Case Study with Supporting Media and Simulation Exercise

Securing Trains from Cyber Threats

Real World Inspiration

The Polish Radio Hack was an incident that occurred in 2023 when a threat actor disrupted more than 20 trains in Poland with a simple radio hack. By sending three tonal messages of 150.1 MHz directed at the trains, the attackers halted multiple trains. The affected railway agency claimed that the attack did not have the potential to harm anyone [1]. Other examples of cyber-attacks carried out on railway networks are those that occurred in the UK and New York. The attacks on the UK rail systems were caused by ransomware that was sent via email [2] . The attack on the New York Metropolitan Transportation Authority was from Chinese nationals, but the hackers did not gain any system access [3].

There are many vulnerabilities associated with the Polish Radio System. The RMF radio frequency is vulnerable since it is unencrypted and there was no authorization check, meaning that the sender and integrity of a message that the train receives cannot be guaranteed [1]. This violates the **Secure Information Architecture** CIE Principle, as we allow the manipulation of important data by using an unencrypted protocol. Trains trust all messages that they receive, which allows malicious actors to directly control the trains' actions. This could also lead to issues where attackers could disrupt currently sent messages to prevent them from being sent or change their intent.

These attacks were possible due to the insecure nature of the old radio protocol being used. To prevent these attacks from occurring we would recommend using AES-256 to encrypt the radio messages as this protocol is yet to be broken. Furthermore, when we are using the AES shared key, we must be able to authenticate our communications. For this, we recommend having the radio station to send a timestamp to our train with the respective message encrypted with the shared key between us and the station. This is to prevent replay attacks, as if an attacker intercepts a message, the timestamp will not match. If the train can decrypt this message and the timestamp is within a reasonable margin of error with the current time we can trust the respective radio command. We also recommend implementing a HMAC (Hash Message Authentication Code). This provides a way to verify the integrity of the message that we receive.

An example of more modern train controls are positive train controls that are currently being implemented in the United States. Positive train controls allow for the remote control of a train if it does not meet certain operating conditions. This system can prevent train-to-train collisions, overspeed derailments, incursions into established work zones and movement of a train through a switch in the improper position [4]. These communications are generally carried out via radio communication much like the trains in Poland. However, these radio communications are generally much more secure and implement encryption and authentication features like those listed above. Positive train controls (PTC) have many different implementations.

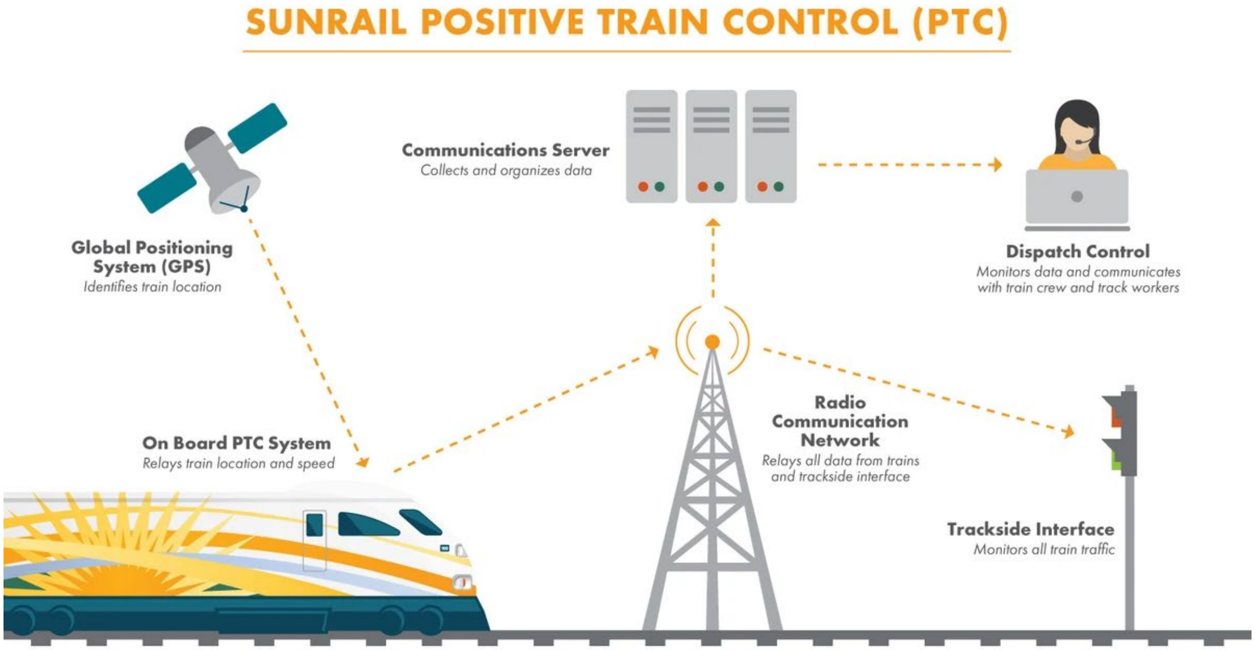
SUNRAIL POSITIVE TRAIN CONTROL (PTC)
Communications Server
Collects and organizes data
Global Positioning System (GPS)
Identifies train location
Dispatch Control
Monitors data and communicates with train crew and track workers
Radio Communication Network
Relays all data from trains and trackside interface
On Board PTC System
Relays train location and speed
Trackside Interface
Monitors all train traffic

Figure 1: “SunRail Positive Train Control Infographic”. ”SunRail.com" About SunRail Trains - SunRail

Kolli et al. Intheir the article, [5], provides some recommendations on positive train control security. They have presented a prototype distributed intrusion detection system (DIDS) to help keep these PTC systems secure. The DIDS lays out additional comprehensive protocols to help aid in preventing unauthorized or maliciously modified radio signals from reaching trains. The DIDS prototype can actively detect replay and forgery attacks and act against them as they occur [5]. This helps with our **Active Defenses,** as implementing the distributed intrusion detection system will allow us to see and respond to attacks as they occur.

To increase security, all train-related infrastructure should follow certain procedures. If radio protocols are used to control trains, they should have an up-to-date encryption protocol along with authentication measures. Employees who have computers that may be connected to networks that have data relating to train operations should also be given proper cybersecurity training. This will help prevent phishing attacks and malware (as seen in the San Fransico and the UK rail attack).

Media Feature for the General Audience

For a custom media clip designed by faculty and students of the University of Pittsburgh, please click on the video file found here: **[https://youtu.be/MH2EpfGkS6g]**

This video offers students a comprehensive introduction to essential engineering concepts surrounding transportation and railways. Additionally, it will help students understand the significance of simulation practice. Real-life examples in this video will highlight how engineering challenges and solutions are viewed by the public. This will help students connect classroom experiences to the real world. Navigating problem solving with an investigative approach will help students to understand principles between various engineering fields. This video should finally guide students to have a deeper understanding of how CIE principles are applied and visualized in practical scenarios, improving their implementation of it into complex cyber engineering systems. Understanding the narrative behind these core principles is crucial for recognizing their importance and application.

Future Policy Implications

The recent disruption of over 20 trains in Poland through a simple radio hack offers critical lessons for future cybersecurity policies in train systems. Adversaries used a basic method by sending three tonal messages at 150.1 MHz to target the trains, demonstrating that even straightforward attacks can cause significant operational disruptions. While this specific incident did not endanger lives, it underscores the vulnerability of critical infrastructure to cyber threats.

In response, train systems should enhance their monitoring and detection systems by implementing continuous monitoring of radio frequencies used in train operations and deploying advanced intrusion detection systems to identify unusual activities. Improving communication protocols is essential, focusing on transitioning to encrypted and authenticated channels to prevent unauthorized access and developing appropriate level of redundancy in systems to ensure resilience continued operation in case of primary system failure.

Stakeholder collaboration and training should be prioritized, fostering cross-industry partnerships and conducting regular cybersecurity drills for employees. Addressing the issue of legacy systems is crucial; train systems must prioritize upgrading of outdated infrastructure with modern, secure technologies and allocating resources to support these initiatives. Developing robust incident response plans and conducting regular security audits will ensure that security measures keep pace with evolving threats.

Given the complexity and volume of train equipment that needs protection, it is vital to adopt a systematic approach to cybersecurity. This involves categorizing assets based on their criticality and implementing tailored security measures for each category. For example, high-priority systems like signaling and communication networks should receive the most robust protections, including encryption and real-time monitoring. Additionally, integrating cybersecurity considerations into the design and procurement processes for new equipment can help mitigate risks from the outset. Regular maintenance and updates are essential to keep all systems resilient against emerging threats.

Stricter regulations and government support are necessary to enhance the cybersecurity posture of train systems. Addressing insider threats requires immediate revocation of access for departing employees and cultivating a culture of security awareness through regular training and audits. Finally, fostering closer collaboration between government agencies, private sector experts, and train system operators will enhance the sharing of best practices and improve overall security readiness. By implementing these measures, train systems can better protect against cyber threats and ensure the continued safety and reliability of rail transportation.

Part 1: Expand Your Understanding with the Following Exercise

(a) Hypothetical Scenario 1: You are a Lead Project Engineer overseeing the development of a new system intended to direct and control metro passenger trains. The system will control the speed and direction that each train travels, and there will be predetermined limits for the speed. The controls will be accessible by a human operator that is physically distant from the train. Because the system is designed to control trains and limit their speed, the operator has complete control over the train via the system.

a. What type of attack would this system be most vulnerable to?

b. Identify and explain the vulnerability that the attack in your previous answer would exploit.

c. What CIE principles could be applied to this system in order to remove the vulnerability that you have identified? In what way would they help?

(b) Hypothetical Scenario 2: You are a train operator for the New York Metro, which has recently implemented a new system used for controlling trains. They have implemented a positive train control (PTC) system which allows for train stoppage if an accident is likely to occur. This system has already stopped accidents by detecting possible derailments, collisions, work zone incursions and switches in the improper position. Since many of these communications are done via radio an attacker tries to find vulnerabilities inside these communications to cause damage.

a. Question 1: What could an attacker potentially do if they are able to exploit the PTC system that aims at preventing collisions.

b. Question 2 : What might the potential impacts be if an adversary is able to exploit the PTC system.

c. Question 3 : How might we be able to stop the adversary from exploiting the PTC system.

d. Question 4: What CIE principle is being covered by implementing an intrusion detection system?

Further Reading and Useful Public Video Links

For further reading, the following references would be suitable to explore at your convenience. [Provide the case study with several references. These references should be cited in the above dialog. The engineering convention is to use brackets for each reference in the text].

[1] Greenberg, Andy. “The Cheap Radio Hack That Disrupted Poland’s Railway System.” Wired, Conde Nast, 27 Aug. 2023, www.wired.com/story/poland-train-radio-stop-attack.

[2] Abrams, Lawrence. “UK Rail Network Merseyrail Likely Hit by Lockbit Ransomware.” BleepingComputer, 28 Apr. 2021, www.bleepingcomputer.com/news/security/uk-rail-network-merseyrail-likely-hit-by-lockbit-ransomware/. Accessed 6 July 2024.

[3] Goldbaum, Christina, and William K. Rashbaum. “The M.T.A. Is Breached by Hackers as Cyberattacks Surge.” The New York Times, 2 June 2021, www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html#:~:text=Hackers%20gained%20access%20specifically%20to%20systems%20used%20by. Accessed 6 July 2024.

[4] Federal Railroad Administration. (2022). Information Guide on positive train Control in 49 CFR Part 236, Subpart i. https://railroads.dot.gov/sites/fra.dot.gov/files/2022-12/2022_12%20PTC%20FAQs_final.pdf

[5] Kolli, S., Lilly, J., & Wijesekera, D. (2018, July 16). Positive Train Control Security: an Intrusion-Detection system to provide Cyber-Situational awareness. IEEE Journals & Magazine | IEEE Xplore. Retrieved July 14, 2024, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8411331

Authors

My name is Ken Barrett, and I am a rising senior at the University of Pittsburgh. I am currently studying computer science and mathematics and I have interests in AI and Cybersecurity.

My name is Alex Bennett, I am a Digital Media major at the University of Pittsburgh with a minor in Creative Writing and certificate in Broadcasting. Additionally, I work in radio and film production.

My name is Aditya Madupur and I am a rising junior at the University of Pittsburgh. I am studying neuroscince and am interested in exploring cybersecurity risks in various fields like healthcare.

My name is Cam Mickey and I am a rising senior at the University of Pittsburgh. I am currently studying Computer Science and Film and Media Studies.