- Firewall Access Control Lists (ACLs) enforce security rules sequentially, making precise rule order, directionality, and switch-level safeguards (like port security) vital for preventing misconfigurations and MAC-level exploits.

Unit Essential Questions:

- How do logical and physical segmentation strategies, such as subnets, VLANs, and DMZs, contain breaches and limit lateral movement across network boundaries?
- How do the functional differences between stateless, stateful, and next-generation firewalls shape traffic filtering capabilities and session visibility?
- Why does the explicit sequence and criteria of Access Control Lists (ACLs) dictate the effectiveness of perimeter and inter-segment firewall policies?
- How do layered network defenses, combining switch-level port security, VLAN isolates, and zone-based firewalls, work together to balance security with network operational availability?

Knowledge and Skills:

Students will know...

- Firewall zones and rules can be used to create a screened subnet (also known as a demilitarized zone, or DMZ)—a network segment that sits between public, external networks like the internet and internal, private networks. A screened subnet is typically a lower security zone than the internal, private networks, and it typically holds an organization's publicly facing resources, separating them from the internal network.
- Subnetting can be used to create different subnets based on IP addressing. If a device is compromised by an adversary, subnets can contain a security breach to reduce the number of exposed devices.
- Switches can be used to create VLANs, which logically separate devices physically connected to central switches.
- Network segmentation refers to the process of dividing a network into smaller, isolated segments or subnetworks (subnets).
- Dividing a network into smaller subnets isolates network traffic, which can prevent attacks on one subnet from impacting devices on other subnets.
- Network segmentation can allow for different security policies and controls to be applied to different segments of the network, allowing for higher security zones and lower security zones.
- Port security on a switch can prevent MAC flooding by limiting the number of addresses assignable to any single switch port.
- A firewall is used to allow or deny network traffic in or out of a network. The firewall itself is software that can be hosted on a standalone device or integrated into another network device, such as a router.
- A stateless firewall filters traffic based on information in packet headers, such as IP addresses, ports, and protocols.
- A stateful firewall (also known as dynamic packet filtering) tracks the state of network connections passing through the firewall and can filter according to connection-related rules in addition to the filtering done by a stateless firewall. This allows for more control over content allowed in and out of a network.
- A next-generation firewall (NGFW) has both the capabilities of typical stateless and stateful firewalls and additional advanced features, such as intrusion prevention, deep packet inspection, and filtering by application type.
- Network administrators create a set of rules, called an access control list (ACL), that a firewall uses to permit or deny inbound and outbound network traffic.
- ACL rules are checked in order and the first rule that matches the criteria will be executed for the specified data.
- A typical ACL will specify the direction of traffic (inbound or outbound), the criterion to filter by (IP addresses, logical port, service, or application), and the action to take (permit or deny).
- Each segment of a network should have a firewall to control the flow of data in and out of that segment.
- Network segments may have different security needs based on the data and services within them. The level of security for each firewall can be set independently.
- Each point of data ingress and egress between the internal network and the public internet should have a firewall.
- The requirements for a firewall will specify what type of traffic from which sources or to which destinations should be allowed or denied.
- Specific rules for a firewall can allow or deny inbound or outbound traffic based on source or destination port or IP address, service, protocol, or application.
- Rules are implemented in order, and changing the order of a set of rules can change which traffic is allowed or denied. Consideration must be given to the precedence of filtering priorities when establishing the order of rules.

Students will be able to...

- Identify security controls, and explain how they mitigate risks.
- Evaluate, with and without the support of AI, the impact of protective risk-management strategies.
- Implement and log mitigations with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 3D OVERVIEW

Content Area: Technology Education

Unit Title: Securing Networks - Detecting Network Attacks

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students learn to apply their risk assessment skills in the domain of networking, identifying vulnerabilities and evaluating the likelihood and impact of a vulnerability being exploited to determine the risk. Students will learn about automated threat detection tools such as NIDS, NIPS, and SIEM systems that analyze large volumes of network and device data to identify potential cyberattacks, generate alerts, and in some cases automatically block malicious activity. The unit will focus on effective monitoring and analysis of logs, network traffic, and system behavior to help security teams detect and respond to attacks.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
3.5.A Identify types of automated security tools used to detect network attacks.
3.5.B Explain how organizations can leverage artificial intelligence(AI) to enhance threat detection and response.
3.5.C Determine a network detection method.
3.5.D Evaluate the impact of a network detection method.
3.5.E Apply detection techniques to identify indicators of network attacks by analyzing log files.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.
b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Security monitoring relies on automated tools, including NIDS, NIPS, and SIEM platforms, to aggregate and analyze massive volumes of system and network logs, enabling human analysts to identify, investigate, and mitigate threats faster than manual review allows.
- Organizations choose between signature-based (efficient for known threats), anomaly-based (baseline behavior tracking for zero-days), and hybrid detection strategies, balancing traffic volume, network consistency, processing overhead, and financial cost.
- AI-driven detection uses probability scoring and threshold tuning to flag malicious activity, requiring security teams to balance the operational drain of false positives (which cause alert fatigue) against the severe risks of false negatives (undetected breaches).
- Specific network exploit techniques, such as ARP/DNS poisoning, MAC flooding, Smurf ICMP spikes, and wireless Evil-Twin or jamming attacks, leave distinct network-based Indicators of Compromise (IoCs) detectable through packet analysis and log correlation.

Unit Essential Questions:

- How do automated detection systems (NIDS, NIPS, SIEM) aggregate and process high-volume log data to assist human analysts in threat detection?
- How do the operational strengths and limitations of signature-based, anomaly-based, and hybrid detection models guide their deployment across different network environments?
- How do security teams use AI probability scores and alert thresholds to balance the operational cost of false positives against the danger of false negatives?
- How do specific network-based Indicators of Compromise (IoCs) reveal active exploits, such as poisoning, flooding, and wireless attacks?

Knowledge and Skills:

Students will know...

- Automated detection tools analyze data collected from an organization’s network and devices, such as switches and routers, servers, firewalls, and user computers. These data are often collected in a log file.

- A network intrusion detection system (NIDS) is an automated tool that analyzes data to determine if malicious activity is taking place on a network. When an attack is detected, it generates an alert.
- A network intrusion prevention system (NIPS) is an automated tool that, like an IDS, analyzes data to determine if malicious activity is taking place on a network. A NIPS can also mitigate or halt an attack by closing ports, blocking specific IP or MAC addresses, or rejecting specific protocols.
- A security information and event management (SIEM) system collects and analyzes data from multiple sources (including firewalls, NIDS/NIPS, device logs, and application logs) to detect patterns that may indicate a cyberattack and raises an alert if a potential attack is detected. Security analysts investigate the alert to determine whether it represents a true threat and follow standard operating procedures to resolve or escalate the alert.
- Computers log every action that users take. Firewalls, IDS, IPS, and other network sensors log all the traffic passing through various points in a network. A medium-sized organization's network is logging millions (or even tens of millions) of data points per day. Even a large team of humans is incapable of analyzing so much data.
- Threat detection teams are creating AI algorithms to analyze large amounts of data and classify the data patterns as malicious or normal.
- AI models for threat detection are based on probabilistic calculations; they report a percentage to indicate the likelihood that something is malicious.
- Organizations determine their own thresholds for what percentage of likelihood of a threat results in an alert. If the threshold is set too high, real attacks may go undetected; if the threshold is too low, the security team will be overwhelmed with false alerts.
- Volume of network traffic is a criterion for determining a detection method. Signaturebased detection is more efficient for networks with high traffic volume. Signature-based detection compares detection data to a database of known indicators of compromise (IoCs), called signatures. Signature databases must be updated with IoCs for the latest attacks. Signature-based detection runs more quickly than anomaly-based detection.
- Consistency of network traffic patterns is a criterion for determining a detection method. Anomaly-based detection is most effective on networks with consistent traffic patterns. Anomaly-based detection compares detection data to a baseline of recorded activity. Baselines must be recorded on uncompromised systems to establish expected data types and volumes. Anomaly-based detection triggers an alert or action when data types or volumes outside of a specified tolerance range are recorded. Anomaly-based detection relies on consistent patterns in network traffic to detect anomalous traffic patterns.
- Degree of sensitivity or criticality of a network is a criterion for determining a detection method. Networks with more sensitive or critical data or services will likely consider a hybrid approach. Hybrid detection combines signature-based and anomaly-based detection. Hybrid detection is more expensive than using either signature- or anomaly-based detection alone, and hybrid-detection models generate more alerts.
- Likelihood of novel attacks on a network is a criterion for determining a detection method. Signature-based detection cannot detect a new attack. When an organization suspects that adversaries are likely to attempt a new attack on a network, anomaly-based detection is the preferred method when the cost of hybrid detection is prohibitively high.
- Speed of detection is a factor in evaluating the impact of a network detection method. Faster detection enables faster response. Signature-based detection methods are faster than anomaly-based detection methods, especially on networks with high traffic volume.
- Cost is a factor in evaluating the impact of a network detection method. Detection tools and ongoing costs need to be within a budget. Anomaly-based detection systems require more expensive hardware to operate than signature based. Hybrid detection is the most expensive option because it combines both anomaly- and signature-based methods.

- False positive rate is a factor in evaluating the impact of a network detection method. Signature-based detection has almost no false positives. Anomaly-based or hybrid detection will have higher false positive rates. Impacts of high false positive rates include:
    - Time and resources are put toward investigating alerts for nonmalicious activity.
    - Alert fatigue is a condition that occurs when responders get accustomed to false positives and take alerts less seriously because they assume alerts are false positives before investigating them.
- False negative rate is a factor in evaluating the impact of a network detection method. A false negative occurs when an adversary can bypass a detection system. Signature-based detection systems are easier to bypass than anomaly-based or hybrid systems. False negatives can result in adversaries causing loss, harm, disruption, or destruction to data and systems.
- Evil-twin attacks can be detected by regularly scanning for service set identifiers (SSIDs) that look suspicious or similar to local legitimate SSIDs. Signal triangulation can be used to locate and disable an access point broadcasting an evil-twin network.
- Jamming attacks can be detected by recognizing that no wireless devices in a specific physical space are able to connect to a wireless network and by scanning for electromagnetic (EM) noise in the wireless range.
- ARP poisoning attacks can be detected by monitoring network traffic for unusual ARP messages (particularly duplicate MAC address ARP packets) and checking the ARP table on the default gateway.
- MAC flooding attacks can be detected by monitoring network traffic for an unexpected surge of Ethernet frames with different MAC addresses and checking the MAC address table on a switch.
- DNS poisoning attacks are difficult to detect. However, if an organization's website experiences an abrupt and otherwise inexplicable drop in traffic, DNS records should be examined as a potential cause.
- Smurf attacks can be detected by watching network traffic for a sudden increase in ICMP requests sent to the network's broadcast address.
- Network-based IoCs are discovered when analyzing network traffic, often in the form of packet capture files. Indicators can be found in source and destination IP addresses, ports, and protocols. These can include:
    - Connections to known malicious IP addresses
    - Unauthorized network scans
    - Unusual spikes or slow downs in network traffic
    - Mismatched port-application traffic

Students will be able to...

- Evaluate the impact of threat detection methods.
- Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- End of Unit Common Assessment
- CodeHS.com activities
- Lesson exercises
- Class participation and discussions

- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:
What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 4A OVERVIEW

Content Area: Technology Education

Unit Title: Securing Devices - Device Vulnerabilities and Attacks

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: Computer devices store, process, and transmit all the digital data in the world. Devices include computer systems and laptops, smart phones and tablets, and a range of items that have microcomputers installed in them, like washing machines and coffee makers—these are often called smart devices or IoT (Internet of Things) devices. In this unit students learn about how malware, such as viruses, worms, trojans, ransomware, spyware, keyloggers, logic bombs, rootkits, and fileless malware, can compromise devices by stealing data, disrupting operations, or giving adversaries unauthorized control. Students will identify device vulnerabilities—including unpatched software, weak authentication, open ports, disabled security features, and inadequate malware protection—can increase security risks, with the level of risk depending on the importance of the device, the data it stores, and the services it provides. .

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
4.1.A Identify types of computing devices.
4.1.B Identify the type of malware used in a cyberattack.
4.1.C Explain how adversaries can exploit common device vulnerabilities to cause loss, damage, disruption, or destruction.
4.1.D Assess and document risks from device vulnerabilities.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Computing devices range from high-capacity servers running critical core network services (DNS, DHCP, FTP) to personal computers, mobile devices, embedded systems, and IoT devices, each designed for specific roles, environments, and performance needs.
- Adversaries deploy varied malicious software, such as self-replicating worms, trojans, ransomware, rootkits, spyware, and fileless memory-resident malware, using distinct payload delivery and defense-evasion mechanisms.
- Securing modern endpoint devices requires multi-layered defense practices, including continuous software patching, multi-factor authentication, low-level BIOS/UEFI firmware security, and strict control over physical interfaces and open network ports.
- System risk levels (high, moderate, or low) are evaluated by measuring the likelihood of exploitation against the operational criticality, data sensitivity, and network role of the target device.

Unit Essential Questions:

- How do functional differences between server infrastructure, personal endpoints, embedded devices, and IoT hardware influence their roles and attack surfaces?
- How do different malware categories, from traditional file-based payloads to fileless memory attacks, execute their malicious objectives and evade security detection?
- How do system hardening controls, such as BIOS/UEFI settings, patch management, and authentication, protect devices against technical and physical exploits?
- How do defenders evaluate the likelihood and impact of vulnerabilities across diverse endpoint types to prioritize cybersecurity risk mitigation?

Knowledge and Skills:

Students will know...

- Server computers are devices that provide one or more services to other computers (e.g., DNS, DHCP, FTP). Any computer can be a server, and in an enterprise environment servers typically have more processing power and storage than a personal computer.
- Personal computers are devices that are designed to be used by one person for work or recreational purposes (e.g., word processing, graphic design, web browsing, and media production or viewing). These include desktop, laptop, and notebook computers.
- Handheld computers (also called mobile computers or information appliances) are smaller than personal computers and run on battery power. These include tablets, smartphones, and wearable technology like smart watches.
- Embedded computers are devices that are part of a machine. Embedded devices have specific instruction sets for interfacing with the specialized components of the machine they're embedded in. Embedded computers tend to be slower and cheaper than other computers and have minimal storage.
- Everyday devices with embedded computers are often called Internet of Things (IoT) devices. Embedded computers are found in transportation (e.g., cars, trains, and airplanes), devices that operate critical infrastructure (e.g., operating circuit breakers at electrical substations and pumps at water treatment plants), medical equipment (e.g., IV pumps, MRI scanners, pacemakers, and insulin pumps), and everyday devices like washing machines, coffee makers, and thermostats.
- Malware is malicious software that can damage or destroy a device or network, or allow an adversary access to a device and the data on the device.
- Malware is often used as a tool to accomplish part of an adversary's plan to achieve their ultimate goal(s). There are many types of malware, such as:
    - Viruses are malware that must be activated by a user executing or opening a file.
    - Worms spread from one computer to another without human interaction.
    - Trojans are malware embedded in other software that seems harmless. Remote access trojans (RATs) provide an adversary with remote access to the target system.
    - Ransomware encrypts a device's files, preventing the user from accessing files on the device. The ransomware typically presents the user with a screen demanding payment and promising to give the user a decryption key for their files if the user pays within a fixed amount of time.
    - Spyware tracks a user's actions on a computer and sends information back to an adversary.
    - A keylogger is software or hardware that logs the users keystrokes and sends the information back to the adversary. Adversaries can often extract usernames and passwords from keylogger data.
    - Logic bombs are set to trigger their effect only when a specific set of conditions are met; the conditions can include time and date, specific type or version of the operating system, character set the computer is using, etc.
    - A rootkit is sophisticated malware that gets into the target computer's operating system and can control nearly every aspect of the system, including making the rootkit itself invisible to detection.
- While most malware is a file or a collection of files, fileless malware is malicious code that lives in RAM and uses legitimate programs already installed on a device to compromise it.
- Adversaries can develop exploits for known vulnerabilities in software (including operating systems). Devices with unpatched software are vulnerable to these exploits, which could allow an adversary to crash a system, view user actions, enable or disable various services or components on the device (e.g., turning on a webcam or microphone), or even take control of the device to issue their own commands including commands to steal or destroy information on the device.

- Adversaries can take advantage of weak authentication requirements by guessing a user's password or using social engineering to get a user to divulge their password.
- When systems don't have a password on the basic input output system (BIOS) or unified extensible firmware interface (UEFI), an adversary can boot a computer into a special mode (e.g., "recovery mode") that gives them higher-level privileges. Without BIOS or UEFI protection, adversaries can load their own operating system onto a device from an external drive and use specialized tools to alter or create user profiles, including changing user passwords.
- Adversaries can load malware onto an external drive, and if autorun is enabled, then a device will run the malware when the external drive is inserted.
- Adversaries can leverage open ports to connect to a device.
- Adversaries can send malicious data to devices to disrupt them or attempt to take control of them. Devices that have no firewall (or a misconfigured firewall) cannot filter out this malicious data
- Adversaries often attempt to install malware on a device to disrupt or control it. Devices lacking anti-malware software are more vulnerable to this type of attack.
- Risk from device vulnerabilities can come from unauthorized access or malware that allow an adversary to impersonate an authorized user, remotely control a device, encrypt a device's drive to ransom the data, or wipe a device's memory, destroying data or rendering the device inoperable. The level of risk varies depending on the criticality of the device or the services the device provides or data it stores.
- High risks from device vulnerabilities involve potentially compromising sensitive data or critical operations.
- Moderate risks from device vulnerabilities can arise from weak authentication requirements or from vulnerabilities that would be less likely to be exploited.
- Low risks from device vulnerabilities are typically related to vulnerabilities that, if exploited, would have little impact.

Students will be able to...

- Evaluate, with and without the support of AI, the likelihood and impact of risks
- Document, with and without the support of AI, the likelihood and impact of risks.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 4B OVERVIEW

Content Area: Technology Education

Unit Title: Securing Devices - Authentication

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: Computer devices store, process, and transmit all the digital data in the world. Devices include computer systems and laptops, smart phones and tablets, and a range of items that have microcomputers installed in them, like washing machines and coffee makers—these are often called smart devices or IoT (Internet of Things) devices. In this unit students will know how cryptographic hash functions convert data of any size into a fixed-length output and are widely used to securely store passwords because hashes are repeatable, difficult to reverse, and resistant to collisions. The unit will focus on how authentication can rely on knowledge, possession, biometric, or location factors, and multifactor authentication (MFA) provides stronger security by requiring users to verify their identity using more than one authentication factor.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
4.2.A Explain why hashes (also called hash outputs, checksums, message digests, or digests) are used to store passwords.
4.2.B Explain how password attacks exploit vulnerabilities.
4.2.C Determine the type of authentication used to verify the identity of a user.
4.2.D Configure login settings to make a device more secure.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Cryptographic hash functions convert arbitrary data into deterministic, fixed-length digests characterized by pre-image resistance and collision resistance. Algorithms with discovered collision vulnerabilities (e.g., MD5, SHA-1) become deprecated.
- Systems store salted password hashes rather than plaintext to prevent offline lookup attacks, ensuring that identical passwords generate distinct stored hashes and defeating precomputed rainbow table attacks.
- Adversaries compromise credentials via online methods (password spraying, credential stuffing) and offline methods (brute-force, dictionary, rainbow tables) that target stolen databases free from account lockout limits.
- Defending authentication infrastructure requires combining strong password policies and lockout settings with multi-factor authentication (MFA) across knowledge, possession, biometric, and location factors.

Unit Essential Questions:

- How do mathematical properties of cryptographic hashes, such as determinism, fixed length, and collision resistance, guarantee data integrity?
- How does salting password hashes neutralize precomputed offline database attacks like rainbow tables and duplicate credential matching?
- How do the operational strategies of online password attacks (spraying, stuffing) differ from offline attacks (brute-force, dictionary)?
- How does multi-factor authentication (MFA) mitigate the systemic vulnerabilities inherent to single-factor, knowledge-based authentication?

Knowledge and Skills:

Students will know...

- A cryptographic hash function (also called a message digest function) is a mathematical algorithm that takes binary data of an arbitrary length, processes it according to a set of instructions, and outputs a fixed-length binary string called the hash (or checksum or message digest). Well known cryptographic hashes include:
    - MD5
    - SHA-1, SHA-256, SHA-512 (SHA stands for Secure Hash Algorithm)
    - NTHash
    - RIPEMD-160
- An n-bit hash has 2^n possible outputs. The number of inputs is infinite, and so inevitably two different inputs will produce the same hash. This is called a collision.
- Cryptographic hash functions have the following properties:
    - Hashes are collision resistant; it is difficult to find two different inputs to the same hash function that produce the same output.
    - Hashes have pre-image resistance; given a hash, it is infeasible to figure out the input that generated the hash.
    - Hashes are repeatable; the same input will always produce the same hash.
    - Hashes have a fixed length; the length in bits of the hash for a specific hash function is constant regardless of the size of the input.
- Adversaries try to compromise hashing functions by forcing collisions in their output. If an efficient algorithm exists to force a collision for a specific hash function, then that hash function will be deprecated (no longer used in secure settings). MD5 and SHA1 are examples of deprecated hash functions.
- Password-based authentication services shouldn't store passwords in plaintext, so that if an adversary gains access to the user:password directory they won't immediately know the passwords for all users. Instead, user passwords should be hashed and the hash stored in a database. When a user enters their password, it is hashed, and the hash is compared to the hash stored on file. If the hashes match, then the user is authenticated.
- If two users had the same password, then their passwords would have identical hashes in the user:password directory. To prevent this, a few random bits (called salt) are hashed with a user's password to generate the hash. Each user's salt is unique, so even if two users have the same password they will have a different password hash because they have different salt.
- If an adversary can compromise the password of a legitimate user, and that user's organization has not enabled MFA or other authentication protections, then the adversary can act within that organization with all the access and rights available to the user.
- Password attacks can be classified as online or offline.
    - Online password attacks attempt user:password combinations in an active authentication portal.
    - Offline password attacks have captured a user:password database and can run password attacks against the database on their own computer. This method bypasses any account lock out protections that may be in place.
- Many users reuse the same passwords (or variations of the same password) for all the services and accounts they have, despite warnings not to. When an organization's user database is stolen, the usernames, emails, and passwords are sold to adversaries or posted online. Adversaries often begin an attempt to compromise an account by trying stolen or leaked credentials for a target individual.
- Many users set passwords that are easy to guess, and adversaries will attempt to guess common passwords for a user's account. Password spraying is an attack where an adversary attempts a common password against many different user accounts.

- Some services and devices (e.g., switches, routers, and IoT devices) are preconfigured with a default administrative user and password. Credential stuffing is an attack where an adversary attempts to gain access to these services or devices using common default credentials or account credentials that have been stolen.
- Offline password attacks use automated hashcracking tools to hash possible passwords and compare them against a captured hash. Although hashes can't be reversed, an adversary can use these tools to hash many potential passwords and compare them to the target hash. If an adversary finds a hash that matches, they can use the password that generated the hash to login to the user's account. Offline attacks include:
    - Brute force attacks, where an adversary uses an automated tool to test all the potential passwords that a user could have.
    - Dictionary attacks, where an adversary uses an automated tool to test a list of common passwords.
- A rainbow table attack uses a list of common passwords to generate a rainbow table. A rainbow table is a table that contains each potential password and its hash. The table is then sorted by the hashes, and the adversary uses an automated tool to search the list of hashes for the captured hash. If the hashes match, then the adversary has found a password that generates the same hash, and the password will allow the adversary to login to the user's account.
- Authentication mechanisms are technical controls that verify the identity of a user to ensure that only authorized users access a system. The proof the user provides to identify themselves is called a factor. Common authentication factors include:
    - Something the user knows (knowledge factor).
    - Something the user has (possession factor).
    - Something the user is (biometric factor).
    - Somewhere the user is (location factor).
- Knowledge factors can be passwords, PINs, or answers to preselected challenge questions. For a knowledge factor to be effective it needs to be something an adversary can't easily guess; however, knowledge factors that are difficult for an adversary to figure out can also be harder for a user to remember.
- A possession factor is an object a user has that is unique to them, such as an access card, a bank card, a cell phone, or an authentication token. The more difficult it is for an adversary to obtain the object (or a copy of it), the more secure the possession factor is.
- Biometric factors measure features of the human body and can include fingerprints, palm prints, facial recognition, iris or retina scans, or voice identification. Biometric factors are difficult for an adversary to duplicate because they are unique to an individual.
- Location factors use information about Wi-Fi signals, GPS data, time zone settings, and even IP address information to make determinations about location. Rules can be established for allowing or denying access based on a location factor.
- Multifactor authentication (MFA) is when a system uses more than one factor to authenticate a user. MFA is more secure than single-factor authentication because it requires the user to provide at least two separate factors of authentication.
- Requiring complexity in passwords is a login setting that can be configured. When enabled, users setting a new password must include at least one character from each character set. Passwords with characters from each character set are significantly harder for an adversary to crack than passwords that use characters from only one or two character sets. The main character sets often required are:
    - Uppercase letters (A–Z)
    - Lowercase letters (a–z)
    - Numeric digits (0–9)
    - Special characters (!"#$%&'()*+,-./:;<=>?@ [\ ] ^_`{|}~)

- Requiring a minimum password length is a login setting that can be configured. This means that users must have at least a certain number of characters in their password. The longer and more complex a password is, the longer it will take a digital tool to crack the password.
- Requiring a maximum password age is a login setting that can be configured. When configured, users will receive a prompt to change their password a certain number of days after their last password change, usually every 90 or 120 days. If a user's password has been compromised, changing it could prevent an adversary from gaining access to the user's account. However, some national standards recommend that organizations not require users to change their passwords on predefined intervals to discourage users from developing password patterns (e.g., PasswordFall2028).
- Requiring the system to store a certain number of previous user passwords is a login setting that can be configured. This prevents a user from reusing a password. Many organizations store users' previous 5–10 password hashes to prevent reuse.
- Requiring a lockout period after a certain number of invalid login attempts is a login setting that can be configured. This prevents an adversary from continuously randomly attempting wrong passwords. Many organizations lock a user's account after 3–5 invalid login attempts. The period of the lockout varies.

Students will be able to...

- Identify security controls, and explain how they mitigate risks.
- Determine layered security controls that address vulnerabilities.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 4C OVERVIEW

Content Area: Technology Education

Unit Title: Securing Devices - Protecting Devices

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: Computer devices store, process, and transmit all the digital data in the world. Devices include computer systems and laptops, smart phones and tablets, and a range of items that have microcomputers installed in them, like washing machines and coffee makers—these are often called smart devices or IoT (Internet of Things) devices. In this unit, students learn about how organizations use policies such as acceptable use, password, and software installation policies to define how users should securely access, manage, and use devices, software, and organizational resources. The unit will focus on the importance of security tools such as anti-malware software, regular software updates, and patches that help protect systems by detecting malicious files and fixing known vulnerabilities before they can be exploited.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
4.3.A Identify managerial controls related to device security.
4.3.B Explain how anti-malware software can make a device more secure.
4.3.C Explain why keeping a device's operating system and software updated makes it more secure.
4.3.D Configure a host-based firewall.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.
b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Acceptable Use Policies (AUP), password standards, and software installation restrictions establish baseline operational rules that protect organizational assets, limit user risk behaviors, and reduce productivity distractions.
- Enforcing password policies, governing length, complexity, reuse, and secure vault tools, reduces account takeover risks and reinforces multi-layered access management.
- Host-based firewalls inspect incoming and outgoing endpoint traffic using rule sets filtered by IP addresses, ports, protocols, and application profiles to isolate single devices from network threats.
- Modern endpoints rely on continuous software patching, vulnerability management, and anti-malware solutions that use signature databases to detect, isolate, and remove malicious payloads.

Unit Essential Questions:

- How do administrative policies (AUP, software installation rules, password policies) govern user behavior to reduce organizational attack surfaces?
- How do password complexity mandates and vault management tools mitigate credential misuse and account compromise?
- How do host-based firewalls filter traffic at the endpoint level to provide defense-in-depth within a network environment?
- How do signature-based anti-malware tools and systematic patch management protect individual hosts against known software vulnerabilities?

Knowledge and Skills:

Students will know...

- An acceptable use policy will describe the range of activities that are permissible, prohibited, or required by users on devices owned by an organization and may include:
    - Prohibiting users from accessing specific websites or types of websites (e.g., social media or gaming).
    - Requiring users to keep software updated.

    - Allowing users to connect peripheral devices.
    - Prohibiting users from connecting external drives or media.
- A password policy will detail the requirements for user passwords within an organization and may include:
    - A minimum or maximum password length.
    - A minimum or maximum amount of time a user may keep the same password.
    - A prohibition of password reuse.
    - Rules for password construction (e.g., no dictionary words and character set requirements).
    - A suggestion to use secure password management tools instead of writing passwords down.
- A software installation policy will describe what (if any) software users are allowed to install on their devices and usually also a process for users to request specialized software they may need to perform their role, and it may include:
    - A prohibition against users installing software on their devices.
    - A process for users to request new software needed for their role.
    - A list of approved software for users.
- Anti-malware software (sometimes called antivirus software) has tools to quarantine and remove malware that can corrupt, spy on, or destroy a system. Malware contains indicators that make it detectable; these indicators are called signatures.
- Anti-malware software has a database of malware signatures. It periodically scans the files on a device and checks to see if any of the files match any of the signatures in its database. If there is a match, the software quarantines and removes the malicious files.
- When vulnerabilities in operating systems and software are found, the vendor or organization that maintains the operating system software will fix it and send an update. A small update is called a patch.
- Ensuring that a computer's operating system and software applications are updated to the most recent version prevents adversaries from taking advantage of a known vulnerability
- Host-based firewalls allow or deny traffic into or out of a single device. This provides an extra layer of security in case a host is connected to a compromised network.
- A host-based firewall is software that runs on a device and follows a set of rules (an ACL) like a network-based firewall. Firewall rules are implemented in order, applying the first rule that matches.
- A host-based firewall can also block specified types of outbound traffic. Host-based firewalls should always block ports or services not needed for a given device.
- The rules for a host-based firewall can allow or deny traffic based on source or destination port or IP address, service, protocol, or application.

Students will be able to...

- Evaluate, with and without the support of AI, the impact of protective risk-management strategies.
- Implement and log mitigations with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:
What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:
What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 4D OVERVIEW

Content Area: Technology Education

Unit Title: Securing Devices - Detecting Attacks on Devices

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: Computer devices store, process, and transmit all the digital data in the world. Devices include computer systems and laptops, smart phones and tablets, and a range of items that have microcomputers installed in them, like washing machines and coffee makers—these are often called smart devices or IoT (Internet of Things) devices. In this unit, students learn about how system logs record events such as login attempts, user activities, system processes, and file actions, providing valuable evidence for detecting and investigating cyber incidents through indicators of compromise (IoCs). Students will learn that organizations select detection methods based on factors such as device performance, cost, sensitivity, and detection speed, while analyzing authentication logs can help identify attacks such as password spraying, credential stuffing, and compromised user accounts.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
4.4.A Explain how to detect attacks against devices.
4.4.B Determine controls for detecting attacks against a device.
4.4.C Evaluate the impact of a device detection method.
4.4.D Apply detection techniques to identify indicators of password attacks by analyzing log files.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Computing systems record operations across authentication, process execution, and file activity, providing the foundational telemetry security analysts use to reconstruct cyber incidents.
- Analysts detect unauthorized access and malware activity by identifying host-based IoCs (unexpected processes, altered system files) and file-based IoCs (known malicious signatures, hashes, and non-standard paths).
- Authentication logs reveal online credential attacks, such as password spraying, credential stuffing, and brute-force attempts, by tracking behavioral anomalies like rapid failure sequences, unusual login times, and geographical outliers.
- Selecting security detection strategies (signature vs. anomaly) and deploying Endpoint Detection and Response (EDR) requires balancing resource overhead, system sensitivity, detection speed, and false positive ratios.

Unit Essential Questions:

- How do security analysts use system telemetry and event logs to identify Indicators of Compromise (IoCs) and reconstruct security breaches?
- How do host-based and file-based IoCs, such as altered processes, unauthorized file modifications, and hash signatures, reveal malicious activity on endpoints?
- How do authentication logs help distinguish between normal user access and active credential attacks (password spraying, credential stuffing)?
- How do organizations balance detection speed, system performance, cost, and alert accuracy when choosing between signature-based, anomaly-based, and EDR solutions?

Knowledge and Skills:

Students will know...

- System processes and settings, login attempts, file download attempts, and user actions are logged by computing systems. These logs can be used to reconstruct circumstances leading up to and during a cyber incident.
- An indicator of compromise (IoC) is evidence that an adversary has compromised a device or network.
- Authentication logs (or auth logs) record every attempted login on a system. Analysis of authentication logs can reveal attempted attacks.
- Host-based IoCs are discovered when analyzing logs and configuration settings. Indicators, such as the following, can be found in authentication logs, user activity logs, and system configuration files:
    - Unusual files being created or modified.
    - Unexpected processes or services.
    - Unauthorized changes to system configuration settings.
    - Unauthorized software installation or update.
- File-based IoCs are discovered when analyzing files on a device. Indicators are usually found in executable files and can include:
    - Files whose hash matches known malware.
    - File names that are known to be created by a certain piece of malware.
    - File paths that are associated with malicious activity.
- Behavior-based IoCs are discovered when analyzing logs. Indicators can be found in authentication logs and access logs and can include:
    - Multiple failed login attempts.
    - Unusual login times or locations.
    - Unauthorized attempts to access sensitive data.
    - Attempts to elevate user privileges on a system.
- Performance is a criterion for determining a detection method. Detection tools use system memory and processing power and can impact the performance of a device. Anomaly-based detection tools use more system resources than signature-based tools. Signature-based detection is a better option for devices with less powerful system resources. Many embedded devices do not have enough system resources to run any detection tools on the device.
- Cost is a criterion for determining a detection method. Organizations that purchase detection software need to consider the cost of purchasing enough software licenses for the number of devices they need to monitor. Some organizations purchase an endpoint detection and response (EDR) service from a third-party vendor. Although these services are expensive, they provide a holistic, unified approach to threat detection for an organization's devices; they typically include a centralized alert platform for monitoring possible attacks on devices.
- Sensitivity or criticality of the device is a criterion for determining a detection method. Devices that store or process sensitive information or provide critical services are more likely to be targeted by adversaries and benefit from a hybrid-detection model to offer maximum protection, when possible.
- Speed and performance are factors in evaluating the impact of a detection method. Signature-based detection is faster than anomaly-based detection in general, and that effect is compounded on devices, which often lack the processing power to effectively run anomaly-based detection tools. Implementing resource-intensive detection tools on devices can degrade device performance.
- Phase of the attack is a factor in evaluating the impact of a detection method. To carry out actions on a device, adversaries must first bypass a combination of physical- or network layer protective, deterrent, and detective security controls. Detecting and stopping an attack at the device level can prevent adversaries from accessing sensitive data or disrupting critical services.

- False positives versus ease of bypassing detection is a factor in evaluating the impact of a detection method. Most device-level detection tools are signature-based, and signature-based detection has a low rate of false positives. However, signature-based detection is easier for adversaries to bypass.
- Online password attacks can be detected in authentication logs. A single user attempting many wrong passwords is an indicator of an online password attack. If a user:password hash database has been compromised, all the user passwords in the database should be considered insecure and all users should be forced to reset their passwords.
- If an authorized user is logging in from a different location or IP address than expected, or at a different time than normal, this can be an indicator that the user's password has been compromised.
- An indicator of password spraying is many users trying to log in within seconds of each other from one IP address or from unusual IP addresses.
- An indicator of credential stuffing is a series of default user:password combinations being attempted on a device in quick succession, often from the same IP address.
- Offline password attacks can't be detected, because the attack takes place on the adversary's computer.

Students will be able to...

- Determine strategies and methods to detect attacks.
- Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- End of Unit Common Assessment
- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 5A OVERVIEW

Content Area: Technology Education

Unit Title: Securing Applications and Data - Application and Data Vulnerabilities and Attacks

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: Data is the foundation of the digital world. Every movie or song that is streamed, every website visited, and every financial transaction made online is recorded as digital data. Stealing, modifying, or denying access to data is often the end goal of an adversary. In this unit, students learn how adversaries commonly attack data and applications. Students learn how to set access controls to limit who has what type of access to data. They also learn how to use cryptography to protect the confidentiality and integrity of data both in storage and while it is being transmitted. Additionally, students learn how adversaries attack applications, what to look for in logs as evidence of an attack, and some mitigations that can help limit or stop an attack.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
5.1.A Explain how adversaries can exploit application and file vulnerabilities to cause loss, damage, disruption, or destruction.
5.1.B Explain how application attacks exploit vulnerabilities.
5.1.C Assess and document risks from application and data vulnerabilities.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.
b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Unencrypted files remain vulnerable to unauthorized extraction, making file-level encryption and strict access controls essential to maintaining data confidentiality and preventing privilege escalation via administrative accounts.
- Failing to sanitize user input allows adversaries to execute injection attacks, such as SQL Injection (SQLi) targeting back-end databases and Cross-Site Scripting (XSS) executing malicious code in client browsers.
- Software flaws like buffer overflows overwrite system memory to execute arbitrary code or crash applications, while directory traversal allows unauthorized navigation through web server file structures to expose sensitive files.
- Defending applications and data against CIA Triad compromises requires a combination of input validation, parameterization, strict access controls, and data sensitivity risk assessments.

Unit Essential Questions:

- How do encryption and access control enforcement (such as the principle of least privilege) protect sensitive data stored on endpoints and servers?
- How does failing to sanitize user input allow adversaries to execute injection attacks like SQLi, XSS, and directory traversal?
- How do low-level application flaws, such as buffer overflows, enable adversaries to disrupt availability or execute unauthorized code?
- How do secure coding practices and defensive controls work together to maintain the confidentiality, integrity, and availability of application data?

Knowledge and Skills:

Students will know...

- An adversary can read any unencrypted files if they have access to the device or drive storing the files.
- Computers have standard users and administrative users. Administrative users have access to control system settings and can typically access any files or applications on a system. If regular

users are given administrative privileges on a computer, and an adversary can compromise a user's account, then the adversary will have elevated privileges on the system.

- When access control settings are weakly configured, many users often have permission to view and sometimes even edit files on a system. Adversaries can take advantage of weak access control settings to steal or destroy files or disrupt an application.
- Applications are programs that run instructions on computers; they are executable data. Some applications run locally on a user's computer, while other applications, like web applications, run on a server and are accessed by users through a network.
- Many applications take user input through open-ended input fields where users can type characters (e.g., letters, numbers, punctuation). Developers should include user input checks in their application, such as numeric input when asked for a number of items, to ensure that the user input matches what is expected; the application should reject input outside of the expected parameters. This process of verifying that user input meets expected criteria before processing it is called data validation. Applications that fail to validate user input are vulnerable to injection-type attacks, where adversaries insert unexpected character strings in input fields to alter the behavior of a program.
- Structured query language (SQL) is a computer language used to request information from databases and make changes to databases or entries in databases. Applications that query a database using unvalidated or unsanitized input from users are vulnerable.
- An SQL-injection attack places SQL commands and control characters into a userinput field in an application, which can lead to a breach of confidentiality by causing the application to return more information than it should, or a breach of integrity by modifying or deleting data in the database.
- Websites are written using hypertext markup language (HTML), and many websites use Javascript to create dynamic content on websites or web applications. Because Javascript commands run in the browser of the user visiting the website, those commands can access sensitive data stored in the browser like usernames, passwords, and cryptographic keys.
- A cross site scripting (XSS) attack injects malicious code into a website that a user's browser then executes. The malicious code can be embedded in a link the user clicks (a Type I or Reflected XSS attack) or it can be inserted onto a website through a comment field, forum post, or visitor log, which would affect any user visiting that website (a Type II or Stored XSS attack).
- When applications take user input, that input is written to a buffer. A buffer is a designated section of computer memory with a fixed size. If the amount of data the user enters exceeds the size of the buffer, it can overflow into adjacent memory locations and overwrite other parts of the computer's memory.
- A buffer overflow attack feeds more data into memory than was allotted, which can cause a system to crash or to execute code outside the scope of a program's security policy, effectively allowing the adversary to perform unauthorized actions on a computer, such as accessing, modifying, or deleting files.
- The files that run web applications are stored in directories on servers. When users access web applications, their browsers send GET requests using hypertext transfer protocol (HTTP). A GET request accesses a file somewhere in the filesystem of the server.
- In a directory traversal attack, adversaries modify URLs and GET requests to attempt to access sensitive data (e.g., usernames and passwords) on a server's file system.
- Data security risks can involve a compromise of confidentiality when unauthorized persons can access sensitive data, integrity when data can be manipulated or altered from its intended state, and availability when data can be destroyed or encrypted to prevent others from accessing it.
- High risks from data vulnerabilities often involve highly sensitive data (e.g., data that is governed by laws or regulations) that could be compromised through a highly likely exploit.
- Moderate risks from data vulnerabilities often involve sensitive data not having strong enough encryption or strict enough access controls.

- Low risks from data vulnerabilities often involve less sensitive information being encrypted with shorter keys or having access controls that are not strict enough.

Students will be able to...

- Evaluate, with and without the support of AI, the likelihood and impact of risks.
- Document, with and without the support of AI, the likelihood and impact of risks.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 5B OVERVIEW

Content Area: Technology Education

Unit Title: Securing Applications and Data - Protecting Applications and Data: Managerial Controls and Access Controls

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: Data is the foundation of the digital world. Stealing, modifying, or denying access to data is often the end goal of an adversary. In this unit, students learn how organizations protect data by implementing security controls and policies that comply with legal and regulatory requirements for sensitive information such as personally identifiable information (PII), protected health information (PHI), and payment card information (PCI). Students will learn how data security depends on protecting data at rest, in transit, and in use through measures such as encryption, access controls, cryptography policies, and web application security standards. Students will learn how to implement and enforce appropriate access controls on files and directories.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
5.2.A Explain how the state or classification of data impacts the type and degree of security applied to that data.
5.2.B Identify managerial controls related to application and data security.
5.2.C Determine an appropriate access control model to protect applications and data.
5.2.D Configure access control settings on a Linux-based system.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Data must be protected across all three states (at rest, in transit, and in use), with organizations classifying sensitive assets, such as PII, PHI, and PCI, to satisfy legal frameworks and regulatory compliance standards.
- Cryptography policies specify approved encryption algorithms, key lengths, key generation, and key management lifecycle practices to safeguard stored and transmitted data from unauthorized exposure.
- Organizations enforce access boundaries and least privilege using formal access models, such as Role-Based (RBAC), Rule-Based (RuBAC), Discretionary (DAC), Mandatory (MAC), and security frameworks like Bell-LaPadula, to separate authentication from authorization.
- Operating systems enforce granular access controls using file permission bits; in Linux, permission triplets (read, write, execute across user, group, and others) are viewed with **ls -l** and modified with **chmod** to prevent unauthorized file access or execution.

Unit Essential Questions:

- How do data states (at rest, in transit, in use) and regulatory classification frameworks (PII, PHI, PCI-DSS) dictate specific encryption and compliance requirements?
- How do organizational cryptography and web application policies define baseline standards for key management, encryption algorithms, and vulnerability mitigation?
- How do different access control models (RBAC, RuBAC, DAC, MAC, and Bell-LaPadula) enforce the principle of least privilege to manage user authorization?
- How do Linux file permissions (read, write, execute for user/group/other) control access, and how do administrators inspect (**ls -l**) and enforce (**chmod**) them to secure system resources?

Knowledge and Skills:

Students will know...

- Organizations implement specific security controls to comply with legal requirements based on the types of data they collect, store, process, and transmit.
- Data can be classified by their state:
    - Data at rest are stored on a drive. It is important to protect the physical drive storing the data from destruction or theft. Data at rest can also be encrypted so that if an adversary steals it, they can't immediately read the data.
    - Data in transit are being sent from one device to another. If the data are being transferred over physical media (e.g., cables) it is important to protect the media. Data in transit can also be encrypted so that if an adversary intercepts it, they can't immediately read the data.
    - Data in use are being processed by software or a person. Access controls can be used to limit who or what has the ability to use data in different ways (e.g., view or edit). Data must be unencrypted to be used.
- Organizations often categorize data according to their sensitivity and prioritize a higher degree of security for more sensitive information.
- Laws and regulations can require certain types of data to be stored, transmitted, and handled according to specific rules.
    - Personally identifiable information (PII) is any data that allows someone to be identified and includes (but is not limited to): name, signature, phone number, address, biometric data (e.g., fingerprints), social security number, date of birth, and email address. The protection of this data is covered by many laws but most notably The Privacy Act of 1974 and for children under the age of 13 the Children's Online Privacy Protection Act of 1998.
    - Protected health information (PHI) is any data related to an individual's health, treatment, payment for healthcare at any time and includes (but is not limited to): test results, treatment records, hospital records, doctor visit notes, and health provider payment records. The protection of PHI is included in the Health Insurance Portability and Accountability Act of 1996.
    - Payment card information (PCI) is the data collected by organizations to process payments via cards (e.g., credit cards) and includes the following: name, account number, expiration date, address, and CVV code. The protection of this data is regulated by the Payment Card Industry Data Security Standard (PCI-DSS).
- Organizations that collect regulated data will label them and have policies that comply with the legal or regulatory requirements for the safe storage, transmission, and handling of these data.
- A cryptography policy will describe the acceptable encryption protocols and key parameters for an organization and may include:
    - A list of encryption algorithms approved for specific uses
    - Minimum or maximum key lengths
    - Cryptographic key-generation requirements and parameters
    - Cryptographic key-storage requirements
- A web application security policy will outline the requirements and parameters for testing and mitigating web application vulnerabilities in an organization, and it may include:
    - Parameters for when an application is subject to a security assessment
    - Timelines for remediating vulnerabilities based on level of risk
    - Parameters for how an application security assessment is to be carried out (e.g., using specific tools or according to specific frameworks)
- Access control enforces which users or applications (called subjects) can access, modify, add, or remove (called operations) which files or applications (called objects). Access control models describe how to determine which subjects have what type of access to which objects.

- Role-based access control (RBAC) assigns every subject to a role and defines which roles have which types of access to which objects.
- Rule-based access control (RuBAC) checks a set of rules to determine what type of access a subject should have for a specific object and then allows or denies types of access based on the rules. This access control model is typically layered on top of another access control model.
- Discretionary access control (DAC) gives individual subjects the ability to set the type of access that other subjects have on objects they own. In DAC models some subjects are designated as administrators or super users, and they have the ability to override the access controls established by other subjects.
- Mandatory access control (MAC) follows strict rules for which types of access each subject level has for objects that are above their level, at their level, or below their level. Subject and object levels are assigned by an external administrator.
- The Bell-LaPadula model is a MAC model that is often used by governments and military organizations to control the security of information. This model has the following two important properties:
    - The Simple Security Property states that subjects may not read objects that are above their level.
    - The * (Star) Security Property states that subjects may not write to objects below their level.

  These rules taken together are often summarized as "write up, read down" (WURD).
- The principle of least privilege is the idea that entities should be given exactly as much access as they need to perform their function and no more.
- Authorization is when an entity is granted permission to have a certain type of access to a resource. Access controls are put in place to control which users have what types of access to which data.
- There are three types of access to a file in Linux that can be set, and they always come in the following order:
    - Read access allows a user to view the contents of a file.
    - Write access allows a user to make changes to a file.
    - Execute access allows a user to run a binary file such as a program.

  These are abbreviated **rwx**, respectively. If a user only has read and execute permissions (not write), then it would display as **r-x**. The - symbol indicates the absence of that permission.
- There are three default entities for which permissions are set and always in this order: (1) the file owner, (2) the file group, and (3) all other users. The three sets are displayed with no spaces (e.g., **rwxrwxrwx**).
- To view the current permission settings for a file, use the command **ls -l** , which will show the current settings for the default entities. If there is a + symbol at the end of the permissions, this means that other permissions have been set for that file and it can be viewed with the **getfacl** command.
- To modify the permission settings for a file, use the **chmod** command. This command can be used with the numeric method or the symbolic method.
- To use **chmod** in the numeric method the syntax is **chmod ### filename**. Each of the three ### represents one of the three entities mentioned above (the owner, the group, other nongroup users).
    - The first # = the owner
    - The second # = the group
    - The third # = other nongroup users

  The permission for each entity is determined by adding up the values for the types of access to be granted:
    - 0 = no permissions
    - 1 = execute
    - 2 = write

    - 4 = read

  Therefore 3 sets permission to write and execute, 5 sets permission to read and execute, 6 sets permission to read and write, and 7 sets permission to read, write, and execute.
- To use **chmod** in the symbolic method the syntax is **chmod entity +(or –) permission filename**. The entities are the user owner, the group, and other nongroup users. Each entity is represented with a single letter.
    - u = user owner
    - g = group
    - o = others
    - a = all

  Permission can be either added or removed to any combination of entities.
    - + = add the permission
    - – = remove the permission

  The permissions that can be set are **read, write, and execute**.
    - r = read
    - w = write
    - x = execute

  Entities and permissions can be combined in a single command. To add the read and execute permissions for the group and user owner for a file called **testfile**, the command would be **chmod ug+rx testfile**.

Students will be able to...

- Evaluate, with and without the support of AI, the impact of protective risk-management strategies.
- Implement and log mitigations with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 5C OVERVIEW

Content Area: Technology Education

Unit Title: Securing Applications and Data - Protecting Stored Data with Cryptography

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: Data is the foundation of the digital world. In this unit, students learn how cryptography protects information by converting plaintext into unreadable ciphertext through encryption and restoring it through decryption using cryptographic algorithms and keys. Encryption methods can be symmetric, using the same key for encryption and decryption, or asymmetric, using separate keys, and they may process data as blocks or streams.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
5.3.A Explain how encryption can be used to protect files.
5.3.B Apply symmetric encryption algorithms to encrypt and decrypt data.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Cryptography transforms human-readable plaintext into unintelligible ciphertext using mathematical algorithms and secret keys to preserve confidentiality across storage and communication channels.
- The security of an encryption algorithm relies on the size of its keyspace, where larger keyspace dimensions exponentially increase the computational effort required for adversaries to execute successful brute-force key-guessing attacks.
- Encryption algorithms operate via two distinct key models: symmetric encryption (using a shared secret key for both operations) and asymmetric encryption (using mathematically linked public and private key pairs).
- Cryptographic systems process data using fixed-size chunks (block ciphers) or continuous data streams (stream ciphers), with the Advanced Encryption Standard (AES) serving as the modern industry benchmark across Wi-Fi, storage, and web security.

Unit Essential Questions:

- How do cryptographic algorithms and keyspace dimensions transform plaintext into ciphertext to prevent unauthorized data access?
- How do the operational mechanisms of symmetric encryption differ from asymmetric key management models?
- How do processing models (block vs. stream ciphers) dictate the efficiency and implementation of standards like AES?
- How do command-line tools (OpenSSL) and dedicated software utilities allow security teams to apply encryption keys to protect files and communications?

Knowledge and Skills:

Students will know...

- The purpose of cryptography is to hide information. A cryptographic algorithm defines a process for encrypting and decrypting information. Encryption is the process of hiding the information, and decryption is the process of reversing the encryption to retrieve the original information.
- An encryption algorithm defines a process for combining the information to be encrypted with a predefined key. The information to be encrypted is called the plaintext. The output of the encryption algorithm is called the ciphertext.
- The number of possible keys that can be used in an encryption algorithm is called the keyspace. The larger the keyspace, the longer it will take an adversary to discover the correct key by random chance.

- Cryptographic algorithms are classified by whether they use one key or two keys.
    - Symmetric encryption algorithms use the same key to encrypt and decrypt information.
    - Asymmetric encryption algorithms use two different keys—one to encrypt information and the other to decrypt information.
- Cryptographic algorithms are also classified by whether they process information one bit at a time or in fixed-size chunks of bits.
    - Block encryption handles information in fixed-size chunks called blocks, producing an output block for each input block.
    - Stream encryption handles input information continuously, producing output one element at a time.
- Computer-based encryption algorithms operate on binary data. The most common symmetric encryption algorithm is the Advanced Encryption Standard (AES). AES encryption is used to secure WiFi transmissions, internet browsing, file encryption on disks, and hardware-level encryption on processors.
- AES is a symmetric key block cipher that encrypts data in 128-bit blocks (16 bytes). AES can operate with keys of varying lengths. Longer keys produce more secure encryption but require more time to encrypt and decrypt.
- Symmetric encryption and decryption can be performed using the command line, specialized software, or web-based tools.
    - On a command line interface, users can encrypt or decrypt with OpenSSL.
    - Specialized software like AES Crypt is an open source tool that can encrypt and decrypt files.
    - There are many web-based tools for encrypting and decrypting files.
- Using OpenSSL in a CLI, a user can encrypt and decrypt a file using the following commands (note that the encryption key is derived from the password provided):
    - To encrypt a file named test with AES using a 128-bit key, use the command: **openssl enc -aes-128-cbc -e -in test -k password -out test.enc**
    - To decrypt the encrypted file using the same key, use the command: **openssl enc -aes-128-cbc -d -in test.enc -k password -out text**

Students will be able to...

- Identify security controls, and explain how they mitigate risks.
- Implement and log mitigations with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 5D OVERVIEW

Content Area: Technology Education

Unit Title: Securing Applications and Data - Asymmetric Cryptography

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: Data is the foundation of the digital world. In this unit, students learn how asymmetric encryption enables secure communication without a shared secret by using a key pair consisting of a public key, which is shared openly, and a private key, which must be kept secure. Students will focus on how data encrypted with a recipient's public key can only be decrypted with the corresponding private key, ensuring confidentiality and protecting communications. Students will learn the common asymmetric algorithms such as RSA and ECC provide strong security, with longer key lengths offering greater protection.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
5.4.A Determine the appropriate asymmetric key to use when sending or receiving encrypted data.
5.4.B Explain why the length of a key impacts the security of encrypted data.
5.4.C Apply asymmetric encryption algorithms to encrypt and decrypt data.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.
a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.
c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.
a. Interpret parts of an expression, such as terms, factors, and coefficients.
b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Asymmetric cryptography relies on mathematically inverse key pairs (public and private keys) to allow untrusted parties to securely communicate, encrypt data, and generate digital signatures without sharing secret keys in advance.
- An n-bit key yields a 2^n keyspace requiring an average of 2^{n-1} brute-force attempts. Security teams must balance longer key lengths against higher computational and processing overhead.
- Modern PKI implementations rely on core asymmetric algorithms like RSA and Elliptic Curve Cryptography (ECC) to power digital certificates, digital signatures, and secure key exchanges.
- Command-line utilities (such as OpenSSL) allow defenders to generate, store, and manage asymmetric key pairs and perform file-level encryption, where strict private key confidentiality remains critical to system security.

Unit Essential Questions:

- How do public and private key pairs work together mathematically to enable key exchange, confidential messaging, and digital signatures?
- How does key bit-length (n) dictate keyspace size (2^n), brute-force resistance (2^{n-1}), and computational performance tradeoffs?
- How do asymmetric algorithms (RSA, ECC) support infrastructure applications like digital certificates and Public Key Infrastructure (PKI)?
- How do administrators use utilities like OpenSSL to generate, manage, and safeguard asymmetric key pairs in operational environments?

Knowledge and Skills:

Students will know...

- Asymmetric encryption allows users to communicate securely without prearranging a shared secret key.
- When using asymmetric encryption, each entity that will be receiving data must first generate a key pair. Key pairs are binary strings of equal length that are generated at the same time through a mathematical process. One key is designated as the public key and the other as the private key. The keys are mathematical inverses of each other— each key reverses its partner. Either key can

be used to encrypt information, but only the other key in the key pair will then be able to decrypt it.

- Once the receiver generates the key pair, the private key must be stored securely. If the private key is exposed, shared, stolen, corrupted, or compromised the key pair must be deleted and a new key pair must be generated, because the security of the encryption algorithm rests on the security of the private key. The public key is published for anyone to view and use.
- To send information securely to someone, the sender will use the receiver's public key to encrypt the data and send it. Only the receiver who has the private key will be able to decrypt and read the information.
- Longer keys result in larger keyspaces. For binary keys, an n-bit length key has a keyspace of 2^n.
- Using an application to randomly guess an n-bit length encryption key means that on average an adversary will be able to guess the correct key in $2^n /2$ or 2^{n-1} guesses.
- Although longer keys are more secure, they also require more time to encrypt and decrypt messages.
- Computational processing power and efficiency continue to improve, allowing software to guess keys faster. Key-length recommendations for both symmetric and asymmetric encryption algorithms are periodically increased to account for increased processing power.
- Key-length comparison is only valid when comparing keys for the same cryptographic algorithm.
- Common asymmetric encryption algorithms include RSA and elliptic curve cryptography (ECC). Asymmetric algorithms are used in many applications, including digital signatures and digital certificates.
- As with symmetric encryption, asymmetric encryption and decryption can be performed using the command line, specialized software, or web-based tools.
    - On a command line interface, users can encrypt or decrypt with OpenSSL.
    - Specialized software like RSA Encryption Tool is an open source tool that can encrypt and decrypt files.
    - There are many web-based tools for encrypting and decrypting files.
- In a CLI, a user can generate an asymmetric key pair and encrypt or decrypt files as necessary.
    - To generate a 2048-bit RSA key pair and save the key to a file named **rsa.pem** use thecommand: **openssl genrsa -out rsa.pem 2048**
    - To extract the public key from **rsa.pem** into a file named **public.pem**, use the command: **openssl rsa -pubout -in rsa. pem -outform PEM -out public. pem**
    - To encrypt the file **test** using RSA encryption and the key file **public.pem**, use the command: **openssl pkeyutl -encrypt -pubin -inkey public.pem -in test -out test.enc**
    - To decrypt the **test.enc** file using the **rsa.pem** file, run the command: **openssl pkeyutl -decrypt -inkey rsa.pem -in test.enc -out test**

Students will be able to...

- Determine layered security controls that address vulnerabilities.
- Implement and log mitigations with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:
What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:
What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 5E OVERVIEW

Content Area: Technology Education

Unit Title: Securing Applications and Data - Protecting Applications

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students learn how Secure by Design is an approach that integrates security into every stage of product development by prioritizing customer security, transparency, accountability, and leadership commitment to security practices. Students will learn that developers also improve application security by validating and sanitizing user input to block malicious control characters and prevent attacks such as SQL injection, cross-site scripting (XSS), and directory traversal.

Approximate Length of Unit: 2 weeks

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
5.5.A Identify the application security principles of secure by design and security by default.
5.5.B Explain how user input sanitization protects applications.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:
ELA
L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.
a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.
b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Secure by design is an approach where security is integrated into every phase of product development rather than being added after systems are built.
- Organizations implementing secure by design take responsibility for customer security outcomes by designing products that meet users' security needs.
- Radical transparency and timely sharing of security updates and vulnerabilities strengthen overall system security for all users.
- Secure by default ensures that security features are enabled automatically so that systems and devices are protected out of the box without requiring user configuration.
- Validating and sanitizing user input by removing or rejecting control characters such as quotes and semicolons helps prevent attacks like SQL injection, XSS, and directory traversal.

Unit Essential Questions:

- How does the "secure by design" approach change the way organizations integrate security into the software development lifecycle?
- Why is it important for companies to take ownership of customer security outcomes when designing products?
- How does radical transparency and timely sharing of security updates improve overall cybersecurity for users and organizations?
- In what ways does building a security-focused organizational structure and leadership improve the effectiveness of secure by design practices?
- How do secure by default principles and input validation techniques, such as sanitizing control characters, help prevent attacks like SQL injection, XSS, and directory traversal?

Knowledge and Skills:

Students will know...

- Secure by design is an initiative that encourages companies to include security in all phases of product development including design. When organizations implement secure by design, security is a design principle not just a technical feature.
- Secure by design includes three design principles:
    - Companies should take ownership of customer security outcomes. Companies should build products that meet the security needs of their customers.

    - Companies should embrace radical transparency and accountability. Sharing relevant security-related product news and updates quickly increases security for everyone.
    - Companies should build organizational structure and leadership to implement secure by design. Companies need leaders who are focused on security and have a security-first posture.
- Secure by design includes the concept of secure by default, which is the idea that security features for software and devices should be enabled by default. Devices and software should be secure to use out of the box, with security features already enabled.
- When users enter input into an application, the application typically encases that input in special characters to process it. The characters that encase the user input are called control characters and include the single quote, the double quote, and the semicolon.
- When creating a program that takes user input, programmers should use a function to verify that user input meets their expected criteria and does not include any control characters that could be used to manipulate the system. This verification function can sanitize user input by removing potentially malicious characters, or it can give the user an error and force the user to provide different input. This can protect against many application attacks, including:
    - SQL injection attacks
    - XSS attacks
    - Directory traversal attacks

Students will be able to...

- Identify security controls, and explain how they mitigate risks.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login

UNIT 5F OVERVIEW

Content Area: Technology Education

Unit Title: Securing Applications and Data - Detecting Attacks on Data and Applications

Target Course/Grade Level: Advanced Placement Cybersecurity/Grades 10-12

Unit Summary: In this unit, students learn how devices and systems use logging and accounting to track data access and user activity, which can be analyzed to detect suspicious behavior such as unusual file access, abnormal usage patterns, or attempts to modify or steal sensitive data. Students will analyze detective controls like honeypots, cryptographic hash checks, and automated log analysis to help identify malicious activity, with real-time tools providing faster alerts while hash comparisons and log reviews often detect attacks after they occur. Students will know that organizations use tools like DLP systems and log monitoring to detect specific threats such as SQL injection, XSS, buffer overflows, and directory traversal attacks by identifying known malicious patterns in user input and system requests.

Approximate Length of Unit: 1 week

LEARNING TARGETS

NJ Student Learning Standards:
8.1.12.NI.2 Evaluate security measures to address various common security threats.
8.1.12.NI.3 Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4 Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.EC.1 Analyze controversial technological issues and determine the degree to which individuals, businesses, and governments have an ethical role in decisions that are made.

College Board Standards:
5.6.A Explain how to detect attacks on data.
5.6.B Determine controls for detecting attacks against applications or data.
5.6.C Evaluate the impact of a method for detecting attacks against an application or data.
5.6.D Identify whether a file has been altered by verifying its hash.
5.6.E Apply detection techniques to identify and report indicators of application attacks by analyzing log files.

Career Readiness, Life Literacies, and Key Skills:
9.3.IT.7 Perform standard computer backup and restore procedures to protect IT information.
9.3.IT.8 Recognize and analyze potential IT security threats to develop and maintain security requirements.
9.3.IT.10 Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

Interdisciplinary Connections and Standards:

ELA

L.KL.9–10.2 Apply knowledge of language to make effective choices for meaning, or style, and to comprehend more fully when reading, writing, speaking or listening.

a. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level.

b. Vary word choice and sentence structure to demonstrate an understanding of the influence of language.

c. Demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

RI.CI.9–10.2 Determine one or more central ideas of an informational text and analyze how it is developed and refined over the course of a text, including how it emerges and is shaped by specific details; provide an objective summary of the text.

RI.MF.9–10.6 Analyze, integrate, and evaluate multiple interpretations (e.g., charts, graphs, diagrams, videos) of a single text or text/s presented in different formats (visually, quantitatively) as well as in words in order to address a question or solve a problem.

W.WR.11–12.5 Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

Mathematics

A.SSE.A.1 Interpret expressions that represent a quantity in terms of its context.

a. Interpret parts of an expression, such as terms, factors, and coefficients.

b. Interpret complicated expressions by viewing one or more of their parts as a single entity.

A.SSE.A.2 Use the structure of an expression to identify ways to rewrite it.

Unit Understandings:

Students will understand that…

- Systems log user interactions and file access to establish behavioral baselines, allowing analysts to identify suspicious deviations such as abnormal file deletion, mass copying, or unauthorized access.
- Honeypots and hash verification act as accessible, high-yield detective controls. Honeypots provide zero-false-positive alerts for unauthorized access, while cryptographic hash comparisons verify file integrity and reveal unauthorized tampering over time.
- Choosing between retrospective hash auditing, honeypot traps, and advanced real-time Data Loss Prevention (DLP) systems requires evaluating asset criticality, data sensitivity, deployment costs, and automation capabilities.
- Specific application-layer exploit attempts, including SQL injection, XSS, buffer overflows, and directory traversal, leave distinctive string patterns, character anomalies, and length spikes in user input logs.

Unit Essential Questions:

- How do accounting logs and behavioral baselines help security teams identify compromised user accounts and unauthorized access attempts?
- Why are honeypots and cryptographic hash checks considered high-value, low-cost detective controls for identifying intrusions and file tampering?
- How do organizations balance deployment costs, asset sensitivity, and automation when choosing between real-time DLP tools and retrospective log analysis?
- How do specific attack signatures, such as input length anomalies or script syntax, appear in web server and database logs during application exploits?

Knowledge and Skills:

Students will know...

- Devices track and log when data are accessed and by whom. The process of recording and monitoring user activities is called accounting. Analysis of these logs can reveal malicious activity when an adversary attempts to access, copy, move, or delete data. Suspicious activity can include:
    - Accessing files that aren't typically accessed.
    - Accessing files or applications outside of a user's normal patterns (including time of day, location, and device type).
    - Attempts to delete or copy sensitive files.
- A honeypot is a file that appears as if it contains valuable data (e.g., credit card information, PII, passwords), but the data in the file are fake. A system can alert defenders if someone attempts to access the honeypot. Since the honeypot is a fake file, there is no legitimate reason to be accessing it, and any attempted access would be an indicator of malicious activity.
- Cryptographic hash functions can generate a digest for data and can reveal if data have been altered. If a file has changed unexpectedly, this can be a sign of malicious activity.
- Cost is a criterion in determining detective controls. Detective controls like honeypots and using hash values to check data integrity are inexpensive. Some organizations invest in third-party data loss prevention (DLP) services, which monitor data access, usage, and transmission by users throughout the organization to detect suspicious activity; DLP services provide strong detection capabilities at a higher cost.
- Sensitivity or criticality of data or applications is a criterion in determining detective controls. More sensitive or critical data or applications are more likely targets of an adversary and should be monitored more closely.
- Classification of data is a criterion in determining detective controls. Data that have been classified as private, educational, healthcare, or financial often have legal or regulatory detection and monitoring requirements.
- To operate at an effective speed, log analysis needs to be augmented with some automation. Honeypots offer near instantaneous detection capabilities.
- Some DLP tools, honeypots, and realtime automated log analysis provide alerts as an attack is happening. These tools allow for a prompt response that can stop an attack before it does more harm. Retrospective log analysis and the use of cryptographic hashes to verify data integrity identify attacks after they have occurred.
- False negatives can occur in applications and data attack detection. Cryptographic hash functions only detect if data have been altered. An adversary could view and steal data without altering it, and a cryptographic hash function would not detect this. Honeypots cannot detect adversaries that do not attempt to access them.
- Cryptographic hash functions can help identify changes in a file because they are repeatable: the same input always produces the same output for a given hash function.
- Hashes can be calculated using the command line on a computer, a website, or specialized software.
    - In Windows Powershell, if a user wanted to generate the SHA256 hash for a file named **testfile**, they would use the command: **Get-FileHash testfile -Algorithm SHA256**
    - In BASH the same could be accomplished with the command: **sha256sum testfile**
    - In zsh, the common command line terminal on Apple computers, this could be accomplished with the command: **shasum -a 256 testfil**e
- A file can be hashed and its hash output recorded. Then it can be hashed again later, and the second hash output can be compared to the previous hash output for the same file. If a file's hash changes, then the file was altered between when the first and second hashes were generated.
- SQL injection attacks can be detected by reviewing application and server logs of user input for SQL control words and symbols such as:

    - A single or double quote character: `` , `
    - Boolean conditions like OR 1=1
    - A double dash (which indicates a comment in SQL): --
    - SQL control words (always in capital letters) like **WHERE, IN, FROM**
- XSS attacks can be detected by reviewing user input for suspicious tags, particularly the **<script>.....</script>** tag.
- For web applications, buffer overflows can be detected by checking the amount of data the user is sending to the web application in their request. The fields commonly checked are the URL length, cookie length, query string length, and total request length. Long strings in any of these fields can be an indicator of an attempted buffer overflow attack.
- Directory traversal attacks can be detected by reviewing application and server logs. **HTTP GET** requests that include paths with sequences of ../ are indicators of an adversary attempting a directory traversal.

Students will be able to...

- Determine strategies and methods to detect attacks.
- Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.

EVIDENCE OF LEARNING

Assessment:

What evidence will be collected and deemed acceptable to show that students truly "understand"?

- End of Unit Common Assessment
- CodeHS.com activities
- Lesson exercises
- Class participation and discussions
- Case Studies
- AP College Board Practice Questionnaire

Learning Activities:

What differentiated learning experiences and instruction will enable all students to achieve the desired results?

- Teacher demonstrations over Screen Share software
- Scenarios Analysis
- Real World Case Studies
- Sharing ideas and classroom discussions
- Reinforcement worksheets and extra practice

RESOURCES

Teacher Resources:

- Demonstrations of worked out solutions from CodeHS.com
- Teacher designed worksheets
- CodeHS.com lesson exercises and videos
- College Board AP Classroom resources and Quizzes

Equipment Needed:

- Classroom Computers/Chromebooks
- Access to high speed internet
- AP Classroom College Board login
- CodeHS.com login