High Assurance MLS File Service
GEMSOS™ Security Kernel
Demonstration

War fighters have increasingly urgent needs to access the whole range of available information in real time, from coalition combat units and intelligence forces, to US intelligence, weapons and command & control systems, to law enforcement and emergency first responders. Today, it requires redundant terminals, networks and computers to separate all these users, because none of the systems is trusted to keep secrets secret when they are interconnected.

However, devices with Verifiable Protection virtually eliminate the need for multiple computer terminals at everyone's desk, or in command posts and operations centers. Verifiable Protection refers to specific requirements of the Common Criteria called "EAL7" and to the "Class A1" requirements of its TCSEC predecessor, or more commonly the "Orange Book." These specify how to design, build and deliver computer systems that have Verifiable Protection against subversive threats. "Class A1" goes further to specify how to control information sharing across widely disparate sensitivity levels of users and data – that is, Multilevel Security (MLS) – with Verifiable Protection.

By way of comparison, Microsoft Windows and Solaris both have an "EAL4" certification, but you should note that the difference between "EAL4" and "EAL7" is non-linear - "EAL7" and "Class A1" systems, which protect against subversion, must be designed with that as a primary objective from the very start. "EAL7" and "Class A1" products are the only ones to provide verification that they protect against subversion throughout the life cycle of the computer system, from design through development, deployment, operation, maintenance and retirement.

This technology demonstration shows a shared MLS file service running on a preproduction version of Aesec's GEMSOS Security Kernel.

The NSA certified that a previous version of the GEMSOS Security Kernel provides the Verifiable Protection needed to meet Orange Book Class A1 (EAL7 equivalent) requirements. The GEMSOS Security Kernel strictly controls the MLS information sharing WITH NO ADDITIONAL TRUSTED APPLICATION CODE. The result is to make lower-classified data easy to access for users with higher clearance levels, with no risk of high-to-low information flows through the file server.

GEMSOS can support a full range of information sharing services (including web servers, Windows file sharing, and UNIX file sharing), or can enable a single MLS terminal to reliably access multiple networks at widely disparate security levels. In each case, GEMSOS delivers immediate-access high assurance MLS information sharing via untrusted applications to users while achieving verified protection in the process.

GEMSOS Security Kernel was evaluated as part of the Class A1 Gemini Trusted Network Processor (GNTP), and provides the Verifiable Protection for these (and similar) solutions appropriate for Director Central Intelligence Directive (DCID) 6/3 Protection Level 5 accreditation (which could enable direct Internet connectivity from even TS/SCI systems). Commercially supported products with Verifiable Protection (Class A1/EAL7) are deliverable within two years for specific configurations.

For further information contact:

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