A SMART CARD ALLIANCE INTERNET OF THINGS SECURITY COUNCIL WHITE PAPER

Embedded Hardware Security for IoT Applications

Publication Date: December 2016

Publication Number: IoTSC-16001

Smart Card Alliance

191 Clarksville Rd.

Princeton Junction, NJ 08550

www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information, please visit http://www.smartcardalliance.org.

Table of Contents

1 Introduction

From connected homes to cities to international industrial applications, it is no longer possible to consider the Internet of Things (IoT) as a novelty. The world of IoT crossed the six billion connected endpoints mark in 2016, according to Gartner's market research.[1] Every day over five million new *things* are being connected. It has been projected that by 2020, the world will have over 20 billion connected devices – that's around three smart objects for every single person on the planet.[2]

Healthcare, smart city, consumer electronics, industrial, payments and numerous other verticals are developing services that rely on an IoT infrastructure. Security is a core inherent requirement to deliver safe and reliable IoT services spanning from the cloud to connected devices. Industry security practices, however, differ significantly, leading to a lack of common ground to deploy these services with ease, consistency, and ubiquity.

High-profile cases from hacking of IoT devices have already been reported. In July 2015, Fiat Chrysler announced a voluntary recall of 1.4 million vehicles to fix security issues after two security researchers hacked into a Jeep. They were able to interfere with the vehicle's entertainment system, engine, and brakes while it was being driven on the highway, miles away from the hackers. While this received media attention due to a direct and potential deadly impact to consumers, there have been other incidents that have not received as much mainstream press. In 2014, Germany's Federal Office for Information Security (BSI) issued a report that a steel plant had suffered "massive" damage due to the digital manipulation and disruption of control systems to such a degree that a blast furnace could not be properly shut down.[3] The attackers gained access to the steel mill through the plant's business network using a spear-phishing attack.

The vertical markets using IoT are expanding and include a wide variety of applications, many of which have critical security requirements. Examples include industrial and manufacturing applications, healthcare applications and automotive applications.

- Industrial and manufacturing market sectors leverage connected IoT devices to monitor and control manufacturing equipment. Sensors may monitor wear and operating temperatures and trigger maintenance activities when required prior to regularly scheduled service. IoT connection enhances efficiency, prolongs the equipment service life, and reduces manufacturing cost and lengthy machine downtime. Security objectives for these applications must include preventing unauthorized access to the device to prevent attempts to sabotage equipment or to manufacture products that do not meet specifications.
- Healthcare is another market example. IoT connected medical devices are embedded in hospital clothing to simplify use and enhance patient experience. Wearable IoT devices make it easier to use wireless IoT devices to monitor patients and collect critical health data. Wearable

[1] "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," Gartner press release, Nov. 10, 2015, http://www.gartner.com/newsroom/id/3165317

[2] Derived from statistics provided at http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

[3] https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

IoT devices may be used in hospital rooms to eliminate the many wires and cables that connect the various devices that monitor a patient's vital signs. Some wearable IoT devices are designed to be worn outside of a medical facility and are embedded in items of everyday clothing. This allows healthcare providers, such as emergency response teams, to use portable equipment to quickly gather information at the scene of accidents or other venues where rapid responses are deployed. Security objectives must address privacy issues (e.g., those required by HIPAA) and protect the integrity of collected data, since the data may be used to make treatment decisions.

- Automotive is yet another example where connected IoT devices add value. Just as in the industrial and manufacturing sectors, IoT sensors monitor operation of vehicle components wirelessly and provide information on engine temperature, transmission fluid condition, brake wear, tire pressure and navigation functions to name a few examples. These IoT devices may be wireless and connected to the vehicle instrument dashboard without the use of complex cabling harnesses. Security considerations for auto manufacturers today focus on access control. Separation of the navigation system and engine control or braking system is an important factor in this market so that an IoT-connected navigation system does not provide access to other vehicle systems.

The Smart Card Alliance IoT Security Council was formed to develop and promote best practices and provide educational resources on implementing secure IoT architectures. This white paper is the first in a series of efforts to provide an overview of considerations for securing IoT ecosystems. IoT security encompasses many different aspects of security such as secure boot, device authentication, encryption, secure communication, authorized transactions and lifecycle management. Multiple software- and/or hardware-based approaches may be employed in the industry to implement security in each of these areas to meet the requirements of the specific market.

This white paper describes basic security principles that are critical for IoT implementations and then reviews the application of these security principles for an example use case – managing the lifecycle of IoT devices. The white paper discusses embedded security – where hardware and/or software security mechanisms are built into the end devices used in an IoT architecture. The white paper then further focuses on embedded *hardware* security, where end devices include hardware features and functions to ensure that the appropriate security requirements are implemented and maintained.

2 Security Principles

The security principles for IoT devices include important aspects such as the proper authentication and verification of the identity in order to ensure that only legitimate users are accessing the resources while any access intentions of unauthorized users are rejected. The devices, as well as users, need to be authenticated, and it is equally essential to guarantee protected procedures for authorization, confidentiality, integrity and availability.

Security Principles

The CIA security model[4] contains three principles that are essential in information security: confidentiality, integrity and availability. The CIA security principles form core objectives of information security efforts.

- ***Confidentiality*** refers to the protection of information, such as computer files or database elements, so that only authorized persons may access it in a controlled way.
- ***Integrity*** refers to not being able to modify information unless proper authorization is used.
- **Availability** refers to the presence of information when it is needed by authorized personnel and accessed using proper security measures.

Security Principles for IoT Devices

IoT devices are potential entry points to wider IoT ecosystems. For example, the term, "thingsbots," has already been coined to point to the risk that these devices may become part of wider botnets, where many different devices – all connected to each other, all network-enabled – can send data, making it harder to detect spam attacks or detect and respond to denial-of-service attacks.[5] Through different IoT devices, including both new connected devices and more traditional network equipment, unauthorized access to wider networks, databases, and systems can be obtained, therefore increasing an attack vector. Hence, it is critical to not only ensure confidentiality, integrity and availability, but also to take into account proper access control mechanisms – specifically identification, authentication and authorization procedures. The white paper will focus on these principles in more depth in specific IoT device use cases in Section 3.

Implementation of Security Principles

The current trend indicates that there is an increased need and market opportunity for embedded hardware and/or software security in IoT ecosystems. Which mechanisms to implement will depend on the security requirements of the specific IoT application.

Security principles can be applied in the IoT ecosystem at the device level (among other levels) through the use of embedded hardware which can ensure proper authentication and access control mechanisms. Embedded hardware may be a "secure element,"[6] or another IoT device hardware

---

[4] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[5] "Thingbots: The Future of Botnets in the Internet of Things," SecurityIntelligence, February 20, 2016, https://securityintelligence.com/thingbots-the-future-of-botnets-in-the-internet-of-things/

[6] Global Platform defines a secure element as a tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. (https://www.globalplatform.org/mediaguideSE.asp)

element with security functionality (such as incorporating the Trusted Execution Environment (TEE) in the microprocessor). The secure element may be a Universal Integrated Circuit Card (UICC) form factor or an embedded secure chip.

Hardware-based secure elements can provide the high level of security required by many IoT applications. Embedded hardware security can provide:

- Robust, tamper-resistant storage of cryptographic keys
- Integrated cryptographic functions
- A proven, standardized means for securing communications between the device, the security-focused hardware element, and external entities such as mobile network servers and other systems interfacing to the IoT ecosystem
- Protection against both virtual and physical attacks (such as power analysis or tampering), with appropriate up-to-date shielding techniques
- Portability among devices, for example as when implemented as a UICC
- Support for authorized and authenticated device lifecycle management (e.g., downloading, activating, changing and deleting the subscriptions)

Embedded hardware security can deliver significant benefits for IoT environments that have critical security requirements – those that require the highest level of confidentiality, integrity and availability and that need to ensure authenticated and authorized access.

Challenges with Security Principles

Security must be balanced with cost, implementation effort and end user convenience. There is an unavoidable give and take between the level of security and convenience provided by any solution. The degree of confidentiality, integrity, availability and authentication needed will always be measured on a sliding scale, depending on the application, use case, and environment. It is critical to strike the proper balance between required security levels, and cost or even feasibility of implementation. For example, a portion of IoT devices, such as certain sensors, may lack sufficient processing capability for advanced cryptographic operations.

Achieving an architecture that is standardized among different devices, applications and networks is also a challenge to implementing defined security principles and standards. Use of standard security architectures would eventually drive higher product quality, faster innovation and integration, and a broader community, and enable a more dynamic response to unwanted interruptions if and when they occur. Leveraging design elements such as secure chip technology to support a more secure ecosystem also makes sense to support ecosystem growth and maintenance.

3 Applying Security Principles in the IoT Ecosystem: Lifecycle Management Use Case

This section reviews an IoT ecosystem use case from an IoT device lifecycle perspective, and discusses how embedded hardware security can be used to meet security requirements. The IoT device use case discussed below is common across multiple IoT ecosystems and applications.

Because IoT ecosystems involve a multitude of IoT devices, have users bringing their own devices, and have the potential to be extremely complex, the process of securely onboarding, configuring, updating, and operating devices must be taken into account across device categories and industries. This becomes ever more important as network-connected objects and individuals become sensitive targets for hackers seeking vulnerable IoT equipment to exploit, such as devices worn by individuals, and field-deployed meters, sensors and actuators.

To identify how to apply CIA and related security principles within IoT ecosystems, it is useful to analyze the problem through the connected device's lifecycle that covers:

- Product development
- Manufacturing
- Provisioning
- Operation
- Change of ownership
- Removal from service

Starting at the product development stage, embedded security should be included in the product design. This will ensure that the device can progress through the prototyping, testing and certification phases with the highest level of confidentiality, integrity and availability. Designing with embedded security from the beginning will ensure that the IoT device can benefit from embedded security through its usable life.

During product development, a decision must be made whether to apply embedded hardware security principles to IoT devices in an embedded or removable form factor. A removable secure element is beneficial when it is expected that the stored credentials will travel from device to device (e.g., a mobile phone) while an embedded secure element may be desired in tamper-resistant devices (e.g., insurance telematics module in vehicles) – the latter example providing more total device integrity than the former.

During manufacturing, a device ID in the form of a credential can be stored in a secure element. This device ID can be used to uniquely identify the IoT device and ensure its proof of origin, and take into account the confidentiality and integrity principles. In the case of an IoT device that will connect to a mobile network, an initial mobile network operator subscription can also be provisioned to the secure element.

After manufacturing, a device must then be provisioned and registered to a network regardless of the integrated wireless technology; provisioning may be done by the manufacturer or other ecosystem participants. For this to happen, the integrity of the device must be trusted. A root of trust and device ID from a tamper-proof secure element can be used to ensure this integrity. This integrity can be verified during the authentication process.

Throughout the device's operational lifecycle authentication and encryption can be used to deliver:

- Authenticity – certainty that the sensor or device that sent the message is real and known
- Integrity – certainty that the message is unmodified
- Confidentiality – certainty that the communication has not been intercepted and read by others

A secure element can enable a secure communication channel between the IoT device and the backend to provide encryption (e.g., through a virtual private network (VPN)). A secure element could also be used to store device or user authentication credentials.

IoT devices will be deployed for a multitude of use cases and may change ownership multiple times through their service life. Lifecycle management should ensure that integrity and proof of origin of the device are verified before the device is being placed in service on another network. During the operational phase, lifecycle items such as software updates and lost/stolen devices must also be addressed.

In addition, privacy is a concern where the previous user's credentials must be securely removed and the new owner's provisioned.

At the end of an IoT device's life it should be de-provisioned to the point where it is removed from service and cannot be placed back on the network. Two options for de-provisioning that use embedded security principles with stored keys are:

- The device can be set back to factory default mode keeping the initial secrets loaded in the device, and enabling it to be brought back to life at a later stage.
- Depending on the implementation, the device could be "blacklisted" on the server, so that it cannot be re-attached to the network, until its status on the server is changed.

Lifecycle management of IoT devices is important for all IoT ecosystems and should be considered during the design of the ecosystem and applications to prevent potential security vulnerabilities over time. The features provided by embedded hardware security can also be leveraged to protect the normal functioning of ecosystems with critical security requirements.

4 Conclusions

Too often, security is an afterthought in emerging markets experiencing rapid growth and lacking strong standards and regulations. With the rapid growth in IoT deployment, and with no security standards in place, the IoT market falls into that category. There is already evidence of weak security implementations in numerous IoT implementations that have led to IoT systems being hacked – some by security researchers who are highlighting issues and others by criminals who are leveraging the vulnerabilities for their own goals.

Each IoT ecosystem needs to assess its security requirements and its potential for impacting the security of other systems and determine the appropriate level of security that should be implemented. For those systems that impact life safety or the functioning of critical infrastructure, the Smart Card Alliance advocates the addition of embedded security in IoT devices.

Embedded hardware security, among other embedded security techniques, can protect the "identity" of each device, to prevent unauthorized tampering with how these devices are designed to work, and to protect the privacy and security of the vast amount of data the devices generate. A principle behind the security of smart chips is that the chips not only control how the devices perform under normal conditions, but also control how the devices react when they are attacked or tampered with in any way, including self-destruction. Applying embedded security techniques, including hardware-based – as already proven and implemented for other security use cases – can deliver adequate security mechanisms for the billions of connected IoT devices.

The Smart Card Alliance IoT Security Council welcomes participation from organizations involved in the many IoT ecosystems to develop best practices and advocate for the use of standards for IoT security implementations. Cross-industry collaboration can help to fuel the growth of secure IoT infrastructures and expand the opportunities for a wide variety of new products and services.

5 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance IoT Security Council to provide an educational resource on the value of embedded hardware security in end devices used in IoT applications.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank Council members for their contributions. Participants involved in the development of this white paper included: Accenture; Allegion; CH2M; Discover Financial Services; Exponent, Inc.; First Data; Gemalto; Giesecke & Devrient; Hewlett Packard Enterprise; Intercede Limited; IQ Devices; Metropolitan Transportation Commission (MTC); NextGen ID, Inc.; NXP Semiconductors; Safran Identity & Security; SigNet Technologies, Inc.; TSYS; Underwriters Laboratories (UL); Verifone.

The Smart Card Alliance thanks Council members who participated in the project team to write the document, including:

- **Stu Cox**, Giesecke & Devrient
- **Cindy Custers**, Discover Financial Services
- **Willy Dommen**, Accenture
- **Imran Hajimusa**, Verifone
- **Diane Kehlenbeck**, Allegion
- **Gonda Lamberink**, UL
- **Katherine McClure**, TSYS
- **Cathy Medich**, Smart Card Alliance
- **Jyrki Penttinen**, Giesecke & Devrient
- **Jerome Schang**, NXP Semiconductors
- **Lars Suneborn**, Smart Card Alliance
- **Nicholas Vondrak**, Safran Identity & Security

The Smart Card Alliance thanks Council members who participated in the review of the document, including:

- **Steve Abbanat**, MTC
- **Elizabeth Batista**, Safran Identity & Security
- **Tony Damalas**, SigNet Technologies
- **Jatin Deshpande**, Giesecke & Devrient
- **Jack Jania**, Gemalto
- **Russ Kent**, Hewlett Packard Enterprise
- **Lolie Kull**, Hewlett Packard Enterprise
- **Tom Lockwood**, NextGen ID
- **Cheryl Mish**, Discover Financial Services
- **John Neal**, NXP Semiconductors
- **Jon Payne**, Intercede
- **Steve Rogers**, IQ Devices
- **Brian Stein**, CH2M
- **Sridher Swaminathan**, First Data
- **Christopher Williams**, Exponent

Trademark Notice

About the Smart Card Alliance IoT Security Council

The Smart Card Alliance IoT Security Council was formed to develop and promote best practices and provide educational resources on implementing secure IoT architectures using “embedded security and privacy.” The Council focuses on IoT markets where security, safety and privacy are key requirements and will leverage the industry expertise and knowledge gained from implementing embedded security technology for payment, identity, healthcare, transport and telecommunications systems to provide practical guidance for secure IoT implementations. The Council provides a unified voice for the industry to the broader IoT ecosystem.