IIC Endpoint Security Best Practices

IIC:WHT:IN17:V1.0:PB:20180312

Steve Hanna, Srinivas Kumar, Dean Weber

This document recommends best practices for endpoint[1] security in industrial applications under the broader scope of industrial internet security. By providing a concise description of the countermeasures needed to achieve a desired level of security for an endpoint whilst also achieving the appropriate safety, reliability, resilience and privacy, the reader can more easily apply existing best practices. The basis for this document is the detailed analysis in the various industrial guidance and compliance frameworks that already exist (IISF [IIC-IISF2016], Industrie 4.0 [Ind4.0-ITSec], IEC 62443 [IEC-62443-11], and NIST SP 800-53 [NIST-800-53r4] [NIST-800-53r5]). Subsequent IIC Best Practices documents are planned to cover other aspects of industrial internet security, based on the six building blocks in the *Industrial Internet Security Framework* (IISF). We do not cover related aspects of equipment safety or data privacy.

The intended audience includes industrial equipment manufacturers, integrators, and industrial equipment owners and operators. All can benefit by obtaining a clear description of what countermeasures and controls are generally recommended for each level of security. Equipment manufacturers and integrators can define which security level their products, systems, and solutions are designed to meet. Insurers and policy makers may benefit by having a common benchmark that can be used to analyze risk and encourage security improvements. And while this document is not intended as the basis for certification or as a checklist, certifying organizations may wish to review it as they develop their own certification programs.

The common uses of this document are illustrated in Figure 1:

Figure 1: Use of Endpoint Security Best Practices

[1] The IIC Vocabulary defines an *endpoint* as a "component that has computational capabilities and network connectivity". Thus endpoints may include edge devices (e.g., embedded medical devices, sensors and actuators in vehicle controls systems as well as pumps, heaters, and flow meters in manufacturing systems), communications infrastructure, cloud servers or anything in between.

While regulations may compel some organizations to comply with industrial security requirements, those who are not subject to regulation should still pay attention. Poor industrial security has direct negative effects such as safety problems and equipment damage, and indirect effects such as customer dissatisfaction, poor quality and reliability, possible liability, and eventually reduced profits. Conversely, good security can drive a virtuous cycle of reduced costs and increased reliability and safety.

The best practices listed in this document are horizontal, not tuned to the specific needs of one sector such as manufacturing or transportation. Readers may need to adjust these practices to reflect sector-specific requirements or regulations. Future editions of this document may contain sector-specific sections. Absent such guidance, these best practices provide field-tested advice that can be used across sectors, in conjunction with a careful risk analysis.

Because of the difficulty of modifying existing deployed endpoints to increase their security, this document is primarily targeted at new endpoints. However, some of the core concepts included here (e.g., tamper resistant change controls) may be valuable for legacy endpoints. Endpoints should include secure update capabilities but inevitably as endpoints age they will eventually become legacy endpoints. For legacy endpoints with inadequate security, other security measures such as network security must be employed.

RELATIONSHIP WITH OTHER IIC DOCUMENTS

The *Industrial Internet Security Framework* (IISF) provides a secure design architecture for industrial internet security so that system designers can understand overall security architecture and context. We will publish additional security best practices documents to cover other IISF domains such as data protection, communications and connectivity.

System designers can use this *Endpoint Security Best Practices* document to understand how controls can be applied to achieve a particular security level (basic, enhanced, or critical) when building or upgrading Industrial Internet of Things (IIoT) endpoint systems. The necessary security level is determined through risk modeling and threat analysis.

The *Security Maturity Model* is a separate approach for analyzing the security maturity of an organization. An organization operating at a high security maturity level uses an established process to assess risks, decide how they should be addressed, and apply the right level of security mechanism needed by the organization, industry and system. As part of this process, certain systems may be identified as especially threatened or critical and therefore meriting a higher security level. Appropriate countermeasures may then be selected, employing the best practices described here as a guideline.

The *IIC Vocabulary* [IIC-IIV2017] provides terminology and definitions for this document and other IIC documents. All acronyms are listed towards the end of the document and are hyperlinked in the text, marked with dotted underlines.[1]

SECURITY LEVELS

We define three levels of security: basic, enhanced, and critical. These levels correspond to security levels 2, 3, and 4 as defined in IEC 62443 3-3 [IEC-62443-33], chosen as one of the most mature of the industrial guidance and compliance frameworks dating back to ISA99's original work at the turn of the century. We do not describe best practices for security levels 0 and 1 in IEC 62443-3-3 as they cover low security environments, which is inappropriate for industrial internet environments. NIST SP 800-53r4 similarly defines three levels of security.

Security Level Basic (SLB) provides protection against "intentional violation using simple means with low resources", such as an ordinary virus. Security Level Enhanced (SLE) steps up to defend against "sophisticated means with moderate resources", such as exploiting known vulnerabilities in Industrial Control System (ICS) software or systems. Security Level Critical (SLC) steps up further to defend against attackers with "sophisticated means with extended resources", such as the ability to develop custom zero-day attacks. Each endpoint should have an appropriate level of security.

Operators must determine which level of security is required for their situation based on a careful risk assessment. The language used in these recommendations is similar to the control objectives of the various compliance frameworks, so follow-on matching of security recommendations against compliance or regulatory considerations is relatively straight-forward.

Vulnerability descriptions, threat descriptions, and risks differ widely by compliance or regulation type, although they do have common foundations. Discussions regarding vulnerabilities and threat models can be found in documentation such as NIST 800-82 *[NIST-800-82]* and IEC 62443 3-3.

Security does not stand alone but is interwoven with other system characteristics such as safety, privacy, reliability and resilience in the face of environmental disruptions, human errors, system faults and attacks. Trustworthiness is the degree of confidence one has that a system performs as expected with respect to these five characteristics. Choices made to attain one characteristic will have impact and influence on the others so solutions need to be devised iteratively and in concert to achieve the overall trustworthiness goals.

[1] We refer to multiple standards' development organizations most commonly known by their acronyms. These include International Standards Organization (ISO), Institute of Electrical and Electronic Engineers (IEEE), International Electrotechnical Commission (IEC), Internet Engineering Task Force (IETF) or National Institute for Standards and Technology (NIST).

SECURITY ARCHITECTURES

There are several full-stack architectures for endpoint security offering increasing security levels. They are based on open standards and interoperability between multi-vendor multi-platform endpoints across architectural patterns such as *three-tier*, *gateway-mediated edge*, or *layered databus*. Regardless of the architectural pattern employed, the endpoints must include resistance to attacks commensurate with the level of risk for those endpoints.

Figures 2, 3, and 4 show the countermeasures selected for the three security levels defined in this document: Security Level Basic, Security Level Enhanced, and Security Level Critical. The detailed rationale for why particular countermeasures are selected for a particular level of threat can be found in existing documents such as IEC 62443 and NIST SP 800-53.

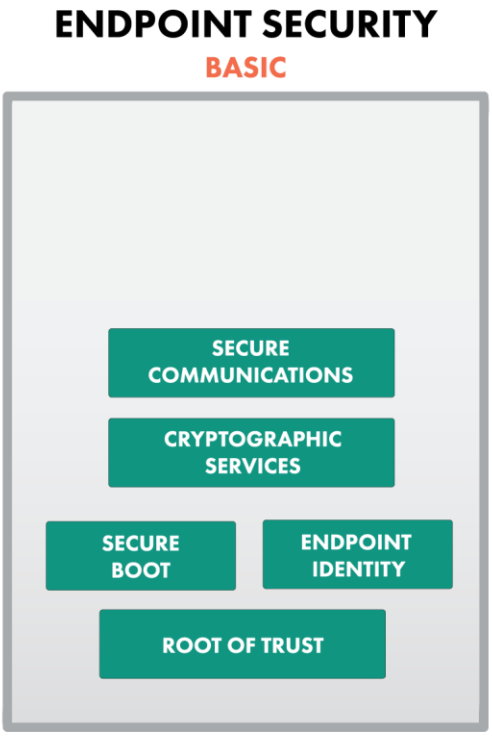

Figure 2: Security Level Basic

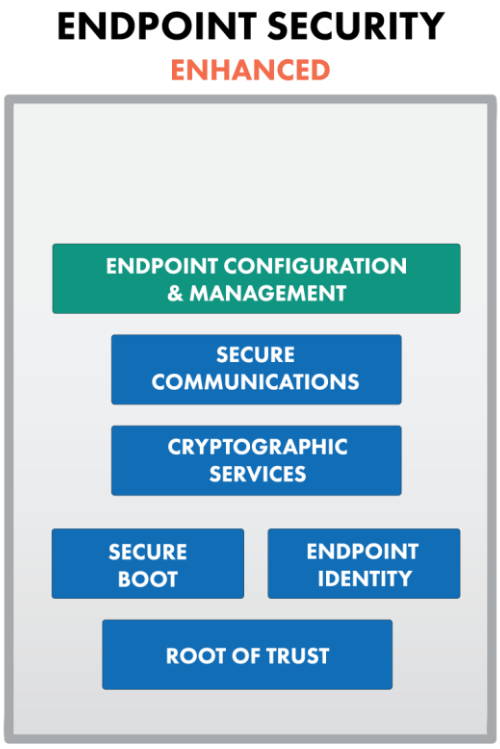

Figure 3: Security Level Enhanced

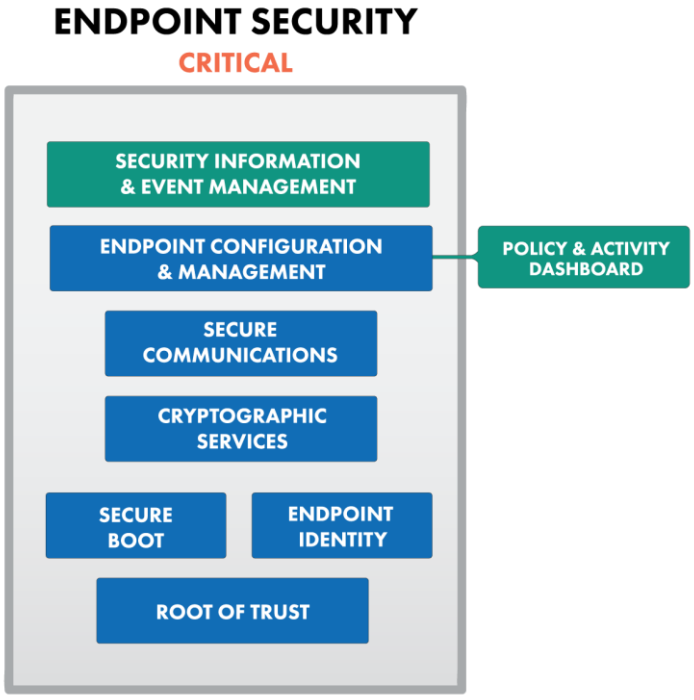

Figure 4: Security Level Critical

The following sections describe the elements of these architectures in more detail. Security requirements are marked with a grey background and followed by the security levels where they are required, in parentheses.

ROOT OF TRUST

Each endpoint contains a *Root of Trust* (RoT) that forms the basis for the endpoint's security, providing security functions such as:

- endpoint identity (SLB, SLE, SLC)[1]
- attestation of software and hardware identity and integrity (SLE, SLC)[2]

The strength of the RoT determines the level of trust attainable by the device. This strength depends on how the RoT is implemented (software, hardware, etc.). The RoT should be simple and well protected against compromise to ensure its integrity. For enhanced or critical security levels, the RoT should be implemented in hardware (SLE, SLC)[3]. In order to obtain protection against physical hardware tampering, a discrete hardware security chip or an integrated hardware security block with tamper resistance may generally be needed. The phrase "attestation of software and hardware identity and integrity" above means that a device can provide cryptographically protected information about its hardware and software version.

ENDPOINT IDENTITY

Endpoint identity is a fundamental building block essential for most other security measures. Public Key Infrastructure (PKI) support is mandatory for basic, enhanced and critical security levels, while other options may be used if necessary. Open standard certificate management protocols (e.g., EST) are used to automate the issuance, renewal, update and revocation of certificates issued by an internal or external certificate authority. (SLB, SLE, SLC)[4] Certificate chaining from the endpoint endorsement certificate provides supply-chain provenance for transfer of ownership to an endpoint management system.

---

[1] NIST description https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust
NIST SP 800-147, IEC 62443-3-3 section 5.7.3.1

[2] NIST SP 800-155

[3] [IEC-62443-33]: 5.7.3, 5.7.4

[4] [IEC-62443-31]: 3.1.4, 3.1.5, 3.1.6, 3.1.25, 3.1.26, 3.1.34, 5.4, 5.7, 5.10
[IEC-62443-33] 5.10.4, 5.11.4, 7.6
NIST 800-53r5: AC-6, AC-20, IA-3, SC-2, SC-7, SC-14, SC-29, SC-30, SC-44, CM-3, CM-5, IA-5, IA-8, IA-9, MA-4, SC-12, SC-17, SC-23, SC-24, SI-7
NIST 800-125 supplemental virtualization guidance

SECURE BOOT

Secure boot attestation of the firmware (immutable or cryptographically protected bootstrap code executed at power on) and UEFI or U-Boot bootloaders for multi-stage boot may be performed using PKCS standards based cryptographic key hashes. (SLB, SLE, SLC)[1] This extends the platform-level attestation from bootstrap to OS startup, and assists in the prevention of unauthorized firmware, bootloader or boot image updates over-the-air or over-the-network.

CRYPTOGRAPHIC SERVICES

Comprehensive endpoint security requires proper use and implementation of cryptography across transport protocols (data-in-motion), storage (data-at-rest), and applications (data-in-use). (SLB, SLE, SLC)[2] Confidentiality and integrity should be protected with:

- PKCS standards-based asymmetric and symmetric cipher suites, hashing functions, and random number generators of appropriate strength[3],
- NIST/FIPS standards-based validated cryptographic algorithm implementations,
- cryptographic algorithm agility with in-field upgrade capability, especially in light of the rise of quantum computing and the expected need to deploy post-quantum cryptography,
- dynamically deployed policy-based control of application use of cryptographic functions based on permissible cipher algorithms and suites and
- interoperability of cryptographic key types and certificates across multi-vendor systems, as needed to enable secure communications within an ecosystem.

While there may exist valid reasons in particular circumstances to ignore some of the recommendations in the immediately preceding bulleted list, the full implications must be understood and carefully weighed before choosing a different course.

ENDPOINT CONFIGURATION AND MANAGEMENT

Any remote or automated updates to the firmware, OS, configuration, or applications, must be verifiable without relying on blacklists and whitelists for scalability across millions of endpoints in the operational technology (OT) realm. This requires use of PKCS standards for data encryption

[1] NIST 800-147
NIST 800-53r5 SI-7
[2] [IEC-62443-33] 8.5
NIST Post-Quantum Initiatives NISTIR 8105
NIST 800-53r5 IA-3, SC-7, and throughout AC-x
[3] [NIST-800-57p1r4]

and certificate-based validation of signers (supply-chain provenance) and recipients (authorized endpoints) for secure end-to-end reliable content delivery with confidentiality and integrity in the update workflow. To perform scalable verification of firmware and software integrity, consistent implementation of remote attestation (e.g., TNC and TPM) is required across platforms from endpoint to cloud. (SLE, SLC)[1]

SECURE COMMUNICATIONS

A secure end-to-end communications protocol stack is required (SLB, SLE, SLC)[2], including as appropriate:

- support for extensible authentication protocols with endpoint level non-repudiation or authentication,
- support for cryptographically protected endpoint-to-cloud connectivity, when appropriate,
- support for cryptographically protected endpoint-to-endpoint connectivity (for example based on standards based group key PKI for key lifecycle management),
- trusted data transport based on secure public-private key pairs (PKI), and use of modern quantum resistant cipher suites,
- local endpoint firewall for network whitelisting and ingress/egress access controls,
- leveraging hardware for secure key store,
- interoperability across multi-vendor systems (based on relevant RFC specifications),
- complete suite of transport protocols relevant to the system (for example TLS, DTLS, SSH, IPsec, IKE, Wireless, GDOI), and
- compatibility with security mechanisms used by core connectivity protocols defined in the Industrial Internet Connectivity Framework [IIC-IICF2017] regardless of whether these mechanisms are implemented with open-source stacks or closed-source stacks.

CONTINUOUS MONITORING

Real-time and continuous monitoring of the endpoint is required (SLC)[3], including:

[1] NIST 800-53r5 CM-x, PM-9, PS-8, SI-12
NIST SP 800-12, 800-30, 800-39, 800-100
[2] IEC 62443 3-3: 5.10
NIST 800-53r5 AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SC-8, SC-12, SC-13, SI-4
[3] NIST 80053r5: CA-7, CA-7, CM-5, CM-8, CM-9, CM-11, IA-3, PL-8, RA-5, SA-10, SA-12, SA-22, SC-37, SI-2, SI-3, SI-7

- configuration controls to detect and prevent unauthorized changes that modify the behavior of the firmware, OS, or installed applications and
- application-level controls to detect and prevent unauthorized activities (e.g. use of insecure ciphers, hash algorithms) that compromise the confidentiality or integrity of data.

POLICY & ACTIVITY DASHBOARD

For visibility and control of remote distributed endpoints in the field, OT operators and administrators require (SLC)[1]:

- remote policy management to define security controls,
- policy orchestration across multiple endpoints for distribution and
- event data that provides context with totality, relevance, and timeliness for incident response.

SYSTEM INFORMATION & EVENT MANAGEMENT

For incident response and audits, event logs are required as a valuable input that can be used to measure and assess risks continually and mitigate threats. (SLC)[2] This requires the ability to:

- provision policy based risk monitoring profiles,
- distribute rules or manage behavioral analysis using open interfaces, data models or extensible formats (e.g. REST APIs, JSON) across industry sectors,
- trigger rules and feed behavioral analysis with contextual event related data and
- log the generated events to SIEM services and data historians in extensible formats (e.g. CEF, SNMP).

CONCLUSION

By describing best practices for implementing industrial security appropriate for agreed-upon security levels, this document empowers industrial ecosystem participants.

- Owner-operators can define and request the security that they need.
- Integrators can build systems that meet customer security needs efficiently.
- Equipment manufacturers can build products that provide necessary security features efficiently.
- Governments can drive adoption of best practices for industrial security.

[1] NIST 800-53r5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-9, CM-5, IA-2, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, SC-7, SC-13, SC-37

[2] NIST 800-53r5: AU-3, AU-6, MP-6, RA-5

- Insurers can provide incentives for stronger industrial security.

Through the use of best practices, improvements in industrial security can be achieved at substantially lower costs than through ad hoc approaches.

Over time, this document will be revised as best practices are improved.

ACRONYMS

CEF	Common Event Format
DTLS	Datagram Transport Layer Security
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards
GDOI	Group Domain of Interpretation
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IISF	Industrial Internet Security Framework
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISA	International Society of Automation
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
OCSP	Online Certificate Status Protocol
NIST	National Institute for Standards and Technology
OS	Operating System
OT	Operational Technology
PCR	Platform Configuration Register
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
REST	Representational State Transfer
RFC	Request For Comment (a series of standards from IETF)
RoT	Root of Trust
SIEM	Security Information and Event Management
SLB	Security Level Basic
SLC	Security Level Critical
SLE	Security Level Enhanced
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security

TNC	Trusted Network Communications
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface

REFERENCES

[Ind4.0-ITSec] IT Security in Industrie 4.0: Action fields for operators, November 2016, retrieved 2017-12-12 http://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/guideline-it-security-i40-action-fields.html

[IEC-62443-11] International Electrotechnical Commission: IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, 2009, retrieved 2016-09-02 https://webstore.iec.ch/publication/7029

[IEC-62443-31] International Electrotechnical Commission: IEC 62443-3-1:2013, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems, 2009, retrieved 2017-12-22 https://webstore.iec.ch/publication/7031

[IEC-62443-33] International Electrotechnical Commission: IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, 2013, retrieved 2016-09-02 https://webstore.iec.ch/publication/7033

[IIC-IICF2017] Industrial Internet Consortium (IIC): Industrial Internet of Things, Volume G5: Connectivity Framework, version 1.00, 2017-February-28, retrieved 2017-12-12 https://www.iiconsortium.org/IICF.htm

[IIC-IISF2016] Industrial Internet Consortium (IIC): Industrial Internet of Things, Volume G4: Security Framework, version 1.00, 2016-September-26, retrieved 2017-12-12 https://www.iiconsortium.org/IISF.htm

[IIC-IIV2017] Industrial Internet Consortium (IIC): Industrial Internet of Things, Volume G8: Vocabulary, version 2.00, 2017-July-19, retrieved 2017-12-12 https://www.iiconsortium.org/vocab

[NIST-800-53r4] National Institute of Standards and Technology (NIST): Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, 2013 April, retrieved 2016-09-02 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[NIST-800-53r5] National Institute of Standards and Technology (NIST): Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5, 2017-August, retrieved 2017-12-22 https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

[NIST-800-57p1r4] National Institute of Standards and Technology (NIST): Special Publication 800-57, Recommendation for Key Management Part 1: General Security, Revision 4, 2016-January, retrieved 2018-01-12 http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4

[NIST-800-82] National Institute of Standards and Technology (NIST): Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, revision 2, 2015-May, retrieved at 2016-09-02 http://dx.doi.org/10.6028/NIST.SP.800-82r2

AUTHORS AND LEGAL NOTICE

A publication of the Security Working Group, authored by Steve Hanna (Infineon), Srinivas Kumar (Mocana), and Dean Weber (Mocana).