How Much Security is Enough?

White Paper

October 2015

How Much Security is Enough?

Introduction

Determining the appropriate level of security for a system is a complex problem. It is difficult to determine technical mitigations to potential attack vectors. When business considerations such as cost-benefit analysis are added, it becomes a multi-dimensional optimization problem with several hidden factors. This whitepaper enumerates several strategies that are helpful for answering the basic protection-design question, “how much security is enough?”

Modeling the Impact of Security Failures

To develop a cost-benefit analysis, one must understand the impact of a security failure. To gain an intuition for this impact analysis, consider the following common security objectives:

- Prevent damage or denial-of-service to critical systems
- Prevent loss of IP or data
- Enforce licensing or usage policy

The damage-prevention objective encompasses physical security (guns/gates/guards) as well as role and user-based access control systems. Malicious actors may seek to damage systems for many reasons, such as:

- Covering the traces of other malicious activity
- Causing capital loss as a means of weakening a competitor
- Disabling other security features as part of a larger cascaded attack on a system

Damage may also be immediate or delayed; for example, consider the Michelangelo virus of the early 1990s, which disabled PC-based computers on a specific date. In a Defense context, delayed damage may be used to disable security features in coordination with a planned operation. For example, consider the 2015 report that a German Patriot missile battery on the Turkish-Syrian border was briefly taken over by an unknown cyber actor. For security systems that seek to prevent damage or denial of service, what impacts could a precisely timed attack produce for the end-user of a system, for the supply chain (spares and inventory), and for the manufacturer's value proposition (perceived expertise, reduced value at market entry, and so on)?

The IP and data loss prevention objectives typically center around maintaining a technological advantage, either as a key business differentiator or a tactical battlefield advantage. The motivation of malicious actors who steal IP and data may be to produce counterfeit systems, to enhance a technology offering in order to eliminate a competitive disadvantage, or in the case of military systems, to produce countermeasures or other technology-defeat mechanisms, for example, to analyze systems for cyber-vulnerabilities that will be leveraged later in a damage-seeking attack. Following are the key considerations in determining the impact of IP and/or data loss:

- What value does the IP or data objectively represent to the business? Is it a key differentiator? How will the business suffer if it is delivered directly to a competitor? How quickly is the technology evolving? Is there a time when it will be relatively obsolete?
- Is the adversarial actor capable of producing the IP or data independently? Could they acquire a similar technology from another vendor? On what timeline?
- What damage-seeking threat vectors could be enabled by IP or data theft? For security IP, what countermeasures could be developed to defeat the security technology?

The licensing and usage-policy enforcement objectives center around monetizing IP or data as commodity products. Malicious actors typically seek to use IP or data without paying licensing costs or royalties.

Determining the Acceptable Loss Point

Security is a game that is never won. Anyone who tells you otherwise is in marketing or sales. Consider that even the NSA has security breaches. Are your controls and penalties as rigorous as theirs? Therefore, there is a point when your security will fail. The key question is, “what is the optimal trade between the 'cost of security required to delay failure until time t' and the 'cost of security failure at time t'?”

Practical examples of this trade-analysis arise in the computer-game industry: The majority of sales of a new computer game occur within the first few months. If piracy can be prevented during that period, most of the revenue capture will have occurred, and the cost of a subsequent security failure is negligible. Similar analyses apply to fast-evolving technology domains; if your technology is obsoleted every two months, then a two month protection period is likely sufficient.

It was mentioned earlier, but is worth reiterating: in the IP-loss context, if your competitor can organically develop an equivalent technology (or acquire such from a 3rd party), the acceptable loss point should be no further out than the estimated timeline for that organic development.

Tailoring Defenses to the Capabilities of the Adversary

Inasmuch as the business-case side of the analysis requires estimates of how long it may take a competitor to develop equivalent features, the engineering analysis requires an estimate of the capability of the potential attackers.

If your adversaries are nation-state or organized-crime level adversaries, that is, well-funded, dedicated adversaries, then one should consult the security specifications for industries that routinely deal with this level of threat. Examples are the level 4 criteria of the FIPS 140 specification and the excellent payment-card industry (PCI) specifications for hardware security requirements on payment processing equipment. In defense contexts, you should seek out the AT delegate for the relevant service branch for guidance.

If your adversaries are competitive corporations, then you have a few routes to determining acceptable protection methods. You might model adversarial capabilities by assuming they are similar to your own engineering capabilities - in this case it is reasonable for engineers to select protection techniques that could prevent themselves from being able to compromise the system on the desired timeline. (If pursuing this route, refer to the Microsemi® white-paper titled *"Threat Driven Security"*.) Alternatively, many companies offer security assessment services, in both collaborative analysis ("blue-team") or penetration-testing ("red-team") modes. Others offer protection design consultation and services.

In some cases, the adversary model assumes a good-natured user; protection simply intends to keep honest users honest. Examples of this are license-expiry checks in periodically licensed software. IT departments are frequently reactionary rather than proactive in renewing licenses, and these techniques simply serve as a reminder that a license payment is due.

Iteration

The cost-benefit analysis spans the business-case analysis and engineering design. As such, it will be an iterative process wherein a desired acceptable loss point is defined with a desired budget, and engineering feasibility studies are conducted to determine whether the business objective is achievable within the budget.

How Microsemi Can Help

Microsemi has a strong security focus. In addition to our numerous security-oriented products, the Microsemi Security Center of Excellence provides consultation and services for risk/threat assessment, protection design, protection implementation, and protection testing as follows.

Risk Assessment Services

Microsemi system security analysts evaluate a customer's system in detail to access critical system data/functions, discover vulnerabilities, enumerate threats, and outline the likelihood and consequence of system compromise. These services, performed by engineers experienced in attack tree modeling, reverse engineering and exploitation tools and techniques, provide the basis for protection planning and security engineering services. System risk assessments supply information helpful in analyzing costs and benefits, and assist in making critical security decisions to mitigate threats with minimal impact to program cost or schedule. Risk assessments are typically conducted in collaboration with project engineering staff and full access to design documentation and product specifications.

Protection Planning Services

Using risk assessment and any other compiled data customers receive a report with protection implementation cost estimates, presentation materials and a protection design document. This report describes how to mitigate identified system vulnerabilities and ensure successful verification and validation of the system. All possible mitigations are considered and proposed including hardware, firmware/IP, or software. In addition, protection evaluation services review the security of customers' protection designs and document the residual vulnerabilities in the exposed system.

Red and Blue Teaming Services

Microsemi red teaming services start with a black-box approach, pitting experienced reverse engineers with state-of-the-art attack tools against a customer's system in a deployed setting. Results from a red teaming services engagement can reveal vulnerabilities that are not otherwise found during most other evaluation exercises. Blue teaming services use the same experienced engineers, but provide them with full access to documentation, architecture diagrams and other engineering expertise. A blue teaming approach typically reveals flaws in protection design or protection implementation.

Security Engineering Services

Microsemi's dedicated engineering team specializes in tools, processes and methods required to design, implement, test and adapt existing systems to ever-changing environments. The company's services may be employed to implement protection designs or to consult with government information assurance and anti-tamper experts within Microsemi's resource network. Additionally, engineers can develop custom security solutions and novel protection mechanisms unique to a customer's product.

Side-channel Analysis and Mitigation

Microsemi utilizes a DPA testing framework and workstation platform for evaluation of side-channel threats. The testing platform offers measurable, objective and repeatable testing for resistance to side-channel attacks across all applications where tamper resistance is critical. Microsemi is the only US-based, independent test lab for Differential Power Analysis (DPA).

Security Forum and Webinars

As defense-grade services are an important aspect of security design, Microsemi holds a yearly Security Forum as well as a series of webinars on the subject of security for its broad array of current and future customers across multiple markets, including industrial and commercial, automotive, medical, and aviation. For more information on the Security Forum and/or Microsemi's security webinars, email sales.support@microsemi.com.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA

Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

E-mail: sales.support@microsemi.com

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at **www.microsemi.com**.