Investigation on Cyberattacks on Signalling and Train Control Systems

Gaurav Sharma, De-Montfort University
Emad Sherif, De-Montfort University
Dr. Hongmei (Mary) He, De-Montfort University
Prof Eerke Boiten, De-Montfort University

PROJECT TIMELINE:

Start date: January/2022.
Finish date: June/2023.

INTRODUCTION:

The project, Cognitive and Socio-Technical Cyber Security for Modern Railway Systems (CoSTMoRS) is focusing on the cybersecurity of signalling and train control systems. The current task is to investigate the impact of classic cyber-attacks on the signalling and train control system and create the attack tree and kill chains.

AIM:

Highlight the impact of cyber-attacks on modern railway systems, especially the singling and train control system, and improve the awareness of cyber-attacks in railway industry.

WHY:

Smart railway initiatives bring many cyber risks to railways. The signalling and train control system is a safety-critical system that lies at the core of railway infrastructure. Threat agents' cyber-attacks on the railway infrastructure could have more severe implications, including danger to life.

METHODOLOGY:

The methodology is to execute cyber-attacks on the simulated environment on the cyber range.

- Design a minimal train control system
- Construct the system on cyber-range
- Simulate quay chain and DDoS attack.
- Analyse attack trees of classic attacks.
- Identification of critical threat intelligence.

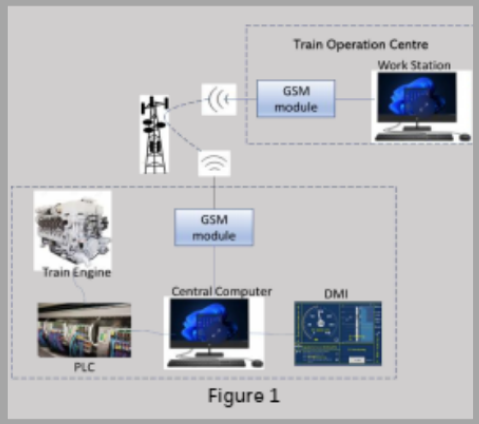

Figure 1

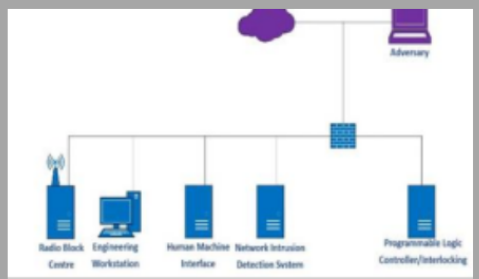

Figure: 2

EXPECTED IMPACT:

We expect demonstration on cyber range could enhance the awareness of cybersecurity in railway systems.

KEY OUTCOMES:

- The simulated cyber-attacks, e.g., Quay chain attack and DoS attack.
- The minimal signalling and train control systems on cyber range.
- The kill chain and attack trees of classic attacks on the system.
- Demonstration of the simulation.

MAJOR FINDINGS:

- How a DoS attack is spreading in the railway system;
- Which components are the most attackable.
- How attacks could affect the functionality of a railway system, and throughput and latency of the network.

USER PARTNERS:

National Cyber Security Centre, East-West Railway, Birmingham Centre of Railway Research and Education, COSTAIN, National Skills Academy, Global Vega Systems, Cerberus Security Lab.

ACKNOWLEDGMENT:

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1

PUBLICATIONS:

G. Sharma, E. Sherif, H. He and E. Boiten, "Investigation of Vulnerability in Signalling and Train Control Systems", IEEE International conferences on Interdisciplinary approaches in technology and management for social innovation (IATMSI-2022), to be submitted