SECURING THE IoT:
ASSESSING THE REQUIREMENTS FOR AN IoT SECURITY STRATEGY

REPORT BY

beecham research

Shaping the IoT future

1. INTRODUCTION

Security is critical to the success of the Internet of Things market. Successful attacks in industrial M2M have highlighted hereto hidden aspects of cyber attacks. In addition, attacks on consumer IoT in connected lighting and white goods, have demonstrated the broad capability for attacks and the rapid impact of fear on consumers as they react to perceived loss of control to cyber criminals. These issues, challenges and fears, justified or not, will have significant potential impact on market adoption of IoT technology and its ultimate success or failure.

The target users of IoT devices and associated services cover a wide range. They include "Main Street" Consumers who will consume large volumes of connected home goods, and who already are alerted to security concerns through the mainstream press; through to more technically able Professional IoT Consumers, who will integrate and maintain large scale systems. Further users include technical experts who may have significant teams available to them.

Security is fundamental in enabling the implementation of solutions for all of these user groups. It is required to enable the development, deployment and maintenance of systems in factories and in homes; it underpins the majority of the high value services to be evolved in the cloud and on devices; it is critical in assisting the management of liabilities across system implementation; and it is essential in providing a common framework to enable the growth of multi-vendor solutions. Security is therefore a critical feature of all solutions and must be considered early in the marketing and engineering cycles of devices, software and services. The consumer experience in this domain is king, and therefore security must be both tightly integrated and practically invisible to provide the best consumer experience. The threat from cyber-attackers cannot be ignored in this marketplace and governments are now working with cross-industry forums to help close the knowledge gap and define the problems we face.

This report examines the requirements for an IoT Security strategy. It starts with some important definitions, then looks at control requirements for Consumer and Industrial IoT. It assesses important considerations for IoT and, from this, draws 8 key conclusions. Finally, it provides an example of these findings being used in practice – Infineon's OPTIGA ™ Trust X, a hardware-based approach to security-by-design.

2. SECURITY IN THE BUSINESS ENVIRONMENT

Security is transitioning from a specialist technology to a level of pervasiveness and strategic importance where it is no longer sufficient for just the CSIO (Chief Security & Information Officer) and a specialist team to understand the technology. Instead security is becoming the concern of everybody in the organization from CEO down to system designers and implementers. As such it is critical that it remains accessible and understandable to a broad audience who need to understand how it works in practice.

2.1 Security Definitions

With this in mind, the following are definitions of key security terms in common use:

1. Authentication

Authentication is the act of confirming the truth of an attribute of an entity or a single piece of data. In contrast with Identification, Authentication is the process of actually confirming the Identity or confirming that data arriving or leaving is genuine.

2. Authorization

Authorization is the function of specifying access rights to resources and ensuring that any request for data or control of a system is managed within these policies. During operation, the system should use the access policies to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected), and what actions should then be taken on any disapproved access, for example logging failed requests to enable analysis of where failed events originated.

3. Availability

Availability has two definitions within the IoT domain. Firstly as with mainstream Information Assurance, the system must provide data and resources in a timely manner for a set percentage of the time (e.g. 99.99% uptime availability). Secondly in the IoT it is critical that many devices are available, or retain their critical functionality, even if the system has undergone an attack. For example a home heating system must retain core functionality even if the device's communications have been compromised.

4. Confidentiality

Confidentiality is a set functionality that limits access or places restrictions on certain types of information with the goal of preventing unauthorized access.

5. Identification

Identification is defined as allowing that a device or service can be specifically and uniquely identified without ambiguity. This may take the form of an IP address, global unique identifier, functional or capability identifiers, or data source identifiers.

6. Integrity

Integrity is a critical measure in information assurance and is defined as providing consistency or lack of corruption within an electronic system. In this context it is required that data cannot be modified without detection.

7. Non-repudiation

Non-repudiation is an aspect of authentication that enables systems to have a high level of mathematical confidence that data, including identifiers, are genuine. This allows that either a transmitting or receiving party cannot later deny the request occurred (cannot later 'repudiate') and provides data integrity around the system.

8. Root of Trust / Chain of Trust
A Root of Trust is an immutable boot process within a system based on unique identifiers, cryptographic keys and on-chip memory, to protect the device from being compromised at the most fundamental level. The Chain of Trust extends the Root of Trust into subsequent applications and use cases.

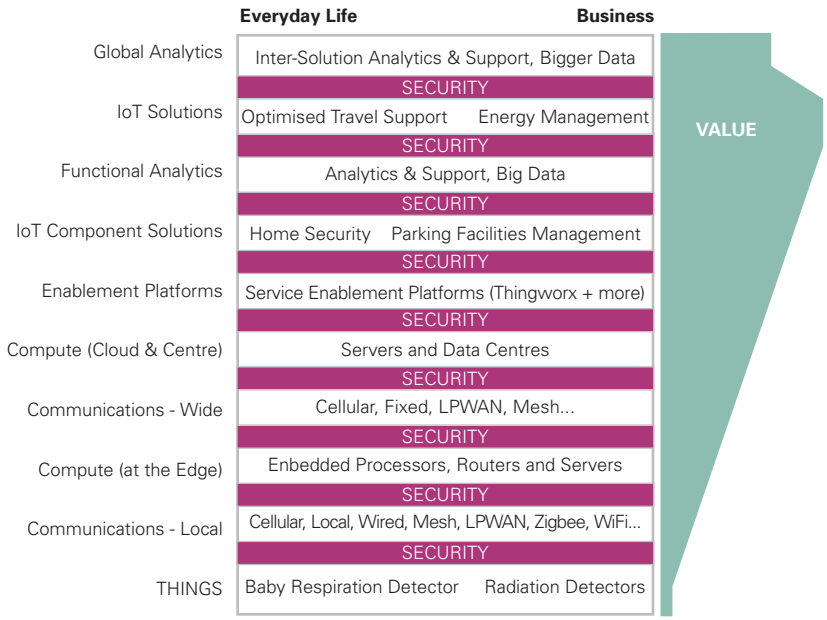
9. Secured Update
Updates, by their nature are significant security threats and allowing only correctly signed firmware updates to be applied is critical for long life-cycle devices.

In the evolving IoT market, security is not just about security of information. The timely transfer of, and correct actions based on, the information in an IoT system is clearly dependent on sufficient security protection. Similarly, devices need to display a level of resilience against a growing range of attacks, including hardware, software and physical tampering.

2.2 Defining IoT Systems & Components

The Internet of Things is a hierarchy of multiple levels of capability and functionality from Global Analytics based on wide swathes of processed data down ultimately to the Things that source the data or are actors within systems. These levels all need to be suitably secured as outlined in Figure 1, where security can not be restricted to a consideration of one or even all of: secured things, secured communications or secured encryption.

Figure 1: Hierarchy of levels in IoT solutions



Source: Beecham Research

In a similar fashion, value needs to be ascribed to the different layers of this model to allow that costs, benefits and players within the ecosystem are well understood. Taking as an example a Connected Washer Dryer, the "Thing" may simply give the ability to pause the machine at a given time, and hence is little more than a simple microcontroller with a relay. However, the value in connecting this to the network adds value as the "Pause" request is made by an external actor. The true value is perhaps in the Functional Analytics or IoT Solution where the Home Owner may subscribe to their Utility Company's scheme for discounted energy, where the Home Owner assists by reducing peak power grid loading. In this way the Home Owner sees a strong value compared with surrendering a small amount of control of their device.

3. CONTROL REQUIREMENTS IN IoT

While individual edge devices will execute a prescribed set of functionalities, any IoT systems need to operate against a set of rules or recipes.

3.1 Control Requirements for Consumer IoT

In the Consumer space, for example, this may be adjusting the heating based on the temperature across a set of monitoring points, or starting a dishwasher in the middle of the night based on a system timer or externally sourced request. These rules must be defined, and the system is expected to then present back a dashboard of current status.

In advanced IoT systems it is expected that control definition can take place on a number of differing compute platforms, including but not limited to mobile phones and tablets or personal computers, either through specific applications or via web interfaces.

IoT systems are expected to exchange information with external systems, however this must be achieved in a simple framework for non-technical users, which probably excludes open APIs except for advanced users. As such it is likely that subscription channels will become a dominant solution in this domain. For example, end-users may wish to subscribe to weather forecasts for their local region, to add additional resilience to the thermostat. This may be in addition to the service originally integrated through personal preference, or may leverage more precise solutions that evolve into the market later in time.

Similarly, it is likely that users may subscribe to external data sinks. For example a patient who needs to monitor blood pressure, weight and activity may wish to set up a specific and unique data channel to their healthcare provider. This connection must be simple to use, robust and secured in its implementation, and possible to subscribe to but then exit when the user no longer wishes to share their information.

This latter point again points to the likelihood that, in the Internet of Things, people must be confident that they always own their own data, and that systems can in no way be subverted to "spy" on their behaviour.

The control scheme defined by the user may be executed at many different points within the system. The application may operate directly on the device that has been used to define the control parameters, such as a tablet computer or PC, or it may operate within a cloud container or on a gateway device. In many cases control may be even pushed onto the edge devices themselves, especially in distributed control

systems where peer-to-peer communications can provide the fastest and lowest latency solution. Each approach has benefits and weaknesses, many of which are discussed later, and many systems will implement a mixed approach to the solution.

3.2 Control Requirements for Industrial IoT

Industrial or professional IoT systems must be tightly integrated into other business operations software such as large scale DCS (Distributed Control Systems) or SCADA (Supervisory Control And Data Acquisition) systems, which in turn may be integrated into profession ERP (Enterprise Resource Planning) solutions. As such Industrial IoT systems require open and flexible APIs to enable seamless integration, however these must be tightly defined to allow security issues are dealt with carefully.

The nature of Industrial IoT solutions is that there is a certainty that there are expert system integrators implementing and operating the systems. However, there is also a continued need to reduce setup and integration costs. Hence while flexibility, control and "water-tight" security must remain, there is a significant push to leverage many of the concepts raised by Consumer IoT solutions back into the Industrial space, such as enhanced subscription services, simple authentication and authorization, and the ability to utilize many vendors' devices and networks to reduce costs.

The location of critical services is a matter of some debate. Many components of the system, including system behavior (DCS/SCADA), and Policy Management / white listing of known devices, are typically contained within the system to provide maximum control and minimum latency. However these systems also require integration to cloud services for identification and authentication from the device or silicon vendor, for example accessing a cloud based registry for public keys based on the system's identifiers as part of the authentication process.

Analytics and malware resistance are also key issues within the Industrial domain. In this domain, system analysis of the system, or processes, has naturally needed to be secured within the enterprise, as this is likely highly confidential information. However, while sensitive information must still be retained within the enterprise firewall there are many applications where access to some system data from a wide variety of users will deliver significant advantages to all users. For example, if all of the users of a specific pipeline actuator share usage data there may be the possibility of picking up design flaws earlier or allowing predictive maintenance to be carried out at a low-cost point, rather than having to close a pipeline in an emergency situation. Similarly from a malware perspective the more devices that are "open" to sending behavioural information and system heuristics the quicker those sharing the data may be able to identify potential attacks, enabling more time to mitigate the impact and develop a firmware update.

4. KEY CONSIDERATIONS FOR IoT

Security is traditionally a trade-off between the robustness of the security and the flexibility the system requires. It is possible to create a nearly perfect security system. However, this requires it to be disconnected from the Internet, have physical alarms surrounding it, and be protected by armed guards. These systems do exist, especially for the production of dangerous or extremely high value assets like bank note printing. However, the costs to manage and maintain these systems is high and their flexibility is low.

A more mainstream example is the Subscriber Identification Module (SIM) found in mobile phones and many first-generation smart metering applications. In this context the device has a very robust boundary and is hardened against physical attack but consequently offers very limited functionality such as managing the subscriber ID and rights prescribed and limited by the network operator subsidizing the handset.

In mainstream IoT there are a number of trade-offs that must be managed:

4.1 Interoperability
It is hoped that the IoT will lead to an explosion in the number of devices and solutions available to the market. From a security perspective it is critical that the industry enables IoT through interoperability but acts to constrain the potential attack surfaces.

4.2 Innovation
Innovation and challenging legacy systems are key motivators for the IoT and will rapidly change the way we think and act over the next 10 years. The security interoperability frameworks must enable innovation, not stifle it.

4.3 Cost Management
Security is traditionally seen as a cost burden, whereas in reality security is fundamental in enabling all of the value of the system, device or gadget to be realized. If you cannot trust your device why use it?

However, it is important that the cost of security be as small as possible to allow lightweight solution and to limit unaffordable impacts on the end device and service costs. To achieve this, it is important that the fundamental silicon chips and underlying intellectual property contribute strong security features that can be exposed upwards to OEMs and System Integrators.

4.4 Cloud and Local Processing
Cloud computing concepts are central to the Internet of Things with substantial value evolving from reducing technical requirements on customers and the ability to mine crowd-sourced data for meta-trends.

Where the entire system is managed by a single vendor, such as the Nest or Hive thermostat, it is relatively simple to define a secured solution. The direction of travel for many of these systems is that some will become a primary home gateway for services and over time subsume other sensors around the home.

While the Cloud remains the pivotal technology in managing and supporting IoT systems there are an increasing number of use cases where the operation and management of systems may take place locally on a flexible gateway device operating as a local Cloud, or Fog compute engine. (Fog computing as defined by Cisco as the Cloud being bought down to the ground).

4.5 Lifecycle
Lifecycle is a massive consideration for the Internet of Things as this market has many of the features of normal fast-moving consumer electronics (FMCE), such as mobile phones and tablets, but critically many of these IoT systems will operate over far longer timescales. While it is not impossible for consumers to upgrade their

thermostat or smart lights every three years there is far less expectation of this happening than in the FMCE domain. As such, many critical devices need to be serviceable for ten to twenty years.

This extended in-service period is more closely aligned with experience in the industrial and automotive marketplaces. These include delivering upgrades and patches remotely, support of anti-malware over long timescales, and general support of devices over a longer period than traditionally experienced, all of which require substantial security frameworks to be implemented.

4.6 Liability

Liability for issues occurring in systems within the IoT is an area of ongoing development, but should represent a key focus for organizations supplying devices or services into this domain. In the automotive domain if a vehicle is found to have a design flaw in a critical capability the supplier must recall the vehicles and implement the fix. For IoT the first challenge is that many of these systems will become hardwired into people's homes, creating physical challenges in returning units and potentially requiring service personnel to visit many homes if a fix cannot be applied over the air. Secondly with many devices being deployed from a huge array of vendors there may be significant issues with which vendor's unit has failed, or potentially where the mixture of multiple specific vendors' units creates a particular issue. Thirdly if a device fails and it causes a failure or fire in a critical control system, which then may destroy a building the vendor may become liable to big losses directly coupled with significant brand damage.

To manage liability, it is important that vendors can demonstrate that their device operates correctly via industry- or self-certification and prove that the device was protected against reprogramming or wilful misuse. In both cases this requires protection of core functionality and proof that the device is protected, both ultimately relying on a robust security foundation.

5. KEY REQUIREMENTS FOR AN IOT SECURITY STRATEGY

This analysis has identified a range of requirements for developing an IoT Security strategy. The following are particularly significant:

1. Security is fundamental in enabling all of the value of the system, device or gadget to be realized. It should not be viewed as a cost burden. It is a value enabler. This means that a security solution should be optimized for IoT devices and use cases and assist in overcoming typical business and operational challenges.
2. Security must become a number one priority and be integrated from the beginning and must be designed-in from the start. It cannot be added later as an afterthought.
3. it is critical that the industry enables IoT through interoperability but acts to constrain the potential attack surfaces.
4. Innovation and challenging legacy systems are key motivators for the IoT and will rapidly change the way we think and act over the next 10 years. The security interoperability frameworks must enable innovation, not stifle it.
5. Building trust between IoT devices is the first step in a holistic strategy. IoT devices need strong protection for tamper resistance. This degree of protection cannot be provided by software alone – it needs hardware-based security.

6. Consistent with this, it is important that the cost of security be as small as possible to provide lightweight solutions and to limit unaffordable impacts on the end device and service costs. To achieve this, it is important that the fundamental silicon chips and underlying intellectual property contribute strong security features that can be exposed upwards to OEMs and System Integrators.
7. Many critical devices need to be serviceable for ten to twenty years. These include delivering upgrades and patches remotely, support of anti-malware over long timescales, and general support of devices over a longer period than traditionally experienced, all of which require substantial security frameworks to be implemented.
8. It is important that vendors can demonstrate that their device operates correctly via industry- or self-certification and prove that the device was protected against reprogramming or wilful misuse. In both cases this requires protection of core functionality and proof that the device is protected, both ultimately relying on a robust security foundation.

6. HARDWARE-BASED SECURITY SOLUTIONS OPTIMIZED FOR THE IoT

Consistent with these findings, Infineon offers a hardware-based approach as the first step in a security-by-design IoT strategy, the OPTIGA™ Trust X. This approach is optimised for IoT devices, which means companies match the right security solution to their unique use cases.

Take for example a factory owner who has started to deploy robots in a new factory location. By using OPTIGA ™ Trust X, the factory owner can authenticate the robots and thus trust the resultant data and insights. In turn, it can trust that the predictive maintenance schedule can be triggered without disrupting operations. On the other hand, if a consumer electronics manufacturer wishes to supply remote maintenance services to its customers, OPTIGA™ Trust X only allows authorised access to the company's products so that no one else but them can access those products. The resultant data is also securely stored, thus demonstrating good security practice to its customers and ICOs.

The OPTIGA™ Trust X is the result of designing security solutions specifically for IoT devices. It is a turnkey solution in the form of hardware, operating system, applications already running in the chip and the host code that can be downloaded to the MCU that in turn communicates with Trust X. It is certified, easy to integrate and ready to use in any type of IoT devices that need to be connected to the Internet. These are applicable to consumer use in smart homes, to industrial mission critical environments such as factories and building automation, and to multi-domain applications such as intelligent transport systems and traffic management.

7. CONCLUSION:

Sustainable business cases rely on a thought through and tailored IoT security strategy.

Hardware-based security enables and eases its implementation and provides the strong and tamper-resistant protection which is needed to capitalize in full on IoT opportunities.