CYbersecurity in the RAILway Sector

A use-case for applying MILS through network separation in critical infrastructure

MILS Workshop 2018
2018-06-25, Luxembourg

Markus Engqvist and Staffan Persson
atsec Information Security AB and the CYRail consortium

CYRail consortium

Evoleo Technologies LDA (Portugal), Euskoiker (Spain), FORTISS GMBH (Germany), International Union of Railways (France), Airbus Defence & Space (France), atsec Information Security AB (Sweden).

Funding

CYRail has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No. 730843.

Summary

A presentation of the CYRail project and MILS in rail infrastructure.

1. INTRODUCTION

Railway infrastructures are moving towards more intelligent, connected, user-centric and collaborative systems. The current developments within railway focus on providing more services to passengers. Examples are on-board entertainment, real-time schedules and tools to plan trips using intermodal transports. While these developments bring many advantages for the industry and its users, they also present new opportunities for cyber-criminals and terrorists.

Cybersecurity in the railway sector (CYRail) is a project within Shift2Rail. The CYRail project is identifying not only the IT security risks, but also appropriate methods for addressing them, including specifications and recommendations for secure modern rail systems design and operation. The scope of the project is limited to focus only on cybersecurity.

2. CYRAIL PROJECT

The project is structured into Work Packages (WPs) that each deal with one part of the cybersecurity chain. We (atsec) are in charge of the last deliverable and the project will finish in October 2018. The WPs are arranged as follows:

- **WP1 – Project management**
  Overall coordination and management, establishing internal communication tools and procedures.
- **WP2 – Operational context and scenarios**
  The initial requirements for the railway and a realistic railway scenario are defined. This scenario is then used as the basis for the rest of the project.
- **WP3 – Security assessment**
  Specifying a security assessment methodology, defining security zones and vulnerabilities in the scenario, and performing risk assessment.
- **WP4 – Threat analysis, attack detection and early warning**
  Identifying threats, specifying attack detection solutions and incident management.
- **WP5 – Mitigation and Countermeasures Specification**
  Specification of mitigation strategies and countermeasures based on the security assessment. Definition of resilience mechanisms.
- **WP6 – Protection profiles**
  Developing a modular Protection Profile for network devices that provides network separation using the MILS approach.
- **WP7 – Dissemination and Outreach**
  Such as establishing a web site, presenting the project at conferences (such as this one).

Specific advantages with the CYRail approach:

- The project has branch specific competence from the railway sector. This means that we know that the threats and the operational scenarios are realistic. This means we know the operational environment and the problems we have to solve.
- The project has good security specific competence, e.g. MILS or Common Criteria competence. This means that we know how the threats could be addressed by MILS principles and specified as requirements in a Protection Profile.
- We are focused on using industry standards that would allow us to use more standard components and competences from other industries. The problem we are facing for railways are not expected to be unique. This also means that market for security solutions may not be limited to the railway sector only.

- We are do not want to invent everything ourselves, but have been looking for other, similar approaches taken by others. This means that we have focused on what is critical for the railways and that we have not been able to find elsewhere.
- The result of WP6 that atsec is responsible for will be publicly available and we hope others will continue our work.

2.1 PROJECT WORKFLOW

The project implements a top-down approach throughout and the WPs build directly onto each other. The WPs also make use of different sources of input, which help support this wholistic approach. A complete railway system is considered for the project.

The security requirements and railway scenario of WP2 mostly makes use of internal railway expertise within the consortium. The WP3 is based on standards, mainly ISA/IEC 62443 and ETSI with the TVRA model (Which in turn is based on Common Criteria). For ISA/IEC 62443, the 62443-3 documents are used, as they target systems. WP4 makes use of previous security incidents, along with state-of-the-art threat detection and incident management expertise. WP5 then uses the earlier results to apply appropriate countermeasures and mitigate security risks. This is based on internal expertise and state-of-the-art industry developments. The NIST SP-800 standards are used throughout the project, e.g. to define security concepts. Finally, WP6 makes use of ISO 15408 Common Criteria. As the WPs are connected, the standards used in earlier WPs are also important later in the project, i.e. ISA/IEC 62443.

This connected structure, building heavily on industry standards, increases the applicability of the project and helps ensure that the focus of the project does not become too narrow. We desire common requirements between different sectors if possible, as not to cause any unnecessary fragmentation. Also, having these chained WPs enables traceability all the way from the identification of vulnerabilities to the specification of countermeasures.

3. MILS APPROACH

To build secure large infrastructures, such as the one used by the railway, we need a security architecture. In an ideal situation it is built using secure and well-designed components that supports the overall security architecture. Unfortunately, this is not really the case or even possible to achieve. Many components of the systems may be single-purpose or legacy products that cannot protect themselves. Nor can the components be replaced without significant cost and effort. The current development in railway with interconnectivity and new services will then lead to an increased attack surface. To mitigate threats, these components need to be isolated from possible attackers.

The CYRail project therefore presents two approaches for addressing security in these situations. One approach is to build a MILS architecture that enables separation and isolation of systems and components. The other is to support an architecture that enables efficient and secure monitoring and management. These solutions are part of WP5 and WP6. However, arriving at such conclusions and specifying them accurately is not feasible to do without performing the earlier work.

Systems that handle information of different security criticality must be separated into different security zones. This is specified in the ISA/IEC 62443 standard. Such zones require separation measures, and the conduits between them require information flow control. However, zones within a railway infrastructure are not single devices but can involve big systems that are distributed over large areas. These zones or systems therefore require further measures than only platform-based MILS (i.e. separation kernels). This means that we require a MILS concept on the network level, where separation can be performed for large systems and infrastructures. While platform-based MILS is useful in the railway, there is already ongoing

work in this area (i.e. certMILS). This was one of the reasons that we did not write a Protection Profile for separation kernels, to avoid having two conflicting Protection Profiles. Instead, the CYRail project suggests MILS as a general approach, but the Protection Profile will focus on network separation.

4. PROTECTION PROFILE

In the last work package (WP6) we are writing a Protection Profile for devices that provides network separation. The Protection Profile will be a modular Protection Profile, with a PP-base and a number of PP-modules each addressing different types of network separation.

The goal of the Protection Profile is to specify requirements for a device that allows for implementation of the above described approaches. Mainly, it will support the implementation of a MILS architecture on the network level. Products compliant with the Protection Profile can be used in infrastructure to ensure security, especially for legacy/unprotected systems and untrusted devices. We have chosen the assurance package EAL4 for the PP.

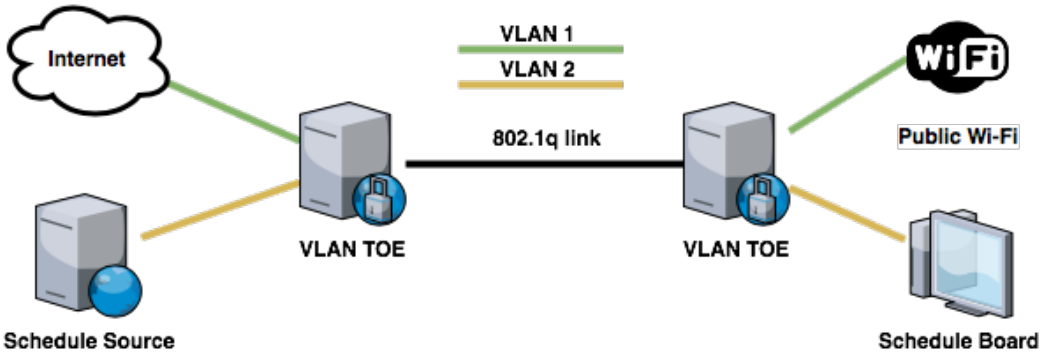
The PP is the final deliverable of the project. This is as it will make use of all the previous WPs and help to summarize the project. The common thread through the earlier WPs will help in compiling the assumptions, threats and objectives for the PP. This also helps ensure the PP will be applicable to real world scenarios.

5. SEPARATION USE CASES

Being a theoretical research project, the results of do not specify exactly how the mitigations of the threats, including the MILS approach, should be implemented. Presented below are possible use cases to help visualise the possible applications for logical separation of network traffic. The technologies are positioned at different abstraction levels of the network stack and will therefore be applicable in different situations.

Example 1 – Virtual LAN

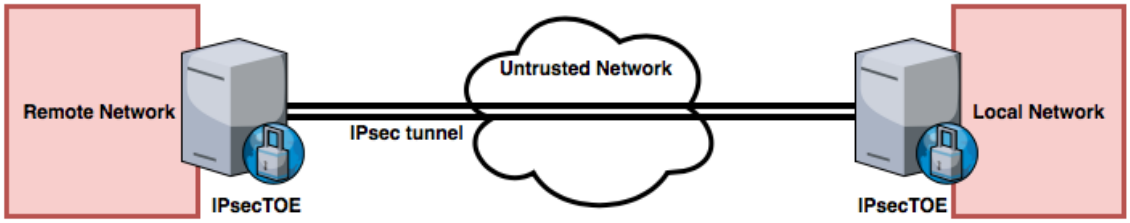
Virtual LANs (VLAN) are used to separate traffic at a lower level, meaning that the separation will not impact most applications or services. While traffic transmitted through the device is separated, VLANs provide no protection against attackers who have access to the physical network infrastructure. It should not be used as the only protection for critical applications. In the example below, two potentially untrusted services are separated to avoid interference.



Example 2 – Virtual Private Networks

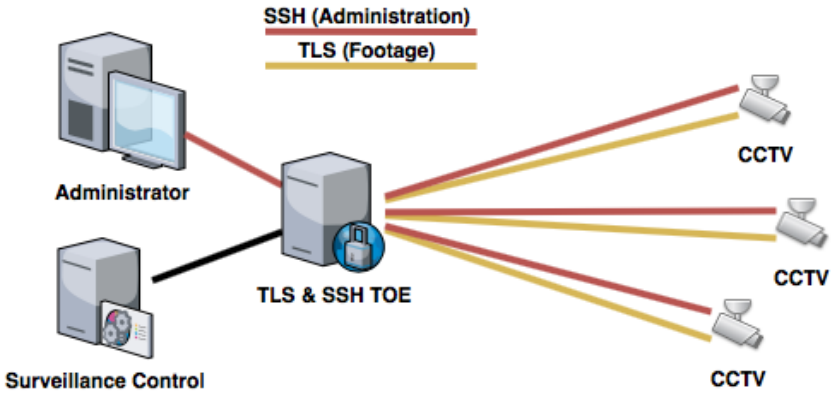
Virtual Private Networks (VPN) are used to connect two remote networks over potentially untrusted intermediary networks (i.e. the internet). In addition to separating the traffic flow, this mechanism will

also isolate traffic between two endpoints within a cryptographically secure tunnel. In the example below, a remote control center is connected to a local network over the internet.



Example 3 – Trusted Channels

Trusted Channels will be established on the higher levels of the network stack. They will be used to protect traffic between two applications over an exposed network. These channels can be used in different ways thanks to their independence to the underlying infrastructure. One example, as visualized below, is the traffic between CCTV cameras and a control server. Should footage be transferred over a wireless network, there may be no guarantee that an attacker cannot listen to the traffic. As such, the transmitted footage should be protected from the rest of the network.



6. FUTURE WORK

Our focus was to identify and address the cyber security issues for railway operators, but we know that both the security problems as well as the solutions are not unique to railway operators. This means that we have tried to use methodologies and solutions that are general available. The goal is that since the issue for separation is also present in other sectors, the PP and the results may also be applicable there. We desire a large userbase for the PP. Hopefully, this work will also increase the security awareness within the industry and provide ways for new organizations/industries to make use of ISO 15408.

A goal for the future would be to further establish these kinds of requirements for separation within the CC standard. During the work, we have looked towards the Network Device cPP for inspiration of our Base-PP. A suggestion would be to create similar additions detailing separation mechanisms, as we have seen that this is a need not only in rail but other sectors as well. Building upon already established work, such as the Network Device cPP, will help counteract fragmentation of security requirements or certification.

7. CONCLUSION

During the work we studied other sectors to determine if the issues identified within CYRail are shared between sectors. It was recognized that not only were the problems similar or identical, but often also the same solutions were proposed. We have also seen the importance of using existing standards. The

usage of standards within the CYRail project has enabled the project to focus on actually solving the problems. We believe that the usage of these standards may also lead to a wider applicability of the results.

Finally, we have seen within CYRail the necessity of different competencies and different backgrounds. This results in being able to address the actual problems by identifying appropriate solutions. Work performed may be subject to further discussion or explanations. This leads to higher quality of the results, as certain topics or discussions could otherwise be overlooked.