Technical Article

Amazon Web Services and TI Team up to Provide an End-to-end OTA Solution for IoT Devices

Nick Lethaby

Over-the-air (OTA) updates enable remote patching of bugs or security flaws and are an important asset to connected devices. A poorly implemented OTA process, however, introduces significant risk to both original equipment manufacturers (OEMs) and consumers. Because a flawed update can “brick” (render nonfunctional) a connected device, OTA updates offer an opportunity for the introduction of malware that can compromise security for both consumers and the OEM.

I recently had an OTA update go wrong when my Android phone hung during the early stages of an update. There was no way to force a reset manually, and I had to wait 12 hours until the battery died. After resetting, my phone began correctly using the previously installed version of Android.

Fortunately I was at home at the time, so having a phone was not critical. However, had I been out meeting engineers and relying on my phone’s navigation to get around, I would have been in serious trouble. I was thankful that my phone had one key OTA safety-net feature built-in: the ability to revert to the previous software version so that my device worked again. I would just rather not have had to wait 12 hours for that reversion to occur!

There have been publicized cases of Internet of Things (IoT) products such as smartlocks that were rendered permanently unusable by OTA updates unless they were sent back to the manufacturer to be fixed. So when designing a connected device, it's important to implement OTA updates in a manner that avoids reliability or security problems.

OTA Out of the Box

Since an OTA implementation requires the interaction of cloud-based software services with embedded software on the connected device, providing a pre-integrated solution requires cooperation between the cloud-computing vendor and the semiconductor provider. Amazon Web Services (AWS) and Texas Instruments (TI) have worked together to provide an end-to-end OTA solution that reduces the probability of security breaches or bricked devices. This solution combines the AWS IoT Core service, Amazon FreeRTOS and TI's SimpleLink™ Wi-Fi®-connected microcontrollers (MCUs).

Amazon FreeRTOS is an embedded software stack based on the FreeRTOS operating system, optimized to run on MCUs with limited memory. Amazon FreeRTOS includes embedded software components that communicate with the cloud-based AWS IoT platform, which provides device management and telemetry. Device-management services include support for OTA updates, which in turn leverage other AWS services such as Amazon Certificate Management for code signing. The embedded software stack provides an OTA agent that executes on the MCU as a FreeRTOS task, coordinating OTA operations such as downloading a new image from the cloud, authenticating the image and handling any interruptions during download.

SimpleLink Wi-Fi MCUs and the associated SimpleLink software development kit (SDK) include wireless networking, security, storage, bootloader and OTA image-management software. Amazon FreeRTOS uses these SimpleLink software components to implement its OTA update mechanism (see Figure 1).

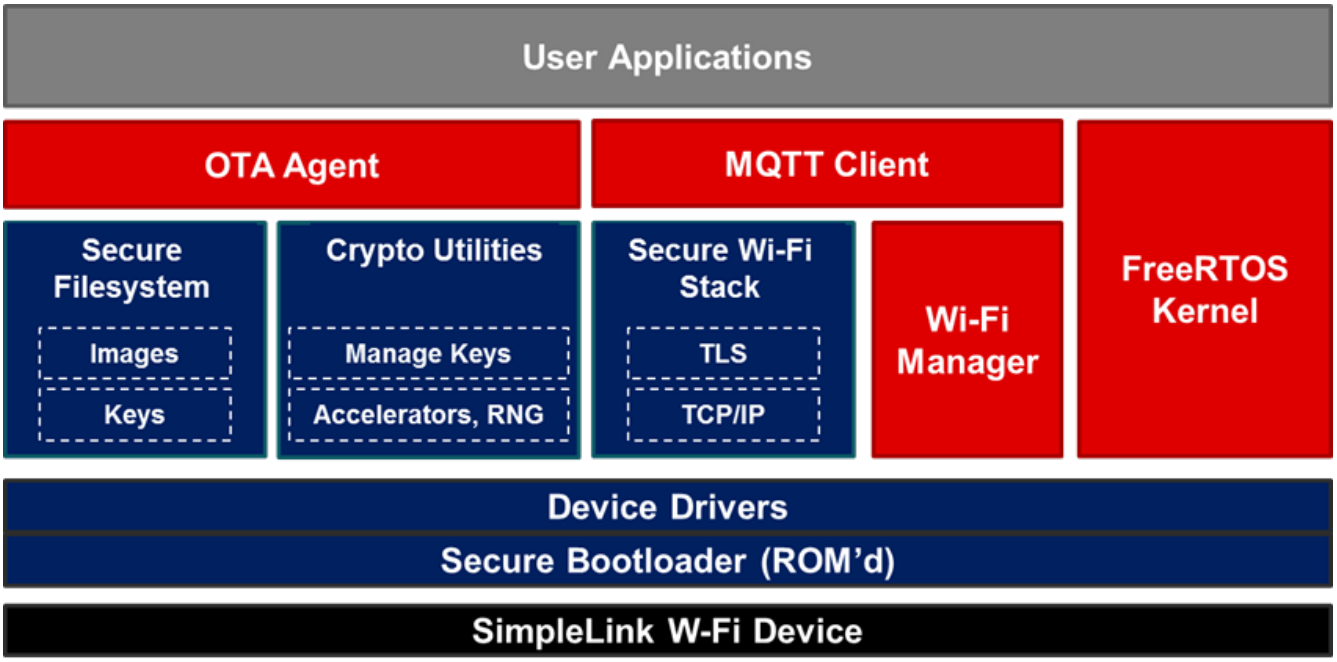

Figure 1. Amazon FreeRTOS (Red) Leverages Many SimpleLink Features (Blue) in Its OTA Update Solution

SimpleLink Wi-Fi devices offer a complete Transmission Control Protocol/Internet Protocol and Wi-Fi stack with Transport Layer Security to enable a secure, encrypted Message Queuing Telemetry Transport connection to the AWS cloud. SimpleLink Wi-Fi on-chip cryptographic accelerators enable the AWS OTA agent to efficiently authenticate the origin and integrity of the OTA image and guard against man-in-the-middle attacks attempting to substitute malware.

The OTA agent uses the SimpleLink Wi-Fi file system to securely store OTA images so hackers cannot access them and enables a test boot of the OTA image. In cases where the OTA image hangs or fails its self-test, the device automatically reverts to the previous image version available, thus preventing a bricked device.

SimpleLink Wi-Fi MCUs also include special pins for use in your design that enable consumers to force the IoT product to boot using its original factory image. This would have been very useful for my phone to have, as I could have had it working again immediately rather than waiting 12 hours.

Additional Resources

To Learn More about Amazon FreeRTOS and TI's SimpleLink Wi-Fi Devices:

- Download the white paper, "A more secure and reliable OTA update architecture for IoT devices."
- Access detailed documentation for Amazon FreeRTOS OTA updates and get started with Amazon FreeRTOS and SimpleLink Wi-Fi devices.
- Navigate to the SimpleLink Wi-Fi SDK and documentation.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265