Protecting People, Data and Profits with Security-Optimized Embedded Designs

Atmel White Paper

Author:

Todd Whitford, Product Marketing Manager, Atmel Corporation

How much security can you afford to add to your next design? In many cases, equipping an embedded system to protect its proprietary intellectual property (IP) and the data it's entrusted with represents only a small fraction of the unit's overall cost - but can you afford even this small increase and still remain competitive in the unforgiving global technology market?

Or, is it better to ask if you can afford to not include it?

Figure 1 – The money saved by not adding security features to your product is often outweighed by the hidden price of the losses incurred due to hacking, IP theft or other types of cyber attack.

Understanding the Real Cost of Security Technologies

It can be difficult to precisely calculate the cost-to-benefit ratio security technology provides, but it's easy to imagine what the real-world cost to your company would be if it faced one of these situations:

You're cruising the show floor of a conference where your team just introduced its new flagship product line. Re-inventing the embedded platform you launched your business on a decade ago has been a two year push and a bet-the-farm-sized chunk of capital – most of which went into the code for the microcontrollers (MCUs) and field programmable gate arrays (FPGAs) that form the heart of the new system. Walking back from the official roll-out event, there's lots of high-fiving and a spring in everyone's step because the audience's response confirms the reports from your beta customers that the system is light-years ahead of its competition. The mood suddenly changes, however, when your senior designer spots a small booth at the edge of the show floor with a piece of hardware that's eerily familiar. A couple of your engineers tuck their badges into their pockets and saunter over to the booth. They return a few minutes later, looking puzzled – and worried. The unit being exhibited by a small overseas company has virtually all the features your new product has – and costs 30% less than yours. A week later the engineering team manages to confirm that the software and FPGA code from one of the beta units was somehow extracted, lightly-re-written and is now running in your new competitor's cut-rate products.

Or, consider this scenario:

You're a product line manager for an industrial equipment manufacturer, trying to figure out why this quarter has seen a 10% drop in sales of your most popular product line – despite usually reliable industry forecasts which predict a 5%-7% increase in demand for this type of equipment for the year. You comb the weekly statistics of your sales, marketing and service groups until a small note at the bottom of a service team's report provides the first clue. It seems they are getting a growing number of warranty support requests for units with serial numbers that don't match up with the sales group's records. Stranger still, they are getting calls on a unit with one of those odd serial numbers from several different customer locations. In addition, the aftermarket sales group reports a steady decline in orders for the chemical dispenser cartridges, filters and other consumables which, until now, have provided a reliable bump to your revenue stream. After a few calls to key distributors and customers, it becomes apparent that an offshore manufacturer who somehow acquired the EEPROM-based firmware in your system's MCUs and used them to make a knock-off of your system. They also copied the security codes embedded in the dispenser cartridges' driver chips. Your lead engineer says this is impossible because he'd added a simple encryption algorithm to the EEPROM firmware to prevent this sort of tampering - but the declining sales figures say otherwise.

It might be tempting to dismiss these hypothetical nightmare scenarios as unrealistic or overly paranoid, but the news is full of examples of what happens when a company under-invests, or chooses a poor security strategy for its products.

Some of the incidents which recently made the headlines include:

- In 2011, hackers exploited a security weakness in the network that connected a popular gaming system to steal the personal information contained on the private accounts of at least 77 million users. The resulting 24-day service outage and other blow-back from the incident cost the company an estimated $170M in direct losses, and the long-term costs of lost customers is still being tallied.

- Since they were first reported in 2008, several security flaws have been discovered in pacemakers, insulin pumps and other medical devices which could allow a hacker to turn them into lethal weapons. While there have been no recorded fatalities attributed to the breaches, they have been responsible for several expensive product recalls and millions in lost sales.

- Recent reports of battery fires in laptop computers seem to coincide with the increased appearance of cloned versions of OEM batteries, cables, chargers, printer cartridges and other accessories on several popular e-commerce sites. Notably, some of these copycat products appeared almost immediately after the computer manufacturer's legitimate products arrived on store shelves and included proprietary details specifically intended to discourage would-be counterfeiters.

- In addition to lost revenues, manufacturers may lose customer loyalty or brand reputation if their customer's user experience is compromised by bad accessories. This can be as innocuous as poor range from a sub-par Bluetooth adapter or poor print quality from a cloned ink cartridge, but could be disastrous as a fire or explosion when a poorly engineered knock-off battery experiences thermal runaway.

IP Theft – A Growing Menace

This small sampling of the many incidents occurring throughout the high-tech economy illustrates some of the challenges embedded systems designers face in defending their products, and the customers who use them against sophisticated cyber-attacks. Many of these are various forms of

cyber-theft which seek to extract the information stored or transported by an embedded system. Once limited to simply pirating copyrighted movies, audio and other multimedia, IP theft has evolved rapidly over the last decade as industrial spies and other cyber-criminals have learned to extract the firmware, FPGA code and other details of a product's design for their own use or sale to the highest bidder.

It takes a seasoned hacker equipped with a laptop and some inexpensive tools only a few days to extract an electronic product's sensitive design information, proprietary algorithms and other types of IP which often required millions of dollars and many months (or years) to develop. The information contained in leading-edge products is in high demand by many second-tier manufacturers (often located offshore) who employ it to produce copycat products -- or as an inexpensive alternative to doing their own R&D.

Some of the most common ways that stolen IP can undermine both the immediate profits and long-term success of legitimate manufacturers include:

- *Hardware cloning*: A time-honored tradition in black-market electronics, whereby a product's circuit boards, components and often even its mechanical design are copied and used to produce unlicensed knock-offs. Modern cloning practices usually also include use of pirated firmware and FPGA code. When grey-market manufacturers begin selling unauthorized knock-offs of propriety peripherals and accessories (ink cartridges, cables, batteries and other consumables), the OEM loses a reliable revenue stream.

- *Overbuilding*: A relatively recent variant of cloning in which an authorized 3rd-party assembly facility deliberately builds more units than a client has ordered with the intent of selling them through alternate channels. Unless a product was designed with provisions to secure it against this practice, overbuilding is nearly undetectable.

- *Reverse engineering*: Even if a competitor does not produce a copy of your product, stolen IP can allow them to inexpensively acquire proprietary technologies and features which give your products market differentiation.

- *Shortened design cycles*: Pirated designs allow would-be competitors to bring their products to market quickly, reducing the time an innovative company gets to enjoy the marketing advantages and premium pricing that a product's unique features make possible.

Intrusion, Theft, Sabotage – Real Possibilities

A complete security strategy must also address traditional security concerns about securing the system's wired and wireless network connections. Encryption of network data, secure key management, verification and other traditional (but often overlooked) security measures are necessary. After all, your customers won't buy products unless they know that they will protect their data, services and infrastructure against intrusion, theft and sabotage.

Unless properly secured, network connections can become a prime target for interception of sensitive data and theft of multimedia streams or other services. A poorly secured communication port can also be susceptible to man-in-the-middle attacks and other techniques intended to inject malicious code during routine software upgrades. Once inside your system, the new code can turn it into a convenient point of entry to your customer's (or your) network that can be used to gain access to sensitive consumer and corporate data.

The same techniques can be also used by those with more sinister intent to do physical harm. Several Pentagon studies, and recent real-world incidents such as the Flame and Stuxnet viruses, should serve as clear warnings that cyber-terrorism is a real possibility – especially in applications involving public infrastructure (utilities, communication, transportation) or mission-critical systems (medical, industrial control, etc…).

Secure Products Mean Secure Profits

Figure 2: A small investment in security protects your profits – and your customers' assets.

Because of the role they play in creating and protecting revenues, embedded security technologies which protect the data, IP and profits of both manufacturers and their customers have become critical elements of nearly any business plan. Protecting your embedded designs against hacking, IP theft and other security measures is necessary in order to:

- *Protect Your Revenue*: Secure IP prevents over-builds, hardware and software clones and other violations of contract manufacturer agreements. Often the consumables, peripherals and accessories used by an embedded system enjoy a much higher profit margin than the system itself and are often are a critical element of a product's overall profitability. Design security and authentication technologies help protect these important revenue streams from being eroded by opportunistic knock-off artists.

- *Protect Your Competitive Advantages*: A secure design prevents reverse-engineering of proprietary features and technologies which differentiate your product from its competition. Denying would-be competitors easy access to your "crown jewels" can help preserve your competitive lead in an unrelenting market.

- *Protect Your Customers:* Your customers must be assured that your product will protect their networks, data and revenues against intrusion or theft.

- *Protect Your Brand Image*: Cheap, poorly performing look-alike products can tarnish a premium product's reputation and perceived market value.

- *Reduce liability exposure*: If a copycat product fails to perform properly, or causes injury to its user, it may still be a costly effort for the legitimate manufacturer to prove its innocence in the matter. Unauthorized accessories and consumables are also a liability-. For example, knock-off batteries are often more susceptible to explosions or fires while low-quality copy-cat consumables used in medical systems can result in inaccurate diagnoses – or worse.

Optimizing Your Security Strategy

Part of the design process is to decide which of the issues listed above apply to your product and whether they are a primary or secondary requirement. Once the product's security requirements are defined, they can be used to develop a security strategy which serves as a tool for selecting the technologies and products best-suited to meet the application's unique combination of threats, performance requirements and cost constraints. The security strategy should also consider whether the security solutions must be capable of being updated to deal with new threats as they emerge.

Depending on the level of security and performance required by your application, you can protect your system using a strategy based on software, hardware or a mixture of both. Each of these strategies has its own unique advantages and drawbacks.

No Security

The simplest strategy is to not include any security in a design. In certain cases, the lower BOM and manufacturing costs, faster time to market and lighter MCU workload in the absence of security-related software outweigh the hidden costs of leaving a product vulnerable to hacking. But since some basic security measures can be implemented at little or no cost, few, if any, applications can afford to ignore security altogether.

Software-Only Solutions

- If the existing MCU has sufficient memory and processing cycles to support it, a security algorithm can be implemented in software. In most software-only security solutions, critical items such as keys are stored in the MCU's existing memory resources (EEPROM, Flash).

- Advantages: These solutions are often perceived to be free – although they may have hidden costs due to additional development time/cost.

- Disadvantages: Storing keys in unsecured memory resources puts them at risk. In addition, there is always a possibility that the system's security algorithms may have errors in their implementation which could render it vulnerable to attack.

Software/Hardware Hybrid Solution (e.g. hardware on client, software on host)

- A client-side system's MCU can be augmented with a hardware security device which provides secure key storage, and implements some, or all, of the security algorithm in hardware.

- Advantages: Lower overall solution cost because no security device is required on host.

- Disadvantages: In this solution, the host-side system's keys are stored in an unsecured resource, putting them at risk for interception, theft or alteration. In addition, the software for the host-side algorithm may contain flaws in its implementation which leave it vulnerable to hacking techniques.

Defendable Hardware-Based Solution

- An all-hardware solution includes tamper-resistant secure key storage devices used at all critical points in the system.

- Advantages: With its keys securely stored in a hardened device specifically designed for the purpose and its security algorithm implemented in hardware, the resulting system is much more resistant to hacking without burdening the host processor. In addition, the development time required to bring a fully tested verified product to market is dramatically shortened.

- Disadvantages: Many designers avoid all-hardware solutions because they are perceived as adding potentially unnecessary cost to a design.

Conclusions

The real-life and speculative scenarios presented here are compelling examples of why OEMs can no longer afford to ignore security or count on "security by obscurity" to protect their products. IP theft has become a major industry, with skilled teams of engineers extracting software, FPGA code and even entire designs which are used to produce cut-rate products that eat into a legitimate manufacturer's sales and possibly their reputation. Producers of copyrighted audio, video and other licensed IP are being similarly impacted by both amateur and professional data pirates. Worse yet, the cost of lost markets, tarnishing of a company's brand image and product liability issues resulting from failure to properly secure an embedded system can produce even larger, more persistent impacts to a company's revenue stream.

The growing presence of embedded systems in nearly every type of infrastructure and mission-critical equipment also makes them an attractive target for cyber-criminals bent on either profit or mayhem. Meanwhile, increased use of networking technologies provides would-be hackers with a potentially convenient means of entry.

Fortunately, today's silicon manufacturers have developed an arsenal of versatile tools and products which greatly reduce the cost and difficulty of implementing security. Once a designer clearly identifies the level of security their application requires, they can explore a spectrum of solutions to find the one which meets the price and performance goals appropriate for their target market.

Amongst the most cost-effective security technologies available today are tamper-proof secure key storage and management devices. These devices can be paired with virtually any MCU to create an embedded system which is highly-resistant to the attacks commonly used to steal sensitive data, software and other types of IP. The concluding article of this series will explore this technology using Atmel's tamper-proof secure key storage solutions as examples. Details of several core use models will be presented to illustrate how secure key storage and management devices can help customers cost-effectively protect their design investment.

Editor's Notes About Atmel Corporation

Atmel Corporation (Nasdaq: ATML) is a worldwide leader in the design and manufacture of microcontrollers, capacitive touch solutions, advanced logic, mixed-signal, nonvolatile memory and radio frequency (RF) components. Leveraging one of the industry's broadest intellectual property (IP) technology portfolios, Atmel is able to provide the electronics industry with complete system solutions focused on industrial, consumer, communications, computing and automotive markets. Further information is available at www.atmel.com.

Atmel Corporation
1600 Technology Drive
San Jose, CA 95110
USA
Tel: (+1)(408) 441-0311
Fax: (+1)(408) 487-2600
www.atmel.com

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

Atmel Japan G.K.
16F Shin-Osaki Kangyo Bldg.
1-6-4 Osaki, Shinagawa-ku
Tokyo 141-0032
JAPAN
Tel: (+81)(3) 6417-0300
Fax: (+81)(3) 6417-0370