Building trust in IoMT security 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 IoT 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) 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 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 devices enables a simpler but more effective approach to implementing and maintaining IoT device and ecosystem security.

3 Medical Devices

Medical devices must comply with the regulations and guidelines described above, as well as a thicket of national and international regulations, standards and other guidelines to be certified as safe for use in the management of human health. When these devices gain an Internet connection and become part of 'the Internet of Medical Things (IoMT)', the concerns multiply. They include:

- Cybersecurity risks, such as hacking, which could change the device's functionality, endangering patients' lives, or subject their most sensitive data to misuse.

- Patient safety, for example by making an IoMT device less resilient because part of its functionality has been passed to cloud services whose accessibility is subject to the reliability of a network connection.

- Regulatory compliance, including full adherence to multiple standards that may be evolving, as well as the costs and complexity of achieving full validation and verification.

- Interoperability issues, such as integrating with arbitrary existing healthcare systems and other medical devices to achieve easy data exchange.

- Data management issues that are common in many other IoT contexts, but with the added challenge of handling large volumes of ultrasensitive personal health data.

- Enhanced product liability issues for medical device makers, caused by the additional complexity brought on by adding Internet connectivity to medical devices.

- Maintenance and software update issues, which present a particular challenge for devices that are in daily use.

Medical device makers already must comply with multiple standards, and slightly differently drawn regulations in different countries and regions. Here are some which are relevant to IoMT devices and deployments.

3.1 European Union (EU)

Medical Device Regulation 2017/745

- Governs the safety and performance of medical devices in the EU. Annex 1 of the regulation, on general safety and performance requirements, focuses on reducing patient risk. It says in part: “Risk control measures adopted by manufacturers for the design and manufacture of the devices shall conform to safety principles, taking account of the *generally acknowledged state of the art.*” [Author’s emphasis.]

It also suggests, in a section on ‘electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves’, that “manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access, necessary to run the software as intended.”

In Vitro Diagnostic Regulation

- Regulates in vitro diagnostic devices within the EU. Borrows much of the language and intent of the Medical Device Regulation.

GDPR

- Comprehensive data protection and privacy regulation for all EU citizens.

NIS Directive

- Focuses on improving the cybersecurity of networks and information systems in the EU.

Radio Equipment Directive

- Standards for devices using radio frequencies in the EU.

3.2 United States (US)

Federal Food, Drug, and Cosmetic Act (FD&C Act)

- The main law under which the FDA regulates medical devices.

Food and Drug Administration (FDA) - Medical Device Cybersecurity Guidance

- Guidelines for ensuring cybersecurity in medical devices. Section 524B(a) of the FD&C Act says that IoMD developers need to give regulators information that shows that their device, among other requirements, 'design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available post-market updates and patches to the device and related systems."

Health Insurance Portability and Accountability Act

- Establishes national standards for the protection of health information. Under its security standards for the protection of electronic protected health information, Section 164.312 of the Act's technical safeguards says that entities must implement proper access controls, use encryption, run audit logs, have policies that stop health information from being altered or destroyed, have schemes for authenticating users, secure the health data when it is being transmitted, among other requirements. Although these regulations were enacted some years ago to cover large-scale health information systems, they apply to IoMT devices and ecosystems.

21st Century Cures Act

- Promotes the use of digital health technologies while ensuring safety.

CISA

- Facilitates cybersecurity threat information sharing between government and private sectors.

3.3 United Kingdom (UK)

UK Medical Devices Regulations (UK MDR 2002)

- Governs the regulation of medical devices in the UK, including adaptations post-Brexit.

DPA

- UK law that works alongside the GDPR to ensure data protection.

NIS Regulations

- Implements the EU's NIS Directive in the UK, focusing on cybersecurity.

Radio Equipment Regulations 2017

- Governs the use of radio equipment in the UK, including connected medical devices.

International Medical Device Regulators Forum

- A consortium of medical device regulation bodies, which published "Principles and Practices for Medical Device Cybersecurity" in March 2020. Among the recommendations of its section on cybersecurity, the guide says designers should consider how communications between devices/systems will authenticate each other; whether encryption is required; and how unauthorized replay of previously transmitted commands or data will be prevented.

The best approach to authentication for IoMT devices and ecosystems appears to remain an open question. A 2022 paper entitled ***Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues***, by academics at King Abdulaziz University and King Khalid University in Saudi Arabia, published in *Applied Science,* conducted a systematic review of IoMT authentication schemes. The authors reviewed 118 published papers to understand the schemes available and to produce a taxonomy. They found that most schemes relied on a distributed authentication architecture and public key infrastructure, with hybrid cryptography becoming popular to overcome the shortcomings of a single cryptographic approach. They concluded by arguing that IoMT authentication schemes need to go beyond identifying IoMT entities to the system, to support mass scalability, and end-to-end, cross-layer, and cross-domain authentication.

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 medical devices which are now becoming part of IoMT deployments, are getting specific standards, regulation, and best practice guides, reflecting their sensitivity and vulnerability. The rapidly evolving nature of the IoMT market, and of the threats to which it could be subject, means that the standards and regulatory landscape will continue to develop for some time to come.

The good news is that all the activity surrounding the IoMT, the wider IoT, and general cybersecurity issues, is helping to build the sense that IoT networks will soon be much more trustable. What is missing from these approaches is a strong way of knowing that the devices that populate an IoT 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 the IoMT devices and the ecosystem of which it is a part.