

Executive Summary
Weapons Systems Avionics Security
PNUM 40

Background: The purpose of the project is to support, advance, and complete the coordination of open systems security standards establishment, refining their features and services for the weapons system community, and foster their acceptance within recognized standards communities that promote specifications and guidance for the Portable Operating System Interface (POSIX) standard, [ISO/IEC 9945-1:1990; IEEE STD 1003.1-1990].

The major focus of the effort has been the assessment of the draft POSIX security standards with respect to their applicability to military avionics and weapons systems. The effort has also sought the identification of additional security services not currently provided in the POSIX standards but critical to military and industrial partners, especially critical for weapons systems. A technical document was produced which provides a comparative analysis of the various security features and capabilities of POSIX to the weapon systems avionics security requirements. The document cites those security features that are not included in POSIX as a delta requirement (hence the document has been called the "Delta Document"). The task participants followed the IEEE PASC security group activity and investigated the possibility of establishing a study group to address additional security requirements of importance to the military weapon systems community.

The efforts begun in FY 97 will continue in FY 98 with central focus on the identification of critical military security services and the expansion of the security-relevant Delta Document. The task will continue to seek opportunities to advance security for military systems through involvement in selected investigations and participation in various open system standards bodies and standards-related activities. Areas of interest include security features and models appropriate for real-time systems, security solutions available in the Joint Technical Architecture (JTA) and DoD Information Infrastructure Common Operating Environment (DII COE), and the development of a secure real-time Common Object Request Broker Architecture (CORBA) standard.

Problem and Solution: Integrated weapon systems are increasingly dependent on application software (often developed by different companies and organizations) that shares the same resources (buses, processors, disks, and memory). Software bugs/viruses and other "program threats" that modify or destroy data, cause denial of service, or cause unintended actions are particularly onerous when they affect "real-time" servo control loops essential for safety of flight, calculating firing solutions, and controlling countermeasures.

Having adequate standards based practices that are acceptable to both DoD and industry has become a top priority in order to address issues in real-time embedded system security such as:

- The increasing dependence of both the DoD and the civilian community on information services,
- The escalating "hacker" threat,
- Increasing connectivity of formerly physically isolated, real-time systems,
- Exposure to compromise due to use of shared resources,
- The emergence of the "infosphere" as a recognized battle space,
- The emergence of information warfare as a recognized mission area, and
- Ensuring secure interoperability among members of potentially diverse communities.

The operating system combined with additional trusted applications and hardware platforms forms the key elements of a system's Trusted Computing Base (TCB). The TCB ensures that software security features developed by one entity does not inadvertently or intentionally interfere with those written by other entities, and that there is interoperability among supported platforms. This is especially important for Commercial-Off-The-Shelf (COTS) products and reusable application software, where genesis and "trust assurance" of the software may be unknown.

Major Beneficiaries: All major DoD organizations, offices, and programs that address weapons and avionics systems such as Joint Strike Fighter Program, US Army Tank Automotive Command, Ballistic Missile Defense Office, and Theater Air Defense Program will benefit from this effort. Commercial entities, such as Railway Control Systems, Air Traffic Control Systems, Urban Transit Systems, and Civilian Crisis Management Systems, employing real-time control/information systems can also benefit from this effort.

Participation in Standards Bodies: Participants include personnel from SPAWAR Systems Center – San Diego, Lloyd Lamont Design (LLD), DISA Center for Standards, and Hughes Aircraft Company (HAC). The participants in this effort are associated with various standards bodies including IEEE PASC and The Open Group.