Allegro

7 Key Elements of Proactive IoT Security

How to Reduce the Risk of IoT Hacks, Breaches, Data Theft, and Ruined Reputations

February 2017

Allegro Software

1740 Massachusetts Avenue
Boxborough, MA 01719
Telephone: 978 264-6600 Fax: 978 266-2839
www.allegrosoft.com

Introduction

All types of Internet of Things (IoT) devices are under attack. They are routinely recruited as unwitting members of botnets used for Distributed Denial of Service (DDOS) attacks, hosting various malware, and extracting sensitive data. Why are hackers drawn to these devices? Two specific reasons: the data has a high enough value, and most IoT devices are ill equipped to beat back cyber attacks.

Unfortunately, these attacks are typically not discovered for weeks or even months while the potential damages continue to rise. Tremendous economic and social brand damage is inevitable and can often lead to uncomfortable conversations with the media, industry, and even government regulators. Until recently, embedded device security hasn't been a topic for the C-Suite. Thankfully, executives are now starting to ask whether their products are at risk, demanding solutions, and looking for assurance from their engineering teams to deliver security.

What proactive approaches can engineering teams take to reduce IoT related risk?

Read on to see how the "7 Key Elements of Proactive IoT Security" can increase your security presence and reduce the exposure of your IoT ecosystem to hacks, breaches, data theft, and lost brand equity.

Element #1: Root of Trust

Without a fixed device identity, the opportunity for device hacks, breaches, data theft, liability claims, harsh compliance fines, and ruined brand equity is real. To avoid such nightmare scenarios, IoT ecosystems must be confident of the integrity and resulting data from all participating IoT devices. Without this confidence, the promise of business agility and increased productivity are lost.

The genesis of a root of trust occurs during the manufacturing process. A unique key (often the private key of a public/private pair for the IoT device) and identity (a signed certificate with the serial and version number of the IoT device) are inserted into the product, along with several other public keys for network assets that the IoT device will use when deployed.

This suite of information, in conjunction with cryptographic routines, empower IoT devices to confidently communicate and actively engage with the larger IoT ecosystem. IoT devices can securely communicate configuration, command and control, status and other sensitive operational data to cloud resources. Furthermore, using this suite of information with a secure, multistage bootloader and secure provisioning (discussed in a following section) eliminates nearly all risk of losing control of an IoT device to rogue botnets.

The Challenge: How to prevent identity theft, data corruption, and use of fraudulent hardware?

The Solution: Implement a method for establishing a root of trust during manufacture. When Public Key Infrastructure (PKI) technology is used, a Certificate Authority (CA) is required. GlobalSign and DigiCert are two vendors that provide commercial IoT CA implementations. Another popular but less secure option is to be your own private certificate authority.

The Benefits: Authentication, authorization, and validation of IoT devices into the larger IoT ecosystem significantly reduce risks associated with fraudulent data, hardware, data theft, loss of control, and much more.

"An IoT Root of Trust starts with a Certificate Authority (CA). Allegro has partnered with leading enterprise CAs with solutions specifically engineered for the unique needs of IoT ecosystems. These solutions offer high availability, reliability, and high-volume transactions for a broad range of deployed IoT scenarios. The Allegro Cryptography Engine (ACE™) also includes a flexible and pre-integrated CertBuilder utility for creating private self-signed certificates."

---

sales@allegrosoft.com
www.allegrosoft.com

Element #2: Secure Parameter and Key Storage

Establishing and maintaining a root of trust for an IoT device relies on the ability to store and retrieve keys securely, along with operating and configuration parameters. This is more difficult with IoT applications because these devices are often readily exposed to potential physical threats. There are various options for storing security parameters and keys, some of which use specialized hardware. The choice depends on the risk profile of the device. For example, a medical device typically would need a stronger risk profile than a residential lighting control device.

The following table lists various types of parameter storage technology and their relative risk levels.

Table 1. Secure Key and Parameter Storage Technologies (most secure to least secure)

Technology	Risk	Specialized Hardware?	Description
On-Chip Secure Zone	Lowest	Yes	Various silicon vendors offer support for "trust zones" within the chip that are separate from the core processor, memory and bus structure. This approach offers the least risk to exposing critical data.
Trusted Platform Module (TPM)	Low	Yes	This is an additional item on the bill of materials. It is the favored technology by the Trusted Computing Group for storing critical data and establishing a root of trust.
Hardware Security Module (HSM)	Low	Yes	Similar to a TPM, HSMs also represent an additional item on the bill of materials and are typically optimized for specific cryptographic operations to offer overall performance.
Hybrid – NVRAM using Software TPM	Medium	No	The Trusted Computing Group also suggests solutions for software-based TPMs. While these are less secure than hardware modules, they offer tremendous flexibility and lower cost.
NVRAM using Cryptographic Routines	High	No	Similar to a software TPM, this implementation uses a simple hash or cipher with static keys. This can be secure as long as the keys are not discovered.
Keys stored as part of executable image	Highest	No	Unfortunately, this is the normal mode of operation for many IoT devices. Many vendors have seen their devices compromised and enrolled as unwitting servants of rogue DDOS botnets.

The Challenge: How to securely store operational parameters and keys on an IoT device that is often deployed in potentially harsh environments where keys can be compromised?

The Solution: Use industry-proven technologies for storing keys and critical operational parameters. On-Chip solutions offer the least risk, while storing keys in the code is not recommended.

The Benefits: Device identity is intact and the overall risk for malicious intent is dramatically reduced.

"The Allegro AE suite includes a simple API for securely storing keys and parameter data with on or off silicon TPM, HSM or custom secure NVRAM modules. Allegro's FIPS validated ACE library also offers API access to a broad range of cryptography including: bulk encryption, decryption, calculating message digests, digital signature generation and verification, key generation, and key exchange capabilities."

---

sales@allegrosoft.com
www.allegrosoft.com

Element #3: Secure Device Updates

Every IoT device is likely to need a firmware update. The provisioning process to provide these updates must be engineered for security. The loss of identity and insecure re-provisioning of IoT devices have been identified as the root cause for many recent DDOS attacks worldwide. More importantly, these types of DDOS attacks represent unprecedented levels of network traffic at a previously unseen and unthought-of scale. With billions of operational IoT devices, the threat is very real and accelerating at an alarming rate.

From the time of product manufacture to the time of product End Of Life (EOL), an engineered provisioning model that securely installs and updates firmware and operating parameters is a critical element for IoT security.

As provisioning models go, there is no one-size-fits-all model for the IoT application space. However, secure provisioning models all use digital signing for firmware or parameter updates. Digitally signed updates offer three specific advantages:

1. Authentication – authenticates that the new firmware is indeed a valid update from the manufacturer.
2. Authorization – enables the IoT device to authorize the execution of the new firmware.
3. Validation – validates the new firmware to ensure nothing was lost in the transmission of the update.

This technology often works hand in hand with a multistage secure bootloader to ensure that all firmware images are authorized, loaded, and executed in the proper order.

The Challenge: How to install and safely update firmware or operating parameters securely while the IoT device is deployed in operational environments?

The Solution: An engineered provisioning solution that uses digital signatures in combination with a secure multistage bootloader to implement firmware and parameter updates for devices deployed in the field.

The Benefits: A system designed to ensure secure updates provides an extremely valuable service to the end customer and dramatically reduces the risk of a rogue actor enrolling IoT devices in large-scale DDOS attacks.

"The Allegro AE suite of toolkits provide the communication and security capabilities for an engineered provisioning solution. From simple to complex provisioning models, Allegro's toolkits combine secure communications with a rich set of FIPS 140-2 validated cryptography for calculating message digests, digital signature creation and verification, bulk encryption and decryption, key generation, and key exchange. Used stand-alone or pre-integrated with other Allegro AE toolkits, ACE provides government validated implementations of sophisticated encryption algorithms for use in embedded systems."

Element #4: Operational Data Security

Besides protecting the security parameters, an IoT device also needs to protect the application or operational data..

Securing Data-In-Motion

Using secure communications protocols between an IoT device and the larger ecosystem protects operational data. Transport Layer Security (TLS) is the industry standard for keeping communications secure. Solutions specifically engineered for the rigors of embedded computing are the best solutions for resource-constrained IoT devices.

Securing Data-At-Rest

Many IoT devices need to protect the data in the device as well as protecting the communications with the outside world. For example, IoT applications in the financial and medical arenas are two examples that have specific requirements for ensuring application data is stored securely in the device. The unique requirements go beyond just encrypting all data with a single key. For example, medical records must be encrypted with a unique key for each patient to avoid patient-to-patient crossover on a device. You can think of it as multiple patients using the same infusion pump or hospital bed in a day. You want to prevent new patient records from being mixed with the previous patient records.

Public Key Infrastructure (PKI) technology provides an ideal solution for this problem. With PKI, an IoT device encrypts all patient data using a patient's public key before storing or transmitting it. The data is rendered useless until decrypted using the patient's private key. The patient private key is typically part of the larger hospital information systems and electronic medical records interface.

The Challenge:	How to securely store and communicate generated IoT application data to the larger IoT ecosystem?
The Solution:	Secure data-in-motion using the latest TLS protocols and secure data-at-rest using PKI technology.
The Benefits:	All data exchanged between the IoT device and the larger IoT ecosystem is protected by TLS. If a breach occurs with a physical endpoint, data stored on the device is rendered useless.

"Allegro offers the latest implementations of TLS specifically engineered for the rigors of resource-constrained IoT environments. In addition, Allegro's ACE library is pre-integrated with our Secure File System storage toolkit. The toolkit makes extensive use of FIPS validated cryptography and offers the flexibility for encrypting application data at the file, directory, group of directories or entire volume. This is specifically applicable for medical, financial, and defense IoT applications with unique data separation requirements."

Element #5: Access Control and Key Management

Access Control

The single mostly highly used attack on deployed IoT devices is the use of factory-defined access credentials. An IoT device should require new and unique usernames and passwords on initial startup. This approach eliminates the most common and easiest hacking attack. This requirement is applicable for all management interfaces (web-based management, CLI, etc.) and for all open ports. Additionally, robust access control supports separate user privileges with separate application data privileges. To meet application data separation requirements, PKI technology and Key Management are crucial.

Key Management

IoT applications in the healthcare, financial, and defense industries have specific regulated data separation requirements. Overall, key management and the use of PKI based technology play significant roles in fulfilling these requirements. To secure medical records, for example, an IoT device can request a unique public key for every patient using the standards-based Simple Certificate Enrollment Protocol (SCEP). Once application data is encrypted with the public key, only users with the appropriate access to the private key can decrypt and view the data. The ability to create and control access to keys dynamically for the application data life cycle ensures privacy.

The Challenge: How to manage IoT device keys, configuration, and user credentials securely?

The Solution: Use standards-based certificate management tools in partnership with an IoT-focused CA or custom implementation of a private CA with a robust infrastructure.

The Benefits: Implementation and effective use of certificates embeds multiple layers of security into an IoT device. This empowers developers with the ability to create mutually exclusive data stores to store critical data effectively and safely throughout the life cycle of the IoT device.

"The pre-integrated suite of Allegro AE toolkits offer FIPS validated cryptography combined with CLI and patented web-based device management for implementing access control on IoT devices. The suite of toolkits also offer the ability for IoT devices to access cloud-based resources via HTTPS and SCEP for effective key management. The combination of certificates and key management for creating secure data stores ensures privacy throughout IoT life cycle."

Element #6: Monitoring and Remediation

Monitoring and remediation provide a vital feedback function for an IoT ecosystem. Monitoring application communication and data patterns can provide valuable insight into the overall behavior of the ecosystem.

Monitoring

An active and successful IoT ecosystem has a healthy level of intra-system communication. Application data is a natural by-product of a deployed IoT ecosystem. The de facto standard for IoT interoperability with cloud-based resources uses secure XML-based communications. A proactive approach to monitoring the natural ebb and flow of XML application data from IoT nodes can provide a wealth of insights. These insights when combined with big data analysis from other parts of the corporation can lead to a variety of actionable business decisions. Additionally, if specific IoT nodes fall outside normal operating and communication patterns, they can be flagged for inspection and possible remediation.

Remediation

An IoT ecosystem is the sum of all the IoT device nodes, the cloud services and the application specific data that flows through the system. A proactive approach to monitoring and remediation enables the larger ecosystem to identify potentially faulty or rogue devices and take appropriate action. For devices flagged for inspection, remediation and removal, re-initialization, or provisioning are critical to the overall health of the ecosystem at large. In practice, remediation models vary greatly and should be engineered for the specific application space. Remediation for a CT, CAT or MRI scanner, for example, would be far different from schemes for an office lighting system or personal treadmill.

The Challenge: How to monitor and remediate the deployed IoT devices to keep the ecosystem healthy?

The Solution: Implement a secure, flexible, and configurable IoT communications, command, and control architecture based on TLS, XML, RESTful APIs, or SOAP.

The Benefits: Strong monitorying leads to a healthy IoT ecosystem with secure IoT nodes actively reporting application data. Proactively identifying potential threats and inconsistencies prevents the disruption of the quality and overall health of the IoT ecosystem.

"Allegro's toolkits provide secure TLS communications along with the ability to parse and frame XML application data, and actively participate with cloud resources for command, configuration and control. Used stand-alone or integrated with the other Allegro AE product suite, our toolkits offer a highly integrated set of capabilities for OEMs to build robust and secure device management. This is the same technology which Allegro provides to our global customer base and is currently deployed in over 200 million devices."

Element #7: Validated Cryptography

Cryptography is a means to an end. In a high-tech world, cryptography is the underlying technology that keeps sensitive data from prying eyes. Although the landscape of digital threats continues to evolve and force change, the perceived power of cryptography maintains an unprecedented level of trust. Cryptography is steeped in advanced math concepts and, to be useful, it must be tightly coupled with computer science and implementation skills. Moreover, for resource-constrained IoT devices, an understanding and respect for the limits of embedded computing are mandatory. With all this to consider, it is easy to see why experts highly recommend avoiding a do-it-yourself approach, which can lead to a false sense of security. Using validated cryptography provides a level of assurance that the cipher suites and complex cryptography algorithms have been properly vetted by an independent third party. In addition, using validated cryptography ensures interoperability and functionality with other deployed devices and services.

The Challenge: Does the cryptography used in my IoT device implement the cipher suites and complex algorithms correctly?

The Solution: Use validated cryptography – cryptographic solutions that have gone through independent third-party evaluation and extensive testing to ensure proper operation. Using validated cryptography also ensures interoperability and functionality with other deployed platforms.

The Benefits: Using FIPS-validated cryptography leads to a high level of trust that the private data in IoT devices and their connected ecosystems remains private.

"Allegro has specifically engineered ACE for resource constrained IoT environments and taken the product through FIPS 140-2 validation. ACE provides software implementations of FIPS-approved algorithms for calculating message digests, digital signature creation and verification, bulk encryption and decryption, key generation, and key exchange. Used stand-alone or pre-integrated with other Allegro AE toolkits, ACE provides government validated implementations of sophisticated encryption algorithms for use in embedded systems."
