Combining System Integrity Verification With Identity and Access Management

Markku Kylänpää and Jarno Salonen
VTT Technical Research Centre of Finland Ltd, Espoo, Finland
markku.kylanpaa@vtt.fi
jarno.salonen@vtt.fi

Abstract: Digital transformation and the utilization of Industrial IoT (IIoT) introduces numerous interconnected devices to factories increasing among others the challenge of managing their software versions and giving attackers new possibilities to exploit various software vulnerabilities. Factory networks were earlier isolated from the Internet. However, this separation is no longer valid and there can be connections that allow intruders to penetrate into information systems of factories. Another issue is that although factories typically are physically isolated, it is not necessarily safe to assume that physical security is in good shape as the novel supply networks comprise subcontracted activities and temporary work force. Another threat can also arise from unauthorized monitoring of devices and the unauthorized replacement of existing ones. Based on the previous, it is crucial that IIoT security should be built into factories of the future (FoF) right from the design phase and even low-end devices need to be supported. Trusted computing concept called remote attestation should be used. Remote attestation allows remote parties to verify the integrity of each system component. System components should include trusted hardware components that can be used to measure executable software. The term measurement means calculating the cryptographic hash of the binary component before passing control to it. Trusted hardware components should also have a mechanism to protect the integrity of the measurement list and cryptographic keys that can be used to sign integrity assertions. The verifier part should have a storage of reference integrity metrics identifying the expected values of these measurements. Deploying trusted computing and remote attestation concepts to industrial automation is not straightforward. Even if it is possible to use remote attestation with suitable hardware components, it is not clear how remote attestation should be integrated with various operational technology (OT) industrial automation protocols. Approaches to use remote attestation with existing industrial automation protocols (e.g., OPC UA) is discussed. Advanced identity and access management (e.g., OAuth2, OpenID Connect) can be used to combine integrity measurements with device identity information so that the remote attestation process is triggered by authentication during the first transaction. The focus is on machine-to-machine (M2M) communications with immutable device identities and integrity evidence transfer.

Keywords: industrial IoT, remote attestation, OT protocols, factory of the future, IAM, trusted computing

1. Introduction

Typically, IIoT protocols are focused on network security without support for end-point integrity assessment. However, as the complexity of factory installations is growing, it becomes clear that there is a need to have software inventory of all installed software and mechanisms that can be used to verify the installation status and integrity of system components. Factory networks are no longer fully isolated as there are many connectivity requirements. As this separation is no longer valid, there can be connections that allow intruders to penetrate into factory information systems. If IIoT devices are left unpatched, there is a threat that these vulnerabilities can be utilized by attackers. There is a need to update software versions and quickly apply security patches. Physical security also needs rethinking. Typically, the FoF supply networks comprise subcontracted activities and temporary work force. Unauthorized monitoring of devices and the unauthorized replacement of existing devices can be a threat. Attackers may, e.g., seriously harm factory operations, join factory devices to a botnet, use factory devices for cryptocurrency mining, and install ransomware to them, just to name a few potential threats. In order to mitigate these threat scenarios, IIoT security needs more focus when developing factories of the future. The integrity of system components is a foundation for all security mechanisms and should be implemented already at design phase. Integrity protection should also include low-end devices that are often omitted when designing security mechanisms.

Remote attestation is a trusted computing concept that allows remote parties to verify the integrity of system components. Integrating trusted computing and remote attestation concepts to industrial automation is a challenging task as systems have a long lifespan and typically utilize legacy protocols. It is not realistic to assume that all components will quickly support recently added standardized features. The lack of trusted hardware, especially in low-end IIoT components, has been a challenge but the situation is gradually improving. However, even if it is possible to use remote attestation with suitable hardware components, it is not clear how remote

attestation should be integrated with various OT industrial automation protocols since legacy protocol specifications do not include mechanisms for end-node integrity verification.

The convergence of IT and OT protocols with wider adaption of Internet-originated IT protocols in industrial automation is another IIoT trend. This will introduce more choices to combine integrity verification with advanced Identity and Access Management (IAM) approaches. Advanced IAM approaches for the factory of the future can be one approach to combine integrity measurements with device identity information so that the remote attestation process is triggered by authentication during the first transaction. Advances in confidential computing to build trust on remote systems can be considered as an analogue problem.

Basically, there are two approaches to endpoint integrity verification in IIoT systems. Either extend the existing legacy protocols or use IT originated IAM approaches to contain integrity verification of the endpoints. In this paper, these two approaches are discussed with examples from research literature. The purpose of this article is to collect information and clarify how this could be done by studying existing industrial automation protocols and figuring out what kind of approaches could be feasible. The focus is on M2M communications with immutable device identities and integrity evidence transfer. The rest of the paper is structured as follows. First, section 2 covers main remote attestation technology alternatives for IIoT devices. Section 3 describes IAM alternatives for IIoT devices including discussion and example use cases of remote attestation. Section 4 comprises some examples of extending legacy IIoT protocols to support remote attestation and section 5 contains the concluding remarks.

2. Remote attestation alternatives for IIoT devices

2.1 Background

The concept of remote attestation originates from the secure and measured boot research, where early prototypes, e.g., Tygar and Yee (1991), were using physically secure coprocessors as security hardware. Arbaugh et al. (1997) introduced the chained layered integrity checks model. These concepts inspired the Trusted Computing Group (TCG) industrial consortium to start the development of Trusted Platform Module (TPM) that is nowadays included in almost all PC hardware. TPM provides a root of trust that can be used to implement secure boot-time integrity measurements that can be extended to the operating system level. Attestation of network endpoints was one of the original goals of TCG (Berger 2005).

TCG defines attestation as the process by which an independent verifier can obtain cryptographic proof as to the identity of the device in question, evidence of the integrity of software loaded on that device when it started up, and then verify that what's there is what's supposed to be there (TCG 2019a). Coker et al. (2011) state that remote attestation is the activity of making a claim about properties of a target by supplying evidence to an appraiser over a network. They also identify some principles to guide the development of attestation systems (Coker et al. 2011). The first principle is that attestation must be able to deliver temporally fresh evidence, which is needed to prevent replay attacks. The second principle is that comprehensive information about the target should be accessible which requires that the attestation measurement mechanism should cover essential parts of the system. The third principle is that the target, or its owner, should be able to constrain disclosure of information about the target. This is sometimes hard to achieve if there are strict privacy requirements but that is not a case in IIoT systems. The fourth principle is that attestation claims should have explicit semantics to allow decisions to be derived from several claims. The verification process should be able to replay the measurement process and be aware of expected measurement values. The fifth principle is that the underlying attestation mechanism must be trustworthy. Typically, this requires that there is an isolated execution environment that can be used to protect the integrity of attestation measurements and to sign attestation evidence reports. (Coker et al. 2011)

In practice, remote attestation requires hardware support, as there must be trustworthy measurement mechanisms. The lack of hardware support has been an obstacle to the deployment of remote attestation in the IIoT environment. This is now changing as there are alternatives to implement isolated execution environments also to microcontroller class devices. There are multiple ways of implementing remote attestation and some examples are described in this section.

2.2 Standardization efforts

Nowadays, multiple organizations are standardizing trusted computing related security hardware and remote attestation. TCG was established already in 2003. Their main effort has been to specify the functionality of the TPM hardware component (TCG 2019b) focusing on Personal Computer (PC) platform but later they have expanded their scope. IETF has standardization efforts related to remote attestation. TCG has also developed a recommendation for the use of TCG technology in IIoT context (TCG 2022).

Additionally, IEEE, ENISA, and NIST have published many recommendations and specifications for IoT-related secure device identity and firmware update issues.

Classic remote attestation, described in Figure 1, is utilizing TCG TPM as a secure hardware. Measurement is a calculation of a cryptographic hash from a software component. One measurement mechanism example is Linux kernel Integrity Measurement Architecture (IMA) component, originally proposed by Sailer et al. (2004), which measures all loaded executables before execution. Measurements are stored as a measurement log that includes integrity protection using TPM Platform Configuration Register (PCR) values.

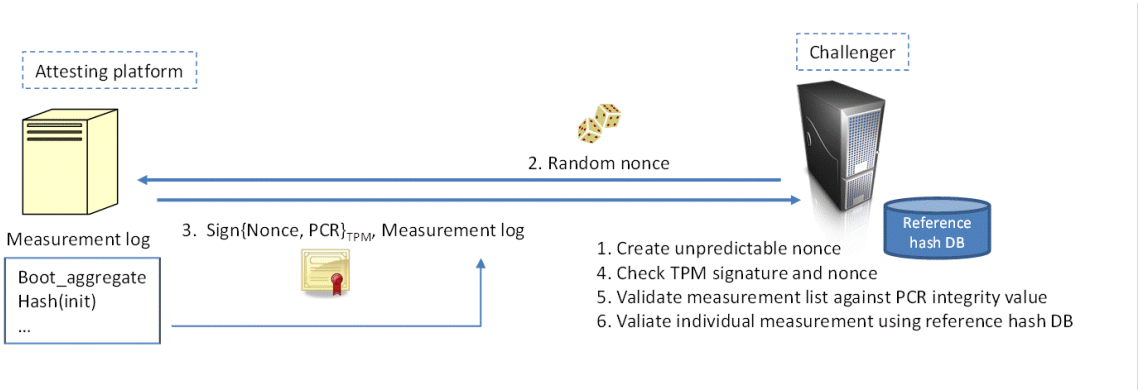

Figure 1: Classic remote attestation request/reply scenario utilizing TPM

TPM is not the only security hardware alternative. TCG Device Identifier Composition Engine (DICE) remote attestation (TCG 2020) expects that there is a statistically unique, device-specific, secret value called Unique Device Secret (UDS). The UDS must be stored in the non-volatile memory so that it is only accessible by the DICE layer. The DICE layer is using the UDS value to compute another secret called Compound Device Identifier (CDI) that is passed to the next layer.

IETF has a working group called Remote ATtestation procedureS (RATS) that covers remote attestation technologies. Their focus is networking infrastructure (e.g., routers) and not IIoT, but common topics and issues can still be found. The charter of the working group states that the entity (relying party) may require attestation evidence from a remote peer containing information about device identity, system component integrity, and device state.

The charter text also mentions that there are already domain-specific attestation mechanisms for TPM, FIDO Alliance attestation, and Android Keystore attestation. The goal of the working group is to standardize formats for describing assertions/claims about system components and their associated evidence. Another goal is to standardize procedures and protocols to convey these assertions/claims to relying parties. The working group has specified an Entity Attestation Token (EAT) that is used to transfer claims about device identity and state (Lundblade et al. 2021).

2.3 Industry initiatives

Platform Security Architecture (PSA) is an initiative of ARM that provides a security framework for IoT ecosystem. The framework is built to utilize ARM TrustZone for Cortex-M technology, also known as TrustZone-M, which provides isolated execution environment for microcontroller class devices (Pasham 2020). PSA also includes remote attestation.

Although attestation of cloud services is a different problem than the integrity verification of IIoT devices, both use quite similar technologies. There is a growing interest for confidential computing that requires remote attestation (Mulligan et al. 2021). Microsoft Azure Attestation (Baldwin et al. 2021) provides remote verification of the trustworthiness of a cloud platform and integrity of the binaries running in the cloud platform. Other cloud providers have similar offerings. For example, Amazon provides attestation support for their Nitro Enclaves (AWS 2022).

2.4 System level attestation

System level remote attestation has scalability problems when there are lots of nodes whose integrity status needs to be verified. The classic model describes only two-party communications. If the client needs to request attestation from all nodes this will easily become a bottleneck in the system. Attestation information is typically bound to low-level details, e.g., a cryptographic hash of firmware image or cryptographic hashes of certain application executable and library versions. The obvious idea is to split the system into subsystems with a gateway node that takes care of attestation of the subsystem nodes. Gateway nodes could hide low-level details from other system nodes and make higher level integrity claims of the system state. Property-based attestation is trying to define higher level properties that can be used outside of the subsystem.

Asokan et al. (2015) define a swarm-based attestation called Scalable Embedded Device Attestation (SEDA). The protocol includes two phases, offline and online. The offline phase includes device registration to a swarm. The online phase is the remote attestation operation. The verifier sends an attestation request to one swarm node. The node is then sending attestation requests to its neighbours. The operation is then repeated until all nodes have received the attestation request.

Remote attestation protocol is typically assumed to be a synchronous request-reply type of protocol. This is natural in simple cases as the process cannot proceed until the integrity status of the remote peer is verified. This can be a problem if there are lots of nodes as it requires that attestation operations must be done in a serial manner. Individual attestation operations to remote peers could be done in parallel. When replies from all remote peers have been received the process can continue. Dushku et al. (2020) describe asynchronous remote attestation.

3. IAM alternatives for IIoT devices

Modern authentication is an umbrella of mechanisms that can be used to replace traditional username/password-based mechanisms.

- Authentication methods: multi-factor authentication, smart cards, client certificates
- Authorization methods: OAuth2.0, OpenID
- Conditional access policies

Nowadays these are widely used in the office environment, e.g., Microsoft. Something similar can be used in factories also including M2M communications.

OAuth 2.0 developed by IETF Web Authorization (OAuth) WG is an industry-standard protocol for authorization. It is typically used in web-based services, but it is also increasingly used in IoT services (Hovsmith 2017, Sandoval 2017). IETF has a working group called Authentication and Authorization for Constrained Environments (ACE) that specifies a framework for authentication and authorization in IoT environments called ACE-OAuth (Seitz et al. 2021). The framework is based on a set of building blocks including OAuth 2.0 and the Constrained Application Protocol (CoAP).

OpenID is an open standard for authentication, promoted by the non-profit OpenID foundation. OpenID Connect is built on OAuth 2.0 protocol and is standardizing areas that OAuth 2.0 is not specifying, such as scopes and endpoint discovery. It is specifically focused on user authentication and is widely used to enable user logins on consumer websites and mobile apps.

Leicher et al. (2010) have described how remote attestation information can be merged into OpenID Connect transactions. They have added TPM-based integrity verification to OpenID Connect. The client is assumed to include a TPM and TPM PCRs are used to secure integrity measurements. The scenario begins in the same way

as a normal OpenID Connect scenario when a client is accessing a service and the service provider is delegating authentication to the OpenID provider. The difference is that now the OpenID provider initiates the remote attestation challenge/response messaging with the client. OpenID provider then verifies the attestation response message and grants access to the service after the authentication and integrity is successfully verified. The scenario is presented in Figure 2.

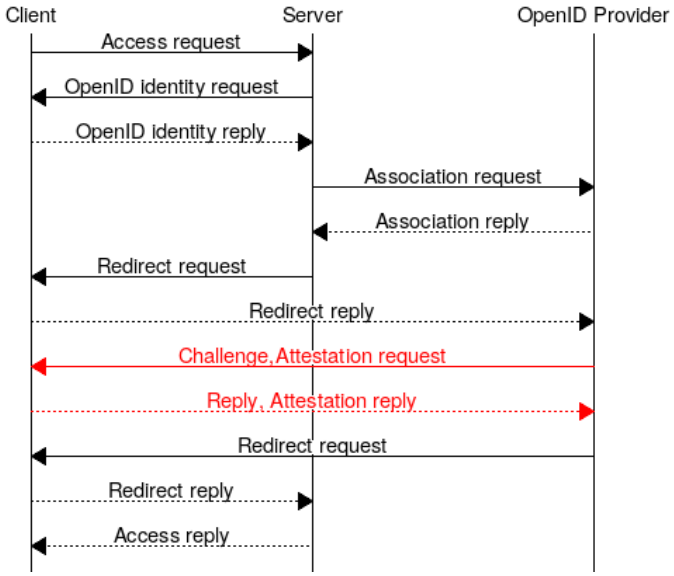

Figure 2: Integrate remote attestation with OpenID Connect transaction

Suomalainen et al. (2021) have extended OpenID Connect and OAuth 2.0-based authentication and authorization framework with DICE-based device integrity verification and remote attestation to verify the integrity of IoT devices.

SAML is an XML-oriented framework for transmitting user authentication, entitlement, and other attributes. The framework allows two federation partners to select and share identity attributes using a SAML assertion/message payload. SAML is using an XML-based syntax. SAML assumes three key roles in any transaction (Naik and Jenkins 2017). There is a trusted organization called Identity Provider. The Service Provider provides access-controlled services and User accesses these services. The SAML 2.0 specification describes assertions, protocols, bindings, and profiles (OASIS 2005). Ali et al. (2010) provide an example of the use of SAML-based federated identity management system with remote attestation.

4. Combining remote attestation with legacy IoT protocols

In this section we study a couple of widely used IoT protocols and discuss about possible ways to include remote attestation information. The goal is to extend existing protocols to carry remote attestation information. The convergence of IT and OT technology can introduce widely used Internet messaging protocols to industrial automation. Older protocols typically have fixed message structures and optimized wire protocols making it difficult to extend these protocols to support remote attestation.

4.1 OPC UA

OPC UA is a platform independent service-oriented M2M communications architecture targeting industrial automation. The specification is very large and complex consisting of more than 15 documents and over 3000 pages. The specification consists of multiple profiles (OPC 2017). Each profile includes a functionality set called a conformance unit. Despite the large size of the specification, the OPC UA security model (OPC 2018) does not yet include concepts that could be used to validate the integrity of connected devices. Recent study shows that there are large number of publicly accessible insecure OPC UA deployments (Dahlmanns et al. 2020).

Birnstill et al. (2017) have studied how OPC UA protocol can be integrated with remote attestation. Their approach is to include Trusted Platform Module (TPM) and use it as a hardware-based root of trust. Remote attestation is added as a separate conformance unit. Bienhaus et al. (2021) are also using TPM with OPC UA. Their focus is on securing a gateway node, but they also discuss about ideas of using sealed keys bound to certain

TPM PCR values. Another example of using OPC UA with remote attestation is by Matischek and Bara (2019). Instead of TPM they propose the use of a Secure Element (SE).

IETF draft by Birkholz et al. (2021a) proposes passing attestation information as part of existing security information exchange mechanism (e.g., X.509 certificates) that are already used in each protocol. OPC UA is using X.509 certificates and remote attestation evidence information is proposed to be embedded into an X.509 certificate as a certificate extension. Thus, remote attestation related information could be natively encoded in X.509 certificate extensions or could be encoded in some other format, which in turn is then encoded in an X.509 certificate extension. Certificates are normally considered to have relatively long lifetime, but remote attestation information is queried frequently. The approach may require the use of certificate chains, device acting as a certificate authority, and short-lived certificates.

Other possible approaches are to extend node endpoint information that is normally queried before a communications channel is created to contain attestation evidence information or use specific resource names that can be used to access attestation information.

4.2 DNP3

Distributed Network Protocol 3 (DNP3) is a protocol that is used, e.g., in SCADA industrial automation systems and electric power systems. DNP3 is also standardized as IEEE1815 (2012). DNP3 has had many protocol level vulnerabilities. Some of these are discussed by Lu and Feng (2018). Although the authors do not use remote attestation terminology, the measurement mechanism is described and remote attestation related modifications to DNP3 are discussed. DNP3 security framework has evolved to fix vulnerabilities, removing complex features, and adding new functionalities (e.g., features adapted from TLS) (Self 2020). TLS is often mentioned as a mechanism to secure DNP3 communications when communicating using Internet connections (PJM 2020). DNP3 seems to have many shortcomings and recent survey article by Pliatsios et al. (2020), covering proposed enhancements to SCADA with DNP3, does not refer to remote attestation at all.

4.3 OMG DDS

An article by Pardo-Castello and Lang (2013) discusses adding TPM and remote attestation to protect embedded systems. Their approach is to add a trusted hypervisor that can be used to run guest operating systems whose integrity can be measured by the hypervisor. The OMG DDS protocol is used to transfer integrity measurements to the attestation verifier using OMG DDS-based publish-subscribe protocol (OMG 2010).

There is another OMG DDS-based remote attestation example that describes hardening of nodes that are using OMG DDS based communications with Intel SGX Enclave based Trusted Execution Environment (TEE). The approach is described in three blog articles by Upchurch (2019). Intel SGX Enclaves use SCONE that can also be used to attest applications running in SGX Enclaves (Arnautov et al. 2016). The blog articles are more focused on providing confidentiality than discussing the integrity aspects and remote attestation.

Both examples are used in the Intel x86-based server room environment and not directly in the factory. OMG DDS is used just as a publish-subscribe protocol to carry integrity evidence information and not as an application protocol that will also include attestation information.

4.4 CoAP

The Constrained Application Protocol (CoAP) (Shelby et al. 2014) is a lightweight protocol that can be used as a replacement for HTTP in resource constrained environments. CoAP is typically used as a transport for higher-level protocols and not as an application protocol itself.

CHARRA is a proof-of-concept implementation of the "Challenge/Response Remote Attestation" interaction model of the IETF RATS Reference Interaction Models for Remote Attestation Procedures using TPM 2.0 (Eckel 2021). The mechanism has been applied to CoAP protocol.

IETF RATS WG work in progress draft “Reference Interaction Models for Remote Attestation Procedures” contains Appendix A with a title “CDDL Specification for a simple CoAP Challenge/Response Interaction”

(Birkholz et al. 2021b). The example describes the embedding of attestation information to CoAP FETCH request and response messages. Some of the authors of the draft are also working on CHARRA.

IETF RATS WG provides interaction models for remote attestation, but one must note that these are not transparent. If there are protocols on top of CoAP, changes are needed to include remote attestation support.

4.5 HTTPS

The original HTTP protocol was a simple request-reply protocol without transport layer confidentiality and integrity. Soon there was a need to utilize HTTP transport also for transactions that contain sensitive information. Secure Socket Layer (SSL) implementation by Netscape solved the problem by adding encryption and signing to provide confidentiality and integrity to communications. The approach was later standardized as Transport Layer Security (TLS). TLS is nowadays widely used in Internet traffic (all URLs starting with the prefix https). TLS also supports client certificates for (mutual) authentication.

Although TLS solves the security issues of communications, it does not provide integrity evidence of connected nodes. In a generic setup this is out of scope, as there is no way to get reference integrity metrics for heterogeneous end nodes. It is also a privacy issue as attestation evidence can reveal unwanted details. Factory environment is a more restricted environment. We can assume that the network node configuration is known and as there is no personal data in factory floor M2M communications, there are no privacy issues either. This means that it is feasible to add remote attestation to TLS.

Trusted Computing Group has a protocol called Trusted Network Connect (TNC) which includes remote attestation support using TPM as a security hardware. TNC never gained wide popularity but inspired developers to add remote attestation functionality to TLS. For example, Yu et al. (2013) are using TPM and the handshake protocol extensions of TLS to implement remote attestation functionality.

There are multiple examples of adding remote attestation to TLS with Intel SGX used as security hardware. Knauth et al. (2019) describe how they seamlessly combine Intel SGX remote attestation with the establishment of a standard TLS connection. Remote attestation is performed during the connection setup. There are no changes to the TLS protocol and not even modifications to existing protocol implementations. Intel has also SGX examples that include remote attestation support (Mechalas 2018).

TLS is often proposed as a mechanism to secure any legacy protocol by running it on top of TLS connection. As it is also possible to extend TLS to include remote attestation, this provides a mechanism to deploy remote attestation as well. However, there are still requirements for a measurement mechanism using isolated execution environments and reference integrity metrics. Error reporting also requires attention if remote attestation should take place transparently without the legacy protocol being aware of any integrity verification issues.

5. Conclusions

The factories of the future will interconnect and bring together OT and IT environments. The existing literature states that increased connectivity will also expose earlier isolated subsystems to attackers, which our research also supports. Network security provides confidentiality and integrity protection to communications preventing message eavesdropping, tampering, and replay attacks. However, according to our research, network security alone is not enough to protect IIoT systems. There is a need to have immutable device identities that are secured by security hardware and remote attestation mechanisms that can be used to verify the integrity of the connected device to detect that the device is in expected state. Our research shows that this is especially important in critical infrastructure systems but is also expected to be more widespread as hardware support for isolated execution environments in IoT devices becomes more common.

This paper first briefly described remote attestation mechanism alternatives for IoT. Based on our research work, remote attestation could be used in IIoT systems either as part of the shift towards IT protocols or there can be extensions to legacy protocols that are used in industrial automation. The literature shows that remote attestation is typically not used in identity and access management systems because of lacking security hardware and deployment complexity. However, we have noticed that cloud service providers have started to use remote

attestation as part of confidential computing initiatives, giving examples of how it can be used in IIoT systems as well.

Legacy industrial automation protocols are difficult to extend because of their optimized fixed message structure. Some legacy protocols also have shortcomings in integrity and confidentiality protection. Even modern protocols like OPC UA do not yet contain options to support remote attestation. Based on our research, we argue that the current specification is not enough, but instead further specification work is needed. The IETF RATS working group has been active in specifying formats and reference architectures to remote attestation deployment in the IoT environment. We feel that especially their Entity Attestation token specification will be widely adopted as a model how to encode attestation evidence.

Acknowledgements

The work presented here has been carried out in the ITEA4 project 17032 CyberFactory#1.

References

Ali, T., Nauman, M., Amin, M. and Alam, M. (2010) "Scalable, Privacy-Preserving Remote Attestation in and through Federated Identity Management Frameworks", *2010 International Conference on Information Science and Applications*, 2010, pp. 1-8, doi: 10.1109/ICISA.2010.5480294.

Arbaugh, W. A., Farber, D. J. and J. M. Smith (1997) "A Secure and Reliable Bootstrap Architecture", *in IEEE Computer Society Conference on Security and Privacy*. IEEE, 1997, pp. 65–71.

Arnautov, S., Trach, B., Gregor, F., Knauth, T., Martin, A., Priebe, C., Lind, J. Muthukumaran, D., O'Keeffe, D., Stillwell, M.L., Goltzsche, D., Eyers, D., Kapitza, R., Pietzuch, P. and Fetzer, C. (2016) "SCONE: Secure Linux Containers with Intel SGX", *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16)*, 978-1-931971-33-1, pp. 689-703, USENIX Association.

Asokan, N., Brasser, F., Ibrahim, A., Sadeghi, A.-R., Schunter, M., Tsudik, G. and Wachsmann, C. (2015) "SEDA: Scalable Embedded Device Attestation", *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*. Association for Computing Machinery, New York, NY, USA, pp. 964–975, doi: 10.1145/2810103.2813670

AWS (2022) "AWS Nitro Enclaves User Guide", Available at: https://docs.aws.amazon.com/enclaves/latest/user/enclaves-user.pdf (Accessed: 25 Jan 2022).

Baldwin, P., Lyon, R., Sindhuri, D., Coulter, D. and Vilaysim, S. (2021) "Microsoft Azure Attestation", Microsoft, Available at: https://docs.microsoft.com/en-us/azure/attestation/overview (Accessed: 25 Jan 2022).

Berger, B. (2005) "Trusted computing group history", Information Security Technical Report, Volume 10, Issue 2, 2005, pp. 59-62, doi: 10.1016/j.istr.2005.05.007.

Bienhaus, D., Ebner, A., Jäger, L., Rieke, R. and Krauß, C. (2021) "Secure gate: Secure gateways and wireless sensors as enablers for sustainability in production plants", *Simulation Modelling Practice and Theory*, Volume 109, 2021, doi: 10.1016/j.simpat.2021.102282

Birkholz, H., Thaler, D., Richardson, M., Smith, N. and Pan, W. (2021a) "Remote Attestation Procedures Architecture", work in progress, IETF RATS draft, Available at: https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/ (Accessed: 25 Jan 2022).

Birkholz, H., Eckel, M., Pan, W. and Voit, E. (2021b) "Reference Interaction Models for Remote Attestation Procedures", work in progress, IETF RATS draft, Available at: https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/ (Accessed: 25 Jan 2022).

Birnstill, P., Haas, C., Hassler, D. and Beyerer, J. (2017). "Introducing remote attestation and hardware-based cryptography to OPC UA", *22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1-8, doi: 10.1109/ETFA.2017.8247591.

Coker, G., Guttman, J., Loscocco, P., Herzog, A., Millen, J., O'Hanlon, B., Ramsdell, J., Segall, A., Sheehy, J. and Sniffem, B. (2011) "Principles of remote attestation", *International Journal of Information Security* 10, pp. 63–81, doi: 10.1007/s10207-011-0124-7.

Dahlmanns, M., Lohmöller, J., Fink, I. B., Pennekamp, J., Wehrle, K. and Henze M. (2020) ''Easing the conscience with OPC UA: An internet-wide study on insecure deployments,'' in Proc. ACM Internet Meas. Conf. New York, NY, USA: ACM, 2020, pp. 101–110, doi: 10.1145/3419394.3423666

Dushku, E., Rabbani, M. M., Conti, M., Mancini, L. V. and Ranise, S. (2020) "SARA: Secure Asynchronous Remote Attestation for IoT systems", *in IEEE Transactions on Information Forensics and Security*, vol 15, pp. 3123-3126, doi: 10.1109/TIFS.2020.2983282.

Eckel, M. (2021) "CHARRA: Challenge-Response based Remote Attestation with TPM 2.0", Sep. 2021, Available at: https://github.com/Fraunhofer-SIT/charra (Accessed: 25 Jan 2022).

Hovsmith, S. (2017) "Adapting OAuth2 for Internet of Things (IoT) API Security", blog article, Approov, Available at: https://blog.approov.io/adapting-oauth2-for-internet-of-things-iot-api-security, (Accessed: 25 Jan 2022).

IEEE1815 (2012) "IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," *in IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010)*, pp.1-821, doi: 10.1109/IEEESTD.2012.6327578.

Knauth, T., Steiner, M., Chakrabarti, S., Lei, L., Xing, C. and Vij, M. (2019) “Integrating Remote Attestation with Transport Layer Security”, arXiv:1801.05863.

Leicher, A., Schmidt, A. U., Shah, Y. and Cha, I. (2010) "Trusted Computing enhanced OpenID," *2010 International Conference for Internet Technology and Secured Transactions*, pp. 1-8.

Lu, Y. and Feng, T. (2018) “Research on trusted DNP3-BAE protocol based on hash chain”, *EURASIP Journal on Wireless Communications and Networking*, 108, doi: 10.1186/s13638-018-1129-y.

Lundblade, L., Mandyam, G. and O’Donoghue, J. (2021) “The Entity Attestation Token (EAT)”, work in progress, IETF RATS draft, Available at: https://datatracker.ietf.org/doc/draft-ietf-rats-eat/ (Accessed: 25 Jan 2022).

Matischek, R. and Bara, B. (2019) "Application Study of Hardware-Based Security for Future Industrial IoT," *22nd Euromicro Conference on Digital System Design (DSD)*, pp. 246-252, doi: 10.1109/DSD.2019.00044.

Mechalas, J.P. (2018) “Software Guard Extensions Remote Attestation End-to-End Example”, Intel code sample, Available at: https://www.intel.com/content/www/us/en/developer/articles/code-sample/software-guard-extensions-remote-attestation-end-to-end-example.html (Accessed: 25 Jan 2022).

Mulligan, D.P., Petri, G., Spinale, N., Stockwell, G. and Vincent, H.J.M. (2021) "Confidential Computing—a brave new world," *2021 International Symposium on Secure and Private Execution Environment Design (SEED),* pp. 132-138, doi: 10.1109/SEED51797.2021.00025.

Naik, N. and Jenkins, P. (2017) "Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect," *11th International Conference on Research Challenges in Information Science (RCIS),* pp. 163-174, doi: 10.1109/RCIS.2017.7956534.

OASIS (2005) “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”, OASIS Standard, March 2005, Available at: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf (Accessed: 25 Jan 2022).

OMG (2010), “The Real-time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol Specification (DDS-RTPS)”, Version 2.1, Available at: https://www.omg.org/spec/DDSI-RTPS/2.1/PDF (Accessed: 25 Jan 2022).

OPC (2017) “OPC UA - Part 7: Profiles”, Available at: https://reference.opcfoundation.org/Core/docs/Part7/ (Accessed: 25 Jan 2022).

OPC (2018) “OPC UA - Part 2: Security Model”, Available at: https://reference.opcfoundation.org/Core/docs/Part2/ (Accessed: 25 Jan 2022).

Pardo-Castello G. and Lang, U. (2013) “Trusted remote attestation for secure embedded systems”, Embedded.com, Available at: https://www.embedded.com/trusted-remote-attestation-for-secure-embedded-systems/ (Accessed: 25 Jan 2022).

Pasham, N. (2020) “Demystifying ARM TrustZone for Microcontrollers (and a Note on Rust Support)”, blog article, Medium, Available at: https://medium.com/swlh/demystifying-arm-trustzone-for-microcontrollers-and-a-note-on-rust-support-54efc62c290 (Accessed: 25 Jan 2022).

PJM (2020) “DNP SCADA over Internet with TLS Security”, Jetstream Guide, December 4, 2020, Available at: https://www.pjm.com/~/media/etools/jetstream/jetstream-guide.ashx (Accessed: 25 Jan 2022).

Pliatsios, D., Sarigiannidis, P., Lagkas, T. and Sarigiannidis, A. G. (2020) "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics”, *in IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942-1976, doi: 10.1109/COMST.2020.2987688.

Sailer, R., Zhang, X., Jaeger, T. and van Doorn., L. (2004) “Design and implementation of a TCG-based integrity measurement architecture”, *Proceedings of the 13th conference on USENIX Security Symposium*, Volume 13 (SSYM'04), USENIX Association, USA, 16.

Sandoval, K. (2017) “OAuth 2.0 – Why It’s Vital to IoT Security”, blog article, Nordic APIs, Available at: https://nordicapis.com/why-oauth-2-0-is-vital-to-iot-security/ (Accessed: 25 Jan 2022).

Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S. and Tschofeng, H. (2021) “Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)”, work in progress, IETF ACE draft, Available at: https://datatracker.ietf.org/doc/html/draft-ietf-ace-oauth-authz (Accessed: 25 Jan 2022).

Self, H. (2020) “Overview of DNP3 Security Version 6”, Available at: https://www.dnp.org/Resources/Public-Documents (Accessed: 25 Jan 2022).

Shelby, Z., Hartke, K. and Bormann, C. (2014), “The Constrained Application Protocol (CoAP)”, IETF RFC7252, Available at: https://datatracker.ietf.org/doc/html/rfc7252 (Accessed: 25 Jan 2022).

Upchurch, J., (2019) “DDS Security the Hard(ware) Way - SGX”, a three-part blog article, RTI, Available at: https://www.rti.com/blog/author/jason-upchurch (Accessed: 25 Jan 2022).

Suomalainen, J., Julku, J., Vehkaperä, M. and Posti, H. (2021) “Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions”, *in IEEE Open Journal of the Communications Society*, vol. 2, pp. 1590-1615, doi: 10.1109/OJCOMS.2021.3093529.

TCG (2019a) “TCG Remote Integrity Verification: Network Equipment Remote Attestation System”, Version 1.0, Revision 9b, June 15, 2019, Available at: https://trustedcomputinggroup.org/wp-content/uploads/TCG-NetEq-Attestation-Workflow-Outline_v1r9b_pubrev.pdf (Accessed: 2 Feb 2022).

TCG (2019b) “Trusted Platform Module Library Specification”, Family “2.0”, Level 00, Revision 01.59 – November 2019, Available at: https://trustedcomputinggroup.org/resource/tpm-library-specification/ (Accessed: 25 Jan 2022).

TCG (2020) “DICE Layering Architecture”, Version 1.0, Revision 0,19, July 2020, Available at: https://trustedcomputinggroup.org/wp-content/uploads/DICE-Layering-Architecture-r19_pub.pdf (Accessed: 25 Jan 2022).

TCG (2022) “TCG Guidance for Securing Industrial Control Systems Using TCG Technology”, Version 1.0, Revision 109, January 10, 2022, Available at: https://trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_Industrial_Control_Systems_v1_r109_pub10jan2022.pdf (Accessed: 2 Feb 2022).

Tygar, J. and Yee, B. (1991) “Dyad: A system for using physically secure coprocessor”, Technical Report CMU-CS-91-140R, Carnegie Mellon University, May 1991.

Yu, Y., Wang, H., Liu, B. and Yin, G. (2013) "A Trusted Remote Attestation Model Based on Trusted Computing," *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1504-1509, doi: 10.1109/TrustCom.2013.183.