The Internet of Things on AWS – Official Blog

Ten security golden rules for IoT solutions

by Nima Sharifi Mehr | on 20 AUG 2019 | in AWS IoT 1-Click, AWS IoT Analytics, AWS IoT Button, AWS IoT Core, AWS IoT Device Defender, AWS IoT Device Management, AWS IoT Events, AWS IoT SiteWise, AWS IoT Things Graph, Best Practices, Internet Of Things, Security | Permalink | Share

The Internet of Things (IoT) solutions help transform your operations and customer experiences across a variety of industries and uses. That unlimited opportunity brings excitement, but it also brings security, risk, and privacy concerns.

To protect customers, devices, and companies, every IoT solution should start and end with security. The best IoT security solution offers multi-layered protection from the edge to the cloud, letting you secure your IoT devices, connectivity, and data.

Ideally, you could rely on a publicly known and reusable list of security practices for every building block in your IoT solutions that are aligned with your unique requirements and constraints. However, in reality, you must plan at least some of your security strategy yourself by using security rules as your guide.

I compiled the following best practices to help you protect your business and IoT ecosystem, from design and implementation to ongoing operations and management. A list of high-level recommendations follows each rule as well. These recommendations are not an exhaustive list and only clarify the underlying concepts behind each rule.

1. Provision devices and systems with unique identities and credentials.
2. Apply authentication and access control mechanisms.
3. Use cryptographic network protocols.
4. Create continuous update and deployment mechanisms.
5. Deploy security auditing and monitoring mechanisms.
6. Build continuous health checks for security mechanisms.
7. Proactively assess the impact of potential security events.
8. Minimize the attack surface of your IoT ecosystem.
9. Avoid unnecessary data access, storage, and transmission.
10. Monitor vulnerability disclosure and threat intelligence sources.

Glossary of terms

Familiarize yourself with the following terms to help you navigate both this list of best practices and the larger world of IoT resources that exist across the internet.

Attack surface: All entry points of your systems that a bad actor could target to obtain unauthorized access to your assets, such as sensitive data, device functionalities, or computing and networking capabilities.

Deployment artifacts: All source code, configuration, and binary files that users need for secure and reliable software or firmware installation on IoT devices or general-purpose hosts.

IoT ecosystem: All elements and building blocks of your IoT solution, including device hardware and firmware, on-premises and in-cloud systems and software, and processes such as device manufacturing, shipping, and provisioning.

Principle of least privileges: A security best practice to only grant identities with the least number of privileges required to perform their intended operations within expected contexts.

Threat model: A living document that captures your assets and the systems that interact with them. It also includes the trust boundaries of your systems and their entry points, relevant threats to your assets, and corresponding mitigation or accepted risks.

1. Provision devices and systems with unique identities and credentials

- Assign unique identities to all devices and on-premises or in-cloud systems of your IoT ecosystems.
- Assign unique and cryptographic credentials such as X.509 certificates to each identity.
- Create mechanisms to facilitate the generation, distribution, rotation, and revocation of credentials.
- Opt to use hardware-protected modules such as Trusted Platform Modules (TPMs) or hardware security modules (HSMs) for storing credentials and performing authentication operations.

AWS resources

AWS provides the following assets and services to help you identify, sort, and secure your IoT assets:

- Security and Identity for AWS IoT
- Amazon Cognito, a service that provides authentication, authorization, and user management for your web and mobile apps
- AWS Identity and Access Management (IAM), a service that enables you to manage access to AWS services and resources securely

2. Apply authentication and access control mechanisms

- Establish clear trust boundaries in your IoT ecosystem based on your threat model, and enforce access controls on all access outside those boundaries.
- Identify and mitigate issues with entry points in your IoT ecosystem that can facilitate forging or spoofing identities and unauthorized escalation of privileges.
- If your threat model includes potential physical access to devices by unauthorized actors, tamper-proof your devices' hardware and disable any unused hardware interfaces physically and/or at the firmware or operating system layer.
- Create mechanisms to assess the credentials and privileges of your IoT ecosystem periodically as well as when their associated identities transition through lifecycle events.
- Consider physical access controls such as tamper-proofing devices as an additional layer of defense.
- Enforce resource consumption limits and throttling to protect the availability of shared resources.

AWS resources

AWS provides the following assets and services to help you authenticate and manage access:

- Security and Identity for AWS IoT

- Amazon Cognito
- AWS Identity and Access Management (IAM)
- Deploy Secrets to the AWS IoT Greengrass Core

3. Use cryptographic network protocols

- Protect the confidentiality and integrity of inbound and outbound short and long-range network communication channels that you use for data transfers, monitoring, administration, provisioning, and deployments.
- Protect the integrity of data, regardless of classification level, by using cryptographic network protocols to detect any unauthorized modification.
- For resource-constrained devices that cannot support cryptographic network protocols, you should limit their network activity to short-range connections within network-level trust boundaries as identified in your threat model.
- Employ open and standard cryptographic network protocols that the security community publicly and continuously vets and peer-reviews. Using cryptographic primitives such as one-way hash functions or encryption functions cannot replace cryptographic protocols for protecting data in transit. Cryptographic protocols consider contextual information required for enforcing data transportation security controls. These include recipient authentication, secure cryptographic key exchange or negotiation, and message order integrity and successful message delivery verification.

AWS resources

AWS provides the following assets and services to help you encrypt your networks:

- AWS IoT SDKs, to help you securely and quickly connect your devices to AWS IoT
- Amazon FreeRTOS Libraries, to provide additional functionality to the FreeRTOS kernel and its internal libraries

4. Create continuous update and deployment mechanisms

- Use cryptographic network protocols for transferring deployment artifacts.
- Apply and verify digital signatures on distributed deployment artifacts.
- Apply a default configuration for deploying security updates and patches automatically.
- Employ authentication and access controls on deployment artifact repositories and their distribution systems.
- Maintain an inventory of the deployed software across your IoT ecosystem, including versions and patch status.
- Monitor status of deployments throughout your IoT ecosystem and investigate any failed or stalled deployments.
- Use version control mechanisms to prevent unauthorized actors from forcing firmware or software downgrades.
- Maintain notification mechanisms to immediately alert stakeholders when your infrastructure can’t deploy security updates to your fleet.
- Create mechanisms to identify and replace constrained-devices that are not capable of receiving updates.

- Create detection and response mechanisms to handle unauthorized changes in deployed software or firmware.

AWS resources

AWS provides the following assets and services to help you organize and maintain a continuous development and deployment pipeline:

- Amazon FreeRTOS Over-the-Air Updates
- OTA Updates of AWS IoT Greengrass Core Software
- AWS IoT Jobs, to define a set of remote operations that you send to and execute on one or more devices connected to AWS IoT
- AWS Release Notes

5. Deploy security auditing and monitoring mechanisms

- Deploy auditing and monitoring mechanisms to continuously collect and report activity metrics and logs from across your IoT ecosystem.
- Monitor on-device and related off-device activities such as network traffic and entry points, process execution and system interactions for any unexpected behavior.
- Maintain and regularly exercise a security incident response plan along with containment and recovery mechanisms. This should be in correspondence to the technical skill level of operators of your IoT elements and their deployment and ownership model.

AWS resources

AWS provides the following assets and services to help you monitor your security at varying levels:

- AWS IoT Device Defender, to secure your fleet of IoT devices
- Monitoring AWS IoT with CloudWatch Logs, to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service
- Logging AWS IoT API Calls with AWS CloudTrail, to provide a record of actions taken by a user, a role, or an AWS service in AWS IoT
- Monitoring with AWS IoT Greengrass Logs
- Amazon GuardDuty, to continuously monitor for malicious activity and unauthorized behavior to protect your AWS accounts and workloads
- AWS Security Incident Response Guide

6. Build continuous health checks for security mechanisms

- Continuously check that your security controls and systems are intact by using mechanisms such as canary tests.
- Verify that security controls prevent unauthorized access and maintain their integrity in the event of external dependency or internal system failures.
- Test your IoT devices to ensure that they maintain their security controls in the event of failures such as:

  - Low or fluctuating battery power
  - Low memory or processing resources
  - Malfunctioning physical sensors or other attached devices
  - Ingestion of malformed inputs including sensed data
  - Absence of network connection or intermittent connectivity

AWS resources

AWS provides the following assets and services to help you monitor the integrity of your security apparatus:

- AWS IoT Device Defender
- AWS Config, to assess, audit, and evaluate the configurations of your AWS resources
- Amazon CloudWatch

7. Proactively assess the impact of potential security events

- Create and maintain a threat model that encompasses all assets and systems across your IoT ecosystem.
- Identify and measure the impact of a security event on your IoT devices, their sensed environment and actuation systems, their associated on-premises and cloud infrastructure, human operators and supply chain systems, and processes.
- Consider different elements of security events such as scale, sophistication, and level of unauthorized access to assess potential impact and create corresponding in-depth layers of prevention, detection, containment, and recovery.
- Provision your devices and field gateways with credentials that grant only the required privileges.

AWS resources

AWS provides the following assets to help you determine the effects of a security breach:

- AWS Shared Responsibility Model for security and compliance

8. Minimize the attack surface of your IoT ecosystem

- Identify and eliminate unused entry points on your devices, field gateways, and backend systems.
- Disable unused device sensors, actuators, services, or their unused functions.
- Disable unused functionality or insecure-by-default configurations in your dependencies.
- Use the least possible number of dependencies, such as third-party libraries and network services.
- Employ secure-by-default configurations across your IoT ecosystem.
- Only add well-maintained dependencies, and establish a mechanism to keep them up-to-date.
- Regularly review and identify attack surface minimization opportunities as your IoT ecosystem evolves.

AWS resources

AWS provides the following assets and services to help you analyze and reduce your attack surface:

- AWS Cloud Security

- Security and Identity for AWS IoT
- AWS IoT Greengrass Security
- AWS Well Architected Framework, IoT Lens, a document that covers commonly encountered IoT use cases and identified key solution elements to ensure that your workload architecture uses established best practices

9. Avoid unnecessary data access, storage, and transmission

- Identify and classify data collected throughout your IoT ecosystem and learn their corresponding business use-case.
- Identify and execute on opportunities to stop collecting unused data or adjusting their granularity and retention time.
- Consider using tokenization and one-way cryptographic hashing wherever you don't need specific data in its entirety.
- Consider using asymmetric cryptography to protect data at rest on IoT devices and devices that are only responsible for temporarily collecting and batching data and periodically submitting the data to other systems for processing.
- Only store and transmit data to central systems with strong ownership and strict security controls.
- Follow the principle of least privilege in granting access to any collected data.
- Identify and consider the unique capabilities of your IoT devices. This could include mobility, actuation, sensory data collection and transmission, and ownership transfers that impact your regulatory and legal compliance.
- Consider privacy and transparency expectations of your customers and corresponding legal requirements in the jurisdictions where you manufacture, distribute, and operate your IoT devices and systems.

AWS resources

AWS provides the following assets and services to help you limit access to data and other resources:

- AWS Data Privacy
- AWS Privacy Notice
- AWS Compliance Programs and Offerings
- AWS Compliance Solutions Guide

10. Monitor vulnerability disclosure and threat intelligence sources

- Stay informed about disclosed vulnerabilities, adversarial techniques, tactics, and procedures used in recent attack campaigns and assess their impact on the security of your IoT ecosystem.
- Correlate information from vulnerability disclosures and threat intelligence with auditing events, configuration, and metadata from your IoT ecosystem. This way, you can detect any trends of involvement or abuse of your infrastructure in the context of ongoing adversarial campaigns.
- Create a vulnerability disclosure program for your IoT solutions to facilitate engagement with security researchers and their responsible disclosure of potential security issues.

AWS resources

AWS provides the following assets and services to help you keep up-to-date on security news:

- AWS Security Bulletins

Conclusion

This post reviewed some of the best practices for keeping your IoT infrastructure secure. I hope this helps guide you in your efforts to protect your IoT devices, their connectivity, and the data that they generate. To learn more about how AWS IoT services help you achieve end-to-end security for your IoT solutions, check out the on-demand webinar, Securing Your Devices from the Edge to the Cloud.

If you have your own best practices for maintaining IoT security, comment here to share your insights.

TAGS: internet of things security, IoT Best Practices, IoT Security, Secure IoT devices