Lesson 3 – Outline

General Lesson Information

Title: Exploring GPS Cybersecurity: Hands-On Cyberattack Demonstration

Overview/Annotation: In this lesson, students will engage in a hands-on experiment to understand how GPS systems work and how cyberattacks can manipulate location data. Using a GPS-enabled device, a laptop, and cybersecurity tools, students will observe a live demonstration of GPS spoofing or jamming. They will discuss the attack's impact, real-world implications, and explore mitigation strategies. The lesson promotes critical thinking, teamwork, and cybersecurity awareness in transportation and technology.

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 hands-on activities (10 minutes)
- In-class live demonstration (20 minutes)
- Discussion and questions (15 minutes)
- Wrap-up (5 minutes)

Researcher Biography

Name & Professional Title:

Research Assistants

- Mamade Conneh, Undergraduate Research Assistant
- Kyla Crumpler, 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

- understand how GPS functions by examining a real GPS-enabled device and understanding its connection to satellites.
- observe and discuss real-time GPS signals using a computer and software that demonstrates how GPS data is transmitted and received.
- Observe how cyberattacks like spoofing and jamming manipulate GPS signals and impact location accuracy.
- identify real-world implications of GPS cyberattacks in transportation, aviation, and other critical industries.

Additional Learning Objectives: *N/A*

Preparation Information

Approximate Time of Lesson: 50 Minutes

- Introduction of hands-on activities (10 minutes)
- In-class live demonstration (20 minutes)
- Discussion and questions (15 minutes)
- Wrap-up (5 minutes)

Materials and Resources

- Computer or laptop with internet access

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

Technology Resources Needed:

Teacher**:**

- Computer or laptop with internet access
- Projector for live demonstration
- Speakers for clear audio during the video lesson

Students**:**

N/A

Background and Preparation

- Check laptop, GPS device, projector, and internet connection before class.
- Prepare a backup demonstration (e.g., video) in case of technical issues.
- Test all equipment
- Run a trial demonstration to ensure smooth execution.
- Remind students about the upcoming hands-on activity on Friday.

Procedures and Activities

Engagement

1. **Ask a question to connect with students' experiences:**
    - *"Have you ever used Google Maps or a GPS to find directions? What if it suddenly showed you in the wrong place?"*
    - *"What industries rely on GPS? What could happen if GPS data was wrong?"*
2. **Introducing today's lesson:**
    - Explain that students will witness a **real-time cyberattack** on a GPS device and explore ways to detect and prevent such attacks.
    - Briefly introduce the concept of **GPS spoofing and jamming** and how attackers can manipulate location data.
3. **Common misconceptions to address:**
    - *"GPS always provides accurate locations" → (Incorrect: GPS signals can be manipulated by cyberattacks.)*
    - *"Only military or government systems are targeted" → (Incorrect: Everyday devices like phones, cars, and ships are vulnerable.)*

Main Activity

- Demonstrate a working GPS device (5 minutes)
- Show a real GPS-enabled device (smartphone, GPS tracker).

- Display the live location on a projector/screen using mapping software.
- Introduce the cyberattack setup (5 minutes)
- Show the laptop with attack simulation software (preconfigured for demonstration).
- Explain how the attack manipulates GPS signals to show incorrect locations.
- Launch the attack and observe the effects (10 minutes)
- Run the GPS spoofing or jamming simulation.
- Ask students:
    - *"What do you notice about the GPS location?"* (Answer: The location changes unexpectedly.)
    - *"Does the device know it's under attack?"* (Answer: No, GPS receivers trust signals without verification.)
- Real-world connections (discussion, 10 minutes)
- Discuss the impacts of GPS cyberattacks in different industries:
    - Self-driving cars: Could be tricked into going the wrong way.
    - Aviation: Planes could be misdirected.
    - Military & Shipping: Unauthorized access to critical locations.
- Ask students:
    - *"How do you think GPS systems detect and prevent attacks?"*
    - *"What are the consequences of unreliable GPS data?"*

Wrap up and Reflection

Small Group Discussion (5 minutes)

- Students work in groups of 3-5 to brainstorm how GPS security can be improved.
- Each group presents one idea.

Reflection Questions:

- "What was the most surprising thing you learned today?"
- "Why is GPS cybersecurity important in transportation?"
- "How can we prevent or detect these attacks in real life?"

Common misconceptions to correct:

- "GPS devices can't be hacked" → (Incorrect: GPS receivers trust external signals without verification.)
- "Only advanced hackers can perform GPS attacks" → (Incorrect: Even small devices can simulate GPS spoofing.)

Final product/Summative evaluation

Options for evaluation:

- Kahoot/Quiz (Immediate Assessment – 5 minutes)

- Short written reflection (Homework or Next Class Period)

Attachments

Not applicable