WHITE PAPER

Security in Internet of Things

Internet of Things (IoT) poses unique security, privacy and compliance challenges for businesses worldwide.

In the traditional computer world, these issues are associated with software and its implementation. In IoT, with the convergence of the physical and computer worlds, these issues extend beyond software to the entire IoT solution. They encompass secure provisioning of physical devices, secure connectivity and data transmission between them and the cloud, and secure data protection in the cloud during processing and storage.

Popular IoT platforms such as Microsoft® Azure® IoT Hub and AWS® IoT address these security challenges successfully with end-to-end, multi layered protection.

THINXTREAM®

Introduction

Intelligent connectivity of physical devices – popularly known as Internet of Things (IoT) – is driving massive gains in productivity, business growth, efficiency and quality of life. It is a global technological opportunity of unprecedented scale. The inter-connectivity of wide range of devices, networks and people promises to deliver game-changing products, solutions and services along with huge cost savings, increased safety, increased process efficiencies, better customer experiences and new revenue streams.

However due to the exponential growth in connected devices and networks, IoT poses unique privacy, security and compliance challenges for businesses worldwide. As a result many businesses are hesitant to deploy IoT in their organizations. The major point of concern is due to the uniqueness of the IoT infrastructure, which merges the computer and physical worlds together, combining risks from both. Protecting IoT solutions requires secure provisioning of devices, secure connectivity between these devices and the cloud, and secure data protection in the cloud during processing and storage.

This whitepaper explores the various aspects of IoT security solutions and methods to address these issues based on tools from Microsoft Azure IoT Hub and AWS IoT.

Truths about Security

Continuous Journey: Securing IoT devices, and other physical and cloud infrastructure is really a continuous journey, not a goal. Typically, you incorporate a few security measures in your products and assume that they will be totally secure. But that is not the case, as malicious actors are continuously becoming smarter and trying to find and exploit security gaps.

Defense in Depth: It is necessary but not sufficient to build security. You require multiple layers of security to ensure that even if one layer is compromised, another will continue to protect. Layered security uses multiple components to protect operations at multiple levels.

End-to-End: The IoT infrastructure can be considered totally secure only if you protect the entire chain starting from the device, the operating system, the app running on the IoT device, the network infrastructure and all the way up to the cloud. End-to-end security is a mandatory requirement.

Not "If", But "When" & "How": The security questions paramount at all times are – when an attack occurs, are you prepared to tackle it? And are you going to be intact after the attack? Security readiness is a continuous priority.

Key Considerations

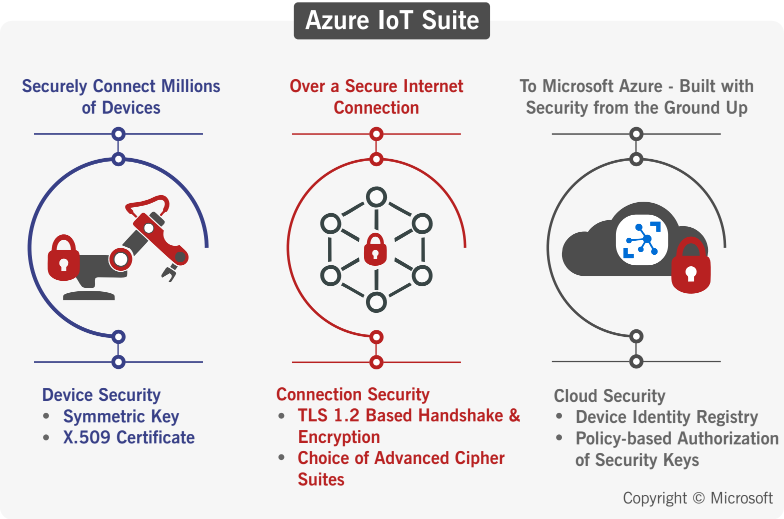
IoT security encompasses the protection of IoT devices and IoT data. Protecting IoT devices includes device on-boarding and provisioning, and device identity and authentication. Protecting IoT data includes confidentiality and integrity of communication, protection against malicious devices and protection of data at rest.

The key security features to be considered for IoT solutions can be broadly classified into:

- **Authentication:** IoT devices must be identified and authenticated before joining the IoT network. Each entity in the IoT network requires a unique identifier (UID). This also involves heterogeneous network authentication.
- **Confidentiality:** IoT data must be accessible to only authorized users. Confidential messages should be protected from hackers and snoopers.
- **Redundancy:** If a device in an IoT network fails or is compromised, then other devices must be able to provide a minimum level of security functionality with relevant security services, and still be able to protect the IoT solution from any attack.

- **Data Freshness:** An IoT solution may require access to the most recent messages or data to function effectively even when there is a security breach.
- **Anonymity & Misuse:** In some situations, users of IoT solutions may want to keep their identity secret and need assurance that their personal and other data will not be misused.
- **Liability:** In case of any misuse, loss, theft or unusual event, accountability and responsibility should be defined across the different stakeholders.

Security in Azure IoT Hub


Azure IoT Suite
Securely Connect Millions of Devices
Over a Secure Internet Connection
To Microsoft Azure - Built with Security from the Ground Up

Device Security
- Symmetric Key
- X.509 Certificate

Connection Security
- TLS 1.2 Based Handshake & Encryption
- Choice of Advanced Cipher Suites

Cloud Security
- Device Identity Registry
- Policy-based Authorization of Security Keys

Copyright © Microsoft

Figure 1. IoT Security in Azure

Microsoft Azure IoT Hub suite provides IoT security solutions by comprehensively addressing the following security areas:

- **Device Security:** Securing IoT devices while they are deployed in the field.
- **Connection Security:** Ensuring that all data transmitted between the IoT devices and IoT Hub is confidential and tamper-proof.
- **Cloud Security:** Providing a means to secure data while it moves through, and is stored in the cloud.

Azure IoT Hub uses per-device security credentials and access control to enable reliable and secure bi-directional communication between IoT devices and Azure services such as Azure Storage, Azure Service Bus, Azure Machine Learning and Azure Stream Analytics.

Azure offers several IoT security solutions:

- Azure Security Center for IoT is an Azure based cloud security service providing comprehensive IoT device threat protection from the devices to the cloud. This service unifies security management and enables end-to-end threat detection and analysis across hybrid cloud workloads and respective Azure IoT solution.
- Azure Sphere is a comprehensive IoT security solution (which includes hardware, OS and cloud components) to actively protect devices, businesses and customers. Highly secure, best in class MCU-based IoT devices can be built using this service.
- Azure Sentinel is an intelligent security analytics service, which uses AI to make threat detection, investigation and response smarter and faster.
- Azure IoT Edge is a fully-managed service built on Azure IoT Hub. This service decreases the risk of security threats, ranging from physical tampering to IP hacking, while the data and analytics is moved to the intelligent edge.

Device Security

Azure IoT Hub secures IoT devices by the following methods:

- Providing each IoT device or a group of devices a unique identity key (SAS based security tokens), which can be used by the device to communicate with Azure IoT Hub.
- Enabling each IoT device to establish Transport Layer Security (TLS) mutual authenticated connection via:

  - Self-signed X.509 certificate based authentication (BYOC) – the device and the Azure IoT Hub cloud service authenticate each other using the TLS flow. It is enabled by the Azure IoT Device SDKs.
  - Certification Authority (CA) signed X.509 certificate – identify a device and authenticate it with Azure IoT Hub, using a X.509 certificate generated and signed by a CA.

- Supporting wide range of secure hardware modules (HSMs), where each IoT device has private key in a hardware-based security module with intrinsic, immutable identity, which can be retrieved cryptographically and proven via a TLS connection.
- Protecting against malicious devices:
  - Authorization – the device token generated by Azure IoT Hub provides custom access control policies, which controls what a device can do in the cloud (read, write or both).
  - IP blocking/unblocking – the ability to enable or disable device access based on the IP Address of the device.
  - Unsolicited inbound connection – using the device SDKs, the device can only connect to services like Azure IoT Hub but will not accept any inbound connections.

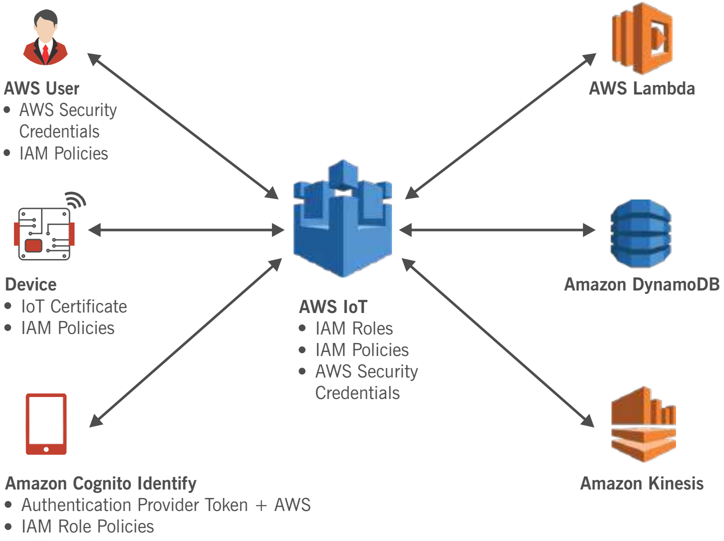
Connection Security

Internet connection between the IoT device and Azure IoT Hub is secured using the TLS 1.2 standard.

Cloud Security

Azure IoT Hub allows definition of access control policies for each security key. It uses the following set of permissions to grant access to each IoT Hub endpoint. Permissions limit the access to an IoT Hub based on functionality. The functionality can be limited based on access to identity registry (read/write), access to cloud service facing communication end points and device facing end points.

Security in AWS IoT



AWS User
- AWS Security Credentials
- IAM Policies

Device
- IoT Certificate
- IAM Policies

Amazon Cognito Identify
- Authentication Provider Token + AWS
- IAM Role Policies
- IoT Policies

AWS IoT
- IAM Roles
- IAM Policies
- AWS Security Credentials

AWS Lambda

Amazon DynamoDB

Amazon Kinesis

Copyright © AWS

Figure 2. IoT Security in AWS

AWS IoT provides secure, bi-directional communication between Internet-connected devices such as sensors, actuators, embedded micro-controllers or smart appliances and the AWS Cloud. This enables the secure collection of telemetry data from multiple devices and storage and analysis of the data.

The core components of AWS IoT are Device SDK, Device Gateway, AWS IoT Message Broker, Authentication and Authorization, Device Shadow, Rules Engine, AWS Identity and Access Management, Device Registry and Alexa Voice Service (AVS) Integration. Each of these components and services have a big role to play in securing devices, communication between the cloud and devices and the data stored on the device and the cloud.

The Security and Identity service in particular provides shared responsibility for security in the AWS Cloud. The Message Broker and Rules Engine use AWS security features to send data securely to devices or other AWS services.

AWS IoT provides IoT security solutions by comprehensively addressing the following security areas:

- **Device Security:** Securing IoT devices while they are deployed in the field.
- **Transport Security:** Securing communication between IoT devices and AWS IoT.
- **Cloud Security:** Protecting the data which moves between AWS IoT and other AWS Services and also the data at rest in the cloud.

Device Security

Each device must have its unique identity. AWS IoT supports identification based on X.509 certificates generated by AWS IoT or issued by a CA. A unique certificate for each device helps in fine-grained management including certificate revocation. Devices must support replacement of expired certificates for smooth operation.

Identities can be authenticated using AWS IoT Authentication as well as custom authentication procedures. When using the former, the AWS IoT Message Broker is responsible for authenticating the devices and when using the latter, custom authorizer is responsible for authenticating the devices.

In addition, server-side certificates allow devices to verify that they are communicating with AWS IoT and not another impersonating server. For the device to validate AWS IoT server certificate, the VeriSign® Class 3 Public Primary G5 root CA certificate needs to be installed on the device.

Transport Security

The AWS IoT Message Broker and Device Shadow service encrypt all communication with TLS 1.2. TLS is used to ensure the confidentiality of the application protocols (MQTT, HTTP) supported by AWS IoT. TLS encrypts the connection between the device and the broker. TLS client authentication is used by AWS IoT to identify devices.

AWS IoT Device Defender® helps in auditing the configuration of devices, monitor connected devices to detect abnormal behavior and mitigate security risks. It gives the ability to enforce consistent security policies across the IoT device fleet and respond quickly when devices are compromised.

The edge analytics service, AWS IoT Greengrass® authenticates and encrypts device data for both local and cloud communications so that data is never exchanged between devices and the cloud unprotected. Hardware-secured end-to-end encryption can be leveraged for messages sent between an AWS IoT Greengrass Core and the AWS cloud, and also the messages sent between an AWS IoT Greengrass Core and other local devices using the AWS IoT Device SDK.

Cloud Security

AWS Config® service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations. It provides customizable, predefined rules called managed rules to help you get started. You can also create your own custom rules. While AWS

Config continuously tracks the configuration changes that occur among your resources, it checks whether these changes violate any of the conditions in your rules. If a resource violates a rule, AWS Config flags the resource and the rule as noncompliant.

AWS Security Hub provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices. Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.

Best Practices

A comprehensive security strategy can be developed and executed with the active participation of various stakeholders involved with the manufacturing, development, and deployment of IoT devices and infrastructure based on recommended best practices.

- IoT hardware manufacturer/integrator:
  - Scope hardware to minimum requirements
  - Make hardware tamper proof
  - Build around secure hardware
  - Make upgrades secure

- IoT solution deployer:
  - Deploy hardware securely
  - Keep authentication keys safe

- IoT solution developer:
  - Follow secure software development methodology
  - Choose open-source software with care
  - Integrate with care

- IoT solution operator:
  - Keep the system up-to-date
  - Physically protect the IoT infrastructure
  - Protect against malicious activity
  - Audit frequently
  - Protect cloud credentials

Microsoft recommends a threat modelling technique called STRIDE to identify, define and mitigate IoT security threats. The idea is to classify all threats according to one of the 6 STRIDE categories – Spoofing of user identity, Tampering (integrity), Repudiation, Information disclosure (privacy breach or data leak), Denial of service (DoS), Elevation of privilege (access privilege). Microsoft also provides a threat modeling tool (https://www.microsoft.com/en-us/sdl) which can be used to design the IoT infrastructure. The tool generates the threats and one can identify and list out the mitigations for the generated threats.

Conclusion

Security is a major challenge facing IoT today. In developing new IoT solutions, businesses must consider the larger context and implications of security and privacy from the start and select the right partner, tools, methodologies best suited to serve both existing and new technologies in their customers' unique environments.

As an IoT services provider, Thinxtream has expertise in IoT security as a hardware designer and integrator, solution developer, and solution operator across Azure IoT Hub and AWS IoT. By leveraging the IoT expertise built over a decade, Thinxtream ensures cost-effective, quality and timely delivery of IoT solutions.

References

- https://www.microsoft.com/en-us/sdl
- https://aka.ms/iotarch
- https://aws.amazon.com/whitepapers/aws-security-best-practices/
- https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices

Thinxtream Technologies is a global software company with a portfolio of innovative software platforms, components, solutions, patents, competences and services for Internet of Things (IoT) across several industry verticals and applications, successfully enabling leading customers, including Fortune 500 companies, meet their application, product and business goals.

Interested in learning more? For more information contact:

Thinxtream Technologies Pte. Ltd.
220 Orchard Road #05-01
Midpoint Orchard
SINGAPORE 238852
Phone: +65 66358625
Email: info@thinxtream.com

Thinxtream Technologies, Inc.
10260 SW Greenburg Road
Suite 400 Portland, OR 97223
U.S.A.
Phone: +1 971 230-0729
Email: info@thinxtream.com

www.thinxtream.com

LinkedIn/thinxtream

All prices, specifications and characteristics set forth in this publication are subject to change without notice.

THINXTREAM®