Building trust in industrial IoT devices through standards, sharing and regulation

Version 1.0

Table of Contents

Our growing reliance on online services and Internet of Things (IoT) devices and ecosystems has increased our vulnerability to cyber threats. Strong cybersecurity measures are essential to protect against data breaches, identity theft, and financial loss, ensuring the safety of, and trust in, our online existences and the IoT ecosystems that sustain our offline lives.

Strong cybersecurity measures are increasingly being recommended or mandated by industry groups, standards committees and regulators as an important part of engaging in many market sectors. Strong cybersecurity measures are therefore increasingly being regarded as an important part of the added value of a product or service, rather than as a burdensome design overhead and ongoing administration challenge.

Fortunately, a combination of evolving standards, hardware and software innovations, the sharing of best practices, and developing regulation, is making it easier to achieve strong cybersecurity features in IoT devices. This is particularly true if an industrial IoT (IIoT) device's cybersecurity implementation can be based upon a root of trust embedded in the hardware, intelligently exploited by its embedded software, and managed through sophisticated tools.

1 The Cybersecurity Landscape

IoT devices and ecosystems are already subject to cybersecurity standards efforts and legislation, formulated in other contexts, to protect personal data and enforce product liability. IoT companies face serious financial and reputational risks if their work is non-compliant, with penalties that may include fines, personal liability for those who allow security breaches, as well as cease-and-desist orders, erasure of data, and product recalls. For example, the European Union's General Data Protection Regulation (GDPR) specifies fines of up to €20 million, or 4% of global turnover, whichever is greater, for misusing, or allowing the misuse of, personal data.

Other broad EU regulations also apply to the IoT. CE marking addresses the safety, health and environmental impact of products sold in the EU. The EU's Network and Information Security Directive applies to IoT providers designated as either an Operator of Essential Services such as gas, electricity and water, or a Designated Service Provider such as an online marketplace.

In the US, the Federal Trade Commission Act (FTCA), the Cyber Security Information Sharing Act (CISA), and the Children's Online Privacy Protection Act (COPPA), are all relevant to IoT deployments.

The FTCA regulates anti-competitive behavior, and the Commission has brought cases against IoT device makers that failed to ensure their products' security. Sanctions can include restitution payments, audits, product recalls, and lawsuits. Those who violate the FTCA may face fines of $41,484 *per violation, per day*.

CISA encourages the sharing of cybersecurity information and may relieve those who participate in its activities voluntarily of some potential legal liabilities.

Under COPPA, IoT providers should not knowingly collect children's data, should anonymize any data that they do collect, and ensure that any third parties that they work with do the same.

Three key acts apply in the UK: the Data Protection Act 2018 (DPA), the Consumer Rights Act 2015 (CRA), and the Digital Economy Act 2017 (DEA).

The DPA implements the GDPR in the UK. Companies in breach of the DPA can be searched, fined, and have their data forfeited or erased. Directors can be held liable.

The CRA defines digital content as 'data produced and supplied in digital form', which must be of 'satisfactory quality'. The implication is that IoT providers need to ensure their offerings work for years after they are sold, and that they may be held liable for the impact of low-quality digital content – such as devices shipped with malware.

The DEA has provisions relevant to suppliers of specific types of IoT goods and services, such as for use in digital infrastructure, which may also affect IoT providers that manage networks, or access to the internet and online content. IoT providers in the utility sectors are also subject to information-sharing and processing requirements under the DEA.

2 The Emergence of IoT-Specific Legislation

Legislation is constantly evolving to regulate the quality and security of IoT devices and IoT deployments.

2.1 European Union (EU)

On 21 March 2019, the European Union adopted the EU Cybersecurity Act. This gives ENISA, the European Union Agency for Cybersecurity, a permanent mandate. The Act also establishes an EU framework for cybersecurity certification, to improve cybersecurity in a broad range of digital products, including IoT devices and services.

On 12 March 2024, the European Parliament approved the Cyber Resilience Act (CRA), which says that IoT device makers must include cybersecurity measures throughout their products' lifecycles, from design through to maintenance. Key requirements include secure-by-design principles, regular updates, and rapid vulnerability management. The Act categorizes products into two classes, based on their risk levels, with stricter conformity assessments for higher-risk products. It also obliges companies to report cybersecurity incidents to ENISA. There is a detailed website for the CRA here.

The CRA's detailed measures cross over with those of other standards bodies including CEN, CENELEC, ETSI, ISO, IEC, and the ITU. The Commission and ENISA have produced a document that maps between the CRA's requirements and existing standards, available here.

A quick keyword search in this mapping document shows, for example, that ETSI EN 303 645, V2.1.1 (2020-06) already calls for cybersecurity provisions for consumer IoT devices, including the use of default passwords, secure storage of sensitive parameters and the management of credentials such as password generation, user authentication and change of default values.

Another search shows that section 3.1.6 of the CRA calls for the protection of "the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user". Among the techniques that should be applied are "symmetric or asymmetric encryption

schemes (including public key infrastructures (PKIs)) to ensure that the integrity of exchanged data is protected." Multiple existing standards call for similar facilities; the mapping guide's gap analysis shows where these efforts fall short of what is envisaged in the CRA.

2.2 United States (US)

In 2020, the US enacted the Internet of Things Cybersecurity Improvement Act. The Act mandates the publication of guidelines on the appropriate use and management of IoT devices, a review of agency information-security policies relating to the IoT, and the introduction of policies and principles as necessary. The Act also mandates the development of guidelines for sharing information about security vulnerabilities that could affect government agencies. And it says that agencies can't buy or use IoT devices if doing so would prevent compliance with the new standards and guidelines.

In May 2021, President Biden signed an Executive Order to further strengthen the US's cybersecurity and protect federal government networks. The Order calls for better information sharing between the government and private sector on security breaches, updated cybersecurity standards in the federal government, better software supply-chain security, the establishment of a cybersecurity review board and a standard approach to cyber incidents, and better detection of cybersecurity incidents on federal government networks.

The US National Institute of Standards and Technology (NIST) is developing guidance for IoT device makers, available in a series of Internal Reports (NIST IRs). For example, NIST IR 8259 covers "Foundational Cybersecurity Activities for IoT Device Manufacturers". It explicitly asks device makers to consider using a hardware root of trust to provide trusted storage for cryptographic keys and to enable secure boot strategies and the confirmation of device authenticity.

NIST IR 8259A defines an "IoT Device Cybersecurity Capability Core Baseline". And NIST IR 8425 refines this work to produce a "Profile of the IoT Core Baseline for Consumer IoT Products." This calls for IoT product developers to gather and document many aspects of their design, including "Trustworthiness and protection of software and hardware elements implemented to create the IoT product and its product components (e.g., secure boot, hardware root of trust, and secure enclave)."

2.3 United Kingdom (UK)

The UK Product Security and Telecommunications Infrastructure (Product Security) regime came into effect on 29 April 2024. It is meant to improve the security of consumer smart devices, particularly IoT devices, and to help protect the country's telecoms infrastructure.

There are three main provisions for consumer IoT devices. The first is a ban on the use of default passwords on new products, so consumers must set their own. The second requires that IoT device makers establish and maintain a public point of contact for the disclosure of security vulnerabilities. The third requires that IoT device makers tell consumers for how long their devices will continue to get security updates.

On the telecoms side, the PSTI regime aims to make it easier to introduce high-speed broadband and 5G networks, by speeding up the process for obtaining permissions and resolving disputes related to access and site installation. It also gives the UK government

powers to enforce security requirements on telecoms providers to protect networks from sophisticated cyber threats, for example by other countries.

The PSTI Bill is part of the UK's broader strategy to enhance digital security and infrastructure. This goes back to the launch of a National Cyber Security Strategy in 2016. The Strategy was followed up in 2018 with the publication of a Code of Practice for Consumer IoT Security, which set out the security principles that should be applied by manufacturers and others involved in the market. Among its provisions is one on securely storing credentials and security-sensitive data. It says:

> "Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable."

It goes on to argue that it is too easy to discover hard-coded usernames and passwords embedded in software, even if they have been obfuscated.

> "Security-sensitive data that should be stored securely includes, for example, cryptographic keys, device identifiers and initialization vectors. Secure, trusted storage mechanisms should be used."

While this Code of Practice was in development, the UK was also contributing to the development of a European standard, EN 303 645 for consumer IoT device security. There's a direct mapping between many of the guidelines in the UK Code and clauses in the EN 303 645 standard, to ease compliance.

Many of these 'contextual' regulations, standards and codes of practice assume that makers can implement robust security measures in their IoT devices that ensure their long-term compliance, without saying how to do so. In some cases, they suggest or mandate the use of security features, such as secure boot routines or authentication schemes, which can best be implemented using hardware roots of trust.

The advantage of a hardware root of trust is that it provides a unique, immutable and unclonable identifier that developers can use as the foundation of their approach to IoT security. Implementing such a root of trust can also prompt developers to improve the way they produce embedded code for IoT devices, by providing a more robust source of unique identifiers and high-quality randomness for use as seeds in the related cryptographic processes that protect the device. Shifting the root of the chain of trust that enables the secure management and updating of IoT devices on to the devices themselves enables a simpler but more effective approach to implementing and maintaining IoT device and ecosystem security.

3 The Industrial Internet of Things (IIoT)

Many of the concerns about the cybersecurity of the IIoT match those of the wider IoT ecosystem and specific markets such as the automotive or medical sectors. These include concerns about the creation, handling and storing of private data; the ability to communicate securely; the opportunities for mayhem if a device is hacked, and so on. The particular concern about the IIoT is that it often sits at the interface between what some call the operational technology (OT) of a business i.e. the equipment that controls industrial processes, and its information technology (IT) i.e. the computers and mobile devices through which the business operates. The fear is that connecting a company's IIoT estate to its IT systems in this way vastly increases the opportunities for misuse (the 'attack surface', in the

jargon). If your central payroll computers are vulnerable to a hacked sensor node that you've forgotten exists in a factory halfway around the world, you've got problems.

Consultancy McKinsey argues that this sort of concern about cybersecurity is holding back the development of the IoT and that if they were fully addressed, companies would spend between 20 and 40% more on it. It forecasts that the total available market for IoT equipment could be $500 billion by 2030, with $120 billion of that being spent by the manufacturing and industrial sector. If all cybersecurity concerns are successfully addressed, McKinsey says the IIoT sector could be worth $145 billion instead. This would make the IIoT the most valuable part of the whole IoT market. McKinsey asked IoT buyers and providers what they cared most about in the development of IoT systems and the joint top concerns, with 61% of those surveyed calling the issues critical, were privacy and 'digital trust', in other words the extent to which users felt that IoT systems could be relied on to work as planned and to be robust against accidental or deliberate misuse.

IoT regulators, standards bodies, and industry associations, are aware of the importance of cybersecurity for the safe and rapid development of the IIoT sector, and are developing standards, recommendations and guidelines designed to help IIoT suppliers and users to achieve effective cyber security. Many of these set IIoT issues in the wider OT context, with layered models that try to achieve robust security in every layer.

For example, NIST's *Guide to Operational Technology Security*, published in September 2023, "provides an overview of OT and typical system topologies, identifies common threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks."

The layered model it uses in the cybersecurity strategy it outlines is as follows:

- Layer 1 – Security Management
- Layer 2 – Physical Security
- Layer 3 – Network Security
- Layer 4 – Hardware Security
- Layer 5 – Software Security

The Guide says that hardware security protection mechanisms provide the foundation for supporting security and trust for the devices within an environment. It lists some of the hardware security capabilities available to enhance endpoint security including:

- Root of trust
- Monitoring and analysis
- Secure configuration and management
- Endpoint hardening
- Integrity protection
- Access control
- Device identity
- Physical security

In a later section (5.3.7.1) on Application and Infrastructure, The Guide recommends that "Organizations should consider the following endpoint security capabilities of the IIoT devices being deployed":

- Endpoint tamper resistance capabilities

- Endpoint root of trust
- Cryptographic techniques
- Capability to harden endpoints
- Endpoint identity
- Endpoint access control
- Endpoint integrity protection
- Endpoint data protection
- Endpoint monitoring and analysis
- Endpoint configuration and management

The Connectivity Standards Alliance, an industry group promoting open standards for the IoT, launched an IoT Device Security Specification 1.0 in March 2024. It's an effort to consolidate requirements from the three most popular baseline definitions of IoT cybersecurity from the United States, Singapore, and Europe, into one specification and certification program. You can ask for a download of the specs, as they relate to various aspects of the IoT, here. The Technical Requirements section of the IoT Device Security Specification Version 1.0 is written in the rather strident language of such documents, includes statements such as that:

- 5.1.1.1 Unique Identity **–** The IoT Device SHALL be uniquely identifiable for cybersecurity purposes.
- 5.2.1.1 Authentication for Configuration Changes – If the IoT Device makes or allows Security-Related Configuration changes, including Critical Security Parameters and passwords, via a network or other interface, the related configuration changes SHALL only be accepted after authentication and authorization. Best Practice Cryptography SHALL be used.
- 5.2.3.2 Security Best Practices – If the IoT Device makes use of Critical Security Parameters, including passwords, they SHALL conform with Security Best Practices, including, length, complexity, generation of keys from passwords, secure management processes, and secure storage. Best Practice Cryptography SHALL be used.
- 5.2.3.5 Cryptographic Agility – The IoT Device SHOULD support updating Cryptographic Algorithms and primitives.
- 5.4.1.1 Restricting Access to Security-Relevant Information **–** The IoT Device SHALL require authentication and authorization when exposing Security-Relevant Information via the network interfaces of the device.
- 5.4.1.2 Confidentiality Protection – The IoT Device SHALL, by default, ensure the confidentiality of Security-Relevant Information and Sensitive Data exchanged with IoT Devices and IoT Associated Services. Best Practice Cryptography SHALL be used.
- 5.4.1.3 Remote Trust Relationships – For two-way communication, the IoT Device SHALL establish a trust relationship ensuring that both parties at each end of a network connection are authenticated. Best Practice Cryptography SHALL be used.

This is just a sampling of the requirements that must be met to achieve certification to the IoT Device Security Specification. You can sense that much of the document is about codifying basic steps that designers should take (e.g. don't leave unused interfaces active, remember to validate all inputs), which are often overlooked. You can also see the emphasis

that the specifications' authors have attached to the use of up-to-date cryptography to enable authentication and to protect information at rest or on the move in IoT ecosystems.

Back in September 2021, cloud services provider AWS published a much less formal *Ten security golden rules for Industrial IoT solutions*. Number three on its list is another take on this imperative, arguing for the use of hardware to provide an anchor or root for cybersecurity tools such as authentication schemes and cryptography:

- Provision modern IIoT devices and systems with unique identities and credentials and apply authentication and access control mechanisms
- Assign unique identities to modern IIoT devices such that when a device connects to other devices or cloud services, it must establish trust by authenticating using principals such as X.509 certificates, security tokens or other credentials.
- Create mechanisms to facilitate the generation, distribution, rotation, and revocation of credentials.
- Establish Root of Trust by using hardware-protected modules such as Trusted Platform Modules if available on the device.
- Ensure least-privilege access controls for OT/IIoT devices, edge gateways and agent software accessing local and cloud resources.
- Avoid hard coding or storing credentials & secrets locally on OT/IIoT devices.
-

The Industry IoT Consortium, another body which is trying to accelerate the uptake of the IIoT and which has just merged with the Digital Twin Consortium, has produced its own guidance for endpoint security in IIoT applications. It defines three levels of security: basic, enhanced, and critical, which correspond to security levels 2, 3, and 4 as defined in IEC 62443 3-3. It then defines the endpoint security functions needed to meet each level of threat:

- To counter *basic* threats, endpoint security functions should include:
    - Root of trust
    - Secure boot
    - Endpoint identity
    - Cryptographic services
    - Secure communications
- To counter *enhanced* threats, add:
    - Endpoint configuration and management
- To counter *critical* threats, add:
    - A policy and activity dashboard connected to the Endpoint configuration and management system
    - Security information and event management

The guidance then elaborates on each of these functions.

The *Root of Trust (RoT)* provides security functions such as:

- Endpoint identity
- Attestation of software and hardware identity and integrity

The strength of the RoT determines to what extent the device can be trusted and depends on how it is implemented. 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**.** 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."

Endpoint identity is essential for most other security measures. Public key infrastructure (PKI) support is mandatory.

Secure boot attestation of the firmware and bootloaders for multi-stage boot may be performed using PKCS standards based cryptographic key hashes. This extends the platform-level attestation from bootstrap to OS startup, and helps prevent unauthorized firmware, bootloader or boot image updates.

Cryptographic services: Comprehensive endpoint security requires proper implementation of cryptography across transport protocols, storage, and applications.

4 Conclusion

The introduction of billions of low-cost IoT devices to the internet has only increased the security challenge. Governments, international standards bodies, industry groups and more are now moving quickly to make IoT implementations more trustworthy. This is being addressed through the development of checklists, guidelines, standards, business processes, certification schemes, and legislation.

Certain application areas, including the industrial sector, are getting specific standards, regulation, and best practice guides, reflecting their sensitivity and vulnerability. The rapidly evolving nature of the industrial market, and of the threats to which it could be subject, mean that the standards and regulatory landscape will continue to develop for some time to come. The challenge for the IIoT is to ensure make its cybersecurity is robust enough, and perceived to be robust enough, for organizations to allow their OT systems to be intimately connected to their IT systems.

The good news is that all the activity surrounding the industrial sector, the wider IoT, and general cybersecurity issues, is helping to build the sense that IIoT networks will soon be much more trustable. What is sometimes missing from these approaches is a strong way of knowing that the devices that populate an IIoT ecosystem are genuine and still under the control of the people who introduced them to the Internet. This can only be achieved through hardware by embedding a unique and immutable identifier within a chip in every device, whose presence can be used to verify the device's unique identity and so provide the foundation for a chain of trust that protects an organization's OT and the IT systems to which it is connected.