Chapter 12

A SECURITY FRAMEWORK FOR RAILWAY SYSTEM DEPLOYMENTS

Raymond Chan

Abstract Railway systems are critical transportation infrastructure assets that must be protected from cyber attacks. However, deployments and upgrades of operational technology systems are always challenging due to the short timeframes available for maintenance. Specifically, there is insufficient time to test the safety and robustness of software updates and patches during railway system operation. Cyber security guidelines have been specified for the railway sector. However, the guidelines only mention the security requirements, not how they should be implemented in railway systems. This chapter proposes a security framework for railway system deployments. The framework can also be used as a reference for cyber security testing.

Keywords: Railway systems, cyber security, deployment

1. Introduction

Railway systems are critical transportation assets. The recent SolarWinds attacks demonstrate the vulnerabilities of the transportation infrastructure.

Although cyber security solutions are available, it is difficult to deploy them in operational railway systems. The principal challenge is the limited time available for maintaining and repairing railway systems. For example, they may not be enough time to test the safety and robustness of a software patch during operating hours. Also, when existing devices are upgraded and new devices are installed, concerns are raised about whether the deployments are secure and are not beset by human error.

This chapter proposes a security framework for railway system deployments. The framework can also be used as a reference for cyber security testing.

Published by Springer Nature Switzerland AG 2022
J. Staggs and S. Shenoi (Eds.): Critical Infrastructure Protection XV, IFIP AICT 636, pp. 247–253, 2022.
https://doi.org/10.1007/978-3-030-93511-5_12

2. Related Work

The CYRAIL Project [4] supported by the European Commission has released cyber security guidelines for the railway sector. The guidelines cover methodologies for adding new equipment and replacing old equipment while maintaining the safety and security levels. Also covered are deployment agreements established between suppliers and railway managers related to product security requirements and support for products over their lifetimes. However, no details are provided about implementing the security requirements in railway systems.

Wi-Fi jamming attacks pose significant risks to railway system deployments [8]. Since communications-based train control in a railway system operates at a similar frequency as normal Wi-Fi, the reliability of control signals decreases when many passengers attempt to connect to a Wi-Fi access point on a train. Indeed, a well-resourced attacker could leverage the Wi-Fi access point to connect to a train control system.

Researchers have demonstrated that similar techniques have been used to access elevator control systems [3]. Gransart et al. [6] and Frangie et al. [5] discuss threats to railway systems that leverage wireless communications. Alguliyev et al. [2], Huq et al. [7] and Thaduri et al. [10] discuss various threats to railway systems.

Unfortunately, the trend in transportation systems, including railway systems, is to incorporate smart devices that rely on wireless communications [9]. However, few, if any, studies address the concerns raised by deploying such devices in railway systems.

3. Security Framework

This section describes the proposed security framework for railway system deployments. The framework has four phases: (i) procurement phase, (ii) testing phase, (iii) deployment phase and (iv) post-deployment phase.

3.1 Procurement Phase

The procurement phase is the important first phase of the deployment framework. During this phase, vendors are selected and checks are made to identify and mitigate security issues. Railway system operators must conduct the following analyses to ensure that railway systems and devices meet the security requirements:

- **Supply Chain Analysis:** A railway system operator should verify the provenance and trust levels of the procured systems and devices. The operator should maintain a trusted vendors list and

perform annual auditing to ensure that vendors adhere to the security requirements. The costs of products and services should factor in the decision making, but security should have higher priority. The systems should be maintained and supported by trusted local service teams where possible because it difficult to guarantee 24/7 support by remote, let alone, overseas personnel.

- **Product Lifecycle Analysis:** A railway system operator should ensure that systems and devices are supported by vendors and maintained and replaced by service providers over their lifecycles. Vendors should continue to support their products for at least ten years. Service providers should provide security patches and updates to ensure that applications are secure.

- **Security Requirements Analysis:** A railway system operator should develop security requirements before procuring products. Since railway systems are typically regulated by government agencies, all systems and devices should be procured by issuing tenders to ensure transparency. Bids should not be accepted unless the vendors and service providers satisfy all the security requirements considered in the supply chain analysis and product lifecycle analysis.

  The CYRAIL Project [4] has identified the following security requirements for railway systems:

  - *Personnel Requirements:* Requirements must be imposed on the personnel involved in operating railway automation and telemechanical systems and devices. A railway operator must collect requirements from the stakeholders involved in developing, administering and operating the railway system. Additional security requirements should be solicited from cyber security experts.
  - *Physical Protection Requirements:* Systems and devices must be isolated and protected from access by unauthorized staff and passengers. The physical protection requirements should include video monitoring, physical locks and alarms, and periodic checks by staff.
  - *Access Management Requirements:* Access to operational technology systems must be managed securely and effectively to prevent misuse and mitigate human error. A railway operator must define system access rights for all personnel and ensure that the rights are managed and controlled properly.

- *Data Protection Requirements:* A railway system has to collect large quantities of data for regulatory and analytic purposes. Data collection, access, dissemination and retention must follow the applicable government and industry data protection requirements. The requirements should be considered carefully during the procurement phase.
- *Software Requirements:* Software must be compatible in existing and new operating environments. Software must be supported by vendors and updates and patches provided regularly for at least ten years.
- *Intrusion Detection Requirements:* Adequate measures must be taken to detect and alert to cyber attacks. Data related to railway system operation and potential anomalies and attacks should be archived and secured, and passed promptly to relevant personnel and organizations.
- *Incident Response Requirements:* Requirements for effective incident response, especially incident analysis and mitigation activities, must be specified to reduce risk and negative impacts to railway system operations.
- *Reliability Requirements:* Reliability requirements must be imposed on systems and devices to ensure reliable operation over their lifecycles.

3.2 Testing Phase

Activities during the testing phase ensure that newly-installed systems and devices interoperate seamlessly in the operational environment. Although testing can be conducted using an experimental testbed or simulated environment, it is important to ensure that the testing environment models the operational environment with high fidelity to provide assurance.

The following activities should be conducted during the testing phase:

- **Vulnerability Assessment and Penetration Testing:** Vulnerability assessments and penetration tests are routinely conducted for information technology systems. To enhance reliability and resilience and reduce operational risk, the assessments and tests should be performed for information and operational technology assets in railway systems.
- **Simulation and Digital Twin Testing:** It may not be possible to test a new system or device in an operational environment

before their deployment. In such cases, a high-fidelity simulation or digital twin should be used for testing. The tests should be performed in an integrated environment with and without the new system or device.

3.3 Deployment Phase

In a railway system, the timeframe for deployment and maintenance may be only a few hours starting at midnight. The following activities must be performed during the deployment phase:

- **Security Deployment Checklist:** Security deployment checks must be conducted to verify the configurations and settings of systems and devices. If the time required for deployment is more than the maintenance timeframe, the checklist should include the configurations and settings that must be verified every time the checks are conducted.
- **Rollback Procedure:** A rollback procedure must be performed to stop a deployment and return the system to the previous state if the deployment cannot be completed within the maintenance timeframe. The rollback procedure should also verify that the system is working properly after the rollback.
- **Deployment Verification:** Deployment verification checks that a deployment has been completed and the newly-installed system or device is working as expected. Deployment verification should also use the security deployment checklist to ensure that the configurations and settings are correct.

3.4 Post-Deployment Phase

During the post-deployment phase, a railway operator should perform the appropriate procedures for maintaining and monitoring the systems and devices:

- **Patch and Upgrade Procedure:** This procedure includes the testing and deployment phase activities to ensure that the patch or update does not affect system functionality and reliability. The patch and upgrade procedure may require an additional deployment to address follow-up actions.
- **Drill Procedure:** Drills must be conducted periodically in the experimental and production environments during the maintenance timeframe, if possible. The drills must be performed after new

systems and devices are deployed, patched or upgraded. They should also simulate intruder attacks and the operator should be able to react appropriately to the simulated attacks and mitigate the impacts on the railway system.

- **Monitoring and Open-Source Intelligence Workflow:** A railway operator must implement standard operating procedures to react to security alerts and security incidents. A decision to apply a quick fix and monitor system behavior must be made before a patch is deployed.

4. Conclusions

Railway systems are critical transportation infrastructure assets that must be protected from cyber attacks. The security framework for railway system deployments presented in this chapter covers activities that must be performed during the procurement, testing, deployment and post-deployment phases of systems and devices. The framework also serves as a reference for cyber security testing.

The security framework was intended to be applied to transportation systems operated by the Singapore Land Transport Authority (LTA) and Mass Rapid Transit (SMRT), but discussions were suspended due to the COVID-19 pandemic and may resume in the near future.

Future research will extend the work to apply continuous integration and delivery concepts in software development to railway systems. Additionally, research will attempt to apply modified versions of the security framework to deployments of other critical infrastructure assets such as building management systems and industrial control systems.

References

[1] Acute Market Reports, Railway Signaling Systems Market Size, Market Share, Application Analysis, Regional Outlook, Growth Trends, Key Players, Competitive Strategies and Forecasts, 2020 to 2028, Report ID: 5232539, New York, 2020.

[2] R. Alguliyev, Y. Imamverdiyev and L. Sukhostat, Cyber-physical systems and their security issues, *Computers in Industry*, vol. 100, pp. 212–223, 2018.

[3] R. Chan and K. Chow, Threat analysis of an elevator control system, in *Critical Infrastructure Protection XI*, M. Rice and S. Shenoi (Eds.), Springer, Cham, Switzerland, pp. 175–192, 2017.

[4] CYRAIL Project, Cybersecurity in the Railway Sector, Evoleo Technologies, Maia, Portugal (`cyrail.eu`), 2017.

[5] R. Frangie, A. Mihalic, T. Chehab, J. Kan, C. Luk and S. Perinpacumarasamy, Smart railways ... or not so smart: A cyber security perspective, *Proceedings of the Conference on Railway Excellence*, pp. 230–239, 2018.

[6] C. Gransart, V. Deniau, E. Simon, A. Fleury, S. Lecoeuche, P. Millot and E. Masson, Cyber security of the railway wireless system: Detection, decision and human-in-the-loop, *Proceedings of the Seventh Transport Research Arena*, 2018.

[7] N. Huq, R. Vosseler and M. Swimmer, Cyberattacks Against Intelligent Transportation Systems, TrendLabs, Trend Micro, Tokyo, Japan, 2017.

[8] S. Lakshminarayana, J. Karachiwala, S. Chang, G. Revadigar, S. Kumar, D. Yau and Y. Hu, Signal jamming attacks against communications-based train control: Attack impacts and countermeasures, *Proceedings of the Eleventh ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 160–171, 2018.

[9] P. Radanliev, D. De Roure, J. Nurse, R. Nicolescu, M. Huth, S. Cannady and R. Mantilla Montalvo, New Developments in Cyber Physical Systems, the Internet of Things and the Digital Economy – Discussion on Future Developments in the Industrial Internet of Things and Industry 4.0, Unpublished Manuscript (`www.preprints.org/manuscript/201903.0094/v1`), 2019.

[10] A. Thaduri, M. Aljumaili, R. Kour and R. Karim, Cybersecurity for e-maintenance in the railway infrastructure: Risks and consequences, *International Journal of System Assurance Engineering and Management*, vol. 10(2), pp. 149–159, 2019.