Q&A for Tech Talk Topic: IoT Security

Q: Where are the presentations for previous Tech Talks?
A: All previous Tech Talk recordings and slides are available at https://www.silabs.com/about-us/events/tech-talks

Q: Can you compare Wi-Fi, Z-Wave and Bluetooth security at a high level; which is most robust?
A: This is a hard question, because it depends on how you define security strength. All protocols are evolving into more secure versions of themselves. And all protocols have some need to provide backwards compatibility, which can weaken security. At the moment, BLE and Z-Wave are favored targets in the security research community. I expect that the outcome of this activity will result in stronger implementations of each.

Q: Is there any universal platform of trust available in the Americas?
A: If you are referring to standards-based security used by all chips on the market, there is no such thing. Different vendors provide various levels of security features either implemented in HW (secure element, PUF, DPA, encryption blocks) or SW implementations of encryption algorithms.

Q: If company A deploys an IoT system based on company B's IoT solution, which company bears the responsibility to meet the regulatory requirements? A, B, or both?
A: Regulatory requirement responsibility will likely fall to the product maker, at least that's how regulations in other industries are enforced. In the event of a security vulnerability in Silicon Labs hardware or software, we share in the burden of mitigation and communication. If a security researcher notifies one of our customers of a vulnerability in their product whose root cause is in one of our stacks or hardware, we expect that customer to reach out to us so we can help. Our website for reporting security vulnerabilities is here: https://www.silabs.com/security/product-security

Q: Is the Bluetooth mesh stack reliable for large-scale applications?
A: Yes, we test every release of our Bluetooth mesh stack on our own large-scale test network with a rigorous QA process. You can learn more about large-scale testing at https://www.silabs.com/products/wireless/learning-center/mesh-performance. Also see our AN1137 here: https://www.silabs.com/documents/public/application-notes/an1137-bluetooth-mesh-network-performance.pdf

Q: I appreciate your chips. I use Silabs on all my projects since Bluetooth indoor applications to Wi-SUN based stack developed by my company.
A: Thank you for your business!

Q: What is the architecture of your secure element MCU?
A: It's a 32-bit core, which is isolated and independent of the main Cortex-M33 core and runs Silicon Labs signed firmware.

Q: Is any of this somehow related to Zentri Device Management Service and/or OTA? Any starting documentation to look at if so?
A: The Zentri DMS is based on a different technology. Most of this presentation is focused on our Series 2 wireless devices and we have several application notes covering Secure Boot with RTSL, Secure Debug and how to use the Bootloader. Here are some links:

https://www.silabs.com/documents/public/application-notes/an1218-secure-boot-with-rtsl.pdf
https://www.silabs.com/documents/public/application-notes/an1190-efr32-secure-debug.pdf
https://www.silabs.com/documents/public/application-notes/an1222-efr32xg2x-production-programming.pdf
https://www.silabs.com/documents/public/user-guides/ug266-gecko-bootloader-user-guide.pdf

Q: Does Silicon Labs offer security features beyond what ARM provides?
A: The security functionality of the Series 2 products, including Secure Boot with RTSL, Secure Debug, crypto accelerators, DPA countermeasures, TRNG, secure key storage, and anti-tamper do not use or depend on ARM technology in any way.

Q: We use the MGM210PA22. Will it be possible to upgrade to the MGM210PB22 with software?
A: You cannot, because the internal IC is different (EFR32MG21A vs. EFR32MG21B). To upgrade your module to use Secure Vault you will need to use the 'B' part number. They are pin-compatible.

Q: How do you implement anti-rollback in EFR32 architecture?
A: This link explains the anti-rollback feature in detail: https://www.silabs.com/security/anti-rollback

Q: How do you interface the BG22 to an external SPI flash memory?
A: The BG22 does have a SPI interface, supported by any of the USARTs.

Q: Is there any way to recover an erased PUF?
A: To maintain appropriate safeguards, erasing a PUF key is by design a one-way operation.

Q: Are Silabs secure elements integrated with OpenSSL?
A: We don't support the OpenSSL library. Instead we use ARM's mbedTLS TLS/crypto library which supports ARM PSA. This is an open source library released under the Apache 2.0 license.

Q: Got the SCA and DPA...what about fault injection via power glitches, laser, and RFI?
A: We handle this through the tamper detect feature in the EFR32xG21B with Secure Vault, which includes hardening the SE code to add glitch resistance around critical security operations.

Q: A key feature of security moving forward appears to be the ability to support software/firmware updates in the field to address any future vulnerabilities identified. However from previous tech talks a number of the new BLE/Zigbee/Thread parts do not have enough flash to support this robustly. How do you suggest these parts are kept up to date with the latest security features/patches?
A: The answer depends on which piece of firmware is being patched. In all cases the OTA storage area must be large enough to contain the entire application and an entire SE firmware image (which is ~49k). Patches to the SE firmware take up SE flash space but do not take up M33 flash space once they are applied. If a stack is patched, you are correct, the device needs to have sufficient flash to hold the new stack + application instance. Other options are to store an OTA image in external SPI flash, or choose a chip with additional flash.

Q: What solution being provided for quantum computing - rotating curves, keys, etc..?
A: We don't have any accelerators to support quantum-resistant algorithms today (because we don't know at the moment which ciphers are going to be widely adopted). For some elliptic curves, we support parameterized variants so if a NIST curve is found to be vulnerable we can accept an augmented curve equation. Rotating keys is a different question altogether whose answer depends on which keys are being considered.

Q: Can just your data be corrupted (i.e. ransomware. etc.)
A: I'm not aware of any ransomware attacks like this on IoT systems, but if a hacker was able to achieve remote code execution they could conceivably encrypt sensitive data and hold it hostage. This is a harder exploit to undertake on Cortex-M than Cortex-A, and can be made even harder by configuring the device to not execute code from RAM (NX).

Q: Can PUF be erased when power is OFF?
A: The PUF keys are extracted from the IC only when power is applied (there is no key present when power is off), but if the flash page containing the helper data is erased by another means, such as UV light after decapping, that would effectively erase the key.

Q: This was a great overview of how the security functions on each chip or node. It there an overview of how a product company would handle millions of nodes and the associated keys?
A: Key management can certainly be a real maintenance headache. We try to minimize the number of keys required as follows: 1) You don't have to store the device certificates for each device in your fleet because you can perform the signature check of the entire device certificate chain every time you need to do an authentication operation. 2) All the other keys on the device have fleet-wide scope, which includes the Sign key used for secure boot and secure updates and the Command key used for Secure Debug.

Q: Is PUF based on TRNG?
A: Both a PUF and a TRNG are entropy sources. However, a PUF is more like an entropy source that implemented in NVM. It's unique for each device, but for each device it provides the same answer every time you power it on. The physical construction of the PUF is an SRAM array. The physical construction of the TRNG is an array of detuned oscillators.

Q: Can you recommend a good tutorial for Simplicity Studio?
A: We have several quick starting guides for different protocols. For example, if you are interested in Bluetooth you can use the following QSG, and it covers Simplicity Studio as well:
https://www.silabs.com/documents/public/quick-start-guides/qsg139-getting-started-with-bluetooth.pdf

Q: Is the self certificate device available on all Series 2 products , or only on the one which has the keystore ?
A: Secure Identities is a feature only available on Vault products.

Q: Can RTSL be disabled at development time?
A: Secure Boot with RTSL is disabled by default and must be explicitly enabled by the user, either during production time or via a mailbox command if the device is already in service. Once enabled, Secure Boot will be enabled for the life of the device. It can't be disabled by any means, even if you erase the flash memory completely. Usually you will develop your product with Secure Boot disabled, and then Enable Secure Boot in the late stages of development to ensure proper functionality and operation.

Q: What relationship/contract is likely required between device designers/manufacturers and SiLabs to get the greatest benefits of SiLabs security features? Is there a likely lower scale threshold where that isn't going to work? I compare with custom USB PIDs piggybacking on Silabs IDs, which has worked well even for very small device runs/small manufacturers.
A: Our long-term goal is to make strong security so easy to implement that everyone can do it and achieve the same great results. In the meantime, we will be writing Application Notes and User's Guides that describe best practices for secure system design. For specific questions around device-level and firmware-level recommendations, please open a support ticket and we will help out. If your questions extend beyond the device, we can also recommend some third parties have security expertise in applications and cloud services.

Q: Great presentations! Thanks!
A: