Allegro Software

Best Practices for Managing IoT Related Risks

Best Practices for Managing IoT Related Risks

- Evolving security risks demand new and dynamic approaches
- IoT-Fueled outcomes implies a deep trust in data
- With billions of IoT endpoints feeding data into billions of digital twins that interact and exchange data, how can you manage IoT security related risks?
- “Best Practices”
  - Our Research
  - 20+ Years of Experience

Allegro

Critical Requirements

Regardless of IoT application (healthcare, financial, military, government, industrial, infrastructure, etc.) there are 5 common recurring requirements for IoT ecosystem security.

Device Integrity

Is the device known to be in “good standing” with the larger IoT ecosystem? The enterprise element of an IoT ecosystem must authenticate each device and validate any data received from the device (none was lost in transmission). Likewise, the device must authenticate and validate all command-and-control messages from the enterprise system before taking any action. A unique and immutable root-of-trust for each device enables authentication and validation services. This in turn gives rise to a chain-of-trust authenticating and validating all firmware, application software, and stored data from the moment power is applied. This drastically reduces the risk that a rogue software update will take over a deployed device, receives a command to send valuable or sensitive data outside of the IoT ecosystem, or enrolls in a coordinated botnet for DDOS attacks.

Data Security

In general terms, the earlier data can be encrypted and later it can be decrypted for use provides the greatest level of confidentiality. Often referred to as end-to-end security, it forces system architects to define a data lifecycle and policy driven access and control. In many cases data is wrapped with additional layers of encryption (using a different set of keys) when stored at rest or when in motion over a network (wireless, wired, or combination of both). Using multiple sets of keys along with different types of encryption provide a defense in depth solution. Additionally, both the enterprise environment and the device should employ digital signing techniques to authenticate and validate messages sent and received. This gives a high level of confidence that any data sent or received is complete and is coming from a known entity.

Operate at Scale

Creating a system that can properly function while meeting the demands of an IoT deployment can be difficult. Even the simplest of architectures will stress critical security components at large scale. This often reduces to a deep understanding of temporal operational security requirements at the device level. A Failure Modes and Effect Analysis (FMEA) applies this knowledge to the overall IoT ecosystem. Outcomes from this analysis determine critical key management strategies (e.g. PKI architectures, when and if to use pre-shared keys, how and when to replace or renew keys, etc.) and processing loads placed on essential security components. Another outcome from the analysis provides valuable insight into how the system will react if a critical component slows down or completely fails.

Regulatory and Compliance

Various industries have specific requirements for meeting regulatory and compliance guidelines. Many military, government, industrial, healthcare and financial IoT applications require FIPS 140 validated cryptography. This provides an additional level of confidence that the complex encryption algorithms perform as expected and specific operational parameters are defined when using it. Meeting these encryption standards is critical if a system or data breach has been identified. When data is properly encrypted it is rendered useless without knowledge of the encryption methods and appropriate keys.

Monitoring and Remediation

Some IoT ecosystems employ thousands or even millions of deployed devices and must include some type of monitoring and remediation capabilities. This functionality is critical for identifying units that are not performing to specifications and need repair or replacement due to hardware malfunction, environmental changes or other potential failure modes. Until a field technician can repair or replace the device (if even possible), the affected unit can be taken offline to support overall system functionality and data integrity.

Functional Implementation

The requirements above are broken into the following three broad functional implementation categories (Device Reputability, Data Confidentiality, and Operational Assurance) in support of managing IoT-related security risks. Each category has functional components representing implementation best practices for firmware and application software. For a more detailed discussion of security components, refer to Allegro's white paper

"7 Key Elements for Proactive IoT Security"

Device Reputability

There are three primary functional components necessary for implementing IoT device reputability: *Root-of-Trust*, *Secure Boot*, and *Validated Cryptography*. Each functional component is briefly described below.

Root-of-Trust

A root of trust is an immutable identity often assigned to an IoT device during the manufacturing process. Typically, a small suite of critical information unique to each device that includes: a signed certificate with serial and hardware version numbers, a unique key (often a private key of a public/private key pair for the IoT device), along with additional public keys for additional network assets that the device will use when deployed.

Device Reputability

Secure Boot

Immediately after a restart or power-up event, the IoT device must enter a secure boot process to perform a series of Power On Self Tests (POST). POST and the overall Secure Boot process is specifically utilized to authenticate, validate, and authorize all software modules and ensure they have not changed since power was last removed. This creates a chain-of-trust that extends to the application running on the device and significantly reduces risk.

Validated Cryptography

All device and overall ecosystem security is based on the use and proper implementation of sophisticated encryption algorithms. This is challenging in enterprise execution environments and becomes even more challenging in resource constrained situations. Validated cryptography also provides an added level of assurance that the algorithms are implemented properly and function as expected.

Allegro

Data Confidentiality

IoT devices generate rich streams of data. In many use cases, IoT devices collect and correlate data that is considered personal, confidential, or in the case of critical infrastructure or military applications – extremely sensitive. There are two primary functional components for implementing data confidentiality: *Data Access Policies* and *Data Preservation*. Each functional component is briefly described below.

Data Access Policies

Ecosystem access, utilization, and overall data lifecycle are driven by polices developed to safeguard the information at all times. The intent is to provide end-to-end data confidentiality ensuring only the persons or applications with the appropriate policy defined authority can access the unencrypted information.

Data Preservation

When necessary, this includes properly encrypting data at rest and before taking flight across a network. All data traveling across a network must also travel via an encrypted tunnel (SSH or TLS).

Operation Assurance

Operation Assurance strives to always deliver a fully functional, and fully populated ecosystem delivering the necessary data to make the best IoT-fueled decisions possible. There are two primary functional components for implementing Operation Assurance: *Secure Remote Provisioning* and *Monitoring and Remediation*.

Secure Remote Provisioning

Secure remote provisioning is a critical component to all IoT-based ecosystems. Device Integrity relies on a robust and secure provisioning architecture to handle onboarding, upgrades, and updates (including key management). More specifically, the provisioning architecture must have the capability to independently track every device (which could be millions or more), provide fine-grain control (update a single device, group of devices, all devices, etc.), and command broad or specific updates while minimizing impact on the overall ecosystem. This is essential to actively support crypto-agility and patch new exploits and vulnerabilities as they become known.

Operation Assurance

Monitoring and Remediation

With large numbers of deployed devices, even with the best operational characteristics, at any given moment some devices will not function properly. Once identified, a device or group of devices requires attention to ensure their overall activity and data being reported into the larger ecosystem is valid. This requires monitoring capabilities at both the macro and micro level. If a deployed device needs to be re-provisioned or worse replaced, the larger ecosystem must be able to continue working without any issues. Remediation capabilities may include resetting and re-provision or even commanding a unit to go dormant to preserve network bandwidth.

Conclusion

Perimeter-based defenses and conventional threat detection technologies are not enough to defend against modern cyber-attacks on IoT ecosystems. The rich data streams originating from these IoT devices are driving the next generation of digital business and operational ecosystems. While the promised gains from increased efficiencies, better productivity, and enhanced performance are attractive, the increased exposure to attack can create sleepless nights. Unlike the past, manufacturers must rely on sound “secure by design” principles to establish a proactive stance on overall data integrity and device security.

The above “Best Practices” represent the combination of personal experience along with 20+ years of experience discussing and implementing device connectivity and security with our prospects and customers around the globe.

Allegro

About Allegro Software

Since 1996, Allegro has been providing superior products to the embedded industry. Many companies have discovered the advantages of creating devices that are active members of the Internet of Things (IoT) and work with Allegro to meet their networking connectivity needs.

Allegro customers include many of the leading developers of computer systems, networking equipment, and IoT devices such as Arris, Baxter Healthcare, Bose, Brocade Networks, Cisco, D-Link, General Dynamics, Harman International, HP, IBM, Kronos, Microsoft, Motorola, Nielsen, OpenTV, ResMed, Siemens, Sumitomo, Xerox and Yamaha.

These customers, and others, have found that Allegro's connectivity and security toolkits are well suited for embedding in devices like printers, routers, automobiles, medical equipment, UPS systems, enterprise phone systems, set-top boxes, and networked digital media products. With over 300 design wins and over 275 million deployed devices worldwide, Allegro delivers robust and field-proven Internet software for your embedded device. Visit our website to learn more: www.allegrosoft.com.