Q&A for Security in IoT Webinar

Q: Is there a survey for today's session?
A: No survey today, but you can ask questions via Q&A and we will answer here. Mike may answer them live, or we will follow up with you later with a PDF of all questions and answers.

Q: Who defined the “legislation” for IoT devices security in the US
A: The short answer is that in the US there is no central regulation, each US state is writing their own legislation. We believe that NIST will be used by the courts as guidance as to what "reasonable security" constitutes.

Q: Is there a Silabs doc explaining each feature presented in the secure portfolio slide?
A: Yes. The best launchpad of an overview of our security technologies is www.silabs.com/security. More documentation will be added in due course such as application notes.

Q: Mike, does Silabs present asymmetric acceleration? what is your rational for this?
A: The products that Mike is talking about support both symmetric (AES-128, 192, 256) and public key (ECC-256 and other curves) acceleration engines and hashes (SHA-256, etc.)

The rationale for using public key methods for authentication and key derivation is that sensitive private keys for Secure Boot, for example, don't need to be loaded into the device... Hacking a single device doesn't give a hacker the ability to sign firmware images like it does with symmetric cryptography methods.

Q: How can you tell which feature set (basic, root of trust, secure element, Secure Vault) applies to which SiLabs IoT product part no.?

A: Some example families are listed at the very bottom of each column. The data sheets and reference manuals for the products will also contain the info regarding the crypto features included in the product.

Q: Does all the security hardware affect the ASP of the chip, and reduce SiLabs profitability for the IOT?
A: Certainly, but it is a flat playing field that all vendors have to participate in both due to regulation and to protect the market from malicious intent.

Q: Mike, are you saying that with the challenge and response you don’t need a certification authority? How does that work?
A: Silicon Labs is a certificate authority for our device certificates. We also offer certificate customization services which allow the certificates to be issued from an external certificate authority, like AWS IoT, Azure, etc.

Q: Does Secure Vault implement the TPM spec? (Trusted Platform Module)
A: No, not currently. We took the elements of the NIST recommendations including Common Criteria, SESIP, and other standards to inform our security architecture, design principles and feature set. We have some customers looking at Secure Vault to provide TPM functionality.

Q: How do you position your solution against the stand-alone vendor solutions?
A: Talking specifically to Secure Elements. External Secure Elements implement the same functions as those integrated into a chip, but they do not create a secure system by simply placing them on the board.

You still need a microcontroller to run the Application and Stack that MCU still needs to be securely booted and updated meaning this still needs to be a secure MCU. The MCU and SE need to be securely bound to maintain the overall system security, which is not a trivial exercise. Putting the SE into the secure MCU will inherently take care of this complex binding issue, reducing attack vectors and simplifying costly developer effort.

Furthermore, integrating the Secure Element reduces board space and Bill-of-Materials.

Q: Thank you guys for your answers!
A: Thanks! We appreciate your thoughtful questions and participation!

Q: I may have missed this... on the "versions and features" table, there were different levels of security for different components. Are those enhanced security features associated with more expensive components, or are the security features increased because the components are newer releases?
A: In the versions and features table, some columns in the table represent generational differences between older families and newer families, some older devices may not have the required hardware to run certain security features.

As an example, some older devices do not have the hardware support to offer advanced features such as Secure Key storage or advanced Tamper detection and response capability.

Q: Can you elaborate on mass Over-the-Air (OTA) updates?
A: Upgrades are a key requirement seen in many of the new emerging regulation. Upgrades can be done in many different ways, but Over-the-Air upgrades allow developers and manufacturers a mechanism where they can update an entire deployment within a short period of time. This maybe to close security holes, or to address product feature sets. Over-the-air updates provide for a closer relationship between end customers and manufacturers.

Q: How does the Secure Vault respond to environmental conditions like voltage?
A: The Vault products have a sophisticated Tamper Detection and response subsystem.

Example tamper sources can include environmental excursions including over and under temperature or over and under voltage, as well as glitch detection on clocks, power rails, and via EMI probes.
The response to tampers is configurable. Developers can choose to ignore, generate interrupt, generate reset, and even decommission a device in the extreme cases.

Q: What IoT verticals does SiLabs see security being required?
A: All IoT market segments should consider adding security to their products as the Ecosystem is only as strong as its weakest link. Any IoT device could create some problem for the Ecosystem or could be used in Pivot Attacks. A solid secure base helps cover attack vectors holistically.

Q: So is the primary drive of these attacks to get server access? Because I can imagine more basic "nuisance" attacks (like making a window think it's constantly opening and closing) could be quite hard to defend against if the sensor only sends out fairly basic signals.
A: Not necessarily, there are many reasons those with an intent to attack a device may want to do it. User data from a server is one aspect, but ransomware attacks are focused on operational technology (OT). Ransomware attacks are about creating inconvenience such that you pay for it to stop... however that is achieved whether at the sensor or at the server.

In the case of a window sensor, security can be used to stop a ransomware attack creating a nuisance that manifests as brand damage.

Q: Is ZigBee stack/SDK plan to have network key / link key stored in a secure way using vault mechanism or is this need to be developed/implemented by customer?
A: Stack integration of Vault Secure Key Storage is in the short-term roadmap item for all of our stacks that have sensitive keys, such as Zigbee.
Once implemented, the stacks will automatically use Secure Key Storage if they are running on a Vault-enabled device, and if not, they will store the key as securely as the device is able.

Q: How does the Secure Vault manage key provisioning and ongoing certificate management, does SiLabs have relationships in industry?
A: Silicon Labs is a certificate authority for our device certificates.
The device certificates are provisioned during device manufacture and burned into OTP memory and last for the life of the device (or 100 years, whichever comes first).
We do offer customization services that enable us to issue and provision certificates from an external certificate authority as well.

Q: Security costs money. If as a manufacturer, I want to save some money and yet make a reasonably secure system, what would be the most recommended security features provided by SiLabs HW that I should use?
A: The most foundational security that I believe all products should now implement are:
1) Secure Boot: to verify the software running on a device is what you think it does - and it is not modified by malware or ransomware. A good attack would appear to allow the device to operate as expected but also run stealth operations.
2) Secure Key Management: because keeping the secret keys secret is the basis of all security systems and architectures.

Q: Are you Azure Sphere certified?
A: Azure Sphere is designed mostly to support larger MPU/A-Class processors, our products are much smaller low-cost, low-power MCU type products.

Q: Could you provide more details regarding key provision using the PUF in the Secure Vault? Do you keep a database to manage the public keys of all of the devices that you provision, or can this be managed by the customer themselves?
A: The PUF is only used to derive a unique hardware encryption key that is used for Secure Key Storage. We don't use the Physically Unclonable Function (PUF) key for device identity. For Secure Identities, which is where device-specific public keys come into play, during device manufacturing we tell the device to generate a unique key pair using its True Random Number Generator (TRNG) and to securely store its private key (which gets encrypted by the PUF key in this process). We export the public key from the device and wrap it in an X.509 device certificate that is signed into a Silicon Labs certificate chain. By default, we don't keep a record of all of the public keys associated with

the device certificates we issue because we don't need to. Any device can be authenticated by verifying its certificate chain against the root certificate stored in our external Certificate Authority (CA) website.

Q: When you say update, isn't it weird to sell and end device that does a simple task and have to periodically update the software?
A: There are classes of devices, mostly unconnected ones, that will never need or be able to support software updates. But connected devices require a software update capability because they expose an attack surface that can be accessed remotely. A vulnerability in a simple device can still be used to exfiltrate sensitive data or to repurpose the device to support a malicious intent. Being simple is no excuse for being unsecure.

Q: How do you select the level of security? The standards seem to say: "secure everything with the maximum security". How do you make tradeoffs on security features?
A: The regulations today lack the details regarding the definition of what "acceptable level of security" is for each application. Different applications will have different security level requirements. For example, medical devices may require a higher level of security than a connected toy. The way that the industry is moving is that the security requirements for a given system or market will be defined by a specific protection profile that products can be measured against to determine if their level of security is sufficient. However, until those guidelines are in place, the definition of "acceptable level of security" is determined by the court.

It should be noted that the NIST type organization are setting the minimum bar as opposed to the maximum bar for security.

Q: Do you offer provisioning services for Keys, certificates, ... which are customer related.
A: We offer device and security customization services in which we can program customer firmware, public keys, or sensitive keys. We can also provision and customize device certificates as well, with some degree of flexibility.

Q: For a remote functional devices - there's a need for an updater. For secure OTA updates, you will need to have 2 sets of memory - how to?
A: If we take a Bluetooth OTA upgrade as an example, there are several options and configurations. In the typical case, the OTA upgrade is delivered to the Application, and the Application stores the OTA upgrade in local storage, which can be on-chip (if there is sufficient flash available) or an off-chip memory such as a SPI flash. After the image has been verified and stored, the Application marks the image for upgrade and resets the device. On reset, the bootloader notices the upgrade is pending, verifies the image for authenticity, and then applies the upgrade over the old Application. If you look at recently introduced Bluetooth SoC's, you will see a shift in the ratio of flash to RAM because manufacturers are putting additional flash memory on the device specifically to store upgrade images.

Q: Thanks!
A: You're welcome! Thanks for attending!