Why Hardware-Based Design Security is Essential for Every Application

By Gregory Guez, Executive Director, Embedded Security, Maxim Integrated

maxim integrated™

Table of Contents

Abstract

Design security is often an afterthought. But, with the regularity of security breaches impacting an array of industries, it's now more of an imperative to build security into designs early on. This paper addresses why security can't be neglected even in the most seemingly innocuous products, and examines why hardware-based security technologies can better protect against vulnerabilities than software-based approaches.

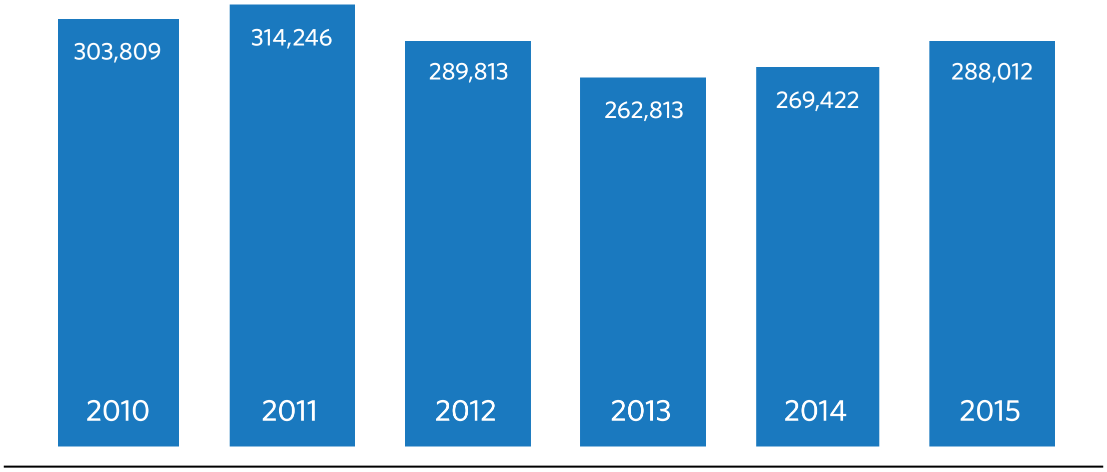
Introduction

Cybercrime is costly, but many companies still aren't considering design security until it's too late.

Even baby monitors have been hacked

In the fall of 2016 a massive internet outage brought down the likes of Amazon, Twitter, Netflix, and PayPal. The culprit? CCTV video cameras and DVRs hacked by a botnet based on the Mirai malware strain. Earlier this year, WikiLeaks made headlines when it revealed that it had internal CIA documents showing that it had uncovered a way to access Apple and Android smartphones, Samsung SmartTVs, and internet-enabled cars.

With increasing regularity, we hear stories about everyday products being attacked—products that we assume would be safe. Think baby monitors, toys, security cameras (ironically), and even medical devices. In some cases, the attacks were conducted by "white hat" (or ethical) hackers, simply to determine if it is possible. In other cases, the breaches stem from more nefarious sources. Hacking was even a major storyline in the most recent U.S. presidential election.



MORE THAN 3.4 MILLION INTERNET CRIME COMPLAINTS LOGGED BY IC3 SINCE ITS INCEPTION
SOURCE: FBI

Figure 1. The FBI's 2015 Internet Crime Report captures public complaints submitted to the bureau's Internet Crime Complaint Center over Internet-facilitated crimes.

A Juniper Research report estimates that data breaches of traditional computing devices could grow the cost of cybercrime to $2.1 trillion by 2019. The report notes that most of these breaches come from existing IT and network infrastructure.[1] Add to this the growing number of smart, connected devices—particularly products that deal in sensitive, personal data—and the propensity for havoc and harm grows that much larger and more dangerous. Forrester predicts that 2017 will see a large-scale internet of things (IoT) security breach.

The analyst firm believes that the most vulnerable areas are those that have quickly adopted IoT technologies:

- Fleet management in transportation
- Security and surveillance applications in government
- Inventory and warehouse management applications in retail
- Industrial asset management in primary manufacturing

What's more, Forrester also notes that hackers will continue to exploit IoT devices to carry out distributed denial of service (DDoS) attacks.[2] The FBI's Internet Crime Complaint Center (IC3) tracks public complaints about suspected Internet-facilitated criminal activity. According to the bureau's 2015 Internet Crime Report, IC3 has logged more than 3.4 million complaints since it was formed in May 2000, averaging nearly 300,000 complaints per year over the last five years. Figure 1 tracks complaints received since 2010. The same FBI report also notes the cost associated with Internet-facilitated crimes. Figure 2 provides a breakdown from 2015 (the most recent such report available at the time this white paper was published).

In the face of all of these threats and risks, why is security such an afterthought in so many industries? The simple truth is that, for many companies, security takes a back seat because of the perceived cost and time it adds to the product development cycle. However, neglecting design security comes with even greater costs in terms of lost revenue, brand reputation damage, and even personal harm. What's more, software-based security approaches do not provide the strongest protection, as many are led to believe. Hardware-based security delivers a much more rock-solid methodology.

Cybercrime costs could grow to $2.1 trillion by 2019

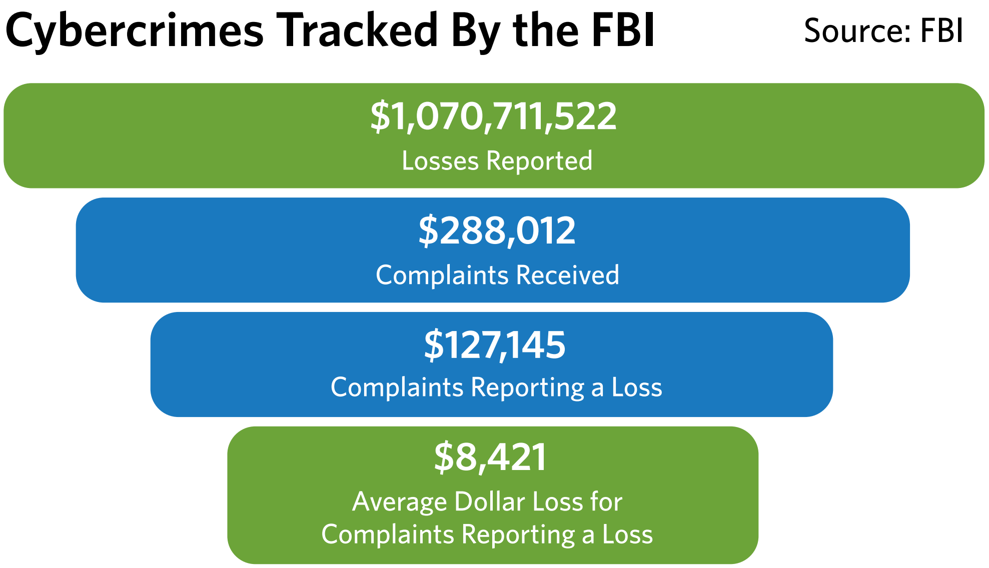


Figure 2. Internet-facilitated crimes tracked by the FBI's Internet Crime Complaint Center.

300,000 internet-facilitated crime complaints tracked by the FBI each year

Even the Financial Industry Isn't Foolproof

The heavily regulated financial industry is subject to various standards, including ISO 27000 series, which recommends best practices for information security management within the context of an overall information security management system; Standard Information Gathering Questionnaire (SIG), managed by the Shared Assessments Program, a third-party risk assessment organization; and the Payment Card Industry Data Security Standard (PCI DSS), a proprietary information security standard designed to reduce credit card fraud. Financial institutions that do not adopt these standards can face significant fines when breaches occur. Despite these regulations, a 2016 Financial Industry Cybersecurity Report from SecurityScorecard[3] analyzed more than 7000 financial institutions on its platform and identified some alarming findings:

- 75% of the top 20 U.S. commercial banks were infected by malware
- Almost one out of five financial institutions use an email service provider with severe security vulnerabilities
- 95% of the top U.S. commercial banks received a network security grade of C or below

One noteworthy point is that PCI DSS relies on software-based security. For point-of-sales (POS) financial transactions, hardware-based security is a much more robust approach. The Payment Card Industry (PCI) Security Standards Council maintains, evolves, and promotes security standards for the industry worldwide. The council, founded by major payment products companies, is behind the PIN Transaction Security (PTS) standard, PCI-PTS, which provides for robust, hardware-based security controls for payment systems. These guidelines can help develop an approach to protect against tampering and other physical and data breaches.

Even though the industry has some deficiencies in this area, the cybersecurity report still ranks financial services as well as the information services, technology, and construction industries as top performers based on cybersecurity ratings. Bottom performers include the transportation, energy, non-profit, and food sectors.[4] Indeed, it's disturbing that the financial industry—although highly regulated and inherently sensitive about its data—is still so vulnerable to attack. Even more worrisome is the fact that most industries do not have such standards to follow, so then it becomes incumbent upon designers themselves to consider security.

Smarter Devices Are Even Less Secure

There are a variety of other industries where security should be a key design consideration.

- Industrial is transitioning from previously isolated systems to fully networked systems that could expose equipment to remote attack
- Healthcare comes with privacy, data integrity, and patient safety issues should medical records or equipment and devices fall under attack
- Online banking is at risk because it's hard to guarantee identity visually
- Retailers with mobile sales channels must ensure safe transactions and communications
- Communications requires end-to-end security to protect against a variety of attacks that could intercept data or bring down systems
- With connected cars, the automotive industry needs to guard against threats such as remote hacking (Remember when white-hat hackers remotely disabled a Jeep on a St. Louis highway in 2015?)

Heavily regulated financial industry still vulnerable to attack

- Infrastructure such as the smart grid or other utilities need to be safeguarded against attacks that could disrupt cities or harm people

Smart devices aren't always smart about security

Obviously, in an industry like finance, there are clear rewards for perpetrators who are able to, say, break into a credit card system. The risks are great, too, but the potential rewards for someone who's able to get away with this crime could outweigh the risks. Today, we're surrounded by a growing amount of smart, connected devices, each with many more potential points of vulnerability than our "dumb" devices have ever had. In some cases, the risk has become smaller because of accessibility. From doorbells and home security systems to medical devices, factory/building control systems, autonomous vehicles, and city infrastructure functions, the array of things that have sensing, connectivity and communications capabilities are anticipated to number 20.8 billion by 2020, according to Gartner[5]. Often valuable data travels from these devices to the cloud and back—and can be intercepted at multiple points along the way.

Unfortunately, many decisions around security come down to budget, often in a misguided manner. The cost of a security breach can be high in terms of dollars as well as reputation and customer confidence. Figure 3 uses consumables as an example to illustrate how much counterfeiting can impact the bottom line. But many companies are still playing their own balancing game, weighing the time, effort, and cost of building in security against the pressure to get to market quickly while keeping development costs down. Plus, for many, security adds zero functionality to a product, so it becomes an unfortunate

Without Security IC	
10 Mu Sales @ $10	$100M
Less 15% counterfeit	**-$15M**
Net Sales	**$85M**
Product Cost: 10Mu @ $3	-$30M
Profit	**$55M**

With Secure Authenticator @$0.50	
10 Mu Sales @ 10$	$100M
Less 0% counterfeit	$0M
Net Sales	**$100M**
Product Cost: 10Mu @ $3.50	-$35M
Profit	**$65M**

Figure 3. Security does come with a cost, but so does a loss of revenue, profits, and brand reputation due to counterfeiting.

afterthought. However, as evident in Figure 3, foregoing security can actually be more costly in the end.

Why Hardware-Based Security is More Effective

When you're ready to think seriously about security (and we hope the data points presented in this paper have convinced you), there are hardware- and software-based security approaches to consider. While software encryption is deemed to be cost effective and easy to implement and update, it really is "as strong as the level of security of the operating system of the device. A security flaw in the OS can easily compromise the security provided by the encryption code," notes infosecurity magazine[6]. Indeed, operating systems (and their patches) are typically so complicated that it's hard to exhaustively determine all of the potential interactions that could lead to a breach, which leaves the system with potentially many points of vulnerability.

Since hackers are constantly targeting software security tools and network vulnerabilities, a software-based approach can leave designs open to someone trying to gain control of the board or the main microcontroller. In its article, "Hardware-based security more effective against new threat," ZDNet argues that products would be better protected if hardware-based security is utilized because cybercriminals find it hard to alter the physical layer. The article, citing an RSA spokesperson, further notes that the physical layer eliminates the possibility of malware infiltrating the operating system and penetrating the virtualization layer[7].

Hardware-based security is, indeed, more robust than its software-based counterpart. Establishing a "root of trust" starts with trusted software that stems from a hardware-based approach. The only way to guard against attacks that attempt to breach an electronic device's hardware is to use a secure microcontroller that executes software from an internal, immutable memory. Stored in the microcontroller's ROM, this software is considered to be inherently trusted because it can't be modified (and is, therefore, the root of trust). This "non-modifiable" and trusted software can now be used to verify and authenticate the application software's signature.[8]

"Root of trust" with a hardware-based approach provides the strongest security

Requirements	
Trust	Device Authentication
	Usage Control/Features Enablement
	Secure Boot/Download
IP Protection	Anti-Cloning
	Firmware Encryption
Secure Communications	Certificate Distribution and Verification
	Packet Encryption
	Full TLS Support
	Encryption

Figure 4. Mandatory IoT security needs for three key pillars.

Indeed, it makes sense to start at the very base level, where the design is architected, so you can integrate security into that level plus all of the layers that are added on top. With a hardware-based "root of trust" approach that starts from the bottom, you can close off more potential entry points into your design. Plus, some designs—like small sensors that are part of a larger, distributed sensor network—don't lend themselves to hosting complicated software. Figure 4 highlights the three pillars of IoT security.

Embedded security ICs, such as security managers, secure microcontrollers, and secure authenticators, can ease the process of safeguarding entire systems, from each sensor node to the cloud. Such ICs can provide a turnkey security solution, delivering capabilities and features such as layers of advanced physical security, cryptographic algorithms, secure boot, encryption, secure key storage, and digital signature generation and verification.

- Security managers that include advanced physical security with on-chip, non-imprinting memory can protect secret/private keys and confidential data from even minor attempts at physical or environmental tampering
- Secure microcontrollers with built-in cryptographic engines and secure boot loader can guard against threats such as cryptanalysis intrusions, physical tampering, and reverse engineering
- Secure authenticators can be a cost-effective means to protect IP, prevent cloning, and authenticate peripherals, IoT devices, and endpoints

For fast design prototyping, there are also a number of highly integrated, vetted reference designs available. Good reference designs include more than just the basics, offering resources such as Gerber files, evaluation and development tools, test data, drivers, and bill of materials (BOM). Using a reference design provides an opportunity to thoroughly evaluate the authentication and other security capabilities of the embedded security ICs integrated onto these boards.

Summary

The regular stream of hacking headlines should be evidence enough that design security can't be overlooked. And when weighing software- versus hardware-based approaches, it's clear that implementing system safeguards via hardware provides a more robust option. Today's embedded security ICs can provide an easier, lower cost way to integrate your designs early on with layers of advanced security, support for cryptographic algorithms, tampering detection, and many other protections.

Learn More

Read more about embedded security solutions that can safeguard your next design in our DeepCover® Embedded Security Solutions Selector Guide:

Download Now ›

Sources

[1] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[2] http://www.forbes.com/sites/gilpress/2016/11/01/internet-of-things-iot-2017-predictions-from-forrester/#7d8c5a7a6bb6

[5] http://www.gartner.com/newsroom/id/3165317

[6] https://www.infosecurity-magazine.com/magazine-features/tales-crypt-hardware-software/

[7] http://www.zdnet.com/article/hardware-based-security-more-effective-against-new-threats/

[8] http://www.embedded.com/design/safety-and-security/4438300/Securing-the-IoT--Part-2---Secure-boot-as-root-of-trust-

For more information, visit:
www.maximintegrated.com