Methodology for a Security Audit of ERTMS

Robert Stroud
Adelard LLP
London, United Kingdom
rjs@adelard.com

Ilir Gashi
Centre for Software Reliability
City University London
London, United Kingdom
i.gashi@csr.city.ac.uk

Abstract—**In this paper we discuss the methodology we used for a security audit of the European Railway Traffic Management System (ERTMS) specifications. ERTMS is a major industrial project that aims at replacing the many different national train control and command systems in Europe. We discuss the stages of the audit, threat model used, and the output of each stage of the audit.**

Keywords: security review; security audit; ERTMS; safety-critical systems.

I. BACKGROUND

This paper reports on the methodology we used for a security audit of the European Railway Traffic Management System (ERTMS) specifications that was commissioned on behalf of key UK railway stakeholders and UK government. ERTMS is a major industrial project that aims at replacing the many different national train control and command systems in Europe with a standardised system and consists of two major components:

- ETCS, the European Train Control System, is a train control and automatic train protection system (ATP) to replace the existing national systems;
- GSM-R, a radio system for providing voice and data communication between the track and the train, using Global System for Mobile Communications (GSM) technology over frequencies reserved for railway use.

The ERTMS/ETCS System Requirements Specification [1] provides a technical specification of the overall system.

Network Rail, the authority responsible for the UK's rail network, are preparing to introduce ETCS and GSM-R as part of an upgrade of the signalling and communications systems running on Britain's rail infrastructure.

Within the rail industry, safety has always been paramount, but security has not always been considered. However, this upgrade has the potential to increase the risk of an electronic attack on the rail infrastructure, as it brings more systems under centralised control. The purpose of our security audit was to identify potential vulnerabilities and attack scenarios and suggest mitigations.

ERTMS is implemented using a number of trackside and on-board sub-systems, and the ERTMS/ETCS specifications describe the interfaces by which these various sub-systems interact.

In the next section of this paper, we discuss our methodology for performing the security audit to identify vulnerabilities and our use of attack scenarios to assess the impact of these vulnerabilities. However, we do not provide specific details of vulnerabilities or attack scenarios, which can be found in our detailed reports [2], [3].

We stress that the vulnerabilities we identified are vulnerabilities in the interoperability specifications rather than an actual implementation of ERTMS. There are many aspects of ERTMS security that depend on details of the national implementation of ERTMS, and it would be valuable to explore these issues in more detail in the future.

II. REVIEW METHODOLOGY

The ERTMS/ETCS safety analysis [4] considers the specifications from a safety perspective to derive the safety requirements for technical interoperability. A review from a security perspective needs to consider a rather different set of potential threats and undesirable consequences.

A security analysis usually considers threats to confidentiality, integrity, and availability, but here we are concerned with train movements rather than the security of data, so our primary concern is integrity, then availability, and finally confidentiality. Loss of integrity could result in accidents or collisions, whereas loss of availability would bring the system to a halt. Loss of confidentiality is less of an immediate threat, but might result in the leak of sensitive operational information. Finally, reliability is also important, since an unreliable train service will result in a loss of public confidence in the railway operators.

Thus, the hazards or potential failures or undesirable outcomes that ERTMS should avoid are the following:

- a collision involving multiple trains;
- an accident such as derailment involving a single train;
- widespread disruption of train service over a large area;
- disruption to individual trains, or trains in a local area;
- creation of a situation that leads to panic and potential loss of life (e.g., an emergency stop and uncontrolled evacuation onto the track);
- creation of a situation that leads to passenger discomfort and dissatisfaction, (e.g., stopping a train indefinitely in a tunnel);
- loss of public confidence in the railway system due to intermittent low-level problems affecting the reliability of the service;
- leak of sensitive information (e.g., movements of VIPs).

A security analysis also needs to consider the capabilities of the attacker. It is usual to make a distinction between an

insider and an outsider, in other words, someone with legitimate access to a system who abuses their position and privileges, either willingly or under duress, as opposed to someone outside the system with limited access, who seeks to break into the system out of curiosity, malice, or for personal gain. Historically, railway systems have relied on highly specialised, proprietary technology, and there has been a relatively small community with the necessary knowledge to exploit vulnerabilities. However, the widespread adoption of open standards like ERTMS/ETCS that are designed to promote interoperability and the commoditisation of technology could make both the necessary knowledge and the necessary tools more readily available to potential attackers.

The key points we addressed in our security analysis were whether ERTMS/ETCS:

- introduces any new vulnerabilities or threats to the railway infrastructure;
- makes it easier to compromise the system;
- shifts the balance between the potential for abuse and the likelihood of being detected.

Our approach to the security analysis was to consider the context in which ERTMS/ETCS operates, and its trust relationships with other systems. ERTMS/ETCS is implemented using a number of trackside and on board sub-systems, and the ERTMS/ETCS specifications describe the interfaces by which these various sub-systems interact, and how the ERTMS/ETCS application responds to messages via these interfaces and ensures that trains move safely.

In our security analysis we considered:

- whether there are safeguards built into the system that protect against messages being corrupted in transmission by the input channel;
- whether these safeguards protect against all possible threats to the input channel (for example, deliberate attacks on the channel, as opposed to random failures);
- whether the source of the input is trustworthy, or whether it is possible for the input source to have been compromised;
- whether there is adequate protection at the application level to guard against malicious messages generated by an attacker who controls the input source.

With this approach in mind, we performed a systematic security audit of the ERTMS/ETCS specifications by examining the ERTMS/ETCS application itself, and considering its interfaces and trust relationships with other components of the ERTMS/ETCS system, both trackside and on board the train. We approached the problem using both a top down and a bottom up methodology. Working from the top down, we considered possible failures of the system (as listed above) and how ERTMS/ETCS guards against these failures, and working from the bottom up, we reviewed key specifications in detail to identify any assumptions, weaknesses, inconsistencies, or vulnerabilities in the specifications that might provide an opportunity for an attacker to compromise the system. Full details can be found in our first report [2].

Having identified some potential vulnerabilities in the ERTMS/ETCS specifications, we were asked to devise attack scenarios to explore the ways in which an attacker could exploit these potential weaknesses and vulnerabilities to achieve one of the undesirable outcomes listed above. Full details can be found in our second report [3].

We identified seven attack scenarios and then analysed each in detail by considering the following questions:

- how is the attack performed?
- what vulnerabilities does the attack exploit?
- where can the attack be launched from?
- what are the possible mitigations?

We then graded each attack according to a range of criteria:

- the type of access required to exploit a vulnerability;
- the level of technical sophistication required to exploit a vulnerability;
- the type of failure caused by a successful attack;
- the scale of effect for a successful attack;
- the scalability of the attack from the attacker's perspective;
- the type of impact caused by a successful attack;
- the types of mitigation strategy that are possible;
- the level of difficulty for implementing each mitigation.

Our analysis and grading methodology was partially based on a technique for scenario analysis that was devised by a NATO Research Task Group for a study on the Dual Use of High Assurance Technologies [5].

We considered several different categorisations but chose these particular categories because we thought they were the most informative and provided a good summary of the issues raised by each scenario. We deliberately did not attempt to rank the various attack scenarios using a weighted average of the category scores because we believe that such a ranking would be too simplistic – the relative weighting of the various categories and the ranking of the scenarios is a matter for government and industry stakeholders. Similarly, we did not attempt to estimate the likelihood of attacks being successful because this would depend on the national implementation of ERTMS and is therefore best left to the domain experts.

Our attack scenarios have been presented to experts in the ERTMS/ETCS technologies, who commented very favorably on both the approach and the analysis and grading methodologies we used.

References

[1] UNISIG SUBSET-026, System Requirement Specification, Version 2.3.0, http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-026.aspx

[2] Bloomfield, R., Stroud, R., Gashi, I., Bloomfield, R.: Information Security Audit of ERTMS, Technical Report (2010).

[3] Stroud, R., Gashi, I., Bloomfield, R., Bloomfield, R.: ERTMS Specification Security Audit - Analysis of Attack Scenarios, Technical Report (2011).

[4] UNISIG SUBSET 088, ETCS Application Levels 1 & 2 — Safety Analysis, Version 2.3.0, http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-088.aspx

[5] Bloomfield, R., Craigen, D., Miller, A.: Dual Use of High Assurance Technologies (2009), Technical Report, http://www.rto.nato.int/Pubs/rdp.asp?RDP=RTO-TR-IST-048

NOTE: Reports [2] and [3] above are currently not publicly available; however, copies of the reports can be made available on request, subject to approval from the stakeholders.