http://dx.doi.org/10.25673/111636

Compliance with Industrial Security Standards by Implementing Remote Attestation

Florian Kohnhäuser and Sören Finster

ABB AG, Corporate Research, Ladenburg, Germany
{florian.kohnhaeuser,soeren.finster}@de.abb.com

Abstract. To mitigate the risk of cyber threats on industrial systems, security standards are currently emerging and providing an important framework to ensure security. While security standards define desired security outcomes, they often lack specific implementation strategies. This leads to the application of inconsistent or inadequate security measures. In this work, we focus on a novel security measure called remote attestation, which is capable of verifying the authenticity and integrity of remote devices and systems. We analyze remote attestation and its relation to the industrial security standards IEC 62443, NERC CIP, NIST SP 800, ISO/IEC 27002, and PCI DSS. In detail, we map remote attestation to requirements of the analyzed security standards, highlighting the degree to which these requirements can be fulfilled by remote attestation. The results demonstrate that remote attestation is highly relevant to the analyzed security standards and offers both technical mitigation of cyber threats as well as compliance with well-established security standards.

1 Introduction

With the increasing connectivity and openness of industrial systems, security has become a crucial requirement. To address the need for security, regulations and standards are becoming more and more important. They serve as a framework that organizations, products, and services must satisfy to mitigate security threats. While security standards specify the desired outcome in terms of security requirements, they typically lack instructions and implementation strategies to reach that outcome. Some security requirements, such as secure communication between industrial components, are comparatively easy to implement, as all modern communication protocols have built-in security modes. Yet, other requirements, such as secure auditing, logging, and device integrity, are much harder to fulfill. This gap between the definition and implementation of security requirements can result in inconsistent or inadequate security measures, leaving systems and data vulnerable to potential threats and compromises.

Remote attestation is an emerging security technology that addresses the growing concerns on the trustworthiness and integrity of computer systems [4]. Attestation allows to verify the integrity of the hardware, software, and configuration of a remote system. During verification, tampering of the remote device is detected, which provides a strong defense against various threats, including

malware and unauthorized modifications. However, remote attestation is not yet well-understood regarding its provided security capabilities and compliance with security standards, which hampers its adoption in practice.

In this work, we analyze remote attestation regarding its compliance with industrial security standards. To this end, we first provide an introduction into remote attestation and security compliance (Chapter 2). Next, the provided security properties of remote attestation are mapped to the well-established security standards IEC 62443 [6], NERC CIP [7], NIST SP 800 [8], ISOIEC 27002 [9], and PCI DSS [10] (Chapter 3). The mapping lists specific requirements of the analyzed security standards that can be fulfilled by implementing remote attestation. In specific, it is investigated to which degree the requirements can be fulfilled and how potential gaps can be addressed. It is shown that remote attestation is highly relevant to the analyzed security standards (Chapter 4).

2 Background

2.1 Remote Attestation

Remote ATtestation procedureS (RATS) [5] are a security measure to verify the integrity and trustworthiness of a remote device or system. Although RATS have been proposed two decades ago [4], they recently gained attention due to the availability of secure hardware, open source implementations, and standardization efforts [5]. RATS functioning relies on secure hardware that allows a remote system, commonly referred to as the verifier, to assess the integrity of another system, known as the prover. This assessment involves generating a unique cryptographic signature or measurement of the prover's software, hardware, and configuration. The verifier compares this measurement against a predefined reference, or known-good configuration, to determine whether the prover has been compromised or altered in any way. The primary purpose of RATS are to establish trust in remote devices or systems, ensuring that they have not been tampered with. Their security goals include detecting unauthorized modifications, protecting against malware, and providing evidence of the remote system's trustworthiness, thereby enhancing security in scenarios like remote device management, secure bootstrapping, and establishing secure communication.

2.2 Security Compliance

Security regulations and standards serve as a framework that organizations, products, and services must adhere to, in order to ensure the protection of sensitive data, maintain customer trust, and mitigate the risk of cyber threats. By complying with these standards, actors demonstrate their commitment to data security, privacy, and integrity by establishing robust security controls, implementing best practices, and undergoing regular assessments to identify and address vulnerabilities. Security regulations and standards exist at national and international level, such as the German BSI KRITIS regulation [1] and European

Cyber Resilience Act [2]. Although they exist for various industries, this work focuses on the standards regarding the electric utility industry (NERC CIP), payment card industry (PCI DSS), organizational processes (ISO 27002), government agencies (NIST SP800), and industrial control industry (ISO 62443).

3 Evaluation

In this section, we map Remote ATtestation procedureS (RATS) [5] to the requirements of the industrial security standards NERC CIP, NIST SP 800, ISO/IEC 27002, PCI DSS, and IEC 62443. In case a requirement can be fulfilled by implementing RATS, we assess whether it has a low, medium, or high relevance to RATS, and describe its relevance, including gaps, in detail.

3.1 NERC CIP

North American Electric Reliability Corporation Critical Infrastructure Protections relates to the preparedness and response to serious incidents that involve the critical infrastructure assets in the electrical power grid [7].

CIP-005 1.5 Malicious communication (low relevance)

Requirement: Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

Relevance: While RATS do not monitor communication, outbound malicious communication must originate in a local process. RATS provide means for observing local processes and detecting unwanted changes in them. Thus, the root cause for outbound malicious communication can be detected using RATS.

CIP-007 2.1-4 Patch management (medium relevance)

Requirement: A patch management process includes tracking, evaluating, and installing cybersecurity patches for relevant cyber assets. This involves identifying sources for patch releases and conducting evaluations every 35 days. After evaluation, one of these actions must be taken: (i) apply the patches, (ii) create a dated mitigation plan, or (iii) revise an existing mitigation plan.

Relevance: While this patch management process does not require for checking if patches have been applied, its intention shows that all relevant security patches should be installed. With RATS, periodic checking of the software that is currently in use is done. This automatically provides means of checking that software is on the desired patch level.

CIP-007 3.1 Detect malicious code (high relevance)

Requirement: Deploy methods to deter, detect, or prevent malicious code.

Relevance: This is a direct function of RATS with the capability to even detect malicious code on already compromised systems. This is a feature that the suggested measures (e.g., antivirus) do not provide.

CIP-007 3.2 Malicious code mitigation (high relevance)

Requirement: Mitigate the threat of detected malicious code.

Relevance: RATS provide timely and automatic detection and can initiate manual processes and automatic measures to mitigate the threat.

CIP-007 3.3 Up to date measures (high relevance)

Requirement: For methods identified in part 3.1 that use signatures or patterns to detect malicious code, have a process to update of the signatures or patterns.

Relevance: This requirement is relevant in two ways. First, RATS must be provided with information about the known-good software state. This corresponds to the signatures or patterns described in this requirement. Second, RATS can measure the installed signatures or patterns on a system and thus provide checking if signatures or patterns are installed correctly.

CIP-008 1.1 and 1.4 Incident response (low relevance)

Requirement: Establish one or more processes to identify, classify, and respond to cyber security incidents.

Relevance: RATS verification services can play a supporting role in incident response for quickly identifying and analyzing security incidents.

CIP-010 2.1 Configuration change detection (high relevance)

Requirement: Monitor at least once every 35 calendar days for changes to the baseline configuration. Document and investigate detected unauthorized changes.

Relevance: As configuration can be included in RATS reports, the automatic and regular monitoring of changes is a direct result of implementing RATS.

CIP-010 3.1-4 Vulnerability assessment (high relevance)

Requirement: Conduct a paper or active vulnerability assessment every 15 months. Additionally, perform an active vulnerability assessment in a test environment every 36 months, mimicking the production environment's configuration, and document the results along with any differences from the test environment.

Relevance: RATS can cover large parts of vulnerability assessments and reduce manual effort. This is very relevant, as assessments need to be done regularly.

3.2 PCI DSS V3.1.2

Payment Card Industry (PCI) Data Security Standard (DSS) is a set of security requirements and best practices designed to protect payment card data and prevent data breaches within organizations that handle credit card transactions.

Do not use vendor-supplied defaults (2) (low relevance)

Requirement: Do not use vendor-supplied defaults for system passwords and other security parameters.

Relevance: RATS can help ensure that such defaults are not present on target systems, if the corresponding databases (e.g., password database) is checked against the whitelisted version by the verifier.

Malware and anti-virus (5) (high relevance)

Requirement: Protect all systems against malware and regularly update anti-virus software or programs.

Relevance: Detection and escalation of unwanted software (e.g., malware) is a core functionality of RATS. Additionally, RATS can protect against missed updates of anti-virus software by checking against the whitelisted current version.

Protection from known vulnerabilities (6.2) (medium relevance)

Requirement: Ensure that all system components and software are protected from known vulnerabilities by installing vendor-supplied security patches. Install critical security patches within one month of release.

Relevance: RATS provide a constant monitoring of the installed software and therefore helps ensuring that all software is free from known vulnerabilities.

Audit trails (10.2) (low relevance)

Requirement: Implement automated audit trails for all system components to reconstruct the following events: (i) use of and changes to identification and authentication mechanisms, and (ii) creation and deletion of system-level objects.

Relevance: Some of the audit trails can be fulfilled by applying RATS. Especially changes to system-level objects or authentication databases will show up in RATS reports and further actions can then be initiated by the verifier.

Deploy change-detection (11.5) (high relevance)

Requirement: Deploy a change-detection mechanism (e.g., file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Relevance: This is a direct requirement for the service RATS provide securely.

3.3 ISO/IEC 27002

ISO/IEC 27002 is an international standard that provides guidelines and best practices for information security management, helping organizations establish and maintain effective security controls and risk management processes [9].

Asset Management (8.1.1) (low relevance)

Requirement: Assets associated with information and information processing should be identified and an inventory of these assets should be maintained.

Relevance: Especially with the further clarification in mind, that prescribes asset inventory to be "accurate, up to date, consistent and aligned with other inventories", RATS can provide a significant portion of this requirement.

User access provisioning (9.2.2) (high relevance)

Requirement: A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.

Relevance: User access rights can be included in RATS reports. This provides a timely checking current user access rights compared with desired access rights. Especially with the further clarification to "periodically reviewing access rights with owners of the information systems or services", RATS can provide at least a source for the needed information.

Use of privileged utility programs (9.4.4) (high relevance)

Requirement: The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Relevance: RATS provide the desired tight control of the usage of all programs, especially privileged utility programs.

Controls against malware (12.2.1) (high relevance)

Requirement: Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Relevance: Detection and escalation of unwanted software (e.g., malware) is a core functionality of RATS. The implementation of RATS and their integration with SIEM systems therefore provide a large part of this requirement.

Installation of software on operational systems (12.5.1) (low relevance)

Requirement: Procedures should be implemented to control the installation of software on operational systems.

Relevance: While RATS typically do not control the installation of software, implementation guidance point f) "an audit log should be maintained of all updates to operational program libraries;", is part of RATS functionality.

Management of technical vulnerabilities (12.6.1) (high relevance)

Requirement: Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion. The organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken to address the associated risk.

Relevance: Since RATS can provide an inventory of the used software, the evaluation of the exposure to known technical vulnerabilities is easy to implement by simply checking the inventory of used software on the verifier.

Secure system engineering principles (14.2.5) (medium relevance)

Requirement: Principles for engineering secure systems should be established, documented, maintained and applied to any information system.

Relevance: RATS can be a crucial part of secure systems engineering.

Responsibilities and procedures (16.1.1) (medium relevance)

Requirement: Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Relevance: Implementation guidance for this requirements lists "procedures for monitoring, detecting, analysing and reporting of information security events and incidents;", which can be fulfilled with RATS functionality.

Collection of evidence (16.1.4) (medium relevance)

Requirement: The organization should identify, collect, acquire and preserve information, which can serve as evidence for security breaches.

Relevance: RATS provide identification and collection of information which can serve as evidence.

Technical compliance review (18.2.3) (high relevance)

Requirement: Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.

Relevance: RATS regularly evaluate systems for compliance. The clarification demands "Technical compliance should be reviewed preferably with the assistance of automated tools". RATS provide such automated tools.

3.4 NIST SP800 – 171A

NIST SP 800-171 is a set of guidelines and controls by the National Institute of Standards and Technology (NIST) to enhance the security of Controlled Unclassified Information (CUI) in non-federal systems and organizations [8].

Audit and accountability (3.3.1) (medium relevance)

Requirement: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

Relevance: RATS creates the required system audit logs that allow to monitor, analyze and investigate unlawful or unauthorized system activity.

Configuration management (3.4.1) (medium relevance)

Requirement: Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Relevance: RATS can at least support if not fulfill especially the following requirements: (3.4.7) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services; (3.4.8) Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software; (3.4.9) Control and monitor user-installed software.

Security Assessment (3.12.1) (medium relevance)

Requirement: Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Relevance: RATS can be a part of security assessments and especially help to fulfill the requirement for periodic assessments since RATS assessments can be done automatically.

System and information integrity (3.14.2, 3.14.3) (high relevance)

Requirement: Provide protection from malicious code at designated locations within organizational systems. Monitor system security alerts and advisories and take action in response.

Relevance: Detection and escalation of unwanted software (e.g., malware) is a core functionality of RATS. The implementation of RATS and their integration with SIEM systems therefore provide a large part of this requirement.

3.5 IEC 62443

IEC 62443 is an international series of standards addressing cybersecurity for operational technology in automation and control systems [6]. These standards apply a risk-based approach to prevent and manage security for both entire systems (IEC 62443-3-3) and their components (IEC 62443-4-2). Five security levels (SL0-SL4) are described, with SL4 offering the highest security guarantees.

CR 1.2 – Software process and device identification and authentication (low relevance)

Requirement: Components shall provide the capability to identify itself and authenticate to any other component. If the component is running in the context of a human user the identification and authentication of the human user may be part of the component identification and authentication process.

Relevance: RATS typically provide means to unique identify devices through a hardware root of trust. E.g., trust established via a TPM chip and its associated certificates can be used to uniquely identify and authenticate devices.

CR 3.2 – Protection from malicious code (medium relevance)

Requirement: The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.

Relevance: RATS aim at remotely detecting malicious code on devices. Thus, this requirement directly applies to RATS.

CR 3.4 – Software and information integrity (high relevance)

Requirement: Components must support integrity and authenticity checks on software, configurations, and data. The results of the integrity checks shall be recorded and reported. For SL 3 and SL 4, a configurable entity must be automatically about unauthorized changes.

Relevance: This requirement fully matches RATS, as RATS are about performing integrity checks on software, configuration, and further data, as well as reporting the results to an external party. Note that other mechanisms, such as secure boot, provide integrity checks, but are unable to report the result in a secure way to an external party. However, care must be taken to achieve SL3 and above, as RATS are typically invoked by an external party. Thus, to achieve SL3 and higher, provers must be equipped with the feature to perform self-checks.

EDR 3.12 – Provisioning product supplier roots of trust (medium relevance)

Requirement: To validate the authenticity and integrity of hardware, software, and data, a trusted source of data, known as the "root of trust" is required. This root of trust can be cryptographic hashes of known-good software or the public part of an asymmetric cryptographic key pair used for verifying cryptographic signatures. The root of trust is crucial for verifying critical components before booting to ensure that the system starts in a known secure state.

Relevance: RATS builds upon cryptographic hashes of known-good software states as a root of trust in order to validate that software, firmware, and data are uncompromised. Therefore, this requirement applies to RATS.

EDR 3.13 – Provisioning asset owner roots of trust (medium relevance)

Requirement: To safeguard component security when extending functionality, asset owners should be able to validate and approve origins, necessitating the provision of secure "roots of trust" by product suppliers that can differentiate between authorized and unauthorized origins.

Relevance: RATS can be implemented in a way that the trust established by the product supplier is extended to the asset owner.

EDR 3.14 – Integrity of the boot process (medium relevance)

Requirement: Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot and runtime processes prior to their use.

Relevance: RATS verify the integrity of the firmware, software, and configuration data, but perform the verification after executing the component. Nevertheless, there are existing modifications to RATS that also enable a local verification, e.g., the IMA-appraisal feature of the Linux Integrity Measurement Architecture.

CR 6.2 – Continuous monitoring (high relevance)

Requirement: Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

Relevance: RATS goal is to continuously monitor whether malicious code and data is being executed on a remote component. Thus, this requirement fully maps to RATS. To ensure a timely response, the frequency in which the verifier quires and checks the integrity of the prover needs to be chosen appropriately.

4 Conclusion

The increasing connectivity of industrial systems made security a crucial requirement, leading to the emergence of security regulations and standards. These standards serve as a framework to mitigate security threats, but often lack specific implementation guidance, which can result in inadequately implemented security measures. Remote attestation is a promising security measures to ensure the integrity of remote devices and systems. However, its security capabilities and compliance with standards is not well-understood. This work analyzed remote attestation's alignment with industrial security standards and showed that it is highly relevant to the analyzed standards, in particular, NERC CIP and IEC 62443. Thus, remote attestation not only mitigates cyber threats on a technical level, but also provides proof for strong security by providing compliance with well-known security regulations and standards.

References

1. Manuel Atug, "Zertifizierungen im Kontext KRITIScher Infrastrukturen: Vorgaben und Möglichkeiten für KRITIS-Betreiber", Datenschutz und Datensicherheit (2020).
2. Chiara, Pier Giorgio. "The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction." International Cybersecurity Law Review (2022).
3. Leander, Björn, Aida Čaušević, and Hans Hansson. "Applicability of the IEC 62443 standard in Industry 4.0/IIoT." Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019.
4. Sailer, Reiner, et al. "Design and implementation of a TCG-based integrity measurement architecture." USENIX Security symposium. Vol. 13. No. 2004.
5. Birkholz, H., et al. "RFC 9334 Remote ATtestation procedureS (RATS) Architecture." (2023).
6. ISA-62443 Security for Industrial Automation and Control Systems. Standard, International Society of Automaton (2017).
7. North American Electric Reliability Corporation (NERC) Cyber Security Standards. https://nerc.com/pa/Stand/Pages/Cyber-Security-Permanent.aspx (2006).
8. NIST Special Publication 800-82: http://dx.doi.org/10.6028/NIST.SP.800-82r2 (2015)
9. Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002) (2017).
10. Payment Card Industry Data Security Standard (PCI-DSS) Version 3.2.1 (2018).