Internet of Things (IoT) Security

GFCE Global Good Practices

GFCE
Global Forum on Cyber Expertise

CSA SINGAPORE

Ministry of Economic Affairs and Climate Policy

TNO innovation for life

Preface

The Internet of Things (IoT) is changing the way people live, do business, and interact with their governments. The IoT's massive interconnections of devices, or "things", lead to new efficiencies and capabilities and unlock tremendous value for consumers, organizations and governments. These technologies can improve government operations, support better living, create new business opportunities, and support stronger and safer communities.

But these advantages come with enormous challenges. Consumer privacy and safety can be undermined by the vulnerability of individual devices, connectivity and back-end infrastructure, and the wider economy faces an increasing threat of large scale cyber-attacks launched from large numbers of insecure IoT devices. By some measures, at this moment less than 4% of IoT devices are secure by design[1]. For IoT to be successful, useful and acceptable, the hazards that come with the introduction of IoT must be managed to risk levels acceptable to society.

The process of establishing an IoT security policy and living up to it in the long term should be based on evidence and experience. Resources, while plentiful, are often difficult to decipher and digest. The good practices in this document are based on previous research and literature reviews and augmented by interactive sessions and expert meetings such as GFCE's 2018 IoT Security Roundtable[2], during which experts and policymakers from organizations including Singapore's Cyber Security Agency[3], the Ministry of Economic Affairs of the Netherlands[4], the Netherlands National Cyber Security Center[5], and the U.K. Department for Digital, Culture, Media and Sport[6] were consulted and surveyed.

[1] IoT Security: From Design to Lifecycle Management, ABI Research, 2017
[2] https://www.sicw.sg/iot
[3] https://www.csa.gov.sg/
[4] https://www.government.nl/ministries/ministry-of-economic-affairs-and-climate-policy
[5] https://www.ncsc.nl/english
[6] https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport

Table of Contents

1. Introduction

What is the Internet of Things?

According to the Internet Engineering Task Force (IETF)[7], "the Internet of Things (IoT) refers to devices, that are often constrained in communication and computation capabilities, now becoming more commonly connected to the Internet, and to various services that are built on top of the capabilities these devices jointly provide. It is expected that this development will usher in more machine-to-machine communication using the Internet with no human user actively involved."

IoT deals with uniquely-identifiable, resource-constrained devices that measure and possibly control their environments and communicate over networks using standard protocols. All IoT devices include sensors to collect information from the environment: these might be temperature sensors, motion sensors, air quality sensors, or light sensors, to name a few. Some devices may also contain actuators, which are entities responsible for moving or controlling a system or mechanism. Devices also contain power supplies, often batteries. There is necessarily a module that provides connectivity, although the nature of this connectivity varies widely. There is also a certain amount of processing power provided by a microcontroller unit, some storage capacity, and often a minimal operating system and an application running on it.

As discussed, IoT devices are often resource-constrained. With IoT devices we do not have the luxury of measuring memory in gigabytes, nor of measuring processing power by number of cores. Most IoT devices have a microcontroller rather than a full-fledged microprocessor, and speeds in megahertz rather than gigahertz. Additionally, IoT devices may have physical constraints imposed by the operational environment, e.g. pacemakers within the human body.

Why is IoT security important?

Attacks on critical IoT devices, such as connected cars and medical devices, can target the device itself and disrupt its integrity or availability, endangering the user of the device and potentially those in the vicinity[8]. Since many IoT devices are closely coupled to the physical world, the threat to human beings includes physical harm. For less critical IoT devices, such as thermostats or cameras, a major threat is device compromise, where the devices become part of a botnet to support DDoS attacks, spam bots or ransomware campaigns. The Mirai[9] botnet and an evolved version of Mirai called Reaper[10] showed how such large-scale cyberattacks can cascade into national security threats. Finally, for all types of IoT devices,

[7] https://www.ietf.org/topics/iot/
[8] Baseline Security Recommendations for IoT, ENISA, Nov 2017
[9] Mirai IoT Botnet Co-Authors Plead Guilty - https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/
[10] The Reaper IoT botnet has already infected a million networks - https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/

the potential loss of confidential information via the device, its communication infrastructure, or its back-end servers remains a significant threat[11].

IoT Security vs IT Security

In accordance with the above discussions of IoT, we exclude devices that typically require human interaction such as mobile phones and computers. While IoT security and IT security share many fundamental principles, it is inadvisable to apply IT security classifications and mindsets directly to the IoT world [12]. The following considerations apply:

1. IoT devices are often constrained in terms of resources and/or physical environments. This significantly alters the manner in which security is designed; for instance, IoT connections cannot generally rely on TLS for encrypted and authenticated communications because many IoT devices do not have the resources to handle session establishment, communication overheads, or encryption.
2. IoT devices may run without supervision, and for extended periods of time. Many might have zero or limited user interfacing. Thus, patching and updating may not be practical and malfunctioning or rogue devices may not be immediately detectable.
3. The fact that IoT is closely integrated with the physical world increases the impact that cyberattacks may have. While traditional IT cyberattacks could result in data leakage and financial losses, IoT cyberattacks have the potential to cause grievous physical harm.

Moreover, conventional IT security has historically relied on fortifying a "perimeter". In previous decades, organizations could easily define and visualize this perimeter, and create a protection policy to enforce and protect its obvious boundaries. Enterprises still commonly secure corporate networks using the familiar baseline measures of the firewall, the demilitarized zone (DMZ), and some variety of intrusion detection system (IDS). However, each wave of innovation in the digital age has diluted the notion of the perimeter[13]. Network protocols themselves were enabled to allow applications to traverse through the firewall and run on external machines (for example, JavaScript™). Cloud computing has moved storage and computation from the traditional datacenter to third-party servers. IoT potentially takes both client device and server back-end out of the no-longer-defined perimeter[14]. The absence of a perimeter heightens the need to secure IoT devices, back-ends and connectivity.

[11] Baseline Security Recommendations for IoT, ENISA, Nov 2017
[12] ITU-T Y.4806, Security capabilities supporting safety of the Internet of things
[13] IBM Red Paper, Understanding IT Perimeter Security
https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf
[14] https://www.networkworld.com/article/3223952/internet-of-things/5-reasons-why-device-makers-cannot-secure-the-iot-platform.html

2. Good Practices

The practices described in this guide, while relevant on an individual basis, also form a process or a flow that policymakers can follow in order to achieve a secure IoT environment. IoT security needs to be based upon fundamentally sound cybersecurity principles. In order to achieve security in practice, these principles must lead to concrete guidelines and standards. Standards can be used as a basis for evaluation and certification, and in turn these certifications should be legally mandated and backed by governmental legislation. Owing to the inadequacy of IoT security legislation today and a lack of consumer awareness, there is currently no real incentive for IoT vendors to spend on security in a fast-moving industry where time-to-market, usability and cost are key considerations and margins are razor-thin. Finally, since IoT is by definition a global phenomenon and is not limited by national boundaries, it is further essential to align country-specific legislation and adopt a global approach to IoT security.

This leads to five good practices that are detailed below; the practices may be summarized visually as shown in Figure 1. Many challenges continue to exist; some of these are detailed in the subsequent section.

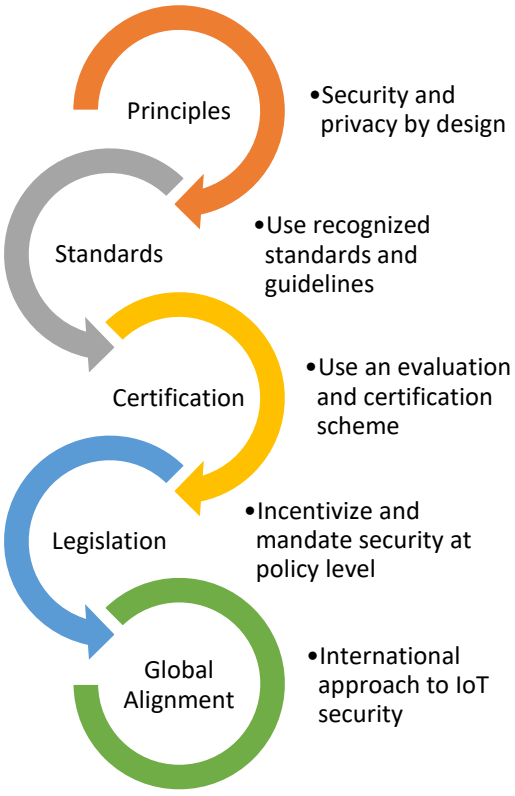

Figure 1: Steps to IoT Security

Good Practice 1: Security and Privacy by Design

It is necessary to identify fundamental security principles in order to build cybersecurity and privacy by design into IoT devices. While much of this knowledge does exist in the context of IT systems and solutions, there is a gap in relation to the move towards increasingly connected and interdependent systems and devices.[15]

Several organizations including ABI Research[16] and OWASP[17] have discussed the principles behind IoT security. OWASP, in particular, presents[18] a comprehensive list of principles to follow when designing for secure IoT. Some of these principles include:

1. **Assume a Hostile Edge**
    - Edge components are likely to fall into adversarial hands. Assume attackers will have physical access to edge components and can manipulate them, move them to hostile networks, and control resources such as DNS, DHCP, and internet routing.
2. **Test for Scale**
    - The volume of IoT means that every design and security consideration must also take into account scale. Simple bootstrapping into an ecosystem can create a self-denial of service condition at IoT scale. Security countermeasures must perform at volume.
3. **Exploit Autonomy**
    - Automated systems are capable of complex, monotonous, and tedious operations that human users would never tolerate. IoT systems should seek to exploit this advantage for security.
4. **Protect Uniformly**
    - Data encryption only protects encrypted pathways. Data that is transmitted over an encrypted link is still exposed at any point it is unencrypted, such as prior to encryption, after decryption, and along any communications pathways that do not enforce encryption. Careful consideration must be given to full data lifecycle to ensure that encryption is applied uniformly and appropriately to guarantee protections. Encryption is not total - be aware that metadata about encrypted data might also provide valuable information to attackers.

Besides the above, several organizations including the U.S. Department of Homeland Security[19] and the U.K. Department of Digital, Culture, Media & Sport (DCMS)[20] have defined concise IoT security principles such as "reducing the burden on consumers" which leads to convenient and automated updates and patching, and "ensuring resilience" which encompasses vulnerability management, incident response and

[15] ITU-T Y.4806, Security capabilities supporting safety of the Internet of things
[16] IoT Security from Design to Lifecycle Management, An Embedded Perspective; ABI Research, 2018.
[17] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
[18] https://www.owasp.org/index.php/Principles_of_IoT_Security
[19] Strategic Principles for Securing the Internet of Things, U.S. Dept of Homeland Security, 2016
[20] Secure by Design: Improving the cyber security of consumer Internet of Things. Policy report UK Government, March 2018.

recovery. The following good practices rely on carefully-chosen principles; each subsequent activity should tie back to at least one of the principles.

Further, it is important to educate manufacturers and developers as well as consumers regarding the need for security in IoT devices. Most IoT consumers do not have a basic understanding of their IoT devices and the impact on their physical environment – this awareness needs to be created. On the other hand, companies should train their employees[21] in good security practices, recognizing that technological expertise does not necessarily equate with security expertise.

Good Practice 2: Use Recognized Standards and Guidelines

Standards development organizations (SDOs) such as ITU[22], NIST[23], ETSI[24], IETF[25], and ISO[26] develop standards intended for global adoption. Most SDOs have begun IoT initiatives, generally focusing on the full space of IoT challenges including business cases and interoperability but often addressing IoT security as well[27]. DCMS UK, the EU Agency for Network and Information Security (ENISA), and the Alliance for IoT Innovation (AIOTI) have specifically released recommendations, guidelines or best practices for IoT security.

UK DCMS Code of Practice[28]

DCMS UK has proposed a code of practice for the security of consumer IoT products and associated services. Many severe cyber security issues stem from poor security design and bad practice in products sold to consumers. The guidance is listed in order of importance and, according to DCMS, the top three should be addressed as a matter of priority.

1. No default passwords,
2. Implement a vulnerability disclosure policy,
3. Keep software updated,
4. Securely store credentials and security-sensitive data,
5. Communicate securely,
6. Minimize exposed attack surfaces,
7. Ensure software integrity,
8. Ensure that personal data is protected,
9. Make systems resilient to outages,
10. Monitor system telemetry data,

[21] Future Proofing the Connected World, Cloud Security Alliance, 2016
[22] https://www.itu.int
[23] https://www.nist.gov/
[24] http://www.etsi.org/
[25] https://www.ietf.org/
[26] https://www.iso.org
[27] 'Summary literature review of industry recommendations and international developments on IoT security', PETRAS, 2018 https://www.gov.uk/government/publications/secure-by-design
[28] Code of Practice for Consumer IoT Security, DCMS UK, October 2018.

11. Make it easy for consumers to delete personal data,
12. Make installation and maintenance of devices easy,
13. Validate input data.

ENISA Security Recommendations

The baseline security recommendations for IoT from ENISA[29] include a number of policy, organizational and technical measures. Technical measures include the use of a hardware-based immutable root of trust, and security features such as specialized security chips / coprocessors that integrate security at the transistor level providing trusted storage of device identity, protecting of keys at rest and in use, and preventing unprivileged access to security sensitive code. The overwhelming breadth and depth of coverage make this inventory impressive, but at the same time it may be difficult to implement in practice, especially given the cost and resource constraints of IoT devices.

Good Practice 3: Use An Evaluation and Certification Scheme

It is important to use globally-recognized cybersecurity evaluation and certification regimes for IoT devices. Certification plays a critical role in increasing trust and security in products and services that are crucial for a digital economy. Without a common certification framework, there is an increasing risk of fragmentation and barriers in the market. A comprehensive certification framework or self-certification solution for IoT devices does not yet exist. Given that a system of secure components is not by definition a secure system, evaluation and certification regimes should include individual components, the wider network of systems and components, and the global ecosystem.

EU Cybersecurity Certification Framework

The European Union has proposed an EU Certification Framework[30] for ICT security products. The proposed certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. This will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards. While the use of certification schemes will be voluntary for the time being, the framework does avoid multiple certification processes in different Member States and creates an incentive to certify the quality and verify the security of the products and services in question.

IoT Security Foundation Compliance Framework

The IoT Security Foundation's (IoTSF) IoT Security Compliance Framework[31] is one of the first attempts to consistently evaluate the security of IoT devices. In order to make the framework more practical across a range of applications, IoTSF adopts a risk-based approach derived from the commonly used CIA Triad.

[29] ENISA 'Baseline Security Recommendations for IoT', November 2017
[30] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[31] https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

The framework defines five Compliance Classes that achieve progressively higher levels of Confidentiality, Integrity and Availability as depicted in the below table.

- Class 0: where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or organization
- Class 1: where compromise to the data generated or loss of control is likely to result in no more than limited impact on an individual or organization
- Class 2: in addition to class 1, the device is designed to resist attacks on availability that would have significant impact on an individual or organization, or impact many individuals. For example by limiting operations of an infrastructure to which it is connected
- Class 3: in addition to class 2, the device is designed to protect sensitive data including sensitive personal data
- Class 4: in addition to class 3, where compromise to the data generated or loss of control have the potential to affect critical infrastructure or cause personal injury

For instance, a thermostat is considered to fall under Class 1 since

- it does not store sensitive or personally-identifiable information
- it needs to report accurate data and external tampering with data values could result in business impact
- individual device unavailability would have little impact but a DoS of multiple devices could result in significant business impact

In order to evaluate the security of a given product, a risk assessment is conducted on the product in the target environment (Figure 2) in order to determine the applicable Compliance Class. Based on the determined Compliance Class, a checklist of requirements is to be filled in. Such a completed checklist could be made mandatory by procuring parties, as could a third-party audit to verify compliance with the checklist. This compliance framework forms a possible basis for a comprehensive certification scheme.

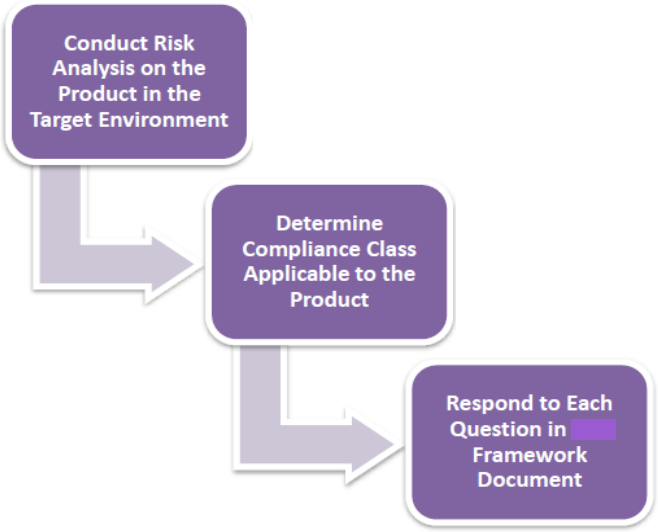

Figure 2: IoTSF Steps for Compliance (Source: IoTSF Compliance Framework)

Common Criteria

Traditional IT products, such as firewalls and switches, are routinely subjected to Common Criteria (CC) evaluations using independent laboratories. Certificates are issued by participating national governments and recognized by signatories worldwide. The CC allows product developers to document their product's Security Functional Requirements (SFRs) in a Security Target (ST). An independent laboratory can conduct a CC evaluation to assess the product against the SFRs.

The flexible nature of CC evaluations allows each developer to choose the SFRs against which their product is evaluated, but this flexibility can make it difficult to compare similar products. For example, two firewall vendors could choose different SFRs and yet market their products as having achieved Common Criteria certification. To address this, Protection Profiles (PPs) exist for some types of common IT products. Each PP includes a set of SFRs along with specific test and assurance requirements. Products submitted for PP-based CC evaluations must exhibit exact conformance with the PP.

Signatories to the CC Recognition Agreement (CCRA), such as the Netherlands, Singapore, the United States, the United Kingdom, Australia, Canada, Japan and India, all recognize CC certification[32] and specifically the collaborative Protection Profiles (cPPs)[33]. The cPP for Network Devices v2.1[34] seems to be the profile to build on for IoT Security; however, it is noted that this cPP lacks IoT-specific criteria pertaining to, for example, device resource constraints and the heterogeneity of devices and network environments.

In theory, the CC approach would allow an IoT product developer to demonstrate that their product meets specific security functional requirements. Having said that, CC certifications tend to be elaborate

[32] https://www.csa.gov.sg/programmes/csa-common-criteria
[33] https://www.commoncriteriaportal.org/pps/?cpp=1
[34] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf

and expensive to implement and the suitability of CC for rapidly-deployed, low-cost IoT devices remains an open question.

Good Practice 4: Incentivize and Mandate Security at Policy Level

There is no point in having a certification scheme if vendors have no reason to get their products certified. Clearly, IoT certification needs to be made either worthwhile or compulsory. Had there been genuine consumer demand for certified products, vendors would have been obliged to undertake certification activities. However, the reality is that most consumers globally do not know or care enough to demand certified IoT devices and pay a premium for them. It is also pertinent to note that an attack may not perceptibly affect the consumer at all – e.g. a home camera being used as part of a botnet might not lead to a noticeable change in its functioning.

One option for policymakers is to simply make certifications mandatory. Some governments, such as the United States and Singapore, already have such requirements for their own procurement. Another option is to modernize liability laws that require manufacturers to prove in the event of a breach that they were not negligent. In the case of *strict* liability, the manufacturer may be held liable for a defective product even if the manufacturer was not negligent in making that product defective. The manufacturer thus becomes a de facto insurer against its defective products, with premiums built into the product's price. It may be noted that liability laws do exist in virtually every country in the form of consumer protection laws or domain-specific regulations, but they are mostly designed for non-connected products and almost invariably need to be revamped for modern IoT environments.

While cybersecurity legislation is gradually being implemented by policymaking bodies around the world, there is very limited legislation specific to IoT security. We examine a few initiatives below.

U.S. IoT Cybersecurity Improvement Act of 2017

For years, cybersecurity experts have asked the U.S. government to improve cybersecurity and use its buying power to push through new security standards.[35] The IoT Cybersecurity Improvement Act[36] is a bill mandating minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies. This can be a way to raise the bar across the industry more easily than larger, more direct legal measures. U.S. Government-purchased IoT devices would need to:

- Be free of known security vulnerabilities, as defined in the NIST National Vulnerability Database.
- Have software or firmware components that accept “properly authenticated and trusted” patches from the vendor.
- Uses acceptable standards for communication, encryption, and interconnection with other devices or peripherals (which means that feeble old Telnet would not acceptable as an administrative mechanism).

[35] https://www.wired.com/2008/08/securitymatters-0807/

[36] https://www.congress.gov/bill/115th-congress/senate-bill/1691/text

- Not include any “fixed or hard-coded” credentials (that is, passwords) used for remote administration, delivery of updates, or communications.
- Have notification and disclosure methods in place for discovered security vulnerabilities.
- Be patched or have security vulnerabilities removed in a timely manner.

The legislation would also require government agencies to set inventories of IoT devices and update them every 30 days. Agencies would be required to publicly disclose which IoT devices have gone out of support and which have liability protections.

California Senate Bill 327

California's SB 327 law[37], approved in September 2018 and due to take effect in January 2020, requires all "connected devices" to have a "reasonable security feature." Security experts point out that the law is well-intentioned and while it may not actually solve the problems that plague IoT security[38] [39], it is nevertheless a good start.

Privacy regulations

From 2018 onwards, IoT stakeholders, including those in the supply chain, must be compliant with the General Data Protection Regulation (GDPR) in Europe and with similar privacy laws such as PDPA (Personal Data Protection Act) in Singapore. Personal data should be collected and processed fairly and lawfully, and never collected and processed without the data subject’s consent. Personal data should be used for the specified purposes for which they were collected. IoT stakeholders should comply with applicable privacy regulations. Users of IoT products and services should be able to exercise their rights to information access and erasure.

EU Cybersecurity Act

In December 2018, the European Union passed the Cybersecurity Act[40] to reinforce the mandate of the EU Agency for Cybersecurity, (European Union Agency for Network and Information and Security, ENISA) so as to better support Member States with tackling cybersecurity threats and attacks. As referenced above, the Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices – although, as noted previously, certification is voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to satisfy a specific security need. It is also noted that this Act is not specific to IoT security, although it does cover IoT products.

[37] http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[38] https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html
[39] https://www.zdnet.com/article/first-iot-security-bill-reaches-governors-desk-in-california/
[40] https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

Good Practice 5: International Approach to IoT Security

IoT security is a fundamentally global problem and demands a global solution. Numerous large-scale initiatives, alliances, pilots and testbeds focused on IoT security have been started in the last few years by various countries, consortia and organizations. Notable initiatives include the Alliance for IoT Innovation (AIOTI)[41], the IoT Security Foundation[42], the Industrial Internet Consortium[43], and ITU-T Study Group 20 on IoT and Smart Cities[44]. While most of these are global in terms of membership, there is a distinct skew towards Europe and America. Furthermore, industry players appear to be significantly more cooperative than nation-states – government involvement is limited, particularly for non-European initiatives. Global governmental initiatives are necessary in order to achieve any measure of IoT security, since connected devices can reach (and be reached from) any corner of the globe. Furthermore, many devices use components that are manufactured in a different country – this makes international alignment even more essential. The abovementioned EU Cybersecurity Act is a good example of international collaboration in the field of cybersecurity. Outside Europe, however, such collaborations are rare.

The GFCE itself provides a unique global platform for countries, international organizations and private companies to exchange best practices and expertise on cybersecurity, with the aim of identifying successful policies, practices and ideas and multiplying these on a global level. This makes the GFCE a suitable forum for aligning IoT security best practices across nations and governments.

[41] https://aioti.eu/
[42] https://www.iotsecurityfoundation.org/
[43] https://www.iiconsortium.org/
[44] https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx

3. Key Challenges

Key Challenge 1: Liability and Supply Chain

Modern products are assemblies of parts supplied by multiple vendors. To accelerate time-to-market and to reduce costs, device manufacturers increasingly use as many as possible off-the-shelf components and contract manufactured parts. Consequently, the role of suppliers and the supply chain is gaining prominence.

However, the increased numbers of external parties in the manufacturing process has been an unfortunate enabler for IP theft and cloning. The danger lies in original designs meant for critical and functional safety applications being used to create low-quality or possibly even compromised devices. By some estimates, up to 80% of breaches may originate in the supply chain[45]. The cloning of electronic devices is widespread and especially problematic in supply chain manufacturing[46].

In 2011, the Semiconductor Industry Association estimated[47] the cost of electronics counterfeiting at US$7.5 billion per year in lost revenue. Device compromise in transit and component-level vulnerabilities are other supply chain risks that can lead to devastating consequences.

Manufacturers' liability will play a crucial role in maturing security implementations throughout the supply chain. This will allow security to be priced into the product, and company business models will change accordingly.

Liability issues need to be addressed in the context of global and national legislation and case law. Where gaps are identified in said legislation, these should be addressed. The challenge is to identify the responsible entities and hold them liable. This is a supply chain management challenge in a global market.

Key Challenge 2: Fragmented Approach

Currently, there is no common approach to cybersecurity in IoT. The overwhelming number of standards and guidelines including those released by ENISA, AIOTI, IoTSF, DCMS and many others is likely to intimidate manufacturers; indeed, according to ENISA[48], most companies and manufacturers are taking their own approach when implementing security into IoT rather than following common standards and good practices, causing interoperability issues between devices from different manufacturers, and between IoT devices and legacy systems.

The fragmentation of regulations also poses a barrier when Critical Information Infrastructures are seen hand in hand with the IoT world, since there is no regulation that forces security measures and protocols

[45] Combatting Cyber Risks in the Supply Chain - https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252
[46] IoT Security: From Design to Life Cycle Management, ABI Research, 2017
[47] https://www.semiconductors.org/news/2011/11/08/news_2011/sia_president_testifies_at_senate_armed_services_committee_on_dangers_of_counterfeit_chips/
[48] ENISA 'Baseline Security Recommendations for IoT', November 2017

in the different levels of an IoT ecosystem, including the devices, the network, and the back-end. Conversely, the application of one-size fits all standards across the IoT ecosystem might be seen as a hindering factor for innovation and research in the area. One needs to also consider the fact that different application areas have diverse security requirements.

While standards are generally appreciated and supported by the industry, different stakeholders have different R&D chains and this inherently drives fragmentation in industry-developed standards. This may be overcome by nation-states and government bodies who can drive collaboration. The procurement process is another means to harmonize standards and requirements for IoT systems, as seen in the case of the U.S. Cybersecurity Improvement Act[49] discussed earlier in this paper.

Key Challenge 3: Lifecycle Management

It is necessary to incorporate secure lifecycle management to control massive numbers of connected IoT devices throughout their (extended) lifespan. IoT devices and products will have to evolve in a secure way to consistently provide, through their whole lifecycle, the solution for which they were created. IoT devices should ideally be patched and updated securely and regularly[50] with verified software/firmware to ensure their correct operation and to amend the vulnerabilities that are continuously being discovered. Given that most IoT users do not have an understanding of their IoT devices and their impact on their environment and may never manually update their devices, this places heavy responsibilities on vendors, and may lead to unique situations when vendors themselves go out of business or stop supporting certain products. Manufacturers must consider end-of-life issues ahead of time and communicate to manufacturers and consumers their expectations regarding the device and the risks of using a device beyond its usability date.[51]

As ABI Research identifies[52], lifecycle device management offers manufacturers the ability to continue providing value long after a device has been sold and even re-sold; however, that management service only has value if it can be tied securely back to the device. Without this process, any future service provisioning for the device post-market is vulnerable. The increased recognition that the IoT opportunity cannot be realized without trust is a significant driver for market adoption.

In addition, best practices for IoT deployment should be defined. These may include recommendations for specific configurations of devices and networks or the need to implement cybersecurity monitoring systems to detect anomalies in the deployed infrastructure[53].

The growth of IoT has led to the emergence of cloud-based IoT platforms from many cloud service providers (CSPs) such as Amazon's AWS, Microsoft Azure and Google Cloud. Most of these offer comprehensive device management functions, e.g. registration/enrollment, identity management, provisioning, permissions, monitoring and troubleshooting, status queries, and over-the-air (OTA)

[49] https://www.congress.gov/bill/115th-congress/senate-bill/1691/text
[50] Code of Practice for Consumer IoT Security, DCMS UK
[51] Strategic Principles for Securing the Internet of Things, U.S. Dept of Homeland Security, Nov 2016
[52] IoT Security: From Design to Life Cycle Management, ABI Research
[53] ENISA 'Baseline Security Recommendations for IoT', November 2017

firmware updates. Platforms allow IoT users scale device fleets and may reduce the cost and effort of managing large and diverse IoT deployments. However, cloud computing comes with its own challenges. ENISA[54] describes security challenges that arise from the convergence of cloud computing and IoT, including the lack of standardization across cloud providers, the fact that the security requirements depend on the industry vertical being served, the vulnerability of edge devices that can then be used to gain access to the cloud, and the difficulty of securing heterogeneous communication protocols between devices and cloud.

Key Challenge 4: Root of Trust

Trust must start with the device, in the hardware itself, if it is to be effective[55]. Inherently, this starting point is with a Root of Trust (RoT) – a security primitive comprising functions and data in a device whose correctness is implicitly trusted[56]. The RoT constitutes the foundation for integrity of the device, incorporating the following elements:

- A key immutably bound to the device that represents the highest authority for issuing authorized firmware or software for the device.
- Cryptographic primitives for hashing, public key cryptography and optionally symmetric encryption.
- A secure boot process that can use the cryptographic primitives to authenticate the firmware or software that will ultimately run on the system in its mission mode.

A RoT may be implemented entirely in hardware, in which case it cannot be changed by virtue of being physically built into the system[57]. Alternatively, a RoT may be implemented in a bootstrap read-only memory (ROM), allowing some flexibility to make changes to the RoT without requiring radical changes to the architecture of the integrated circuit. Parts of the RoT may also be implemented in cryptographically signed firmware or software that executes in random access memory (RAM); this approach provides the most flexibility as new versions of RoT code can be provided to fielded devices. However, a hardware RoT should be used for critical IoT devices[58] [59]. The challenge is to do this under possibly severe constraints of cost and time-to-market, with limited device resources.

[54] Towards secure convergence of cloud and IoT, ENISA, Sept 2018
[55] IoT Security: From Design to Lifecycle Management, ABI Research, 2017
[56] Security Guidance for Critical Areas of Embedded Computing, prpl Foundation, Jan 2016
[57] Security Guidance for Critical Areas of Embedded Computing, prpl Foundation, Jan 2016
[58] Strategic Principles for Securing the Internet of Things, U.S. Dept of Homeland Security, Nov 2016
[59] Baseline Security Recommendations for IoT, Nov 2017

Key Challenge 5: Monitoring and Analytics

Although we strive to develop secure systems that are resistant to threats, no solution is perfect. History shows that vulnerabilities are invariably found after a product is deployed, and often exploited in "zero-day" attacks[60]. It is vital to be able to detect unforeseen vulnerabilities, anomalies and threats in live IoT deployments, and to respond quickly, recover and remediate. Besides developing technologies to perform these tasks intelligently and automatically, it is equally important to devise and plan for new paradigms of IoT security monitoring, incident management and recovery. Among the techniques that may prove useful is the honeypot, a computer security mechanism that appears to be a legitimate device containing information of value but is actually isolated and monitored. A honeypot resource is never meant for legitimate use; therefore, any access to the honeypot resource is illegitimate, and either accidental or hostile in nature[61]. The attack strategies are recorded by the honeypot, resulting in the collection of data including port numbers, network traffic, payloads, malware samples, and the toolkit used by the attacker. Most honeypot implementations also provide comprehensive analytics and visualization tools for deriving intelligence from attack data. Honeypots can form a cornerstone of an IoT monitoring and analytics strategy[62] that would then be able to share cyber threat information with various stakeholders[63]. Identifying and sharing information about vulnerabilities allows manufacturers to patch insecure products.

Key Challenge 6: Skills and Manpower

As identified by the Cloud Security Alliance[64], IT security staff are already required to keep up with a constantly-evolving cyberthreat and cybersecurity landscape and with a steady stream of new technologies and products. IoT introduces an additional dimension to the challenge. Product Security Officers and their teams now have to concern themselves with vulnerabilities within software as well as hardware, ways that attackers can compromise their product to affect safety in the physical world, and secure mechanisms for creating and distributing firmware and software updates to thousands or millions of devices. New training must provide security teams with an understanding of:

1. The new technologies associated with IoT
2. New threat profiles associated with IoT vulnerabilities
3. The impact of a compromise of IoT systems (across potentially millions of devices)

As suggested earlier in this document, companies should train their employees in good security practices, recognizing that technological expertise does not necessarily equate with security expertise. Further,

[60] https://en.wikipedia.org/wiki/Zero-day_(computing)
[61] Honeypots: A Security Manager's Guide to Honeypots, Eric Cole and Stephen Northcutt, https://www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide
[62] IoTPOT: A novel honeypot for revealing current IoT threats, Yin Minn Pa Pa et al, Journal of Information Processing Vol.24 No.3 522–533 (May 2016)
[63] https://www.globalcyberalliance.org/smart-cities-and-iot/
[64] Future-Proofing the Connected World, Cloud Security Alliance IoT Working Group, 2016

differences in terminology such as the concepts of safety and security and the differences between “business IT” security and IoT security need to be appreciated by practitioners.

This document was drafted and developed in cooperation with the Cyber Security Agency of Singapore, the Ministry of Economic Affairs and Climate Policy of the Netherlands and TNO. It is based on the "IoT Security Landscape" published on 2 October 2019.