Defense Security Products and Services

Defense Market Challenge

The Department of Defense (DoD) anti-tamper (AT) mandate 5000.2 and the corresponding Verification and Validation (V&V) process is both difficult to understand and expensive to satisfy, yet failure to meet these requirements results in delayed deployments and significant financial losses. At the same time, each program has unique security, platform, performance, and business requirements. AT is therefore a strategic and technological problem for program managers and developers. It is generally unfeasible to solve these problems using a single technology. Using an independent systems integrator with mature AT products and established expertise is far more effective.

Microsemi® can provide AT technology products and services for our government clients throughout the AT life-cycle. We empower program managers to successfully navigate the V&V process through a combination of skilled security professionals and targeted AT technologies.

Importance of Anti-Tamper

Failure to meet the DoD anti-tamper 5200.39 policy and corresponding V&V requirements can result in delayed deployment and significant financial losses.

The Need for AT

The US Navy Lockheed EP-3 landed on Hainan Island after a collision with a Chinese F-8 Finback. The Chinese military boarded the EP-3 and thoroughly stripped and examined the aircraft's equipment. Speculation exists that the crew were only partially successful in their destruction of the on-board data and technology.

Products

Microsemi Security Solutions products create layered security over critical program information (CPI). Our products enable engineers to efficiently build custom hardware, crypto, and software protection schemes to meet their security requirements.

Hardware Anti-Tamper	EnforcIT® is a set of VHDL IP cores for Microsemi System-on-Chip (SoC) field programmable gate arrays (FPGAs), Xilinx, and Altera. Each IP core is a standalone protection mechanism mitigating one or more reverse engineering, counterfeiting or tampering attack. Suite B cryptography cores are FIPS 140-2 certified.
Software Anti-Tamper	CodeSEAL™ secures desktop and real-time embedded operating systems running PowerPC or x86 chipsets against reverse engineering and tampering. Layers of active software security forces adversaries to attack a complex network of countermeasures.
Cryptography	Microsemi's WhiteboxCRYPTO™ product combines mathematical algorithms, data, and code obfuscation techniques to transform the key and related crypto operations in complex ways requiring deep knowledge in multiple disciplines to attack. Importantly, the key is never present in static or runtime memory. Rather, the key becomes an inert collection of data that is useless without the uniquely generated white box algorithm. Support is provided for AES, RSA, ECC, and many other public and custom ciphers. The EnforcIT product includes Suite B, FIPS 140-2 certified cryptography cores.

	The Microsemi Advantage
Skilled Professionals	Microsemi offers a full staff of experienced security professionals including cleared protection engineers, researchers, red-team analysts, software developers, and project managers. A secure facility can be used for offsite work if required.
Targeted Security Products	FPGA IP cores, software, and cryptography anti-tamper products along with dedicated security products from partners allow developers to leverage years of experience and efficiently implement comprehensive system protection.

Defense Security Products and Services

Professional Services

Microsemi's dedicated services are performed by highly skilled service engineers. End-to-end solutions include creating AT plans, develop and implement protection designs, and execute red-teaming of protected systems to ensure CPI is properly protected. We work with program managers and the development team to design protections that best leverage characteristics of the underlying platform and to build a robust protection network with no single point of failure.

Risk Assessment Services provide the inputs necessary to identify, scope, and integrate security requirements with program capabilities. A risk assessment supplies information helpful in analyzing costs/benefits, as well as in making critical security decisions to mitigate threats with minimal impact to program cost or schedule. A risk assessment reviews your system in detail to 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.

Protection Planning Services help customers step through the acquisition process to support required inputs for each design review, technical interchange meeting, and the Milestone Decision Authority. Our personnel have experience in developing protection plans as well as providing inputs and deliverables for classified annexes. Using a risk assessment and other compiled data, you will receive documentation including a protection design and an implementation approach. The documentation describes how to mitigate identified system vulnerabilities and ensure successfully navigation of the V&V process.

Protection Evaluation Services review the security of your protection design to document vulnerabilities in the exposed system. **Red Teaming Services** start with a black-box approach, pitting experienced reverse engineers with state-of-the-art attack tools against your system in a deployed setting. **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 the Protection Design or Protection Implementation. While similar to a Red Teaming exercise, Blue Teams can produce results in a shorter time frame.

Security Engineering Services assists customers by providing an engineering team experienced with the tools, processes, and methods required to analyze, design, implement, and test security features for existing systems to satisfy ever changing protection requirements. Our engineers can develop custom security solutions and novel protection mechanisms that are unique to your application.

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.

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
email: sales.support@microsemi.com
www.microsemi.com