Forming a Security Foundation for Trustworthiness in IoT Infrastructures

Dr. Stephan Spitz[1], Haydn Povey[2], and William Payne[3]

[1]Senior Director Technologie, G+D Mobile Security GmbH
[2]CEO securethingz/IAR and Founder securethingz
[3]IoT M2M Council

Abstract

It's quite common now to read studies and forecasts predicting hundreds of billions of IoT devices in a few years. Indeed we may not be far off this, especially when on a daily basis we see new ideas, prototypes and field-trials leveraging the benefits of highly connected sensors and actuators in verticals such as smart cities, smart agriculture, supply chain management and many more areas of daily life.

For a security expert this dynamic can appear scary, knowing how quickly the attack surface and vulnerability of crucial infrastructures grows with all these billions of new IoT endpoints. This article outlines an overview of technologies to mitigate these risks and activities that standardization bodies, governments and industry groups are carrying out to harmonize risk mitigation measurements.

European IoT Regulations

A number of countries and economic blocs have instituted, or are in the process of instituting, regulations to govern cyber security of IoT devices.

The European Union has already one major directive in place that affects how firms and organisations in certain sectors regulate and protect IoT based infrastructure. This is the Network and Information Security Directive, commonly shortened to the NIS Directive, or NISD.

As a directive of the EU, it requires being passed into each member state's legislation. Out of the 28 members of the EU, only six have legislated it into law, despite a May 2018 deadline to do so.

The NIS Directive can incur stiff penalties for failure either to protect infrastructure adequately, or for late or confused reporting of data breaches to national regulators. It means that an attack on IoT infrastructure within sectors such as energy, healthcare, gas and oil, or transport could incur large fines if the regulators judged that such an attack was reasonably preventable. It is likely that attacks that replicate the patterns, attack surfaces or vectors of previous attacks would be considered reasonably preventable under the directive.

The United Kingdom, which has passed NISD into law, has established fines up to £17 million for failures to protect infrastructure adequately. Denmark, another country to legislate NISD into law, has instituted fines up to €5 million.

The NIS Directive affects operators of critical infrastructure. It includes health, energy, banking, telecommunications and transportation, utilities, and operators of other essential services. The directive includes operators of online electronic platforms, and covers cloud computing providers, search engine operators and digital marketplaces.

Of particular relevence to IoT vendors and operators, the NIS Directive covers cyber attacks involving malware on physical infrastructure, such as energy grids, hospital systems, transportation networks, oil rigs, water and sewage systems, etc.

It also covers security and data loss involving banking, shopping, or travel apps used on mobile devices. Indeed, any data loss or data breach involving a cloud service falls under its remit.

While the NIS Directive affects IoT devices employed in certain, critical, sectors, by way of being a part of essential infrastructure, the EU is also looking a more broad ranging legislation to regulate IoT devices directly: the EU Cybersecurity Bill.

The EU Cybersecurity Bill also differs from the NIS Directive in being a bill not a directive. That means it will come directly into force across all EU member states, rather than relying on potentially diffident interpretations at national parliament stages.

The EU Cybersecurity Bill would create a single certification scheme for data and information devices. The stated intention of the bill is to create trust in IoT based products, and encourage the creation of a single EU digital marketplace, including IoT devices and services.

The bill also intends to bolster the position of ENISA, the EU Agency for Network and Information Security, making it a permanent EU-wide cybersecurity agency.

This is a contentious proposal. At present, ENISA is a panel of experts drawn from different member states that acts in an advisory capacity to both the Commission and to member states on cybersecurity matters.

The bill would elevate ENISA from an advisory position to a certification authority from the whole of the European Union. ENISA would become responsible for certifying IoT products across all current 28 member states.

Certification of IoT devices under the Cybersecurity Bill would test security compliance of data collected or transmitted by devices. This would include the security of data availability, authentificity, integrity and confidentiality. It includes processed data, as well as the services and functions of that data offered by devices. As such, it must include the mobile and telecommunications infrastructure, cloud processing and storage of IoT device data as well as the devices themselves.

US IoT Regulatory Efforts

The focus of this paper is on developments within the European Union. However, the EU is not alone in developing IoT focused cybersecurity regulations and legislation.

A bipartisan bill, the IoT Cybersecurity Improvement Act, was introduced to the US Senate by Cory Gardner and Mark Warner in July 2017. The bill was described by Warner in an interview with Reuters as "the lightest touch possible". The bill is currently stuck in committee stage.

A second bipartisan bill, the IoT Consumer Tips to Improve Personal Security Act, was introduced by Roger Wicker and Maggie Hassan to prompt the US Federal Trade Commission to act on IoT cybersecurity with effective guidance to consumers in December 2017.

In September 2018, California became the first US state to pass into law an IoT cybersecurity bill. SB-327 requires manufacturers to equip IoT based devices with "reasonable" security features. These features must prevent unauthorised access, modification or data breach.

International IoT Regulatory Efforts

China enacted a new Cyber Security Law in 2016, which came into force in June 2017. The law places obligations on "Critical Information Infrastructure Operators" (CIIOs) to maintain privacy and protection of both personal and "critical" data, however collected. This would include data collected from mobile devices, such as personal identification data, and would also cover data collected from health care devices.

Critical data is more ambiguous. It is defined as data relating to defence, economic development, or the public interest. As such, it would seem to include data collected, processed and stored from critical infrastructure such as telecommunications, energy, utilities and transportation. However, it could also cover data from manufacturing systems, logistics and supply chains, as these also would relate to economic development and public interest.

The Chinese regulatory environment for IoT is still evolving, with definitions of general principles in the CS Law, and accompanying directives, promised to be defined in due course.

Japan has a Cybersecurity Act that dates to 2014. In 2018, the country's government announced a new Cybersecurity Strategy. This is aimed at raising awareness among Japanese companies of the risk of cyberattacks, and advocates that companies should prioritise the defence of their assets. It offers tax breaks to those companies making investments in defending their IT and operational technology assets.

Singapore has enacted the Cybersecurity Act (CSA), which came into effect in February 2018. This act defines a framework for regulating cyber-defence of critical infrastructure, and authorises the Cyber Security Agency of Singapore to prevent and respond to cyber attacks and incidents.

The act promulgates an approach of "security by design". Critical infrastructure operators are required to put in place mechanisms to detect and report cybersecurity threats.

Risk and Liability in context of IoT

The main aim of implementing security measurements is to reduce vulnerability and increase robustness and availability of IoT infrastructures. With the knowledge that 100% security is impossible (attacks will happen), there's a need to strike a balance – between the level of investment in security, and dealing with the impact of an attack. This balancing act is quite difficult, especially as new IoT solutions are showing up at a fast pace in many different verticals.

In addition, in many cases the impact of an attack is underestimated when new IoT solutions emerge. For example, cheap connected light bulbs might at first glance not appear to be a significant target for an attacker. Taking a closer look, these light bulbs are connected to an energy grid and might eventually form a path in the whole power management infrastructure of a smart city. As a result, a security vulnerability in the light bulb could enable a hacker to gain control over a large portion of crucial infrastructure.

Governments and regulatory bodies are aware of such risks and have already started work on security certification schemes for critical IoT infrastructure. For example, the EU Cybersecurity act demands a security assessment of every IoT infrastructure depending on the criticality according to a “basic”, a “substantial” or a “high” evaluation scheme. In order to obtain this kind of certification system (see figure 1), it is clear that industry, standardization bodies and regulatory authorities need to collaborate closely.

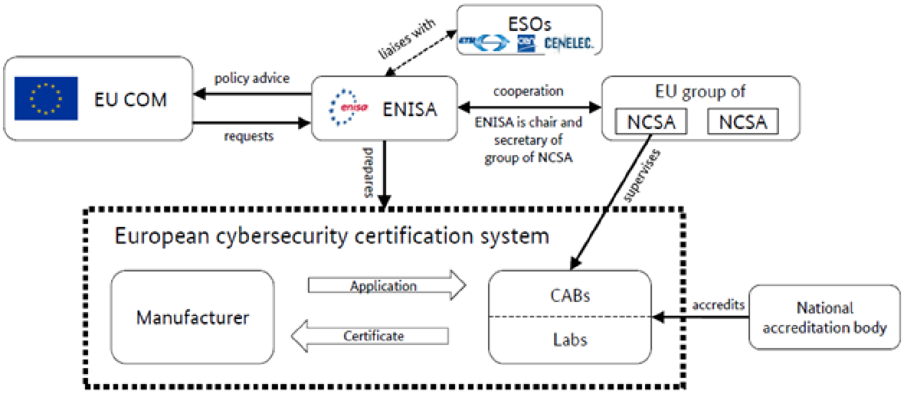
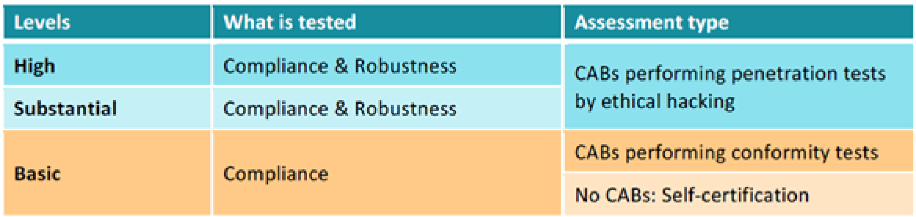


Fig. 1 Stakeholder within the EU Cybersecurity Act according the German Federal Office for Information Security

Such certification schemes help provide industry alignment – giving manufacturers guidance on security-hardened products, and also helping to reduce liability with their IoT products and solutions. This is important in cases such as the light bulb manufacturer, who can be held liable for an attack impacting the whole power infrastructure of a city resulting from an attack via its light bulbs.

Measurements and Technologies to mitigate risk and liability

One common factor in all guidelines, certification schemes and regulations to ensure IoT security is the importance of considering security policies early in the design and development phase of IoT infrastructure and devices. In fact, the review of the security design plays an important role in all certification schemes. According to the EU Cybersecurity Act, such a review can either be self-assessed for the lowest "basic" grade, or a CAB (Certification Assessment Body) can be involved to provide an independent assessment.



Levels	What is tested	Assessment type
High	Compliance & Robustness	CABs performing penetration tests by ethical hacking
Substantial	Compliance & Robustness	
Basic	Compliance	CABs performing conformity tests
		No CABs: Self-certification

Fig.2 Different levels of certification of IoT devices according the EU Cybersecurity Act

During the design phase of an IoT device the most important aspect is the choice of a robust root- of-trust, which forms the trust anchor for the life-cycle management of the device and the whole service infrastructure in which the IoT device is integrated. The requirements of different regulations including the EU Cybersecurity Act demands such a root-of-trust in every IoT endpoint fulfilling a higher security level – either directly or indirectly. This trust foundation is essential to safeguard the boundaries of the infrastructure, which are formed by the endpoints as highlighted in the light bulb example.

Importance of a Root-of-Trust in the IoT endpoint

A root-of-trust gives an IoT endpoint a unique identity while also providing the security anchor for data and control services within the infrastructure via that endpoint. As a result, this root-of-trust can be the trust foundation for the following security critical services:

- Authorization of access to the endpoint e.g. for maintenance of the endpoint such as FUOTA (Firmware Update Over-the-Air)
- Ensuring integrity of the endpoint's firmware and if necessary confidentiality of data stored on the endpoint
- Protection of malware intrusion and theft or loss of data
- Assigning an identity to the endpoint, which can be used in IoT management infrastructure and assigned to data generated by this endpoint
- Tunnel endpoint in conjunction with cryptographic protocols such as TLS (Transport Layer Security) or DTLS (Dynamic TLS).
- Obfuscation of data or the endpoint identity for privacy protection in the infrastructure in case the endpoint is assigned to a person
- Protection of the endpoint manufacturer against overproduction and counterfeiting and helping manage software releases and updates.

It is obvious that such a root-of-trust needs to be established in a secure manner otherwise an attacker can misuse this process to place a backdoor to the whole IoT infrastructure.

A root-of-trust typically consists of security critical low-level code in conjunction with cryptographic keys, which are protected in a hardware security enclave. These cryptographic keys have to be personalized in a secure process as close as possible to manufacturing line. The earlier this happens in the manufacturing process of the IoT device the broader the foundation for security is. In the best case this is close coupled to the silicon manufacturing process of the IoT device's System-on-Chip (SoC).

It is widely acknowledged in the security industry that strong security mechanisms have to be based on hardware, because software can be always circumvented by software. By establishing trust as an inherent part of the IoT device's SoC, it is possible to provide some confidence that the whole infrastructure is based on a secure foundation.

A very efficient way to establish such a root-of-trust is in conjunction with the design process of IoT device hard- and software. Specialized development tools allow streamlined security development by addressing the following aspects early in the IoT device design stages:

- Identity management of the IoT device
- Scalable Secure Boot Manager for flexible Service configuration
- Secure deployment in the manufacturing line including key personalization
- Multiple eye principle for the mastering of the manufacturing line provisioning process
- FUOTA and Release management with versioning and update infrastructure

Conclusion

The rapid growth of IoT infrastructure connected via many billion endpoints poses increased levels of risk. These risks can be addressed by governmental and certification bodies as well as by security technologies from different suppliers. Both have to go hand-in-hand to guarantee robustness of the IoT infrastructure and secure the technology investment. Given all the government initiatives and the choice of technologies, it is important at the same time to try and avoid fragmentation.

Regulation of IoT devices, and penalties for failure to defend adquately IoT assets connected to critical and industrial infrastructure, are increasingly being put into place in different regions around the world.

In this article, we showed that a common root-of-trust established early in the life cycle of the IoT device directly at SoC level can help go a long way towards achieving security technology convergence.

In addition, the harmonization of governmental initiatives is essential, especial an international recognition of the different certification schemes of National Accreditation Bodies. This gives the necessary assurance to IoT technology and solution vendors, infrastructure operators and companies in different verticals to invest in security and so reduce the liability.