THE IoT SECURITY LANDSCAPE

ADOPTION AND HARMONISATION OF SECURITY SOLUTIONS FOR THE INTERNET OF THINGS

TNO innovation for life

Jointly commissioned by:
Cyber Security Agency of Singapore
Ministry of Economic Affairs and Climate Policy of the Netherlands

COLOPHON

This Internet of Things Security Landscape Study was developed by TNO as an outcome of the bilateral IoT Security Workshop between Singapore and the Netherlands in The Hague on 18 May 2017 and the Global Forum on Cyber Expertise (GFCE) meeting in Brussels on 30 May 2017. It is executed under the MoU between the Cyber Security Agency of Singapore (CSA) and the National Cyber Security Centre (NCSC) of the Netherlands as signed 14 July 2016 in Singapore[1]. The study is supported by the Ministry of Economic Affairs and Climate Policy (MEAC) of the Netherlands, in charge of cybersecurity in IoT.

The study was authored by Dr Mark van Staalduinen and Yash Joshi of TNO with the help of the following experts:
- Dr. Oskar van Deventer, Senior Scientist, TNO
- André Smulders, Strategic Advisor Information Security, TNO
- Dr. Josine van de Ven, Senior Consultant Cyber Operations, TNO
- Thijmen Verburgh, Researcher, TNO
- Jules Vos, Senior Consultant, TNO

Special thanks to:
- Eddy Ong, Senior Assistant Director (Cybersecurity Engineering Centre), CSA
- Caslyn Tan, System Engineer (Cybersecurity Engineering Centre), CSA

For any queries, please contact:
mark.vanstaalduinen@tno.nl

ISBN 9789090324913

Ministry of Economic Affairs and Climate Policy

1 https://www.csa.gov.sg/news/press-releases/csa-signs-mou-with-the-netherlands-to-strengthen-cyber-security-cooperation

THE IoT SECURITY LANDSCAPE

ADOPTION AND HARMONISATION OF SECURITY SOLUTIONS FOR THE INTERNET OF THINGS

TNO innovation for life

September 2019

Dr Mark van Staalduinen
Yash Joshi


mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
elif operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
print("please select exactly two objects
OPERATOR CLASSES
Mirror Tool
0 10 1 0

FOREWORD

Cities around the world have ushered in the era of digital transformation. Singapore is no different, as we work towards our vision of a Smart Nation. The Smart Nation journey empowers the Singapore economy through technology and digital innovation, and aims to bring about a better quality of life for all. The Government, through policies and initiatives, also aims to better prepare and equip Singapore to embrace the ever-changing digital landscape.

The Smart Nation initiative rests on bridging communications and enabling digital services. This brings about the phenomenon of manufacturing every type of device to be "smart". From traffic cameras to lampposts and even the most mundane of devices like rice cookers and baby-monitors are now part of the "Internet of Things" or IoT. The rapid proliferation of such independently designed devices creates an extremely complex IoT ecosystem. These complexities create vulnerabilities that can easily be exploited by individuals or groups with malicious intent. This is a challenge that the world is facing now, and we ought to study the gaps in the IoT ecosystem and to develop frameworks, policies and innovative solutions to enhance the security of such devices.

With the exponential growth in the deployment of IoT devices, the security threat is multiplied many fold. Singapore may not be the first to solve this issue, but we are willing to respond quickly and boldly to create a safe and secure IoT cyberspace.

I am pleased that Singapore has established strong cybersecurity ties with the Netherlands. We have embarked on a journey to study and identify the security challenges of the IoT landscape. The outcome of this report highlights the need for collective responsibility between industries and governments. It is important for the ecosystem to stay vibrant and develop new innovative solutions to better secure our IoT against malicious and evolving threats.

As we face this uphill challenge in the IoT cyber domain, industries and governments need to pool together resources, strengthen defenses and remain aligned through international standards and governance.

Cyber threats are often global, transboundary and increasingly sophisticated. The security challenges can only be addressed when all stakeholders, Governments, industry, academia and consumers, work together. This report is the first of many collaborations with the Netherlands and all other like-minded nations and partners, as we forge towards a more trusted and resilient digital society.

David Koh
Commissioner of Cybersecurity
and Chief Executive
Cyber Security Agency of Singapore

CONTENTS

EXECUTIVE SUMMARY

The Internet of Things (IoT) is growing at a staggering rate. Gartner[2] forecasts that the number of connected things in use globally will surge from 8.4 billion in 2017 to 20.4 billion by 2020, with total spending on endpoints and services exceeding $2 trillion[3]. IoT unlocks tremendous value for the individual, for organisations and for governments; however, it also presents enormous security challenges. The 2015 VTech data breach[4], the Mirai botnet[5] of 2016, and the recent Silex malware attack[6] are some of the many incidents that have affected IoT in this early stage of its evolution. The potential of IoT will only be fully realised if cybersecurity and privacy are built in by design, and the following risks[7] are addressed and mitigated:

1. Consumer privacy and safety are undermined by the vulnerability of individual devices, connectivity, and back-ends; and
2. The wider economy and critical infrastructures face an increasing threat of large-scale cyber-attacks launched from massive numbers of insecure IoT devices.

The International IoT Security Roundtables held in 2016, 2017 and 2018[8] by the Cyber Security Agency[9] (CSA) of Singapore and the Ministry of Economic Affairs and Climate Policy (MEAC) of the Netherlands[10], as well as this study of the IoT security landscape, provide input for global efforts towards creating a safe and secure cyberspace of things; a global approach is required since IoT security is not limited by national boundaries.

These efforts shall lead to a global platform to share ideas and experiences, shape technologies and architectures, and drive standards and collaboration in creating a next-generation, inherently secure IoT ecosystem that upholds security and privacy expectations.

We identify and formulate the below problem statement based on our observations and the inputs of experts from CSA and MEAC as well as the Netherlands National Cyber Security Centre (NCSC)[11].

Vulnerable IoT devices are deployed fast, globally and with unknown lifespan, while a level playing field on common standards and technical solutions for cybersecurity in IoT is lacking for the industry. This creates safety, environmental and social hazards that are not well understood and likely to be unacceptable for society.

Using the problem statement as a starting point, this study identifies and discusses 11 interdependent IoT security challenges and presents findings and recommendations. We believe that addressing these challenges will allow IoT security to mature to a point where the IoT ecosystem can develop and flourish in a manner that is acceptable for society.

2 https://www.gartner.com/en
3 https://www.gartner.com/newsroom/id/3598917
4 https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge/
5 https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained
6 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-silex-malware-bricks-iot-devices-with-weak-passwords
7 Secure by Design: Improving the cyber security of consumer Internet of Things. Policy report UK Government, March 2018.
8 https://www.sicw.sg/iot
9 https://www.csa.gov.sg/
10 https://www.government.nl/ministries/ministry-of-economic-affairs-and-climate-policy
11 https://english.ncsc.nl/

TACKLING THE CHALLENGES

Many government agencies, academic institutes, industry alliances and individual vendors have made efforts towards tackling IoT security challenges; however, there is limited collaboration between these initiatives. Consequently, there exist hundreds of documents[12] with significant duplications and possible contradictions. IoT product developers, and vendors involved in the IoT supply chain and life cycle, may find themselves overwhelmed – or they may take advantage of the lack of clarity to do nothing at all. There is an immediate need for harmonisation on security recommendations and guidelines as well as coordination on security assurances in the form of regulation and certification. Given the continuing exponential growth in the number of IoT devices, there is no time to lose.

12 https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

1 INTRODUCTION

From homes to hospitals, the power grid, the highway, and the high seas, the Internet of Things (IoT) is destined to change 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, organisations and governments. Imagine an intelligent hospital system that links patient monitoring devices with drug infusion pumps to prevent overdoses and reduce false alarms. Or a smart city that automatically schedules maintenance work to minimise street blockages and uses smart lighting to de-escalate conflict situations in real time[13]. Or connected farms that control their irrigation systems based on the moisture content of the soil and on the weather forecast, all the while deriving algorithmic insights into optimal ways to grow and water crops. IoT is one of the key enabling technologies to realise these visions.

The number of IoT devices in operation continues to grow exponentially. Gartner forecasts that the number of connected things in use globally will surge from 8.4 billion in 2017 to 20.4 billion by 2020, with total spending on endpoints and services exceeding $2 trillion.[14]

Smart cities and smart nations[15] are enabled by the adoption of IoT along with related technologies such as cloud computing and big data analytics. These technologies can improve government operations, support better living, create new business opportunities, and support stronger and safer communities.

But the aforementioned opportunities come with enormous challenges. Beckstrom's Law of Cybersecurity[16] is a recent Internet aphorism that, slightly paraphrased, states the following:

1. Anything attached to a network can be hacked.
2. Everything is being attached to a network.
3. Therefore, everything can be hacked.

This pronouncement has proven largely accurate. In December 2015, VTech, a manufacturer of educational toys such as electronic learning devices, announced a security breach exposing the personal data of over 6 million people.[17] Reports suggested that the breach exploited a SQL injection vulnerability at the server and that the account registration services did not use encrypted communication.[18] The devices themselves were not compromised; however, the online services that the devices connected to were not sufficiently secured. On October 21, 2016, multiple distributed denial-of-service (DDoS) attacks targeted Domain Name System (DNS) provider Dyn, causing major Internet platforms and services to be unavailable to users in Europe and North America.[19] The attack was accomplished by issuing a large number of DNS lookup requests from as many as 600,000 Internet-connected devices[20] – such as printers, IP cameras, residential gateways and baby monitors – that were infected with the

13 https://www.tue.nl/en/our-university/departments/built-environment/research/smart-cities-program/collaboration/living-labs/stratumseind/
14 https://www.gartner.com/newsroom/id/3598917
15 https://www.smartnation.sg – Singapore Smart Nation website.
16 https://dld-conference.com/articles/its-a-mad-mad-mad-cyber-world
17 https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge/
18 https://www.bbc.com/news/technology-34963686
19 https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained
20 https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

Mirai malware to create a “botnet”; Mirai was also used for similar attacks on websites such as Krebs on Security.[21] On June 25, 2019, a new IoT malware called Silex was found to be wiping device firmware after gaining access via default credentials – the standard user name and password that devices are shipped with. The malware, which only operated for one day, managed to brick thousands of IoT devices.[22]

These examples highlight two primary risks facing IoT[23]:

1. Consumer privacy and safety are being undermined by the vulnerability of individual devices, connectivity, and back-ends; and
2. The wider economy and critical infrastructures face an increasing threat of large-scale cyber-attacks launched from massive numbers of insecure IoT devices.

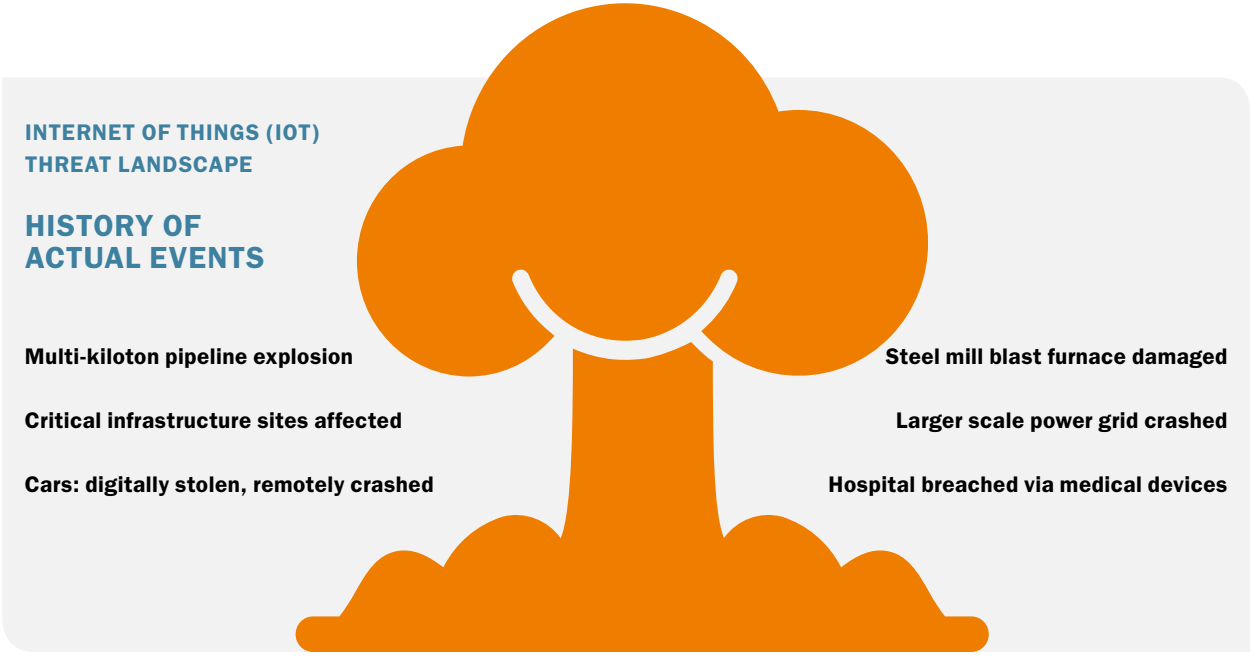


Figure 1: *IoT Threat Landscape: Actual Events (Source: Symantec)*

21 https://krebsonsecurity.com/
22 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-silex-malware-bricks-iot-devices-with-weak-passwords
23 Secure by Design: Improving the cyber security of consumer Internet of Things. Policy report UK Government, March 2018.

According to ABI Research, at this moment less than 4% of IoT devices are secure by design.[24] The real-life incidents depicted in Figure 1 emphasise the urgency of improving IoT security. For IoT to be successful, useful and acceptable, the hazards that come with the widespread use of IoT must be managed to risk levels acceptable for society.

1.1 OBJECTIVES

This study provides input to global efforts in creating a safe and secure cyberspace of things; a global approach is required, since IoT security is not limited by national boundaries. These efforts shall lead to a global platform to share ideas and experiences, shape technologies and architectures, and drive standards and collaboration in creating a next-generation, inherently secure IoT ecosystem that upholds security and privacy expectations.

The objective of this study is to define the problem spaces, determine the security challenges and identify gaps based on the current technological and policy landscape for each challenge in order to present key findings and recommendations, thus formulating the foundations for global actions and dialogue. In some industries, such an approach has been followed for decades: for example, the automotive industry develops designs in competition, while safety is based on common global standards (car safety certifications) and responsibilities (the manufacturer bears the cost of recalls).

1.2 PROBLEM STATEMENT

The problem statement is formulated based on the following observations of the IoT ecosystem.

1. IoT is by definition vulnerable – IoT is a network of physical devices using open network standards and software. Recent history has shown that such a network is highly vulnerable, especially given the resource-constrained nature of the devices and their often-unsupervised operation.
2. IoT devices are deployed fast, on a global scale and with unknown lifespan – IoT is one of the main drivers of innovation in today's world and, owing to the almost borderless digital economy, IoT solutions are developed for a global market. As a result, the pace of technology development is high and competition is fierce. At the same time, product lifecycles may be long, and devices can be used for a longer period than intended by the manufacturers.
3. No level playing field for IoT device manufacturers – Owing to the lack of legislations and the differences in legislative environments in different countries, there is no level playing field for vendors nor a common expectation of security functionality.
4. Lack of security in the IoT business equation – Time-to-market, usability and cost are key considerations for many solutions, and the razor-thin margins for these devices leave manufacturers with less to spend on security with virtually no incentive[25]: indeed, an attack on a device may affect neither the manufacturer nor the user but heavily impact a third party target in a botnet scenario.
5. Lack of IoT security awareness[26] – The current landscape is too complex for most end-users to really understand the risks to themselves and to others – for instance, few consumers would appreciate the very real risk of their refrigerators or smart TVs being used as part of a botnet in a DDoS attack.

Given these observations, we formulate the following problem statement:

Vulnerable IoT devices are deployed fast, globally and with unknown lifespan, while a level playing field on common standards and technical solutions for cybersecurity in IoT is lacking for the industry. This creates safety, environmental and social hazards that are not well understood and likely to be unacceptable for society.

24 IoT Security from Design to Lifecycle Management, An Embedded Perspective; ABI Research, 2018.
25 The economics of the security of consumer-grade IoT products and services, Internet Society / Plum Consulting, April 2019.
26 'Towards a secure connected digital society' – Advice regarding cybersecurity of IoT, by Dutch Cyber Security Council, 2018. In Dutch.

1.3 JUSTIFICATION AND METHODOLOGY

Data for this study was collected as follows.

1. Desk research and analysis focusing on publications from governments, standards development organisations, and industry, as well as scientific publications.
2. Interactive sessions including workshops, panel discussions and International IoT Security Roundtables[27] featuring participants from government, industry and academia.
3. Consultations with experts and policymakers from organisations including Singapore's Cyber Security Agency[28], the Ministry of Economic Affairs of the Netherlands[29], the Netherlands National Cyber Security Centre[30], Germany's BSI[31], and the UK Department for Digital, Culture, Media & Sport (DCMS)[32].

Based on the collected data, we identify fundamental IoT security challenges and map them to three problem spaces. We summarise recent developments related to each challenge and derive conclusions and actionable recommendations based on our findings. We also identify priority challenges based on input from experts in government, academia and industry.

While every effort is made to ensure that information is up-to-date, the IoT space continues to grow exponentially and we cannot guarantee completeness of coverage, particularly regarding initiatives and technology developments.

1.4 TARGET AUDIENCE

This report presents a wide-ranging discussion on the IoT security landscape and provides findings and recommendations towards securing IoT ecosystems to support policy initiatives and to inform the industry as well as interested stakeholders. Hence, the target audience includes government and industry bodies as well as vendors of IoT products and services, and organisations responsible for IoT security. This report is also useful for executives responsible for IT and/or innovation activities in their organisations, such as Chief Information Security Officers (CISOs).

1.5 LANDSCAPE STUDY STRUCTURE

The chapters in this study are organised as follows.

- Chapter 2: Definitions and concepts used in this study.
- Chapter 3: Specific challenges in IoT security, and a survey of expert opinions on the importance of each challenge given the current state of the art.
- Chapter 4: Overview of key initiatives that contribute to one or more of the identified challenges.
- Chapter 5: Discussions on each challenge, including a description of the current landscape and recent developments.
- Chapter 6: Conclusions and recommendations towards a more secure IoT ecosystem.

27 https://www.sicw.sg/iot
28 https://www.csa.gov.sg/
29 https://www.government.nl/ministries/ministry-of-economic-affairs-and-climate-policy
30 https://english.ncsc.nl/
31 https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html
32 https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport

2 DEFINITIONS AND BACKGROUND

2.1 INTERNET OF THINGS (IOT)

The IEEE provides the following definition for IoT[33]:
Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability.

According to the Internet Engineering Task Force (IETF)[34]:
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.

The U.S. Department of Homeland Security states[35] the following:
IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

According to the ITU-T[36], the IoT can be viewed as "a global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communication technologies". ITU-T emphasises that the IoT is characterised by its large-scale (compared to the current Internet) interconnections of heterogeneous devices that closely couple the physical and virtual worlds without the need for human intermediation; further, these devices may sleep, wake up, and change location while possibly being in operation without supervision for extended durations.

33 https://iot.ieee.org/definition.html
34 https://www.ietf.org/topics/iot/
35 Strategic Principles for Securing the Internet of Things, Department of Homeland Security, May 2016
36 ITU-T Y.2060, Overview of the Internet of Things

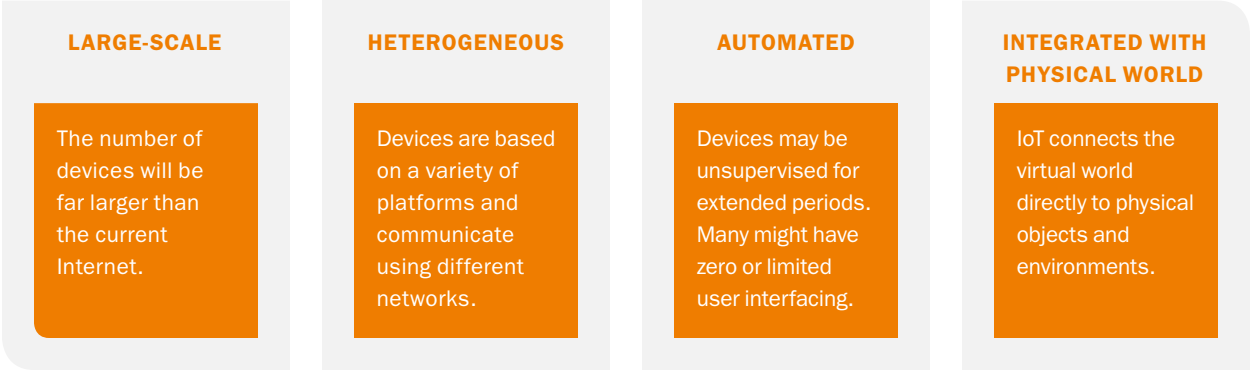


Figure 2: *IoT Characteristics*

It is clear from the above definitions that IoT deals with uniquely-identifiable, resource-constrained devices that measure and possibly control their environments and communicate over networks. We therefore exclude devices that are primarily intended for human interaction, such as mobile phones and computers; having said that, the extensive work done on IT security (or computer security[37]) over the past few decades provides useful fundamentals for IoT security.

2.2 IOT DEVICE AS A RESOURCE-CONSTRAINED DEVICE

A representation of a generic IoT device is shown in Figure 3. IoT devices are extremely varied in nature and may consist of some or all of the components depicted. 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 contain actuators for moving or controlling a system or environment. 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 (MCU), storage such as non-volatile RAM (NVRAM), and often a minimal operating system (OS) and a dedicated application.

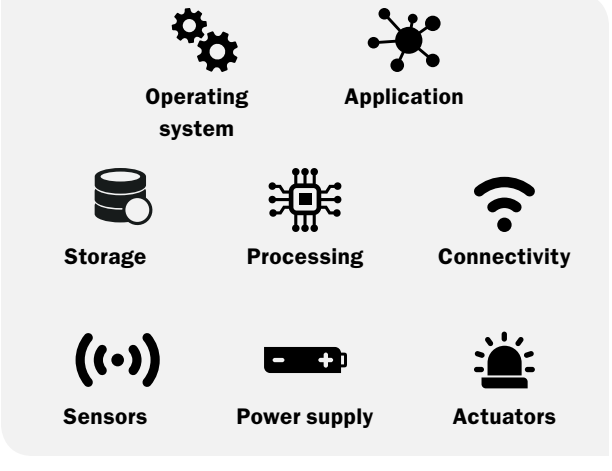


Figure 3: *An IoT Device*

37 https://en.wikipedia.org/wiki/Computer_security

As discussed, IoT devices are often resource-constrained; we may not have the luxury of measuring their memory in gigabytes, nor of measuring their processing power by number of cores. Most IoT devices use a microcontroller rather than a full-fledged microprocessor, and run at a few MHz rather than GHz. Specific resource constraints for IoT devices are shown below.

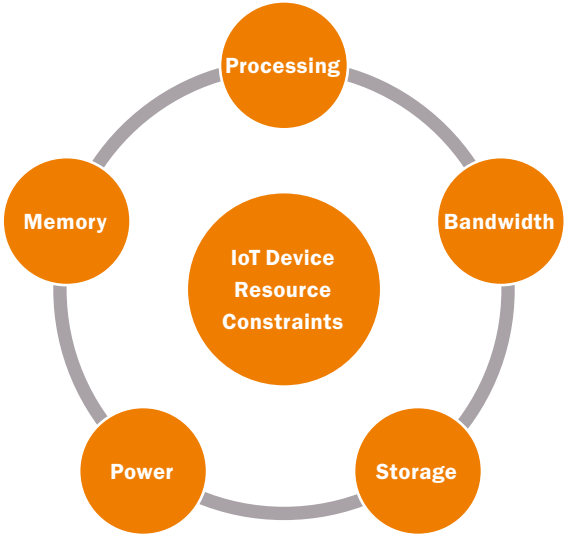


Figure 4: *IoT Device Resource Constraints*

Additionally, IoT devices may have physical constraints and accessibility constraints imposed by the operational environment, e.g. pacemakers within the human body. And, finally, cost is a critical constraint for IoT devices.

Of course, different devices can be constrained to different degrees – the varied nature of the devices needs to be accounted for in any discussion of IoT. The IETF classifies resource-constrained devices as depicted below.[38]

Classification of Resource-Constrained Devices	
Class 0	Pre-configured, sensor-like devices that communicate only with gateways and support bare-minimum management functionality such as a health indicator or heartbeat.
Class 1	Devices that are quite constrained and cannot easily talk to other Internet nodes employing a full protocol stack such as HTTP/TLS but can use protocols designed for constrained nodes and can integrate into an IP network using limited memory, storage, and power.
Class 2	Devices that are capable of supporting most of the protocol stacks used on computers. However, even these devices can benefit from lightweight and energy-efficient protocols and from consuming less bandwidth.

38 https://tools.ietf.org/html/rfc7228, IETF RFC 7228, May 2014, Terminology for Constrained-Node Networks

2.3 IOT SECURITY VS IT SECURITY

In accordance with the above discussions, this study excludes IT devices that require significant human interaction such as mobile phones and computers. Extensive work has been done in the field of IT security[39] over the past few decades. While IoT security and IT security share the same fundamental principles, it is often inadvisable to apply IT security classifications and mindsets directly to the IoT world[40] given the unique nature of the IoT ecosystem[41]. The following considerations apply:

1) As discussed, IoT devices are often constrained in terms of resources and/or physical environments. This significantly alters the way security is designed; for instance, IoT connections cannot generally rely on TLS/SSL 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, possibly in hostile environments – making them particularly susceptible to hacking. Many might have zero or limited user interfacing; thus, patching and updating may not be convenient and malfunctioning or rogue devices may not be immediately detectable.
3) The fact that IoT is closely integrated with the physical world can increase the impact of cyber-attacks. While IT cyber-attacks have resulted in data leakage and financial losses, IoT cyber-attacks have the potential to cause direct physical harm.

Moreover, conventional IT security has historically relied on fortifying a "perimeter". In previous decades, organisations could easily define and visualise this perimeter, and create a protection policy to enforce and guard its obvious boundary. Enterprises still commonly secure corporate networks using familiar baseline measures such as the firewall, the demilitarised zone (DMZ), and some variety of intrusion detection system (IDS). However, the traditional perimeter has been eroded by the widespread adoption of mobile devices, virtual private networks (VPNs), web-based applications and cloud computing[42]; IoT potentially takes both client device and server back-end out of the no-longer-defined perimeter[43], making it necessary to re-think security practices.

2.4 IOT THREATS AND VULNERABILITIES

The IETF defines[44] a threat as "a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability." Vulnerabilities can be exploited by a threat agent in an attack. The result can potentially compromise the confidentiality, integrity or availability of a resource.

Attacks on critical IoT devices and systems, such as connected cars and medical equipment, can target the device itself and disrupt its integrity or availability, endangering the user of the device and potentially those in the vicinity. For less critical IoT devices, such as thermostats or cameras, a major threat is device compromise, where the devices can be harnessed as part of a botnet to support DDoS attacks, spam bots or ransomware campaigns. The aforementioned Mirai[45] botnet and an evolved version of Mirai called Reaper[46] showed how

39 https://en.wikipedia.org/wiki/Computer_security
40 ITU-T Y.4806, Security capabilities supporting safety of the Internet of things
41 https://www.ibm.com/blogs/internet-of-things/security-iot/
42 IBM Red Paper, Understanding IT Perimeter Security https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf
43 https://www.networkworld.com/article/3223952/internet-of-things/5-reasons-why-device-makers-cannot-secure-the-iot-platform.html
44 IETF Internet Security Glossary, https://tools.ietf.org/html/rfc4949
45 Mirai IoT Botnet Co-Authors Plead Guilty - https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/
46 The Reaper IoT botnet has already infected a million networks - https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/

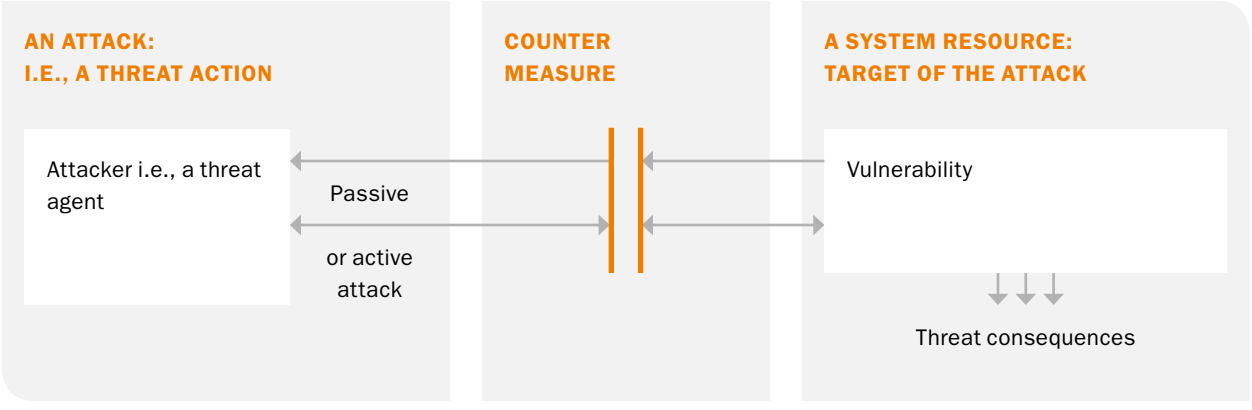


Figure 5: *Threats, Vulnerabilities and Attacks (Source: IETF)*

such large-scale cyber-attacks can cascade into national and international security threats. Finally, for all types of IoT devices, the potential loss of confidential information via the device, its communication infrastructure, or its back-end servers remains a significant threat. Table 1 briefly discusses some of the threats and vulnerabilities facing IoT that are most commonly cited by sources such as IRTF[47], OWASP[48] and others[49,50], as a prerequisite to discussing IoT security challenges.

47 State-of-the-Art and Challenges for the Internet of Things Security, IRTF T2T Research Group, https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/?include_text=1
48 OWASP IoT Project, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
49 Practical Internet of Things Security, Brian Russell, from p257, 2016.
50 https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

IoT Threats and Vulnerabilities		
1	Vulnerable device software	IoT devices rely on software that might contain poor design choices and/or security bugs such as buffer overflows and improper exception handling. This makes them vulnerable to many different attacks that can compromise data confidentiality or integrity.
2	Privacy threat	Device location tracking poses a privacy risk to users; an attacker can infer sensitive information from data gathered and communicated by devices. Such information may be sold to interested parties for marketing purposes or used for unauthorised surveillance.
3	Eavesdropping	Communication over an IoT network can be intercepted and deciphered if the communication channel is not sufficiently protected, for instance if keying material, security parameters, or configuration settings are exchanged in the clear or if weak or unsuitable cryptographic algorithms are used. Related attacks include man-in-the-middle, session hijacking, or message replay.
4	Denial of Service (DoS)	Devices, being resource-constrained, are susceptible to denial of service attacks launched by attackers sending continuous requests to deplete device resources. On the other hand, compromised devices can themselves be used to disrupt the operation of other networks or systems via a Distributed DoS (DDoS) attack.
5	Firmware-level attack	An attacker may be able replace device firmware during device commissioning or under the guise of a routine upgrade.
6	Device cloning or substitution	A non-trusted factory can clone the physical characteristics, firmware/software and security configuration of the device. Deployed devices might also be compromised and their software reverse-engineered, allowing for cloning. Cloned devices may be sold cheaply in the market and can contain functional modifications including backdoors. Alternatively, a genuine device may be substituted with a variant or clone during transportation or commissioning.
7	Data leakage	Disclosure of sensitive data, intentionally or unintentionally, to unauthorised parties. Confidential data may be captured by an attacker from individual devices, during transit, or from the back-end.
8	Malware	Devices can be infected with programs designed to carry out unauthorised actions on a system, possibly using existing vulnerabilities in software or firmware.
9	Weak user/admin credentials and authentication	Poor credential management such as weak password choices and lack of multi-factor authentication for the user and administrative interfaces of devices, gateways or back-ends is a common vulnerability in many information systems including IoT.

Table 1: *IoT Threats and Vulnerabilities*

2.5 SECURITY VS SAFETY

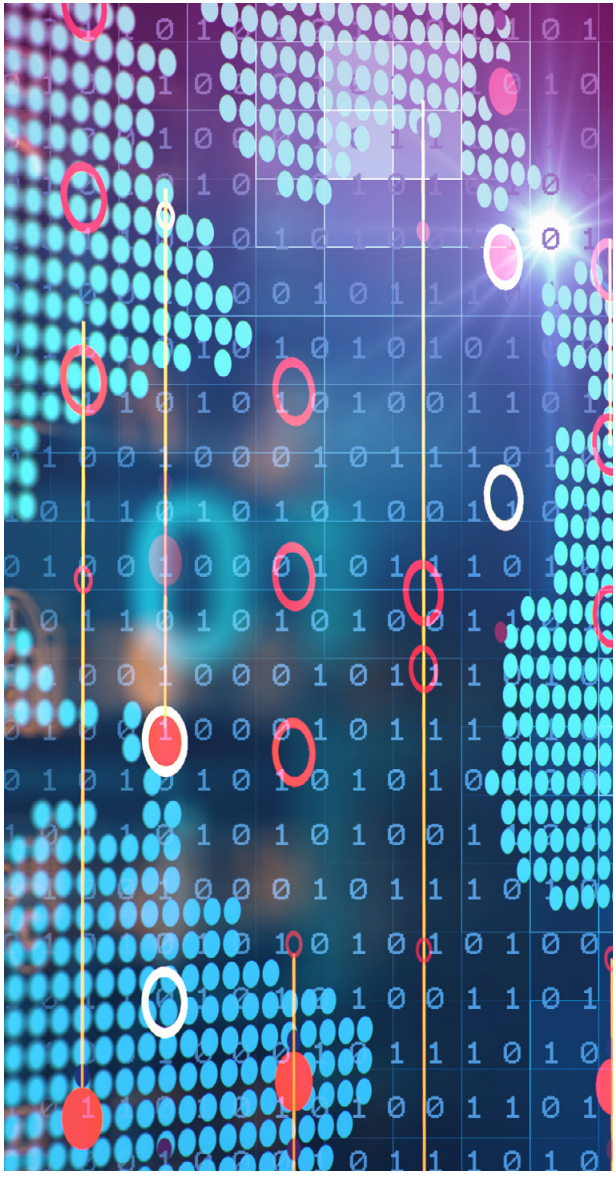
While the terms “safety” and “security” tend to be used interchangeably in informal situations, they have acquired specific meanings[51,52] in the domain of Information Security.

Safety is the condition of a system operating without unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment. (IEC)

Computer security, cybersecurity or IT security is the protection of computer systems from theft or damage as well as disruption or misdirection of the services they provide. (Wikipedia)

Safety measures focus on preventing losses due to unintentional actions by benevolent actors, while security measures emphasise the prevention of losses due to intentional actions by malevolent actors[53]. Security threats, as described in the previous section, tend to be rooted in malicious intentions, typically deriving from crime, terrorism, geo-politics or hacktivism, and they evolve over time, meaning that there should be a continuing strategy to react, adapt and defend against these threats. Safety hazards, on the other hand, are typically accidental and stem from environmental situations or human error.

Having said that, many security threats can lead to safety losses – indeed, the fact that IoT devices are closely integrated with the physical world[54] increases the likelihood of a malicious attack cascading into a significant safety loss.



51 https://www.iec.ch/functionalsafety/explained/
52 https://en.wikipedia.org/wiki/Computer_security
53 Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory, Young and Leveson, Communications of the ACM, Feb 2014
54 https://www.iotsecurityfoundation.org/safety-security/

3 IOT SECURITY PROBLEM SPACES AND CHALLENGES

This study identifies 11 cybersecurity challenges in the IoT landscape based on a review of existing literature as well as expert input from the International IoT Security Roundtables and conversations with practitioners and policymakers during and after the Roundtables.[55] Figure 6 maps the identified challenges to three problem spaces: Principles, Governance and Legislation; Ecosystem Development; and Technical References and Standards.

This study explores these IoT security challenges in a domain-agnostic manner, with IoT devices modelled as generic resource-constrained devices that require security controls. Orthogonal to the generic approach would be a domain-specific approach; a given domain can impose specific physical and technological constraints and have specific security requirements. We briefly address in Annex A the IoT security requirements in two rapidly-growing domains: smart mobility and smart health.

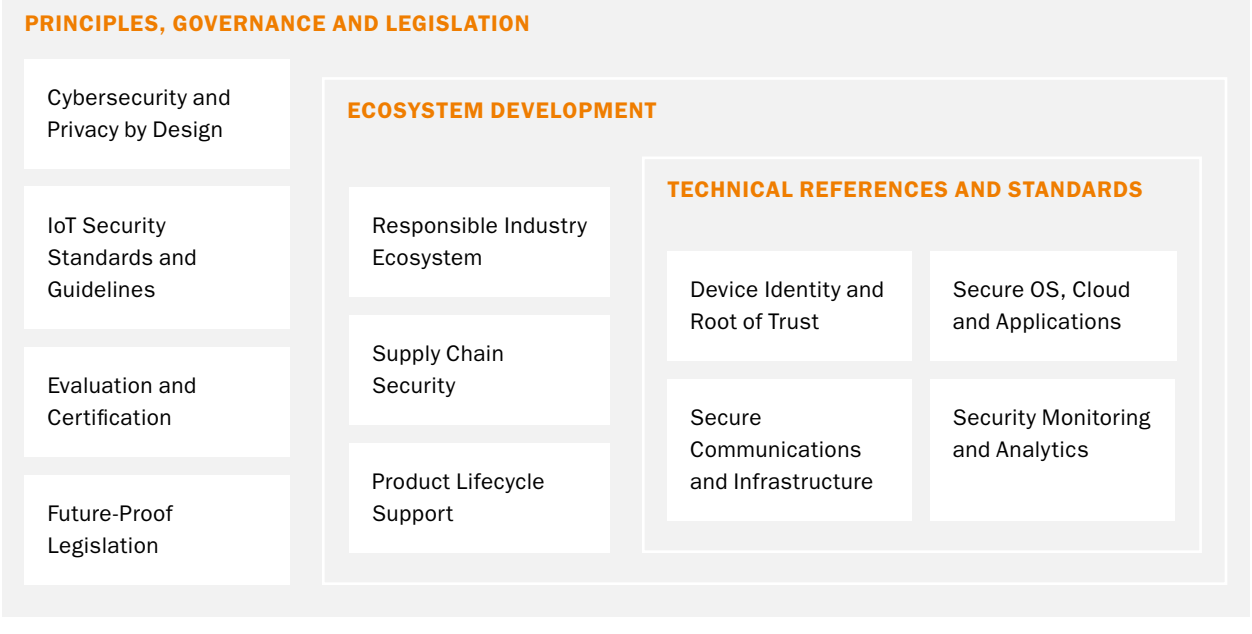


Figure 6: *IoT Security Problem Spaces and Challenges*

55 https://www.sicw.sg/iot

3.1 PRINCIPLES, GOVERNANCE AND LEGISLATION

IoT security needs to be based upon fundamentally sound cybersecurity principles. To achieve security in practice, these principles should lead to concrete guidelines and standards. Standards are used as a basis for evaluation and certification. For certification schemes to be successful, there must either be demand for certification from customers/users or governmental legislation mandating a minimum assurance level. Finally, since IoT is a global phenomenon and is not limited by national boundaries, it is essential to align country-specific legislations and adopt a coherent global approach to IoT security to drive standards and collaboration in creating an IoT environment that upholds security and privacy expectations. We identified the following challenges in this problem space.

1. **Cybersecurity and Privacy by Design** – To identify and define foundational principles to build cybersecurity and privacy by design for IoT devices.
2. **IoT Security Standards and Guidelines** – To set and harmonise IoT security standards and recommendations over different application domains.
3. **Evaluation and Certification** – To develop globally recognised and adopted cybersecurity evaluation and certification regimes for IoT devices.
4. **Future-Proof Legislation** – To develop regulatory policies that are sufficiently flexible to deal with societal security needs and a constantly evolving industry.

3.2 ECOSYSTEM DEVELOPMENT

As mentioned in the introduction to this document, time-to-market, usability and cost are key considerations for IoT solutions, and the razor-thin margins for devices leave suppliers with less to spend on security. Besides incentivising manufacturers to implement security, it is important to cultivate an ecosystem that fosters security in IoT supply chains and throughout device lifecycles. This study identified the following challenges in this problem space[56].

5. **Responsible Industry Ecosystem** – To transform to a responsible industry that proactively implements cybersecurity in IoT devices.
6. **Supply Chain Security** – To create a framework for all suppliers and service providers involved in the supply chain to adopt security principles and to deliver secure IoT components.
7. **Product Lifecycle Support** – To implement a framework for secure device lifecycle management and patching that is adopted by all parties involved.

3.3 TECHNICAL REFERENCES AND STANDARDS

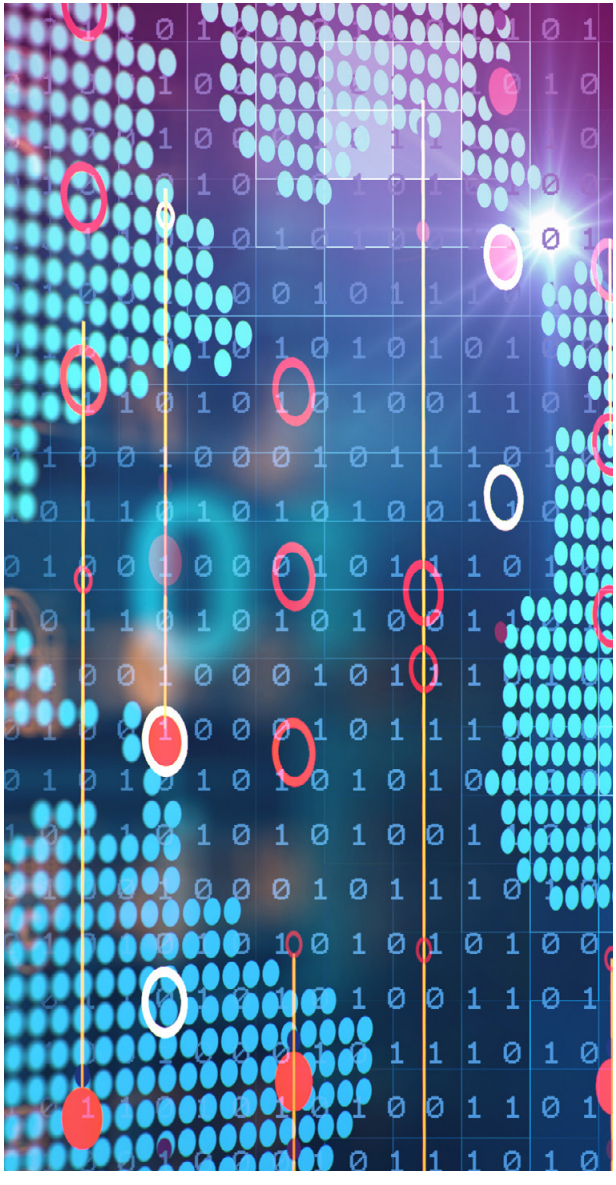
Finally, this study examines the security challenges in the IoT technologies themselves: the devices and firmware, the operating systems and applications on the devices and back-end servers, and the communication infrastructure connecting devices to gateways and back-ends. The identified technical challenges are aligned with "the four cornerstones of security" identified by Symantec[57].

8. **Device Identity and Root of Trust** – To establish a chain of trust from a root of trust on resource-constrained IoT devices to develop foundationally secure devices.
9. **Secure OS, Cloud and Applications** – To provision security controls in device OSes as well as cloud and back-end applications to guarantee security within the IoT ecosystem.
10. **Secure Communications and Infrastructure** – To ensure data and source integrity in the communication networks of resource-constrained IoT devices.
11. **Security Monitoring and Analytics** – To detect vulnerabilities, anomalies and threats in IoT deployments and to quickly respond, recover and remediate.

56 Numbering of the challenges continues from 1 to 11 over the three problem spaces.

57 Smart Nation: Cloud Delivery of Managed Security Services, Brian Witten, Symantec. Delivered during SICW International IoT Security Roundtable 2017.

Challenges 8 to 10 should provide a technical security baseline. However, history shows that vulnerabilities are invariably found after a product is deployed; therefore, we need to continue to monitor and analyse IoT deployments for advanced attacks, exceptions and other deviant behaviour. This is addressed under challenge 11. Of course, newly-found attack vectors should lead to solutions deployed in the form of patches or updates – which ties this challenge back to the product lifecycle and ecosystem.



3.4 EXPERT OPINIONS ON PRIORITY CHALLENGES

As described in Chapter 1, this study makes extensive use of material gathered during interactive sessions with cybersecurity and IoT practitioners and policymakers. The sessions included workshops, panel discussions and International IoT Security Roundtables[58], and expert opinions were sought from a number of individuals and several organisations including Singapore's Cyber Security Agency[59], the Ministry of Economic Affairs of the Netherland[60], the Netherlands National Cyber Security Centre[61], the UK Department for Digital, Culture, Media and Sport[62], and Germany's BSI[63].

To determine the relative importance of each challenge and thereby identify priority challenges for policymakers and industry, a number of experts were surveyed. They were asked which of the identified IoT security challenges are, in their opinion, the most relevant and urgent given the current state of IoT security; their responses are summarised in the chart below. Each respondent chose up to 3 priority challenges.

As Figure 7 on the next page reveals, there is a wide range of opinions among the expert community on which challenges are most critical; indeed, this is reflective of the nebulous state of IoT security today. Having said that, it is clear that the community expects security to be built into IoT devices and ecosystems by design. The development of effective evaluation and certification schemes built upon widely-accepted security standards (themselves based on sound cybersecurity and privacy principles) is increasingly seen as a cornerstone of IoT security, as is the establishment of a secure supply chain and managed device lifecycle. The security of the hardware devices is also seen by the expert community as important; in particular, the hardware root of trust is emphasised by security practitioners in the field. The streamlining of monitoring efforts with the supply chain and lifecycle challenges represents a key opportunity.

These inputs suggest that certain security challenges should be addressed on a priority basis; this is discussed in the conclusion of this study after an examination of the current landscape and recent developments related to each challenge.

58 https://www.sicw.sg/iot
59 https://www.csa.gov.sg/
60 https://www.government.nl/ministries/ministry-of-economic-affairs-and-climate-policy
61 https://english.ncsc.nl/
62 https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport
63 https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

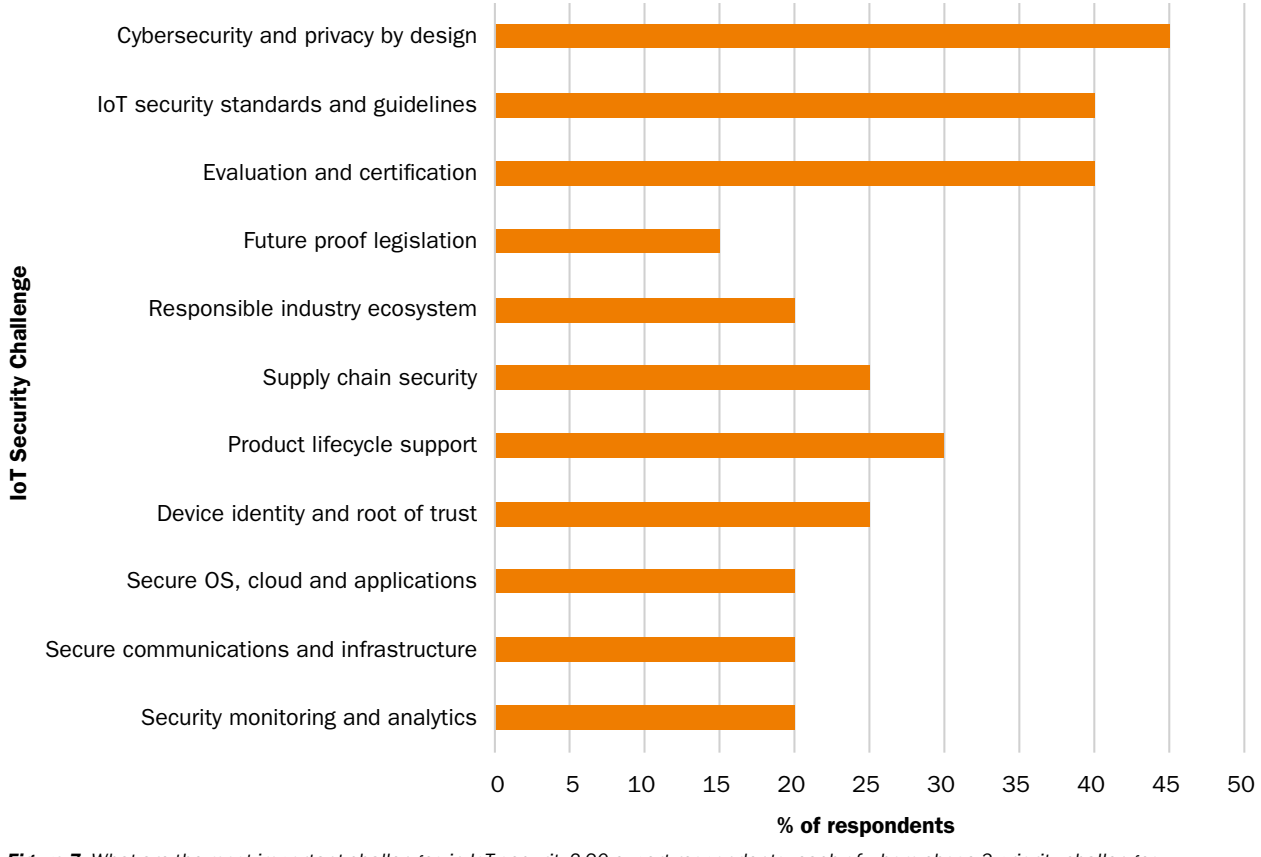


Figure 7: *What are the most important challenges in IoT security? 20 expert respondents, each of whom chose 3 priority challenges*

4 KEY INITIATIVES

4.1 INVENTORY OF KEY INITIATIVES

Numerous IoT security initiatives have emerged in recent years. We have identified 25 major initiatives for further examination; each initiative is described in more detail in Annex B. The initiatives have been chosen based on their focus on and contributions to IoT *security* rather than IoT in general. These initiatives contribute to and, to some extent, define the state of the art in IoT security.

The initiatives broadly fall within the below categories.

- IoT-focused groups formed by standards development organisations (SDOs) such as ETSI, the International Telecommunications Union (ITU)[64] and the Internet Engineering Task Force (IETF)[65].
- Professional bodies such as the Industrial Internet Consortium (IIC)[66], the IoT Security Foundation[67], and the Cloud Security Alliance[68].
- Governmental initiatives such as the IoT security divisions of NIST[69] and ENISA[70], and the Alliance for IoT Innovation (AIOTI)[71].
- Alliances focused on networking standards, such as GSMA[72], Zigbee[73] and LoRa[74].
- Initiatives dedicated to hardware platforms, such as the Trusted Computing Group (TCG)[75], UEFI[76] and GlobalPlatform[77].

Table 2 indicates the IoT security challenge/s primarily addressed by each key initiative. The table reveals a strong emphasis on standards as well as connectivity, and comparatively less focus (in terms of number of initiatives) on supply chain and lifecycle. It is noted that several of the initiatives are dedicated chiefly to a single challenge: Wi-SUN[78], Zigbee, LoRa and IETF are focused primarily on IoT networking and communications (and the accompanying standards), the Global Cyber Alliance[79] deals with threat analytics and intelligence, and UEFI and GlobalPlatform largely address hardware security. Some bodies, such as the IoT Security Foundation (IoTSF) and the Industrial Internet Consortium (IIC), have a much wider focus.

Table 3 describes the primary membership of each initiative in terms of professional domain (government, industry or academia) and geographical region. We observe that government involvement is limited, particularly for non-European initiatives. Also, there is a strong tendency towards continental initiatives, focusing on the Americas or Europe. Only the IoT Acceleration Consortium[80] and Wi-SUN are oriented towards Asia, specifically Japan. Given that Asia is a manufacturing hub for computer hardware and microelectronics, we would expect to find more IoT security activity in this region – although it is possible that we have been unable to identify Asian initiatives owing to language barriers. We were also unable to find major initiatives operating in Africa, although we note that the IoT Forum Africa[81] is held annually in Johannesburg. Table 4 reiterates that global governmental initiatives are lacking – the sole international government-driven initiative appears to be the ITU-T Study Group 20[82].

64 https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx
65 https://www.ietf.org/topics/iot/
66 https://www.iiconsortium.org/
67 https://www.iotsecurityfoundation.org/
68 https://cloudsecurityalliance.org/
69 https://www.nist.gov/topics/internet-things-iot
70 https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot
71 https://aioti.eu/
72 https://www.gsma.com/iot/
73 https://www.zigbee.org/
74 https://lora-alliance.org/
75 https://trustedcomputinggroup.org/
76 https://uefi.org/
77 https://globalplatform.org/
78 https://www.wi-sun.org/
79 https://www.globalcyberalliance.org/smart-cities-and-iot/
80 http://www.iotac.jp/en/
81 http://iotforumafrica.com/
82 https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx

	IoT Security Initiative / Challenges Addressed	Cybersecurity and Privacy by Design	IoT Security Standards	Evaluation and Certification	Future-Proof Legislation	Responsible Industry Ecosystem	Supply Chain Security	Product Lifecycle Support	Device Identity and Root of Trust	Secure OS, Cloud and Applications	Secure Communications and Infra	Security Monitoring and Analytics
1	Alliance for IoT Innovation	●	●		●							
2	Cloud Security Alliance		●							●		
3	ENISA IoT	●	●		●							
4	ETSI	●	●									
5	GlobalPlatform			●					●			
6	Global Cyber Alliance											●
7	GSMA		●								●	
8	Internet Engineering Task Force		●								●	
9	Industrial Internet Consortium		●			●	●	●	●	●	●	●
10	IoT Acceleration Consortium		●									
11	IoT Consortium					●						
12	IoT Cybersecurity Alliance		●							●	●	●
13	IoT European Platforms Initiative					●						
14	IoT Security Foundation	●	●	●		●	●	●	●	●	●	●
15	ITU Study Group 20		●								●	
16	LoRa Alliance		●	●							●	
17	NIST Cybersecurity for IoT Program		●									
18	Open Connectivity Foundation		●								●	
19	OWASP IoT Project	●	●							●	●	
20	Prpl Foundation								●		●	
21	Thing-to-Thing Research Group		●							●	●	
22	Trusted Computing Group								●	●		
23	UEFI Forum		●						●			
24	Wi-SUN Alliance		●	●							●	
25	Zigbee Alliance		●	●							●	

Table 2: *IoT Security Initiatives – Challenges Addressed*

	IoT Security Initiative	Membership (primary focus)		Government	Industry	Academia		Americas	Europe	Asia	Global
1	Alliance for IoT Innovation				●			●	●		
2	Cloud Security Alliance				●	●					●
3	ENISA IoT			●					●		
4	ETSI			●	●	●			●		
5	GlobalPlatform				●						●
6	Global Cyber Alliance				●						●
7	GSMA				●						●
8	Internet Engineering Task Force				●	●					●
9	Industrial Internet Consortium				●						●
10	IoT Acceleration Consortium			●	●	●				●	
11	IoT Consortium				●			●	●		
12	IoT Cybersecurity Alliance				●			●	●		
13	IoT European Platforms Initiative			●					●		
14	IoT Security Foundation				●			●	●		
15	ITU-T Study Group 20			●	●	●					●
16	LoRa Alliance				●						●
17	NIST Cybersecurity for IoT Program			●				●			
18	Open Connectivity Foundation				●						●
19	OWASP IoT Project				●	●		●	●		
20	Prpl Foundation				●						●
21	Thing-to-Thing Research Group				●	●		●	●		
22	Trusted Computing Group				●						●
23	UEFI Forum				●						●
24	Wi-SUN Alliance				●					●	
25	Zigbee Alliance				●	●		●	●		
	Total numbers			**6**	**22**	**8**		**8**	**10**	**2**	**12**

Table 3: *IoT Security Initiatives – Membership*

	Global	Americas	Europe	Asia
Government	1	1	2	1
Industry	11	7	7	2
Academia	3	3	3	1

Table 4: *IoT Security Initiatives – Membership (Region vs Domain)*

At the same time there are numerous national research initiatives, typically at university level, focusing on IoT security. Notable examples include the PETRAS[83] research hub formed by a group of U.K. universities led by University College London.

4.2 APPLICATION-SPECIFIC INITIATIVES

Many pilots address IoT security in the narrower context of a specialised application domain such as automotive or healthcare[84], often under domain-specific names such as "intelligent transportation", “smart mobility”, "smart grid", or "e-health". In the automotive domain, notable examples include the Centre of Excellence for Testing and Research of Autonomous Vehicles (CETRAN)[85] at the Nanyang Technological University in Singapore and the Security Credential Management System (SCMS)[86] of the U.S. Department of Transportation. Enterprise Singapore has published a set of provisional national standards, known as Technical Reference (TR) 68, to guide industry in the development and deployment of fully autonomous vehicles in Singapore. The TR includes cybersecurity principles and assessment methodology.

A vehicular IoT technology that is already widely deployed is the EU-wide eCall initiative[87], intended to bring rapid assistance to motorists in the event of a crash by communicating the vehicle’s location and direction to emergency services; eCall has been mandatory for all new cars sold within the EU since April 2018.

The Smart Mobility Working Group of AIOTI[88] has done substantial work detailing the application of IoT principles to connected vehicles. Intelligent Transportation Systems (ITS) groups worldwide, particularly ERTICO[89] in Europe, are involved in a number of pilot projects in the area of smart mobility. ERTICO has also released recommendations[90] on communication technologies for future Cooperative ITS (C-ITS) scenarios. At the same time, consumer privacy is a concern in automotive IoT applications; the American Future of Privacy Forum[91] and National Automobile Dealers’ Association (NADA) have published a consumer guide[92] highlighting the types of data that connected cars collect and transmit.

In healthcare, efforts include in-home monitoring services for the elderly[93] from Fujitsu and Panasonic, the M.A.I.L. (Motion capture and Artificial Intelligence assisted Liposuction)[94] system from Korean plastic surgery provider 365mc, and remote monitoring and management of in-vitro diagnosis (IVD) devices[95] by Roche Diagnostics[96] in China. Cybersecurity concerns have naturally begun to emerge: in 2015, the U.S Food and Drug Administration (FDA) ordered hospitals to stop using the Hospira Symbiq infusion pump, which delivers medications directly into the bloodstream,

83 https://www.petrashub.org/
84 We discuss these domains in more detail in Annex A.
85 http://erian.ntu.edu.sg/Programmes/IRP/FMSs/Pages/Centre-of-Excellence-for-Testing-Research-of-AVs-NTU-CETRAN.aspx
86 https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf
87 https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018
88 https://aioti.eu/aioti-wg09-report-on-smart-mobility/
89 http://ertico.com/
90 http://erticonetwork.com/ertico-releases-guide-about-technologies-for-future-c-its-service-scenarios/
91 https://fpf.org/
92 https://fpf.org/2017/01/25/fpf-and-nada-launch-guide-to-consumer-privacy-in-the-connected-car/
93 http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0625-01.html
94 https://customers.microsoft.com/en-us/story/365mc-azure-iot-suite-machine-learning-korea-en
95 https://customers.microsoft.com/en-us/story/roche-diagnostics
96 https://www.roche.com/about/business/diagnostics.htm

after a security researcher showed that the pump could be accessed remotely over WiFi and allowed an attacker to change dosage settings or use it as a gateway to attack hospital networks[97].

While there are numerous pilots and also several American and European initiatives to address specific domains such as automotive and healthcare as discussed above, global IoT security initiatives and standards are lacking in these domains.

4.3 KEY FINDINGS

- Most initiatives have a generic focus, and application-specific initiatives (e.g. for automotive or healthcare) are largely country- or region-specific.
- Most Standards Development Organisations (SDOs) have initiated work on IoT Security standards.
- Most initiatives are industry-driven, and we observe a lack of government involvement outside Europe.
- National or continental initiatives are centred on the Americas or Europe; a global approach is lacking.
- Substantial initiatives with a broad security focus include the Industrial IoT Consortium and the IoT Security Foundation.

97 https://www.reuters.com/article/us-hospira-fda-cybersecurity-idUSKCN0Q52GJ20150731

5 IOT SECURITY CHALLENGES

This chapter articulates the 11 IoT security challenges in detail. For each challenge we describe the current landscape and recent developments to examine the gap between the challenge and the state of the art. The full set of findings for the 11 security challenges are input for the conclusions and recommendations to drive IoT cybersecurity forward.

5.1 CYBERSECURITY AND PRIVACY BY DESIGN

To build cybersecurity and privacy by design into IoT, a set of security principles should be adopted and adhered to. These principles form the basis for standards, future-proof legislation, and operational security solutions.

5.1.1 Current Landscape and Recent Developments

The United States Department of Homeland Security (DHS)[98], OWASP[99], the Korea Internet & Security Agency[100], and the Alliance for IoT Innovation (AIOTI)[101] have all defined sets of IoT security and privacy principles.

Strategic Principles by DHS

The U.S. DHS describes the risks associated with IoT and provides a set of principles and best practices to build security into IoT.[102]

US Department of Homeland Security – Strategic Principles for Securing the IoT	
1	Incorporate Security at the Design Phase
2	Advance Security Updates and Vulnerability Management
3	Build on Proven Security Practices
4	Prioritise Security Measures According to Potential Impact
5	Promote Transparency across IoT
6	Connect Carefully and Deliberately

IoT Security Principles from South Korea

The seven principles of common security for IoT as proposed by Korea Internet & Security Agency[103] should be considered by the providers (developers) of IoT devices and services, and by users as well.

Korea Internet and Security Agency – IoT Common Security Principles	
1	Design IoT products and services in consideration of the need to protect information and strengthen privacy.
2	Apply and verify technologies for the development of safe software and hardware.
3	Provide a method of establishing safe initial security.
4	Comply with the security protocol and set safe parameters.
5	Update security patches against the weak points of IoT products and services continuously.
6	Provide a system for information protection and privacy to ensure safe operation and control.
7	Provide a system capable of coping with infringements of the IoT and a method of detecting the responsible entity.

98 https://www.dhs.gov/
99 https://www.owasp.org/index.php/Main_Page
100 https://www.kisa.or.kr/eng/main.jsp
101 https://aioti.eu/
102 https://www.dhs.gov/sites/default/files/publications/ Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
103 IoT Common Security Principles v1.0, Korea Internet & Security Agency.

IoT Security Principles from DCMS UK

The U.K. Government's Department for Digital, Culture, Media and Sport (DCMS) has published a report[104] on IoT security in which five guiding principles are identified to inform future action. The report also describes the development of the U.K.'s Code of Practice[105] on IoT Security.

UK Government – Improving the Cyber Security of Consumer IoT	
1	Reducing Burden – Many consumers struggle to understand what is required of them, or conducted on their behalf, to keep their products secure. Reducing the burden on consumers will likely require everyone in the supply chain to pay more attention to security.
2	Transparency – Greater transparency is an essential part of a secure by design approach. Being open and explicit about security mechanisms that have been put in place to secure a product or service, allows for accountability and scrutiny, thereby enabling others in the supply chain to make informed choices.
3	Measurability – A secure by design approach should not just be about putting in place good security mechanisms, but also being able to measure the effectiveness of those mechanisms.
4	Facilitating Dialogue – Facilitating dialogue means maintaining effective communication between all parties across the supply chain and with consumers.
5	Resilience – A secure by design approach should further have provisions to increase the resilience of critical functions and services. This includes conducting business continuity planning, establishing a "fallback framework" and undertaking regular risk assessments to anticipate and mitigate future problems.

IoT Security Principles by OWASP

OWASP states sixteen principles[106] that cover the full spectrum of IoT from system hardening and lifecycle support to authentication and isolation.

IoT Security Principles by OWASP	
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 consider scale. Simple bootstrapping into an ecosystem can create a self-denial of service condition at IoT scale. Security countermeasures must perform at volume.

104 Secure by Design: Improving the cyber security of consumer Internet of Things. Policy report UK Government, March 2018.
105 https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security
106 https://www.owasp.org/index.php/Principles_of_IoT_Security

3	Internet of Lies – Automated systems are extremely capable of presenting misinformation in convincing formats. IoT systems should always verify data from the edge to prevent autonomous misinformation from tainting a system.
4	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.
5	Expect Isolation – The advantage of autonomy should also extend to situations where a component is isolated. Security countermeasures must never degrade in the absence of connectivity.
6	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 life cycle 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.
7	Encryption is Tricky – It is very easy for developers to make mistakes when applying encryption. Using encryption but failing to validate certificates, failing to validate intermediate certificates, failing to encrypt traffic with a strong key, using a uniform seed, or exposing private key material are all common pitfalls when deploying encryption. Ensure a thorough review of any encryption capability to avoid these mistakes.
8	System Hardening – Be sure that IoT components are stripped down to the minimum viable feature set to reduce attack surface. Unused ports and protocols should be disabled, and unnecessary supporting software should be uninstalled or turned off. Be sure to track third party components and update them where possible.
9	Limit what you can – To the extent possible limit access based on acceptable use criteria. There's no advantage in exposing a sensor interface to the entire internet if there's no good case for a remote user in a hostile country. Limit access to white lists of rules that make sense.
10	Life cycle Support – IoT systems should be able to quickly onboard new components, but should also be capable of re-credentialing existing components, and deprovisioning components for a full device life cycle. This capability should include all components in the ecosystem from devices to users.
11	Data in Aggregate is Unpredictable – IoT systems can collect vast quantities of data that may seem innocuous at first, but complex data analysis may reveal very sensitive patterns or information hidden in data. IoT systems must prepare for the data stewardship responsibilities of unexpected information sensitivity that may only be revealed after an ecosystem is deployed.
12	Plan for the Worst – IoT systems should have capabilities to respond to compromises, hostile participants, malware, or other adverse events. There should be features in place to re-issue credentials, exclude participants, distribute security patches and updates, and so on, before they are ever necessary.
13	The Long Haul – IoT system designers must recognise that the extended lifespan of devices will require forward compatible security features. IoT ecosystems must be capable of aging in place and still addressing evolving security concerns. New encryption, advances in protocols, new attack methods and techniques, and changing topology all necessitate that IoT systems be capable of addressing emerging security concerns for years after they are deployed.

14	Attackers Target Weakness – Ensure that security controls are equivalent across interfaces in an ecosystem. Attackers will identify the weakest component and attempt to exploit it. Mobile interfaces, hidden API's, or resource constrained environments must enforce security in the same way as more robust or feature rich interfaces. Using multi-factor authentication for a web interface is useless if a mobile application allows access to the same APIs with a four-digit PIN.
15	Transitive Ownership – IoT components are often sold or transferred during their lifespan. Plan for this eventuality and be sure IoT systems can protect and isolate data to enable safe transfer of ownership, even if a component is sold or transferred to a competitor or attacker.
16	N:N Authentication – Realise that IoT does not follow a traditional 1:1 model of users to applications. Each component may have more than one user and a user may interact with multiple components. Several users might access different data or capabilities on a single device, and one user might have varying rights to multiple devices. Multiple devices may need to broker permissions on behalf of a single user account, and so on. Be sure the IoT system can handle these complex trust and authentication schemes.

AOITI Basic Privacy Principles

The Alliance for IoT Innovation (AIOTI) organised a workshop in 2016 in Sophia Antipolis, France, to explore and identify design principles for IoT security.[107] One of the workshops was dedicated to practical privacy in IoT, and participants identified the following principles.

AIOTI Basic Requirements on Practical Privacy in IoT	
1	Common Understanding – Design, manufacturer and assemble components of Things and IoT ecosystems with clear understanding of what means what, and to what extent there is consensus in the related complex value chain and ecosystems. Promoting the goals of data protection such as limiting the scope of data processing to the necessary level; data segmentation, mapping, categorisation, purpose limitation, data isolation, and data control and data access of personal data are seen as prerequisite elements.
2	No Personal Data by Default, 'As-If' by Design & De-Identification by Default – Data minimalisation starts with only requesting, collecting, obtaining, deriving and processing personal data to the extent necessary (need-to-know principle), and. The 'As-If' principle it to design and engineer ecosystems in IoT as if these will (now or in a later phase) process personal data. The As-If principle is closely related to the privacy by design and privacy by default principles. Design de-Identification capabilities so personal data is de-identified as soon as legally possible.
3	Manufacturer-Implemented Parametrisation – Rights management for accessing data controlled by the user based on the assessment where and when a Thing or IoT ecosystems in its life cycle comes into contact with personal data, creates/derives (new) personal data, or otherwise processes personal data, while keeping in my mind the contextuality of purposes and use, as well as multi-purpose Things and IoT ecosystems.

107 AIOTI Workshop On Security and Privacy in the Hyper-Connected World, Report, 2016

4	Accountability & Risk Impact Assessment by Design – Any data controller and processor to be accountable for regulatory, contractual and ethical compliance. If data is compromised, disclosed, accessed or lost, clear statement by vendors, data controllers and data processors on impact is another prerequisite.
5	Awareness & Information Supplied with Indication of Purpose – Technically regulating access to data to define who can use it for what purpose, and how that can be made transparent, and subsequently measured and monitored. Design in a transparent way, so the data subject is and remains clear and aware of privacy issues, choices it makes and possible consequences thereof.

5.1.2 Key Findings

- There is no single set of IoT security and privacy principles that is internationally recognised and adopted.
- The diversity in proposed IoT security principles between different countries and initiatives illustrates a lack of collaboration, especially between governments.
- Due to the lack of globally-adopted principles, a language towards common understanding of shared IoT challenges and issues is lacking. Such a language is required to define a global governance process.
- Consumers and companies are not uniformly aware of the cybersecurity risks and may not be equipped to respond properly.

5.2 IOT SECURITY STANDARDS AND GUIDELINES

While numerous standards exist in the IoT space, IoT *security* has not been standardised significantly until now; a recent ETSI standard is one of the first efforts to standardise IoT security.[108] While numerous sets of IoT security recommendations exist, it is important to harmonise and align these for global acceptance and adoption as a precursor to developing evaluation and certification schemes.

5.2.1 Current Landscape and Recent Developments

Standards development organisations (SDOs) such as ITU[109], NIST[110], ETSI[111], IETF[112], and ISO[113] have all undertaken IoT-specific efforts. Gartner's Hype Cycle for IoT Standards and Protocols[114] profiles as many as 30 IoT standards, 15 of which have been marked to deliver "high business benefit." Six of those are expected to become mainstream in the next five years, including the below networking standards.

- 6LoWPAN: IPv6 over Low-Power Wireless Personal Area Networks is an IETF standard to deliver IPv6 connectivity over non-IP networking technologies such as NFC and LoRa using extremely low power, such that compliant devices can potentially run for years on battery power.
- OneM2M: a machine-to-machine service layer that can be embedded in hardware and software to connect devices.
- Random Phase Multiple Access (RPMA): a proprietary standard for connecting IoT objects.
- Sigfox: a proprietary low-power, low-throughput technology for IoT and machine-to-machine (M2M) communications.

108 https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security
109 https://www.itu.int
110 https://www.nist.gov/
111 http://www.etsi.org/
112 https://www.ietf.org/
113 https://www.iso.org
114 https://www.gartner.com/doc/3762285/hype-cycle-iot-standards-protocols

While many of the above standards include a security component, this section focuses on recommendations that deal with IoT security in general. Technical networking standards (including security aspects) are discussed in the section on Secure Communications and Infrastructure.

The UK Department for Digital, Culture, Media & Sport (DCMS), the EU Agency for Network and Information Security (ENISA), the Alliance for IoT Innovation (AIOTI), and GSMA[115] have released recommendations, guidelines or good practices specifically for IoT security. We briefly discuss these below.

UK Code of Practice

DCMS UK has proposed a Code of Practice[116] for the security of consumer IoT products and associated services. The Code identifies that many severe 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. Minimise 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,
11. Make it easy for consumers to delete personal data,
12. Make installation and maintenance of devices easy,
13. Validate input data.

The Code of Practice is based on IoT security recommendations from the PETRAS IoT Hub[117]. In February 2019, the European Standards Organisation ETSI launched a globally-applicable industry standard for IoT devices based on the Code of Practice.[118] It is expected that CEN/CENELEC will also be involved in the further development and dissemination of this standard (see https://www.cencenelec.eu/standards/Sectorsold/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx).

ENISA Security Recommendations

The Baseline Security Recommendations for IoT from ENISA[119] include a number of policy, organisational and technical measures. Technical measures include the use of a hardware-based immutable root of trust, and security features such as specialised security chips / coprocessors that integrate security at the transistor level providing trusted storage of device identity, protecting 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 possibly challenging to implement in practice.

AIOTI Recommendations for Standards

AIOTI has done considerable work in this area, as referenced by the activity underway within the AIOTI Standards Working Group[120] (WG03). According to AIOTI, basic requirements for IoT devices include[121]:

– Testing and Certifying Security – Using existing, proven certifications recognised as state-of-the-art based on assessed risk level; additional introduction of a classification system to certify devices for particular use-case scenarios depending on the level of risk.

115 https://www.gsma.com/
116 https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
117 https://www.petrashub.org/
118 https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security
119 ENISA 'Baseline Security Recommendations for IoT', November 2017
120 https://ec.europa.eu/digital-single-market/en/news/internet-things-platforms-and-standardisation-workshop
121 AIOTI Workshop On Security and Privacy in the Hyper Connected World Report 20160616

- Security Labels – Proven labels such as an 'Energy efficiency label' of appliances in order to classify the IoT device.
- Preset Certified Security Structures – Encryption requirement for identities, access, communication channels and secure storage of keys and to store data at rest – also for secure boot process.
- Security Rationale – Explanation of implemented security measures related to well understood hazards in order to define acceptable level security risks from any designer of IoT device, auditable by independent third party.
- Information exchange – Sharing information about incidents/potential vulnerabilities between manufacturers.
- Defined functions – IoT devices should only be able to perform documented functions, making sense for device/service.
- Standardisation – Interoperability of components and communication protocols.

NIST IoT Cybersecurity Program

NIST's Cybersecurity for the Internet of Things (IoT) Program[122] is undertaking efforts to identify a core set of cybersecurity capabilities to form a baseline for IoT devices. In September 2018, NIST released a publication entitled "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" in order to help federal agencies and other organisations better understand and manage the cybersecurity and privacy risks associated with their IoT devices throughout device lifecycles[123]. This publication is intended to be an introductory foundation for a planned series of publications on more specific aspects of this topic. As of mid-2019, NIST is focusing on engaging with stakeholders[124] via workshops, seminars and a draft discussion paper[125] in order to gather feedback for a Core IoT Cybersecurity Capabilities Baseline.

Industrial Internet of Things Security Framework[126]

Early IoT applications included industrial control systems, or Operational Technology (OT), that converged with IT to create an Industrial IoT. Such an IoT system connects and integrates industrial control systems with enterprise software and business processes and analytics to improve decision-making, operations and collaboration among a large number of increasingly autonomous control systems. The Industrial Internet Consortium's IIoT Security Framework approaches IoT in a generic and detailed manner, and provides concrete recommendations for endpoint security, communications security, and data protection, making this report highly relevant for IoT device manufacturers.

GSMA IoT Security Guidelines[127]

The telecommunications industry, which the GSMA represents, has a history of providing secure products and services to their customers at a very large scale. According to the GSMA, the provision of secure products and services is as much a process as it is a goal. Vigilance, innovation, responsiveness and continuous improvement are required to ensure that the solutions address the threats. To help ensure that the new IoT services coming to market are secure, the GSMA has created a comprehensive set of security guidelines[128] for the benefit of service providers who are looking to develop new IoT services.

Taking this a step further is GSMA's assessment checklist[129], which enables the suppliers of IoT products,

122 https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
123 https://csrc.nist.gov/publications/detail/nistir/8228/final
124 https://www.nist.gov/blogs/i-think-therefore-iam/lets-talk-about-iot-device-security
125 https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf
126 http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
127 https://www.gsma.com/iot/iot-security/iot-security-guidelines/
128 IoT Security Guidelines Overview Document, Version 2.0, 31 October 2017
129 https://www.gsma.com/iot/iot-security-assessment/

services and components to self-assess the conformance of their products, services and components to the GSMA IoT Security Guidelines. Completing a GSMA IoT Security Assessment Checklist allows an entity to demonstrate the security measures they have taken to protect their products, services and components from cybersecurity risks. Assessment declarations can be made by submitting a completed declaration to the GSMA.

5.2.2 Key Findings

- Security standards and guidelines are required for development and operations to stimulate the adoption of secure IoT devices.
- A number of IoT security good practices, guidelines and recommendations exist, but efforts from established standards development organisations such as ETSI and NIST are very recent.
- Manufacturers may not have the expertise to make use of the available guidelines and recommendation. Usability of security guidelines is a challenge and requires more research.
- Harmonisation of IoT security guidelines and recommendations is required to stimulate adoption. Harmonisation should be supported by global cybersecurity research initiatives.
- It is important for standardisation processes to stay aligned with technological developments without stifling innovation.

5.3 EVALUATION AND CERTIFICATION

A comprehensive global IoT certification framework or self-certification solution does not yet exist; it remains an open challenge to develop globally recognised and adopted cybersecurity evaluation and certification regimes for IoT devices. Given that a system of secure components is not by definition a secure ecosystem, evaluation and certification regimes should include individual components, the wider network of systems and components, and the global ecosystem.

An evaluation and certification scheme should be based on a generic and common framework, possibly with business- or application-specific provisions. Such a framework may provide assurance similar to the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). An alternative approach to certification may be to strengthen and modernise liability laws to encompass IoT products and ecosystems; this is discussed in the section on Responsible Industry Ecosystem.

5.3.1 Current Landscape and Recent Developments

Independent laboratories such as UL[130], Brightsight[131], and Riscure[132], as well as government bodies such as US-CERT of the U.S. Department of Homeland Security, provide cybersecurity assessment and certification services and typically focus on vulnerability scanning and architecture design reviews. While they have taken early steps in IoT, they may not be ready for more comprehensive functional testing of IoT devices or for domain-specific testing; for instance, the security of a software application can be tested but not the effects that cascade from cybersecurity to functional safety. This is also because of the lack of globally-accepted IoT security standards and certification schemes to test and certify against.

Trusted IoT security labels

An IoT security label should give a baseline security requirement of protection, and the level of assurance for

130 https://www.ul.com/inside-ul/ul-2900-2-3-helps-mitigate-iot-cybersecurity-risk/ --- New Standard for Software Cybersecurity for Network-Connectable Products UL 2900 / ANSI https://industries.ul.com/blog/new-standard-for-software-cybersecurity-for-network-connectable-products

131 https://www.brightsight.com/en/archieven/1111

132 https://www.riscure.com/market/iot-healthcare/

this needs to be defined. The label should provide a clear indication of the security achieved. AIOTI's workshop on Security and Privacy in the Hyper-Connected World[133] introduced a set of possible labels:

1) Security certified by third party
2) Managed security (maintained)
3) Secure update mechanism implemented (maintainable)
4) Access-controlled device, based on "trusted manufacturer" and self-assessment of security
5) No security.

Separately, the Ministry of Economic Affairs and Climate and the Ministry of Justice and Security in the Netherlands[134] have requested the industry to design a security labelling system and guidelines specifying:

- Level of security,
- Whether the device is automatically updated,
- Lifespan of support by the manufacturer,
- Device performance and functions when it is disconnected from the internet.

In parallel, during the 2018 edition of the Singapore International Cyber Week (SICW)[135], the Cyber Security Agency of Singapore hosted a leadership dialogue with various National Certification Bodies to exchange perspectives on a practical and balanced approach to address the evaluation of IoT devices, in consideration of the fact that this space is characterised by fast-moving innovations.

IoT Security Foundation

The IoT Security Foundation's (IoTSF) IoT Security Compliance Framework[136] aims to consistently evaluate the security of a wide range of IoT devices. To make the framework more practical across a variety of applications, IoTSF adopts a risk-based approach derived from the commonly used CIA Triad. The framework defines five Compliance Classes that achieve progressively higher levels of Confidentiality, Integrity and Availability as depicted in Figure 8.

- Class 0: where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or organisation.
- Class 1: where compromise to the data generated or loss of control is likely to result in limited impact on an individual or organisation.
- 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 organisation, or impact many individuals. For example, by limiting operations of an infrastructure to which it is connected.

Compliance class	Security objectives		
	Confidentiality	**Integrity**	**Availability**
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

Figure 8: *IoTSF Compliance Classes[137]*

133 AIOTI Workshop On Security and Privacy in the Hyper-Connected World Report 20160616

134 https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software - Roadmap digitaal veilige hard en software, 2018. By Ministry of Economic Affairs, the Netherlands, in Dutch.

135 https://www.sicw.sg/

136 https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

137 https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

– 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.

Based on the Compliance Class determined for a particular product, a checklist of requirements is provided. Such a checklist could be made mandatory by procuring parties, as could a third-party audit to verify compliance with the checklist.

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 recognised 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 robustness of the evaluation depends on the desired Evaluation Assurance Level (EAL). In theory, this approach allows an IoT product developer to demonstrate that their product meets specific security functional requirements.

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) recognise CC certification[138] and specifically the collaborative Protection Profiles (cPPs)[139]. The cPP for Network Devices v2.1[140] 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.

Separately, the German Federal Office for Information Security (BSI)[141] advocates for trustworthy products and systems in the energy network and has developed a protection profile for the gateway of a smart metering system[142] that follows the rules of Common Criteria in describing the threats to a certain target that needs protection and defining the minimum requirements for appropriate safety precautions.

While well established, CC certification is often said to be a slow and expensive process typically costing manufacturers six figures and taking many months[143]. While it appears well-suited for testing computer systems for sale to governments, it may not be as appropriate for the fast-moving and low-cost world of IoT. Non-CC alternatives can

138 https://www.csa.gov.sg/programmes/csa-common-criteria
139 https://www.commoncriteriaportal.org/pps/?cpp=1
140 https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf
141 https://www.bsi.bund.de/EN/Home/home_node.html
142 https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf
143 Standardisation and Certification of Safety, Security and Privacy in the 'Internet of Things', JRC Technical Report, Leverett et al.

provide a light-touch approach to certification and may prove more suitable.

EU Cybersecurity Certification Framework

The European Union has identified that certification plays a critical role in increasing trust and security in products and services that are crucial for the EU Digital Single Market . At the moment, a number of different security certification schemes for ICT products exist in the EU. For example, smart meter producers currently need to undergo separate certification processes in France, the UK and Germany. Without a common framework for EU-wide valid cybersecurity certificate schemes, the EU identifies an increasing risk of fragmentation and barriers in the single market.

In this context, the EU has proposed an EU Certification Framework 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. ENISA will work towards implementing this certification process. The resulting certificate will be recognised in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

While the use of certification 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.

144 http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm

145 https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

5.3.2 Key Findings

- There is a distinct lack of labels to inform end users about IoT device security and risks. However, efforts to create a labelling scheme are under way in various parts of the world. It should be ensured that these schemes are aligned in order to create a level playing field for vendors.
- There are as yet no CC cPPs specifically for IoT devices. It should be determined whether these can be generic or specific to application domains.
- Non-CC alternatives can provide a light-touch approach to certification and should be explored.

5.4 FUTURE-PROOF LEGISLATION

Legislative policy solutions should be sufficiently flexible to deal with societal needs as well as constantly evolving technologies. Regulatory measures for IoT security should make use of inputs from consumers as well as industry representatives on the rights and responsibilities of consumers and vendors. This would help to ensure that the approach taken is effective in the present and fit for the future, and promotes innovation in an efficient way. The introduction of highly stringent measures and legislation by regulators could, counterproductively, prove restrictive for security research; it may be more effective to instead create initiatives to stimulate the development of security by the industry.

Besides cybersecurity regulations, liability laws can also effectively drive IoT security; the section on Responsible Industry discusses this point.

5.4.1 Current Landscape and Recent Developments

There are only a few legislative efforts aimed at IoT security; we describe these below. It is noted that IoT security is differently organised in different countries, so not every cybersecurity agency is tasked with the same roles and responsibilities. While many industry organisations globally collaborate on a voluntary basis, we found a dearth of initiatives where governments work together for secure IoT.

U.S. IoT Cybersecurity Improvement Act of 2017

For years, cybersecurity experts have asked the US government to improve cybersecurity hygiene and use its buying power to push through new security standards.[146] The IoT Cybersecurity Improvement Act (see https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt) is a bill mandating minimal cybersecurity operational standards for Internet-connected devices purchased by U.S. Federal agencies. This can be a way to raise the bar across the industry more easily than larger, more direct legal measures. Government-purchased IoT devices would need to:

- Be free of known security vulnerabilities, as defined in the NIST National Vulnerability Database[147].
- Have software or firmware components that accept "properly authenticated and trusted" patches from the vendor.
- Use non-deprecated, industry-standard protocols for communication, encryption, and interconnection with other devices or peripherals.
- 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 replaced to fix any vulnerability in a timely and secure manner.

The legislation would also require American agencies to establish and maintain inventories of IoT devices and update them every 30 days.

U.S. SMART IoT Act

The State of Modern Application, Research, and Trends of IoT Act or SMART IoT Act directs the U.S. Department of Commerce to conduct a study on the state of IoT in the United States.

California Senate Bill 327

California's SB 327 law[148], 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, it is nevertheless widely considered a good start.[149,150]

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. The complex mesh of stakeholders involved asks for/implies the necessity of a precise allocation of legal responsibilities among them regarding the processing of the individual's personal data, based on the specificities of their respective interventions.

EU Cybersecurity Act

In December 2018, the European Union passed the Cybersecurity Act[151] to reinforce the mandate of the EU Agency for Cybersecurity (ENISA) to better support Member States with tackling cybersecurity threats and attacks. As referenced in the previous section, the Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices. Certification is voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to satisfy a specific security need.

146 https://www.wired.com/2008/08/securitymatters-0807/
147 https://nvd.nist.gov/
148 http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
149 https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html
150 https://www.zdnet.com/article/first-iot-security-bill-reaches-governors-desk-in-california/
151 https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

Common Position on Cybersecurity in Connected Devices

The Common Position paper[152] by Infineon, NXP, STMicroelectronics and ENISA proposes some key priorities for the European Commission (EC), but these priorities are globally applicable:

- Define baseline requirements for security and privacy that minimise risk, are neutral in technological terms, and remain open to innovation.
- Introduce a Trust Label, based on various security levels and a related risk assessment.
- Ensure that reliable security processes and services are developed and support industry in implementing security features in products (e.g. through providing information and training on state-of-the art security solutions).
- Encourage the development of mandatory staged requirements for IoT security and privacy.
- Create an equal level playing field for cybersecurity and look into incentives to reward the use of good security practices.

NIS Directive

The Directive on security of network and information systems (NIS Directive) was adopted by the European Parliament on 6 July 2016[153] and entered into force in August 2016 . The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring

- Member States' preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.
- cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States.
- a culture of security across sectors that are vital for the economy and society, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by Member States as operators of essential services are required to take appropriate security measures and notify serious incidents to the relevant national authority.

5.4.2 Key Findings

- Although there are numerous industry initiatives and best practices in this area, their adoption is voluntary. IoT security legislation is in its infancy and virtually non-existent outside the US and EU.
- Enforcing procurement by governments of secure IoT devices can contribute towards IoT security when large countries participate; smaller economies such as Singapore and the Netherlands can work together for greater impact. The EU's single digital market approach can support IoT security as well.

5.5 RESPONSIBLE INDUSTRY ECOSYSTEM

The market for IoT devices is global. Within this competitive industry, time-to-market, usability and cost are key considerations. The razor-thin margins for IoT devices leave suppliers with less to spend on security. From the perspectives of cybersecurity and national security, security must also become part of the business equation; the cost of implementing security functionality needs to be offset in some manner. Currently, owing to the lack of enforcement of security in IoT devices, there is no level playing field for IoT device vendors nor a common expectation of security functionality.

5.5.1 Current Landscape and Recent Developments

The competitive advantage in the IoT industry is currently focused on time-to-market rather than secure-to-market. This balance should be shifted so that a specific level of security and privacy is required before market release. Defining security frameworks supported by baseline security measures can be a way forward in this direction.

152 https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

153 https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

The use of certification and labelling can encourage better understanding and transparency in terms of IoT security and can additionally benefit end users and consumers by educating them and making them more aware of IoT security. Alternatively and perhaps complementarily, liability laws can be strengthened and modernised to hold manufacturers accountable in the event of a breach.

Figure 9: *Regulatory Approaches to IoT Security*

Regardless of the regulatory approach adopted, it is important for cybersecurity regulators as well as the industry to work together and act as a global community that learns from incidents and vulnerabilities proactively. This requires an open culture of sharing incidents and mutual learning.

Liability

Product liability is the area of law in which manufacturers, distributors, suppliers, retailers, and others who make products available to the public are held responsible for damage caused by those products. The Dutch roadmap for safe hardware and software[154] has identified liability laws as a key driver for IoT security.

Liability litigation historically focused on negligence on the part of the vendor, or a breach of warranty. Under the notion of *strict* liability, the manufacturer is liable if the product is defective even if the manufacturer was not negligent in making that product defective[155]. The manufacturer thus becomes a de facto insurer against its defective products, with premiums built into the product's price. Strict liability also seeks to diminish the impact of information asymmetry between manufacturers and consumers: manufacturers have better knowledge of their own products' dangers than do consumers; therefore, manufacturers should bear the burden of finding, correcting, and warning consumers of those dangers.

The 1985 European Product Liability Directive[156] created a regime of strict liability for defective products: according to this Directive, a product is “defective” when it does not provide the “safety which a person is entitled to expect” (Article 6). While one may assume that this provides a baseline of liability for IoT devices, the use of the term “safety” is telling – security issues that are not outright safety defects may not be addressed at all unless those security issues can be proven to cascade into safety losses or traditional damage such as harm to human health or property. Even more fundamentally, Article 2 of the Directive states that it applies to “movables” – while this may have seemed perfectly reasonable in the 80s for products such as toasters or lawn mowers, for modern connected devices this terminology may entirely exclude the connectivity and server-side components. A recent EU research report[157] identifies that vendors may take advantage of this by simply placing critical functionality on the server in order to escape liability.

154 https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software - Roadmap digitaal veilige hard en software, 2018. By Ministry of Economic Affairs, the Netherlands, in Dutch.

155 https://en.wikipedia.org/wiki/Strict_liability

156 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985L0374:en:HTML

157 Standardisation and Certification of Safety, Security and Privacy in the ‘Internet of Things’, JRC Technical Report, Leverett et al.

Liability issues for IoT need to be addressed in the context of global and national legislation and case law; in most cases, liability legislation will need to be modernised to account for the unique nature of the IoT ecosystem.

Industry collaborations

The inventory of initiatives in Annex B shows a substantial number of industry collaborations. AIOTI[158] is an example of industry collaboration that promotes good practices across the diverse IoT ecosystem. The IoT Consortium[159] is an industry body that aims to stimulate the growth of the IoT market by leading the industry's efforts through strategic partnerships. Specifically, it generates opportunities for companies to meet and collaborate, forms industry committees to identify and address areas of common concern, exercises thought leadership in driving forward the most important conversations on IoT at industry events and in the press, promotes business development opportunities, and leads efforts to raise IoT awareness among consumers, sales channels, and investors.

IoT-EPI[160] is a European initiative for industry collaborations in IoT platform development. At the core of IoT-EPI are seven research and innovation projects: Inter-IoT, BIG IoT, AGILE, symbIoTe, TagItSmart!, VICINITY and bIoTope. Each project is run by several industry partners in collaboration and aims to solve one of the issues currently faced by the IoT ecosystem. For instance, Big IoT[161] addresses the interoperability gap by defining a generic, unified Web API for smart object platforms, with the intention of establishing a marketplace where platform, application, and service providers can easily monetise their assets. Big IoT is spearheaded by Siemens AG (Germany), Bosch Software Innovations (Germany), and Atos (Austria).

Within these initiatives the role of governments is limited; indeed, close collaboration between governments appears uncommon. Within the European Union, ENISA[162] is a key player in this domain to establish collaborations.

5.5.2 Key Findings

- Owing to the lack of legislation and regulation to enforce security in IoT devices, there is no level playing field for IoT device vendors nor a common expectation of security functionality.
- Liability is likely to be an effective mechanism to drive the industry towards IoT security, but legislation needs to be modernised to address IoT.
- Encouragingly, numerous industry collaborations exist and provide opportunities for knowledge sharing and mutual learning; however, the role of governments in such initiatives appears limited especially outside the EU.

5.6 SUPPLY CHAIN SECURITY

Modern products are assemblies of parts and components 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 using complex, globally distributed, and interconnected supply chains composed of various entities with multiple tiers of outsourcing.

However, vulnerabilities can be introduced and exploited at any point in the supply chain.[163] Cyber supply chain risks include the insertion of counterfeits, unauthorised production, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices upstream.

158 Alliance for Internet of Things Innovation - https://aioti.eu
159 https://iofthings.org/about/
160 https://iot-epi.eu/
161 https://iot-epi.eu/project/big-iot/
162 https://www.enisa.europa.eu/
163 https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management

5.6.1 Current Landscape and Recent Developments

Managing cyber supply chain risks requires ensuring the integrity, security, quality and resilience of the supply chain and its products and services. Supply chain security is an often-overlooked component in IoT security even though, by some estimates, up to 80% of breaches may originate in the supply chain[164]. In 2011, the Semiconductor Industry Association estimated[165] 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 significant consequences.

The U.S. National Institute of Standards and Technology (NIST)[166] identifies Cyber Supply Chain Risk Management (C-SCRM) as the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT products and service supply chains.[167] NIST's workshop on Best Practices in C-SCRM[168] discussed that the global complexity of supply chains, the increase in potential disruptions, and emerging cybersecurity risks to the supply chain have dramatically increased the risks that:

- Suppliers could intentionally or unintentionally introduce software, firmware, or hardware in which confidentiality, integrity or availability has been compromised.
- Supply chain disruptions could create a scramble for parts that enables poor quality or counterfeit products to enter the supply chain.
- High-value intellectual property shared with suppliers could be misused.
- Service suppliers – including contract manufacturers, outsourced legal and accounting, and repair and maintenance providers – could tamper with a company's information based on their access to a company's information system, if the data is not adequately protected.
- Adversaries can use vulnerabilities of different components within the supply chain to attack a company's information systems.

IoT supply chain risks, and more generally IT supply chain risks, are associated with an organisation's decreased visibility into, and understanding of, how the technology they acquire is developed, integrated, and deployed.[169] Maintaining sufficient controls to minimise risk and maximise transparency requires close relationships with vendors, clear understanding of the risks involved and strict adherence to procedure.

According to NIST, a primary objective of C-SCRM is to identify, assess, and mitigate "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain." C-SCRM activities include:

- Determining cybersecurity requirements for suppliers,
- Enacting cybersecurity requirements through formal agreement (e.g., contracts),
- Communicating to suppliers how those cybersecurity requirements will be verified and validated,
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies,
- Governing and managing the above activities.

164 Combatting Cyber Risks in the Supply Chain - https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252

165 https://www.semiconductors.org/news/2011/11/08/news_2011/sia_president_testifies_at_ senate_armed_services_committee_on_dangers_of_counterfeit_chips/

166 https://www.nist.gov/

167 https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management

168 https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Business-Case.pdf

169 NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organisations

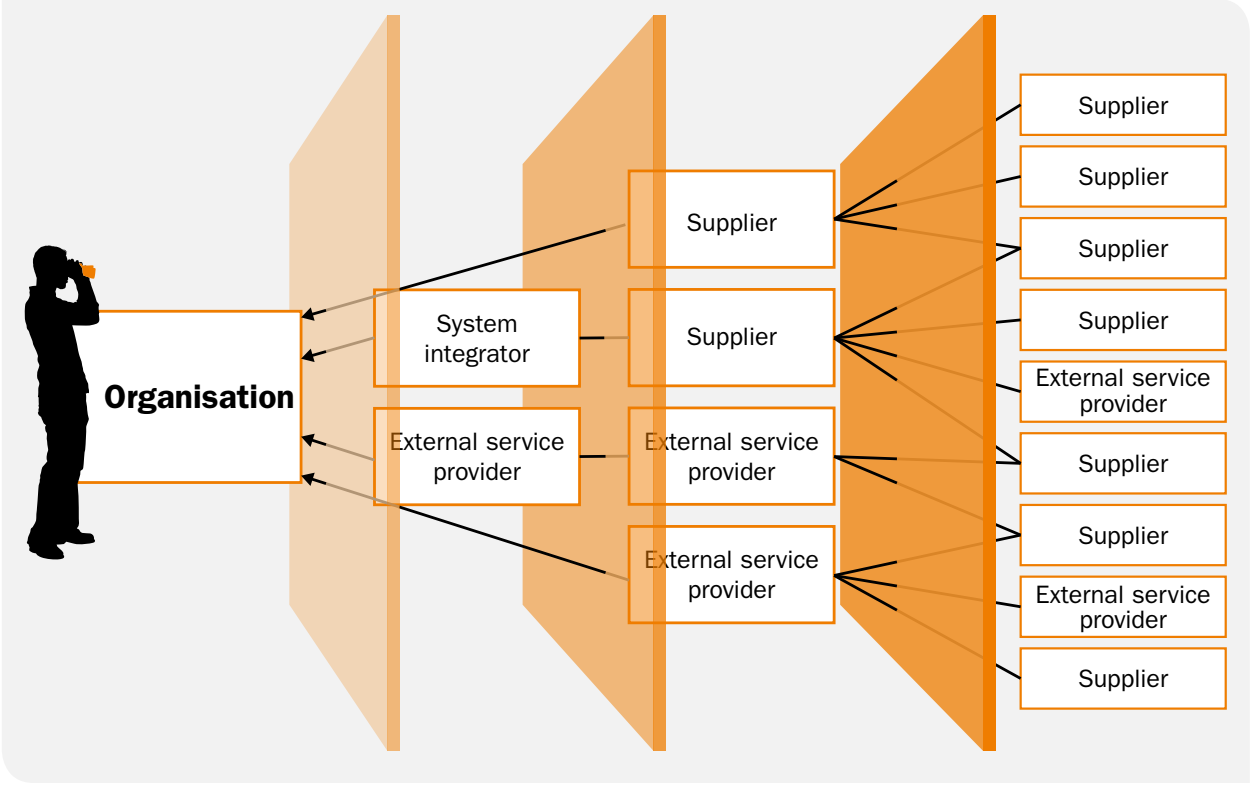


Figure 10: *Organisational Supply Chain (Source: NIST)*

The U.K.'s National Cyber Security Centre (NCSC)[170] provides 12 principles for supply chain security, including the establishment of minimum security needs for suppliers and building security considerations into contracting processes (and ensuring that the suppliers do the same).

While the principles proposed by NCSC may appear intuitive, they are followed by a surprisingly low percentage of organisations. The U.K. Cyber Security Breaches Survey 2016[171] survey showed that, while most businesses have rules or controls for their own operations (and most medium or large organisations have formally documented their approaches), they are much less likely to set minimum standards for their suppliers: only 13% were seen to do this.

170 https://www.ncsc.gov.uk/collection/supply-chain-security
171 Cyber Security Breaches Survey, Klahr et al, Ipsos MORI, DCMS UK

1. UNDERSTAND THE RISKS
- Understand what needs to be protected and why
- Know who your suppliers are and build an understanding of what their security looks like
- Understand the security risk posed by your supply chain

2. ESTABLISH CONTROL
- Communicate your view of security needs to your suppliers
- Set and communicate minimum security requirements for your suppliers
- Build security considerations into your contracting process and require that your suppliers do the same
- Meet your own security responibilities as a supplier and consumer
- Raise awareness of security within your supply chain
- Provide support for security incidents

3. CHECK YOUR ARRANGEMENTS
- Build assurance activities into your approach to managing your supply chain

4. CONTINUOUS IMPROVEMENT
- Encourage the continuous improvement of security within your supply chain
- Build trust with suppliers

Figure 11: *Principles of Supply Chain Security (Source: NCSC/CPNI)*

Supply chain security is predicated on careful supplier management. Examples of best practices in supplier management from a security perspective include the following[172].
- Procurement and sourcing processes are developed jointly with input from IT, security, engineering, and operations personnel; sourcing decisions receive multi-stakeholder input.
- Standard security terms and conditions are included in all requests for proposals (RFPs) and contracts, tailored to the type of contract and business needs.
- Since many risk assessments depend on supplier self-evaluation, a number of companies employ on-site verification and validation of these reviews. Some companies cross-train personnel to be stationed at supplier companies so that security criteria can be monitored year-round.
- New suppliers enter a test and assessment period – to test the capabilities of the supplier and its compliance with various requirements – before they actively join the supply chain. In high risk areas, for example, a supplier might go through a series of pilots before they fully enter the supply chain.
- Quarterly reviews of supplier performance are assessed among a stakeholder group.
- Annual supplier meetings ensure that suppliers understand the customers' business needs, concerns and security priorities.
- Mentoring and training programs are offered to suppliers, especially in difficult or key areas of concern to the company, such as cybersecurity.

It may be noted that organisations wield both contractual and economic power over suppliers: contracts can stipulate security requirements and penalties in detail, and economic clout can be multiplied via industry and inter-governmental alliances. According to NIST, organisations can pose the following specific questions[173] to suppliers to determine the

172 https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/Best-Practices

173 https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

risk levels associated with their suppliers' cybersecurity practices.

- Is the supplier's software/hardware design process documented? Repeatable? Measurable?
- How is configuration management performed? Quality assurance? How is code tested for quality or vulnerabilities?
- What steps are taken to "tamper proof" products? Are backdoors closed?
- Is the mitigation of known vulnerabilities factored into product design (through product architecture, run-time protection techniques, code review)?
- How does the supplier stay current on emerging vulnerabilities? What are the capabilities to address new "zero day" vulnerabilities?
- What controls are in place to manage and monitor production processes?
- What levels of malware protection and detection are performed?
- What physical security measures are in place? Documented? Audited?
- What access controls, both cyber and physical, are in place? How are they documented and audited?
  - How do they protect and store customer data? How is the data encrypted?
  - How long is the data retained?
  - How is the data destroyed when the partnership is dissolved?
- What type of employee background checks are conducted and how frequently?
- What security practice expectations are set for upstream suppliers? How is adherence to these standards assessed?
- How secure is the distribution process? Have approved and authorised distribution channels been clearly documented?
- What is the component disposal risk and mitigation strategy?
- How does the supplier ensure security throughout the product life-cycle?

NIST's workshop on Best Practices in C-SCRM further identified[174] that vetting supply chain partners beyond the first tier is a challenge for many companies: manual methods can be difficult and do not scale for companies with hundreds or thousands of tier-one suppliers and numerous sub-tier suppliers. Additionally, smaller companies lack the economic power and relationships to get the information they need. To fill these gaps, consultants such as BitSight[175] offer to collect, manage and centralise supplier risk management data. This can result in increased efficiencies for organisations as well as reduce the burden on suppliers who may be asked to fill out similar informational forms for each customer.

According to ENISA's Baseline Recommendations[176], "For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to suppliers and partners." Standards such as ISO28000[177] specify supply chain security requirements in sufficient detail to allow self-declaration of conformance by an organisation or, alternatively, third-party certification by an accredited body to demonstrate contribution to supply chain security.

Emphasising the importance of supply chain risks, NIST's Risk Management Framework (RMF)[178], which is published as NIST SP 800-37 Revision 2, integrates supply chain risk management concepts into the RMF to protect against untrustworthy suppliers, insertion of counterfeits, tampering, unauthorised production, theft, insertion of

174 https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf
175 https://www.bitsight.com/
176 Baseline Security Recommendations for IoT, ENISA, Nov 2017
177 https://www.iso.org/standard/44641.html
178 https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview

malicious code, and poor manufacturing and development practices throughout the SDLC.

5.6.2 Key Findings

- IoT hardware and software manufacturers and suppliers should adopt a cyber supply chain risk management framework (ISO28000, NIST).
- Cybersecurity requirements, risk and liability should be cascaded into the supply chain via contractual agreements. Organisations wield both contractual and economic power over suppliers.
- It is important to encourage the use of open frameworks and provide transparency for supply chain security information flows.

5.7 PRODUCT LIFECYCLE SUPPORT

Building a device today that will stand up to the ever-evolving security requirements of the next several years without any updates or modifications may well be impossible; in the absence of patching and device management, devices quickly become outdated from a security perspective. However, updates typically require changes in device firmware – this makes it difficult for regular users to manage these devices. Remote update capability needs to be designed into the device to allow security updates, yet, the specialised operating systems used for embedded devices may not support this by default. Further, the life cycle for IoT devices varies widely in duration: industrial devices may be in the field for decades, consumer products such as smart home appliances or autonomous vehicles could run for about 10 years, and wearables may be in use for only a year or two. Clearly, managing IoT device lifecycles is a tremendous challenge.

5.7.1 Current Landscape and Recent Developments

As ABI Research identifies[179], 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. Secure hardware (such as secure elements and secure MCUs) is at the forefront of providing this trust. Without this process, any future service provisioning for the device post-market is vulnerable. The increased recognition that this opportunity cannot be realised without trust is a potential driver for industry adoption of secure hardware.

Soos et al[180] present a model for IoT device lifecycle management that maps the phases of the IoT device lifecycle to three broad life stages: Beginning of Life (BoL), Middle of Life (MoL) and End of Life (EoL). Figure 12 depicts the security features and functions that should be in place during each step of a device's lifecycle.[181] During initialisation or boot-up, a firmware integrity check and secure boot process should be used to ensure that firmware and bootloader software have not been modified or tampered with. Once initialisation is complete, the communication between device and device, device and the Internet, or device and user interface (through mobile apps or web apps) should be encrypted. Authentication should use a second factor wherever possible, and default passwords must be changed. During normal operation, monitoring, analytics and audit procedures should be in place. The device should detect abnormal events and operations and provide a warning to the backend and/or end user. Secure firmware-over-the-air (FOTA) updates should themselves be integrity-checked and verified before installation.

179 IoT Security: From Design to Life Cycle Management, ABI Research

180 IoT Device Lifecycle – a Generic Model and a use case for Cellular Mobile Networks, Soos et al, Conference Paper Aug 2018

181 Device Life Cycle Overview, Steven Hsu, Trend Micro Whitepaper, https://www.trendmicro.com/us/iot-security/content/main/document/IoT%20Security%20Whitepaper.pdf

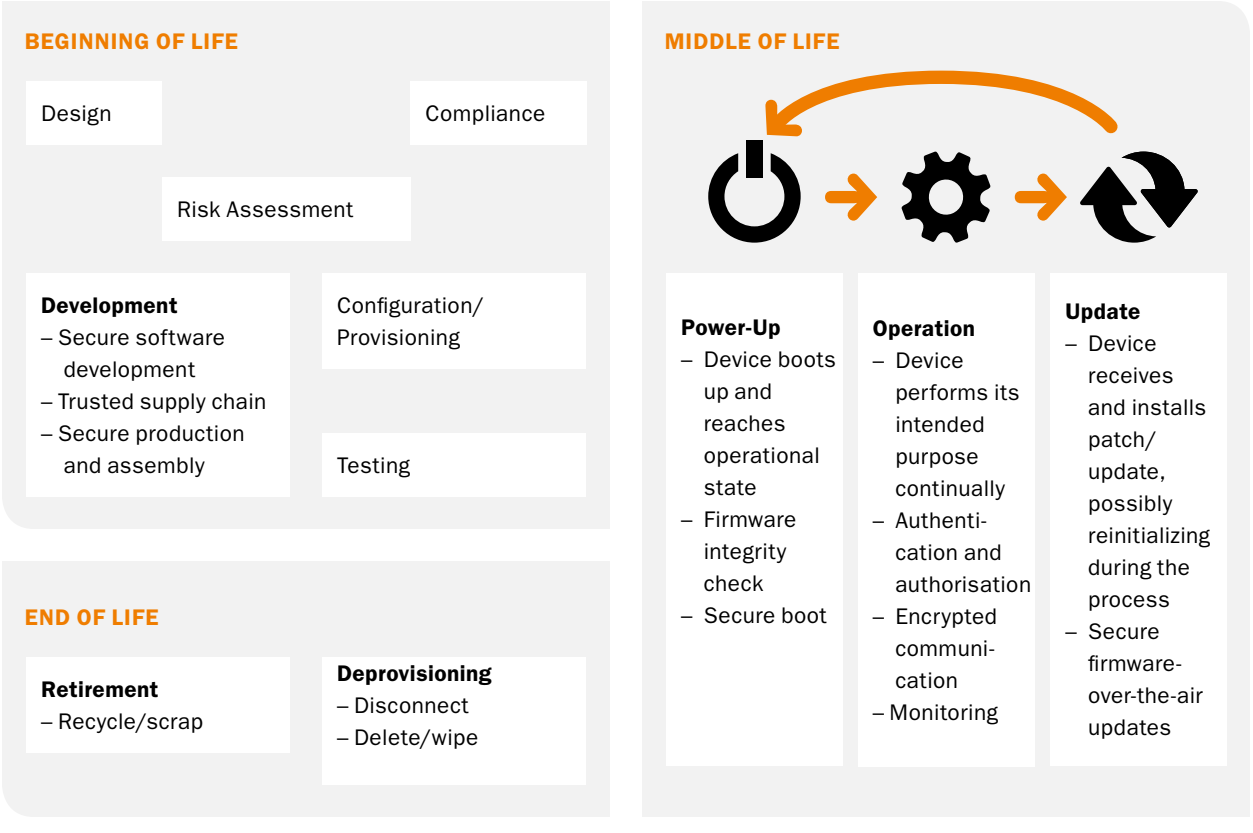


Figure 12: *Security Considerations Through the Device Lifecycle*

According to AIOTI[182], device management is defined as software or firmware updates as well as configuration or fault and performance management. Device management can be performed using existing protocols e.g. BBF TR-069[183] or OMA LWM2M[184].

Vulnerability Disclosure

History shows that vulnerabilities are invariably found after a product is deployed – and often exploited in "zero-day" attacks. It is vital to be able to detect unforeseen vulnerabilities, anomalies and threats in live IoT deployments, and to respond quickly, recover and remediate. A strategy to deal with discovered threats and vulnerabilities includes a Coordinated Vulnerability Disclosure (CVD) program that balances security with the interests of manufacturers and stakeholders, as well as a clear understanding of liability. CVD is standardised by the ISO[185] under ISO/IEC 29147 and ISO/IEC 30111. While

182 Alliance for Internet of Things Innovation - https://aioti.eu
183 https://www.broadband-forum.org/standards-and-software/technical-specifications/tr-069-files-tools
184 http://openmobilealliance.org/iot/lightweight-m2m-lwm2m
185 ISO Vulnerability Disclosure, https://www.iso.org/standard/72311.html

CVD is currently used mainly by the IT industry, it is imperative for open, standardised vulnerability management to be implemented across all sectors where security is becoming a critical component of safety.

Platform-Based Device Lifecycle Management

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 across the device lifecycle, e.g. device registration/enrolment, identity management, provisioning, permissions, monitoring and troubleshooting, status queries, and over-the-air (OTA) firmware updates. Platforms allow IoT users scale device fleets and may help to reduce the cost and effort of managing large and diverse IoT device deployments. Microsoft Azure, in particular, has comprehensive device management functionality built into its IoT Hub.[186] This includes the use of a "device twin" for each connected physical device that stores device metadata and essentially acts a proxy for the actual device.

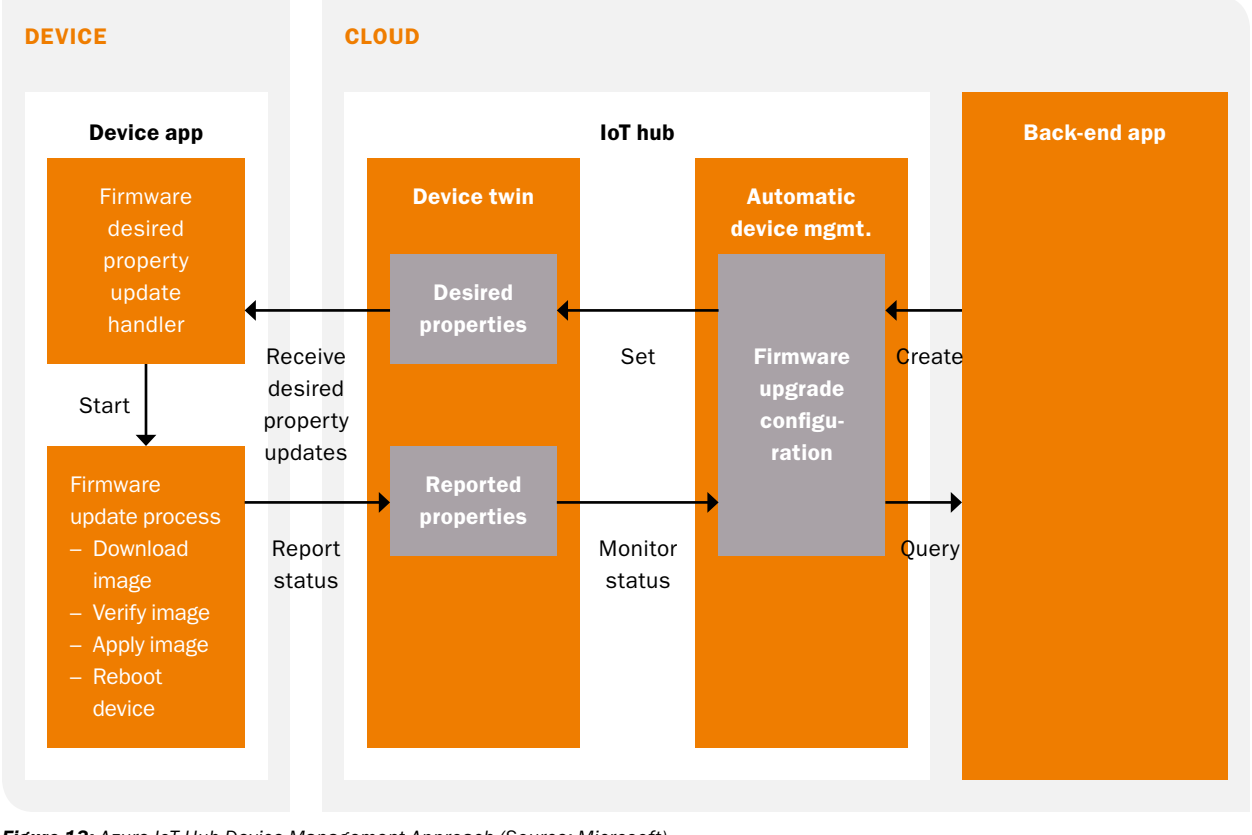


Figure 13: *Azure IoT Hub Device Management Approach (Source: Microsoft)*

186 https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-device-management-overview

5.7.2 Key Findings

- Keeping software up to date and allowing for patches and updates is critical for a secure IoT device. Updates should be delivered and deployed using a secure and verifiable methodology.
- Device manufacturers should adopt a secure software development lifecycle, with a documented vulnerability management process in accordance with ISO/IEC 29147 and ISO/IEC 30111.
- The manufacturer should bear responsibility for an IoT device throughout its product lifecycle, including a responsibility to manage suppliers.
- Existing device lifecycle management protocols include OMA LWM2M. Cloud-based IoT platforms offer comprehensive, albeit unstandardised, device management functionality.

5.8 DEVICE IDENTITY AND ROOT OF TRUST

The raison d'être for the Internet of Things are the Things themselves, i.e. the devices that interact directly with the physical world, measuring and sometimes controlling their environments. Securing these devices presents a challenge that is somewhat distinct from securing a laptop or a mobile phone. In this section we specifically discuss the security of the device and its firmware; the supply chain for the device and the management of its lifecycle are equally important and discussed in dedicated sections above. The device may run a minimal operating system (OS) and application and is expected to provide them with the necessary computational and storage resources as well as a secure execution environment. It is also noted that device security is closely linked to the security of its communication, since the device includes a connectivity module and authenticates itself as an initial step during any communicative exchange. Therefore, there are close links between the material discussed in this section and that presented in the sections on OS, communication, lifecycle and supply chain.

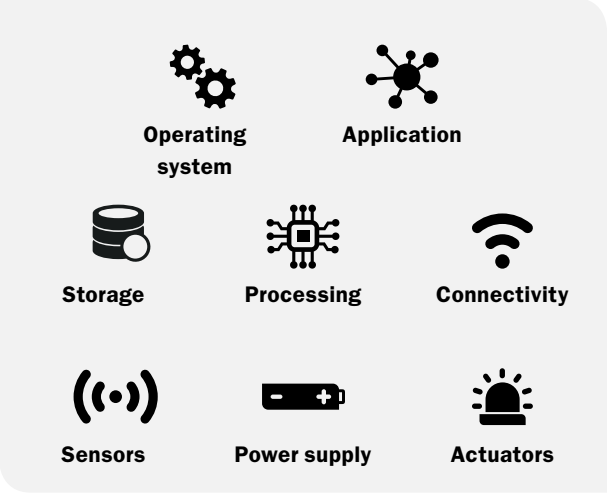


Figure 14: *An IoT Device*

We refer to the depiction of a generic IoT device presented in Chapter 2. IoT devices are extremely varied in nature and may consist of some or all of the components depicted the figure. All IoT devices include sensors: these might be temperature sensors, motion sensors, air quality sensors, or light sensors, to name a few. These sensors automatically collect information from the environment. Some devices may contain actuators for moving or controlling a system or mechanism. Devices also contain power supplies, often batteries; managing and replacing these batteries is a major operational consideration for IoT. There is 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 (MCU), storage such as NVRAM, and often a minimal operating system and an application running on it.

It may be argued that the smaller the device, the harder it is to protect. With IoT devices we do not have the luxury of measuring memory in gigabytes, nor of measuring processing power by the number of cores. Most IoT devices

have a microcontroller rather than a full-fledged microprocessor, and speeds in MHz rather than GHz. Additionally, the low cost of these devices means razor-thin margins for the supplier and less to spend on security. Nevertheless, security should be part of an IoT device from an early design stage and is something that should never be passed over in the interest of decreasing manufacturing costs or time to market.

Once designed, IoT devices are mass-produced. There may be thousands to millions of similar IoT devices. With consideration for the requirements and capabilities of these devices, the design should be fundamentally secure. Cryptographic identifiers are a common approach, but these are vulnerable because many devices manage secret keys with software, which if breached can expose the key. This leads to the challenge (as identified by ENISA[187] and MITRE[188]) of establishing a chain of trust based on a root of trust embedded in the device.

5.8.1 Current Landscape and Recent Developments

Recent developments focus on the device elements that are important from a security viewpoint: root of trust (which can physically reside in the processor or storage, or on a separate chip), firmware, and storage.

Root of Trust

A root of trust (RoT) is a hardware or software component that is inherently trusted[189] due to its immutability. A RoT must be secure by design, should be small and protected and ideally implemented in hardware or protected by hardware. RoTs are trusted to perform or support one or more security-critical functions, e.g. verify software, protect cryptographic keys, and perform device authentication[190].

In fact, a RoT anchors several of the security functionalities that we discuss below and in subsequent sections. The main uses of the RoT include the following.

- Identity: The RoT can securely hold a device identifier that can be queried by communicating entities.
- Authentication: Secure communication is available after successfully completing an authentication and key exchange protocol, typically using an ephemeral symmetric session key for encryption and an HMAC key for authentication. These keys can be generated and stored in the RoT, keeping them protected from on-chip attacks.
- Data Encryption: Encryption can protect data stored locally on the device as well as data transmitted over networks. The RoT can store encryption keys. Only indirect access to these keys is allowed and managed by permissions and policies on the application layer.
- Secure Boot: Validation of the code and/or data on the device following power-up, based on trusted material stored within the RoT. This prevents the execution of unauthorised code and the exposure of embedded boot code and software IP.

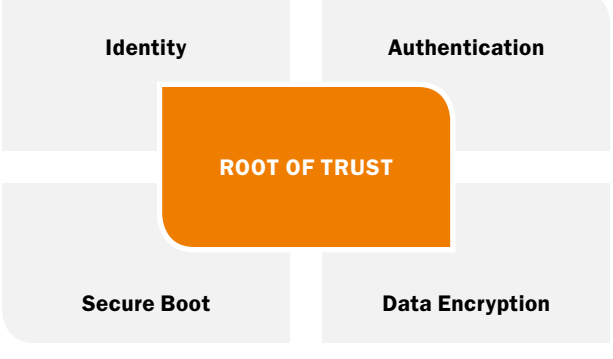


Figure 15: *Root of Trust Functionalities*

187 ENISA 'Baseline Security Recommendations for IoT', November 2017
188 https://www.mitre.org/research/mitre-challenge/mitre-challenge-iot
189 https://blog.nxp.com/security/getting-to-the-root-of-trust
190 https://www.synopsys.com/designware-ip/technical-bulletin/understanding-hardware-roots-of-trust-2017q4.html

GlobalPlatform defines[191] a Secure Element (SE) as a tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. keys). On the other hand, GlobalPlatform defines a Trusted Execution Environment (TEE)[192] as a secure area within a main processor that runs in an isolated environment and guarantees that the code and data loaded within are protected with respect to confidentiality and integrity. Trusted applications running in a TEE have access to the full power of a device's main processor and memory, but hardware isolation protects these components from applications running in the main operating system. Software and cryptographic isolations inside the TEE protect trusted applications from each other. Two common hardware technologies that support TEE are ARM TrustZone and Intel SGX. Synopsys' DesignWare tRoot Hardware Security Modules (HSMs) also provide a TEE (see www.synopsys.com/dw/ipdir.php?ds=security-troot-hw-secure-module).

In a similar vein, a Trusted Platform Module (TPM)[193] is a cryptographic coprocessor that is present in many commercial PCs and servers. The TPM specification is a recommendation from the Trusted Computing Group (TCG) to securely identify individual connected devices and to securely generate and store keys within these devices. However, the inclusion of a TPM in IoT devices does lead to increased costs and resource requirements.

Cisco's implementation of a hardware RoT is the Trust Anchor. Secure Unique Device Identifier (SUDI[194]) credentials including the a SUDI certificate, the associated key pair, and its entire certificate chain are stored in the tamper resistant Trust Anchor chip. The identity is implemented at manufacturing and chained to a publicly identifiable root Certificate Authority (CA). The hardware chip is used as an anchor for a secure boot process. The Trust Anchor is compliant with NIST specifications and provides a NIST SP 800-90A[195] and B certifiable Random Number Generator (RNG) that extracts entropy from a true random source within the chip.

Similar to the Trust Anchor, Google's Titan security chip[196] offers secure boot as well as an end-to-end cryptographic identity system for the servers in Google's data centres as well as the Pixel mobile phone. The Titan chip's manufacturing process generates unique keying material for each chip, and securely stores this material into a registry database. The contents of this database are cryptographically protected using keys maintained in an offline quorum-based Titan Certification Authority (Titan CA). Individual Titan chips can generate Certificate Signing Requests (CSRs) directed at the Titan CA, which – under the direction of a quorum of Titan identity administrators – can verify the authenticity of the CSRs using the information in the registry database before issuing identity certificates.[197] While the chip may not yet offer a practical solution for Class 0-2 IoT devices owing to cost considerations, it does provide a good indicator of the direction of RoT security.

Having said that, a general drawback of CA-based approaches is that the CA must be secure and trustworthy; the DigiNotar incident[198] has illustrated that CAs may themselves be vulnerable.

191 https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf
192 https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf
193 https://trustedcomputinggroup.org/work-groups/trusted-platform-module/
194 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trust-anchor-technologies-ds-45-734230.pdf
195 https://en.wikipedia.org/wiki/NIST_SP_800-90A
196 https://cloud.google.com/blog/products/gcp/titan-in-depth-security-in-plaintext
197 https://cloud.google.com/blog/products/gcp/titan-in-depth-security-in-plaintext
198 https://en.wikipedia.org/wiki/DigiNotar

SIM and eSIM

A Subscriber Identity Module, widely known as a SIM card, securely stores a user's mobile phone number and associated symmetric key. The traditional SIM card is a removable piece of plastic – a smart microprocessor chip built on universal integrated circuit card (UICC) technology, which is inserted into a mobile device for use on GSM and successor networks. The key is programmed during manufacture and used by mobile network operators to authenticate and identify devices accessing their networks and services. The SIM has played a pivotal role in the rise of mobile communications over the last few decades – today, 4.8 billion people use mobile services worldwide and there are 400 million cellular machine-to-machine (M2M) connections.

SIM cards can also support additional security capabilities that can be harnessed for IoT[199]; indeed, a SIM card can act as a secure RoT to provision and store digital certificates and other kinds of security credentials, such as passwords. These credentials can be used to identify and authenticate an IoT device to interact with a server-side application or IoT platform.[200]

With the advent of IoT, remote provisioning has also become an important requirement for SIM cards.[201] Remote provisioning is the ability to remotely change the SIM profile on a deployed SIM card without having to physically change the SIM card itself. As GSMA identifies[202], replacing physical SIM cards is problematic for many IoT/M2M use cases, given that many IoT devices are remotely located, often hermetically sealed, and have lengthy lifespans. GSMA highlights that many of the interfaces and processes needed to make the remote provisioning of SIMs work are virtually identical to current SIM personalisation processes and interfaces used by mobile operators today.

Remote provisioning capability can be deployed on both removable and non-removable UICCs: the term embedded UICC (eUICC) is used to refer to a SIM card that can be remotely provisioned. An embedded SIM (eSIM) is one that supports remote provisioning and is physically integrated into the device during manufacture.

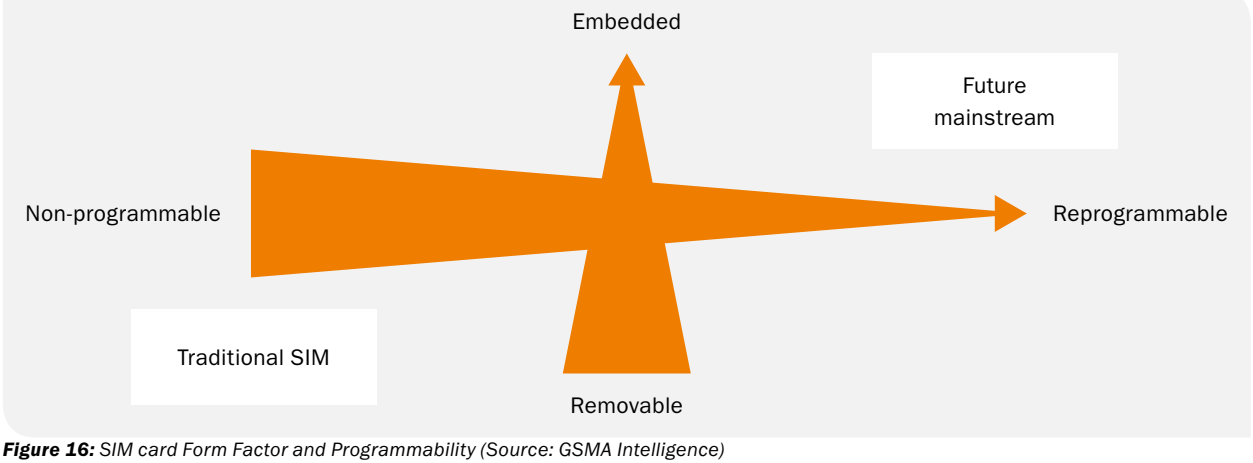


Figure 16: *SIM card Form Factor and Programmability (Source: GSMA Intelligence)*

199 Case Study: Leveraging the SIM to Secure IoT Services, GSMA
200 Solutions to Enhance IoT Authentication Using SIM Cards (UICC), GSMA IoT, 2016
201 The future of the SIM: potential market and technology implications for the mobile ecosystem, GSMA Intelligence, Feb 2017
202 https://www.gsma.com/iot/embedded-sim/

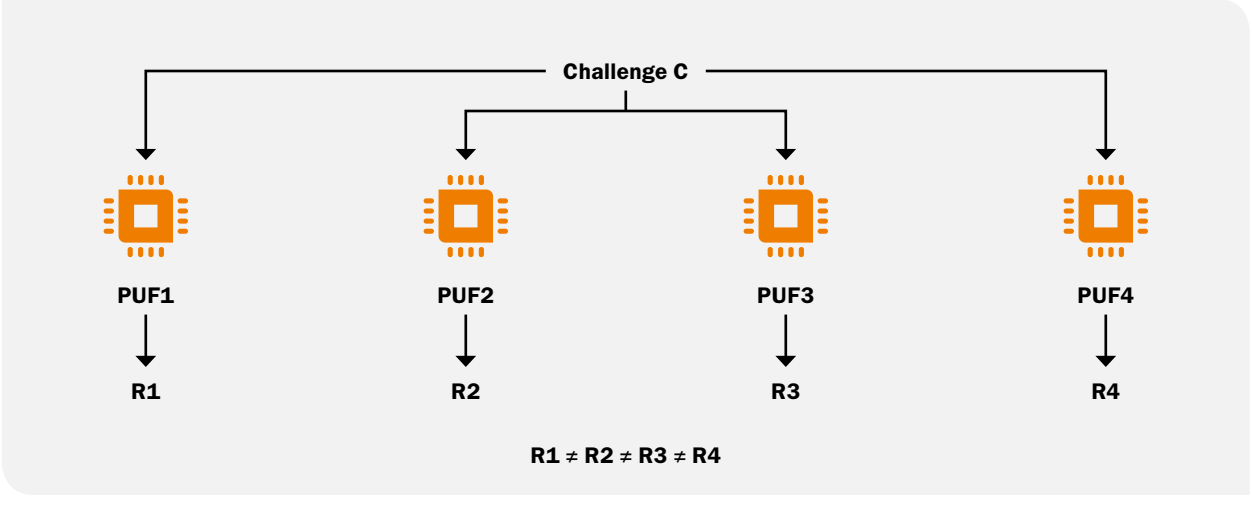


Figure 17: *Physical Unclonable Function (PUF)*

Remote provisioning technology has been deployed widely in the IoT/M2M market: IHS Markit reported 108.9m eSIM shipments in 2016.[203] Also in 2016, the GSMA published the eSIM technical specification[204] for connecting consumer companion devices (such as tablets, smart watches and fitness devices) as well as handsets; future growth is expected to be driven by consumer as well as IoT devices.

Physical Unclonable Functions

A Physical Unclonable Function (PUF) is an interesting approach to device identification that does not require key storage. A PUF provides a silicon biometric that is unique for every chip, reacting to an input in an unpredictable (but repeatable) way due to the complex interaction of the stimulus with the physical microstructure of the chip, and deriving its uniqueness from uncontrolled variations in the chip manufacturing process. PUFs are increasingly used as building blocks in many secure systems for applications such as device authentication and secret key generation, providing an attractive alternative to *storing* secret random bits in volatile or non-volatile memory by instead *generating* these bits every time the PUFs are evaluated. Several vendors offer commercial PUF implementations including Intrinsic ID[205] and Verayo[206], both of which deliver identification and authentication solutions based on their respective PUF technologies. Intrinsic ID's Spartan authentication module[207] is specifically intended for IoT devices, using PUFs to provision products with secure keys and platform-compliant certificates in a scalable and cost-efficient way while also offering integration with the AWS IoT cloud platform.

203 https://cdn.ihs.com/www/pdf/1118/abstract-digital-security.pdf
204 https://www.gsma.com/esim/esim-specification/
205 https://www.intrinsic-id.com/sram-puf-technology-solutions/
206 http://verayo.com/tech.php
207 https://www.intrinsic-id.com/products/spartan/

Attestation and Privacy

Consider a device communicating with a server that wants assurance of the device's identity, i.e. the server wants the device to authenticate itself. However, the device (more specifically, its user) may want privacy and therefore may require that the server only learns that the device is trusted. In principle, the problem could be solved by embedding a single secret key in every device and in the server, or using public-key cryptography with a single private key across all devices and a public key in the server. However, if any one device were compromised and the secret key extracted and published, the server would no longer be able to distinguish between real devices and fake ones.

To address this, TCG initially proposed an intermediate certification authority called the Privacy CA, which has the obvious drawback that the Privacy CA[208] needs to be involved in every transaction and thus must be highly available and yet as secure as an ordinary CA that normally operates online. The newer Direct Anonymous Attestation (DAA) scheme is a digital signature algorithm supporting anonymity, allowing devices to uniquely authenticate themselves without the need for a Privacy CA . Unlike traditional digital signing, in which an entity has a public verification key corresponding to a single private signing key, DAA provides a common group public verification key associated with many unique private signing keys. DAA was created so that a device could prove its membership of a trusted group to an external party without needing to provide device identity. The DAA scheme was adopted by TCG as part of TPM 1.2.[209]

Intel's Enhanced Privacy ID[210] (EPID) is an enhancement of DAA that allows revocation of a private key given a signature created by that key, even if the key itself is still unknown. Also, each private key is actually a large set of key values, and a device can use a different key value in every transaction. This prevents anyone – including the manufacturer, the verifier, and the certificate authority – from tracing the key back to the root key or from identifying multiple transactions as emanating from the same device. EPID is the basis of Secure Device Onboard[211] (SDO), a service developed by Intel that securely brings IoT devices online in an automated manner. SDO attests the device and connects it to the owner's IoT platform, and is supported by several IoT platform providers including AWS and Google.

Firmware and Secure Boot

When power is first switched on, a device is relatively dumb and can read only part of its storage called read-only memory (ROM) or firmware. For complex devices, the firmware (called Basic Input-Output System, or BIOS) typically initiates a multi-step procedure, calling code at the Master Boot Record (MBR) which in turn calls a bootloader to run a larger program such as an operating system. An alternative to BIOS is offered by the Unified Extensible Firmware Interface (UEFI); modern versions of Linux and Windows support UEFI with BIOS backward compatibility.[212]

Simpler embedded devices often have (minimal) software systems entirely in ROM firmware or flash memory; little or no loading is necessary. Some designs may use an intermediate technique where minimal bootloader-like code is loaded into device RAM by the integrated boot ROM.[213]

208 https://en.wikipedia.org/wiki/Direct_Anonymous_Attestation
209 https://trustedcomputinggroup.org/resource/tpm-main-specification/
210 https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/intel-epid-iot-security-white-paper.pdf
211 https://www.intel.sg/content/www/xa/en/internet-of-things/secure-device-onboard.html
212 https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface
213 https://www.embedded.com/design/mcus-processors-and-socs/4008796/2/Fundamentals-of-Booting-for-Embedded-Processors

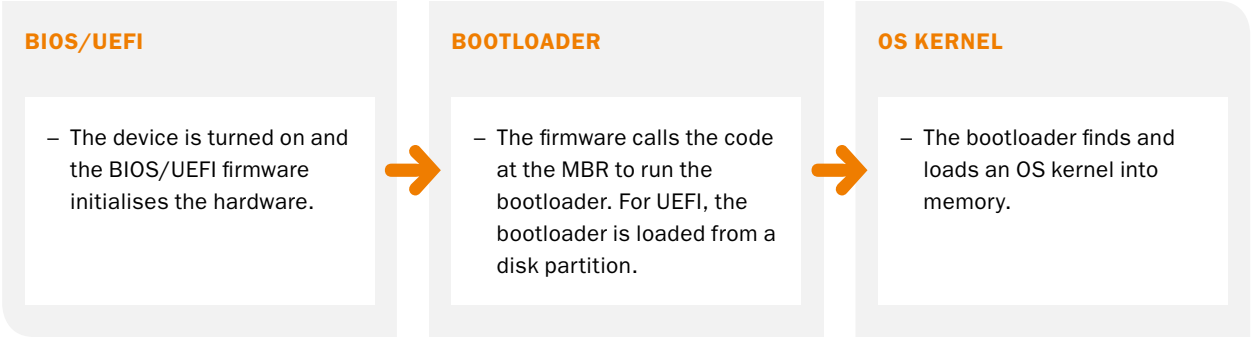


Figure 18: *Typical Boot-Up Process for Complex (Class 2) Devices*

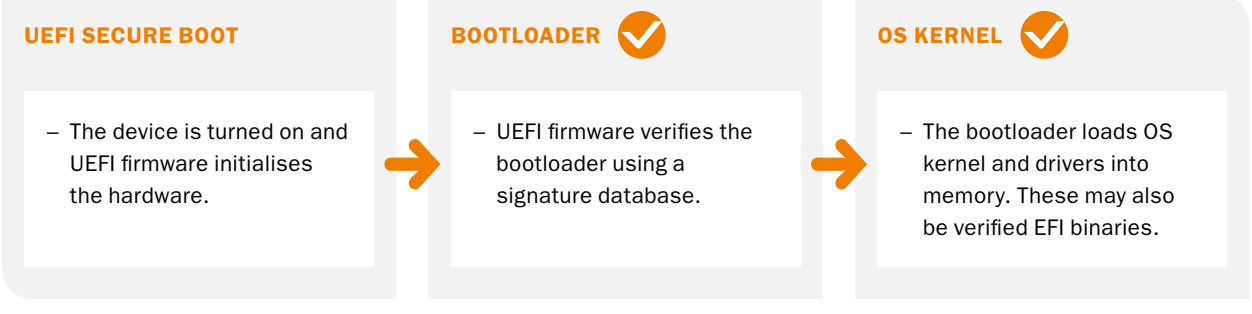


Figure 19: *Secure Boot Process*

Regardless of the exact design used, implementing a secure boot process is critical to device integrity[214] since a compromised boot process allows hackers to inject malware or entirely replace firmware ("boot kit"), leaving the entirety of a connected system vulnerable. A secure boot process also makes other security features available to the operating system and applications by providing a necessary degree of trust. At its simplest, a secure boot process prevents the execution of unauthorised code at the time of device power-up and prevents the exposure of embedded boot code and software IP. A secure boot can be achieved in different ways, including using digitally signed binaries, secure and trusted boot loaders, boot file encryption, and security microprocessors.

The UEFI Forum is an industry body that advocates a standardised interface for secure booting. UEFI's Root of Trust white paper[215] addresses the use of hardware roots of trust such as AMD's Platform Security Processor and ARM's TrustZone. UEFI[216] Secure Boot, specified by the UEFI 2.3.1 Errata C specification[217] (or higher), describes a boot process that prevents the loading of drivers or OS loaders that are not signed with an acceptable digital signature.

214 http://www.embedded-computing.com/embedded-computing-design/iot-security-starts-with-secure-boot

215 http://www.uefi.org/sites/default/files/resources/UEFI%20RoT%20white%20paper_Final%208%208%2016%20%28003%29.pdf

216 https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

217 http://www.uefi.org/specifications

When Secure Boot is active, the UEFI firmware is responsible for verifying components such as drivers and bootloader. At commissioning, the device is initially placed in Setup Mode, which allows a public part of a Platform Key (PK) to be written to the firmware. The private part of the PK is used to sign a Key Exchange Key (KEK) which protects a signature database. Following this, Secure Boot enters User Mode, where only drivers and loaders whose signatures match the database can be loaded by the firmware. If an invalid binary is loaded while Secure Boot is enabled, the user is alerted, and the system will refuse to boot with the tampered binary. Additional signatures can be added to the database, but they must be signed by the private part of the KEK.

While Secure Boot mitigates the problem of untrusted firmware, care must be taken in system design to protect secure boot databases. In addition, vendors must develop security processes to protect various signing keys and to sign only approved payloads[218].

Seven Properties of Highly Secured Devices

Microsoft Research has identified seven properties[219] that highly secured devices need to have: hardware based root-of-trust, small trusted computing base, defence in depth, compartmentalisation, certificate-based authentication, security renewal, and failure reporting. Microsoft's Azure Sphere platform is designed around these properties, offering a secured, connected, crossover microcontroller unit (MCU), a custom high-level Linux-based operating system (OS), and a cloud-based security service.
The Azure Sphere MCU, along with its operating system and application platform, enables the creation of secured, internet-connected devices that can be updated, controlled, monitored, and maintained remotely.[220] Specifically, the MCU's Pluton Security Subsystem generates its own key pairs, implements a true random number generator (RNG), and accelerates cryptographic operations,[221] enabling measured boot as well as remote attestation.

Local Device Storage

Stored data should always be protected with encryption[222]. Of course, a technique commonly used in IoT is to not store data locally but send it to a server where it can be easily encrypted. Having said that, some devices incorporate local self-encrypting drives (SEDs) that provide confidentiality while being easy to use and manage and having minimal impact on system performance. At the most basic level, SEDs provide hardware-based data security by continuously scrambling data using a key as it is written to the drive, and then descrambling the data as it is retrieved. The contents of an SED are always encrypted, and the encryption keys are themselves encrypted and protected in hardware that cannot be accessed by other parts of the system.

The SED standards[223] from TCG enable encryption to be built into drives, improving security while avoiding the overhead of software encryption and ensuring that equipment can be cleansed for reuse simply by telling the drive to change its key. As with TPM, the SED standard is available in a wide variety of interoperable products, including hard drives, solid state drives, hybrid drives and enterprise storage systems, from a variety of vendors. SEDs are already in use in a number of devices, including printers, copiers and multi-function devices as well as point of sale systems.

218 http://www.rtcgroup.com/whitepapers/files/Insyde_Embedded_Secure_Boot.pdf
219 https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf
220 https://docs.microsoft.com/en-us/azure-sphere/product-overview/what-is-azure-sphere
221 https://azure.microsoft.com/en-us/blog/anatomy-of-a-secured-mcu/
222 https://www.gemalto.com/enterprise-security/enterprise-data-encryption
223 https://trustedcomputinggroup.org/resource/storage-work-group-storage-security-subsystem-class-opal/

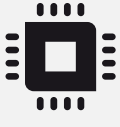
Key Provisioning

The provisioning of cryptographic keys into devices is a critical initial step in establishing a security baseline. This provisioning is done in one of three ways[224]:

- Pre-provisioning: Secure Elements (SEs) destined for IoT devices are typically purchased from a silicon vendor with all required keys pre-provisioned on the chip by this vendor. This means that the IoT device maker does not need to deal with provisioning keys for his device, but the SE approach comes with downsides such as increased costs and complexity in purchasing, supply chain and inter-chip interfacing.
- Key Injection: Cryptographic keys can be injected into a device at different points in the supply chain. After injection, the keys are stored on the device. Most widely used embedded key storage methods are based on Non-Volatile Memory (NVM) such as Electrically Erasable Programmable Read Only Memory (EEPROM), Flash, or One-Time Programmable (OTP) memory such as fuses and anti-fuses. With these memory types, the provisioning of root keys comes with trade-offs among flexibility, key-exposure liability, cost, reliability and security.
- On-board Key Generation: An internal Random Number Generator (RNG) on the chip can derive a random secret and use it to generate cryptographic keys. This method increases the flexibility within the supply chain compared to key injection (assuming the target chip contains a random number generator), but it does not make any difference regarding how the root key is stored.

5.8.2 Key Findings

- A hardware RoT is the only immutable trust anchor; the chain of trust should build on a hardware RoT. Currently, only 4% of IoT devices use a hardware RoT.[225]
- RoT-based cybersecurity can be provided by several solutions including Secure Elements, TPMs, TEEs, Cisco Trust Anchor, Microsoft's Pluton Security Subsystem, and SIM cards.
- Solutions to secure firmware and booting are being proposed as a joint effort of the hardware and software industry, however, their adoption for IoT devices is still in the initial stage.



Pre-provisioning: The use of a secure element may increase cost and complexity

Key injection: non-volatile memory can be provisioned with keys early in the supply chain

On-board Key Generation: Using an RNG, keys can be generated internally on the chip

Figure 20: *Key Provisioning (Source: Intrinsic ID)*

224 Protecting the IoT With Invisible Keys, Intrinsic ID Whitepaper, 2018

225 IoT Security from Design to Lifecycle Management, An Embedded Perspective; ABI Research, 2018.

5.9 SECURE OS, CLOUD AND APPLICATIONS

Large amounts of data are generated as a consequence of the interaction between IoT devices and the physical world. In general, software applications running on an operating system collect and process this data. Given the resource constraints of IoT devices, computationally-intensive data processing is usually performed in a back-end system, which is usually part of a cloud environment. The operating system and applications on the device as well as the back-end operating system and applications need to be provisioned with appropriate security controls.

5.9.1 Current Landscape and Recent Developments

Russell[226] provides a practical guide to support developers and architects in building secure IoT systems. Open source software – particularly copyleft licenses – may not always be the first choice of industry but offer higher code quality and more secure code due to the increased numbers of contributors and reviewers[227].

Operating Systems

IoT device operating systems are typically referred to as "embedded" or "real-time" operating systems, reflecting their minimal nature and time-critical response requirements. Traditional operating systems such as Windows and iOS were not designed for IoT applications: they consume too much power, need capable processors, and in some cases, lack features such as guaranteed real-time response. Consequently, a wide range of IoT-specific operating systems has been developed to suit many different hardware footprints and feature needs. IoT-focused operating systems include VxWorks, ARM Mbed OS, Zephyr, Nucleus RTOS, Contiki and TinyOS.

Hahm et al[228] present a well-founded analysis of different IoT operating systems. Although it touches upon security as an important feature, a benchmark of the cybersecurity mechanisms available in the different operating systems is lacking; typically, this is the case for most of the literature[229] on IoT operating systems. This observation leads to the recommendation to deliver this benchmark with a cybersecurity focus as input for security standards for IoT operating systems.

To secure the operating system, at least the below security controls should be in place[230]:

- Malicious application protection – Applications can contain many hidden threats for IoT devices. Even some legitimate software can be exploited for fraudulent purposes.
- Malware protection – Malware can be installed on an IoT device with malicious intentions. Malware can send unsolicited messages, or give an attacker control over the device, all without informing the owner.
- Spyware protection – Spyware is installed to collect or use private data without informing or approval. Data commonly targeted by spyware includes location, history, contacts and private data. This stolen information could be used for identity theft or financial fraud.
- Privacy protection – Privacy threats could be caused by applications that are not necessarily malicious, but gather or use sensitive information (e.g., location, contact lists, personally identifiable information).
- By default, the OS should disable as many services and features as possible, allowing developers and deployment configurations to enable features as necessary in order to minimise the attack surface. The framework should allow for configuration reporting

226 Practical Internet of Things Security, Brian Russell, 2016.
227 J.-H. Hoepman and B. Jacobs, "Increased security through open source," Communications ACM, vol. 50, no. 1, pp. 79–83, Jan. 2007.
228 Operating Systems for Low-End Devices in the Internet of Things: A Survey, O. Hahm et al, 2016
229 Survey of Operating Systems for the IoT Environment, Borgohain et al. 2015;
230 P. Gaur, M.P. Tahiliani, "Operating Systems for IoT Devices: A Critical Survey", 2015 IEEE Region 10 Symposium, 2015;
231 http://secure-os.com/privacy-security/

and potentially for remote configuration changes to respond to ecosystem changes.

Cloud and IoT

IoT devices send captured data to a back-end for analysis and possible further action. Since the deployment of IoT devices is progressing at a rapid pace and at large scale, the amount of data being generated is unprecedented. Cloud computing offers computing capabilities, storage, applications and services, in a highly scalable manner, and is thus considered a natural fit for the IoT ecosystem. Consequently, recent years have seen the emergence of a number of cloud-based IoT platforms, which facilitate communication, data flow, device management and user interfacing, and the functionality of applications. All of the major cloud service providers (CSPs) including AWS, Google and Microsoft have offerings targeted at the IoT market; widely-used IoT platforms include Amazon's AWS IoT, Google Cloud, Microsoft Azure IoT, IBM Watson, and Cisco IoT Cloud Connect. Having said that, research has found significant gaps in domain support in existing cloud computing platforms, and a notable absence of standardisation.[231]

Cloud computing is a shared technology model where different organisations are responsible for implementing and managing different parts of the stack. As a result, security responsibilities are also distributed across the stack and thus across the organisations involved. This is commonly referred to as the shared responsibility model. As described by the Cloud Security Alliance (CSA)[232], the exact distribution of security responsibilities depends on the service model.

Software as a Service: The cloud provider is responsible for most of the security, since the cloud user can only access and manage their use of the application and cannot alter how the application works. For example, a SaaS provider is responsible for perimeter security, logging/ monitoring/ auditing, and application security, while the consumer may only be able to manage authorisation and entitlements.

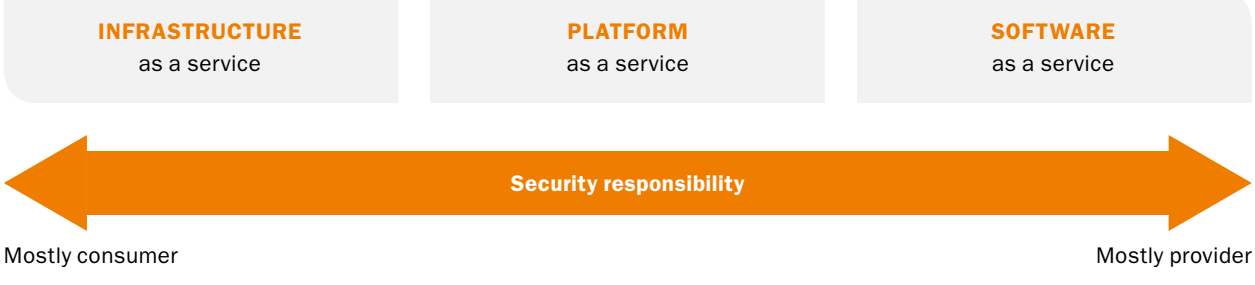


Figure 21: *Security Responsibilities in the Cloud (Source: Cloud Security Alliance)*

231 A survey of IoT cloud platforms, Partha Pratim Ray, 2017.

232 Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, 2017

Platform as a Service: The cloud provider is responsible for the security of the platform, while the cloud consumer is responsible for everything they implement on the platform, including how they configure any offered security features. For example, when using a Database as a Service, the provider manages fundamental security, patching, and core configuration, while the cloud consumer is responsible for everything else, including which security features of the database to use, and managing accounts as well as authentication methods.

Infrastructure as a Service: The provider is responsible for foundational security, while the cloud consumer is responsible for everything they build on the infrastructure. This places far more responsibility on the cloud consumer. For example, the IaaS provider will likely monitor their perimeter for attacks, but the consumer is fully responsible for how they define and implement their virtual network security based on the tools available on the service. CSA provides further guidance[233] for various aspects of cloud security across the above service models, including good practices such as the use of multi-factor authentication (MFA) for privileged access, "architecting for failure" to ensure business continuity, carefully understanding the responsibilities and contract of the cloud provider, and using appropriate encryption and key management to ensure the protection of sensitive data. CSA also suggests a simple high-level process for implementing cloud security, as shown below.

As an example, Google Cloud Platform servers use a variety of technologies to ensure that they are booting the correct software stack, including cryptographic signatures over low-level components like the BIOS, bootloader, kernel, and base operating system image[234]. This security is based on the Titan security chip which was also discussed in the previous section.

ENISA describes[235] security challenges that arise from the convergence of cloud computing and IoT, including 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.

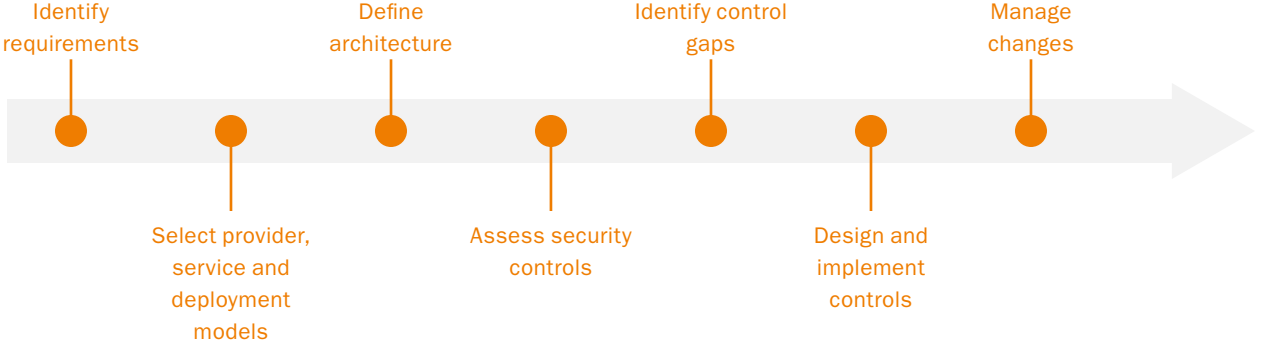


Figure 22: *Cloud Security Process Model (Source: Cloud Security Alliance)*

233 Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, 2017

234 https://cloud.google.com/blog/products/gcp/titan-in-depth-security-in-plaintext

235 Towards secure convergence of cloud and IoT, ENISA, Sept 2018

Applications

As identified by Subramanian and Swaminathan[236], applications in a typical IoT environment fall into the following categories:

1. Device applications that reside on the nodes and/or gateways.
2. Controlling applications that typically reside in the data centre or on a user or operator's mobile device.
3. Consuming applications that typically reside in the data centre and receive data from the devices for further processing and analytics.
4. Relay services that format and transfer data between different components, e.g., APIs and web services.

To realise safe and secure software, it is important to adopt a secure design and development methodology. Useful guidelines for secure software development are provided by OWASP[237], which also offers a comprehensive developer checklist that covers input validation, access control, session management, error handling, logging, database security and memory management.

OWASP's Application Security Verification Standard (ASVS)[238] is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, and even consumers to determine the security level of a given application in a consistent manner. ASVS defines 3 security verification levels of successively increasing depth, with a set of security requirements for each level. OWASP specifically discusses the use of ASVS as the basis of a secure SDLC: developers are encouraged to use the ASVS as a peer review checklist to ensures that unsafe code does not get checked in; further, developers can use the ASVS as part of their automated verification secure unit and integration test suites. The aim is to reduce the risk from waterfall-style "penetration testing at the end", which can lead to expensive refactoring when delivering milestone builds into production.

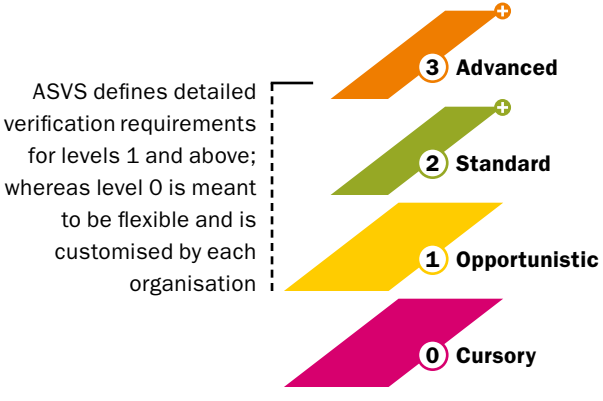


Figure 23: *OWASP Security Verification Levels (Source: OWASP)*

IoT devices (or, more specifically, the applications running on them) should "prove their health", before accessing other IoT devices or services. Associated capabilities include a process for securely determining software and firmware versions and a secure software and firmware update mechanism. For example, the Trusted Computing Group's Trusted Network Connect (TNC) standards, which specify a standard mechanism to check which software or firmware is running on a device, are among the protocols and mechanisms for safeguarding the patch and upgrade process. Malware can be detected at boot time using the device's Trusted Boot and Remote Attestation capabilities, even to the point of finding changes in the device's BIOS or other firmware.

236 https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/security-assurance-in-the-sdlc-for-the-internet-of-things.aspx

237 https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

238 https:// www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

5.9.2 Key Findings

- The diversity of operating systems, cloud solutions and application development frameworks that populate the IoT market is large. An in-depth evaluation is required on the security claims made for each solution.
- Standards are required for software development, deployment and operation processes to secure the OS, cloud back-ends, and applications.
- IoT-specific secure software development life cycle (SDLC) guidelines need to be defined for developers of IoT applications.

5.10 SECURE COMMUNICATIONS AND INFRASTRUCTURE

IoT devices transmit information to a back-end for processing and analytics. Depending on the computational capabilities of the devices, it may be possible to filter some of the data before transmission or even to take immediate action locally without sending any data at all; however, all IoT systems do, at some point, send data over a network to a back-end. There are numerous ways to achieve this connectivity, ranging from direct cellular or satellite connections to low-power WANs with gateways to reach the back-end. Security is paramount since IoT devices based on different technologies and acquired from various suppliers on the global market communicate via heterogeneous network interfaces in an open network that is untrustworthy and potentially hostile.

5.10.1 Current Landscape and Recent Developments

When a device connects to the back-end, a gateway or other devices, it must authenticate and establish trust. Once trust is established, devices, users and services can securely communicate, interact and transact information. This challenge encompasses all elements that route and transport endpoint data traffic securely over the infrastructure, whether control, management or actual data traffic.

Authentication and Authorisation

Authentication in IoT networks should establish mutual trust between devices, users, gateways, back-ends, networks, and services. Classically, the authentication process relies on the authenticating entity demonstrating knowledge ("something you know"), possession ("something you have"), and/or inherent/behavioural ("something you are") factors, with multiple factors often recommended for stronger authentication. While these factors are applicable to *users* of IoT devices (e.g. to log in to a management console), the "things" themselves are essentially restricted to possession factors relying on a shared secret or asymmetric key. As discussed in previous chapters, the provisioning of a trusted identity is normally done at the time of manufacturing or via key injection.

Public-key infrastructure (PKI) has been used to authenticate machines and servers for decades, and offers an established open standard for interoperability. However, PKI needs to evolve in order to support the scale and heterogeneity inherent in IoT usecases.[239] Specifically, lightweight certificate enrollment procedures should prove useful; the Swedish CEBOT (Certificate Enrollment in Billions of Things) project addresses how lightweight enrollment can be achieved.[240] Additionally, certificate validity periods and future-proof algorithms need to be considered. If implemented carefully using the device's root of trust, PKI-based identities can provide a basis for strong authentication.

The authorisation layer controls the extent of access provided to a device or, more generally, a process. This layer builds upon the core authentication layer by leveraging the identity information of an entity to determine what actions it is allowed to perform. The principle of least privilege dictates that we should only allow the bare minimum of access to an entity, such as a device or process, to allow it to perform the functionality needed of it. With authentication and authorisation in place, a trust relationship is established between IoT devices to exchange appropriate information.

239 https://www.globalsign.com/en-sg/blog/iot-vs-traditional-pki-deployments/
240 https://www.sics.se/projects/certificate-enrollment-in-billions-of-things

Secure network communications

Though some traditional network security solutions are applicable to IoT, the limited processing and communication capabilities of IoT devices preclude the use of full-fledged security suites. Bonetto et al[241] studied this and suggested solutions to the challenge, proposing a lightweight procedure to set up secure end-to-end channels between unconstrained (and remote) peers and IoT devices. Sain et al[242] provide a survey of different wireless technologies and their security strengths and weaknesses in a constrained IoT environment.

We present below a visual representation of some state-of-the-art networking technologies for IoT and the relationships between them. This stack bears some resemblance to the commonly-encountered HTTP-TCP-IP-Ethernet Web networking stack, but features a larger number of protocols and greater complexity. IoT networking protocols typically feature lightweight, low-power operation at relatively lower data rates compared to computer networks, in order to meet the requirements of resource-constrained devices with small amounts of memory and processing power and networks with low bandwidth and high latency.

IEEE standard 802.15.4[244] offers the lower network layers of a low-power wireless personal area network (WPAN or LoWPAN) for inexpensive, low-speed ubiquitous communication between devices, as opposed to other approaches such as Wi-Fi, which offer more bandwidth but require more power. Naturally, many of the devices that use IEEE 802.15.4 connectivity are limited in their computational power, memory, and/or energy availability.

Zigbee[245] is a low-cost, low-power, wireless mesh network standard for WPANs that builds on the physical layer and media access control defined in IEEE 802.15.4. As one of its defining features, Zigbee provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames, and controlling devices[246]. Zigbee uses 128-bit keys to implement its security mechanisms, and assumes

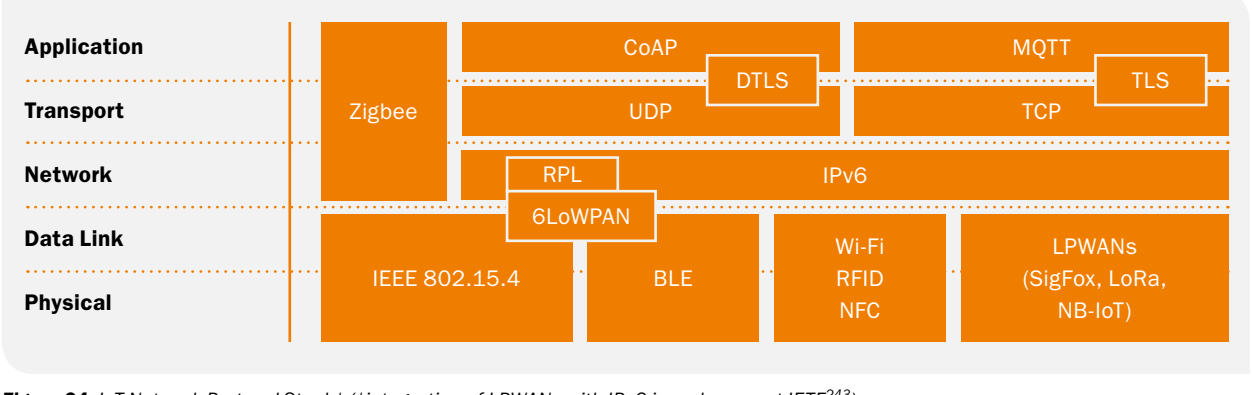


Figure 24: *IoT Network Protocol Stack* (*integration of LPWANs with IPv6 is under way at IETF[243])*

241 "Secure Communication for Smart IoT Objects: Protocol Stacks, Use Cases and Practical Examples", Bonetto et al. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6263790.

242 Survey on Security in Internet of things: State of the Art and Challenges, by Mangal Sain, Young Jin Kang, Hoon Jae Lee, South Korea, 2017.

243 https://datatracker.ietf.org/wg/lpwan/about/

244 https://en.wikipedia.org/wiki/IEEE_802.15.4

245 https://www.zigbee.org/

246 Zigbee Network Protocols and Applications, Wang et al, 2014

adequate protection of all keying material. Trust must be assumed in the initial installation of the keys, as well as in the processing of security information. A key can be associated either to a network, being usable by both Zigbee layers and the MAC sublayer, or to a link, acquired through pre-installation, agreement or transport. Establishment of link keys is based on a master key which controls link key correspondence. The initial master key must be obtained through a secure medium (transport or pre-installation), as the security of the whole network depends on it. Link and master keys are only visible to the application layer. Different services use different variations of the link key to avoid leaks and security risks.

IPv6 promises to be a key enabler for the future of IoT, providing end-to-end connectivity with a distributed routing mechanism as well as a highly scalable address scheme, providing more than 2 billion addresses per square millimetre of the Earth surface[247]. This seems sufficient to address the needs of any present and future communicating device. Moreover, IPv6 is supported by a large community of users and researchers supporting ongoing improvement of its security features.

RFC 4919 describes the requirements for LoWPANs to work with IPv6, and RFC 4944[248] defines the frame format for transmission of IPv6 packets over IEEE 802.15.4 networks. Since IPv6 requires support of packet sizes much larger than the largest IEEE 802.15.4 frame size, an adaptation layer ("6LoWPAN") is defined. This RFC also defines mechanisms for header compression required to make IPv6 practical on IEEE 802.15.4 networks, and the provisions required for packet delivery in IEEE 802.15.4 meshes.

The Routing Protocol for Low-Power and Lossy Networks (RPL) is a routing protocol standardised for constrained IoT environments such as 6LoWPAN networks. Providing security in IPv6/RPL connected 6LoWPANs is challenging because the devices are connected to the untrusted Internet and are resource constrained while using novel IoT technologies and lossy communication links. If a node becomes an internal adversary, it can break network operation without being detected by cryptography mechanisms. Therefore, analysing RPL threats in addition to specifying its operation will help to monitor most of the internal malicious behaviours. RPL in authenticated security mode uses secure messages. Pre-installed keys are used to join a network as a leaf to provide message confidentiality, integrity, and authenticity. To join the network as a router, a second key must be obtained from a key authority.[249]

As opposed to WPANs which are short-range personal-area networks, low-power wireless wide area networks (LPWANs) enable long-range, low-power communication at low cost using simplified, lightweight protocols and either license-free or licensed bands. LoRaWAN[250] is an LPWAN protocol designed to wirelessly connect battery-operated devices to the internet. The LoRaWAN network architecture is deployed in a star-of-stars topology in which gateways relay messages between end-devices and a central network server. The gateways are connected to the network server via standard IP connections and act as a transparent bridge, simply converting RF packets to IP packets and vice versa. The wireless communication takes advantage of the long-range characteristics of the LoRa physical layer, allowing a single-hop link between the end-device and one or many gateways. The LoRaWAN specification defines two layers of cryptography:

247 https://iot6.eu/ipv6_for_iot
248 https://tools.ietf.org/html/rfc4944
249 Routing Attacks and Countermeasures in the RPL-Based Internet of Things, Wallgren et al, 2012
250 https://lora-alliance.org/about-lorawan

– A unique 128-bit Network Session Key shared between the end-device and network server
– A unique 128-bit Application Session Key shared end-to-end at the application level

AES encryption provides authentication and integrity of packets to the network server and end-to-end encryption to the application server. The keys can be Activated By Personalisation (ABP) on the production line or during commissioning or can be Over-The-Air Activated (OTAA) in the field. OTAA allows devices to be re-keyed if necessary. It is possible to use the LoRa physical layer and run a different protocol on top of it, such as Symphony Link[251].

Sigfox is a proprietary LPWAN technology that enables remote devices to connect to an access point over Ultra Narrow Band (UNB) frequencies. Sigfox highlights that devices never have the ability to send data to arbitrary entities via internet and can therefore be considered to be protected by a "firewall". Furthermore, Sigfox devices have the following security features[252]:

– Each Sigfox device is provisioned during manufacturing with a unique symmetrical authentication key. Each message to be sent or received by the device contains a cryptographic token that is computed based on this authentication key. Verification of the token ensures the authentication of the sender (the device for an uplink message, or the Sigfox network for a downlink message) and the integrity of the message. Since the key is unique per device, the compromising of one device has a very limited impact. Sigfox has been working with its ecosystem to increase the security level of devices through the adoption of security best practices. In addition, secure elements dedicated to Sigfox devices are now available to provide tamper resistance.
– Each Sigfox message contains a sequence counter which is verified by the Sigfox Core Network to detect and discard replay attempts. The integrity of the counter is guaranteed by the message authentication token.
– By default, data is conveyed over the air interface without any encryption. However, depending on the application, this data may be very sensitive, and its privacy must be guaranteed. Sigfox gives customers the option to either implement their own end-to-end encryption solutions or to rely on an encryption solution provided by the Sigfox protocol.

The IETF Working Group "IPv6 over Low Power Wide-Area Networks" is currently focused on enabling IPv6 connectivity over several LPWAN technologies including Sigfox, LoRa, WI-SUN and NB-IOT[253].

The LPWAN Technology Security Comparison white paper[254] from GSMA and Franklin Heath discusses the security implications and controls for the abovementioned LPWA technologies, identifying that IoT security needs are driven largely by privacy and safety concerns and suggesting that any deployment using LPWA technologies should be subject to a security risk assessment using tools such as the GSMA IoT Security Assessment[255].

HyperText Transfer Protocol (HTTP) is the dominant application-layer protocol for the Web and has proven to be very suitable for the navigation of interactive, hyperlinked webpages. For IoT devices, most of which support no direct human interaction, consume very little power and frequently have poor network connectivity, HTTP is unsuitable[256]: a single HTTP request requires a minimum of nine TCP packets, even without taking packet loss into account. This overhead adds to IoT operating expenses.

251 https://www.link-labs.com/symphony
252 https://www.sigfox.com/en/technology/security
253 https://datatracker.ietf.org/wg/lpwan/about/
254 https://www.gsma.com/iot/news/new-report-outlines-security-considerations-lpwa-technology/
255 https://www.gsma.com/iot/iot-security-assessment/
256 https://www.edn.com/electronics-blogs/eye-on-iot-/4437056/Why-HTTP-Won-t-Work-for-IoT

Two of the most successful application-layer protocols for small devices are Message Queuing Telemetry Transport (MQTT)[257] and the Constrained Application Protocol (CoAP)[258]. Both MQTT and CoAP:

- are open standards
- are better suited to constrained environments than HTTP
- provide mechanisms for asynchronous communication
- run on existing protocols such as TCP/UDP over IP.

MQTT is a publish/subscribe messaging protocol designed for lightweight device communication, originally developed by IBM and now an open standard. It features a client/server model, where every device is a client and connects to a server, known as a broker, over TCP. Every message is a discrete chunk of data published to an address, known as a topic. Clients may subscribe to multiple topics. Every client subscribed to a topic receives every message published to the topic. Connections may be encrypted using TLS for security[259].

CoAP is defined by the IETF's Constrained RESTful Environments (CoRE) working group[260] for applications that deal with the manipulation of simple resources on constrained networks. This includes applications to monitor simple sensors (e.g. temperature sensors, light switches, and power meters), to control actuators (e.g. light switches, heating controllers, and door locks), and to manage devices. The general architecture consists of devices on the constrained network that are responsible for one or more resources that may represent sensors, actuators, combinations of values, and/or other information.

Devices can

- send messages to change and query resources on other devices.
- send notifications about changed resource values to other devices that have expressed their interest to receive notification about changes.
- publish or be queried about its resources.

CoAP is designed for use between devices on the same constrained network, between devices and general nodes on the Internet, and between devices on different constrained (but connected) networks.

Another RESTful approach to IoT is found in the so-called Web of Things (WoT), which is an application layer that enables access and control over IoT resources and applications using common web technologies (such as HTML 5.0, JavaScript, Ajax, PHP, Ruby on Rails etc.). This approach can enable both developers and vendors to benefit from the popularity and maturity of web technologies. While the W3C has begun standardisation efforts for WoT[261], we do not yet find mainstream adoption of web technologies in the IoT space.

Datagram Transport Layer Security (DTLS)[262] provides security for datagram-based application protocols such as CoAP by allowing them to communicate in a way that is designed (RFC 4347[263], RFC 6347[264]) to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees. The DTLS protocol datagram preserves the semantics of the underlying transport

257 http://mqtt.org/
258 http://coap.technology/
259 MQTT Client Authentication using TLS, IBM Knowledge Center https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_9.0.0/com.ibm.mq.adm.doc/q021330_.htm
260 https://datatracker.ietf.org/wg/core/documents/261
https://www.w3.org/WoT/,
262 https://tools.ietf.org/id/draft-ietf-tls-dtls13-01.html
263 https://tools.ietf.org/html/rfc4347
264 https://tools.ietf.org/html/rfc6347

— the application does not suffer from the delays associated with stream protocols, but has to deal with packet reordering, loss of datagrams and data larger than the size of a datagram network packet.

Internet Protocol Security (IPsec) is a widely-used network protocol suite that authenticates and encrypts packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over IP networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. While IPSec does add overheads to packet size and computation, it is considered a good alternative to SSL for capable IoT devices[265].

5G

Fifth-generation (5G) communications networks are widely expected to revolutionise machine-to-machine communications. The 5G Infrastructure Public Private Partnership[266] (5G-PPP) identifies that 5G networks shall enable not only very high availability or up-time but also high speeds, minimal latency and comprehensive coverage. According to 5G-PPP this implies a security makeover in how confidentiality, integrity, and availability will be maintained and managed in 5G networks.[267] Furthermore, the complexity of securing a network and its services has increased with the introduction of 5G network slicing and the increasing use of software-defined networking (SDN) and network function virtualization (NFV). The 5G PPP identifies specific 5G security risks including unauthorised access or usage of assets, weak slice isolation and connectivity, and traffic embezzlement due to recursive/additive virtualization. In addition, service-specific security requirements must also be considered as the 5G ecosystem is anticipated to be service-oriented.

Secure Gateways

Every IoT system needs some way to connect its sensors/devices to the cloud so that data can be sent back and forth. Gateways act as bridges between devices and the cloud: devices communicate with a gateway, which in turn communicates with the back-end. The benefits of such two-step communication are multi-fold:[268]

- Using a gateway means that devices only need to send data a relatively short distance to the gateway, while the gateway handles the high-bandwidth link ("backhaul") to the cloud. This allows for longer battery life.
- Latency can be minimised by processing some data on the gateway or even on the device itself. However, most IoT devices are too small and underpowered to do such processing themselves. Gateways can reduce latency in time-critical applications by pre-processing the data and issuing suitable actions. This is important for life-or-death situations in the medical realm or for fast-moving objects such as cars.
- A complete IoT application might involve many kinds of sensors and devices that use varying transmission protocols as discussed above. Gateways can communicate with sensors/devices using the right protocols and then translate that data into a standard protocol such as MQTT to be sent to the cloud.
- Devices can generate large amounts of data, only a small fraction of which may actually be valuable. Gateways can pre-process and filter the data to decrease transmission, processing, and storage requirements.

265 https://www.networkworld.com/article/3164531/internet-of-things/ssl-or-ipsec-whats-the-right-approach-for-iot-network-security.html
266 https://5g-ppp.eu/
267 5G PPP Phase1 Security Landscape – White Paper by 5G PPP Security Working Group
268 IoT 101: An Introduction to the Internet of Things, Leverege LLC

– Gateways reduce the number of sensors/devices connected to the internet by "multiplexing" the devices together. This makes gateways the first line of defence against hackers, but also prime targets. Therefore, security needs to be a priority for any gateway.

Highly secured gateways can provide trust anchors within the network. For example, Germany's BSI[269] has standardised the Smart Meter Gateway as an interoperable and secure communication platform[270] with a dedicated Common Criteria profile[271].

Gateways are also considered as solutions to secure legacy hardware such as industrial control systems. For older or proprietary hardware that doesn't support modern networks or security standards, the Trusted Network Connect architecture[272] includes a specification (IF-MAP Metadata for ICS Security) that organises legacy or constraint devices into local enclaves that connect to a trusted network using security gateways. The gateways that link these networks provide encrypted communications and security to the interconnected enclaves, and automatically apply access control policies from a centralised provisioning system.

5.10.2 Key Findings

– The networking and interoperability challenge has seen extensive work as well as significant standardisation; however, an in-depth review is required of the security of these communication solutions and the security and privacy requirements on each level of the communication stack in the IoT ecosystem.
– Good practices are lacking regarding the technical feasibility of security controls running on resource-constrained devices. Security reference architectures are required.
– Secure gateways can provide high-security deployments even with low-cost IoT devices.

5.11 SECURITY MONITORING AND ANALYTICS

History shows that vulnerabilities are invariably found after a product is deployed – and often exploited in "zero-day" attacks. It is vital to be able to detect unforeseen vulnerabilities, anomalies and threats in live IoT deployments, and to respond quickly, recover and remediate. In performing these tasks intelligently and automatically, it is important to devise new paradigms of IoT security monitoring, incident management and recovery.

Since IoT is by definition vulnerable, we need to monitor and analyse dataflows for advanced attacks, exceptions and other deviant behaviour. Furthermore, we should learn from discovered incidents, preferably in real-time, in order to define relevant anomalies and improve protection and detection. No matter how well defence measures are implemented, some threats will still get past even the best defences. Detecting such threats requires strong understanding of what the systems "should" be doing. Machine learning may help to find threats hiding in the noise of trillions of events generated every month.

5.11.1 Current Landscape and Recent Developments

State-of-the-art security analytics are developed by the Industrial Internet Consortium under the Industrial Internet of Things Analytics Framework[273], which is intended for system architects, technology leaders and business leaders looking to successfully deploy industrial analytics systems. Although this framework has a business focus and not a security focus, it addresses the required building blocks for security monitoring and analytics.

269 https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf
270 BSI Presentation by Joachim Weber, during SICW IoT Security roundtable, 2017.
271 Smart Meter Gateway PP, https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf
272 https://trustedcomputinggroup.org/work-groups/trusted-network-communications/tnc-resources/
273 http://www.iiconsortium.org/pdf/IIC_Industrial_Analytics_Framework_Oct_2017.pdf

Schonwalder[274] proposed and investigated a distributed passive monitoring architecture for IoT. The architecture relies on the Routing Protocol for Low-Power and Lossy Networks (RPL), which was discussed in the previous section, to monitor the network in a lightweight manner. Higher-order monitoring nodes can passively listen to the network while participating in its operation. Monitored nodes do not require to be instrumented, nor do they need to dedicate resources to the monitoring tasks which are operated by the cloud.

Coordinated Vulnerability Disclosure

As ISO identifies[275], inappropriate disclosure of a vulnerability could not only delay the deployment of the vulnerability resolution but also give attackers hints to exploit it. Vulnerability disclosure is a process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability. It encompasses actions such as reporting, coordinating, and publishing information about a vulnerability and its resolution. The goals of vulnerability disclosure include the following:

a) ensuring that identified vulnerabilities are addressed;
b) minimising the risk from vulnerabilities;
c) providing users with sufficient information to evaluate risks from vulnerabilities to their systems;
d) setting expectations to promote positive communication and coordination among involved parties.

A strategy to deal with discovered threats and vulnerabilities includes a Coordinated Vulnerability Disclosure (CVD) program that balances security with the interests of manufacturers and stakeholders, as well as a clear understanding of liability. As discussed[276] by US-CERT, CVD practices commonly lead to a strategy for Vulnerability Management (VM), which is the common term for tasks such as vulnerability scanning, patch testing, and deployment. VM practices focus on the positive action of identifying specific systems affected by known (post-disclosure) vulnerabilities and reducing the risks they pose through the application of mitigations or remediation such as patches or configuration changes. This is also discussed in the previous section on product lifecycles.

Data Classification

Combining the computing power available within the cloud with the vast volumes of data that can be generated by IoT, it should be possible to segregate bad actors, limit access to malicious parties, and integrate easily with third party logging and intrusion detection and prevention systems. Data will be collected within the cloud from a variety of data components in the IoT ecosystem. Some data might be highly sensitive, while other data might be relatively benign; a security monitoring framework should provide capabilities to classify data and to protect data based on its classification. Interface controls should limit access and exposure of sensitive data on the basis of classification.

Honeypots

A honeypot is 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 suspicious, and either accidental or hostile in nature. The attack strategies are recorded by the honeypot, and may include network traffic, payload, malware samples, and the toolkit used by the attacker. Some honeypots that are specifically geared towards IoT include IoTPOT[278], Dionaea[279], and ZigBee Honeypot. DutchSec's HoneyTrap offers an advanced system for running and managing honeypots.[280]

274 http://ieeexplore.ieee.org/document/7502833/, Schonwalder, 2015.
275 Information technology — Security techniques — Vulnerability disclosure, ISO/IEC 29147
276 The CERT® Guide to Coordinated Vulnerability Disclosure, August 2017
277 http://www.symantec.com/content/en/us/enterprise/other_resources/building-security-into-cars-iot_en-us.pdf
278 https://github.com/IoTPOT/IoTPOT
279 https://github.com/DinoTools/dionaea
280 https://github.com/honeytrap/honeytrap

Security Event Reporting and Information Sharing
Detailed descriptions of IoT incidents, such as those provided by ENISA[281], can be used as input for evaluations and validations of certain security measures. The analytics framework should operate in the cloud, given that most IoT devices are resource-constrained. This approach creates an opportunity to compare large volumes of dataflows and detect and react to malicious activities over millions of devices. For example, the Malware Information Sharing Platform[282] (MISP) is an open source threat intelligence platform that provides open standards for Threat Information Sharing. This platform is built to collect and share large amounts of data including reporting and alerting solutions.

Gateway-Based Monitoring
The gateway is uniquely suited to monitor traffic to and from the cloud, and should support anomaly detection and integrate easily with existing anomaly and intrusion detection systems. A secure gateway might even support intrusion prevention capabilities to exclude suspicious actors from the ecosystem. A logging and reporting framework should allow the gateway to observe, baseline, and monitor communications traffic and component behaviour.

5.11.2 Key Findings

- Data collection and analytics for massive numbers of IoT devices is a major challenge.
- New metrics and methodologies are required to support IoT infrastructure analytics given the data characteristics of resource-constrained IoT devices.
- Monitoring and analytics capabilities should provide input for vulnerability management programs.
- In case vulnerabilities are not solved by the supplier, monitoring tools should be able to detect and disconnect vulnerable devices from the internet.
- The industry should act as a global community when learning from incidents. This requires an open culture of sharing incidents and mutual learning where security is a joint responsibility.

5.12 INTERDEPENDENCIES AMONG CHALLENGES

The IoT security challenges discussed throughout this study do not exist in isolation; rather, they are closely dependent on each other. These interdependencies are illustrated in Figure 25.

IoT security needs to be based upon fundamentally sound cybersecurity principles, and all IoT products and services must be designed with security and privacy in mind. Manufacturers need to employ secure supply chains and carefully-considered lifecycle management strategies for device deployments. Devices themselves need a root of trust to allow for secure identification, booting and updates. Communications between devices and back-end need to be secured using authentication and encryption. Monitoring and analytics can detect vulnerabilities after deployment, and the information thus gathered can used to patch devices using lifecycle and supply chain management practices. At the same time, vulnerability information should be fed back into the supply chain to narrow down root causes and identify other devices that may be affected.

281 Baseline Security Recommendations for IoT, ENISA, Nov 2017
282 http://www.misp-project.org/

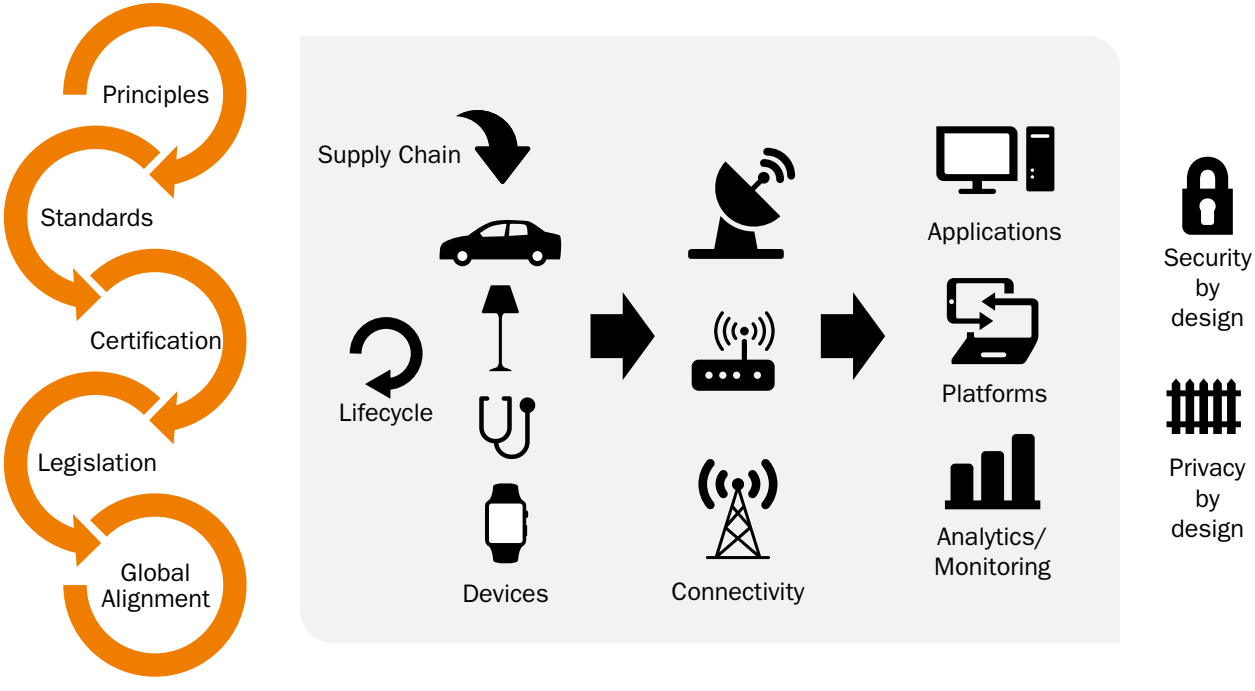
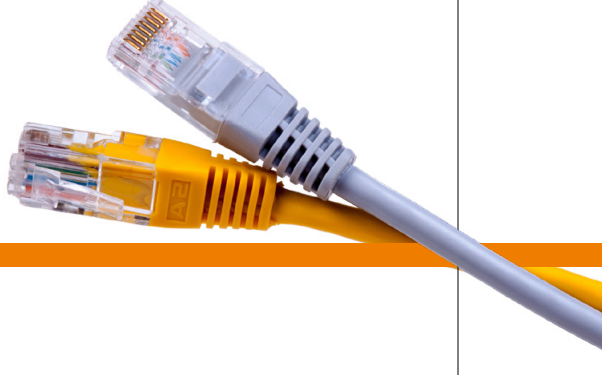


Figure 25: *IoT Security Interdependencies*

At the governance level, cybersecurity principles must lead to concrete guidelines and standards that can be used as a basis for evaluation and certification, and in turn these certifications should be mandated and backed by governmental legislation. Finally, since IoT is a global phenomenon and is not limited by national boundaries, it is essential to align country-specific legislations and adopt a global approach to IoT security.



6 CONCLUSIONS AND RECOMMENDATIONS

The number of connected things in use globally will surge from 8.4 billion in 2017 to 20.4 billion by 2020, with total spending on endpoints and services exceeding $2 trillion[283]. It is seen that IoT devices are often constrained in terms of resources (energy, computing power, memory), physical environment, and cost, such that traditional IT security mindsets cannot be applied directly. Further, IoT devices may run without supervision and for extended periods of time, possibly in hostile environments – making them particularly susceptible to hacking. Many might have zero or limited user interfacing; thus, patching and updating may not be convenient and malfunctioning or rogue devices may not be immediately detectable. This leads to the below risks:

– Consumer security, privacy and safety are undermined by the vulnerability of individual devices.
– The wider economy and critical infrastructures face an increasing threat of large scale cyber-attacks launched from large volumes of insecure IoT devices.

The fact that IoT is closely integrated with the physical world can increase the impact of cyber-attacks: while traditional IT cyber-attacks could result in data leakage and financial losses, IoT cyber-attacks have the potential to cause direct physical harm.

An analysis of key initiatives shows that there are numerous industry collaborations focusing on these IoT security challenges and on IoT in general, but progress in achieving a secure IoT has been limited. At the same time, we have seen few government-led global initiatives. There is no single set of IoT security and privacy principles nor a certification regime that is internationally recognised and adopted. The diversity in proposed IoT security principles illustrates a lack of collaboration, especially between governments. Due to the lack of globally-adopted principles, a common understanding of shared IoT challenges and issues is lacking; this is required to define a global governance process. Separately, consumers and companies are not sufficiently aware of IoT security risks and not equipped to respond to threats.

We have identified 11 foundational IoT security challenges; for most challenges, we face a fragmented space of solutions and gaps that need to be closed.

Security standards are required to stimulate the adoption of secure IoT devices. There is an overwhelming number of good practices, guidelines and standards, but manufacturers may not have the expertise to use them: usability of security standards is a challenge and requires more research. Harmonisation of IoT security standards, guidelines and recommendations is required to stimulate adoption; such harmonisation should be supported by global cybersecurity research initiatives. It is important for standardisation processes to stay aligned with technical developments without stifling innovation. Having said that, cost and time-to-market pressures in the IoT world can make it difficult manufacturers to implement security and comply with standards in the absence of suitable incentives.

There is a distinct lack of labels and certifications to inform IoT end users about device security and risks. Also, a minimum set of security requirements is lacking – such a baseline is vital for supervision and enforcement to prevent the deployment of vulnerable devices. There are as yet no evaluation profiles, e.g. Common Criteria cPPs, tailored to

283 https://www.gartner.com/newsroom/id/3598917

IoT devices; it should be determined whether these can be generic or domain-specific to application domains. In fact, since CC certification is known for being a relatively slow and costly process, a non-CC certification approach may prove more suitable for IoT devices.

Owing to a lack of legislation, the adoption of security guidelines and best practices remains voluntary. An initial step taken by the United States is to mandate that the government shall only procure IoT devices that conform to some measure of security. This approach can contribute significantly towards a secure IoT when large countries participate, but smaller economies such as Singapore and the Netherlands should work together for greater impact.

Liability can prove to be an effective mechanism to drive the industry towards security, although in most cases liability legislation needs to be modernised to account for the nature of IoT. The process of identifying the responsible manufacturer or supplier and holding them liable for a vulnerability is a supply chain management challenge. IoT hardware and software manufacturers and suppliers should adopt a supply chain risk management framework (e.g. ISO28000, TL9000) to cascade cybersecurity requirements, risk and liability up the supply chain.

At the device level, a root of trust (RoT) is an immutable trust anchor; the chain of trust should preferably build on a hardware RoT. RoT-based cybersecurity is provided by several solutions including TPMs and PUFs. IoT security guidelines emphasise hardware roots of trust; yet, established practices are lacking regarding their use in resource-constrained devices. Security reference architectures are required across a range of constraint classes.

There is a diversity of operating systems, cloud solutions and application development frameworks in the IoT market. An in-depth evaluation is required on the security claims made for each solution. Cloud-based IoT platforms offer comprehensive device management functionality including onboarding and patching, but are largely unstandardised. IoT-specific secure software development lifecycle (SDLC) guidelines are necessary for IoT developers, platform operators, industry and manufacturers.

A number of standards have emerged for IoT networking; however, an in-depth review is required of the security of these protocols and the security and privacy requirements on each level of the communication stack in the IoT ecosystem. Regardless of communication protocol, secure gateways are recommended and can provide a level of security even in deployments that use low-cost IoT devices.

History shows that device-level vulnerabilities are invariably found after a product is deployed – and are often exploited in “zero-day” attacks. It is important to be able to detect unforeseen vulnerabilities, anomalies and threats in live deployments, and to respond quickly, recover and remediate. Monitoring is especially vital for IoT, but data collection and analytics for massive numbers of IoT devices remains a challenge. A strategy to deal with discovered threats and vulnerabilities should include a CVD program that balances security with the interests of manufacturers and stakeholders, and includes the propagation of vulnerability information up and across supply chains.

Keeping software and firmware up-to-date via patches and updates is critical for a secure IoT ecosystem. Updates should be delivered and deployed using a secure and verifiable methodology. If a vendor identifies or is informed about vulnerabilities, it must patch them in a timely manner and publish patch information as part of an auditable Vulnerability Management Program.

Most importantly, the industry should act as a global community when learning from incidents. This requires an open culture of sharing and mutual learning, and the understanding that security is a joint responsibility.

It is recommended to set up a global initiative on secure IoT in order to address the below gaps.

– Limited adoption of IoT security practices and lack of harmonised operational expertise – A number of standards, guidelines and good practices are proposed and available; however, harmonisation towards a practical set of security standards is lacking, and clear-cut information on implementing conformant security functionality is scarce. Given that manufacturers are currently not mandated or incentivised to implement cybersecurity measures, and that a widely-accepted IoT security certification framework does not exist, there is no compelling reason for manufacturers to invest in delivering secure products.
– Lack of alignment and information sharing across supply chains and geographies – IoT security is fundamentally a global problem that demands a global solution. Since IoT devices can reach and be reached from distant parts of the world, and modern products use components that may originate in several different countries, it is important to coordinate policies, share knowhow and intelligence, and propagate vulnerability information up and across supply chains.
– Lack of foundational IoT device security – By some measures, only 4% of IoT devices build their cybersecurity on top of a hardware root of trust.

The initiative should focus on the following challenges on a priority basis in order to address the gaps identified above. These are also highlighted by the experts consulted for the study; section 3.4 described their inputs on the priority challenges.

1. Evaluation and certification of IoT devices in order to provide assured security baselines for a wide variety of devices. A globally aligned approach with government involvement is necessary.
2. Monitoring and supply chain security along with global intelligence sharing for cybersecurity and trust at component level. It is important to close the gap between device supply chains and the threat and vulnerability intelligence gathered from a monitoring effort.
3. Hardware security and trusted device identities, focusing on the security of different root-of-trust implementations and their suitability for different device types. More research is needed on the use of alternatives such as PUFs for low-cost IoT devices. In particular, the use of these alternatives in various practical scenarios such as authentication, encryption and secure booting needs to be investigated.

This IoT security initiative should be a partnership with strong involvement of government agencies, industry and academia. Government agencies should set the direction and steer nations towards a secure and safe IoT environment, working closely with thought leaders, cybersecurity and IoT experts from industry, academia and research organisations. The overarching objective is to share ideas and experiences, shape technologies and architectures, and drive standards and collaboration in order to ensure a safe and secure Internet of Things.

ANNEX A – IOT SECURITY IN SMART MOBILITY AND SMART HEALTH

SMART MOBILITY

The societal challenge of smart mobility[284] is to achieve a transport system that is resource-efficient, climate and environmentally-friendly, and functions safely and seamlessly for the benefit of all citizens, the economy and society. IoT is a key enabling technology to solve this challenge.

A modern vehicle can have between 8 and 30 on-board computers that manage various aspects of car functionality, from the speed of the car to the temperature of its interior. These numbers illustrate the observation that a car is not a single IoT device, but more appropriately thought of as a mega-IoT device or, more formally, a system-of-systems of IoT devices. Within this system-of-systems, the constraints are cost, computing power, and bandwidth limitations; physical constraints are usually less critical in a car environment.

A connected car is invariably equipped with Internet access, and usually also with a wireless local area network. This allows the car to share Internet access with other devices inside as well as outside the vehicle.

The successful and safe deployment of connected vehicles in different use case scenarios, using local and distributed information and intelligence, is a challenging task[285] that needs to use reliable, real-time IoT platforms managing safety-critical vehicle services, advanced sensors and actuators, navigation and cognitive decision-making technology, interconnectivity between vehicles (V2V), and vehicle to infrastructure (V2I) communication. Connected vehicles will enable the development of service ecosystems based on collected information (e.g. maintenance, personalised insurance, and even customised in-car entertainment).

As with all IoT devices, the additional functionality offered by a connected car comes with risks and potentially fatal consequences. Researchers have already proven that modern, computerised vehicles can be hijacked with just a laptop computer and easily obtained software. Hackers have demonstrated that they can display false readings on the dashboard, remotely control steering and disable brakes, and switch off the engine remotely when the vehicle is in motion[286].

ENISA identifies[287] good practices to ensure the security of smart cars against cyber threats, categorising these practices into policy, organisational and technical measures. Policy measures include adherence to regulation and establishment of liability; organisational measures include the designation of a dedicated security team within organisational players in the connected car industry, the development of a dedicated Information Security Management System (ISMS) tailored to industry needs, and the introduction of security and privacy controls in the design phase; and technical measures include end-to-end encrypted communications, state-of-the-art standards for cryptography and random-number generation, dedicated and independently-audited hardware security modules (HSMs), and secure key management practices. ENISA also

284 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/smart-green-and-integrated-transport
285 Report: AIOTI WG 9 – Smart Mobility, 2015
286 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
287 Cyber Security and Resilience of Smart Cars, ENISA, Dec 2016

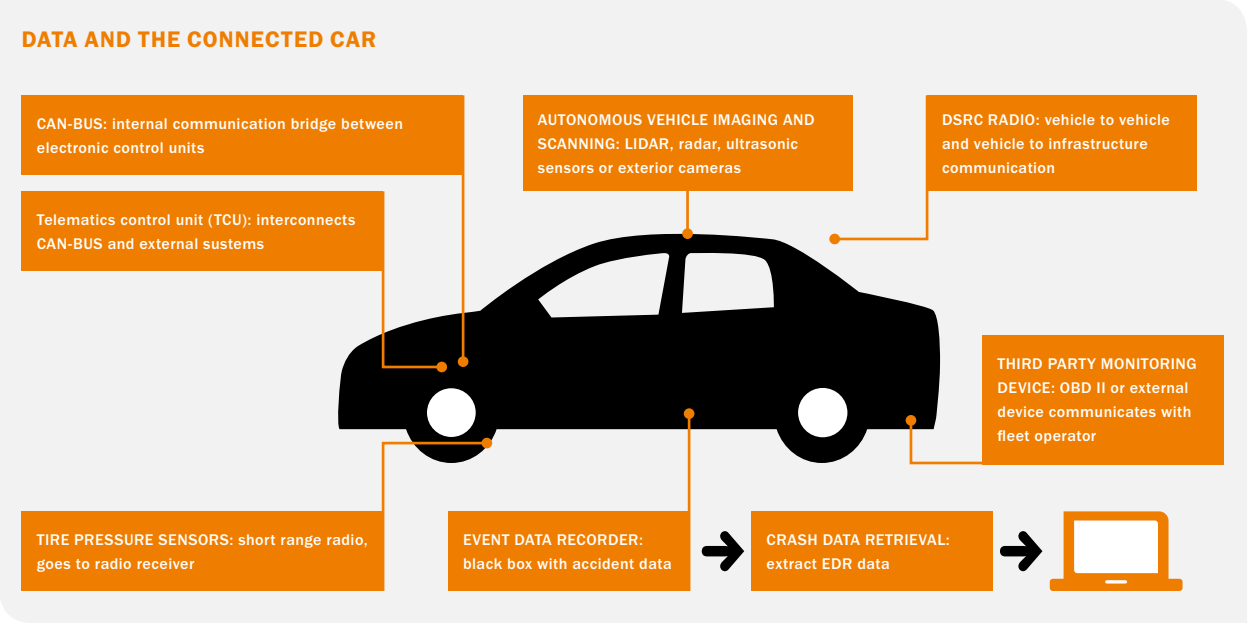


Figure 26: *Connected car with different functions (Source: Future of Privacy Forum)*

recommends improved information sharing between industry stakeholders as well as clarification of liability amongst industry actors.

In addition to safety and security dangers, drivers and passengers face privacy threats. Private data on smart phones, such as e-mail, text messages, contacts and other personal data, could be stolen by hackers. Vehicle location information can be used to determine when the occupants of a home are away, giving burglars a window of opportunity.

Several initiatives have been launched to address the security issues inherent to connected cars. The European Commission's Alliance for IoT Innovation (AIOTI) has a workgroup dedicated to Smart Mobility, which includes IoT use cases pertaining to the car industry. The eCall initiative[288], described in Chapter 4, is intended to bring rapid assistance to motorists in the event of a crash by communicating the vehicle's location and direction to emergency services; eCall has been mandatory for all new cars sold within the EU since April 2018. Intelligent Transportation Systems (ITS) groups worldwide, particularly ERTICO[289] in Europe, are involved in a number of pilot projects in the area of smart mobility. ERTICO has also released recommendations[290] on communication technologies for future Cooperative ITS (C-ITS) scenarios. The American Future of Privacy Forum[291] and National Automobile Dealers' Association (NADA) have published a

288 https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018
289 http://ertico.com/
290 http://erticonetwork.com/ertico-releases-guide-about-technologies-for-future-c-its-service-scenarios/
291 https://fpf.org/

consumer guide[292] highlighting the types of data that connected cars collect and transmit.

The Security Credential Management System (SCMS) of the U.S. Department of Transportation is a proof-of-concept (POC) message security solution[293] for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. It uses a Public Key Infrastructure (PKI)-based approach that employs encryption and certificate management to facilitate trusted communication. Authorised system participants use digital certificates issued by SCMS to authenticate and validate the safety and mobility messages that form the foundation for connected vehicles. To protect the privacy of vehicle owners, these certificates contain no personal or equipment-identifying information but serve as system credentials so that other users in the system can trust the source of each message. SCMS also protects the contents of each message by identifying and removing misbehaving devices, while maintaining privacy.

Amongst industry initiatives, IBM advocates its Design, Build, Drive philosophy that aims to secure each phase of the lifecycle of the connected car. In particular, IBM recognises the need for designing a secure infrastructure in addition to a secure vehicle, given that infrastructure-based attacks such as falsified traffic conditions could wreak havoc by causing unexpected rerouting and braking. The approach also emphasises the need for a trusted supply chain and a trusted maintenance ecosystem.[294]

SMART HEALTH

The societal challenge of health, demographic change and well-being[295] aims to improve the lifelong health and well-being of all citizens; this means high-quality, economically sustainable and innovative health and care systems, as

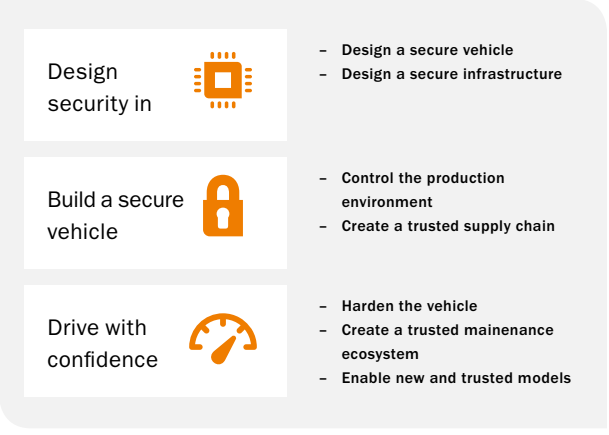


Figure 27: *IBM's Design, Build, Drive Approach (Source: IBM)*

part of welfare systems, and opportunities for new jobs and growth. Smart health includes health services, electronic record management, smart home services and intelligent and connected medical devices.[296]

ENISA has proposed key recommendations for hospital information security executives and industry to enhance the level of information security in Smart Hospitals.[297] Through the identification of assets and the related threats when IoT components are supporting a healthcare organisation, the report describes the Smart Hospital ecosystem and its specific objectives. The solutions to realise a smart hospital (or even more ambitiously, true "Smart Health" – where the boundaries between hospitals and home care start to blur) are broad and diverse. A related technology for home care is Ambient Assisted Living (AAL), which aims at helping older people live as independently as possible by embedding intelligent objects in the environment.[298]

292 https://fpf.org/2017/01/25/fpf-and-nada-launch-guide-to-consumer-privacy-in-the-connected-car/
293 https://www.its.dot.gov/resources/scms.htm
294 IBM Executive Report, Driving security: Cyber assurance for next-generation vehicles, Christopher Poulin
295 http://ec.europa.eu/programmes/horizon2020/en/h2020-section/health-demographic-change-and-wellbeing
296 https://www.activeadvice.eu/news/concept-projects/what-is-smart-health-and-how-do-people-benefit/
297 Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures, ENISA, November 2016.
298 http://www.aal-europe.eu/

AAL technologies range from automatically switching off kitchen appliances or lights to monitoring vital functions and the automatic notification of medical assistance in case of an emergency. One such effort is the in-home monitoring services for the elderly[299] from Fujitsu and Panasonic.

Personal wellness applications based on IoT devices for both generic and health-specific purposes constitute important developments towards Smart Health. These can be accompanied by remote health monitoring and staff identification. Smart Health IoT devices contain and retain highly sensitive personal data of the patients to whom the device is attached, be it temporary (e.g. electrocardiogram) or more permanent (e.g. pacemaker). As can be imagined, vast amounts of Protected Health Information (PHI) are collected by the devices and either retained or shared in real-time for querying and analysis.

As might be expected, there have already been cases of security compromise in the domain of Smart Health. According to Cylance[300], in 2017 Abbott's (formerly St. Jude Medical) found itself the centre of attention for the U.S. Food and Drug Administration[301] (FDA) and unhappy patients over their pacemakers, defibrillators, and other medical devices being vulnerable to third-party man-in-the-middle access via cybersecurity vulnerabilities. Such vulnerabilities could affect how the device operates,

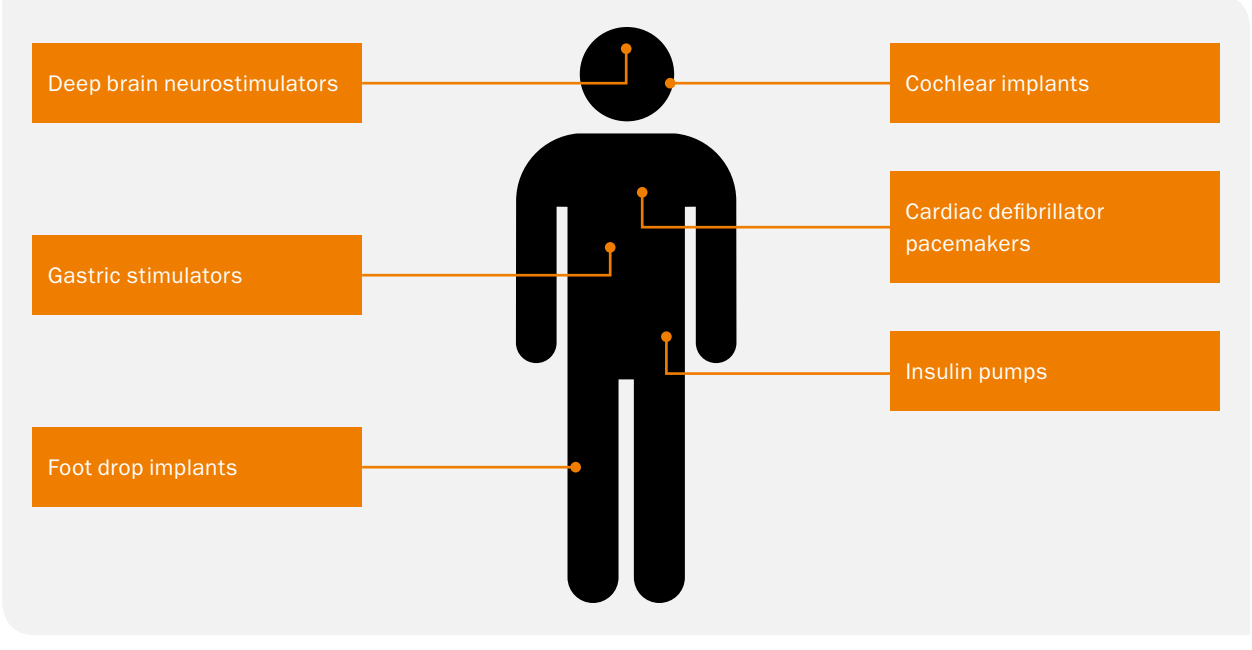


Figure 28: *Wireless Implantable Medical Devices, source: pinstake.com.*

299 http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0625-01.html

300 https://www.cylance.com/en_us/blog/medical-device-security-the-state-of-play.html

301 https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

including “rapid depletion of battery and/or inappropriate pacing or shocks.” In August 2017, the FDA approved a firmware update which addressed these vulnerabilities. Separately, German electronics company Siemens issued a customer alert[302] in July 2017 warning of the highly critical vulnerabilities in many of their medical scanners. Pending a solution, Siemens has directed the devices to be taken offline.

As with smart mobility IoT applications, smart health IoT is vulnerable by definition as well. As a result, cybersecurity flaws can lead to grievous safety losses. This emphasises the need for cybersecurity in smart health devices. Are these devices safe, secure, reliable, and resilient, and do they uphold privacy expectations? Given the critical nature of these devices, the sensitivity of the information they capture, and the complexity of smart health ecosystems and supply chains, it is imperative to work towards an assured security framework for connected medical devices.

302 https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-822184.pdf

ANNEX B – CATALOGUE OF KEY INITIATIVES

AIOTI

Title	AIOTI
Description	The Alliance for IoT Innovation (AIOTI) is an inclusive body with members including key IoT industrial players – large companies, successful SMEs and dynamic startups – as well as well-known European research centres, universities, associations and public bodies. In October 2015, the Alliance published 12 reports covering IoT policy and standards issues. AIOTI also provided detailed recommendations for future collaborations in the Internet of Things Focus Area of the 2016-2017 Horizon 2020 program.
Website	https://aioti.eu
Region / Country	EU
Membership	Primarily industry, and a few academic institutes
Challenges Addressed	Cybersecurity and Privacy by Design, IoT Security Standards, Future-Proof Legislation

CLOUD SECURITY ALLIANCE – IOT WORKING GROUP

Title	Cloud Security Alliance – IoT Working Group
Description	The cloud plays an important role in the successful implementation of IoT. Cloud services include data collection, brokerage and storage, data analytics, inventory management, sensor management, visualisation services and monitoring, as well as device relationship management. Additional cloud services will continue to emerge as new ways of taking advantage of IoT are devised and autonomous relationships are built between web services and IoT device middleware. The Cloud Security Alliance IoT Working Group focuses on understanding the relevant use cases for IoT deployments and defining actionable guidance for security practitioners to secure their implementations.
Website	https://cloudsecurityalliance.org/group/internet-of-things/#_overview
Region / Country	Global, US focus
Membership	Industry
Challenges Addressed	Secure OS, Platform and Cloud

ENISA IOT SECURITY EG

Title	ENISA IoT and ENISA IoT Security Experts Group
Description	ENISA defines Internet of Things as an emerging concept describing a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. With great impact on citizens' safety, health and privacy, the threat landscape concerning Internet of Things is extremely wide. Hence it is important to understand what needs to be secured and to develop specific security measures to protect Internet of Things from cyber threats. ENISA's IoTSEC group is an information exchange platform that brings together experts to ensure security and resilience of the entire Internet of Things ecosystem.
Website	https://resilience.enisa.europa.eu/iot-security-experts-group-1
Region / Country	EU
Membership	Governments and government bodies
Challenges Addressed	Cybersecurity and Privacy by Design, IoT Security Standards, Future-Proof Legislation

ETSI

Title	ETSI
Description	ETSI is a European Standards Organisation (ESO) and a recognised regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. ETSI has a special role in Europe, supporting European regulations and legislation through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognised as European Standards (ENs). While ETSI was initially founded to serve European needs, its standards are now used the world over.
Website	https://www.etsi.org
Region / Country	EU
Membership	Industry, Government and Academia
Challenges Addressed	Cybersecurity and Privacy by Design, IoT Security Standards

GLOBALPLATFORM

Title	GlobalPlatform
Description	GlobalPlatform is a non-profit industry association driven by over 100 member companies. GlobalPlatform's Trusted Execution Environment (TEE) standard defines a secure area in the processor of a connected device that stores, processes and protects sensitive data. GlobalPlatform also relates the idea of Root of Trust to both SE and TEE technologies.
Website	https://globalplatform.org/
Region / Country	Global
Membership	Industry
Challenges Addressed	Evaluation and Certification, Device Identity and Root of Trust

GLOBAL CYBER ALLIANCE

Title	Global Cyber Alliance
Description	The Global Cyber Alliance is an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world. Founding members include the London Police, the New York District Attorney and the Center for Internet Security.
Website	https://www.globalcyberalliance.org/
Region / Country	Global
Membership	Industry, Government
Challenges Addressed	Monitoring and Analytics, Evaluation and Certification

GSMA

Title	GSMA
Description	The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.
Website	https://www.gsma.com/
Region / Country	Global
Membership	Industry
Challenges Addressed	IoT Security Standards, Communications and Infrastructure

INTERNET ENGINEERING TASK FORCE

Title	Internet Engineering Task Force
Description	The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.
Website	https://www.ietf.org/
Region / Country	Global
Membership	Industry, Academia
Challenges Addressed	IoT Security Standards, Communications and Infrastructure

INDUSTRIAL IOT CONSORTIUM

Title	Industrial IoT Consortium
Description	The Industrial Internet Consortium aims to transform business and society by accelerating the Industrial Internet of Things (IIoT). IIC's mission is to deliver a trustworthy IIoT in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes.
Website	http://www.iiconsortium.org
Region / Country	Global
Membership	Industry, US based
Challenges Addressed	Supply Chain Security, Product Life Cycle Support, IoT Security Standards, Secure OS and Applications, Secure Communications and Infrastructure, Security Monitoring and Analytics

IOT ACCELERATION CONSORTIUM

Title	IoT Acceleration Consortium
Description	The creation of innovative business models through the utilisation of IoT and the realisation of a safe and secure society for the public are important goals for Japan. Aiming to discuss necessary efforts or measures to achieve these goals, the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC) have established an IoT Security Working Group (WG) under the IoT Acceleration Consortium.
Website	http://www.iotac.jp/en/
Region / Country	Japan
Membership	Academia, Industry
Challenges Addressed	IoT Security Standards

IOT CONSORTIUM

Title	Internet of Things Consortium
Description	The Internet of Things Consortium (IoTC) is a business development association for the Internet of Things (IoT) ecosystem. It is comprised of leading founders, executives and global companies in IoT. The IoTC's mission is to ignite the growth of the IoT marketplace by leading the industry's efforts through strategic partnerships. The organisation focuses on five key verticals: connected homes, autos, cities, retail and wearables.
Website	http://iofthings.org
Region / Country	Global
Membership	Industry
Challenges Addressed	Responsible Industry Ecosystem

IOT CYBERSECURITY ALLIANCE

Title	IoT Cybersecurity Alliance
Description	The IOTCA alliance is where industry-leading IoT security providers and top IoT experts come together to raise awareness, establish and share best practices, and research and develop methods to holistically secure the IoT ecosystem for the good of all.
Website	https://www.iotca.org
Region / Country	Global
Membership	Industry members including AT&T, IBM, Nokia, Palo Alto Networks, Qualcomm, Symantec and Trustonic
Challenges Addressed	IoT Security Standards, Secure OS, Cloud and Applications, Secure Communications and Infrastructure, Security Monitoring and Analytics

IOT EUROPEAN PLATFORMS INITIATIVE

Title	IoT Cybersecurity Alliance
Title	IoT European Platforms Initiative
Description	The IoT-European Platforms Initiative (IoT-EPI) was formed to build a vibrant and sustainable IoT-ecosystem in Europe, maximising the opportunities for platform development, interoperability and information sharing. With a total funding of 50M€ and a partner network of 120 established companies and organisations, IoT-EPI projects develop innovative platform technologies and foster technology adoption thorough community and business building.
Website	http://iot-epi.eu
Region / Country	EU
Membership	Seven research and innovation projects: Inter-IoT, BIG IoT, AGILE, symbIoTe, TagItSmart!, VICINITY and bIoTope.
Challenges Addressed	Responsible Industry Ecosystem

IOT SECURITY FOUNDATION

Title	IoT Security Foundation
Description	Internet of Things Security Foundation (IoTSF) aims to make it safe to connect things so the many benefits of IoT can be realised. IoTSF is a collaborative, non-profit, international response to the complex challenges posed by security in the expansive hyper-connected world. As such, IoTSF is a destination for IoT security professionals, IoT hardware and software product vendors, network providers, system specifiers, integrators, distributors, retailers, insurers, local authorities, government agencies and others who seek security.
Website	https://www.iotsecurityfoundation.org/
Region / Country	Global
Membership	Industry
Challenges Addressed	IoT Security Standards, Evaluation and Certification, Supply Chain Security, Product Life Cycle Support, Secure OS and Applications, Secure Communications and Infrastructure, Security Monitoring and Analytics

ITU STUDY GROUP 20

Title	ITU Study Group 20
Description	ITU SG20 develops international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. A central part of this study is the standardisation of end-to-end architectures for IoT, and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors.
Website	http://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx
Region / Country	Global
Membership	Government, Academia, Industry
Challenges Addressed	Secure Communications and Infrastructures, IoT Security Standards

LORA ALLIANCE

Title	Lora Alliance
Description	The LoRa Alliance is an open, nonprofit association that has grown to more than 500 members since its inception in March 2015. Its members collaborate and share experiences to promote and drive the success of the LoRaWAN protocol as an open global standard for secure, carrier-grade IoT LPWAN connectivity. With the technical flexibility to address a broad range of IoT applications, both static and mobile, and a certification program to guarantee interoperability, LoRaWAN has been deployed by major mobile network operators globally, with continuing expansion.
Website	https://lora-alliance.org/about-lora-alliance
Region / Country	Global
Membership	Industry
Challenges Addressed	Secure Communications and Infrastructures

NIST – IOT PROGRAM

Title	NIST Cybersecurity for IoT Program
Description	NIST's Cybersecurity for the Internet of Things (IoT) program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and promote U.S. leadership in IoT.
Website	https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
Region / Country	US
Membership	Industry
Challenges Addressed	IoT Security Standards

OPEN CONNECTIVITY FOUNDATION

Title	Open Connectivity Foundation (OCF)
Description	OCF's Mission is twofold: 1. Provide specifications, code and a certification program to enable manufacturers to bring OCF Certified products to the market that can interoperate with current IoT devices and legacy systems. 2. Make the end user's experience better by seamlessly bridging to other ecosystems within a user's smart home and ensure interoperability with OCF compliant devices. OCF Specifications leverage existing industry standards and technologies, provide connection mechanisms between devices and between devices and the cloud, and manage the flow of information among devices, regardless of their form factors, operating systems, service providers or transports.
Website	https://openconnectivity.org/
Region / Country	Global, US/Canada focus.
Membership	Industry
Challenges Addressed	Secure Communications and Infrastructure and IoT Security Standards

OWASP IOT PROJECT

Title	OWASP IoT project
Description	The Open Web Application Security Project (OWASP) Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies. The project looks to define a structure for various IoT sub-projects such as Attack Surface Areas, Testing Guides and Top Vulnerabilities.
Website	https://www.owasp.org/index.php/ OWASP_Internet_of_Things_Project
Region / Country	Global
Membership	Volunteers, Industry
Challenges Addressed	Secure Communications and Infrastructure, Secure OS and Applications, and IoT Security Standards

PRPL FOUNDATION

Title	prpl Foundation
Description	The mission of the prpl Foundation is to: (a) develop, support and promote an open-source, community-driven consortium with a focus on enabling the security and interoperability of embedded devices for the Internet of Things (IoT) and smart society of the future; and (b) undertake other activities as appropriate to further the purposes and achieve the goals set forth above. Historically, the prpl Foundation was developed around the MIPS ecosystem; it has now evolved to become instruction set-neutral in its approach.
Website	https://prpl.works
Region / Country	Global
Membership	Industry, Academia
Challenges Addressed	Device Identities and Root of Trust

T2T RESEARCH GROUP

Title	Thing-to-Thing (t2trg) Research Group by IETF
Description	The Thing-to-Thing Research Group (T2TRG) intends to investigate open research issues in turning IoT into reality, as an Internet where low-resource nodes can communicate among themselves and with the wider Internet in order to partake in permissionless innovation. The focus of the T2TRG is on opportunities for standardisation in the IETF, i.e. starting at the adaptation layer connecting devices to IP and ending at the application layer with architectures and APIs for communicating and making data and management functions (including security functions) available.
Website	https://datatracker.ietf.org/rg/t2trg/
Region / Country	Global
Membership	Industry members
Challenges Addressed	Secure Communications and Infrastructure, Secure OS and Applications, IoT Security Standards

TRUSTED COMPUTING GROUP

Title	Trusted Computing Group
Description	The Trusted Computing Group (TCG) is a not-for-profit organisation formed to develop, define and promote open, vendor-neutral, global industry standards, including of a hardware-based root of trust, for interoperable trusted computing platforms. TCG has developed specifications for a Trusted Platform Module (TPM), which is a cryptographic coprocessor embedded within a computing system to securely identify individual connected devices and generate and store keys within these devices. Separately, the DICE Architectures Work Group of the TCG is exploring new security and privacy technologies applicable to systems with or without a TPM. TCG's SED standards allow encryption to be built into the drives of IoT devices. Also, TCG's Trusted Network Communications (TNC) network security architecture and open standards provide network and endpoint visibility, helping network managers know who and what is on their network, and whether devices are compliant and secure. TNC standards also enable network-based access control enforcement — granting or blocking access based on authentication, device compliance, and user behaviour — and security automation.
Website	https://trustedcomputinggroup.org
Region / Country	Global
Membership	Industry members
Challenges Addressed	Device Identity and Root of Trust, Secure OS, Cloud and Applications, Secure Communications and Infrastructures, Security Monitoring and Analytics.

UEFI FORUM

Title	Unified Extensible Firmware Interface (UEFI) Forum
Description	The UEFI Forum champions firmware innovation through industry collaboration and the advocacy of a standardised interface that simplifies and secures platform initialisation and firmware bootstrap operations. These extensible, globally-recognised specifications bring new functionality and enhanced security to the evolution of devices, firmware and operating systems, as well as facilitate interoperability between platforms and systems that comply with next-generation technologies. The UEFI Forum advocates a standardised interface to simplify and secure platform initialisation and firmware bootstrapping. The UEFI specification includes enhanced security during system boot-up ("UEFI Secure Boot") via a cryptographic chain of trust.
Website	http://www.uefi.org/about
Region / Country	Global, US lead
Membership	Industry members
Challenges Addressed	Device Identity and Root of Trust, Secure OS, Cloud and Applications.

WI-SUN ALLIANCE

Title	Wi-SUN Alliance
Description	Wi-SUN Alliance is an industry association devoted to seamless connectivity. Wi-SUN seeks to promote certified standards that coordinate various wireless systems and standardise power levels, data rates, modulations, and frequency bands, among other variables.
Website	https://www.wi-sun.org/
Region / Country	Primarily Asia (Japan) but also has global industry members
Membership	Industry (including Toshiba and Cisco)
Challenges Addressed	Secure Communications and Infrastructure

ZIGBEE ALLIANCE

Title	Zigbee Alliance
Description	Established in 2002, the Zigbee Alliance is a group of companies that maintain and publish the Zigbee standard, a suite of communication protocols based on IEEE 802.15.4.
Website	https://www.zigbee.org/
Region / Country	Global
Membership	Industry (including NXP and Texas Instruments)
Challenges Addressed	Secure Communications and Infrastructure

19-11070 October 2019

ISBN 9789090324913