Securing the Internet of Things (IoT)

MICROCHIP

When looking at the global market activity related to IoT, all the major brands in all the segments have finally embraced a strategy towards IoT. In addition, the vast majority of small to mid-size businesses have committed investments in the same direction and not an isolated initiative by the high-tech giants. But what does it mean? Really, it comes down to aggregating data from embedded systems starting at the sensor level, to then add intelligence to the information collected and finally create a response. The response can be an executive decision on a business operation, an operator being deployed to repair an air-conditioned unit, an oil and gas plant manager monitoring the operations of the platform to maximize its efficiency. The hype since 2014 has been on the wireless connectivity and protocol standards has shifted to security in 2H'2015. Embedded security is a mandatory function for IoT and yet it is misunderstood and misused by the mass.

Hackers target to penetrate a network is to look for the weakest link in the architecture. For IoT, the "thing" is likely that weak spot. Software used to crawl the internet to identify unsecured devices is easily available online. The Distributed Denial of Service (DDoS) attack on Oct 21, 2016 that took down several major websites (Twitter, CNN, etc.) was made possible by insecure routers and surveillance devices. Hundreds of thousands of these devices where compromised with botnets that generated massive amounts of fake traffic to bring down servers.

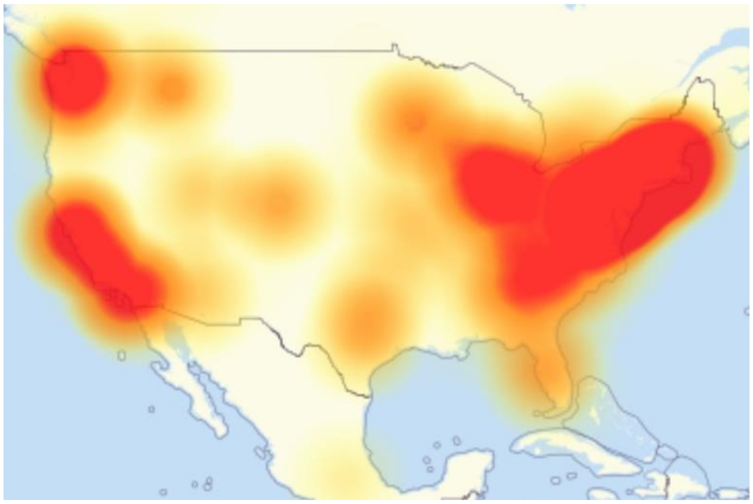

Figure 1: Heat map of the DDoS attack that brought down several websites

Another recent example is the news reported by CNNon 1/5/17 regarding FTC suing D-Link over false advertising related to security. It highlights the beginning of government involvement and legal consequences due to regulations. The article mentions the importance of securing private keys - “*The FTC also noted that D-Link made a major blunder when it exposed the company's coveted "signing key" for six months in 2015 on a public website. Tech companies are supposed to jealously guard these powerful keys because they prove that a software update is legitimate. Hackers who manage to grab them can more easily infect devices*." This example takes us to the core of the security issue to be solved: key storage and provisioning.

Connected systems are already deployed with low level of key protection. It is important to keep the implementation simple to secure design retrofit, minimize the resource budget to maintain or revise deployed software. Here’s where crypto-companion security devices remove complexity while securing the end-product by solving these issues

1. **Secure manufacturing** -To ensure the keys are secure and legitimate, there has to be a chain of trust between the customer and the entities exposed to the certificates and keys (manufacturer, chip providers, design houses, etc.). This chain of trust can easily be corrupted during the manufacturing phase, requiring the manufacturing processes to have a secure production environment. How much do you trust your contract manufacturer to handle your secrets and integrate them into hardware?

2. **Key provisioning and storage -** Provisioning private keys in hardware systems is one of the core issues in the IoT space. Often, certificates used for authentication have been and still are handled by software and pushed over the air. Let’s remember the hacker will aim for the weakest point in the chain. Here is one with software provisioning. Then, once the key is provisioned, the storage location in the embedded system is the other architecture decision to take. The core where the applications are running must be physically separated from where the secrets are stored. Physically separating the application space from the private key storage area will avoid the necessity for back doors. If there is software link, there is a possible access to the private key exposed by the back door.

3. **Scalability, reducing cost, reducing time to market with security in mind –** Software scalability and maintenance add complexity when dealing with large volumes and adding secrets managed by software reduce the flexibility. Offloading the key provisioning and storage to a companion device remove this burden from the lifecycle of a microcontroller once deployed in the market place.

Microchip Security Solutions

Microchip released the AT88CKECC-AWS-XSTK-B zero touch provisioning kit for AWS IoT to address the manufacturing challenge of the chain of trust and the private key provisioning and storage challenges. This true device-to-cloud IoT solution comprises a Wi-Fi link (WINC1500) controlled by an ATSAMG55 (ARM$^{®}$ Cortex$^{®}$-M4) and the Crypto Authentication device: ATECC508. It also leverages FreeRTOS and WolfSSL.

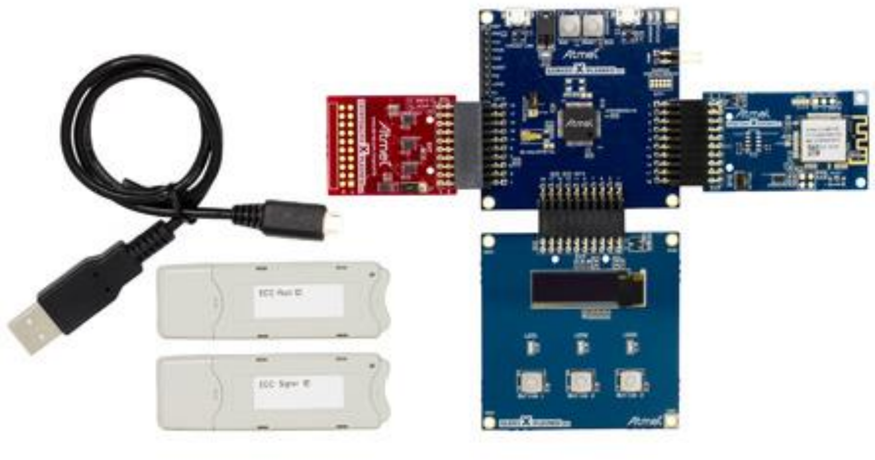

Figure 2: Microchip AWS Zero Touch Secure Provisioning Kit

Features of the kit include the following

- Complete development and prototyping platform for AWS IoT device provisioning
- Microchip's unique, preconfigured, self-signed Root Module for evaluating certificate root operations prior to engaging a Root Certificate Authority
- Microchip's Signer Module for generating Signer Certificates (CA Certificates) and registering them to AWS servers, and provisioning IoT devices with unique certificates
- Three CryptoAuth Xplained Pro (ATCRYPTOAUTH-XPRO) add-on boards, each containing an ECC508 for in-situ provisioning by the signer module
- Built on the modular Xplained PRO platform to enable experimentation with different processor, connectivity, and human interactivity interface modules
- Demonstration for zero-touch AWS secure device on boarding

Microchip addresses the chain-of-trust by working with customers using their root-of-trust to generate a private key inside the ATECC508, inside Microchip secured factories. The private key stored in the ATECC508 matches with an AWS IoT customer account where the signed certificate corresponding to the provisioned device lives. The certificate is placed in the account leveraging the Bring Your Own Certificate (BYOC) feature of the Amazon Web Services, AWS IoT service. A second important function from AWS IoT, is the just in time registration (JITR) function which allows during the first TLS connection to trigger the mutual authentication between the device and the AWS IoT account. The on boarding process makes this solution a zero-touch provisioning solution improving not only the user experience but also setting higher standard of security during manufacturing and key provisioning

.

Summary

The ability to design a secured hardware solution should not be complicated and hardware-based security solutions eliminate the complexity involved with software solutions. The ATECC508A is a crypto-companion IC that physically separates from the controller and adds isolation between the processing core and sensitive information. The philosophy is to keep the secret out of the microcontroller. It helps to achieve stronger security but also make your design more scalable as the keys are not tied to the microcontroller software. The keys are provisioned at Microchip factories during the manufacturing process eliminating risk and burden to the customer. Last but not least, by hosting the private key needed for authentication, any licensing fee schemes imposed by third party vendors are eliminated.

References

1. guardian.com
2. welivesecurity.com
3. FTC sues maker of routers, baby monitors over security
4. AWS IoT