aesec™
The power of verifiable protection™

GEMSOS™ Security Kernel RTOS

High Assurance MLS Security & Performance

The GEMSOS security kernel is a successfully deployed, high performance embeddable RTOS with "out of the box" high assurance MLS and mature multi-processor support.

Scalable Multi-Processor Design

The Gemini Multiprocessing Secure Operating System (GEMSOS) design includes both single- and multi-processor configurations (up to 8 processors), with fully symmetric multiprocessing (SMP). This provides the flexibility for performance that is so valuable for a Real Time Operating System (RTOS).

GEMSOS is designed to be reentrant and highly interruptible throughout its entire execution. This delivers efficient multi-processor performance because the kernel does not become a bottleneck.

The GEMSOS security kernel has very limited locks and associated critical sections, that are localized and of short duration internal to the kernel. The kernel itself is not a critical section, so multiple processors can execute simultaneously in the kernel.

MLS Sharing "Out of the Box"

GEMSOS leverages the Intel IA-32 processor architecture to implement a Reference Monitor that verifiably enforces Mandatory Access Control (MAC) policies. GEMSOS delivers full multilevel security (MLS) capabilities with the highest assurance, as confirmed by previous NSA Class A1 evaluations and deployments.

With GEMSOS controlled sharing, sensitive processing can directly access less sensitive data without massive write-up copies. Yet strong separation of processes and protection domains allow strict isolation where required.

This high assurance protection against even deliberate subversion enables controlled sharing across multiple disparate domains (e.g., TS to Unclassified). High assurance is delivered "out of the box" with no need for trusted application code. This is in sharp contrast to "partition" or "separation" kernel approaches which by definition do not include a Reference Monitor. To provide high assurance MLS, those application developers face the high-risk heavy lifting of developing and certifying new trusted application code.

Embeddable RTOS Features

GEMSOS can boot from ROM or disk and supports optional RAM-disk storage for dynamic run-time data. Diskless and storage-channel-free configurations are part of the product baseline.

GEMSOS uses a two-level, priority-based, preemptive scheduler that virtualizes the physical processors of a system into a number of Virtual Processors (VPs), each of which can support a number of processes. VPs are scheduled much like processes in a more conventional system. A VP runs until preempted by a higher priority VP or until it blocks waiting on an event.

Processes are scheduled in the same way as VPs, except processes can be created and destroyed at runtime. Kernel interface services include a real-time clock and interval timer. The system designer has flexible choices for implementing typical real-time properties.

For Further Information Contact

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

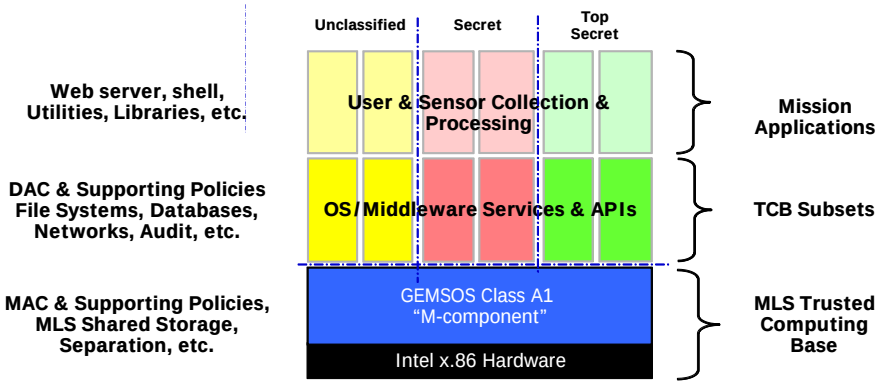

Figure 1 – GEMSOS delivers MLS Sharing "Out of the Box" among strongly separated partitions

Current Intel Processor Support

GEMSOS uses Intel's IA-32 architecture to provide a high performance security kernel. Intel's strong IA-32 commitment assures compatibility with not only current but also future Intel CPU offerings.

This includes compact, low-power, embeddable single-chip processors (e.g., Atom family) up through processors for enterprise-class servers. Even future directions like massively multi-core processor chips reflect Intel's commitment to the IA-32 cores that GEMSOS supports.

Design for Architectural Longevity

GEMSOS is available under a proven OEM business model. Aesec supports system builders to port it to a specific IA-32 chip in unique hardware that evolves over time. Aesec offers a full Software Development Kit (SDK), open source libraries and a structured training course.

The kernel has 14 hierarchical, loop-free layers. Extensive use of information hiding constrains access to internal data structures to a single kernel module. As a result, changes to support new hardware interfaces are isolated and readily identified, facilitating incremental recertification.

Similarly, when support for new devices is added, the GEMSOS split driver architecture provides the hardware interface to device drivers outside the Trusted Computing Base (TCB). The drivers can deliver performance, throughput and functionality while the GEMSOS kernel enforces mandatory access controls.

Gold Standard for Security

Adversaries like foreign intelligence services, organized crime, or terrorist deliberately insert malicious software (like trap doors and Trojan horses) into applications and operating systems. This subverts the very mechanisms relied upon to protect valuable assets from compromise. NSA created the widely respected "Class A1"standard to substantially address subversion.

NSA previously evaluated the GEMSOS security kernel and the product Ratings Maintenance Phase (RAMP) plan at Class A1 in the Gemini Trusted Network Processor (GTNP)[1]. This confirmed that GEMSOS verifiably protects against subversion from malicious software and provided the recipe for rapid evaluatable updates.

NSA demonstrated their confidence when they deployed the GEMSOS kernel for key management and distribution in their Class A1 BLACKER VPN. The kernel was embedded in specialized NSA cryptographic hardware. Other deployments evidenced similar confidence. UK MOD used GEMSOS for their MLS CHOTS Guards. These included interfaces to UK classified cryptographic hardware. The Pentagon used GEMSOS as the front-end communication processor for user access to large IBM mainframes at different security levels. Kernel adaptations support multiple performance-intensive "Bus and Tag" channel connections to mainframe hosts at different classification levels.

[1] http://www.aesec.com/eval/NCSC-FER-94-008.pdf