COMMUNICATIONS
ALLIANCE LTD

G654:2017

INTERNET OF THINGS
SECURITY GUIDELINE

G654:2017 Internet of Things Security Guidelin

First published as IoTAA Internet of Things Security Guideline
February 2017, http://www.iot.org.au/

Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

Disclaimers

1) Notwithstanding anything contained in this Industry Code:

   a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:

      i) reliance on or compliance with this Industry Code;

      ii) inaccuracy or inappropriateness of this Industry Code; or

      iii) inconsistency of this Industry Code with any law; and

   b) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Industry Code.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

G654:2017 INTERNET OF THINGS SECURITY GUIDELINE

AUGUST 2017

INTRODUCTORY STATEMENT

The purpose of the *Internet of Things Security Guideline* is to provide comprehensive, top-level guidance to:

- promote a ‘security by design’ approach to IoT;
- assist industry to understand the practical application of security and privacy for IoT device use;
- be utilised by the IoT industry and digital service providers which use or provide support services for IoT deployments; and
- assist industry to understand some of the relevant legislation around privacy and security.

Malcolm Shore

Outgoing Chair

Workstream 5 *Security and Network Resilience*, IoT Alliance Australia (IoTAA)

February 2017

TABLE OF CONTENTS

1. GENERAL

1.1 Introduction

1.1.1 The development of this Guideline has been facilitated by Workstream 5 Security and Network Resilience of IoT Alliance Australia (IoTAA). Workstream 5 comprises representatives from the IoT and telecommunications industries, government, privacy advocates and consumer groups.

1.1.2 The Guideline should be read in the context of other relevant codes, guidelines, standards and documents.

1.1.3 The Guideline should be read in conjunction with related legislation, including:

(a) the *Telecommunications Act 1997*;

(b) the *Telecommunications (Interception and Access) Act 1979*;

(c) the *Radiocommunications Act 1992*; and

(d) the *Privacy Act 1988*.

1.1.4 Compliance with this Guideline does not guarantee compliance with any legislation. The Guideline is not a substitute for legal advice.

1.2 Scope

1.2.1 This Guideline covers security and privacy of:

(a) data generated by IoT devices;

(b) data carried to and from IoT devices;

(c) data stored in IoT devices;

(d) consumers using IoT devices; and

(e) actuators driven by IoT systems.

1.2.2 This Guideline covers resilience of:

(a) IoT device communications; and

(b) wide area IoT transit communications.

1.2.3 This Guideline deals with IoT devices associated with, but not limited to:

(a) home use by consumers;

(b) business use in the office environment;

(c) business use in operational systems; and

(d) critical infrastructure use.

1.2.4 This Guideline deals with:

(a) the general principles applicable to IoT security and user privacy;

(b) specific interpretation of standard security and privacy controls in the IoT context;

(c) guidance on the use and storage of information obtained through IoT devices;

(d) resilience of networks to and from the IoT device; and

(e) the application of relevant legislation.

1.3 Objectives

1.3.1 The objectives of the Guideline are to:

(a) assist industry in their understanding of the practical application of security and privacy for IoT device use;

(b) be utilised by the IoT industry, carriers, and carriage service providers which use or provide support services for IoT deployments; and

(c) assist industry in understanding the application of relevant legislation.

1.3.2 The Guideline brings together sources of information relating to the security, privacy, and resilience of IoT to assist the IoT industry in delivering quality products and services. It does not endorse any specific technology or approach for use in Australia.

1.4 Guideline review

The Guideline will be reviewed in the event of significant developments that affect the Guideline, or a chapter within the Guideline.

2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 Acronyms

For the purposes of the *Guideline*:

3GPP

means the 3rd Generation Partnership Project

ACL

means Access Control Lists

AES

means Advanced Encryption Standard

AES/CBC

means AES with Cipher Block Chaining Mode

AES/CCM

means AES with Counter-CBC Mode

AES/CTR

means AES with Counter Mode

APP

means Australian Privacy Principles

CANbus

means Controller Area Network Bus

CoAP

means Constrained Application Protocol

CSP

means Carriage Service Provider

DTLS

means Datagram Transport-Layer Security

GSMA

means Groupe Speciale Mobile Association

IEEE

means Institute of Electrical and Electronics Engineers

IETF

means Internet Engineering Task Force

IIC

means Industrial IoT Consortium

IIOT

means Industrial IoT

IoT

means Internet of Things

IoTSF

means IoT Security Foundation

IPSec

means IP Security Protocol

LPWAN

means Low Power Wide Area Network

LR-WPAN

means Low Rate Wireless Personal Area Network

MAC

means Media Access Control

mDNS

means Multicast DNS Service

NB-IOT

means Narrow Band IoT

NGN

means Next Generation Network

NIST

means National Institute of Standards and Technology, US

OAIC

means Office of the Australian Information Commissioner

OIC

means Open Interconnect Consortium

OWASP

means Open Web Application Security Project

PLC

means Programmable Logic Controller

SABSA

means Sherwood Applied Business Security Architecture

SCADA

means Supervisory Control and Data Acquisition

SLA

means Service Level Agreement

SSL

means Secure Sockets Layer

TLS

means Transmission Layer Security

UAV

means Unmanned Aerial Vehicle (drone)

UDP

means User Datagram Protocol

WSN

means Wired Sensor Networks.

2.2 Definitions

For the purposes of the *Guideline*:

Act

means the *Telecommunications Act 1997 (Cth)*.

Australian Privacy Principle

has the meaning given by Schedule 1 of the *Privacy Act 1988 (Cth)*.

Carriage Service Provider (CSP)

has the meaning given by Section 87 of the Act.

Carrier

has the meaning given by section 7 of the Act.

Equipment

means apparatus or equipment used in connection with a Telecommunications Network.

Telecommunications Network

means a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or series of systems, for carrying communications solely by means of radio communication.

Telecommunications System

means a telecommunications network that is within Australia; or a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia; and includes equipment, a line or other facility that is connected to such a network and is within Australia.

2.3 Interpretations

In the *Guideline*, unless the contrary appears:

(a) headings are for convenience only and do not affect interpretation;

(b) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(c) words in the singular include the plural and vice versa;

(d) words importing persons include a body whether corporate, politic or otherwise;

(e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(f) mentioning anything after include, includes or including does not limit what else might be included; and

(g) a reference to a person includes a reference to the person's executors, administrators, successors, agents, assignees and novatees.

3 THE INTERNET OF THINGS

3.1 Background

From a network of connected computers to a network with billions of connected static and mobile devices, the internet is becoming the connectivity fabric for an increasingly diverse array of things – ranging from home furnishings and white-ware to human implants. The mobile revolution saw the number of end-point devices exceed one billion in 2002, and the introduction of smart phone technology and tablets means that now the vast majority of these devices are online.

Over the last twenty years, cars have become highly networked and are increasingly being connected to the internet for safety, navigation and entertainment purposes. A modern car now has multiple networks and dozens of microprocessors. The emergence of vehicle ethernet means that these microprocessors are increasingly becoming directly internet-accessible. Connected traffic management is used to improve driver experience, in-vehicle connectivity allows better fleet management, and public transport systems have become connected to provide schedule notifications. Smart parking and smart paying are emerging as standard in-car services. Intelligent transport systems are continuing to leverage connectivity. Smart driving systems will improve safety by assisting drivers in braking and avoiding incidents.

Hospitals are adopting operational health technology which can be remotely accessed to deliver the eHealth capability, within the hospital confines and through implanted and wearable devices. This is extending into the sports space with online recording of athletes' performance. Such systems are not only becoming connected, but increasingly leveraging cloud-based applications.

Utilities are starting to be connected, with the electricity sector increasingly adopting the SmartGrid technology. Smart water is next, with the benefits of sensing technology to pinpoint leaks helping drive this demand.

Homes are becoming intelligent, with smart home technology appearing in the basic house infrastructure such as lighting and heating, as well as in appliances such as fridges and cookers. Technology companies are responding with delivering the central connectivity through devices such as Google's OnHub, while new start-ups are delivering a bewildering array of sensors all controlled remotely over the internet using smart phone applications.

Agriculture is not immune from the march of progress, with an increasing dependence upon connected sensors for always-on monitoring of crops and environmental conditions, and the vision of smart-farming. The concept of precision agriculture, and indeed intelligent decision agriculture, depends upon telematics and advanced sensing technologies. Unmanned aerial vehicles (UAVs), are increasingly being used to perform aerial monitoring of crop growth. The use of big data collected across the whole farming operation over time enables intelligent navigation of climatic variation, but depends upon connectivity and agility.

Strategically, smarter cities are essential if the world is to respond effectively to the rapid growth in urban living, with development occurring on a strategic roadmap rather than through piecemeal, tactical developments. Cities need to operate much more energy-efficiently, cater for the continuing demand for bandwidth, enable online service delivery across a wide variety of services, and to do this requires highly resilient utilities. Emergency services will also benefit from rapid access to connected data when responding to incidents.

Industrial control systems are increasingly connected to business networks, not only feeding data into those networks but also responding to decisions made by those systems, causing changes in the environment they control.

In summary, there is major potential in many industries for IoT products and services, with significant focus currently on the following application domains:

- Consumer, particularly wearable and home automation products
- Industrial, including oil, gas and mining, manufacturing, and utilities
- Enterprise, including retail and insurance
- Healthcare
- Smart Cities, including intelligent transport, safety and security
- Agriculture and Food Services
- Automotive, including aero applications such as drones.

The complexity and pace of change is a challenge which requires integrated systems across what has traditionally been a siloed set of service solutions, integrating also with humans and physical systems. This requires a smart city framework, along the lines of that documented by the British Standards Institution[1].

The increasing connectivity of physical, digital, and human systems has become known as the IoT. This connectivity brings with it a plethora of risks, and three critical success factors are resilience, privacy and security.

3.2 IoT Architecture, Protocols and Standards

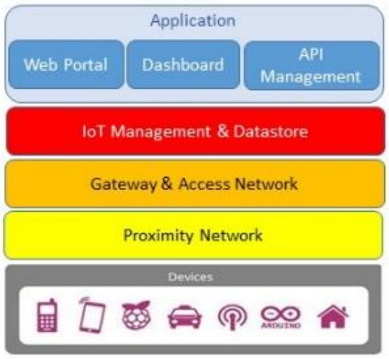
The IoT security architecture is a component of the wider IoT reference architecture. It starts with the business outcomes and derives security requirements and controls traceable to those outcomes. Given the universal applicability of IoT, case specific security architecture viewpoints will need to be developed on demand using standard building blocks. The nature of IoT technology will place unusual demands on the architecture such as low power cryptographic algorithms and low latency communications. Identity and access management is another challenge which requires quite different solutions to traditional enterprise deployments. Secure interoperability will drive the need for security protocol and profile standardisation.

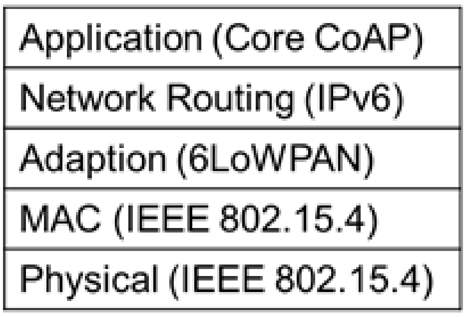
There is no one accepted architectural model for IoT, and the rapid evolution of all areas of the end-to-end technology continues to drive new changes to architectural models. However, for the purposes of this

---

[1] PAS181: 2014: Smart City Framework

document, we can consider a high-level reference architecture for IoT as shown in Figure 1.





Application (Core CoAP)
Network Routing (IPv6)
Adaption (6LoWPAN)
MAC (IEEE 802.15.4)
Physical (IEEE 802.15.4)

Example Communications Stack

FIGURE 1

Reference Architecture for IoT

The end-to-end IoT pathway consists of five main components: IoT devices, a proximity network, gateways and access network, IoT Management and message repository, and end user applications and APIs. This is a logical architecture which doesn’t represent the complexity of physical deployment, as many deployments are blurring the layers by moving application code out to the network edge, in the gateways, or even out to the devices themselves.

CISCO provides a seven layer reference architecture for IoT, which includes also an edge or fog layer for element analysis and transformation, and has separate layers for data aggregation and for data storage. Academic papers proposing three, five, and six layer reference architectures have also been published. This space will evolve.

There are a number of key technical protocols and standards that are being used in the IoT space. As with any new technology, not all will survive, but those that do will be reconciled into the detailed IoT reference architecture.

- Embedded devices connect via a proximity network to their local gateway using short distance protocols such as ZigBee, ZWave, Thread, Bluetooth and Bluetooth LE, and WiFi. There are also a number of long-range IoT protocols such as LoRa, LTE and NB-IoT, as well as newer protocols in development such as 6LoWPAN. Gateways connect the proximity network to the wider internet either directly or using various access or backhaul network links.
- The IEEE has published a proximity network protocol standard called IEEE802.15.4: Low Power Wireless Access Network, and this is used as foundation of higher level protocols such as 6LoWPAN and Zigbee.
- In the home automation sector, the Home Network Automation Protocol (HNAP) is being adopted by many vendors for device management. The protocol was patented originally by Pure Networks, but is now owned and is being further developed by Cisco.
- The Constrained Application Protocol (CoAP) is an IETF protocol which is designed for RESTful applications and uses HTTP semantics (and feeds into HTTP in the wider network) but with a much smaller footprint and a binary rather than a text-based exchange. CoAP is designed to be

used over UDP. MQTT, the Message Queue Telemetry Transport, is an alternative to CoAP and has been deployed as a publish/subscribe messaging protocol for wireless sensor networks.
- The multicast DNS service (mDNS) is commonly used by IoT devices to resolve host names to IP addresses within small networks that do not include a local name server.
- NB-IoT is a 3GPP standard for narrow band IoT, based on the use of LTE cellular technology. The US National Institute of Standards and Technology (NIST) has released their publication SP800-187: Guide to LTE Security.

The UK Government has promoted the development of an IoT interoperability standard known as Hypercat. This standard aims to improve data discoverability and interoperability and to enable a catalogue of devices and capabilities to be published as a web repository of devices with associated metadata. This is currently one of the preferred interoperability options[2].

3.3 Privacy and Security in IoT

A key part of the response to the increasing interconnectivity is to ensure the deployed systems are available on demand and can be trusted to protect a user's privacy. Given the commodity nature of many IoT devices and the implications of security and privacy, a robust trust framework which is incorporated into the design of products is necessary. The approach should be based on an open and federated business model, a service-oriented IT architecture, and a user-centric trust model. Data needs to be more open and interconnected, but privacy and security must be at the heart of how it's stored and used. In particular, centralisation and matching of data can be met with suspicion by citizens and needs to be managed carefully.

There is also a community of devices which require identity, and these have a different trust model entirely. Identity is a complex and deeply personal concept with individuals having multiple overlapping identities each of which has different rights and permissions. Some identities need to be kept separated, and some need to be joined up. Consequently, whether identities are kept separated or joined up needs to be considered on a case-by-case basis, subject to requirements set out in the *Privacy Act 1988* and any other applicable laws. New ways of managing identities need to be developed, as many of the security mechanisms put in place to support identity (passwords, PINs, digital signatures) have in practice acted as barriers to uptake of digital services.

Traditional IT systems implement security based on 25-year-old security control standards which hardly address the current cyber security demands and are quite unsuitable for use as the basis of security and trust in the IoT. The use of enterprise security controls has not worked well in the industrial control systems sector, where the requirement for continuous operation is incompatible with routine patching and restarts. Similarly, it is unlikely that a home light bulb will continuously check for patches, apply

---

[2] IoT Alliance Australia has recommended that the Hypercat Standard be considered by Standards Australia for adoption as an Australian Standard.

updates, and monitor for cyber-attack – with IoT modules at sub-$1, a highly commoditised security paradigm is required.

The evolution of the IoT requires an approach to security and privacy which is agile and supports unforeseen changes, across a wide range of quite different technologies and applications. It requires an approach which recognises a global ecosystem consisting of different sectors using common solutions developed independently, compliant with a common set of principles but implementing a sector specific interpretation of security. A common foundation for this may be the application of security at the data level. End-to-end security across a device-to-application model with secure data analytics may also be part of the solution.

3.4 IoT Resilience

As all sectors of government, industry, and society take advantage of the benefits that can be realised through the IoT, so dependence upon real time connectivity increases. This means that networks must become not only resilient, but must strive for survivability to enable continued operation in the event of cyber-attack.

IoT communications offers some novel challenges with the need for ultra-low-power protocols and algorithms. While some research work has been carried out into survivability, this is an embryonic discipline which needs a great deal of urgent attention.

The approach to resilience is detailed in Section 6.

3.5 5G Considerations

The impact of the launch of 5G technology on network architectures and security requirements should not be underestimated. 5G networks are expected to serve vertical markets with many distinct types of service, each with differing service requirement characteristics. These can broadly be described as:

- xMBB: massive broadband that delivers gigabytes of bandwidth on demand;
- mMTC: massive machine-to-machine communications that connects billions of sensors and machines; and
- uMTC: critical machine-to-machine communications providing minimal latency and high reliability to enable, e.g., remote control over robots and autonomous driving.

It is envisaged that 5G will be provided by carriers to a wide eco-system of carriage service providers, and in doing so will require not only improved networking solutions but also a sophisticated integration of massive computing and storage infrastructures. This will force a massive shift to mobile edge computing and allow service providers access to the underlying network and computing infrastructure. The implication of this is that carriers will need to manage multi-tenancy and multi-service support through network capability orchestration, delivering logical networks. In 5G terminology, these logical networks are known as network slices.

5G networks will enable faster service instantiation, which in turn will require new trust models to support them in an increasingly hostile cyber-threat landscape. This new environment will also require new approaches to user privacy.

5G will likely require the support of new technology approaches such as software defined networking and network function virtualisation resulting in a self-adapting network. It is also likely to require separation of user and control planes, and possibly, redefinition of the boundaries between the network domains (e.g. radio access network and core network). 5G will introduce new concepts such as network-controlled device-to-device (D2D) communication over point-to-point, multi-cast and broadcast protocols, and device duality schemes, where a device can act both as a "normal" end user device or sensor and as a network node extending the infrastructure, as in some existing IoT deployments.

A 5G top level architecture has been proposed by the 5G PPP[3] as shown in Figure 2.

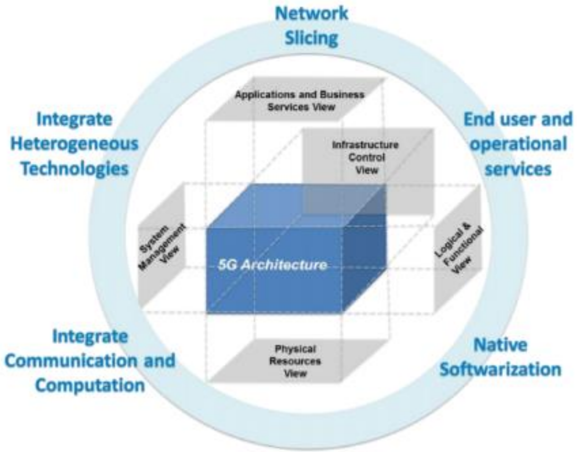


FIGURE 2

5G Architecture

The distinctly different nature of 5G networks will inevitably introduce different and more advanced threats. The key considerations for security in 5G are:

- multi-domain and multi-service models;
- re-definition of operator, user and device roles;
- new service delivery models based on virtualization, network slicing;
- more serious consequences for cyber-attack on critical infrastructure services;
- increasing concerns for user privacy from mass surveillance; and
- the need for lighter and faster encryption systems and algorithms.

---

[3] 5G PPP Architecture Working Group View on 5G Architecture, July 2016

4 PRIVACY

This section will deal with some of the legal issues around privacy given the paramount importance of privacy and data sharing considerations in an IoT context. However, IoT may involve other legal challenges some of which will be discussed in Section 8 of this *Guideline*.

4.1 Privacy Principles

In 2014, a new set of Privacy Principles were enacted[4]. These are set out in the *Privacy Act 1988* and shown in Table 1.

TABLE 1

Australian Privacy Principles (APPs)

Principle	Description
1	Open and transparent management of personal information
2	Anonymity and pseudonymity
3	Collection of solicited personal information
4	Dealing with unsolicited personal information
5	Notification of collection of personal information
6	Use or disclosure of personal information
7	Direct marketing
8	Cross border disclosure of personal information
9	Adoption, use or disclosure of government-related identifiers
10	Quality of personal information
11	Security of personal information
12	Access to personal information
13	Correction of personal information

The APPs are legally binding principles which are the cornerstone of the privacy protection framework in the *Privacy Act 1988*. They set out standards, rights and obligations in relation to the handling, holding, accessing and correction of personal information. They are technologically neutral, principles-based law and apply to:

- most Australian government agencies;
- private sector and not-for-profit organisations with an annual turnover of more than $3 million;
- all private sector health service providers; and
- some small businesses such as businesses trading in personal information.

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable, whether or not the information or opinion is true or the information or opinion is recorded in a material form. For example, in the IoT context, information from a sensor that indicates the presence of a person in a building may be personal information if that individual is reasonably identifiable in the particular circumstances.

A business is 'trading' in personal information if it collects from or discloses to someone else, an individual's personal information for a benefit, service

---

[4] https://www.oaic.gov.au/agencies-and-organisations/guides/app-quick-reference-tool

or advantage. Where a sensor collects personal information for such a purpose, the business would generally need to comply with the APPs.

Many of the APPs will be relevant in the IoT context. Particularly relevant to new IoT projects that involve handling personal information, will be APP 1 on open and transparent management of personal information. APP 1 lays down the first step in the information lifecycle – planning and explaining how personal information will be handled before it is collected. APP entities will be better placed to meet their privacy obligations if they embed privacy protections in the design of their information handling practices. APP entities are required to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs or a registered APP code that binds the entity (APP 1.2). The intention of APP 1.2 is to ensure that privacy compliance is embedded in the design of entities' practices, procedures and systems. APP entities will be better placed to meet their privacy obligations under the *Privacy Act 1988* if they embed privacy protections in the design of their information handling practices.

The Office of the Australian Information Commissioner (OAIC) has published a range of relevant guidance on its website, www.oaic.gov.au. These include:

- Privacy Management Framework (and Privacy Management Plan Template), which provides a comprehensive approach to creating integrated and robust privacy governance systems;
- a Guide to undertaking privacy impact assessments assists entities undertaking a privacy impact assessment of a project, in order to identify the project's impact on the privacy of individuals and to develop recommendations for managing, minimising or eliminating that impact;
- a Guide to securing personal information: 'Reasonable steps' to protect personal information, which provides guidance on the reasonable steps entities are required to take under APP 11.1 to protect the personal information they hold from misuse, interference, loss and from unauthorised access, modification or disclosure. It also includes guidance for the destruction or de-identification of personal information under APP 11.2. The guide is not legally binding, but provides a detailed explanation of the reasonable steps an entity may take, with specific explanation of how this applies in the ICT context; and
- Australian Privacy Principles guidelines, which outline the mandatory requirements in the APPs, provides examples of how the APPs apply in particular circumstances, and includes suggestions for good privacy practice.

4.2 Trust Framework

Protection of personal information can be viewed in terms of a trust framework, an example of which has been proposed by the Online Trust Alliance[5]. This provides for the requirements as detailed in Table 2.

---

[5] https://otalliance.org/

TABLE 2

Online Trust Alliance IoT Framework Minimum Requirements

No	Title	Description
1	Privacy policy	The privacy policy must be readily available to review prior to product purchase, download or activation and be easily discoverable by the user. Such policies should disclose the consequences of opting in or out of policy elements.
2	Privacy policy reading	Display of the privacy policy should be optimised for the reading device to ensure maximum readability.
3	Disclosure	Manufacturers must conspicuously disclose all personally identifiable data types and attributes collected.
4	Personal data sharing	Default personal data sharing must be limited to third parties who agree to confidentiality and limitation of use.
5	Data retention	The term of data retention should be disclosed.
6	Sanitisation	The manufacturer should provide a means of sanitising devices when their use is discontinued.
7	Encryption	Personal data at rest and in motion must be encrypted using industry best standards.
8	Default password	Default passwords must be changed on first use.
9	SSL[6] best practices	All device sites must adhere to SSL best practices using industry standard testing mechanisms.
10	HTTPS	All device sites and cloud services must employ HTTPS encryption by default.
11	Penetration testing	Manufacturers must conduct penetration testing for devices, applications, and services.
12	Vulnerabilities	Manufacturers must have capabilities to remediate vulnerabilities in a prompt and reliable manner either through remote updates and/or consumer notifications.
13	Data breach	Manufacturers must have an up-to-date breach response plan and consumer safety notification plan.
14	Password recovery	Manufacturers must provide secure recovery mechanisms for passwords.
15	Pairing indicator	Devices must provide a visible indicator when they are pairing with another device.
16	Signed updates	All patches, updates, etc. need to be signed and verified.
17	Profiles	For products and services which collect personal information and are designed to be used by multiple users, manufacturers need to incorporate the ability to create and manage personal profiles and/or have parental controls.
18	Contact	Manufacturers must publish and provide a mechanism for users to contact the company regarding issues including but not limited to the loss of the device, device malfunction, device compromise, etc.
19	Transfer of ownership	Manufacturers must provide a mechanism for transfer of ownership including providing updates for consumer notices and access to documentation and support.
20	Manage privacy	The device must have controls and/or documentation enabling the consumer to set, revise, and manage privacy and security preferences including what information is transmitted via the device.

---

[6] The SSL protocol has been discontinued by NIST. The TLS v1.2 protocol should be used in preference to SSL.

21	Support	Manufacturers must publish to consumers a time frame for support after the device/app is discontinued or replaced by a newer version.
22	Disabling smart functions	Manufacturers must disclose what functions will work if smart functions are disabled or stopped.
23	Email authentication	Configure all security and privacy related email communications to adopt email authentication protocols.

Not all of the trust framework requirements will be required by all products and services, but a statement of which requirements are applicable and which are not demonstrates due diligence. Some requirements may need to be interpreted against sector-specific IoT trust requirements, and some requirements may be replaced in the IoT context, for example passwords may be reset rather than recovered.

Entities covered by the *Privacy Act 1988* will separately need to ensure that their personal information handling practices comply with the legal requirements in *Privacy Act 1988*. For example, an entity must have a privacy policy that includes certain prescribed information, must comply with the notice requirements in APP 5 and must only use and disclose personal information in certain limited circumstances set out in APPs 6 and 8.

5 SECURITY

5.1 Security Principles

Traditionally, security at the enterprise level has been considered in terms of confidentiality, availability, and integrity. These attributes are far too limited for thinking about the IoT, and a richer lexicon is required. The SABSA[7] model has been adopted by the Open Group Architecture Forum, and provides a full framework for capturing security requirements and architecting security solutions. A subset of the enterprise architecture will rely on the IoT, and IoT devices will need to meet the relevant enterprise security requirements.

There is no one best design for security in an IoT device or solution, and the selection of which device to use will in part be driven by how well its security functionality meets the security requirements identified in the enterprise security architecture.

The IoT Security Foundation[8] has defined a number of principles for IoT security which together cover many of the common requirements that vendors may come across. These are grouped into seven areas, as shown in Table 3.

TABLE 3

Areas of IoT Security Foundation Security Principles

Group	Question	Principle
1	Does the data need to be private?	Be designed with security, appropriate to the threat and device capability, in mind from the outset.
		Offer appropriate protection for all potential attack surfaces (e.g. device, network, server, cloud etc.)
		Inform users what private data is required in order for the device to function.
		Allow users and security products to review sensitive data to verify the device is maintaining privacy.
		Ensure identifiers are removed or anonymised where necessary.
		Manage encryption keys securely.
2	Does the data need to be trusted?	Integrity of software is verified (e.g. secure boot).
		The device or system uses a hardware-rooted trust chain.
		Authentication and integrity protection are applied to data.
		Compromised or malfunctioning devices can be identified and revoked.

---

[7] Sherwood Applied Business Security Architecture, www.sabsa.org/white_paper

[8] https://iotsecurityfoundation.org/

		Data is isolated from other systems or services where applicable.
		System testing and calibration ensures data is handled correctly.
		Device metadata is trusted and verifiable.
		Re-using existing good security architectures rather than designing brand new ones.
3	Is the safe and/or timely arrival of data important?	Data is accurately time-stamped.
		Integrity of data in the device, server and other parts of the system is designed in from outset.
		Devices should provide failure handling and status monitoring to meet availability requirements.
		Carriers and device managers can identify safety and timeliness needs in a secure, trusted fashion.
		Any reliance on other systems or devices for availability is clearly detailed to the user.
		Devices should identify themselves to a network using a secure identifier.
		Be clear what functionality the device is offering and its intended use. Make users aware of any restrictions or limitations.
4	Is it necessary to restrict access to, or control of, the device?	Defences against hacking are designed in from the outset.
		Development processes incorporate secure coding standards, penetration testing etc.
		Service management occurs over an authenticated channel.
5	Is it necessary to update software on the device?	The vendor update and management process follows best security practice.
		Only authenticated sources are able to provide security updates or patches.
		Users and managers are easily able to see a device's patching update status.
6	Will ownership of the device need to be managed or transferred in a secure manner?	Provide a secure method to transfer ownership of the device to another user.
		Be clear which system components (devices, data, network etc.) are owned by the user.
		Ensure that change of ownership does not impact security updates.
7	Does the data need to be audited?	Managed access to IoT data (for example at a local hub).
		Policy controls to disable unwanted features.

The questions which form the groups in the IoT Security Foundation Principles provide a good start point or IoT security and should be considered at the outset of any IoT development and deployment projects, and the specific principles associated with them applied where relevant. In the longer term, these principles may form the foundation from which sector specific IoT security profiles and controls can be developed.

5.2 Application Layer

The application layer is a rapidly evolving space in IoT, with vendors such as IBM with its Watson for IoT service, Microsoft with Azure IoT, and Amazon with AWS IoT offering full cloud based IoT application and IoT management solutions.

The application layer is solution specific. It can be implemented simply as a dashboard, may involve a web portal to access messages, may use an API through which messages may be pushed or pulled, or may be a fully contained application. The application layer may contain a storage repository in which messages are kept temporarily or as a longer term archive. While the underlying infrastructure may provide security features, the application layer may also extend out to devices to deliver full end-to-end security.

There are two popular application level protocols: the Constrained Application Protocol (CoAP) and the Message Queue Telemetry Transport (MQTT). CoAP is a one-to-one protocol, wheras MQTT supports a one-to-many architecture.

5.2.1 Constrained Application Protocol

RFC 7252: Constrained Application Protocol (CoAP) has become widely adopted as a low cost method of communications between devices and their applications.

CoAP uses the Datagram Transport-Layer Security (DTLS)[9] to secure CoAP messages – this is a variant of TLS which can accommodate the unreliable nature of UDP communications. It has a small number of mandatory minimal configurations defined, as appropriate for constrained environments. This provides support for Confidentiality, Authentication, Integrity, Non-Repudiation and protection against Replay Attacks.

CoAP has four security modes to support key management: NoSec, PreSharedKey, RawPublicKey, and Certificates. The cipher suites used in these specifications are shown in Table 4.

---

[9] RFC 6347: Datagram Transport Layer Security v1.2

TABLE 4

CoAP Cipher Suites

Mode	Cipher Suite
NoSec	-
PreSharedKey	TLS_PSK_WITH_AES_128_CCM_8 and Elliptic Curve Cryptographic
RawPublicKey	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 and Elliptic Curve Cryptographic
Certificate	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 and Elliptic Curve Cryptographic

The DTLS handshake for authentication and key agreement can pose a significant impact on the resources of constrained devices, particularly with the requirement for elliptic curve cryptography. Investigations continue into optimisations of DTLS in IoT environments and the incorporation of elliptic curve cryptography in hardware. A new protocol, DTLS+, has been proposed as a standard lightweight variant.

Research is underway to consider the employment of alternative approaches to secure CoAP communications, in particular the employment of object security rather than transport layer security. This may be achieved by integrating security into the CoAP protocol itself using new security options. This approach enables granular security on a per-message basis, and supports the secure transversal of different domains and the usage of multiple authentication mechanisms.

5.2.2 Message Queue Telemetry Transport

ISO/IEC 20922: Message Queue Telemetry Transport (MQTT) is a publish/subscribe messaging protocol designed for lightweight machine-to-machine communications. It was originally developed by IBM and is now an open ISO standard.

MQTT has a client/server model, where every sensor is a client and connects to a server, known as a broker, over TCP. It is message oriented, where every message is a discrete chunk of data, opaque to the broker.

A message is 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. Topics are arranged in a hierarchical manner and can be accessed individually or as a group using wildcards requests.

MQTT brokers provide authentication using username/password credentials, and confidentiality and privacy through the use of encrypted SSL/TLS protocols.

5.3 IoT Management Layer

The management layer of the IoT reference architecture is where all the activity occurs to enable the devices to interact with the applications successfully. This is where registration of devices occurs. It's also the point of data flow management, and may be the end point for receiving device data, storing it in a management layer repository for applications to access.

Device configuration and modelling may take place at the management layer, as well as security control for issuing and validating certificates.

In traditional networks, there are separate data, control, and management planes, as described in ITU X.805[10]. Research on applying X.805 in the IoT context has been carried out by Raheem et al[11].

5.4 Gateway and Access Layer

The purpose of the gateway and access layer is to provide an upstream connection for the proximity network and pass the data to the access network, typically an IP based backhaul, and vice versa. The requirements of a gateway go beyond being just a firewall. As this is the closest point to the devices, the gateway may also be used as the point of device access control, determining whether the device can connect using its proximity communications. Beyond that, a network gateway serves many needs, including management of traffic and meeting service level agreements or regulatory requirements, and is itself a critical device that must be protected.

In the WiFi scenario, the device will typically authenticate by presenting the network key through the WPA/WPA2 security protocol. In a LoRa network, the device key will have been prepositioned into the network server and the network key will either be pre-positioned also by the service provider or may be negotiated through over the air keying. For NB-IoT, an inserted or embedded sim module will provide authentication to the network.

Communications from the gateway through the access network to the application will be deployment specific. Standard IP protocols such as IPSec are often used to achieve integrity and confidentiality on the access network.

The security of the gateway is a critical part of any IoT end-to-end solution, as it is exposed both in the proximity network to rogue devices and in the access network to internet delivered attacks. ETSI TR 103421: Network Gateway Cyber Defence provides a good overview and set of recommendations concerning cyber defence capabilities at network gateways.

---

[10] https://www.itu.int/rec/T-REC-X.805-200310-I/en

[11] Supporting Communications in the IoTs using the Location/Id Split Protocol: A Security Analysis, Raheem et a, Middlesex University, December 2013

5.5 Proximity Layer

One of the fundamental aspects of the IoT is the manner low-powered devices self-organise and share information (route and data information) among themselves. Even though these sensors are energy constrained, they need to store and process data, dynamically connect to the network, and possibly interoperate with other devices. Some of the devices may act as internal or border routers.

Some proximity network protocols may connect devices directly to the access gateway, while some may connect via other devices. In the latter case, for a route to be established, route information may be transmitted from node to node (multi-hopping) until the desired destination is found. Throughout the route maintenance phase, nodes can add, delete or needlessly delay the transmission of control information (selfish or misbehaving nodes). It is during route discovery or forwarding that malicious nodes can attack. For example, a node can introduce a routing table overflow attack by transmitting a large amount of false route information to its neighbours in a manner that will cause its neighbour's routing table to overflow or be poisoned. A malicious node can advertise a false route with the smallest hop count and with the latest sequence number, hence other nodes, seeing this as a route update, quickly invalidate their old route to innocently accept the new false route. IoT networks require adequate security to enable seamless operation and for users to build confidence. A full set of routing protocol attacks has been identified by David Airehrour, Jairo Gutierrez and Sayan Kumar Ray[12].

Secure routing plays an essential role in the safe and seamless functioning of the entire network, yet finding a universal solution applicable to all the routing attacks is proving to be very difficult. Protocol designers must ensure protection from the known attacks, while minimising the impact on sensor and network performance. There are five key issues to address: secure route establishment, automatic secure recovery and stabilisation, malicious node detection, lightweight or hardware-supported computations, and node location privacy.

5.5.1 IEEE 802.15.4

IEEE 802.15.4 defines the physical layer and media access control for low-rate wireless personal area networks, or LR-WPAN. This is the standard used in personal and industrial applications where there are many sensors and a low-cost, low-speed network approach can be used in the proximity segment. It operates at about 250Kb/s at up to 10 metres. Other standards such as WirelessHART, DigiMesh, ISA100.11a also exist as low power physical layer standards. ZigBee is built on IEEE 802.15.4, as is 6LoWPAN.

At the higher data rates, Ethernet, WiFi and WiMax are well known physical layer standards. In the cellular space, the current 2G-4G standards are deployed and 5G is emerging as a real option for IoT use. At the same time, Narrowband IOT (NB-IOT) has been

---

[12] *Secure routing for Internet of Things: A survey*. Airehrour, Gutierrez and Ray, Journal of Network and Computer Applications, (66) 2016

developed and is in trials as a technology that can co-exist with existing cellular networks to provide IOT solutions now.

IEEE 802.15.4 does not require security, but it can be applied to enable device authentication, payload protection, and message replay protection. An access control list is used to specify the security configuration based on the destination address, and from this the symmetric cryptography for payload protection. Where security is specified, an auxiliary security header will be used. The cryptographic security modes that can be employed in an IEEE 802.15.4 system are as shown in Table 5.

The Advanced Encryption Standard counter mode (AES-CTR) can be used where confidentiality of the link layer encryption only is required, with message integrity being handled at a higher level. However, there are some concerns regarding this mode's susceptibility to denial of service attacks through use of forged packets, and its use is discouraged.

TABLE 5

IEEE 802.15.4 Security Modes

Mode	Description
No security	-
AES-CBC-MAC-32	Data is not encrypted, uses a 32-bit integrity code.
AES-CBC-MAC-64	Data is not encrypted, uses a 64-bit integrity code.
AES-CBC-MAC-128	Data is not encrypted, uses a 128-bit integrity code.
AES-CTR	Data is encrypted, no integrity code.
AES-CCM-32	Data is encrypted, uses a 32-bit integrity code.
AES-CCM-64	Data is encrypted, uses a 64-bit integrity code.
AES-CCM-128	Data is encrypted, uses a 128-bit integrity code.

The CCM mode combines the counter and CBC modes of operation to provide confidentiality, authenticity and integrity at the link layer.

In the mobile space, NB-IOT utilises the security and privacy features that already exist in mobile networks, such as support for user identity confidentiality, entity authentication, confidentiality, data integrity, and device identification.

LoRaWAN incorporates the ability to authenticate the node in the network and to protect the payload using AES encryption. It uses two keys, one at the network layer for message integrity and one at the application layer for confidentiality. LoRaWAN does not allow for the device key to be changed, but does create a unique session key for payload encryption when the device joins a network. AES counter mode (AES-CTR) for payload encryption.

Other protocols at the physical layer also use encryption mechanisms: Bluetooth LE/Smart uses AES, and ethernet can be secured by MACsec (IEEE 802.1AE).

It should be noted that security at the physical and media access control layer requires a certain amount of computing power and this may not be available to very constrained devices, for example in devices such as micro/nano-technology enabled sensors. Energy efficiency and sufficiency for IoT sensors is an active research area. Where possible, symmetric cryptography should be implemented in hardware level in order to achieve acceptable performance.

5.5.2 6LoWPAN

6LoWPAN environments route traffic using the Routing Protocol for Low-power and Lossy Networks (RPL) protocol. Rather than providing a generic approach to routing, RPL provides a framework that is adaptable to the requirements of particular classes of applications. This suits the richer attribute approach to security.

In the most typical setting various 6LoWPAN nodes are connected through multi-hop paths to a small set of root devices responsible for data collection and coordination. RPL defines secure versions of the various routing control messages, as well as three basic security modes: unsecured, pre-installed, and authenticated and adopts AES/CCM as the basis to support security. A secure RPL control message includes a security field after the ICMPv6 message header. The information in the security field indicates the level of security and the cryptographic algorithms employed to process security for the message.

Incorporation of a timestamp and a nonce in a 6LoWPAN message can also protect against fragmentation attacks. Hash chains and purging of messages from suspicious senders can also help protect replay attacks between sensors and 6LoWPAN devices.

6LoWPAN inherits its security model from IEEE 802.15.4. No security mechanisms are currently defined in the context of the 6LoWPAN adaptation layer. RFC 4919, however, discusses the possibility of using IPSec at the network layer, although this may be too processing intensive for smaller IoT devices.

5.5.3 ZigBee

ZigBee specifies an IEEE 802.15.4-based set of high-level communication protocols used to create personal area networks using low-power digital radios. It is intended to be low power, lower cost and simpler to implement than Bluetooth and WiFi. It uses 128-bit encryption keys and is typically used where the end-point device requires long battery life and secure networking. ZigBee devices have low latency and low data rates.

5.5.4 LoRaWAN

LoRaWAN is a Low Power Wide Area Network (LPWAN) specification intended for wireless devices which are battery powered, and provides secure bi-directional communication, mobility and localisation services. LoRaWAN is typically architected as a star-of-stars topology in which a gateway acts as a transparent bridge relaying messages between end-devices and a back-end server.

Communication between end-devices and gateways is spread spectrum, and devices are not IP addressable, both of which provide significant security advantages.

LoRaWAN has comprehensive and well-designed security at both the network and application layer. It uses AES128 as its encryption algorithm, with the base encryption key referred to as the AppKey. The AppKey is stored in a network server, and also stored in the device.

This is used to generate two working keys:

- a unique 128-bit network key to ensure security at the network level (NwkSKey); and
- a unique 128-bit application key to ensure end-to-end security at the application level (AppSKey)

Encryption uses the AES-CCM (Counter with CBC-MAC) mode of operation which provides counter-based integrity.

The activation of a LoRa service depends upon the service provider, however the protocol allows for both Activation By Personalisation (ABP) where the service provider provides the session keys, and Over The Air Activation (OTAA) where these are dynamically created.

5.5.5 Sigfox

SIGFOX is a cellular style system that enables remote devices to connect using ultra-narrow band, UNB technology. It is aimed at low cost machine-to-machine applications where wide area coverage is required and cellular is too costly. The overall SIGFOX network topology has been designed to provide a scalable, high-capacity network, with very low energy consumption, while maintaining a simple and easy to rollout star-based cell infrastructure. SIGFOX allows up to 140 messages per device per day, with the message payload of 12 bytes and a wireless throughput of up to 100 bits per second and is ultra-low power. The SIGFOX network is radio-based using unlicensed frequencies. Data is not delivered directly to the user from the radio system. When data is received from the radio network, a message is sent to user’s server or an aggregator which in turn will dispatch it to the user.

5.5.6 LTE-M and NB-IoT

Another cellular technology being deployed for IoT is LTE Cat-M1, or LTE-M, the enhanced fourth generation long term evolution of the 3G GSM/CDMA cellular technology. LTE is already used in 4G cellular services, so it does not need a completely new infrastructure and can be deployed as a software upgrade to an existing 4G services. LTE-M solutions operate at around 1Mb/s and can support easy handoff for mobile devices in the transportation sector.

LTE solutions can also be deployed in an enterprise form, operating as a radio network with backhaul to an IoT management platform.

The 3GPP began work on a new variant of LTE, LTE Cat-M2 or NB-IoT, in September 2015, and initial results of this work have been strongly supported by Industry. NB-IoT operates at about 200Kb/s. By December 2015, the first pre-commercialisation trial was successfully completed in Spain by Vodafone, Huawei, Neul and U-blox and NB-IoT is now being deployed by carriers.

NB-IoT is designed as a resilient network which is power-efficient and has deep in-building penetration, wide area ubiquitous coverage, and can manage high volumes of small data packets. It includes network access security, network domain security, user domain security, and application domain security. Three algorithms exist to protect the air interface: the SNOW stream cipher designed by cryptographers at Lund University in Sweden; AES; and the ZUC stream cipher designed by the Chinese Academy of Sciences. EPS-AKA is used for authentication and key agreement. Backhaul may be physically protected, or protected by IPSEC and may include a Security Gateway (SEG) to provide protection for the Evolved Packet Core (EPC). It is a sim-based deployment ensures full hardware-based, tamper-proof cryptography.

3GPP has published guidelines for the LTE security architecture in its technical standard TS33.401, and NIST has provide guidelines on LTE security in SP800-187.

5.5.7 5G

3GPP is currently developing standards on the next cellular network technology, known as 5G. Pilot trials of 5G have been successfully completed, and the first production deployments with IoT slices are expected by the end of 2018. A technical report on 5G security has been released by 3GPP as TR89.331.

5.6 Device Layer Security

5.6.1 Security Threats

Security threats to hardware and embedded systems are a well-known concern. Early indications of the problem emerged in the 1990s with security assessments of smart cards, where cryptographic keys have been able to be extracted[13]. More recent revelations suggest that hardware may not only incorporate flaws but could be a vector for malicious attack.

Defending against these threats requires an approach to security testing of hardware components particularly where the product depends upon hardware based random number generators, encrypted bit streams, key storage elements, secured flash

---

[13] http://www.cl.cam.ac.uk/~mgk25/tamper2.pdf

memory, anti-tamper features and other controls. Unless these controls are trustworthy, higher level security controls will be compromised.

A key element in hardware security is the supply chain, and the opportunity and motivation for actors in the supply chain to embed backdoors or malicious circuits at the hardware level. Research related to hardware injected Trojan circuits[14] has identified some solutions for detecting hardware Trojans.

Testing tools are increasingly starting to offer the capability to bridge directly to hardware, for example the latest release of the Metasploit framework includes the ability to link tests directly to hardware[15]. Early applications include automotive systems such as CANBus and industrial SCADA components.

5.6.2 Trusted Execution

Hardware provides a solution to some of the problems of IoT security, for example in having a hardware-based root of trust. ARM introduced its TrustZone architecture into its Cortex processors to provide system wide hardware isolation for trusted software. This has enabled the deployment of what is commonly referred to as the Trusted Execution Environment (TEE – or QSEE on Qualcomm chips).

At this stage the TEE is typically used for vendor supplied secure storage mechanisms, trusted keyboard entry, and cryptography. The TEE is not yet available for consumers to deploy secure applications, although some vendors do enable 3rd party applications to be registered for secure operation.

5.6.3 Securing IoT Devices

More information on the approaches that can be taken to secure and certify IoT devices is provided in Section 8.

---

[14] Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solution. Koley S et al, http://ieeexplore.ieee.org/document/7518284/

[15] http://www.globenewswire.com/news-release/2017/02/02/913426/0/en/Rapid7-Enables-IoT-Hardware-Security-Testing-with-Metasploit.html

6 DOMAIN VIEWPOINTS

Some domain specific guidance has been provided in the consumer, industrial, healthcare, smart cities, and automotive domains.

6.1 Consumer Domain

The IoT Security Foundation has developed a foundation of guidance on IoT security, with the first release focusing primarily on the consumer domestic – or home automation – domain. This includes a set of 33 principles for IoT security, in seven groups, as described in section 5.1.

In addition, the IoT Security Foundation has proposed a compliance regime for demonstrating security in IoT devices and systems. This classes an IoT product into one of five classes – Class 0 to Class 4 - as shown in Table 6.

TABLE 6

IoT Security Foundation Classes

Class	Impact of Compromise	Confidentiality	Integrity	Availability
0	Minimal	Basic	Basic	Basic
1	Limited impact on an individual or organisation	Basic	Medium	Medium
2	Significant impact on one or more individuals or organisations	Medium	Medium	High
3	Significant impact to sensitive data	High	Medium	High
4	Personal injury or damage to critical infrastructure	High	High	High

While there is no governance framework in which to apply a compliance regime, the IoT Security Foundation envisages that an audit process could lead to use of a "Trust Mark" as a qualified public symbol of conformance to best practice.

6.2 Industrial Domain

While many uses of the IoT will involve collection of data from sensors, IoT devices are also remotely activated and configured through central decision making processes. The controlled devices may be as simple as a light switch, or as complex and expensive as aircraft control systems, nuclear reactors and mining systems. Many older systems continue to use SCADA or programmable logic controls (PLCs). SCADA is well known for security weaknesses, with the Stuxnet worm being the most notorious example of a successful and extremely damaging attack.

IoT control systems vary from the low-scale (a home lighting system) to the critical (power supplies for a large city). There are as yet no comprehensive guidelines spanning this range. Some guidelines, predominantly from the US, exist in specific areas such as SmartGrid.

The Industrial Internet Consortium (IIC) has published security guidance[16] on security in the industrial sector. The IIC see the industrial internet of things as being the convergence of information and operational technology across the internet, with a focus on the traditional information security aspects of confidentiality, availability and integrity but also embracing privacy, safety, reliability and resilience to deliver a concept of trustworthiness for industrial IoT.

The approach taken to delivering trustworthiness in the industrial IoT is that of risk management, taking into account the OWASP Top Ten IoT threats, and using Microsoft's STRIDE model for evaluating threats and modelling risk. The concept of trustworthiness is applied from the component design through system building to operational use. This requires a clear identification of security requirements and the ability to trace how these requirements are being met through the supply chain to the end user. This can be achieved using an applied business security architectural approach such as that provided by the SABSA framework.

The functional viewpoint of the industrial IoT security framework comprises six interacting building blocks. This starts with the two basic blocks of security policy model and data protection. There are then four core security blocks of endpoint protection, communications & connectivity protection, security monitoring and analysis, and security configuration & management.

6.3 Healthcare Domain

The US Food and Drug Administration has produced guidelines for the security of medical devices and systems[17]. They consider both pre-market considerations to determine "recommendations for manufacturers to address cybersecurity during the design and development of the medical device" as well as post-market support: "... it is essential that manufacturers implement comprehensive cybersecurity risk management programs and documentation."[18] It could reasonably be expected that failure to do these will not only lead to loss of life, but also to expensive litigation.

A security architecture for healthcare[19] has been proposed by researchers at CISCO Systems, in which they identify not only data and communications as attack surfaces but also the physical device. The paper also identifies the relevant standards activities.

---

[16] Industrial Internet of Things: Volume G4 Security Framework IIC:PUB:G4:V1.0:PB:20160919

[17] U.S. Department of Health and Human Services Postmarket Management of Cybersecurity in Medical Devices http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

[18] Homeland Security, : https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems

[19] http://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_133.pdf

6.4 Smart Cities Domain

Many current smart city deployments are based on custom systems that are not interoperable, portable across cities, extensible or cost-effective. In addition, the standards community has yet to converge on a common language and architecture.

To address this problem, the US National Institute of Standards and Technology has convened a working group[20] to develop a common IoT-enabled smart city framework. This work is at an early stage of development, but it is likely to have a significant impact on how smart cities apply IoT.

6.5 Automotive Domain

Automobile systems use the controller area network (CAN) bus to interact with almost all systems. Brakes and steering are particular subsystems which introduce rigorous safety requirements. Like SCADA this is an old technology with little regard for security. There is a clear entry point by the debugging systems used by automotive repair shops. Telematics systems have been attacked, for example the demonstration at the 2015 Blackhat conference of taking control of a Jeep Cherokee travelling at 70mph.

While alternatives to CANbus are appearing, replacement will be a long-term objective. In the meantime, advice by experts such as NXP's security architect, van Roermund is[21]

- Isolating in-vehicle electronics from external interfaces, with firewalls;
- Applying strict access control to only allow known/trusted entities (partial) access to in-vehicle systems;
- Further adapting in-vehicle networks, in which systems with similar criticality are clustered in separate networks, to better isolate safety-critical systems from others;
- Protecting messages exchanged over in-vehicle networks using cryptography (authentication, and maybe also encryption);
- Using intrusion detection/prevention systems (IPS/IDS) to detect and possibly counter attacks; and
- Protecting the ECUs (microcontrollers and their software) themselves through secure boot, secure update, and other measures.

Almost every automotive system now comprises a sensor network and an actuator network. Many issues arising from sensor data can be managed at higher levels, but these higher levels and connectivity can lead to serious problems when they result in effects at the actuator level. While there are guidelines in many important cases, the scope of the IoT at present rules out generic solutions. Nevertheless, it is critical that attention be paid to these issues.

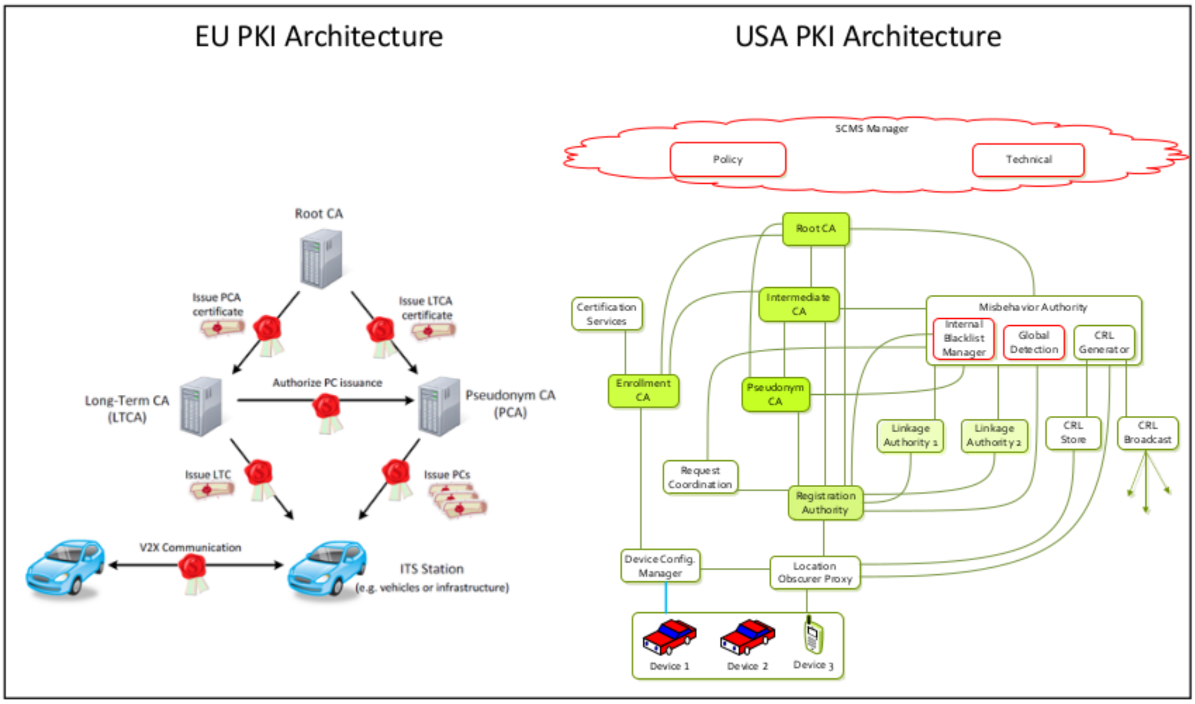
An active research area is Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communications. Although these can offer huge safety benefits, there are also substantial security and privacy concerns. Both the US and the European Union are working towards appropriate standards.

---

[20] https://pages.nist.gov/smartcitiesarchitecture/

[21] Junko Yoshida CAN Bus Can Be Encrypted, Says Trillium http://www.eetimes.com/document.asp?doc_id=1328081&page_number=3

Australia has adopted the C-ITS standard in the 5.9Ghz band[22], aligned with the EU, based on a number of ETSI TS 102 standards. The US has a different standard based on IEEE 1609.2.



Source: From a presentation prepared by Dr. André Weimerskirch of the University of Michigan Transportation Research Institute (UMTRI) on 27 March 2014.

A primary difference is that the EU model applies security at the network layer while the US model applies it at the application layer. The US model has better anonymity, with improved privacy compared to the EU one. A further complication is that the Japanese and Korean standards do not align with either the US or EU standards, making import of cars (particularly used ones) from these countries problematic.

There are two principal sub-categories of V2X: Vehicle to Infrastructure (V2I) and Vehicle to Pedestrian (V2P). In general, V2I can be managed by the above standards although a failure of security can have more wide-reaching consequences. V2P is more complex as pedestrians cannot be guaranteed to carry appropriate devices and pedestrian detection systems may be needed. There do not appear to be specific cyber security related issues, but of course a failure in the vehicle’s security is more likely to be fatal to the pedestrian.

Relevant organisations in Australia include Austroads, Intelligent Transport Systems Australia (ITS Australia) and the recently established Cooperative Research Centre, iMOVE.

---

[22] Cooperative Intelligent Transport Systems (C-ITS) Standards Assessment by David Green, Dr Charles Karl and Freek Faber, Austroads Ltd

6.6 Agriculture Domain

Little attention has been given to the security of IoT products used in agriculture. However the American Farm Bureau Federation has drafted a set of Privacy and Security Principles[23] relating to the use of smart technology on farms, with a focus of enabling secure central repositories of precision agriculture and farm data. These have been incorporated in the *AG Transparency Evaluator*, a checklist approach to the application of the principles.

The principles are shown in Table 7.

It is likely there will be some overlap with the automotive sector as smart farm vehicles and drones gain widespread adoption in the agricultural sector.

TABLE 7
Privacy and Security Principles for Smart Agricultural Technology

Principle	Description
Education	The industry should work to develop programs to create educated customers who understand their rights and responsibilities. Contracts should use using simple, easy to understand language.
Ownership	Farmers set the agreements on data use and sharing with the other stakeholders with an economic interest, such as the tenant, landowner, cooperative, owner of the precision agriculture system hardware, and/or technology provider.
Collection, Access and Control	The collection, access and use of farm data by technology providers should be granted only with the affirmative and explicit consent of the farmer through contract agreements.
Notice	Farmers must be notified that their data is being collected and about how the farm data will be disclosed and used. This notice must be provided in an easily located and readily accessible format.
Transparency and Consistency	Technology providers should notify farmers about the purposes for which they collect and use farm data, and provide contacts for inquiries or complaints. They should explicitly state the types of third parties to which they disclose the data and options for limiting its use and disclosure. The technology provider's principles, policies and practices should be transparent and fully consistent with the terms and conditions in their contracts. Customer contract should not be changed without agreement.
Choice	Technology providers should explain the effects and abilities of a farmer's decision to opt in, opt out or disable the availability of services and features offered by the technology and services. If multiple options are offered, farmers should be able to choose some, all, or none of the options offered.
Portability	Within the context of the agreement and retention policy, farmers should be able to retrieve their data for storage or use in other systems, with the exception of the data that has been made anonymous or aggregated and is no longer specifically identifiable.
Terms and Definitions	Farmers should know the third parties, partners, business partners, or affiliates of their technology provider which have access to their data. Clear language should be used in terms, conditions and agreements.

---

[23] http://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data

Disclosure, Use and Sale Limitation	Technology providers must not sell and/or disclose non-aggregated farm data to a third party without first securing a legally binding commitment to be bound by the same terms and conditions that are in place with the farmer. Farmers must be notified if such a sale is going to take place and have the option to opt out or have their data removed prior to that sale.
Data Retention and Availability	The technology provider should provide for the removal, secure destruction and return of original farm data from the farmer's account upon the request of the farmer or after a pre-agreed period of time. Personally identifiable data retention, availability and disposal policies should be documented.
Contract Termination	Farmers should be allowed to discontinue a service or halt the collection of data at any time subject to appropriate ongoing obligations. Procedures for termination of services should be clearly defined in the contract.
Unlawful or Anti-Competitive Activities	Technology providers should not use the data for unlawful or anti-competitive activities, such as a prohibition on the use of farm data by the ATP to speculate in commodity markets.
Liability & Security Safeguards	Technology providers should clearly define terms of liability. Farm data should be protected with reasonable security safeguards against risks such as loss or unauthorised access, destruction, use, modification or disclosure. Polices for notification and response in the event of a breach should be established.

6.7 Critical Infrastructure Domain

The US Government is developing principles and strategies for managing risk in the critical infrastructure domain[24]. IoT security strategies in this domain will have to align with the US Government principles and strategies. These are summarised in Figure 3.

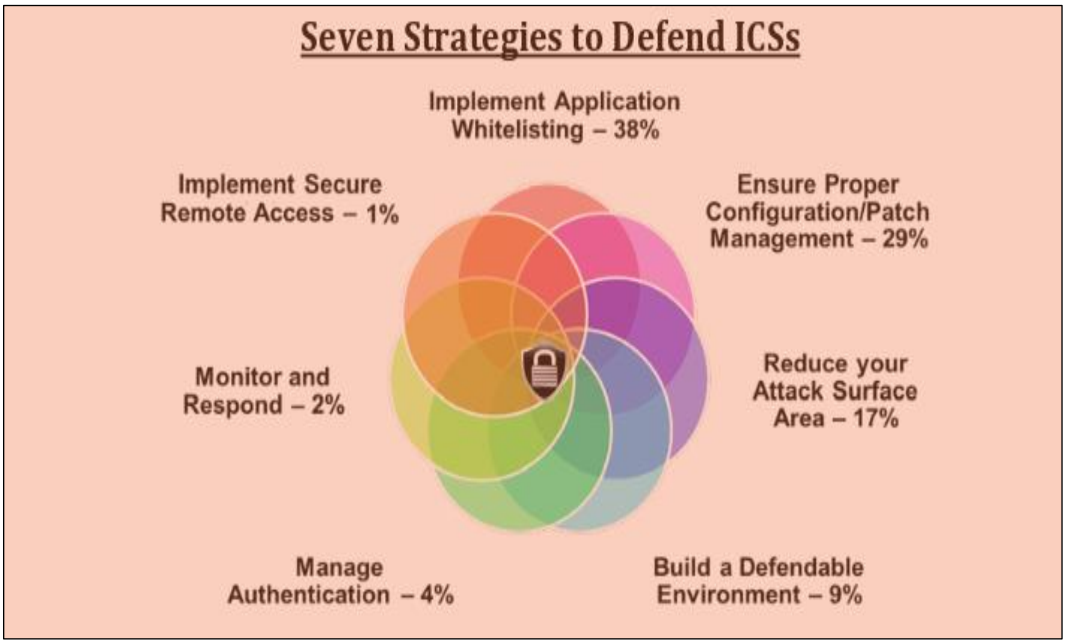


FIGURE 3

ICS-CERT Incidents Mitigated by Strategy[25]

---

[24] Homeland Security, : https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems

[25] https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems

7 RESILIENCE AND SURVIVABILITY

7.1 Resilience

The resiliency of a system can be defined in general terms as its capability to resist external disruption and internal failures, to recover and gain stability, and even to adapt its structure and behaviour to constant change.

Laprie[26] has defined resilience as *The persistence of dependability when facing changes* and provides a view of how resilience, dependability and security interact (Figure 4).

FIGURE 4

Resilience and Other Attributes

The International Telecommunications Union considers the two key attributes of reliability and availability to be characteristic of traditional networks, fixed and wireless, as well as the emerging IP-based Next Generation Networks (NGNs).

RFC 6568 provides some early consideration of the possible approaches to resilience in the light of the characteristics and constraints of wireless sensing devices, and discusses threats due to the physical exposure of such devices which may pose serious demands for resiliency and survivability.

Much more work has been carried out on resilience since Laprie published his model. To be resilient, a system must also be fault tolerant, dependable, and trustable. Beyond this, diversity, adaptation, correlation, causation, and renewal are the most promising directions of research into resilience of complex systems.

The IoT will be so large as to be difficult to monitor effectively and control efficiently, and consequently the resilience of any IoT system will be important. The use of multi-homing on network devices is a common networking strategy to increase the overall resilience of a network. Such a

---

[26] "From Dependability to Resilience", IEEE/IFIP 2008

strategy can usefully be applied to IoT devices, and can be seen in devices which can connect to multiple gateways and peer devices.

7.1.1 Reliability

Interpreting reliability is more critical for IoT than for traditional IT services. An attribute which can be critical for some IoT systems is latency – the delays that are experienced as traffic travels through the various network links from the IoT device to the destination. This is addressed by telecommunications providers in systems such as VOIP through providing a fit-for-purpose class of service. NB-IoT is starting to underpin new telco class of service offerings from the major telco providers.

7.1.2 Availability

Availability can be broken down into three key attributes: built in whole-of-life power sources, the ability to access the internet through the IoT gateway, and the availability of transit paths from the gateway to whatever destination is required either on the fixed line internet or linked through mobile services to a handset data service.

Long-life devices are made possible through low power design, including the use of low power near connectivity, and low power wide area (LPWAN[27]) communications. Some solutions for energy harvesting are also appearing, such as WSN-HEAP[28], which enable greatly extended sensor lifetime. WSN-HEAP sensors can use environmental energy such as light, vibration, and heat using nano-collectors. Cellular networks and standard WiFi require significant power and are not always suitable for sensors. The IEEE has developed a standard 802.15.4 as a low power protocol. A promising solution for low power connectivity based on IEEE 802.15.4 is 6LoWPAN, as adopted by ARM and Cisco. In the wide area, NB-IoT is designed to be a low power requirement protocol to support devices with lifetimes of 10 years or more.

Access to the wide area IoT transit service is usually through a near-area gateway device (also known as an edge node) such as a home hub, although wearable devices may look for direct connectivity with cellular services for mobility.

There are five key issues with the first-hop, i.e. the device to near-area gateway, access:

- signalling, to ensure that data is delivered and meets performance criteria;
- security, especially authorisation, encryption, and open port protection;
- presence detection, to know when an IoT device loses connectivity;

---

[27] https://en.wikipedia.org/wiki/LPWAN

[28] Seah & Chan, Challenges in Protocol Design for Wireless Sensor Networks Powered by Ambient Energy Harvesting, IEEE, Wireless Vitae 2009

- scalability, ensuring bandwidth is available as massive scaling of the IoT takes place; and
- protocol, whether the device connects using IPv4 and uses NAT across the gateway, or connects natively in IPv6 (6LoWPAN carries an IPv6 address and offers internet connectivity without significant additional overhead).

NB-IoT is different to other protocols as it is designed to connect directly with the cellular network and will avoid some of the device to gateway issues.

Where the service involves cloud applications, as was the case with the Wink smart home devices[29], any accidental or scheduled maintenance outage will result in availability issues. Wide-area transit path availability is a requirement that needs to be specified in the SLA for the service, with multiple diverse paths and media designed-in for critical IoT services.

7.2 Survivability

Survivability is not currently a significant consideration for telecommunications and cloud service providers, but will be increasingly important as the IoT places more always-on, real-time demands on them. A class of IoT systems known as Critical IoT is emerging and will need ultra-reliable – approaching survivable – services to be deployed. These include remote health care and surgery, smart grid automation, traffic safety and control, and industrial control. While product developers can do little to ensure survivability of the end-to-end service, these needs should be identified at the design stage and the risks around survivability taken into account in service planning.

One approach to achieving network survivability is to focus on the ongoing operation of lower layer connectivity, in the event of loss or degradation of one or more nodes or links, through static or dynamic link redundancy. Survivability in this context is not applied to higher level services. In the military and critical infrastructure fields, it is common to consider survivability as it applies to the mission or service and, hence, look to end-to-end survivability at all levels. Key to this is establishing the concept of essential services, and ensuring that these are protected at the cost when necessary of non-essential services.

Survivability is not just an issue of maintaining operational status. A service which has an operational core network and set of services is of little use if it cannot be accessed by those users who have a critical part of the business process to perform. For instance, a supervisory control and data acquisition (SCADA) system allowing remote control of a nuclear plant needs to be operational at all times, allowing plant relays, switches, and monitoring sensors to take commands and return status information. However, having the central control room and the remote termination unit both fully available is of little use if users lose network access.

---

[29] www.wired.com/2015/04/smart-home-headaches/

Taylor et al[30] have proposed the Risk Analysis and Probabilistic Survivability Assessment (RAPSA) methodology for designing elements of the critical infrastructure. RAPSA emerged from examining an increasingly significant threat of cyber terrorism to the SCADA systems used to control the electrical infrastructure. The conclusions from this work hold also for malicious or inadvertent damage from malware, external and internal hacking, or system failures. The use of public distributed networks such as the internet makes it impossible to harden the complete end-to-end system, and there is a real possibility that at least part of the system is susceptible to damage through cyber-attack. This is the case also with IoT.

RAPSA has evolved from two separate disciplines – survivability systems analysis and in particular the Survivable Network Assessment (SNA) process[31] with its probabilistic risk assessments. It considers the issues associated with maintaining survivability in unbounded and hostile networks such as the internet, where attacks are frequent and may be zero day – i.e. hitherto unknown and with no countermeasures (e.g. a patch) available. When under attack, even if the attack is successful, the survivable network must maintain its essential services and recover full capability in reasonable time.

---

[30] Taylor C, Krings A., and Alves-Foss J. Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening. *Proceedings of ACM Workshop on Scientific Aspects of Cyber Terrorism.* (Washington DC), November 2002.

[31] Mead NR, Ellison RJ, Linger RC, Longstaff T, McHugh J. Survivable Network Analysis Method. *Technical Report CMU/SEI-2000-TR-013,* Carnegie-Mellon University, 2000

8 DEVELOPING IOT PRODUCTS AND SERVICES

The development environment for IoT spans many programming languages, operating systems, and networks. Hardware is specialised. The attack surface for IoT is enormous, there are no accepted models for security across IoT, and there is a risk that security may become an afterthought due to the demands of getting products to market[32]. In addition, as in the case of industrial control systems, security is only just becoming recognised as a requirement.

8.1 Identifying Security Needs

Security is an important consideration when designing an IoT product or system, and a secure IoT framework should be adopted to ensure that developers do not overlook security while still allowing for rapid application development. The framework should incorporate security components which deliver security by default, transparent to developers. The Open Group enterprise architecture framework provides an approach to defining security requirements[33] based on identifying what are known as business attributes. Examples of a business attribute include confidential, protected, private, available, and resilient. By defining which attributes apply, a risk profile can be determined and the appropriate security controls applied.

Developing a risk profile for the deployment of IoT products helps ensure a product not only is secure from a cyber attack, but that it operates in a manner which promotes privacy and safety. In the same way as security is applied to traditional IT products, the level of rigour at which security is applied in the IoT domain should be proportional to the potential consequences should it fail.

Given the wide scope of IoT, there is no single solution which defines security for IoT. Designers need to identify the security requirements relevant to their products in the context of the design goals, the environment in which the product will be deployed, and with regard to any regulatory obligations that might apply.

8.2 Security Frameworks

8.2.1 Industrial Internet Consortium

The Industrial Consortium has produced a series of documents including the *Industrial Internet of Things Volume G4: Security Framework*. This is a very thorough document covering the business viewpoints of risk and trust and functional viewpoints including protecting endpoints, protecting communications and connectivity, monitoring and analysis, and configuration and management. This is summarised in section 6.2.

This document also pays particular attention to ‘brown fields’ systems where new solutions and components must co-exist and

---

[32] www.networkworld.com/article/2909212/security0/schneier-on-eally-bad-iot-security-it-s-going-to-come-crashing-down.html

[33] www.opengroup.org/subjectareas/security

interoperate with existing legacy solutions. This is in recognition that there are many long-lived systems which are potentially "out of date," and solutions such as locked doors are no longer appropriate.

8.2.2 Open Connectivity Foundation

The Open Connectivity Foundation (formerly the Open Interconnect Consortium, OIC) has designed an open framework for the IoT. This provides detail down to the level of device descriptions, data types, network protocols, and includes an IoT security specification. The framework is still evolving.

8.3 Security Standards and Guidelines

8.3.1 Open Web Application Security Project (OWASP)

The Open Web Application Security Project was originally conceived as an initiative to develop the definitive security and testing guide for web services. OWASP subsequently extended its scope with a developed framework for mobile device testing, and has now produced a similar framework and testing guide for IoT.

The OWASP IoT Security Principles, summarised at Appendix I, can be applied in various ways by manufacturers, developers and consumers as evaluation criteria for various forms of IoT products. These criteria provide the basis of a secure IoT development framework. Their adoption as part of the overall development framework will substantially increase confidence in, and may help minimise the overall cost of security.

8.3.2 Internet of Things Security Foundation

The Internet of Things Security Foundation (UK) has produced a set of *Principles for Security IoT*, based around privacy, trust, integrity, access control, ownership and auditing. The document provides a set of questions in each area which explore the extent of a target device's security. This guidance is summarised in section 6.1.

8.3.3 NIST IoT Security Model

The National Institute of Standards and Technology's *Special Publication 183* provides "an underlying and foundational science to IoT-based technologies on the realisation that IoT involves *sensing, computing, communication*, and *actuation*.[34]" The model is based on five primitives of sensor, aggregator, communications channel, eUtility, and decision trigger. It also has six elements or characteristics of an IoT device: environment in which it operates, cost, location, owner, identifier and snapshot.

---

[34] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

NIST has also released Special Publication 800-160: Systems Security Engineering[35]. This is not a security standard for IoT per se, but represents a set of best practices for cybersecurity in product engineering in order to deliver a trustworthy product. It provides a systems security engineering framework, together with a set of technical and technical management processes.

NIST is also leading the work on development of an IoT-enabled smart city framework as referenced in section 6.5.

8.3.4 GSMA Security Architecture

The GSMA has produced a set of four documents covering IoT security: a security guidelines overview, guidelines for IoT Service Ecosystem, guidelines for IoT endpoint system, and guidelines for network operators[36]. The goal of these guidelines is to resolve the security challenges inherent to its growth. These challenges are:

- Availability: ensuring constant connectivity between endpoints and their respective services in a way which provides security similar to that of cellular networks;
- Identity: authenticating endpoints, services, and the customer or end-user operating the endpoint;
- Privacy: reducing the potential for harm to individual end-users by understanding what privacy identifying information is processed, particularly relating to tracking of people; and
- Security: ensuring that system integrity can be verified, tracked, and monitored by understanding the security in its development lifecycle, whether it uses a trusted computing base, its ability to detect and contain malicious behaviour, and its incident management.

The guidelines provide a set of examples showing how security might be designed into solutions taking into account the challenges above. The guidelines do not provide a new security architecture, rather they identify the questions that should be posed, provide a list of frequently asked questions, and indicate existing standards that might address the solutions.

GSMA observes that IoT technology has collapsed into a predictable model composed of only several variants, with the IoT endpoint expected to take on one of three manifestations:

- the Lightweight Endpoint, e.g. wearables and home security sensors;
- the Complex Endpoint, e.g. appliances and SCADA systems; and
- the Gateway (or “Hub”).

The GSMA security model considers five targets for endpoint attack: networks, network services, console access, local bus and chips.

The network security principles cover secure identification and authentication of users, applications, endpoint devices, networks,

---

[35] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

[36] http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/

and service platforms; security of communications; and availability. The Guidelines list a set of best practice recommendations for service providers to consider.

The Guidelines provide a set of security recommendations for the endpoints and service ecosystem, which are shown at Appendix III.

8.3.5 Cloud Security Alliance

The Cloud Security Alliance has produced a document entitled *Security Guidance for Early Adopters of the Internet of Things*[37]. This covers the security controls which should be in place, across seven primary areas:

- Analyse privacy impacts to stakeholders and adopt a Privacy-by-Design approach to IoT development and deployment;
- Apply a Secure Systems Engineering approach to architecting and deploying a new IoT System;
- Implement layered security protections to defend IoT assets;
- Implement data protection best-practices to protect sensitive information;
- Define lifecycle controls for IoT devices;
- Define and implement an authentication/authorisation framework for the organisation's IoT Deployments; and
- Define and implement a logging/audit framework for the organisation's IoT ecosystem.

The *Guidance* gives substantial further details on these controls.

8.4 Designing Security into Products

8.4.1 Designing for Evaluation and Certification

Design of security for an IoT product should be based on the identified risks, with controls selected from the relevant control sets. A threat risk assessment based on the likely deployment scenarios will identify the risk level to which an IoT device or system is likely to be exposed, and the systemic risk which this introduces to the environment in which it operates.

When designing IoT products and services which are expected to be submitted for security evaluation and/or certification, it is useful to develop and maintain a current set of documents that will support the evaluation process. A key start point will be documenting an Initial Claims Document (ICD) which explicitly calls out the security functionality and a Target of Evaluation (ToE) description which documents the boundaries of the evaluation.

8.4.2 Application Services which Influence Design

There is an increasing number of vendor end-to-end solutions being delivered for IoT deployments. These are expected to produce solutions for a variety of use cases but will likely evolve

---

[37] https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/

quickly as new IoT technologies emerge. Some will be more open than others, and some will leverage and influence industry standards. When employing vendor end-to-end solutions, the security model should be investigated and understood.

An example of this at the component level is Microchip. Microchip and Amazon have collaborated to develop an integrated solution to help IoT devices quickly and easily comply with AWS's mutual authentication IoT security model. The new security solution will help companies implement security best practices from evaluation through production. This is delivered as a hardware chip which integrates with the AWS Software Development Kit.

At the system level, IBM promotes an architecture-based on their Bluemix platform at the application level, with the Watson IoT Platform working in conjunction with the HiveMQ Enterprise MQTT Broker to enable device integration.

Microsoft has released an Internet of Things Security Architecture which promotes a four zone model of Device, Field Gateway, Cloud Gateway, and Services. Each zone segments a solution, and often has its own data, authentication and authorisation requirements. Zones can also be used to isolate damage and restrict the impact of low trust zones on higher trust zones.

8.4.3 Design Patterns

The design and implementation of security controls can be time consuming and costly, requiring a high level of effort in the design and testing phases. Where similar products are being developed, their security solutions are likely to be substantively similar, and the re-use of an existing design can often provide an effective solution requiring little more than design integration and testing. A design pattern is a formalisation of this concept, and is a reliable implementation blueprint for a specific business use case scenario. A repository of software security design patterns has been developed through the Pattern Languages community and documented by the Carnegie-Mellon University Software Engineering Institute[38]. These are for general software security, but provide a foundation for more specific use cases. An increasing number of IoT design patterns are expected to become available as common approaches are adopted by vendors.

IoTAA intends to progressively develop and publish IoT security design patterns to support this *Guideline*.

8.5 Testing Security in IoT Products and Deployments

8.5.1 Testing Schemes

IoT product manufacturers may wish to submit their products for testing by an accredited test laboratory, either under the

---

[38] CMU/SEI Report Number: CMU/SEI-2009-TR-010

National Association of Testing Authority (NATA) scheme or under the Australian Government in the Australasian Information Security Evaluation Programme (AISEP)[39]. Formal testing will, if successful, result in the award of a test certificate and provide evidence of independent security assurance to customers.

Currently there is no mandated requirement for security testing, but the high profile of cyber attacks involving internet of things devices makes this a key area of consideration for users. Having evidence that a device has been security tested will be a competitive advantage.

8.5.2 Assurance Levels

The threat risk assessment used to drive design considerations will also determine the depth of security testing required for the product, and this in turn will determine its assurance level – the extent to which the user can be confident that its security is effective. Assurance levels are commonly referred to as EAL1 to EAL7, where EAL1 is basically just a test that the documentation is correct, and EAL7 has a formally verified design and in-depth testing. Commercial vendors will typically seek to achieve assurance levels of EAL3 or EAL4.

8.5.3 Testing Criteria

There are currently two published criteria for testing IoT devices:

- The IoT Security Foundation has proposed a compliance scheme based on evaluation against their Security Compliance Framework. This has been described in section 6.1.
- OWASP has developed a testing guide for IoT products (see Appendix II) which covers 16 IoT Principles of Security and provides a framework for testing ten different vulnerabilities.

IoT device manufacturers may wish to select the relevant criteria for their device from these two documents, in addition to any device specific functionality not otherwise covered. These criteria will then form the Initial Claims Document for the security testing.

For mission- and life-critical systems, security evaluation should be through, or as a minimum reflect the processes of, the globally recognised Common Criteria approach adopted by the AISEP.

8.6 Cyber security Insurance

The use of cyber insurance is becoming more prevalent and is a useful way for businesses to address the risks of cyber-attack. When considering a business for insurance, the insurance company will assess the cost of cover based on the client risk exposure, and may offer premium reductions where security has been properly addressed.

When marketing and deploying IoT products and systems, the impact on insurance cover may be a significant cost factor and taken into account.

---

[39] https://www.asd.gov.au/infosec/aisep/

IoT products with security certification may result in lower premiums than those without.

9 LEGAL ISSUES

Privacy issues associated with IoT, as discussed in Section 4 of this *Guideline*, are covered by a number of relevant laws and principles. However, there are other areas of legal relevance that arise or are reinforced by the nature of the IoT. Some of these are related to security[40], including areas of national security and cooperation with law enforcement agencies.

9.1 IoT in Telecommunications Law

Section 4 of this Security Handbook discusses how personal information is regulated by the *Privacy Act 1988*. Another important body of security related regulation is imposed by telecommunications law.

If an IoT solution involves deployment of a wireless network and/or includes the sale of carriage services to customers, the solution will (very likely) be regulated by telecommunications law.

Services that provide or resell carriage have onerous security obligations. Information transiting the network must be protected. Use of it and use of the details of its customers is heavily restricted. Unless exempt, there is an obligation to ensure that messages can be intercepted by law enforcement and to retain and make available certain data.

Small changes in the design of a solution and/or making use of third party services can have a big impact on the regulatory obligations that may apply.

9.1.1 Overview of regulatory framework

In order to understand if an IoT solution is regulated by telecommunications law, it is important to understand whether a provider of such a solution is a carrier and/or whether the solution provided is a carriage service.

IoT networks are generally radio communication networks. Radio transmissions are strictly regulated in Australia by the *Radiocommunications Act 1992*.

Broadly speaking the *Radiocommunications Act 1992* permits:

- the operation of certain transmitters under a system of class licencing;
- the auctioning of a right to use certain bands of spectrum time to time and the Australian Communication and Media Authority (ACMA) to auction the right to use spectrum; and
- the issue of apparatus licences that permit the use of specific transmitters in specific frequencies and locations.

Many IoT devices are low powered devices that are permitted to operate in designated spectrum under the *Radiocommunications (Low Potential Interference Devices) Class Licence 2015*. Mobile phone users are permitted to use their mobile phones and devices that use SIM cards by the

---

[40] Taylor Wessing: https://www.taylorwessing.com/download/article_spam_fridge.html

Radiocommunications (Cellular Mobile Telecommunications Devices) Class Licence 2014.

The rules regulating the use of radio transmitters, the radio frequency, power and transmission standards used apply equally to network operators, businesses that use radio enabled sensors, other device owners and users.

The *Telecommunications Act 1997* provides that the owner of a 'network unit' must not use or allow a network unit to be used to provide a carriage service to the public unless the owner holds a carrier licence.

Four types of facilities can be network units:

- single line links connecting distinct places in Australia at least 500 metres apart;
- multiple line links connecting distinct places in Australia where the aggregate of the distances between the distinct places is more than 5 kilometres;
- designated radiocommunications facilities (of any range); and
- facilities specified by the Minister in a written determination.

Places are distinct if they are not all in the same property, or a combined area of contiguous properties where the same person or persons is the principal user (essentially the occupier) of the combined area.

A designated radiocommunications facility is a reference to:

- a base station used, or for use, to supply a public mobile telecommunications service; or
- a base station that is part of a terrestrial radiocommunications customer access network; or
- a fixed radiocommunications link; or
- a satellite-based facility.

A ministerial declaration exempts radio networks that supply services to users that are all in the same place. Without this declaration, WiFi routers used by business owners to provide connectivity at cafes, shops and airports would be "a base station that is part of a terrestrial radio communications access network" and require the relevant provider to have a carrier's licence.

If IoT providers want to operate a radio communications network that supplies services to the public some of whom are not in the same place as the transmitter, they must either obtain a carrier's licence or find a carrier that is prepared to act as the nominated carrier for the network under consideration. Nominated carriers are notified to the ACMA and take regulatory responsibility for the operation of unlicensed carriage networks.

A carriage service provider (CSP) supplies or arranges the supply (an intermediary) of a carriage service to the public using:

- a network unit owned by one or more carriers or operated by a nominated carrier;

- a line link connecting a place in Australia and a place outside Australia; or
- a satellite based facility.

A party is a CSP if it provides a connection into Australia from offshore or resells or arranges the resale of the carriage services of a carrier. An internet service provider (ISP) which does not own any transmission assets will be a CSP, but not a carrier for the purposes of regulation.

CSPs are subject to a range of obligations, but are not required to have a licence.

If part of an IoT business model is to resell customers' access to carriage services on a third-party network, then the IoT provider will be a CSP. On the other hand, if a product or service sends and receives information but using network services arranged by a customer, it is regarded as 'over the top' and does not make the provider of that service a CSP.

9.1.2 Protection of communications

It is important to understand when a provider is a carrier or CSP as carriers and CSPs are subject to various obligations under the *Telecommunications Act 1997.*

A primary security obligation is the duty to protect the confidentiality of information that relates to:

- the contents of communications that have been, or are being, carried; and
- the carriage services supplied; and
- the affairs or personal particulars that come to knowledge or possession by reason of providing the service.
- The disclosure or use of protected information is authorised in limited circumstances, including to employees and contractors acting in accordance with their duties and in connection with the operation of an enforcement agency as required or authorised under a warrant, or otherwise as required under law. Any person to whom such information is disclosed is also prohibited from disclosing it.

Record-keeping requirements are imposed in relation to authorised disclosures or uses of information.

There is also a general obligation to give officers and authorities of the Commonwealth and of the states and territories such help as is reasonably necessary for the purpose of enforcing the criminal law (of Australia or a foreign country) and laws imposing pecuniary penalties, protecting the public revenue and safeguarding national security, which amounts to an obligation to disclose information those authorities require for those purposes (other than the content messages transiting the network), even where they do not have a warrant.

9.1.3 Ability to access and intercept

The Telecommunications (Interception and Access) Act 1979 prohibits the interception of communications passing over a telecommunications system and lays out a number of circumstances in which this prohibition does not apply. These include in the case of emergency requests, where required to do so under various forms of warrant, and where authorised by the Attorney-General for developing and testing interception capabilities.

As an incident of those obligations, *the Telecommunications (Interception and Access) Act 1979* also requires that providers of telecommunications systems such as carriers and CSPs must ensure that their system can:

- enable a communication passing over the system to be intercepted in accordance with an interception warrant; and
- transmit lawfully intercepted information to the delivery points applicable in respect of that kind of service.

It is possible to apply for an exemption from these requirements. Carriers and nominated CSPs are also required to file an 'Interception Capability Plan' with the Department of Communications and the Arts, which sets out how precisely it intends and is able to comply with its obligation to provide interception capabilities.

9.1.4 Mandatory data retention

There is also a mandatory data retention obligation in the *Telecommunications (Interception and Access) Act 1979*. This obligation requires carriers and CSPs to retain for a period of two years certain information relating to accounts and communications, including, broadly, identifying information associated with an account, the source, destination, date, time, type and duration of communications, and the location of equipment used to transmit the communication. This information must be made available to law enforcement and national security agencies on request. If the information is used for any purpose other than to meet these statutory obligations of the data retention regime, any such information must also be provided in response to any civil subpoena seeking disclosure of it.

There is an ability to apply to the Attorney-General for exemption from all or part of the data retention requirements. If the data collected by an IoT solution is unlikely to have any value to law enforcement or national security, an IoT provider may wish to apply for an exemption.

9.1.5 New developments

As of August 2017, the *Telecommunications Sector Security Reforms Act* has been passed by the Australian Senate and has been referred to the House of Representatives. It introduces a broad obligation on carriers and CSPs to protect the security of their telecommunications services and facilities and for carriers and certain CSPs to report any changes to their network or services that may have an impact on security.

9.2 Other Areas Impacted by IoT

9.2.1 Network access

IoT devices often rely on internal network and internet access, and any disruption could result in failure of the IoT system. Such disruption may be caused by a breakdown of net neutrality, inadequate bandwidth provision by an internet provider or the result of a denial of service attack. The legal consequences of such failures should be considered when designing the IoT system.

9.2.2 Liability

An IoT system will generally consist of many components interacting in a complex fashion. The attack surface of an IoT will expand in proportion to the multiple sensors and actuators it contains, as well as by the cloud services it consumes. These components are likely to be manufactured, contracted, or leased from multiple sources. The liability as a result of accidental failure or deliberate cyber breach of any point is not currently clear.

9.2.3 Data Ownership

The deployment of IoT will result in significant data being generated. As IoT evolves, it is likely that an increasing amount of its data will be shared. Data ownership will become more complex, and the consequences of corrupted data (either accidentally or deliberately) may reach beyond its source organisation.

9.2.4 Nation State Activities

IoT will substantially expand the infrastructure surface for nation state attacks from the current critical infrastructure. Such attacks may result from designed backdoors in equipment and/or remote penetration, and will be well-resourced. Both government and utility companies will need to ensure the integrity of devices and systems, and that adequate protection is in place.

APPENDIX

A OWASP Principles of Security

#	Name	Description
1	Assume a Hostile Edge	Edge components are likely to fall into adversarial hands. Assume attackers will have physical access to edge components and can manipulate them, move them to hostile networks, and control resources such as DNS, DHCP, and internet routing.
2	Test for Scale	The volume of IoT means that every design and security consideration must also take into account scale. Simple bootstrapping into an ecosystem can create a self-denial of service condition at IoT scale. Security counter measures must perform at volume.
3	Internet of Lies	Automated systems are extremely capable of presenting misinformation in convincing formats. IoT systems should always verify data from the edge in order 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 lifecycle to ensure that encryption is applied uniformly and appropriately to guarantee protections. Encryption is not total – be aware that metadata about encrypted data might also provide valuable information to attackers.
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	Lifecycle Support	IoT systems should be able to quickly on-board new components, but should also be capable of re-credentialing existing components, and de-provisioning components for a full device lifecycle. This capability should include all components in the ecosystem from devices to users.
11	Data in Aggregate is Unpredictable	IoT systems are capable of collecting 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 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 API's 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.

Source and further details on OWASP security principles:
www.owasp.org/index.php/Principles_of_IoT_Security

B OWASP Security Testing Guide

#	Name	Description
1	Insecure Web Interface	Assess any web interface to determine if weak passwords are allowed Assess the account lockout mechanism Assess the web interface for XSS, SQLi and CSRF vulnerabilities and other web application vulnerabilities Assess the use of HTTPS to protect transmitted information Assess the ability to change the username and password Determine if web application firewalls are used to protect web interfaces
2	Insufficient Authentication/Authorisation	Assess the solution for the use of strong passwords where authentication is needed Assess the solution for multi-user environments and ensure it includes functionality for role separation Assess the solution for Implementation two-factor authentication where possible Assess password recovery mechanisms Assess the solution for the option to require strong passwords Assess the solution for the option to force password expiration after a specific period Assess the solution for the option to change the default username and password
3	Insecure Network Services	Assess the solution to ensure network services don't respond poorly to buffer overflow, fuzzing or denial of service attacks Assess the solution to ensure test ports are not present
4	Lack of Transport Encryption	Assess the solution to determine the use of encrypted communication between devices and between devices and the internet Assess the solution to determine if accepted encryption practices are used and if proprietary protocols are avoided Assess the solution to determine if a firewall option available is available
5	Privacy Concerns	Assess the solution to determine the amount of personal information collected Assess the solution to determine if collected personal data is properly protected using encryption at rest and in transit Assess the solution to determine if Ensuring data is de-identified or anonymised Assess the solution to ensure end-users are given a choice for data collected beyond what is needed for proper operation of the device
6	Insecure Cloud Interface	Assess the cloud interfaces for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) Assess the cloud-based web interface to ensure it disallows weak passwords Assess the cloud-based web interface to ensure it includes an account lockout mechanism Assess the cloud-based web interface to determine if two-factor authentication is used

		Assess any cloud interfaces for XSS, SQLi and CSRF vulnerabilities and other vulnerabilities Assess all cloud interfaces to ensure transport encryption is used Assess the cloud interfaces to determine if the option to require strong passwords is available Assess the cloud interfaces to determine if the option to force password expiration after a specific period is available Assess the cloud interfaces to determine if the option to change the default username and password is available
7	Insecure Mobile Interface	Assess the mobile interface to ensure it disallows weak passwords Assess the mobile interface to ensure it includes an account lockout mechanism Assess the mobile interface to determine if it Implements two-factor authentication (e.g. Apple's Touch ID) Assess the mobile interface to determine if it uses transport encryption Assess the mobile interface to determine if the option to require strong passwords is available Assess the mobile interface to determine if the option to force password expiration after a specific period is available Assess the mobile interface to determine if the option to change the default username and password is available Assess the mobile interface to determine the amount of personal information collected
8	Insufficient Security Configurability	Assess the solution to determine if password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication) are available Assess the solution to determine if encryption options (e.g. Enabling AES-256 where AES-128 is the default setting) are available Assess the solution to determine if logging for security events is available Assess the solution to determine if alerts and notifications to the user for security events are available
9	Insecure Software/Firmware	Assess the device to ensure it includes update capability and can be updated quickly when vulnerabilities are discovered Assess the device to ensure it uses encrypted update files and that the files are transmitted using encryption Assess the device to ensure is uses signed files and then validates that file before installation
10	Poor Physical Security	Assess the device to ensure it utilises a minimal number of physical external ports (e.g. USB ports) on the device Assess the device to determine if it can be accessed via unintended methods such as through an unnecessary USB port Assess the device to determine if it allows for disabling of unused physical ports such as USB Assess the device to determine if it includes the ability to limit administrative capabilities to a local interface only

Source and further details on IoT testing guidelines:
https://www.owasp.org/index.php/IoT_Testing_Guides

C GSMA Security Recommendations[41]

Endpoint	Eco-System
Critical	
Implement an endpoint trusted computing base	Implement a service trusted computing base
Utilise a trust anchor	Define an organisational root of trust
Use a tamper resistant trust anchor	Define a bootstrap method
Define an API for using the TCB	Define a security front-end for public systems
Define an organisational root of trust	Define a persistent storage model
Personalise each endpoint device prior to fulfilment	Define an administration model
Minimum viable execution platform	Define a systems logging and monitoring model
Uniquely provision each endpoint	Define an incident response model
Endpoint password management	Define a recovery model
Use a proven random number generator	Define a sun-setting model
Cryptographically sign application images	Define a set of security classifications
Remote endpoint administration	Define classifications for sets of data types
Logging and diagnostics	
Enforce memory protection	
Boot loading outside of internal ROM	
Locking critical sections of memory	
Insecure bootloaders	
Perfect forward secrecy	
Endpoint communications security	
Authenticating an endpoint	
High Priority	
Use internal memory for secrets	Define a clear authorisation model
Anomaly detection	Manage the cryptographic architecture
Use tamper resistant product casing	Define a communications model
Enforce confidentiality/integrity to/from the trust anchor	Use network authentication services
Over the air application updates	Provisioning servers where possible
Improperly engineered or Unimplemented mutual authentication	Define an update model
Privacy management	Define a breach policy for abused data
Privacy and unique endpoint identities	Force authentication through the service ecosystem
Run applications with appropriate privilege levels	Implement input validation
Enforce a separation of duties in the application architecture	Implement output filtering
Enforce language security	Enforce strong password policy
	Define application layer authentication and authorisation
	Default-open of fail-open firewall rules
	Evaluate the communications privacy model

---

[41] http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.13-v1.0.pdf

Medium	
Enforce operating system level security enhancements	Define an application execution environment
Disable debugging and testing technologies	Use partner-enhanced monitoring services
Tainted memory via peripheral based attacks	Use a private access point name for cellular connectivity
User interface security	Define a third party data distribution policy
Third party code auditing	Build a third party data filter
Utilise a private access point name	
Implement environmental lock-out thresholds	
Enforce power warning thresholds	
Environment without backend connectivity	
Device decommissioning and sun-setting	
Unauthorised metadata harvesting	
Low	
Intentional and unintentional denial of service	Rowhammer and similar attacks
Safety critical analysis	Virtual machine compromises
Defeating shadowed components and untrusted bridges	Build an API for users to control privacy attributes
Defeating a cold boot attack	Define a false positive/negative assessment model
Non-obvious security risks	
Combating focused ion beams and x-rays	
Consider supply chain security	
Lawful interception	

ABOUT IOT ALLIANCE AUSTRALIA, (IOTAA)

The vision of IoTAA is to empower industry to grow Australia's competitive advantage through IoT.

For more information visit http://www.iot.org.au/

Communications Alliance was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507