Best Practices for Edge Security with Amazon FreeRTOS

Dan Griffin

July 30, 2019

Edge security: what’s in it for me?

- Retain customer trust.
- Stay competitive.

aws

Agenda

- What is Amazon FreeRTOS?
- Key elements of security
- Demos
- How to do the demos yourself

aws

What is Amazon FreeRTOS?

- MIT-licensed operating system for microcontrollers
- Easy to program, deploy, secure, and maintain
- Extends FreeRTOS kernel
- Connects and operates devices securely
- https://github.com/aws/amazon-freertos

aws

Key elements of security

- Appropriate credentialing
- Secure onboarding
- Over-the-air updates/patching
- Monitoring
- Auditing
- Remediation

aws

Appropriate credentialing

aws

Appropriate credentialing

- AWS account administrators
- AWS programmatic/script access
- IoT devices

aws

Secure onboarding

aws

Secure onboarding

- Software development lifecycle
    - Pre-tested configurations
    - Automated functional testing
    - Formal modeling
- Device-to-cloud registration
    - Just-in-Time Registration
    - Just-in-Time Provisioning
    - Bulk Provisioning

aws

Over-the-air updates/patching

aws

What are over-the-air updates?

- Firmware upgrades at scale for Amazon FreeRTOS devices
- Deploy firmware updates to one or more devices in your fleet
    - Chunk data over mutually authenticated MQTT
    - Minimize RAM and ROM footprint with this approach
- Uses AWS IoT Device Management
    - Device group selection for scaled roll-out
    - Job scheduling and status tracking
- Digitally sign firmware images to ensure authenticity
    - AWS Certificate Manager
    - AWS Signer

aws

Planning for OTA

- Why patch:
    - Firmware feature enhancement
    - Functional bug fix. For example, https://github.com/aws/amazon-freertos/blob/master/CHANGELOG.md.
    - Security bug fix. For example, https://aws.amazon.com/freertos/security-updates/.
- When to patch:
    - Change validation process
    - Lab testing
- How quickly to patch:
    - Scaled rollout
    - Success criteria

aws

Monitoring

aws

Monitoring

- What are your monitoring goals?
- Which resources will you monitor?
- How often will you monitor these resources?
- Which monitoring tools will you use?
- Who will perform the monitoring tasks?
- Who should be notified when something goes wrong?

aws

Auditing

aws

Auditing

- Ensure security measures are in place
- Baseline against security best practices
- Detect policy drift

aws

Remediation

aws

Remediation

- Establish procedures for tracking policy violations
- Test and deploy the policy fix
- Implement other mitigations as appropriate
- Could there have been data leakage?
- Does a business process need to change?

How to do the demos yourself

- Start with the simulator
  - https://aws.amazon.com/freertos/getting-started/
  - https://docs.aws.amazon.com/freertos/latest/userguide/getting_started_windows.html
- Be aware of the test infrastructure
  - https://aws.amazon.com/freertos/device-tester/
  - https://github.com/aws/amazon-freertos/tree/master/tests
  - https://github.com/aws/amazon-freertos/tree/master/tools/cbmc

aws

Thank you!