IoT Security Architecture and Policy for the Home - a Hub Based Approach

Release 1

Contents

Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org.

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organization which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing

All product names are trademarks, registered trademarks, or service marks of their respective owners.

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this version of the document

John Moor, IoT Security Foundation
Richard Marshall, Xitex Ltd
Stacie Walsh, Oxford Information Labs

Peer Reviewers:
Andrew Wadsworth, PA Consulting
Carsten Maple, University of Warwick
Chris Shire, Infineon Technologies Ltd
David Alexander, PA Consulting
Jeff Day, BT
Madjid Nakhjiri, Samsung
Nick Allot, nquiringminds Ltd
Paul Dorey, IoTSF Chairman
Steve Babbage, Vodafone
Claire B Milne
Plus others – you know who you are!

1 Introduction

1.1 Executive Summary

Home IoT devices and systems need to manage security with minimal – and potentially no – consumer intervention, and without the consumer having any specialist knowledge of security or IT principles. This is in contrast to other IoT environments which are more formally managed and directly regulated, such as enterprise and transportation. One key challenge in the consumer environment is that home IoT solution providers cannot assume a reliable or sufficient level of users' understanding of security governance.

It is also challenging to manage and maintain a complex system of devices available on the market using a variety of proprietary interfaces and protocols in the home environment. Interoperability between IoT devices is a key aspect of not only hub architectures like this one but any IoT deployment implementing multiple devices. Good interoperability assists with security management across the IoT ecosystem and reduces effort required of the home IoT administrator. It also further opens the IoT marketplace for consumers by avoiding vendor or ecosystem lock-in. The issue of incompatibility and security was highlighted recently by McKinsey [ref 20], as being one of the major restrictions on the growth of the IoT market. While this document does not specifically address the issues related to interoperability, it is worth highlighting the work that needs to be done in this area to support adoption of IoT security, hub architectures like this one and consumer value-add.

Market actors must push to get consumers thinking about security in the home IoT space. Consumers already think about safety in other market areas – such as automotive, housing and toys. In the IoT market, solution providers can incorporate good security practices and certifications in their product development and provisioning. Retailers can opt to sell solutions that meet minimum security expectations or can prove compliance by means of certification. These actions will support the incorporation of security into the consumer purchasing process – similar to the form that reviews, and word of mouth come into play – and potentially stimulate the home IoT marketplace. While not all consumers will adopt a security-minded purchasing process, there is value to both the consumer and wider IoT ecosystem in providing security-minded options for consumers.

The IoT Security Foundation is publishing this home IoT architecture as part of a series of Hub-based architectures with the following intentions:

- Reduce/manage complexity of IoT systems by narrowing implementation options
- Demonstrate by example what a good home security regime looks like
- Demonstrate how to support security in IoT with minimal reliance on users
- Explain the benefits of such an approach including achieving security goals, maintaining system hygiene and resilience, managing extensions and life-cycle provisioning
- Helping to foster growth and demand in the home IoT marketplace by making security a part of the purchasing process

This document is intended for OEMs designing devices or smart hubs – as "the Hub" is a key element of the architecture – Service Providers and Retailers, or anyone with responsibilities for architecting, designing, planning and procuring home IoT products (broadly referred to as solution providers). Specifically, consumers and end users are not the intended or expected target audience for this document.

The Hub-based architecture does not prescribe a single IoT device, deployment or sub-architecture. Instead it focuses on supporting a minimum expectation of security and trust in home IoT environments. This is achieved through implementation of a collection of security and trust tools in home IoT and networking solutions. Importantly, it does not rely on the end user having in-depth knowledge of these topics.

In practice, a hub architecture provides selected points for IoT device and network management that can make use of existing infrastructure, as well as provide flexible solutions for individual home IoT deployments. 'Plug and play' Hub devices should support baseline security for the home environment.

For small homes, the architecture may comprise a single hub; larger homes will probably have of a number of hubs for scalability and redundancy. Related devices and solutions that may comprise a central part of the Hub architecture and support the security features described in this document include a router, network management tools such as a firewall or gateway, network access controls, a protocol bridge, or any other device that naturally lends itself to such a role within a network.

Whilst perfect security is likely to remain elusive, this architecture is considered to be a good approach to achieving common security goals of confidentiality, integrity and availability.

Security is not static, it requires a series of on-going processes that need to be managed over the combined life-cycles of system elements including services, devices and networks. This hub architecture supports a layered approach to the security challenge and provides management controls over the lifecycle of the home IoT deployment. As a result, it may also support a number of specific compliance requirements or best practice standards for organizations providing home IoT solutions. For example, a hub-based architecture can help mitigate risk associated with cyber security and data protection regulations such as the European General Data Protection Regulation (GDPR) and Network and Information Systems (NIS) Directive or support adoption of the USA's Cybersecurity Information Sharing Act (CISA).

1.2 Background

Home IoT solutions offer a wide variety of opportunities and benefits for users, spanning concepts such as home and lifestyle management. The current home IoT marketplace includes solutions for the 'Smart Home', (e.g. lighting, heating controls and appliances) and personal devices such as fitness trackers and sleeping aids, to name a few. The drivers for consumers to adopt IoT solutions are many and varied – for example, from supporting green initiatives, to cost savings, time savings or convenience. When consumers look to the market for home IoT solutions, security should be one of the main drivers behind decision-making.

Managing security in home IoT environments is especially important as the benefits of IoT could be overshadowed by the risk of adoption. A recent survey[13] in the USA shows data protection is a key concern with 88% of respondents feeling negatively about companies using their personal data to optimise delivery service times to ensure the customer was at home. In the same survey 72% of respondents who already own a smart security system are worried home security companies would invade their privacy. Consequently, 23% of connected security system owners responded that they deactivate their system completely when they have guests.

It is essential to protect the public internet and its infrastructure from malicious attacks enabled by the mass number of connected consumer devices – currently estimated at over 8 million[14] and growing. For example, the 2016 Dyn domain name service provider cyberattack compromised a large number of home IoT devices such as printers, cameras, and gateways, resulting in distributed denial of service attack (DDoS). The resulting effect was the taking down of a variety of websites and services including Amazon.com, Comcast, and *The Guardian*.

In 2015, Foscam baby monitor hacks not only showed the importance of users changing default passwords to protect against hacks. [15] It also highlighted the need for service providers to think of security throughout the lifecycle of the device, as older and more "hackable" models of Foscam's baby monitors could not be updated or required user initiative to do so. This tactic creates more security blockades as users then needed to be identified, notified of updates, and capable of implementing them. And even for those security-minded users who had turned off some data-sharing capabilities, Foscam continued to communicate data to servers in China. The configuration options only provided a facade of user control.

In a consumer home environment, it is particularly important to develop robust security that requires minimum oversight and management by the consumers. Yet, as we have seen, consumers are concerned with issues related to data protection and security. Addressing those concerns through home IoT solutions, as well as creating a more informed and aware consumer, has the potential to drive consumer demand for home IoT solutions.

1.3 Intended Audience

The intended audience for this document is people with the following roles or responsibilities:

- IoT Service Providers – to better understand IoT products, their system management/security and gaps in the market, particularly:
    - Section 3: Hub-Based Reference Architecture
- Developers – to better understand IoT management and security needs of the home and gaps in the market, particularly:
    - Section 3: Hub-Based Reference Architecture
- OEM Product Management – to better understand IoT management and security needs of home and gaps in the market, particularly:
    - Section 3: Hub-Based Reference Architecture

1.4 Scope

The scope of this document is a Hub-based architecture for IoT devices and solutions implemented and managed in the home.

We do not make assumptions about the business models of IoT product OEMs or solution providers. For this reference architecture, it is assumed that whilst some IoT devices may be owned by the home IoT user – such as an occupant, owner, or manager; some IoT devices will be wholly owned, controlled and operated by an IoT service provider. It is, however, assumed that most IoT devices will have some level of control and management by the home user.

Below is a more detailed list of IoT and related issues considered in scope of this proposed Hub architecture:

- Consumer and service provider IoT solutions for the home (e.g. smart lightbulbs, door locks, toys and refrigerators)
- Devices that connect to and/or provide information via the home's network (e.g. smart refrigerators and washing machines that communicate within and outside the home environment)
- Smart meters provided by utility providers (e.g. gas or electric smart meter) in so far that they communicate via the home network and/or with other IoT devices in the home – such as smart washing machines, electric vehicle chargers or lights. (If the smart meter is only communicating with the utility provider over a dedicated communication network, such a meter is not considered in scope)
- Devices with security features that are managed by the Hub user (e.g. authentication, roots of trust, password control, update)
- Devices with configuration options managed by the home user
- The deployment of IoT devices in the context of a home where the user works from home and needs to segregate domestic and home office network traffic (e.g. smart printer, white boards, and mobile devices)
- Small organizations, like family run businesses, which do not have the technical expertise or knowledge of more technically-minded SMEs or larger enterprises
- The considerations surrounding the change of home occupier, either through house sale or change of tenancy, specifically how IoT devices that form part of the home's fabric or security have their settings and credentials transitioned between the home occupiers. For example this may involve either: the change of the hub and the re-introduction of these IoT devices to the new hub or, where the hub is not changed with the new occupiers, the replacement of the old occupier's details with the new occupier's credentials in the hub
- The situation where the hub develops a fault, requiring replacement and the introduction of a new hub into the home
- The situation where a home user must manage IoT solution end-of-life, end-of-support or change in the supporting organization

The scope of the home IoT category may include utility or other equipment. Explicitly we do not include solutions such as the utility interfaces to smart meters, and especially when communications are sent via a dedicated communication pathway (e.g. not using the home's internet connection). With this in mind, communication between the smart meter, communications hub and other home IoT devices are considered in scope as the meter has then become an element of the home IoT ecosystem. This is to focus effort on covering the majority of domestic use cases and to concentrate on the IoT devices available for sale today or those widely anticipated.

Below is a more detailed list of IoT and related issues considered out of scope for this proposed architecture:

- IoT not in Scope:
    - IoT solutions implemented by *building* owners/managers – such as freeholder, property management agencies or public housing managers – and not within the purview of the *home's* occupier or owner. As suggested here, building and home owners may not be the same entity – for instance the owner of a condominium may pay a lease to the building owner.
    - The IoT management relationship and hand-off between home owners and occupiers
- Other considerations not in scope:
    - Consideration for sector-specific requirements and regulations – such as security and data protection requirements for the utility sectors.
    - The IoT business models provided by manufacturers or solution providers.
    - Direct communications between the solution provider and IoT device which are not sent via a home network (e.g. by using a dedicated mobile connection, not over the home internet connection) are out of scope since such traffic is not visible to the home network. However, principles regarding privacy, informing the customer of the traffic and data, the usage of the traffic and data, and the security principles remain applicable to such devices. Moreover, some of the recommendations – such as traffic monitoring – may assist in addressing risks posed by such external communications.

1.5 Taxonomy

In the requirements sections, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119 [ref 2].

The following terms are used in this document:

Home IoT administrator – an adult individual who carries out the configuration, installation, maintenance, and purchasing where appropriate of the home IoT network. Home IoT administrators may be owners or managers, occupants, trusted parties or service subscribers (such as parents). The administrator will be unique to the home IoT environment and product.

Home occupant – the person(s) residing in the home. Occupants may be any range of individual, including home owners, IoT administrators, or tenants. The home occupant is not necessarily the home IoT administrator or owner of the home IoT deployment.

Home IoT provider – Here, an IoT solution provider is an OEM, Service Provider, or anyone with responsibilities for architecting, designing, planning and procuring Consumer IoT products.

Public Roots of Trust – A publicly trusted root is one whether the root of trust is publically accessible, typically where the trust anchor is publically published by one of the public Certificate Authorities.

Private Roots of Trust – A private root differs from a public root because roots of trust aren't publically accessible. The root(s) of trust will need to be published by the organization whose Certificate Authority created the root of trust, to those entities which need to validate the chain of trust anchored by the private root.

2 Overview

2.1 Aim of Hub Architecture

This Hub reference architecture aims to provide a user-friendly centralized management solution for homes deploying IoT devices and solutions, especially as this typically involves devices from multiple vendors. Importantly, the architecture considers security a primary objective and provides a way forward with this in mind. It is also intended to highlight where security solutions currently available on the market fulfil as well as lack these desired features.

Unlike other IoT architectures, this Hub architecture provides a more secure and easy to manage home IoT ecosystem. There are two key elements to this proposed architecture: the Hub device and the flexible Hub networking model. Importantly, the Hub and its IoT management interface[1] is a user-friendly resource for home IoT administrators.[2] The home environment will be managed by consumers with varying degrees of capability. The Hub architecture enables home IoT administrators to easily oversee and manage their IoT environment by offering tools such as alerts and troubleshooting.

The Hub device acts as a central point for trust and IoT environment management. It also makes use of existing security features – such as update mechanisms – and adds an additional layer of security to the IoT environment – such as traffic monitoring and lifecycle management.

The Hub device achieves this by communicating with network elements such as routers, protocol bridges, and IoT devices, aggregating information to offer support to home IoT administrators. It may also act as a gateway, enabling information sharing between the home IoT environment and other networks or entities, such as the IoT solution provider. For instance, the Hub itself may be a home internet router which acts as a gateway and protocol bridge.

The flexible Hub networking model – which allows for any variation of sub architecture and connected devices or groups of devices as required by the home – is intended to fit any size or type of home deployment. Thus, it does not propose particular devices or network architectures beyond separating IoT and home IT networks. Flexibility allows the consumer to adopt the best IoT solution to suit their needs without compromising on security. For example, the ability to choose which data is kept within the home (e.g. managing sensitive data on the Hub) and when to use cloud solutions. An important element of the Hub which facilitates such control and ease of use for the home IoT administrator is the user management interface. While particulars of this interface are out of scope for this document, it could be provided in a number of ways such as by software or via a cloud solution.

For added security, it is recommended that home IoT devices connect via a dedicated IoT network and not via the primary home user network. For instance, a router could separate the home Broadband into two networks in an easy and user-friendly way – one for general internet use by occupants and another for IoT devices such as lights and smart assistants. The aim is to minimize the home IT and IoT network attack surfaces by protecting home network activities from IoT devices which may be used as an attack vector.

[1] The home management interface is not a focus of this architecture as it is specific to the Hub provider's business model and product, but plays an important role supporting the Home IoT administrator.

[2] An IoT administrator is an adult individual who carries out the configuration, installation, maintenance, and purchasing where appropriate of the home IoT network home IoT administrators may be owners or managers, occupants, trusted parties or service subscribers (such as parents). The administrator will be unique to the home IoT environment and product.

2.2 Visualisation of Hub-Based Architecture Components

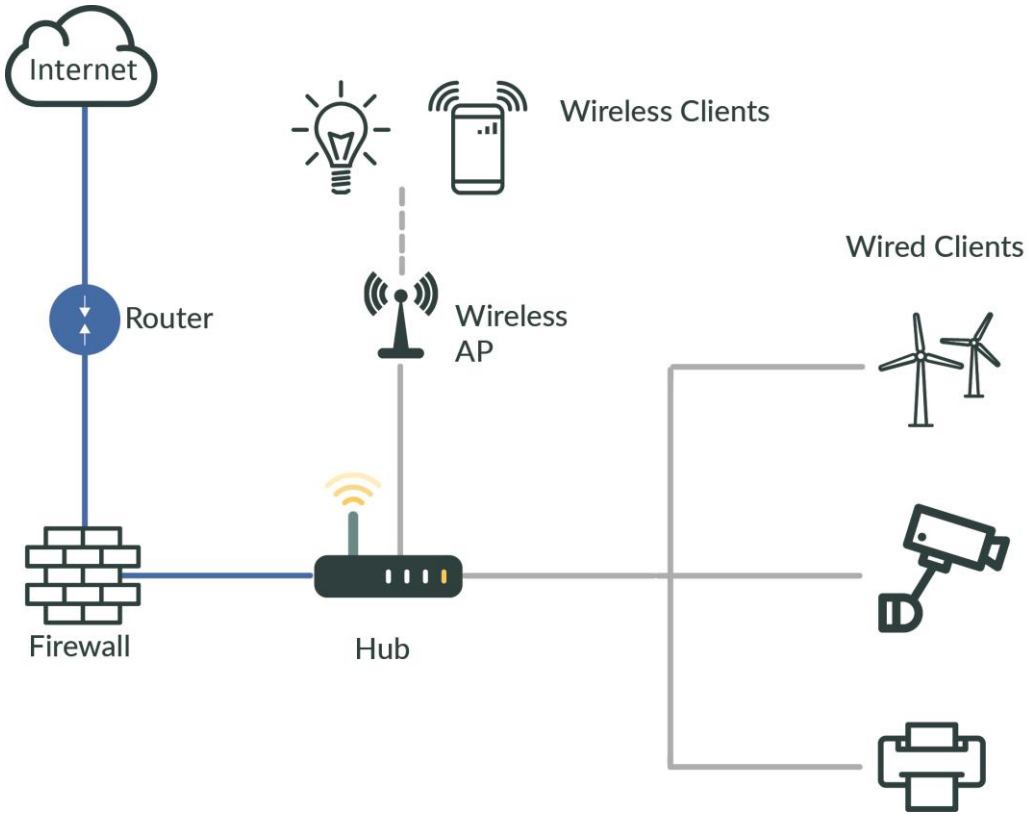

Figure 1: Example Hub Architecture

The visualization in **Figure 2** above shows the multi-layered communication structure within a home IoT environment, and reflects the complex communication structure between devices, networks and the central Hub. The functions of the router and firewall are shown separately but could also be incorporated in the Hub along with other network functions, particularly for those intended for homes with a small number of devices. The **local IoT network** (grey lines) is dedicated to IoT devices and separated from the home's "IT" network. **Devices** (linked by grey lines) use this network to talk between themselves, to the Hub and possibly with external elements via a Hub gateway. **The Hub** is at the center of the IoT ecosystem as it aggregates information and communicates with other architectural elements such as devices and local networks. At the same time, the Hub can act via its connection to the firewall (blue line) as a gateway to external or other home networks as needed.

2.3 Hubs in the Marketplace

There are a variety of home hubs currently in the marketplace which include various aspects of this Hub architecture as elaborated in Section 3 of this document – such as encrypted communications, whitelisting capabilities and with ranges of interoperability. However, it is believed that hubs on the market do not offer the same level of security or services for user-friendly home IoT environment management.

The key elements of this Hub architecture – the Hub device and flexible networking model – facilitate security, interoperability between devices and vendors, and simple user controls to manage the home IoT environment. For instance, most hub offerings are currently provided as software- or platform-as-as-service, but this Hub device could allow for a more traditional owned software solution with strong roots of trust and added benefits of user privacy for the home environment (e.g. by not continuously relaying data to a cloud environment).

Most hubs on the market only support update and patch for the hub device or software itself – not offering a single location to manage home IoT device updates. Lack of a central management point imposes an added level of IoT management on the home user. Additionally, not all hubs on the market are home user-focused. Many are directed at business consumers, with a different range of capabilities and technical capacity.

2.4 Hub-based Reference Architecture

Each home IoT deployment is unique and the proposed Hub architecture is intended to provide a flexible solution which can accommodate a wide variety of home environments and users. It assists OEMs, developers, and service providers to purposefully implement a collection of security and trust tools in their products to support a minimum level of security in different home IoT environments. For instance, some homes may only require a single Hub while homes with multiple occupiers or home offices may require multiple hubs. Because of its central role, the Hub should provide a point to oversee, monitor, and, to a degree, control the home's local IoT ecosystem.

The Hub sits at the centre of this reference architecture, aggregating information and communicating directly with other devices, hubs and network elements in the IoT environment. At the same time, the Hub can be visualised at the edge of a network, providing a secure gateway for communication between networks. The Hub should be user-friendly and support good device management and security practices. In addition, the Hub itself needs to have robust security to protect the information and roots of trust that it manages.

Security considerations are taken at every level of the Hub architecture. This provides layers of security for both the wider network and for those devices that may have minimal or no built-in security features. For instance, this can be done by acting as a gateway to monitor and manage traffic or, for homes with higher expectations and capabilities for oversight, managing device identity and access controls.

As a result, the Hub architecture is proposed as a more robust and secure architecture than others, such as "tree" or "hub-and-spoke". Unlike a Hub, a tree network connects a number of nodes via a direct communication line without a central management point. This Hub architecture provides an information aggregation point (the Hub) for all devices, groups of devices, or other Hubs deployed within the local IoT network. The Hub provides a management point where requests, actions, or troubleshooting can be executed, communicating from one to many devices and vice versa. It is also agnostic to sub-architectures used to implement IoT devices.

2.4.1 Why a Hub?

This paper proposes a Hub-based architecture as a robust foundation for IoT security and management for several reasons, including:

- **Centralized Management** – A Hub is characterized as the focal point in a network, with connectivity to all groups/devices, network management tools or other Hubs. Ideally, a Hub enables IoT ecosystem lifecycle management by supporting network and end-device security. It provides an easy one-stop-shop for home users to manage roots of trust, monitor network traffic, manage devices on the network, updates and patches, and troubleshoot issues. In the case of multiple Hubs within the home environment, a "parent" or "master" Hub solution may be implemented.
- **Software Update and Patch** – The failure or inability to update connected devices is a now well-known security risk [see ref 11]. A Hub enables the management and implementation of software updates within the home IoT ecosystem. This facilitates an additional layer of security by providing an easy update point – the Hub itself – particularly for those devices which do not support endpoint solutions such as updating and patching.
- **Troubleshooting** – A Hub also provides a troubleshoot mechanism for the home IoT ecosystem. From information gathered through traffic and system monitoring, the Hub may provide the Home IoT administrator real-time notifications such as suspicious traffic or anomalies. Furthermore, the Hub may suggest treatment actions the home IoT administrator can take based on basic troubleshooting functions, such as taking a malicious device offline or changing appointed data sharing times to avoid

pinch-points. This will also help build up the home user's knowledge of the security space in a way that supports a variety of backgrounds and capabilities.

- **Fostering growth in consumer markets and demand** – Home IoT solutions that address consumer concerns regarding data protection and security will help foster consumer marketplace growth. It is important to not only incorporate security good practices but also communicate this effectively to the consumer. Certification schemes or marks that show compliance can build consumer confidence in home IoT products. Adopting or addressing the security considerations presented in this Hub architecture supports good security practices and compliance with such schemes, all with the potential to drive marketplace growth.
- **Solution Provider Security Compliance** – A Hub architecture provides a central place to manage layered security and ensure a minimum level of security that protects all IoT devices in the home. For instance, the Hub could act as a firewall and/or provide a simple update and patch mechanism to support an IoT provider's compliance with IoT security certification requirements, frameworks, or best practices. Compliance with recognized certification schemes or frameworks, such as the IoTSF Security Compliance Framework [ref 1], can be used as a tool for both retailers and consumers when making choices in the IoT marketplace.
- **Fostering interoperability of IoT solutions** – IoT devices use a variety of open and proprietary resources such as software, identifiers, and connectivity technologies. The Hub device in this architecture provides an essential space to broker between IP and non-IP networks, convert protocols, and standardize data formats. Currently many IoT solutions result in vendor or ecosystem lock-in for consumers. This architecture uses a Hub device to facilitate interoperability between vendors and devices, further opening the home IoT marketplace and preventing lock-in.

2.4.2 Main Hub Functions

To provide a centralised management point, the Hub will need to support a number of tasks and tools. These include a device and user interface that can act as a repository of information for monitoring – including appropriate data protection – reporting and troubleshooting capabilities, provide alerts and notifications, act as a certificate manager and/or cache, provide access controls, and possibly enable device control functionalities.

The Hub supports three basic IoT device "classes" to assist flexibility. Of the three classes listed below, most IoT devices will fall in Class 2, where the home may centralise as much of the device management as possible within the Hub architecture, but some aspects of management may rest with the service provider.

- **Class 1: Fully controlled and connected** – where interfaces such as IoT device control, data collection and management are fully integrated and controlled by the Hub device and kept within the home
- **Class 2: Partially controlled and/or connected** – where the Hub device may execute some but not all interfaces with the device, such as pushing updates and managing traffic but not collecting sensor data
- **Class 3: Information sharing** – the most basic type of interaction, the Hub would not control or manage the IoT device functions such as updating or data collection, but instead will log basic information such as device status or installed updates

For the purpose of this proposed Hub architecture, the main Hub functions or support capabilities include network management, connecting devices securely, and lifecycle management. Although out of scope, and therefore not included in this document, it is important to note the need for an easy to use user interface, to support the home IoT administrator and Hub functions. Section 3 *Hub-Based Reference Architecture* goes into detail on how these functions may be implemented in the architecture. Below are examples of how each of these Hub functions support home IoT security:

- Network Nanagement
    - **Local IoT network**: A Hub may split the home network to separate traffic, minimize attack surface and protect critical home IoT operations [see section 3.3.1]

- **Gateways and firewalls:** A Hub may act as a gateway or receive information from firewalls to protect networks and data and manage traffic [see section 3.3.2]

- Connecting Devices Securely
  - **Authentication and authorization**: A Hub may act as a "middle man", assisting with device authentication before authorizing it onto the IoT network [see section 3.4.1]
  - **Secure boot**: The Hub should use secure boot to validate its software during installation [see section 3.4.2]
  - **Roots of Trust**: The Hub should support standards and best practices in cryptographic capabilities [see section 3.4.3]

- Lifecycle Management
  - **Monitoring**: The Hub may be able to take actions based on monitoring activities, such as revoking device authorization or sending alerts to the home IoT administrator [see section 3.5.1]
  - **Troubleshooting**: The Hub may have the ability to identify issues for the home IoT administrator, suggest solutions and resolve faults to further strengthen the security of the home IoT environment [see section 3.5.2]
  - **Update and patch**: The Hub may have an update log where it can manage queued updates and provide an update history. It may have the ability to assist in verifying the integrity of updates for home devices with limited capability. [see section 3.5.3]
  - **Manage device identity and authorization:** The Hub may have a log of devices, each with a unique or group identifier and attributes (such as location) that allows the user to authorize or revoke access to the IoT network. [see section 3.5.4]
  - **Managing End-Of-Life**: The Hub may have the capability to erase data from a device, reset factory settings, or change administrative access in various scenarios including device end-of-support, replacement, and ownership transfer [see section 3.5.5]

2.5 Assumptions

2.5.1 Device Ownership

We assume devices will have a mix of privilege and variety of ownership, for example by visitors, owners, managers and occupiers of the home. Devices may be used by many people and require trust properties to reflect this, but without imparting administrative privileges to all users of that device.

2.5.2 Network Security

We assume that with the IoT market still in its relative infancy that the network size is likely to be dynamic and expand to incorporate new technologies as they are rolled out. The need to manage diversity in devices including, importantly, device statuses across the network at any given time, is recognized alongside the need for simple processes for improving and updating network security.

2.5.3 Visitor Access

In addition, each home should have the ability to support strong and established trust policies for devices and groups of devices – such as visitor or guest devices – including levels of trust. Examples of devices which may be assigned particular trust policies include:

1. Parent/adult friends' visitor devices
2. Children's friends' visitor devices
3. Colleague or client visitor devices (e.g. in a home office environment)
4. Tenant guest devices
5. Service provider guest devices

2.5.4 Privileges

We assume that necessary and appropriate device/service access and administrative privileges will be managed by either the end user (e.g. home owner or occupier) or the service provider. Privilege management will be influenced by business and service provider models in the marketplace. Therefore, in addition it is assumed that clear ownership of privilege management will be communicated by service providers to end users and implemented to varying degrees by end users.

We also assume that general users will not be restricted from using the device's full functionality unless the home IoT administrator wishes to designate permissions, such as those for users or groups (e.g. for guests or children) that do not have administrative privileges. For example, a person should be able to make full use of a smart TV and its services – for example save their user profile, parental access controls and regularly watched programs – whilst not being able to access paid services or inappropriate content.

2.5.5 Technologically Neutral

This proposed Hub architecture is intended to be technology agnostic, and therefore should be flexible and broadly applicable to IoT deployments. It is important to keep in mind that the business models of IoT solutions, particular home structures, and unique deployments will all impact implementation of this architecture. Therefore, the following is provided as an example and not a rigid implementation of the architecture described here. Where existing protocols or standards are referenced, they are for illustration only and are not architecture requirements or recommendations.

2.5.6 Informing the Consumer

Information sharing between solution providers and consumers is a key element to the success of this Hub-based architecture. It is assumed that solution providers will provide relevant information to consumers in a user-friendly and appropriate manner, including using simple, clear language and resources such as diagrams, video and audio. In doing so, home users will become more informed about the IoT products and security features. This may help build confidence in IoT solutions, further develop IoT security as a unique selling point, drive market demand for secure IoT devices, and support good solution provider-consumer relations. Examples of the type of information that may be shared are:

- Security features and their intended impact
- Guidance on how to avoid the creation of security vulnerabilities that could impact the user
- Clear requirements of the user to successfully implement the Hub architecture and/or device
- Clear requirements of the solution provider and what is being managed by them
- Processes that are automated, but of which users should be aware (i.e. action is not required of the user)
- The data that is collected, processed and transferred and for what purposes
- Options regarding what data is collected and how it is shared

2.6 Security Principles

There is a huge variety of devices labelled "IoT" and equal variety in the level of security features supported by those devices and solutions. OEMs, developers and solution providers need to understand the security risks when developing IoT solutions or moving them to market, and therefore be aware of common security principles. These principles shall be built into home consumer devices to support a minimum level of security, no matter the deployment environment.

In addition, IoT device and solution providers shall take care to communicate security features to the consumer. Consumers will not necessarily be aware of security principles, but can take informed decisions, including their criteria for security features, when reviewing products in the marketplace. Part of this is educating the consumer to understand the risks that are associated with IoT solutions. The resulting decisions will differ from home to home as no two IoT deployments will be the same – risk appetites differ, and

knowledge of risks will vary. Nevertheless, these principles should be taken into consideration from the outset and can be included as unique selling points by OEMs, developers, and solution providers.

The most modest approach to security focuses on the following three key principles[3], also included in the "IoT Security Compliance Framework" [ref 1]:

- Confidentiality – ensuring information and systems are protected from unauthorized access.
- Integrity – ensuring that information and systems are unaltered and accurate throughout the lifecycle. For instance, information integrity applies to data collection, transfer, use and storage. Code integrity applies to preventing unauthorized changes or additions.
- Availability – ensuring that information and services are accessible by users or systems as and when needed.

From these principles, a wide variety of questions emerge when developing and considering functionalities of IoT solutions. Many of these questions are considered in "Make it safe to connect: Establishing principles for Internet of Things Security" [ref 10] by the IoT Security Foundation, replicated here for ease:

- Does the data need to be private?
- Does the data need to be trusted?
- Is the safe / timely arrival of data important?
- Is it necessary to restrict access to, or control of, the device?
- Will the device need to be updated?
- Will ownership of the device need to be managed or transferred?

Developing these points to take into consideration IoT architectures as well as data security, this proposed Hub architecture expands upon the list above. The following architecture-specific questions are incorporated here:

- What is the Hub's relationship with trust management? [see section 3.4.3]
- How does the Hub architecture support layered security? [see section 3.4]
- To what extent is network access managed and when should access be revoked? [see section 3.3.1]
- Where is it safe to make the data transparent for monitoring and updating? [see section 3.4]
- What permissions are given to a device and does it – and potentially its data – need to be treated differently to other devices? [see section 3.4.1]
- What information about the home or residents does the data provide, what is the relation to sensitive or personal information, and where is the data best managed? [see sections 3.3.1, 3.3.3]
- What should be considered when decommissioning devices or transferring device ownership, for instance when moving houses, changing tenants or updating the home with new IoT solutions? [see section 3.5.4]
- What is the capacity of Home IoT administrators to support a secure IoT ecosystem and what should be automatically managed by the Hub and/or solution provider? [see section 3.4]

Good security hygiene should be the foundation of any IoT management process. Therefore, the principles for this architecture are based in ensuring a minimum level of security across the home IoT ecosystem with minimal reliance on home IoT user and understanding where weak points or attack vectors might be located.

[3] There is a similar "CIA triad" for cryptography in which the "A" stands for Authenticity, but the form using "availability", as is done here, is typical for information security [16].

2.6.1 Threat Assessments and the Hub architecture

This Hub architecture focuses on four security management features identified to support these security principles. The security management tools at the core of this architecture are:

- Network Management
- Connecting Devices Securely
- Device Lifecycle Management
- Information Security Best Practices

Below is a table which highlights how this reference architecture can help a home safeguard against some computer security threats and support solution provider compliance measures. A more detailed table can be found in Appendix A. The examples focus on the exploitation of connected systems and are organized using the widely-known STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) threat classification model. However, these are not the only threats to a home IoT environment, nor is it the only threat or risk model available. Other examples include: PASTA, VAST, Trike, NIST's Cyber Security Framework, NCSC's Risk Management Guidance, ISO/IEC 27000 series (particularly those on information security risk management), and OWASP (application security). A solution provider should select the most appropriate model when executing an assessment.

Threat	Threat Example	Treatment Examples	Hub Architecture Treatment Correlation
Spoofing	Sending spoofed packets to influence the functioning of a device (e.g. stop, start, or modify data collection and transfer)	Implementing gateways and firewalls to identify suspicious traffic Update and patch devices to prevent vulnerability exploitation	Gateways and Firewalls [3.3.2] Update and Patch [3.5.3]
Tampering	Tampering with software to modify permissions, install spyware or malware	Secure management of access controls Secure boot and update to ensure software and hardware are modified only by trusted sources Monitor device status and traffic flow to identify unauthorized activities	Authentication and authorization [3.4.1] Secure Boot [3.4.2] Monitoring [3.5.1]
Repudiation	Device A receives a command seemingly from Device B but it was sent actually by an unknown source and leads to malfunction such as smart door lock failure	Use roots of trust to support non-repudiation Use of digital certificates to support secure identity of users and devices	Roots of Trust [3.4.3] Manage Device Identity and Authorization [3.5.4]
Information Disclosure (Data Breach)	Password leaks or unauthorized password/credential	Separating home and IoT networks Monitor traffic on and	Local IoT Network [3.3.1] Gateways and

	modification	outside of the local IoT network Encryption of data	Firewalls [3.3.2] Roots of Trust [3.4.3] Monitoring [3.5.1]
Denial of Service	Exploiting connected devices to execute a DoS or DDoS attack on a third-party network or site	Use of gateways and firewalls to manage, monitor and block traffic Restricting access to command/control functions of devices Taking compromised and irreparable devices out of the home IoT ecosystem securely	Gateways and Firewalls [3.3.2] Monitoring [3.5.1] Manage Device Identity and Authorization [3.5.4] Managing Device End-of-Life [3.5.5]
Elevation of Privilege	Unauthorized access of a cloud service provider's system enabling access to the home networks	Separation of home IoT and user networks to discourage privileged users from accessing non-relevant home information	Local IoT Network [3.3.1] Authentication and authorization [3.4.1] Monitoring [3.5.1]
Unsupported Endpoint Management	Out of date devices with known exploits or bugs being exploited to access IoT networks or devices	Create a secure environment for devices - separate devices from home user networks Monitor data traffic and enable alerts for suspicious traffic Physically manage updates or push updates where possible	Local IoT Network[3.3.1] Gateways and Firewalls [3.3.2] Monitoring [3.5.1] Update and Patch[3.5.3]

Table 1: Threat Treatment and Architecture Correlation

In addition to the above security threats, solution providers must also manage risk associated with regulatory compliance of home IoT solutions. Adopting a security-minded development and business model can supplement a solution provider's unique selling point by helping prove a provider's compliance with regulations or good practices and reduce risk or liability in the event of a security breach. As shown in the table below, this security-minded Hub architecture supports regulatory compliance by offering solutions to ensure minimum security at every level – from IoT device to network – and provides a central point of information aggregation.

Threat	Threat example	Treatment examples	Hub architecture treatment correlation
Service Provider Regulatory non-compliance	Lack of easily applied metrics to measure IoT solution compliance or identify security shortfalls	Log and report on security features and ecosystem management Enable security best practices Identify, manage, and update regulation compliance measures	Highly dependent on regulatory requirements. Common examples are: Gateways and Firewalls[3.3.2] Authentication and authorization[3.4.1] Monitoring [3.5.1]

Table 2: Regulatory Compliance

2.6.2 A Note on Information Security Best Practices

A variety of guidance exists on information security best practices and is not detailed in this architecture (see recommendations below). However, information security best practices need to be integrated into IoT solutions by the providers, be structured in a way that best meets the needs of the home, and comply with relevant regulations such as local data protection and privacy regulations.

Because many IoT solutions are wholly or in part provided via a cloud-based service it is important to note that an IoT solution provider[4] has a responsibility to assess risks associated with data transfers outside the home and between jurisdictions. This may include home operational data (such as door lock encryption keys, PIN codes and status), sensor data (such as lights and temperature), user data (such as a TV viewer profile or hands-free home assistant interaction data), or other types of data which provide information about the home and its occupants. Data which is sensitive or personal in nature may require additional levels of security and data protection compliance measures or data protection safeguards to be put in place by the service provider such as encrypting smart device communications. Some occupants may desire more hands-on management of the type of data that is collected, transferred or analysed by service providers. Risks associated with external and/or internal data management will be unique to the home and IoT ecosystem, therefore no assumptions are made here about a home's chosen solution.

Information security best practices should be incorporated throughout the IoT system where necessary, for example:

- Data security at rest and in transit
- User authentication and access privileges
- Securing sensitive information (e.g. keys and certificate management)
- Protection against re-identification of anonymized or pseudo-anonymized information

[4] Here, an IoT solution provider is an OEM, Service Provider, or anyone with responsibilities for architecting, designing, planning and procuring Consumer IoT products.

For these reasons there is not a dedicated information security section of this Hub architecture. However, relevant information on this topic is provided where needed.

For more information on this topic specifically, IoT solution providers can consult a range of resources regarding information security standards and best practices made publicly available through independent organizations, standards bodies, and national governments including IoT Security Foundation, ISO, BSI, NIST, and NCSC.

3 Hub-Based Reference Architecture

3.1 Introduction

This section provides a brief overview of the Hub-based reference architecture. Cyber security principles are the foundation of this work, in particular the DCMS "Secure by Design report" section 4.5 [ref 7] and the IoTSF's "Application Note: Mapping the IoT Security Foundation's Compliance Framework to the DCMS proposed Code of Practice for Security in Consumer IoT" [ref 8]. Supporting these principles and enabling easy implementation and control is a primary aim of the Hub architecture which provides a device management point.

The extent to which the Hub provides monitoring and controls depends on the relevant IoT solutions, home structure, and specific implementation of this architecture. The architecture presented here is meant to be a resource which outlines key security considerations, and how a Hub may act as a central information repository, assist IoT deployment and enable long-term management.

This blueprint offers a high-level architectural design as a reference model for home Hub OEMs, IoT service providers and retailers. It does not prescribe or presume certain protocols or solutions, but some reasonable assumptions have been made about the number of connected devices, their physical constraints and the "character" of such devices and networks (e.g. if one person sets up the network, or multiple people have admin rights for different parts of the system). This technology-agnostic approach enables the blueprint to be applied to a wide-range of systems with such constraints.

3.1.1 Hub Architecture Solutions

At the centre of this architecture is a Hub that, as described here, is not yet on the market. Nevertheless, there are IoT management solutions (or hubs) currently available in the marketplace that incorporate different aspects of this architecture, but none have all the desired features described here. With the IoT market rapidly developing, there is a lack of leading internationally recognized standards and user-friendly IoT solution interoperability supporting the management and integration of multi-vendor IoT devices into the home. It is desired that a Hub solution be developed to address this gap in the market.

In the meantime, solution providers should be able to identify and communicate to home consumers the primary IoT and security management features offered by a given IoT solution. Additionally, providers should be able to back up any claims. Adoption of a certification or conformity assessment scheme is one manner of ensuring and showing products have implemented security best practices. One method solution providers may use to do this is utilising the Hub architecture presented here in conjunction with a security framework, such as IoTSF's Security Compliance Framework [ref 1], and a comprehensive risk assessment. Information about security treatments and risks that can be utilised for certification or conformity assessment schemes. Successful assessments may then be used in consumer-focused marketing materials. With this information, home occupiers may then identify those available market solutions that are best suited for their home IoT deployment.

3.2 Example of Hub-Based Architecture

The Hub architecture is elaborated here through five elements. The first is a visualization of the Hub architecture and illustrates how the Hub is connected to other devices and security features on the network.

This is followed by three key processes and their security considerations identified for IoT solution implementation and management, consisting of:

- Network Management
- Connecting Devices
- Lifecycle Management

Lastly, there is a brief overview of security considerations for the Hub itself, including device and software security.

3.2.1 Example of Home Hub-Based Architecture Components

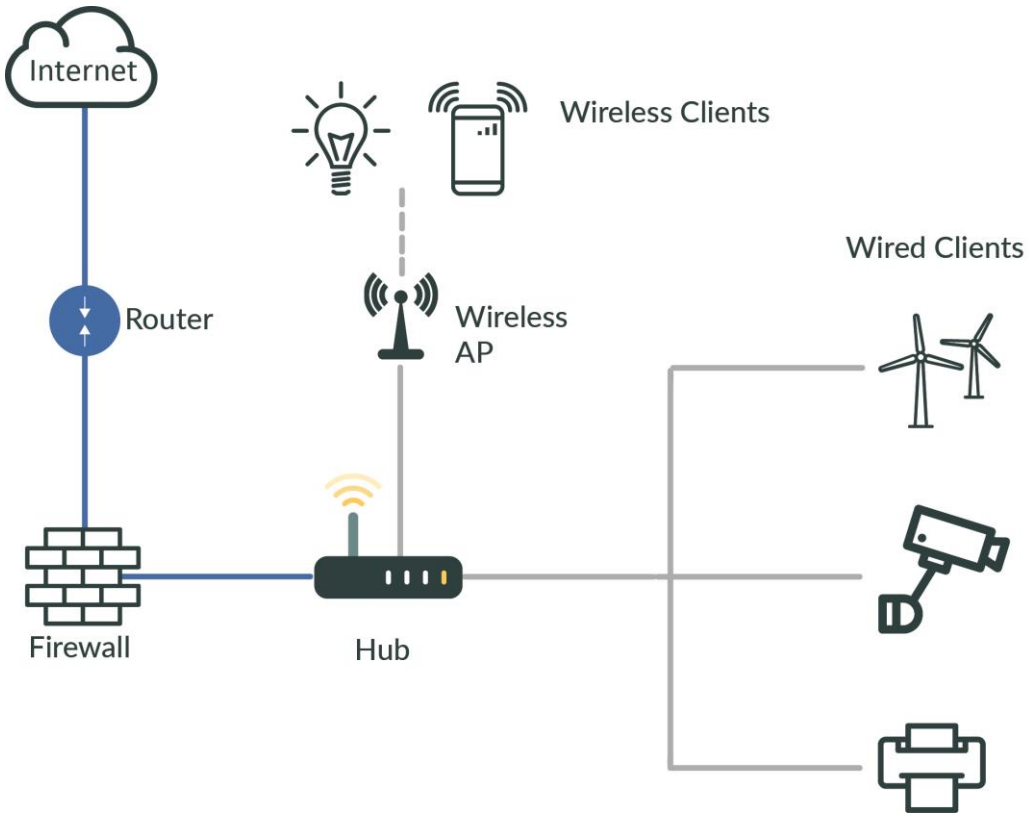

Figure 2: Example Hub Architecture

The visualization in **Figure 2** above shows the multi-layered communication structure within a home IoT environment, and reflects the complex communication structure between devices, networks and the central Hub. The functions of the router and firewall are shown separately but could also be incorporated in the Hub along with other network functions, particularly for those intended for homes with fewer devices. The **local IoT network** (grey lines) is dedicated to IoT devices and separated from the home's "IT" network. **Devices** (linked by grey lines) use this network to talk between themselves, to the Hub and possibly with external elements via a Hub gateway. **The Hub** is at the center of the IoT ecosystem as it aggregates information and communicates with other architectural elements such as devices and local networks. At the same time, the Hub can act via its connection to the firewall (blue line) as a gateway to external or other home networks as needed.

3.3 Network Management

3.3.1 Local IoT Network

Homes function in a variety of network settings. For this architecture, it is considered best practice to have one dedicated network for IoT devices using local internet connections (e.g. home Broadband and Wi-Fi). A Hub may support this by partitioning the home "IT" network (e.g. used for internet browsing). The "local IoT network" and is considered to offer an extra layer of security to both the devices and home via separation of IoT device functions from the home "IT" network in case of a security breach or malfunction. However, it may be that not all Hubs provide network segmentation and it is understood that not all homes will have the capability to set up and manage two local networks. With this in mind, security measures should be built into IoT solutions to accommodate a variety of network architectures while delivering a good level of security.

The recommendations provided below are in order of increasing security, but not necessity. IoT solution providers should take into consideration the variety of home IoT architectures and user abilities when developing Hub and IoT solutions for the home market. For example, solution providers should execute risk assessments and review security requirements to identifying the most desirable Hub features that will maximize security while reducing demand on the end user.

3.3.1.1 Recommendations

- The local IoT network should create an environment dedicated to IoT devices and communications
- The local IoT network should be separate from the home user "IT" network

3.3.1.2 Hub attributes

- The Hub should act as a gateway between the IoT network and other networks
- The Hub should minimize the attack surface, identify and address threat vectors
- The Hub may have the capability to enable and manage network partitioning
- The Hub may have the capability to move existing home IoT devices onto the new local IoT network

3.3.2 Gateways and Firewalls

A gateway is a hardware device that acts as a "gate" between two networks. The gateway function may be incorporated into a home Hub, particularly a router, firewall or other device that controls the ingress and egress of traffic in and out of the network.

By the Hub acting as a "gate" between two networks it is considered to be inevitably at the edge of a network since all the external network traffic must pass through it. Apart from acting as a gate it may also provide protocol conversion, translating connections from the external network into protocols compatible with those supported by devices within the internal network.

A firewall is a more advanced type of gateway, which inspects and filters inbound and outbound network traffic and, where necessary, prevents connections being made with suspicious or unauthorized sources. A further evolution of the firewall that allows application layer (seven) filtering which in turn permits URL level traffic filtering.

The recommendations provided below are in order of increasing security, but not necessity. IoT solution providers should take into consideration the variety of home IoT architectures and user abilities when developing Hub and IoT solutions for the home market. For example, solution providers should execute risk assessments and review security requirements to identifying the most desirable Hub features that will maximize security while reducing demand on the end user.

3.3.2.1 Recommendations

- The home should be able to implement best practice network security through user-friendly firewalls and gateways to protect networks and data flows
- The home gateway or firewall should enable traffic segmentation and routing
- The home gateway or firewall should enable traffic monitoring

3.3.2.2 Hub attributes

- The Hub should act as a gateway to other local home and/or external networks
- The Hub should act as a central point for monitoring local IoT network gateways and firewalls
- The Hub should act as a central point for monitoring network traffic which may also be used for intrusion detection
- The Hub should offer alert and notification to the appropriate party (e.g. service provider or home user) in the event of anomalies
- The Hub or its service provider should provide updates and patches for the firewall software

3.4 Connecting Devices Securely

3.4.1 Authentication and authorization

The secure authentication of an IoT device's identity and its software is critical to ensuring that only approved and trusted devices are deployed into the home. Authentication is the process of verifying that a thing (or person) is what it claims to be or that data has come from the source claimed as its origin. Authenticating a device verifies its identity and/or attributes of the device. Once authenticated, the device can be authorized to function on the network by an authorization manager such as the home IoT administrator.

The home Hub should provide authentication and authorization tools. This may include processes that run automatically, such as validating software, or user-friendly tools such as whitelisting and revoking privileges. In order for successful authentication and authorization in a mixed-vendor environment (i.e. for the home IoT administrator to not be constrained by vendor or ecosystem lock-in) devices need to be interoperable and support internationally recognized standards. Whilst standardization is still in its infancy, there are initiatives in this area, an example is the IETF draft on the remote bootstrapping of PKI credentials [ref 19]. Solving issues of interoperability is not a primary aim of this document, but should be a key consideration for OEMs developing and implementing these hub architectures for the Home IoT. Particular areas that need standardization are:

- Protocol or protocols for IoT devices and hubs which support:
    - Trusted software update which allows the option of a hub to act as a broker between manufacturer and device, particularly within a heterogeneous environment of multiple manufacturers and their devices.
    - IoT device secure credential dissemination which can be authenticated by the Hub or Hubs.
    - A Hub being able to enumerate IoT devices and establish their state in a safe and secure way.
- A common method of describing detected security events acting on an IoT device.

Authentication supports other good security practices such as authorization and non-repudiation. Non-repudiation is "the ability to prove that a person, entity or process cannot deny having carried out an action" [ref 9]. Authorization grants permissions to the device, such as network access and associated parameters. Permissions can be taken away from specific devices, for instance at end-of-life or in the event of ownership transfer. This is particularly important because in a home environment, ownership may transfer for a variety of reasons, such as when home owners or occupants change and inherit IoT solutions or Hubs integrated into the house.

Unlike traditional IT equipment which has either a human interface or a standards-based interface used to configure and load trust credentials, IoT devices are typically "headless". As a result, the installation of the trust

credentials to allow the device(s) and the home's network to authenticate each other represent a challenge to scalable deployment. In the case of network access this can be problematic for a home when a device expects its wireless configuration to be carried out over a local wireless interface and involves the sharing of the home's wireless credentials to the device.

Throughout the lifecycle of an IoT device, authentication and authorization will be used repeatedly to verify and manage devices, including assigning and revoking privileges. The ability to manage authentication and authorization must be user-friendly and accessible by consumers with a range of capabilities. Managing authentication and authorization may be done remotely by the IoT solution provider, automatically via a device, or locally by the home user. It is important that management is clearly defined for users and IoT solution providers as authentication and authorization form a foundation for additional security layers such as those listed below (in order of increasing security, but not necessity).

- **Device identity management** – the ability to identify a device or group of devices, enabling actions such as authorization and privilege management
- **Black or whitelisting** – verifying only desired (e.g. authenticated) devices access the network by managing access or privilege control tools (e.g. granting authorization, and ensuring that the devices shall interact only with trusted servers)
- **Granting privileges** – authorizing access or actions based on attributes (e.g. allowing devices connected using a "visitor profile" access to a smart printer, but not the home IoT network)
- **Revoking privileges** – removing or preventing a privilege based on attributes (e.g. removing authorization to access the Hub system from a decommissioned smart light solution which is installed in the home but no longer in use)
- **Roots of Trust** – use of trust-building tools, such as certificates or encryption, to provide a trust foundation in the IoT system (e.g. using certificate authorities to authenticate devices, providing a trust store)
- **Validating software updates** – with the use of digital signatures and/or encryption based upon a suitable root of trust to validate that the software update is from an authentic source, typically the product's OEM or authorized software provider (e.g. use of public key pinning for websites where updates are retrieved).

In a home environment, a Hub may need to seamlessly manage elements of authentication and authorization without user intervention – such as identifying and logging devices, validating updates, or managing certificates. For this reason, it is important that the Hub is able to aggregate information from a variety of sources (e.g. IoT solution provider, devices, and home user). It may also have default settings for granting privileges with override functions for more technologically adept home users. In a home environment, a hub should not only be flexible with regard to technology or architectures, but also with home user ability level.

The recommendations provided below are in order of increasing security, but not necessity. IoT solution providers should take into consideration the variety of home IoT architectures and user abilities when developing Hub and IoT solutions for the home market. For example, solution providers should execute risk assessments and review security requirements to identifying the most desirable Hub features that will maximize security while reducing demand on the end user.

3.4.1.1 Recommendations

- Home IoT solutions should support cryptographically based credential device authentication to ensure only known devices are allowed on the network and support ongoing trust between devices
- Provide user-friendly authorization management advice for home users to assist in determining and/or assigning a device's privileges such as accessing the local IoT network, routing, and blocking or enabling data transfers
- Support the ability to remotely and/or locally revoke authentication and/or authorization to decommission devices or transfer home IoT administrators. Remote or local management will be influenced by the IoT solution provider model and the regulatory implications of legislation like GDPR
- The Hub should support user authentication and authorization. It should enable user profiles and access privileges, such as the home IoT administrator, adult users, visitors, etc.

3.4.1.2 Hub attributes

- The Hub should be a central point for supporting authentication. It may:
    - Carry out authentication processes automatically or with user support
    - Act as a cache for authenticated devices
    - Store authentication credentials
    - Support varying levels of authentication (e.g. single token, server, and mutual authentication)
- The Hub should be a central point for supporting authorization. It may:
    - Act as a device management tool to apply or revoke privileges
    - Support creation and enforcement of permissions lists (e.g. blacklists and whitelists)
    - Support trusted device/group identity management
- The Hub should provide alerts if an authenticated device has been tampered, its authorization privileges have been modified, or is trying to execute unauthorized actions
- A Hub should use at minimum best practices in password and cryptography systems to support authentication and authorization processes
- A Hub should take into consideration the extent to which certain authorization and authentication functions can and should be automated to reduce reliance on home user capabilities
- A Hub should support communications with a variety of authorized sources – such as IoT solutions providers – as appropriate to enable necessary information aggregation (e.g. for revoking authentication of a device)

3.4.2 Secure Boot

Secure boot is the process through which the device validates the integrity of the software from boot time onwards. The Hub device should have a secure boot function and may also be able to log when an IoT device has completed a secure boot. Secure boot will not be managed by the home IoT administrator but should be inherent to the Hub. The hub shall have one of the three levels of secure boot types, listed below in increasing level of security:

- **Secure Boot**: The device verifies that its bootloader is correctly digitally signed and that no changes have been made to the firmware
- **Trusted Boot**: The device's bootloader checks the digital signature of the operating system and the operating system checks the integrity of every component of the startup process before loading it
- **Measured Boot**: The device's firmware logs the boot process metrics including the Operating System boot and securely sends the metrics to a trusted server that can attest to the trustworthiness of the device

In smaller embedded systems the Secure Boot and Trusted Boot may involve the use of a microcontroller or microprocessor that starts executing software from internal and immutable memory. The software stored in the immutable memory in the microcontroller is considered inherently trusted (i.e., the root of trust) because it cannot be modified. This inherently trusted software then authenticates the software, such as the operating system, not stored in immutable memory, through a cryptographic process such as digital signing or decryption, using a root of trust stored securely within the microcontroller/processor.

The recommendations provided below are in order of increasing security, but not necessity. IoT solution providers should take into consideration the variety of home IoT architectures and user abilities when developing Hub and IoT solutions for the consumer home market. For example, solution providers should execute risk assessments and review security requirements to identifying the most desirable Hub features that will maximize security while reducing demand on the end user.

3.4.2.1 Recommendations

- Home Hub solutions support secure boot to ensure that their integrity cannot be compromised and that only software authorized by the Hub service provider can be deployed onto them

- Home Hubs have the ability to revoke authentication and/or authorization to enable the secure decommissioning of Hubs or transfer Hub ownership
- Secure boot should be an automatic function which relies on minimal home user oversight

3.4.2.2 Hub Attributes

- The Hub should provide alerts if an attempt is made to install unauthenticated software or the Hub has been tampered, authorization privileges have been modified, or is trying to execute unauthorized actions
- A Hub should use at minimum best practices in roots of trust and sources of entropy, for its cryptography systems to ensure support for secure authentication and authorization processes. For further details on this best practice subject please see in the IoTSF "Best Practice Guidelines for Connected Consumer Products" [ref 21]

3.4.3 Roots of Trust

Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. By design, roots of trust must be highly secure since they are used as a fundamental trust anchor. To prevent tampering or extraction of their contents, roots of trust are normally implemented in hardware to provide a strong trust foundation.

On a device (e.g. the Hub) there will at a minimum two roots of trust, one for the trust anchor for the devices identity and the other, the trust anchor used to authenticate the device's software. The later trust anchor being used for authenticating the software on the device or for software updates subsequently delivered to the device. Other potential roots of trust would be for the authentication of any user or application interfaces. The Hub should support industry standards in cryptography and automatically securely store those roots of trust. The home IoT administrator should not have to manage the roots of trust, since public roots of trust are likely provided and managed by the IoT OEM or service provider. Whereas because of the scalability and deployment issues, private roots of trust set up and management by the home IoT administrator are unlikely.

Roots of trust are at the core of this Hub-based architecture because the Hub acts as a central trust anchor and management tool, deciding which devices or network infrastructure to trust. Without a root of trust, particularly public roots of trust, this is a difficult problem to solve. Public roots of trust are considered a more secure and practical solution than private roots of trust in the home context, especially where multiple vendors' products are expected to interwork. Private roots of trust may be suitable for OEM products where communications are within the OEMs or Service Provider's ecosystem and the private roots are managed by the OEM or service provider but not the home user.

If private roots are considered for a particular home IoT deployment, please see the reference documents 4, 12 & 18 for further background.

As their name implies, public roots of trust are ones which are publicly accessible and allow third parties to authenticate each other without prior credential exchange. Embedding public roots of trust where possible helps circumvent issues presented by private roots – such as scalability and cross-vendor applicability – and supports a long-term approach to treating risks associated with Home IoT deployments. Public roots of trust are also better positioned to support other needs such as interoperability.

The recommendations provided below are in order of increasing security, but not necessity. IoT solution providers should take into consideration the variety of home IoT architectures and user abilities when developing Hub and IoT solutions for the consumer home market. For example, solution providers should execute risk assessments and review security requirements to identifying the most desirable Hub features that will maximize security while reducing demand on the end user.

3.4.3.1 Recommendations

- Implementations should support best practices in roots of trust [see refs 4 and 12]
- Roots of trust should be utilized to support authentication and authorization processes
- Roots of trust may be used to support identification of malicious software
- Implementations may be automatic and should not require home user management or technical knowledge
- Roots of trust should be immutable, meaning they cannot be tampered with

3.4.3.2 Hub Attributes

- The Hub shall support the cryptographic hashing and encryption/decryption functions used in the authentication of chains of trust, in particular:
    - a Hub shall support industry standards in cryptography
    - a Hub should support best practices in cryptography [see ref 1].
    - the Hub shall have a hardware root of trust
- The Hub should have the ability to manage private OEM or service provider roots of trust from vendors as needed
- The Hub should be able to support public roots of trust
- The Hub should securely store and/or cache roots of trust
- The Hub may enable roots of trust by acting as an intermediary between device and certificate authority
- The Hub should provide a cryptographically secure method to update and revoke its cryptographic keys, including those keys used for the authentication of updates.
- The Hub may use roots of trust to assist detection of malicious software

3.5 Lifecycle Management

3.5.1 Monitoring

Monitoring of IoT ecosystem devices, networks, resources, and performance is a key element of IoT security. Information and measures resulting from monitoring can be aggregated in a centralized location for better IoT ecosystem visibility and control. A Hub acts as a central repository of information for either the home IoT administrator or solution provider regarding the functioning and statuses of the IoT ecosystem and can be used to inform resulting actions. The home IoT administrator will be able to take necessary action – from contacting a solution provider to taking a device offline – and take informed decisions based on what is learned from the Hub's monitoring and logging tools, particularly with the rapid development of machine learning and data analytics. This includes aggregation of information from other security tools such as firewalls, gateways, and network access controls. These tools may or may not be directly managed from the Hub, however, they may share information such as:

- **Notifications** – A notification is information delivered by the system to the home IoT user and/or administrator as appropriate. This could include push notifications (such as an unexpected incident alert notification) or pull notifications (such as requested status updates). Notifications support security by providing essential information to the home IoT administrator on events and incidents in the ecosystem enabling the administrator to respond appropriately.

- **Alerts** - An alert is a type of notification that is important or time sensitive. For instance, alerts can support IoT security via timely notification, and thus response, when incidents are detected in the IoT ecosystem.

- **Status updates** – Status updates are a type of notification that provide the ability for home IoT administrators to determine the status of an IoT device or network at any given time, such as device status (e.g. on/off, in use/not in use), or software update/ patch status. Status updates support security by contributing to the overall snapshot of IoT ecosystem statuses, health, and security management processes.

- **Report** – A report, such as an incident report or system snapshot, can include historic and current information such as time/date stamps, impacted networks and devices, taken or scheduled actions. Reporting provides an understanding of events and may also assist in communicating problems to third parties such as solutions providers or other tech support resources. A report mechanism can also demonstrate the IoT solution provider's compliance with local and industry-specific regulations.

  IoT solution providers should provide clear and simple information to consumers about data use so that users understand what data is being collected and reported about them. This is particularly important for information that is shared outside the home user's internal system (e.g. to the IoT service provider or their supported platform). Reporting home data can be more invasive than other environments (such as an Enterprise) and may include sensitive personal data.

The recommendations provided below are in order of increasing security, but not necessity. IoT solution providers should take into consideration the variety of home IoT architectures and user abilities when developing Hub and IoT solutions for the consumer home market. For example, solution providers should execute risk assessments and review security requirements to identifying the most desirable Hub features that will maximize security while reducing demand on the end user.

3.5.1.1 Recommendations

- A Home should have tools for monitoring its IoT ecosystem, which supports troubleshooting, checking network health, tracking data flows, and demonstrating policy compliance. This may include:
  - Monitoring devices
  - Monitoring networks and Hubs
  - Monitoring traffic flows
  - Raising alerts and notifications when an event is detected
- A home should have a central location to review alerts, notifications, or reports resulting from monitoring
- Monitoring should be provided in a user-friendly manner to the home administrator to the extent needed to manage the home environment and comply with applicable local market regulations, e.g. in the USA the 'Children's Online Privacy Protection Rule' ("COPPA") [ref 17]. This may include information such as:
  - Metrics on resource consumption (e.g. power)
  - Data transfer and flows (e.g. identification and communication of what information is leaving the home environment and communication of this to the home user in a user-friendly manner)
  - Access requests and logs
  - Changes to device and network parameters
  - Temporary devices and associated actions
- Information shared outside the home environment (e.g. with the IoT solution provider) for monitoring purposes should be personally non-identifiable and users must have the option to disable any sharing.

3.5.1.2 Hub Attributes

- The Hub should enable monitoring. This may be done continuously, be time-constrained or be done routinely
- Information collected to should be non-identifiable to the extent possible when kept in the home environment, and no personally identifiable information should be shared outside the home
- The Hub should provide reporting tools for monitoring, this may include:
  - A user-friendly log of monitoring activity
  - Information about data transfers outside the home environment
  - Access to past reports
  - Query options
- Following monitoring, the Hub should provide alerts or notifications of relevant information such as incidents or measures outside set parameters

- As a result of monitoring, the Hub should enable the home IoT administrator or Service Provider administrator to take necessary actions either directly via the Hub or outside the Hub. This may include actions such as:
    - Controlling traffic flows and segmentation
    - Implementing anti-virus/malware solutions
    - Pushing updates or patches to devices
    - Contacting IoT solution providers or technical support
    - Suggested actions as a result of monitoring
- Hubs supporting roots of trust should be able to report and update roots as necessary
- Where logging is provided, only local home administrators shall have the ability to delete log information. Administrative functions available externally to the home (e.g. on a smart phone) shall not have the ability to delete logging information

3.5.2 Troubleshooting

Should an issue or anomaly in the IoT ecosystem be detected, it is assumed most Home IoT users are unlikely to determine the exact nature and location of the problem or how to resolve it. This is due in part to the complexity of IoT deployments, but more importantly due to the fact that most home users will not have the range of technical knowledge and capability.

Subsequently, a troubleshooting mechanism that can run remediation steps on the home's IoT ecosystem, is an important tool for detecting as well as resolving security issues in a home IoT environment. The Hub should facilitate basic troubleshooting, recommendations and resources for the home users and support the cooperation between the home user and relevant IoT service providers to resolve issues in the IoT environment.

The recommendations provided below are in order of increasing security, but not necessity. IoT solution providers should take into consideration the variety of home IoT architectures and user abilities when developing Hub and IoT solutions for the consumer home market. For example, solution providers should execute risk assessments and review security requirements to identifying the most desirable Hub features that will maximize security while reducing demand on the end user.

3.5.2.1 Recommendations

- The troubleshooting functions can be initiated by the home administrator or the relevant IoT service provider
- The troubleshooting function should be auto-enabled when a fault is detected
- The function should identify the fault, error or problem in the home IoT environment and report this information to the appropriate administrator, be that the home administrator or the Service Provider's
- Results of troubleshooting function may be shared with Home IoT users and/or solution providers as appropriate
- The troubleshooting function should determine possible courses of action to resolve the fault and report this information to the appropriate administrator
- The troubleshooting function should enable home IoT or Service Provider's administrators to resolve the issue(s) with as simpler a process as possible, ideally largely automatically

3.5.2.2 Hub Attributes

- The Hub should provide a troubleshooting function which has the ability to report issues
- The Hub should assist the home IoT or the Service Provider's administrator to resolve the issue, such as pushing updates to IoT or decommissioning devices
- The Hub may be able to provide troubleshoot results to the home IoT administrator and/or solution provider as appropriate

- The Hub may allow a third party to take actions such as access, control and make changes, but only with a positive per instance acceptance of such a request from the home IoT administrator

3.5.3 Update and Patch

A simple but configurable way of securely updating and patching across the IoT ecosystem is an important aspect of IoT security. Updating and patching helps to protect against known threats, fix security vulnerabilities, protect against bugs and improve performance. home IoT administrators should be able to have a central point of reference for related information such as:

- Completed updates
- Scheduled updates
- Update source
- Update verification

Implementing reliable mechanisms for tracking and implementing updates supports the integrity, privacy and security of the IoT ecosystem and helps to enable interoperability.

The recommendations provided below are in order of increasing security, but not necessity. IoT solution providers should take into consideration the variety of home IoT architectures and user abilities when developing Hub and IoT solutions for the consumer home market. For example, solution providers should execute risk assessments and review security requirements to identifying the most desirable Hub features that will maximize security while reducing demand on the end user.

3.5.3.1 Recommendations

- IoT devices should support software and firmware updates and patching from necessary sources (e.g. home IoT administrator, solution provider or manufacturer-pushed)
- Automatic update functions should be default enabled to reduce the burden placed on home IoT users to manage updates and patches
- Home IoT administrators should have the option to schedule, manually start, and decline updates
- The home IoT administrator should be able to log updates/patches and create related reports
- Update mechanisms should include secure boots and regular reboots for devices, such as code signing to verify updates
- Update roll back attacks should be prevented by design

3.5.3.2 Hub Attributes

- The Hub should keep an update/patch log with reporting capabilities, for example:
    - The Hub should log information regarding past and future updates such as time stamps or scheduled updates
    - The Hub should log information about update provenance and verification
    - The Hub should support automatic and manual input
- The Hub should be able to manage updates and patching centrally to the extent possible, for example:
    - The Hub may be able to cache updates for IoT devices
    - The Hub should support devices with limited or intermittent connectivity and multi-part updates
    - The Hub should support automatic and manual initiation of updates
    - The Hub should be able to manage updates from a variety of sources (e.g. home IoT administrator- and manufacturer-pushed)
- The Hub itself should be kept as up to date as possible as it provides a high level of security to the IoT ecosystem and management
    - The Hub should be easy to update
    - The Hub should be able to monitor, and report its update and patch status
    - The Hub should be able to auto-update

3.5.4 Manage Device Identity and Authorization

Device identity solutions are not a primary focus of this proposed Hub architecture. However, it is worth noting that identity has an important role in supporting security functions enabled by this Hub architecture – such as authentication, roots of trust, and device lifecycle management. For instance, identifying a device can support assigning or revoking device privileges and make tracking and implementing updates easier.

In a home IoT environment there may be a variety of identity schemes from IoT and Hub solution providers. The specific technologies, services, or other resources that may be used to assign and/or manage device identity is not within the scope of this proposed Hub architecture. No identity solution or management tool is presumed or prescribed here. There are a range of solutions, both available and developing, that can be successfully used in IoT deployment.

In addition, there may be situations when sharing or assigning a device identity may not be desired by either party, for instance personal devices brought onto the home IoT network by guests, such as smart watches or fitness trackers. Personally identifiable information, particularly that which is not required for IoT functions, is not in scope of this paper and should be handled in a manner consistent with local data protection and privacy policies.

Taking this into consideration, in an IoT ecosystem, it should be possible to assign identity to all devices or groups of devices as appropriate. Identity may be provided via a variety of resources including, but not restricted to:

- Manufacturers
- Private and bespoke identity schemes
- Third party solutions or services
- Hub solutions

A Hub should be interoperable with a variety of proprietary and open identity schemes which, among other benefits, should not unduly restrict consumer choice in the IoT marketplace and, should ideally, implement those schemes with minimal effort by the home IoT administrator. A Hub may:

- Improve overall IoT ecosystem management and security
- Provide a centralized database for device and/or identity management
- Provide flexibility to assign a device to one or multiple groups
- Provide flexibility to assign attributes and authorizations to a device and/or group of devices

3.5.5 Managing Device End-of-Life

An IoT device's lifetime can be unique to each deployment. For an IoT device, the end of life will most likely be the result of a number of factors, including but not limited to:

- Manufacturer end-of-sale or support (such as discontinuing updates and patches)
- Home upgrade or solution change – including integrating new devices and decommissioning old devices
- Change of ownership, where a home user may inherit or transfer ownership of IoT systems (for example in the case of changing home ownership or occupancy)

Security practices included in this architecture support good practices for end-of-life management. For instance, there are several security practices that need to be considered when managing end-of-life, including but not limited to:

- Managing permissions and revoking authorization
- Understanding what home information is accessible by the device and removing/protecting this data
- Data erasure – permanent deletion of any settings, user account information etc.

- Decommissioning or transferring device identity
- Precautions for transferring device ownership, such as data erasure, factory re-set, etc.

A Hub architecture provides a central location to query information about the device, its authenticity, authorizations, network access and in some cases to execute the necessary actions to revoke permissions and decommission a device and/or the Hub itself from the IoT ecosystem.

3.6 Hub Device Security

In the end, the Hub architecture provided here is based on a central device and user interface at the middle of the home IoT ecosystem. Because the Hub is designed to be a foundational element of the home's IoT security, the Hub itself must include robust security. This includes features such as:

- User access permissions that support best practices in system and information security (for example a home IoT administrator profile versus child or guest users)
- Ability to securely store sensitive information such as roots of trust
- Alerts and notification of anomalies
- Security considerations for web and mobile user interfaces as well as network connections
- Secure Boot
- Troubleshooting and auto-fix capabilities
- FAQ or "help" resources to guide users in the case of errors or anomalies. This may include actions such as executing troubleshooting and auto-fix capabilities, contacting the IoT service provider, Hub provider, or other appropriate resource
- Strong physical attributes to protect against unfavorable home environments (e.g. heat and moister in a kitchen)

Although there is a lack of public resources for home users on IoT security best practices, there are public resources available that help developers implement security best practices into their IoT solutions. One example is the "IoT Security Compliance Framework" [ref 1] by the IoT Security Foundation. In this document, security compliance frameworks are laid out for a range of topics related to the four main Hub functions and support capabilities included in this proposed Hub architecture. The compliance framework sections are mapped to the Hub-based reference architecture below.

Hub Functions	Compliance Framework Sections
Network Management	• Cloud and network elements • Secure supply chain and production
Connecting Devices Securely	• Device wired and wireless interfaces • Authentication and authorization • Encryption and key management for hardware • Configuration
Lifecycle Management	• Device hardware and physical security • Device software • Device operating system • Device ownership transfer
Information Security	• Business security processes and responsibility • Web user interface • Mobile application • Privacy

Table 3: Compliance Framework Mapping

4 References and Abbreviations

4.1 References

The following references are used in this document:

1. IoTSF "IoT Security Compliance Framework": https://www.iotsecurityfoundation.org/best-practice-guidelines
2. IETF "Key words for use in RFCs to Indicate Requirement Levels": https://www.ietf.org/rfc/rfc2119.txt
3. NIST Computer Security Resource Center "Roots of Trust": https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust
4. NIST SP 800-57 Part 1 Rev. 4 "Recommendation for Key Management, Part 1: General" https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final
5. NIST SP800-57 Part 3 Revision 1" NIST Special Publication 800 – 57 Part 3 Revision 1 Recommendation for Key Management Part 3: Application - Specific Key Management Guidance" http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
6. FIPS PUB 140-2, Security Requirements for Cryptographic Modules http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
7. UK Government DCMS "Secure by Design report": https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
8. IoTSF "Application Note: Mapping the IoT Security Foundation's Compliance Framework to the DCMS proposed Code of Practice for Security in Consumer IoT": https://www.iotsecurityfoundation.org/wp-content/uploads/2018/03/RELEASE-DCMS_Principles_Application_Note_07_03_2018.pdf
9. ISO/IEC "Information Technology – Security techniques – Information security management systems – Overview and vocabulary: http://standards.iso.org/ittf/PubliclyAvailableStandards
10. IoTSF "Make it safe to connect: Establishing principles for Internet of Things Security": https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf
11. IoTSF "Secure Design - Best Practice Guidelines L Software Update Policy": https://www.iotsecurityfoundation.org/best-practice-guidelines
12. NCSC UK "Guidance - Provisioning and securing security certificates" https://www.ncsc.gov.uk/guidance/provisioning-and-securing-security-certificates
13. Business Insider "New survey shows consumers are wary of smart home devices invading their privacy" http://uk.businessinsider.com/survey-says-consumers-have-privacy-concerns-with-smart-home-devices-2018-4
14. Gartner "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016" https://www.gartner.com/newsroom/id/3598917
15. Computer World "Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny" https://www.computerworld.com/article/2878741/hacker-hijacks-wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html
16. Kolkowska et al., "Information Security Goals in a Swedish Hospital" in *Proceedings of IRIS 31 - 31st Information Systems Research Conference in Scandinavia*, 2008 https://www.researchgate.net/publication/252258774
17. Federal Trade Commission "Children's Online Privacy Protection Rule" ("COPPA"): https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
18. NIST Computer Security Resource Center "Guidelines on Hardware - Rooted Security in Mobile Devices (Draft)": https://csrc.nist.gov/publications/detail/sp/800-164/draft
19. IETF Bootstrapping Remote Secure Key Infrastructures (BRSKI) draft 16, June 21st 2018: https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-16
20. McKinsey "The IoT as a growth driver", March 2018: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-iot-as-a-growth-driver

21. IoTSF “Best Practice Guidelines for Connected Consumer Products”
https://www.iotsecurityfoundation.org/best-practice-guidelines

4.2 Definitions and Abbreviations

For the purposes of the present document, the following abbreviations apply:

GDPR	General Data Protection Regulation (EU) 2016/679
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
TRNG	True Random Number Generator
TBC	To Be Confirmed
TBD	To Be Determined
TLS	Transport Layer Security

Appendix A - Threat and Example Treatment Table

Threat	Threat Example	Treatment Examples	Hub Architecture Treatment Correlation
Spoofing	Sending spoofed packets to influence the functioning of a device (e.g. stop, start, or modify data collection and transfer) Home user unknowingly being directed to a spoofed website of a service provider	Implementing gateways and firewalls to identify suspicious traffic Roots of trust to support trusted identity and access Update and patch devices to prevent vulnerability exploitation Manage device identity to support a compromised devices' authorization and access privileges and end of life provisioning	Gateways and Firewalls [3.3.2] Authentication and authorization [3.4.1] Roots of Trust [3.4.3] Update and Patch [3.5.3] Manage Device Identity and Authorization [3.5.4] Managing Device End-of-Life [3.5.5]
Tampering	Covertly modifying a sensor's data sharing permissions Tampering with software to modify permissions, install spyware or malware	Secure management of access controls Secure boot and update to ensure software and hardware are modified by trusted sources Use roots of trust to support non-repudiation Monitor device status and traffic flow to identify unauthorized activities	Gateways and Firewalls [3.3.2] Authentication and authorization [3.4.1] Secure Boot[3.4.2] Roots of Trust [3.4.3] Monitoring [3.5.1]
Repudiation	Sensor data is modified in transit to the cloud service and Home metrics are affected Device A receives a command seemingly from Device B but it was sent actually by an unknown source and leads to malfunction A group of occupants share a group password/authentication process for accessing a system	Information security best practices – managing individual user access controls Use of digital certificates to support secure identity of users and devices Use of roots of trust to support non-repudiation Public key infrastructure to manage and revoke digital certificates and roots of trust	Authentication and authorization [3.4.1] Roots of Trust [3.4.3] Secure Boot[3.4.2] Manage Device Identity and Authorization [3.5.4] Managing Device End-of-Life [3.5.5]

		Secure boot and update to ensure only authorized modification of software and hardware	
Information Disclosure (Data Breach)	Unauthorized access to security cameras Password leaks or unauthorized password/credential modification Packet capture via man-in-the-middle or similar type attacks	Separating Home and IoT networks Adoption of information security management best practices Privilege-based or other fine-grain user authorization management Encryption of data Monitor and audit traffic on and outside of the local IoT network Alerts for suspicious data traffic	Local IoT Network[3.3.1] Gateways and Firewalls [3.3.2] Authentication and authorization [3.4.1] Roots of Trust [3.4.3] Monitoring [3.5.1] Manage Device Identity and Authorization [3.5.4] Managing Device End-of-Life [3.5.5]
Denial of Service	Using exploits in connected devices to disrupt normal functions of the Home's connected systems Using exploits in connected devices to execute a DoS or DDoS attack on a third-party network or site	Blocking devices from communicating outside the LAN or Home Use of gateways and firewalls to monitor, manage and block traffic Restricting access to command/control functions of devices Taking compromised and irreparable devices out of the Home IoT ecosystem securely	Local IoT Network[3.3.1] Gateways and Firewalls [3.3.2] Monitoring [3.5.1] Update and Patch [3.5.3] Manage Device Identity and Authorization [3.5.4] Managing Device End-of-Life [3.5.5]
Elevation of Privilege	A smart device zero-day exploit that allows a third party onto the LAN Unauthorized access of a cloud service provider's system enabling access to the Home networks Gaining high-level privileges which enable command and	Separation of IoT and Home user networks to discourage privileged users from accessing non-relevant information Privilege-based or other fine-grain user authorization management to prevent access to non-relevant information, controls and	Local IoT Network[3.3.1] Authentication & Authorization [3.4.1] Monitoring [3.5.1] Manage Device Identity and

	control of a thing-bot	devices Lifecycle management and decommissioning old or compromised devices	Authorization [3.5.4] Managing Device End-of-Life [3.5.5]
Unsupported Endpoint Management	Out of date devices with known exploits or bugs being exploited to access IoT networks or devices Devices with outdated software or firmware Inability to encrypt data or assign a root of trust Inability to remotely manage end-of-life	Create a secure environment for devices - separate devices from Home user networks Monitor data traffic and enable alerts for suspicious traffic Manage authorization and access to devices Physically manage updates or push updates where possible	Local IoT Network[3.3.1] Gateways and Firewalls [3.3.2] Monitoring [3.5.1] Update and Patch [3.5.3] Managing Device End-of-Life [3.5.5]

www.iotsecurityfoundation.org