GemSeal™ Guard

High Assurance MLS
Proof of Concept (POC) Demonstration

Class A1 crypto seal release guards can provide Internet or NIPRNET access across system high networks while protecting system high data.

Problem Statement

DoD and IC professionals need to access unclassified information not available on their system high networks. If their environment does not include Internet or NIPRNET infrastructure, the connection demands a controlled interface.

Concept: Crypto Seal Guards

Class A1 GemSeal Guards will cryptographically seal packets entering the system with the label configured for their low sensitivity source. The guards will then forward each low-sealed packet across the system high network to a guard at their low sensitivity destination. Destination guards will validate the seal integrity of each low-sealed packet before its release, using a locally configured destination label. System high data packets cannot exit the system because they will not have a seal with a matching low sensitivity destination label.

Class A1 High Assurance MLS

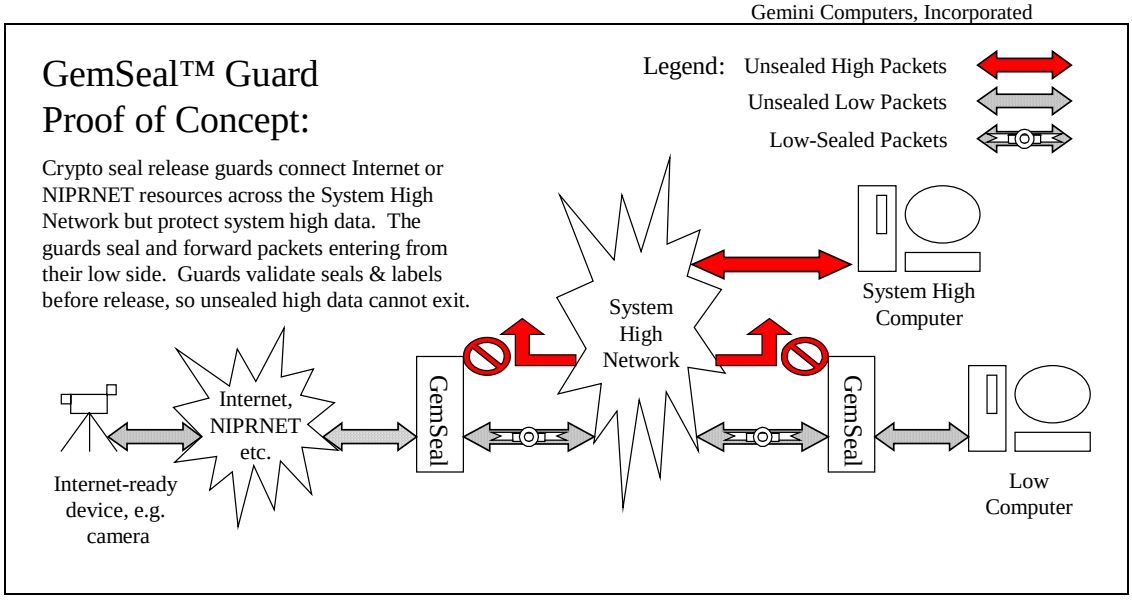
GemSeal Guards will use the GEMSOS™ security kernel's label integrity and distributed key management mechanisms. NSA previously evaluated the GEMSOS security kernel and RAMP at Class A1 in the Gemini Trusted Network Processor (GTNP). NSA deployed the GEMSOS kernel for key management and distribution in their Class A1 BLACKER VPN.

POC Demonstration

The POC demonstrates pre-production guards connecting low sensitivity devices across a system high 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



725 Cowper Street #46
Palo Alto, CA 94301-2650
www.aesec.com
tel: 650.838.9968
fax: 650.838.9315