Building trust in automotive cybersecurity 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 (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 Internet of Automotive Things

The challenge of securing cars from cyberattack is growing due to changes in the way they are designed, made and used. These include:

- Complexity: a modern vehicle may include more than 100 microcontrollers, whose functions are closely coupled and strongly connected
- A strong requirement for systems to analyze and act in real time
- A requirement to enable secure firmware updates in the field – for years after sale

- A Requirement to support multiple interfaces, ranging from the automotive CANbus standard right through to consumer Bluetooth, cellular, and Wi-Fi links
- The uptake of 'drive by wire' strategies, which replace a direct mechanical linkage between driver input and vehicle response with sensors and actuators
- Electrification, which has increased the complexity of onboard electronics, boosted competition and so shrunk the time to market for new models
- The push for vehicle autonomy, which further increases system complexity while making the costs of security breaches much higher
- V2X strategies, which involve vehicles becoming connected to other vehicles, roadside infrastructure, home energy systems, the power grid, infotainment service providers, etc.

As in many other markets, car makers must abide by, and respond to, a wide variety of standards, codes of practice, and regulations, which, together, seek to protect users from cybersecurity breaches. These documents offer advice which ranges in detail from outlining an ambition to providing hard advice about achieving and sustaining vehicle cybersecurity.

ISO 26262 is a standard that requires car makers to think about the functional safety of their vehicles, i.e. how they will respond if something goes wrong. It defines the extent to which functional safety has been considered and addressed through a set of four Automotive Safety Integrity Levels. Properly applied, meeting the requirements of ISO 26262 means embedding consideration of the risks of failure throughout the entire automotive lifecycle, from design to decommissioning.

SAE International's J3061_202112 *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* is a handbook of best practices for establishing and maintaining cybersecurity in what it calls 'cyber-physical vehicle systems'. This includes:

- Defining a lifecycle framework that can be tailored to an organization's development processes to incorporate cybersecurity measures throughout a vehicle's conceptualization, design, production, operation, service, and decommissioning.
- Providing information on common tools and methods used when designing, verifying and validating cyber-physical vehicle systems.
- Providing basic principles on cybersecurity for vehicle systems.
- Providing the foundation for further standards development activities in vehicle cybersecurity.

ISO 21434 takes the story on from J3061, focusing on communications within the vehicle, such as between its engine control units. The standard aims to encourage car makers to define cybersecurity policies and processes, manage cybersecurity risk, and foster a cybersecurity culture that understands and controls cyber risks.

The US Department of Transportation's National Highway Traffic Safety Administration has published a document entitled *Cybersecurity Best Practices for the Safety of Modern Vehicles*, which covers similar ground. In a brief section on cybersecurity (8.2) it says:

> "Cryptographic techniques should be current and non-obsolescent for the intended application.

> "While the selection of appropriate cryptographic techniques is an important design criterion, it should be noted that implementation issues often determine any system's security.
>
> "Cryptographic credentials help mediate access to vehicle computing resources and back-end servers. Examples include passwords, PKI certificates, and encryption keys.
>
> "Cryptographic credentials that provide an authorized, elevated level of access to vehicle computing platforms should be protected from unauthorized disclosure or modification."

In a further section on software updates (8.8) it recommends:

> "Automotive manufacturers should employ state-of-the-art techniques for limiting the ability to modify firmware to authorized and appropriately authenticated parties."
>
> It goes on to comment that "firmware updating systems which employ signing techniques could prevent the installation of a damaging software update that did not originate from an authorized source."

The document's emphasis on using modern cybersecurity techniques, and the importance of how they are implemented, is a reminder that cybersecurity strategies are only as good as their weakest link. Hardware roots of trust, which provide a connected device with a unique and immutable identity, can provide the firmest of foundations for an automotive cybersecurity strategy.

The United Nations Economic Commission for Europe (UNECE) working party #29 (WP.29) has also put forward regulations R155 and R156, which focus on automotive cyber security and cyber security management systems. They are meant to protect vehicles against cybersecurity threats and require countermeasures that underpinned by effective cryptographic protections.

For example, in R155, Table A1 in Annex 5 lists cyber threats and corresponding mitigations. Among these threats are '4.3.7 - Potential vulnerabilities that could be exploited if not sufficiently protected or hardened'. It lists the related attack methods as:

- Combination of short encryption keys and long period of validity enables attacker to break encryption
- Insufficient use of cryptographic algorithms to protect sensitive systems
- Using already or soon to be deprecated cryptographic algorithms

In Table B1, the regulation lists threats and mitigation related to vehicle communication channels. In section 4.2 of the table, it outlines the charmingly named 'Sybil attack', in which a threat actor spoofs the appearance of multiple other vehicles on the road to overwhelm a vehicle's systems. As mitigation it says, 'Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)'. There are similar calls to use strong cryptographic functions to protect the integrity of software providers that are providing software updates, and to prevent the extraction of cryptographic keys.

UNECE Regulation R156 focuses on protecting software updates and software update management systems. In the lengthy list of general specifications that a vehicle maker must meet to gain approval to R156, the regulation says:

"Security - the vehicle manufacturer shall demonstrate:

- The process they will use to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated
- The update processes used are protected to reasonably prevent them being compromised, including development of the update delivery system
- The processes used to verify and validate software functionality and code for the software used in the vehicle are appropriate."

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 automotive sector, are getting specific standards, regulation, and best practice guides, reflecting their sensitivity and vulnerability. The rapidly evolving nature of the automotive 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 good news is that all the activity surrounding the automotive sector, 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 automobile and the ecosystem of which they are a part.

Among the advantages of establishing a hardware root of trust in automotive applications are:

Protection against cyber threats including:

- Host processor compromise
- Non-volatile memory key extraction
- Test and debug interface attacks
- Side-channel and perturbation attacks
- Manufacturing facility compromise

Securing critical systems, such as:

- V2X communication
- Advanced driver-assistance systems
- Infotainment systems

Safeguarding supply chains:

- Ensuring integrity of components across fragmented production sites

Compliance with safety standards, such as:

- ISO 26262 compliance for functional safety

As vehicles become more complex, the need for a firm foundation for cybersecurity strategies will only strengthen.