

Aesec was founded in 2001 to develop verifiably secure platforms. Our platforms can't be subverted by malicious software. Enterprises and government need this for critical systems. Aesec's verifiably secure platforms:

- Have no trap doors or vulnerabilities
- Are not vulnerable to security policy violations by Trojan horses, viruses, or worms
- Need no security patches
- Are designed so independent third parties can evaluate and validate these claims

We will design our platforms to be evaluated at TCSEC Class A1 or the equivalent International Common Criteria EAL7. No other hardened operating system, appliance, or application on the market can come close to this. They're not designed for Class A1/EAL7. By definition, only Class A1/EAL7 validates system protections against malicious software like trap doors and Trojan horses. These are the tools that professionals use to attack the data of critical systems. Verifiability is a difference in kind for security, not merely degree. Aesec is now the only way to get it.

We are currently developing a thin client platform for multilevel secure (MLS) workstations. Enterprises and government can connect these PCs to both sensitive networks and to the Internet simultaneously, in a switched environment, with the verifiable assurance that network or Internet users cannot subvert the PCs. A white paper is available to potential partners on request. We will also build server platforms for Java, Linux, and appliances. These platforms will protect application servers, integration platforms, storage subsystems, VPNs, and other applications.

Enterprises deploying all these applications need to protect the rules for separation and sharing between classes of applications, data, and users. And they need to protect cryptography, roots, keys, and certificates. But no platform on the market verifiably protects any of this against professional attack.

The power of verifiable protection is that Aesec platforms maintain a secure state regardless of the applications built on them. So Aesec platforms can meet all these needs with verifiable protection for a wide variety of Internet applications. Aesec platforms deliver:

- Compartmentation or controlled sharing of real time data among systems
- Protection from bypassing or tampering for security mechanisms like crypto, roots, keys, certificates
- High performance and flexibility for a wide range of applications and platforms
- Seamless user experience for Java, Linux, server based computing, appliances, and virtual machines

Aesec acquired Gemini Computers in 2003. We will build our platforms on Gemini's GEMSOS™ security kernel – the only general-purpose kernel in the world rated *Class A1: Verified Protection* by the National Security Agency (NSA). The GEMSOS kernel has been deployed and proven in high performance military and intelligence applications. It has protected even the most sensitive national interests on the Internet for over a decade, even against subversion from hostile intelligence services with essentially unlimited resources, without even one security patch, ever. Customers have loved it. There is no reason enterprises should expect less sophistication from their attackers over the Internet today, or demand less protection for their critical systems. Aesec is currently refreshing GEMSOS and pursuing partnerships and support for products and updated evaluations. A description of the GEMSOS platform is available on request.

In addition to security and performance, Aesec platforms offer critical product development advantages. The development engineering necessary to adapt many Internet applications to run on GEMSOS is straightforward. This is because GEMSOS is:

- Smart hardware – applications can be adapted to GEMSOS much like porting to new hardware
- Extensible – to protect security services like crypto for security appliances, without changing GEMSOS
- Flexible – product development does not require massive changes to many Java, Linux, other applications
- Versatile – to run on hardware platforms ranging from embedded systems to multiprocessing servers

Aesec's Co-Founder and President, Dr. Roger Schell, is a recipient of the National Computer System Security Award, the highest honor in the information security field. Roger led the original development of GEMSOS, and Aesec brings together an exciting team including several engineers who worked with Roger on GEMSOS. Roger was more recently Corporate Security Architect at Novell. Prior to all that, he was the founding Deputy Director of the NSA's National Computer Security Center, and one of the architects of the TCSEC, or Orange Book.

Potential partners seeking more information should send detailed contact information to info@aesec.com.