

GemSeal™ Guard

High Assurance Integrity for Management & Control

Class A1 crypto seal guards can enable high integrity Management and Control (M&C) of critical systems across untrusted, even Internet, infrastructure.

Problem Statement

Operators of critical systems need to exercise management and control with high integrity even over untrusted or public networks. If operators do not have a (usually dedicated) high integrity infrastructure, a connection to untrusted networks demands high assurance protection, so the shared network can neither manipulate the commands sent nor infect the M&C workstation.

Concept: Crypto Seal Guards

Class A1 GemSeal Guards will use a cryptographic seal to cryptographically bind each packet leaving a high integrity system with a label for its high-integrity source. The guards forward each labeled packet across the untrusted network to a guard at its high integrity destination. Destination guards validate the data and label of each packet against the destination integrity label before releasing it. Altered and other low integrity packets cannot enter the destination because they will not have a crypto seal binding a label to a matching high integrity destination label. GemSeal protects management and control from corruption in the untrusted network.

Class A1 High Assurance MLS

GemSeal Guards will use the GEMSOS™ security kernel's label integrity and distributed key management mechanisms. A guard can be made an integral part of each workstation exercising M&C functions to provide the workstation network interfaces. M&C operators cannot even inadvertently plug into Internet traffic. NSA previously evaluated the GEMSOS security kernel and RAMP at Class A1 in the Gemini Trusted Network Processor (GTNP™). NSA deployed the GEMSOS kernel for key management and distribution in their Class A1 BLACKER VPN.

Completed POC Demonstration

Aesec has delivered a proof of concept (POC) demonstrating crypto seal guards connecting devices across an Internet-technology network. The POC uses a pre-production update of the GEMSOS security kernel derived from the Class A1 GTNP.

For further information contact:

Aesec Global Services
Michael J. Culver, Vice President
michael.culver@aesec.com

© Aesec Global Services, Inc. 2006-2007
Aesec, The power of verifiable protection, GEMSOS, GTNP, and GemSeal are trademarks of Aesec Corporation and Gemini Computers, Incorporated

