Rail Security Expert Group

Security Penetration Testing

23E245
1A
01.07.2024

Modification history

Version	Date	Modification / Description	Editor
0A	27.11.2023	Initial Draft	Jorge Gamelas, Christof Jungo, Oliver Lovric, Richard Poschinger, Max Schubert
0B	19.02.2024	Draft available for internal review	Christof Jungo, Oliver Lovric, Richard Poschinger
1A	01.07.2024	Improvements after internal and external (CER/EIM) review	Christof Jungo, Oliver Lovric, Richard Poschinger, Nicolas Poyet, Max Schubert

Table of Contents

1 Introduction

1.1 Scope

1.1.1.1 The purpose of this document is to give guidance on penetration testing in the railway CCS domain (including EULYNX, ERTMS and the corresponding legacy systems).

1.2 References

1.2.1.1 Subsets and EUG publication are referenced directly with their corresponding ID.

1.3 Other referenced documents:

[1] “RFC 2119,” 1997. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2119.

[2] CREST, „A Guide to Penetration Testing,“ 2022. [Online]. Available: https://www.crest-approved.org/wp-content/uploads/2023/04/A-Guide-to-Penetration-Testing-2022.pdf?ver.

[3] ISECOM / Pete Herzog, “OSSTMM v3.02,” 2010. [Online]. Available: https://www.isecom.org/OSSTMM.3.pdf.

[4] PTES, “PTES v1.0,” 2014. [Online]. Available: http://www.pentest-standard.org/index.php/Main_Page.

[5] NIST, „Technical Guide to Information Security Testing and Assessment,“ 09 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

[6] „CLC/TS 50701: Railway applications - Cybersecurity,“ 2022.

[7] Shift2Rail Joint Undertaking, „Task 9.2 / Deliverable 9.1 Part 1: Security verification and validation testing best practices – Product lifecycle,“ 2021.

1.4 Abbreviations

PTM ..... *Penetration Test Manager*
RAM ..... *Reliability Availability Mantainability*
SAT ..... *Site Acceptance Tests*

ERTMS Abbreviations are listed in SUBSET-023

1.5 Authors

1.5.1.1 The Rail Security Expert Group (RSEG) consists of security experts of the following groups:

- ERTMS Security Expert Group (ESCG) – Part of the EEIG ERTMS Users Group
- EULYNX Security Cluster – Part of the EULYNX Initiative

1.5.1.2 The following members of the Rail Security Expert Group were involved in creating this document:

- ERTMS User Group (EUG) / EULYNX
  - Max Schubert
  - Richard Poschinger
- SBB
  - Oliver Lovric
  - Christof Jungo
- Trafikverket
  - Jorge Gamelas

1.6 Applicability and Document Status

1.6.1.1 In order to ensure the usability for tender documents, this document is using classifications and requirement key words. This classification does not result in any binding requirements for members of the EUG or other involved parties. The documents will be updated in the future to be adapted to a changed threat landscape, updated standards, and newly developed security solutions.

1.7 Definition of Requirement Types

1.7.1.1 This document uses key words indicating requirement levels according to RFC 2119 [1]. Each clause in this document is classified as follows:

M	Mandatory	function must be implemented as specified
O	Optional	not mandatory, must be as specified if implemented
I	Informative	included for clarification purposes only
R	Recommendation	included as recommendation

Texts without a tag do not constitute a requirement.

1.8 Definition of Terms

1.8.1.1 “New Systems” are systems build according to IEC 62443 (e.g. future releases of TSI CCS or EULYNX BL4R1/2)

1.8.1.2 “Legacy Systems” are systems not built according to IEC 62443

1.8.1.3 “PTM” is the Penetration Test Manager for a specific system.

1.8.1.4 “Railway Operators” are Railway Undertakings, Infrastructure Managers and Vehicle Owners

2 Introduction to Penetration Testing

2.1.1.1 Authorised Penetration Testing attempts to actively discover, exploit, and report on, security related vulnerabilities/weakness in components and systems. **(I)**

2.1.1.2 Penetration test could damage or cause disruption of operational systems during testing. **(I)**

2.1.1.3 Penetration testing does not include security functionality testing which is included in CENELEC phases 6 to 9. **(I)**

2.1.1.4 Vulnerability assessment, a less intrusive process (if well configured), may be undertaken alongside penetration testing. **(I)**

3 General Penetration Testing

3.1.1.1 There are multiple penetration testing methodologies and guidelines available. Some of the known penetration testing guidelines are listed below. **(I)**

3.1.1.2 One non-profit organisation referenced by Shift2Rail is CREST, which is an accreditation body who certify organisations that offer penetration test services. CREST provides a guideline named “A Guide to Penetration Testing” [2] **(I)**

3.1.1.3 Open Source Security Testing Methodology Manual (OSSTMM)

OSSTMM “is a methodology to test the operational security of physical locations, human interactions, and all forms of communications such as wireless, wired, analog, and digital.” In addition, ethical guidelines are provided for performing the tests. [3] **(I)**

3.1.1.4 Penetration Testing Execution Standard (PTES)

PTES “cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.” [4] **(I)**

3.1.1.5 NIST SP 800-115

“The purpose of this document is to provide guidelines for organizations on planning and conducting technical information security testing and assessments, analyzing findings, and developing mitigation strategies. It provides practical recommendations for designing, implementing, and maintaining technical strategies. It provides practical recommendations for designing, implementing, and maintaining technical information relating to security testing and assessment processes and procedures, which can be used for several purposes—such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements. This guide is not intended to present a comprehensive information security testing or assessment program, but rather an overview of the key elements of technical security testing and assessment with emphasis

on specific techniques, their benefits and limitations, and recommendations for their use." [5] **(I)**

3.1.1.6 It's necessary to define the scope and objectives, including the purpose of the tests, limitations, and key components of an effective penetration testing approach. **(I)**

3.1.1.7 Reporting on penetration tests shall be treated as highly sensitive with very limited distribution and include thorough documentation of all findings and steps taken during the penetration testing. Reports should be clear, actionable, and provide specific recommendations for addressing identified vulnerabilities. **(I)**

4 Rail-Specific Penetration Testing

4.1.1.1 This chapter provide insights and best practices in conducting effective penetration testing on railway systems. **(I)**

4.2 Responsibilities

4.2.1.1 Regular updates and communication with all relevant stakeholders throughout the testing process shall be maintained. **(I)**

4.2.2 Product Supplier

4.2.2.1 The product supplier shall provide a proof of penetration tests on the product before product release. **(M)**

4.2.2.2 The product supplier should use an independent (third-party) organisation performing penetration test activities. **(R)**

4.2.2.3 Product releases also include any software updates including e.g. OS, firmware or application. **(I)**

4.2.2.4 The product supplier shall provide support for penetration test to the system integrator. **(M)**

4.2.3 System Integrator

4.2.3.1 The system integrator shall conduct penetration tests on the system before Site Acceptance Tests (SAT). **(M)**

4.2.3.2 The system integrator shall provide support for penetration test to the railway operator. **(M)**

4.2.3.3 Penetration test support contains: **(I)**

- Documentation of the system architecture
- Documentation of potential impacts of test
- Documentation of software libraries
- Documentation of security functions
- Documentation of known vulnerabilities and weaknesses
- Technical support contact

4.2.4 Railway Operator

4.2.4.1 The railway operator is responsible for penetration tests of systems in operation and their impact on railway operation. **(I)**

4.2.4.2 The railway operator shall request support for penetration tests from the system integrator or the product supplier before any penetration test. **(M)**

4.2.4.3 Penetration test support is defined in 4.2.3.3 **(I)**

4.2.4.4 The PTM shall assess the potential impact of the penetration test on railway operation. **(M)**

4.2.4.5 The PTM shall organize all relevant approvals before conducting the penetration test. **(M)**

4.2.4.6 Potential impact contains: **(I)**

- Safety impact
- RAM impact
- Financial impact
- Compliance Legal impact
- Unintentional disclosure of sensitive data

4.2.4.7 The PTM shall inform the responsible system owner and security department about relevant results. **(M)**

4.3 Legal aspects of Penetration Testing

4.3.1.1 The railway operator shall ensure that penetration tests are carried out in accordance with applicable legislation. **(M)**

4.3.1.2 The railway operator shall ensure that liability aspects of penetration tests are checked and taken into consideration. **(M)**

4.3.1.3 The railway operator shall ensure that contractual conditions are in place to protect itself from prosecution. **(M)**

4.3.1.4 The railway operator should integrate in tenders the permission to share discovered vulnerabilities with other railway operators**. (R)**

4.3.1.5 If the railway operator discovers vulnerabilities and wants to share them with other railway operators, the railway operator shall ensure that no confidentiality agreements or end user license agreements (EULA) restrict this. **(M)**

4.3.1.6 The railway operator shall disclose vulnerability information according to ISO 29147 to the according suppliers and other railway operators. **(M)**

4.3.1.7 The supplier shall disclose vulnerability information according to ISO 29147 to the affected railway operators. **(M)**

4.3.1.8 The railway operator shall include a Coordinated Disclosure agreement according to ISO 29147 in tenders for the suppliers. **(M)**

4.3.1.9 Additional clauses might need to be added to the tender for Coordinated Disclosure according to e.g. the CRA. **(I)**

4.3.1.10 If an interface communicating with another organisation is affected by the penetration test, the railway operator shall get an approval of the affected organisation. **(M)**

4.4 Depth of testing

4.4.1.1 According to TS 50701 [6] Chapter 9.3.2 (IEC CD 63452 ED, Chapter 9.3.3.2) the security-related tests are structured in the following types: **(I)**

- Security requirements testing
- Threat mitigation testing
- Vulnerability scanning
- Penetration testing

The types of vulnerability scanning and penetration testing are described in this chapter.

4.4.2 Vulnerability scanning

4.4.2.1 The system integrator and system maintainer shall perform vulnerability scans regularly (at least for every update) to test the system. **(M)**

4.4.2.2 The system integrator and system maintainer shall use updated vulnerability test cases to perform the vulnerability scan. **(M)**

4.4.2.3 The system integrator and system maintainer shall use system-specific vulnerability test cases to perform the vulnerability scan. **(M)**

4.4.2.4 The system integrator and system maintainer shall report vulnerabilities identified in vulnerability scans to the railway operator. **(M)**

4.4.3 Penetration testing

4.4.3.1 Penetration testing can be performed in different level of detail and depth.

Based on Technical standards and publications Penetration testing is often categorized in: **(I)**

- Exploitation of known vulnerabilities
- Active search for new vulnerabilities and exploits

4.4.3.2 The system integrator shall test if vulnerabilities identified by vulnerability scans can be exploited. **(M)**

4.4.3.3 The system integrator shall test if vulnerabilities identified by vulnerability scans can be used to cause an impact on the system and analyse the potential impact. **(M)**

4.4.3.4 The system integrator shall search for new vulnerabilities and exploits of the system. **(M)**

4.4.3.5 The system integrator shall report vulnerabilities identified in penetration tests to the railway operator. **(M)**

4.5 Dependencies of high-availability and safety-related tests

4.5.1.1 Testing systems with high availability or safety requirements requires additional measures and considerations to ensure that the availability or safety objective is still met. In the railway domain, such systems include Interlockings, RBC, ATO, Traffic Management (in part). **(I)**

4.5.2 In-Service Systems

4.5.2.1 A real-world penetration test can provide more realistic results in terms of configuration and impact than laboratory testing. **(I)**

4.5.2.2 To perform the testing, the operational systems can be temporarily taken out of service and isolated from the network to provide a realistic system setup without potentially causing unexpected availability issues. **(I)**

4.5.2.3 In-service systems provide the most realistic test environment but can cause negative impacts on operational availability. It should only be performed if either not realistic lab environment is available (see 4.5.3) or if the system cannot be tested while being out of service. **(R)**

4.5.2.4 The PTM shall request an estimation of the possible damage (cost, repair-time) by the manufacturer for the tested system before accomplishing the testing. **(M)**

4.5.2.5 The PTM shall request a confirmation from the rail operator that testing is permitted during a specific period. **(M)**

4.5.2.6 The PTM shall assess the potential impact of the planned test on the system's availability. **(M)**

4.5.2.7 The PTM shall inform the rail operator that the test may have a quantified impact on availability for a specified time after the test. **(M)**

4.5.2.8 The PTM shall ensure that trained technicians are available, to handle system failures during the test. **(M)**

4.5.2.9 The PTM shall establish procedures to ensure that the operational state of the system can be recovered in case of a system failure during the test. **(M)**

4.5.3 In Laboratory

4.5.3.1 A laboratory can provide an isolated environment where it's not possible to cause damage during in-service test. In addition, the availability of laboratories is usually greater than the allocated time slots that can be used for testing in-service systems. **(I)**

4.5.3.2 Laboratories may differ from the in-service systems in the following aspects: **(I)**

- Some endpoints may be stubs/mock-ups or unavailable.
- The number of test endpoints and their capacity is typically lower.
- Networks may differ in timing and other aspects from the in-service network.
- Specific networks may be simulated or replaced by other behaviour (e.g., GSM-R, 5G, FRMCS), so some protocols or techniques may be missing altogether.
- Systems in the lab may not be hardened or provide additional testing capabilities.
- Security features may not be implemented.

4.5.3.3 The PTM shall evaluate the deviations of the laboratory setup from the in-service system and take them into account in the test design. **(M)**

4.5.3.4 The PTM shall evaluate the deviations of the laboratory setup from the in-service system and take them into account in the analysis of test results. **(M)**

4.5.3.5 The PTM shall plan and agree test activities with all relevant stakeholders. **(M)**

4.5.3.6 Relevant stakeholders for the test activities include, but are not limited to, the lab supervisor, the test personnel, the owner of additional equipment required to perform the test, a validator. **(I)**

4.6 Hints on penetration tests

4.6.1.1 This chapter provides guidance on penetration testing for legacy and standardized systems. **(I)**

4.6.1.2 Penetration testing of legacy systems is not intended to provide evidence of vulnerabilities (as these are obvious), but to learn about the specific exploitation. **(I)**

4.6.1.3 Penetration testing of legacy systems is useful in the absence of specific exploitation experience on which to base the design and implementation of countermeasures. **(I)**

4.6.1.4 Penetration tests for (newly) standardised systems (ETCS BL4R1, EULYNX BL4R1 and newer – including EU-Rail Security drafts) can follow the standard procedures for penetration tests (e.g. CREST), as an adequate level of security can be assumed. **(I)**

4.6.1.5 [7] provides a reference between IEC 62443-4-1 (secure development) and CREST. **(I)**

4.6.1.6 The PTM shall plan penetration tests based on a prior assessment of **(M)**

- Security measures for interfaces (integrity protection/encryption)
- Security measures for systems (hardening, secure software development, integrity protection)
- Known vulnerabilities of software or libraries used.

4.6.1.7 The objectives of penetration testing shall ensure that these tests provide additional results compared to document assessments and functional tests. These tests may provide the following additional insights: **(I)**

- Assess the feasibility of an attack
- Closing the documentation gap
  (between available documentation and real implementation)
- Test of countermeasures
- Test of detection systems

4.6.1.8 The software firewall of the systems might specifically allow access from connected systems. If these allow lists are not taken into account during penetration tests, risks of attacks on the system via a compromised connected system might be ignored. Hence the attack surface of systems might vary depending on different perspectives in the network. **(I)**

4.6.1.9 The PTM should deactivate the software firewall or deactivate any blocking software firewall rules of the system to maximise the attack surface. **(R)**

4.6.1.10 This follows the two-step approach by checking first the integration of the firewall and its vulnerability and in the second step the system behind the firewall. Even if the firewall can’t be successfully overcome in reasonable time, by this means a successful breach can be simulated to check all layers of the defence in depth integration. If this recommendation is implemented, the exploitability might be overestimated. **(I)**