

Why End-to-End Security at the Hardware Level Matters

[Electronic Design](#)

[William Wong](#)

Tue, 2014-09-02 11:12

With the proliferation of the Internet of Things, robust security starts with the design of the SoC and continues through the manufacturing supply chain.



With the proliferation of the Internet of Things (IoT), robust security starts with the design of the SoC and continues through the manufacturing supply chain.

[Rambus](#) is one company that is deeply involved in these security issues.

I spoke with Craig Rawlings (*left*), Senior Director of Business Development for the Rambus Cryptography Research, about the issues of end-to-end security.

Wong: Why does end-to-end security at the hardware level matter?

Rawlings: As we have seen on platforms with software-only security, there is no end of endless patches that occur multiple times each week due to vulnerabilities that are too frequent to number. It is well known in the security community that most attacks are in software because software is the easiest part of any system to penetrate. System security is only as good as its weakest link and this is where the attacks will be concentrated. Mounting a hardware attack takes much more specialized skills that are not nearly as abundant and which attacks are generally speaking much more costly and time consuming. Hardware security if implemented properly in each device will provide a robust endpoint which may not be easily attacked and which will not need infinite security patches with constant concerns about the numerous vulnerabilities existing in the operating system and/or applications.

Related

[End-To-End Security Starts With The SoC](#)

[Can The Internet Of Things Be Secure?](#)

[Ethernet Evolves Again To Meet The Internet Of Things](#)

Wong: What are the benefits that hardware security provides that software doesn't?

Rawlings: Although hardware that is not implemented properly also has vulnerabilities and may be attacked, the attacker must be present or have physical possession of the device even for a connected device. Some typical examples of hardware attacks are side channel (Differential Power Analysis) attacks, glitching attacks, test port attacks, or other penetration attacks such as de-processing of a chip and/or microscopic observation. The skills involved with hardware attacks are generally less prevalent and not nearly as easy or convenient for the attacker. Software attacks are commonly done remotely without the victim ever knowing that the attack has taken place. Also if a vulnerability is not found to exploit, often one

can be created or injected into the system since software is easily modified, whereas hardware is fixed. With enough money and time, any device may be compromised. The goal of a security architecture is to make the effort to break a device so difficult as to become economically risky and undesirable. Attackers will always seek low hanging fruit. Systems without good hardware security provide ample low hanging fruit.

Wong: When it comes to embedded electronics, one security weak point is the supply chain itself. Can you describe the process of navigating the global semiconductor supply chain?

Rawlings: Any electronic device supply chain includes the global semiconductor supply chain which starts at wafer test, and then proceeds to final package test. Some flows may have one or two final (package) tests depending on the requirements, one for functional test after package assembly and another possible step for any personalization or feature configuration requirements. In most cases, there is just one package test since handling a chip always incurs some degree of yield loss. The SoC is the most featured chip in most electronic devices. After package test, the chips are then typically drop shipped directly to an ODM (Original Device Manufacturer) or factory which has been contracted to make the final electronic product for the chip maker's OEM (Original Equipment Manufacturer) customer. Board level test is a common step at the ODM for securely provisioning sensitive data at the device level.

Wong: What coming use cases do you see for SoC-based hardware core security?

Rawlings: As devices grow in intelligence there is so much more sensitive data that must be provisioned during the manufacturing process. There are many more security requirements for each sub-system and to support all of the capabilities of a platform SoC. Being able to securely provision sensitive data such as cryptographic keys, identities, codes and hashes during manufacturing assures that each device's security integrity is maintained prior to shipping to the end-customer. For manufacturers, it is a matter of time before product segmentation occurs, which creates multiple inventory units to forecast and manage. This creates a high degree of complexity and overhead. The ability to configure features at any stage of the supply chain simplifies the manufacturing overhead and complexity and reduces inventory. For example, it is much easier to forecast the aggregate of all product types than to forecast the proper mix for each product type. Additionally, it is a powerful marketing tool to be able to securely manage updates to SoCs going into long lifecycle products such as cars or to sell an entry-level product and offer hardware features as a service which may be activated in the field. Additionally, with so much invested in premium content, content owners in the movie industry are insisting on stronger device security and content protections. For devices such as smartphones, electronic wallet applications such as mobile payments and ticketing will drive requirements for more robust hardware core security. Within a few years there will no longer be a need for cards outside of a smartphone. Other applications such as single sign-on become more convenient when the physical presence of your smartphone automatically logs you in to a corporate VPN on your laptop. With the availability of robust security in every application processor going into a smartphone or tablet, new applications and use models will emerge that will make these devices more secure than older legacy computing devices based on software security paradigms.

Wong: What is the upside for SoC manufacturers?

Rawlings: There are multiple benefits to taking a hardware security approach early in the manufacturing stages:

- 1) SoC manufacturers will be able to mitigate their liabilities of handling sensitive key data which in some cases carry liabilities of up to \$1M per leaked key;

2) Operations may be streamlined through the expansion of “soft SKU’ing” or assigning a logical part type just prior to shipping for single physical stock keeping units, saving the manufacturer tens of millions of dollars in operating costs; and

3) Manufacturers will be enabled to offer value-added device services to their customers that create new revenue opportunities.

Wong: Can you describe who wins with better security on mobile phones?

Rawlings: Every legitimate operator and actor in the industry benefits. There is much less temptation to cheat and the really bad actors have a much more difficult time staying in business. While the current generation has little understanding or concern about privacy, most of us understand the threats associated with identity theft. Better security benefits the end-user and the enterprise customers most of all.

Wong: On a broader level, what are the larger problems that plague many security systems that SoC-based security can prevent?

Rawlings: While jail-breaking phones is the domain of a hobbyist hacker, it is the ability to penetrate the secure boot mechanism or sensitive applications, resulting in more serious vulnerabilities of a network or of a user’s device that is not known to the network operator or user. Attackers who are able to do this can gain access to financial information for economic gain. Security experts understand that attacks are performed to obtain illicit financial gain in almost all cases. Most of these attacks are software-based attacks across a network on a connected device. Good hardware security at each device endpoint helps prevent these software attacks from ever happening.

Wong: How do you see hardware security cores continuing to evolve?

Rawlings: There will be continuing improvements with the integration of hardware roots of trust with embedded security software to create very efficient security engines that will drive innovation in secure connected device services when married with robust and secure back-end infrastructure. As described above, these services will support an ever increasing demand for security in all sorts of applications whether that be in smart phones, tablets and embedded intelligent devices as the Internet of Things continues to gain momentum.

Craig Rawlings has a B.S.E.E. degree and M.B.A. from BYU, and has had held senior engineering and executive marketing and sales positions at Blackberry, Kilopass, Progress Software, Resilience, Actel, and Hewlett Packard prior to joining Rambus.

Source URL: <http://electronicdesign.com/embedded/why-end-end-security-hardware-level-matters>