Lesson 2 - Outline

General Lesson Information

Title: Cyber Codenames: GPS Hacking

Overview/Annotation: This lesson focuses on GPS hacking in autonomous vehicles and its impact on cybersecurity. Students will explore GPS spoofing, remote takeovers, and countermeasures through an interactive game inspired by *Codenames*. The activity encourages critical thinking, teamwork, and real-world cybersecurity problem-solving.

Setting or format (outdoors, in groups, lab, etc.): Classroom or Lab

Intended group size (if groups are used): No more than 2-3 (if needed) for group discussion after live demonstration.

Intended grade level(s): 6th-12th

Approximate Time of Lesson: 50 Minutes

- Introduction of Codenames (10 minutes)
- In-class game (25 minutes)
- Discussion and questions (10 minutes)
- Wrap-up (5 minutes)

Researcher Biography

Name & Professional Title:

Research Assistants

- Kyla Crumpler, Undergraduate Research Assistant
- Mamade Conneh, Undergraduate Research Assistant

Advisors

- Sagar Dasgupta, Postdoctoral Fellow, Transportation Systems Engineering
- Mizan Rahman, Assistant Professor, Transportation Systems Engineering

Affiliation:
Connected and Automated Mobility Lab (CAM Lab) (https://mrahman.people.ua.edu/)
Department of Civil, Construction & Environmental Engineering
The University of Alabama

Contact Information:
mconneh@crimson.ua.edu(Mamade Conneh), kacrumpler@crimson.ua.edu (Kyla Crumpler), sdasgupta@ua.edu (Sagar Dasgupta), and mizan.rahman@ua.edu (Mizan Rahman),

Brief Description of Research Interests: Our research focuses on positioning, navigation, and timing (PNT) technology, cybersecurity of next-generation cyber-physical systems, and the transportation digital twin/multiverse. In effect, our interests lie in using an interdisciplinary approach to solving mobility challenges to revitalize our transportation system. The potential benefits of such research transcend the boundaries of social, economic, and environmental domains, which include reduced traffic congestion, delays, crashes, fuel use, emissions, and lowered monetary costs for transportation infrastructure.

Associated Standards and Objectives

Content Standards: *List Alabama Course of Study Standards that connect to lesson*

> CE350: Introduction to Transportation: The fundamentals of transportation, with a focus on roadway and traffic engineering. Key topics include transportation economics, planning, highway design, drainage, construction, traffic control devices, traffic operations, management, and highway capacity analysis.

Primary Learning Objectives:

Students will be able to

- identify and analyze different types of GPS hacking methods, such as GPS spoofing and remote takeovers.
- apply critical thinking and problem-solving skills to detect and prevent cyber threats in a game-based scenario.
- collaborate in teams to develop strategies for protecting autonomous vehicle systems from cyberattacks.
- reflect on real-world cybersecurity implications and discuss best practices for securing GPS-based systems.

Additional Learning Objectives: *N/A*

Preparation Information

Approximate Time of Lesson: 50 Minutes

- Introduction of Codenames (10 minutes)
- In-class game (25 minutes)
- Discussion and questions (10 minutes)
- Wrap-up (5 minutes)

Materials and Resources

- Game materials
- Projector for explaining the game presentation
- Speakers for clear audio during the video lesson

Technology Resources Needed:

Teacher**:**

- Projector for live demonstration
- Speakers for clear audio during the video lesson

Students**:**

N/A

Background and Preparation

Before teaching this lesson, both teachers and students should have a basic understanding of:

- GPS, Maps, and self-driving cars (lesson 1)
- GPS hacking (lesson 1)

Preparation Steps Before the Lesson

Teacher Preparation:

Research and familiarize yourself with real-world GPS hacking incidents (e.g., Tesla or military GPS spoofing cases).

Student Preparation:

Students should have prior knowledge of basic cybersecurity concepts (lesson 1), such as encryption and hacking methods.

Procedures and Activities

Engagement

Ask a question to connect with students' experiences:

- "What do you think would happen if someone hacked into a self-driving car's GPS?"
- "Have you ever used GPS and noticed it was inaccurate? What might cause that?"

Main activity

1. **Explain the Game Rules (5 minutes)**
   - Introduce Cyber Codenames: GPS Hackers, a modified version of Codenames.

2. **Explain the roles:**
   - Cybersecurity Team: Protects the GPS system from hacking threats.
   - Hacker Team: Tries to manipulate the GPS system for cyberattacks.
   - Neutral Words: Random cybersecurity-related terms that don't belong to either side.

- Fatal Exploit (Assassin Word): If a team chooses this, they immediately lose.
- Each team's spymaster will give one-word clues and a number (e.g., *"Satellite 2"* means two words related to satellites)

3. **Play the Game (15–20 minutes)**
   - Students will be divided into 2-3 groups and assigned roles
   - One student from each team is the spymaster, while others guess words
   - Teams take turns choosing words based on clues while avoiding enemy words and the Fatal Exploit
   - First team will identify all their words without hitting the Fatal Exploit wins.

- **Discussion Questions:**
  - "What were some strategies you used to give and interpret clues?"
  - "How does this game relate to real-world GPS hacking?"
  - "What are some ways cybersecurity experts can prevent GPS hacking?

Wrap up and Reflection

- *"What were some strategies you used to give and interpret clues?" (**Answer**: We looked for words that had a strong connection, like "Firewall" and "Encryption" when trying to protect GPS systems.)*
- *"How does this game relate to real-world GPS hacking?" (**Answer**: Hackers use techniques like GPS spoofing to trick navigation systems, while cybersecurity experts use encryption and monitoring to prevent attacks.)*

Final product/Summative evaluation

Options for evaluation:

- Kahoot/Quiz (Immediate Assessment)
- Questions about GPS functionality, spoofing, jamming, and security solutions.
- Short Written Reflection (Homework or Next Class Period)

Attachments

Not applicable