

CodeSEAL

Programmable Tamper Responses with Push-Button Protection

Software Anti Tamper Layers

Microsemi's software protection product CodeSEAL™ enables security engineers to build robust anti-tamper (AT) protection schemes to protect critical technologies and intellectual property against reverse engineering, tampering, and counterfeiting by hostile entities. Built from the ground up and drawing on more than a decade of software protection experience, CodeSEAL takes a defense-in-depth approach to AT by inserting layers of preventative, proactive, and reactive countermeasures into software applications. These protection mechanisms form a dense network of security from common software attacks that cannot be defeated without sophisticated attack tools and capabilities.

Simple, Effective Software Protecting Software

CodeSEAL secures desktop and embedded systems such as VxWorks on PowerPC or Windows/Linux on x86 from numerous software attacks. Active layers of protections are easy to install as drag-and-drop.

Securing Vulnerable Software

Reverse engineering is the first form of attack on any software application. Understanding program structure, flow, and the location of sensitive routines enables adversaries to exploit vulnerabilities and otherwise compromise critical technologies. CodeSEAL adds multiple layers of obfuscation, encryption, anti-debugging, and self-modification to prevent such attacks.

Tampering is the route by which attackers compromise the software, unlock controlled functionality, or otherwise extend software functionality beyond what was deployed. Tampering attacks can extract valuable software components that can then be used in counterfeit systems. CodeSEAL protection mechanisms actively detect and react to changes in the software integrity.

Guards are the building blocks of CodeSEAL protections. Each Guard is a small protection mechanism inserted by the CodeSEAL engine. When the protected software is attacked, Guards provide custom reactions and defend each other against reverse engineering and tampering in a layered network of defense. Guards constantly evaluate the program's security at run time so any reverse engineering attempts are detected. Defensive and offensive reactions can be fired to stop the attacker from further progress.

The CodeSEAL Advantage

Many software security solutions fall short of a strong defense allowing attackers to quickly and easily dispose of any protections. CodeSEAL eases the development of a defense-in-depth security strategy making attacks prohibitively difficult and expensive. The CodeSEAL protection development environment is a streamlined interface that walks you through the process of quickly and easily applying anti-tamper to your system.

Supported Platforms

CodeSEAL protects applications executing Intel x86 or PowerPC instructions running on Windows™, Linux, VxWorks, and other embedded operating systems.

Host OS	Example Boards	CPU	Target OS	Language	Compiler
Windows Linux	MVME 5100	PPC x86	VxWorks Linux Windows	C/C++ Ada	Tornado GCC Workbench
	MVME2604				Visual Studio
	MVME5500				GCC MaxAda Aonix PERC
	SBC8240				
	CW183				

Figure 1: CodeSEAL Platform Support

CodeSEAL

Programmable Tamper Responses with Push-Button Protection

Graphical, Drag-and-Drop Protection Development

The protection development environment contains utilities for generating threat trees, injecting software countermeasures, configuring your protection network, and generating anti-tamper reports. Security can be configured down to the bit level, or viewed at the system level. Injecting

countermeasures is as simple as drag-and-drop. The CodeSEAL Protection Development Environment significantly decreases the complexity and time of implementing a complex, defense-in-depth software protection.



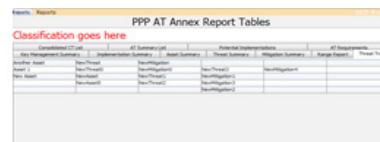
Customize Protections



Build Threat Trees



Drag-And-Drop Security



Generate Reports

Table 1: Features and Benefits

CodeSEAL Features	CodeSEAL Benefits
Active Defense	Active defense means your application can identify attacks and has the power to respond.
Full Automation	Fully automated protection for even the most complex build environments.
No Single Point of Failure	Guards protect each other and your application, significantly challenging the expertise and tools of even the most sophisticated adversaries.
Low, Configurable Impact	Guards are extremely small and highly configurable, allowing you to insert fine-grained protection into your application with an acceptable balance of performance and security.
Ease of Use	A drag-and-drop user interface enables software protection in minutes. Protection defaults get a protection running quickly and are based on best-practices in the industry.
Protection Development Environment	The CodeSEAL Protection Development Environment goes beyond a typical IDE with threat tree development, protection design visualization, and critical technology marking.
Reporting	Threat trees, protection designs, and other info are stored in a central database. Reports easily export these into documents for management and the anti-tamper authority.
Guard Development Kit	Additional, powerful guards can be developed and debugged with a Guard Development Kit giving each application its own unique protection mechanisms, custom reactions, etc.

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.



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

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.

©2015 Microsemi Corporation. All rights reserved. Microsemi and the Microsemi logo are registered trademarks of Microsemi Corporation. All other trademarks and service marks are the property of their respective owners.