The Right Secure Hardware for your IoT Deployment

Published: November 2017

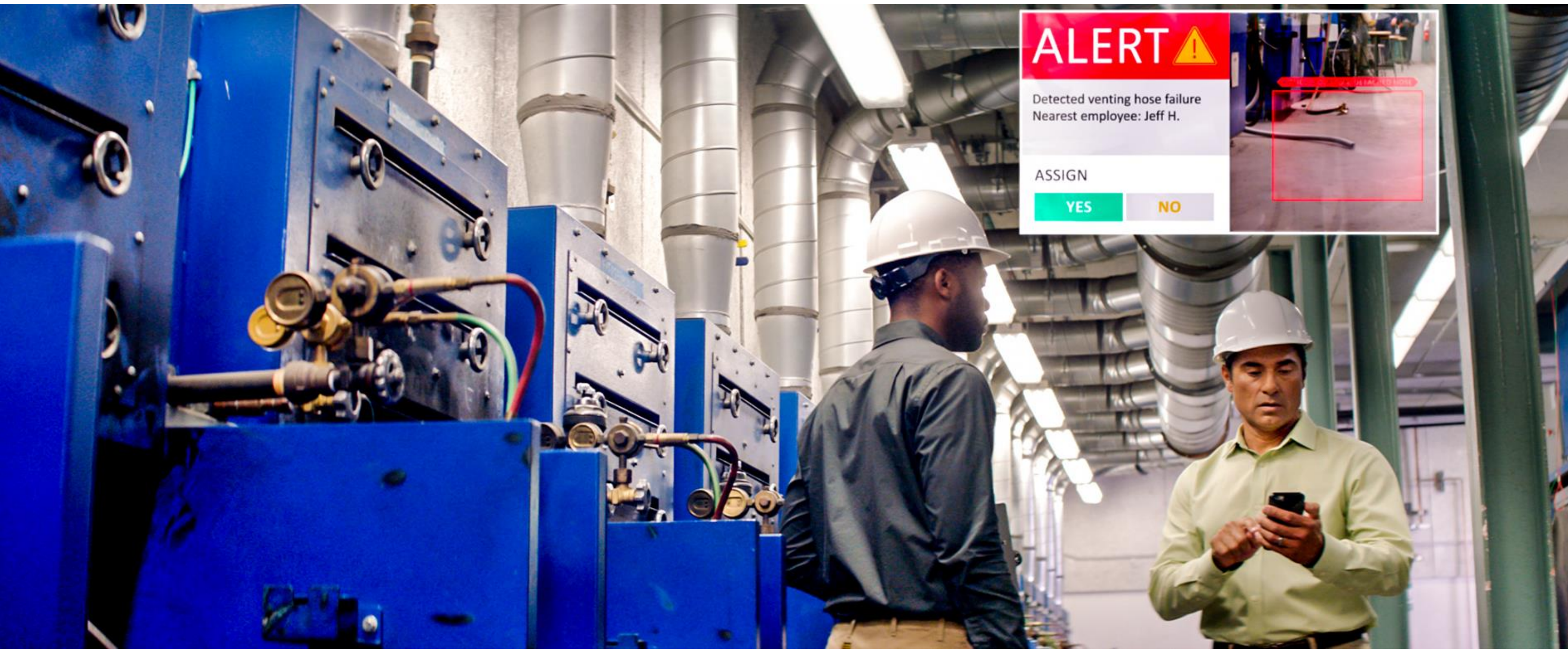
For the latest information, please see www.InternetofYourThings.com

Executive Summary

Securing an Internet of Things deployment end-to-end can be a daunting task. Secure hardware, in particular, is a critical piece of your IoT infrastructure, as the Internet of Things opens up your data and devices to new security threats. But properly balancing the cost and thoroughness of your hardware security can be incredibly challenging.

This paper offers basic guidance on how to select the right secure hardware for your IoT architecture. It begins by defining smart hardware and the two IoT system architecture types. It then offers some detail on common standards that have been developed around usage protocols and application classes to ensure interoperability between the various components in an IoT system. This paper closes by addressing some common security questions regarding IoT hardware deployments and identifying some helpful IoT security resources, including the Azure IoT Device Catalog and Security Program for Azure IoT.

Contents


ALERT
Detected venting hose failure
Nearest employee: Jeff H.
ASSIGN
YES
NO

Introduction

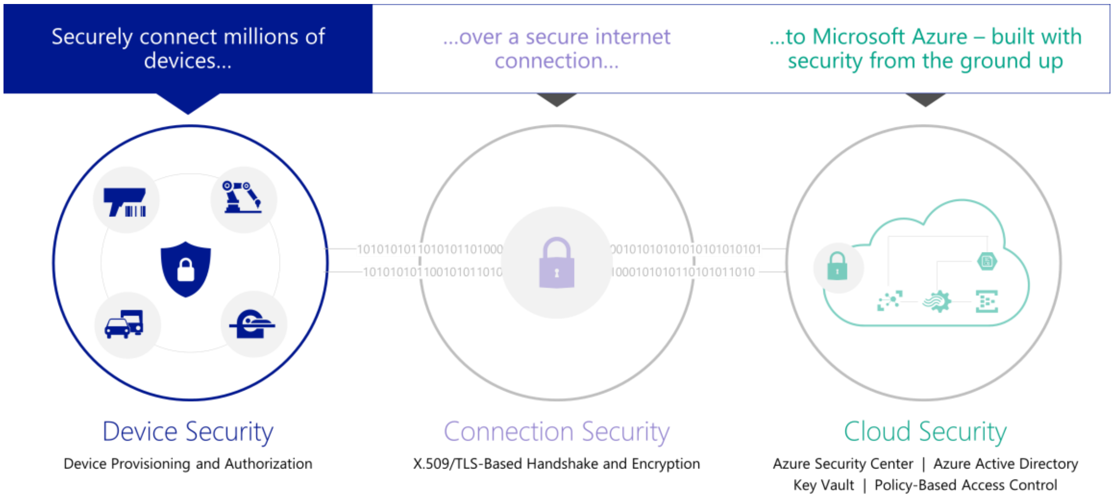
Congratulations! You've made the decision to secure your Internet of Things (IoT) deployment with secure hardware inside your devices. Now you probably find yourself asking a whole new set of questions: What exactly is secure hardware? Where can I find it? How do I choose the right one for my application? And, at the end of the day, how much security do I really need?

You're not alone. These questions are common and important to ensuring you invest in secure hardware that is adequate for your application needs. The answers to these questions will depend on the risk profile of the application at hand, as perceived by the owner. This whitepaper offers some key considerations to help you make the right decisions in securing your deployment.

Scope and target

To be effective, IoT security must take an end-to-end approach. This requires a secure cloud, a secure endpoint, and a secure bidirectional transport between endpoint and cloud.

Figure 1: End-to-end security approach


Securely connect millions of devices...
...over a secure internet connection...
...to Microsoft Azure – built with security from the ground up
1010101011010101101000
1010101011001010110101
0010101010101010101010101
1000101010110101011010
Device Security
Device Provisioning and Authorization
Connection Security
X.509/TLS-Based Handshake and Encryption
Cloud Security
Azure Security Center | Azure Active Directory
Key Vault | Policy-Based Access Control

What is secure hardware?

You might have heard that secure hardware will reliably protect the keys and confidential information in your devices, assuring the security of your IoT deployment. But what really is secure hardware, and how is it different from ordinary hardware?

The term "secure hardware" typically refers to a class of microchips designed to protect sensitive data, such as private keys, even when under attack. You may also hear this referred to as Hardware Secure Modules or HSM.

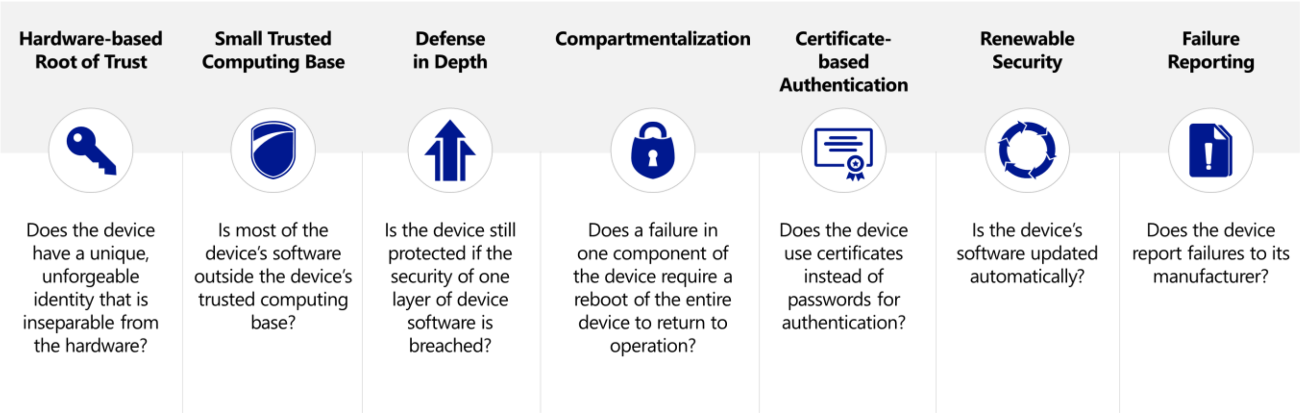
An effective secure hardware protects the data it contains under all conditions, including when in storage or in use. There are several reasons why attackers may attempt to compromise an IoT device. They may be looking to steal the data it contains, or they may want to modify its behavior. These attackers pull from a large repertoire of highly sophisticated equipment and clever techniques, such as subjecting the chip to extreme environmental conditions. Ordinary, unprotected hardware would never stand a chance.

The key advantage of secure hardware over ordinary hardware is its ability to resist attacks. Deploying secure IoT hardware is like storing valuable jewelry in a bank vault. The jewelry may be equally sheltered from the environment at home, but it is far less protected from thieves.

Securing an IoT device

Secure hardware enables devices to protect, use, and manage sensitive information without revealing it to the outside world. But just because an IoT device contains a secure chip does not guarantee that the device itself is fully secure. In some scenarios, secure hardware may successfully protect the authentication keys inside a device, but the broader application might still expose gaps elsewhere for exploits. Securing a device takes careful thought. [The Seven Properties of Highly Secure Devices] article by Microsoft Research offers an excellent guide on how to secure your IoT devices.

Figure 2: The Seven Properties of Highly Secure Devices



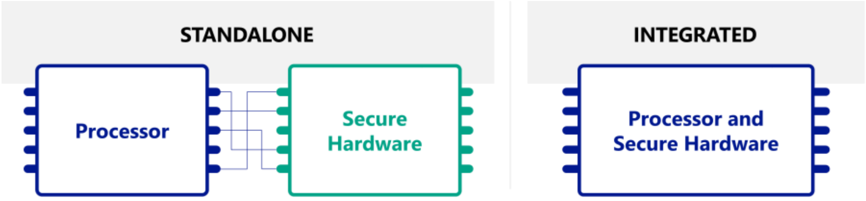
Hardware-based Root of Trust	Small Trusted Computing Base	Defense in Depth	Compartmentalization	Certificate-based Authentication	Renewable Security	Failure Reporting
Does the device have a unique, unforgeable identity that is inseparable from the hardware?	Is most of the device's software outside the device's trusted computing base?	Is the device still protected if the security of one layer of device software is breached?	Does a failure in one component of the device require a reboot of the entire device to return to operation?	Does the device use certificates instead of passwords for authentication?	Is the device's software updated automatically?	Does the device report failures to its manufacturer?

Standalone versus Integrated Security Architecture

An important consideration for your choice of secure hardware is the type of system architecture you envision for your IoT device. All IoT devices require a microprocessor to function. The system architecture is defined by the relationship between the processor and hardware.

There are two architecture types to consider – standalone and integrated. In a standalone security architecture, the secure hardware exists as a separate chip beside the processor and offers security services as a security co-processor. The secure hardware in this type of architecture is sometimes referred to as a secure element. An integrated security architecture combines both the processor and security functions in a single chip.

Figure 3: Standalone vs. Integrated Security Architecture



Determining which architecture type is best for you depends largely on the application in mind. Applications that experience microprocessor evolution across generations of IoT devices tend to favor a standalone security architecture. By separating the processing and security functions, these applications are able to maintain a working security strategy across generations of an IoT product. Applications with unchanging processor requirements, such as secure microcontrollers, tend to favor an integrated security architecture. The advantage with this approach is a lower component count, which typically means fewer interfaces that could leak information.

Deployment details can also influence the type of security architecture you select. The table below provides examples of deployment features to consider. Please note that this is not an exhaustive list. A careful threat analysis will likely uncover additional key aspects to consider.

Feature	Standalone	Integrated	Notes
Greenfield	✓	✓	
Brownfield	✓	***Challenging***	*Easier to add secure hardware without overhauling the processor.*
Ease of initial identity creation for provisioning	✓	✓	*Independent interaction with standalone secure hardware enables initial identity pre-creation scenarios.*
Trusted computing base	✓	✓	*Applicable when all trusted computing is encapsulated in the secure hardware e.g. certificate signing operations.*
Trusted execution	***Challenging***	✓	*Happens in the processor*
Secure boot	✓	✓	*Requires immutable code in processor for code measurements*
Secure firmware updates	✓	✓	*Requires immutable code in processor for code measurements.*
Resilience	✓	✓	*With careful design*

Types of secure hardware

There are numerous classes of secure hardware, each appealing to a particular device segment. This variation presents some challenges, including a lack of interoperability. In response, hardware standards have been developed around usage protocols and application classes. This section lists some of these standards, but is not intended to be exhaustive, as new standards continue to emerge.

Device Identifier Composition Engine (DICE)

DICE is a class of secure hardware based on a set of security protocols standard by the Trusted Computing Group (TCG). DICE aims to solve the problem of security and privacy in the resource constraint devices that are prevalent in IoT. Although DICE is designed to secure IoT systems, it is still incumbent on the system design to properly apply DICE techniques to the security challenges specific to their deployment. DICE secure hardware is most optimal for a standalone hardware architecture.

Trusted Platform Module (TPM)

TPM is a class of secure hardware based on a set of security protocols standard also by the TCG. The TPM protocol enables remotely connected systems to establish trust and communicate securely. While attributes of the standard allow the strength of security to be vetted, it does not specify how the hardware itself has been constructed. TPM is therefore a protocol-inspired de jure standard, created primarily to solve the problem of interoperability. TPM devices are optimal for a standalone hardware architecture.

Secure Smartcard Modules

Secure smartcard modules are a class of secure hardware commonly governed by several de jure standards that specify attributes like form factor and communications protocol, but not security. However, they were inspired by applications that demand high security, such as payment and Subscriber Identity Modules (SIM) cards. Each application vertical has security standards to drive the security requirements for its respective vertical. For this reason, they are often treated as a de facto standard for security. They are commonly used in kiosk-type IoT systems that require removable cryptographic modules. They therefore are optimal for a standalone hardware architecture.

Hardware Secure Modules (HSM)

In the context of IoT, HSM is a catch-all for any secure hardware that does not adhere to a specific security protocol. These may come in various sizes and are sometimes optimized for specific applications or use-cases, such as certificate processing or secure token generation. Essentially, their goal is to protect data against attacks. Most HSMs are optimal for integrated secure hardware architecture.

Other

There is a myriad of other emerging secure hardware technologies that do not exactly fall under TPM, DICE or HSM. One example is a class of technologies known as Physical Unclonable Functions (PUF). Most of these emerging technologies harvest intrinsic and unique properties of ordinary hardware as the basis for secure solutions. Harvesting techniques use either software or specialized circuits that a silicon manufacturer integrates into a piece of hardware. Regardless of technique, these technologies are gaining popularity, as they promise security without any significant additional cost in dollars or physical footprint.

Common questions

Where can I get secure hardware?

Identifying the right secure hardware from a manufacturer can be a laborious and confusing process. To help with this, Microsoft has developed the Azure IoT Device Catalog, which provides filters for the different types of secure hardware. This catalog is open to submissions from secure hardware vendors and includes information like attributes, specifications, certifications, evaluation, and sourcing.

How do I gauge the security of a secure hardware?

There isn't a foolproof way to compare security strength across different types of hardware, as each is constructed using vendor proprietary techniques to protect data against attacks. In reality, security certifications may be the most useful means of evaluating and even grading levels of security. Some industry verticals have specific grading requirements. Standards adopted by experts and governments around the world include:

1. The US National Institute of Standards and Technology (NIST) FIPS 140-2 standard
2. The German Federal Office of Information Security BSI standards
3. The PCI Security Standards Council governing security payment transactions
4. The French Network and Information Security Agency (ANSSI)

In general, it's important to check for commonly adopted standards or standard mandates when deploying products for a specific industry.

How much security do I really need?

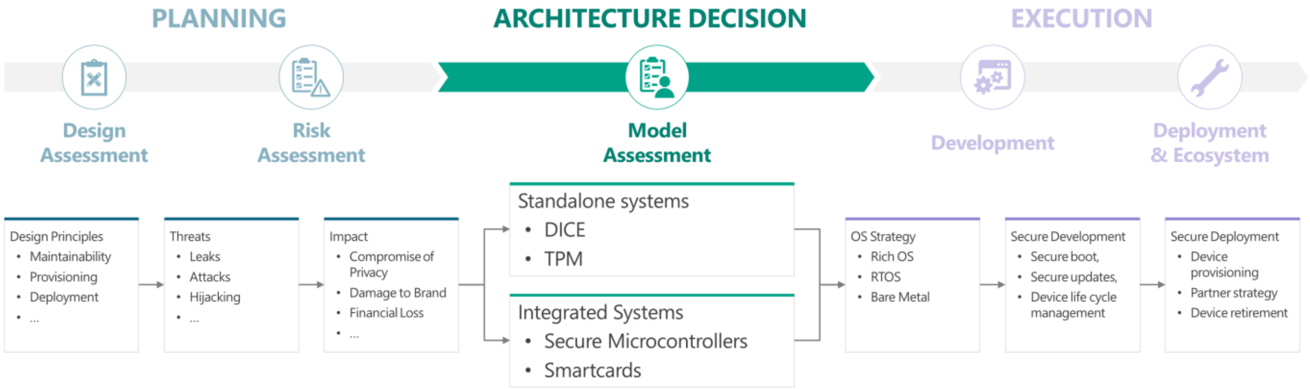
This is the key question to consider. Shortcutting security investments is a waste of resources, as the security of the deployment will only be as good as the weakest link. On the other hand, an overinvestment in security will likely detract from other important aspects of your deployment, like the user experience or your return on investment. So how much security is adequate? How much should you spend on secure hardware?

In reality, these are questions that only you can answer for your deployment. This is because the answers will depend on the perceived threats, their associated impact, and your tolerance to risk. For example, the perceived threat and impact of breaching a pacemaker device is understandably a higher risk than a potential breach to a fitness steps counter. Similarly, while one manufacturer of a certain kind of IoT device may choose to invest in securing their devices to ward off breaches, another may choose to focus their investment other aspects of their business. The bottom line is that the decision is unique to the application, deployment, and your assessment of threats, impact, and risks.

How should you begin assessing the threats to your IoT infrastructure and the impact these threats may have on your business? With the Security Program for Azure IoT, Microsoft maintains a curated set of best-in-class security auditors customers can choose from to evaluate the security of their IoT solutions.

Overall, the decision process for secure hardware should consider every stage of the product lifecycle, from concept to retirement. The optimal secure hardware choice is one that addresses any identified threats and securely accommodates downstream decisions like your operating system strategy, development, deployment, ecosystem, and retirement strategy.

Figure 4: The Secure Hardware Product Lifecycle



Securing any IoT deployment is difficult, and choosing the type of secure hardware that properly balances effectiveness and cost can be daunting. While the right hardware selection depends largely on application-specific and deployment-specific threats and their potential impact, there are several considerations that can help reveal the optimal choice. This whitepaper offers an introductory look into these considerations.

Learn More

- Explore Microsoft's IoT offerings at www.InternetofYourThings.com
- Read more about Evaluating Your IoT Security
- Find evaluator partners in the Security Program for Azure IoT
- Begin a trial solution of Azure IoT Suite

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.