æSec™ Global Services

The power of verifiable protection™

GemSeal™ Guard

High Assurance MLS

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

Introduction

Information professionals need to access unclassified resources not available on their system high networks. If their environment does not include Internet infrastructure, such connections demand a multi-level secure (MLS) interface.

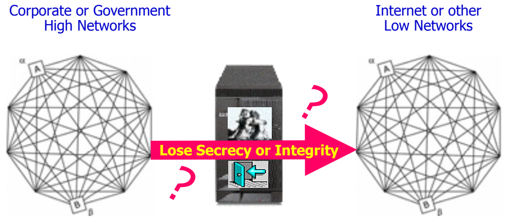
Concept: Crypto Seal Guards

Class A1 GemSeal Guards use a "crypto seal" to cryptographically bind packets entering the system with the label for their low sensitivity source. The guards forward each labeled packet across the system high network to a guard at its low sensitivity destination. Destination guards validate the label of each packet against the destination sensitivity label before releasing it. A system high packet cannot exit the system because it will not have a crypto seal binding a label to a matching low sensitivity destination label.

Challenge: Networking Networks

Any connection between networks with different sensitivity levels is multi-level[Bell]. The nature of network protocols and their ability to find routes between connected devices makes such connections both necessary and multi-level by their nature. These connections must have an assurance level appropriate for the value of the information they protect.

Challenge:
Networking Networks



Computer Security Intermediate-Value Theorem

**Any connection to lower networks is Multi-Level
So it had better be Multi-Level Secure (MLS)**

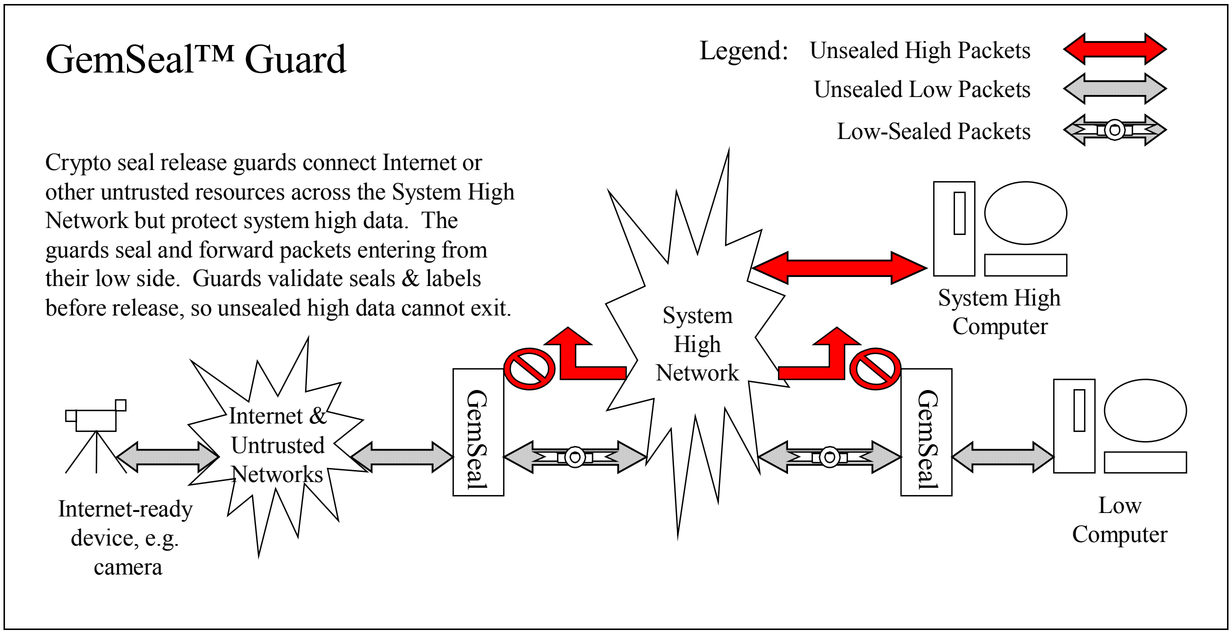
Highly sensitive networks must take extraordinary care to protect their data from attack and unauthorized data disclosure when delivering unclassified (or other lower sensitivity) connections to users. Protection against patient, professional adversaries requires the systematic and verifiable protection of information flow controls provided by systems that satisfy the Class A1 certification criteria.

Class A1 High Assurance MLS

GemSeal Guards rely on the GEMSOS™ security kernel for MLS enforcement and use its label integrity and distributed key management mechanisms. NSA previously evaluated[GNTP] the GEMSOS security kernel and RAMP plan at Class A1 in the Gemini Trusted Network Processor (GTNP). NSA also deployed the GEMSOS security kernel for key management and distribution in their Class A1 BLACKER VPN

[Bell] David Elliot Bell, "Looking Back at the Bell-LaPadula Model", Applied Computer Security Association, 2005 Conference, http://www.acsac.org/2005/papers/Bell.pdf

[GNTP] Final Evaluation Report, Gemini Computers, Incorporated, Gemini Trusted Network Processor Version 1.01, National Computer Security Center http://www.aesec.com/eval/NCSC-FER-94-008.pdf


GemSeal™ Guard

Crypto seal release guards connect Internet or other untrusted resources across the System High Network but protect system high data. The guards seal and forward packets entering from their low side. Guards validate seals & labels before release, so unsealed high data cannot exit.

Customer Problem Statement

Isolation is the bedrock security mechanism used to protect sensitive data. It is not unusual to find isolated enclaves on enterprise networks supporting critical business functions like manufacturing automation, research, development and test facilities, and sensitive services like human resource management and finance. The purpose of these isolated environments is very similar to that of their defense and intelligence community counterparts – protecting enterprise data from unauthorized disclosure and alteration.

But isolating users and systems that deal with sensitive data from the information and services available on the Internet and other less sensitive environments disrupts the synergy and power multipliers that deliver improved user productivity. So, customers face a quandary – how can they connect their users to untrusted networks and still isolate their sensitive data and processes from threats, both internal and external?

Maintaining extra network infrastructure for each sensitivity level in a facility – wiring closets, switches, hubs, routers, firewalls, gateways, etc. – is expensive in both capital and operational expense, especially as the number of network sensitivity levels increases. Some environments have dozens.

History of Crypto Seals

Cryptographically binding the sensitivity label to data is not a new concept. Originally conceived ~1980 for the USAF Korean Air Intelligence System, it was also proposed for use in the RECON Guard[Anderson] design. A number of authors have also recognized crypto seals as a way to insure the integrity of labels in a Data Base Management System.

The TCSEC includes a "Label Integrity" requirement that "Sensitivity labels shall accurately represent security levels of the specific objects with which they are associated." GEMSOS is distinguished as the only Class A1 evaluated commercial product to use crypto seals to meet this Label Integrity requirement. Crypto seals protect the label and data integrity of non-volatile storage.

GemSeal applies this crypto seal concept to network packets forwarded by guards. A GemSeal destination guard assures the integrity of both data and label:

[Anderson] J. P. Anderson, "On the Feasibility of Connecting RECON to an External Network," Technical Report, J. P. Anderson Co., March 1981

- Packet data is not altered, i.e., high data has not contaminated it
- Source sensitivity label is authentic

Crypto Seal Architecture

The crypto seal guard architecture uses two or more guards connected by a common system-high network. Each guard has one high and one or more low interfaces.

Each guard cryptographically binds the sensitivity level of the source network with the contents of each packet it forwards from low-to-high. The guard then forwards these lower-network-labeled ("low-sealed") packets over the system-high network to another guard at their intended destination.

When delivering packets, the destination guard validates the label authenticity and integrity of each packet before releasing it to its lower sensitivity destination. Packets with absent or invalid seals are dropped. Guards will only release packets to interfaces with sensitivity matching their sealed labels.

The seal is a Message Authentication Code (MAC) created by using the Cipher-Block-Chaining (CBC) mode of a symmetric encryption operation. Packet contents and the canonical representation of the source network sensitivity level are included in the CBC computation of the seal[Seal]. The low-sealed packet includes the forwarded packet as well as the seal. The label need not be transmitted as part of the packet, but is established for each security association (network-to-network connection) between GemSeal guards.

Sealed packets can conform to the IETF IPSEC Authentication Header[AH] specifications for IPv6. The configuration choice of symmetric algorithms used in CBC mode to produce the seal will include at least 3DES (168-bit keys).

Class A1 Crypto Seal Design

The design for the Class A1 crypto seal guard GemSeal minimizes new trusted code. GemSeal makes maximum use of previously evaluated security services provided by the GEMSOS security kernel. The new trusted code uses GEMSOS mechanisms to protect the new trusted services from application code.

GemSeal accesses previously evaluated GEMSOS security services by way of published and stable APIs. The vast majority of GemSeal application code (including the network protocol stack) is un-trusted; only two new security services need be trusted – "Seal Packet" and "Release Seal-Validated Packet". To protect these trusted functions the design will use the previously evaluated GEMSOS mechanisms for creating protection domains.

Reusing GEMSOS Features

Since GEMSOS used crypto seals to meet Class A1 Label Integrity requirements (integral to meeting Trusted Recovery & Trusted Distribution requirements), all the pieces and public APIs to create and validate crypto seals are already in place. GemSeal uses these security services to generate and validate sealed network packets.

Previously evaluated public interfaces do not change as application and new security services reuse them. GemSeal will use these stable, published APIs, including:

- MLS Shared Data (memory, disk, event counts)
- True protection Rings (8) to protect trusted applications and services
- Crypto seal device access control and operation
- Cryptographic Key Management (for each sensitivity level)
- Trusted Distribution & Recovery (code, configuration and keys)

[Seal] The seal is the final encryption block of the CBC-mode encryption of the packet source-network sensitivity label (canonical representation) and contents of the packet, using a packet-specific initialization vector (IV) and the configured sensitivity level secret key.

[AH] Kent, S., "IP Authentication Header", RFC 4302, December 2005

Reuse of existing security services will minimize the new trusted code needed to create GemSeal trusted security services. A careless designer might propose a traditional VPN as an alternative. However, the connections between networks need to be multi-level secure, and such VPNs would fail to provide assurance high enough to adequately manage the risk of interconnecting high to low networks.

With a rich supply of available security services, application developers will stay focused on delivering functionality, instead of recreating security assurances.

Benefits of using GEMSOS

The Aesec OEM business model for GEMSOS helps deliver solutions quickly. Aesec does not compete with system integrator partners. GEMSOS is intended for use in integrated products and solutions.

GEMSOS has a COTS design, making it a high assurance, reusable subcomponent of trusted systems. It is scalable, with the ability to support embedded deployments, e.g., distributed sensor interfaces, physical and perimeter security applications, trusted electronic transaction devices, etc.

GEMSOS has demonstrated the flexibility of its Open Architecture:

- Previously evaluated as a PC and multi-processor servers
- Previously evaluated in custom crypto-box (BLACKER)

This combination of COTS design and OEM business model make GEMSOS the ideal base for real-world high assurance MLS:

- Distributed network edge devices
- Local/Regional Support Centers
- Enterprise-class Global Operations Centers

Accreditation Fast-Path

GemSeal uses the modular, layered design required for high assurance evaluations to dramatically simplify initial and subsequent accreditation. GemSeal is created on the GTNP platform, and NSA evaluated a previous version of the GTNP as Class A1 under the Trusted Network Interpretation as a M-Component.

The evaluation included the Ratings Maintenance Phase (RAMP) plan that has already been used. The RAMP plan can be used to update the evaluation on modern hardware. Customers can leverage a previous Class A1 evaluation to certify or assess the GTNP platform once.

Subsequent recertification / reaccreditation efforts can then focus on application-specific (GemSeal) additions and configurations. Outside of the GTNP trusted computing base, most of the application software will not be trusted to provide MLS. Only the cryptographic seal operations need be trusted to generate seals and to only release valid sealed packets.

Next Steps

Customer application, certification and accreditation requirements will determine the appropriate next steps.

- Joint Aesec/customer identification of properties, e.g., interfaces, key management, packet filtering, etc.
- Sponsor accredit new security services
- Customer sponsors GEMSOS port to selected target hardware platform
- Sponsor accredit ported GTNP
- Accredit applications as needed

Completed POC Demonstration

Aesec has delivered a POC demonstrating 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

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