Software Protection: An Essential Layer of Security

Jeff Hughes
AFRL, WPAFB, OH
Jeff.hughes@wpafb.af.mil

Introduction. In December 2001, the Under Secretary of Defense for Acquisition, Technology, and Logistics directed the Deputy Under Secretary of Defense for Science and Technology to establish the Software Protection Initiative (SPI) to prevent the unauthorized distribution and exploitation of DoD application software by our adversaries. The focus of the initiative is to improve the protections of Defense scientific, engineering, and modeling and simulation software. The SPI develops software protection technologies; supports the insertion of these technologies into application software; defines the policy for protected development and distribution of application software; and provides guidance on export control regulations in coordination with the Office of the Under Secretary of Defense (Policy)/Defense Technology Security Administration (OUSD(P)/DTSA).

Objective. The objective of the SPI is to protect critical DoD intellectual property using an application centric approach which complements existing information assurance efforts in network security and operating system access controls. This objective will be achieved by institutionalizing software protection as part of the application software lifecycle, educating and training the community on the SPI vision and goals, developing a wide array of user-friendly protection techniques, and ensuring that protection technology and policy are appropriately applied, balancing mission requirements with security.

Methodology. First generation protection technologies are being inserted into select, critical codes for use within their normal operating environment. Protected codes are being evaluated to determine the level of protection achieved and any impact on code performance. Resultant lessons learned are being incorporated into follow-on protection efforts to improve the level of protection achieved, minimize the impact on code performance and to facilitate ease of use. Additional form factors are being tested to support the diverse user community. A substantial research and development activity is developing next generation protection techniques that advance the state of the art in protection, detection and reaction techniques while minimizing adverse impacts on the user and code performance.

Results. SPI has improved the PCI card based on lessons learned to date and has begun testing of USB and network devices. A Unified Protection Architecture (UPA) has been developed and tested. The development of the UPA provides several advantages that will improve protection technology interfaces. Protection technologies have been inserted into multiple codes currently in use by over 500 DoD users.

Significance. The validation of robust protection techniques, coupled with the development of the UPA, enables the SPI to protect a wide variety of critical applications running on desktops to supercomputers. UPA provides a consistent static interface between the application code and the underlying protection engine, eliminating the need to change the application code as new protection techniques are added or modified. It provides a public and portable kernel–level code that is the "glue" that completes the task of protecting numerous codes simultaneously while maintaining the flexibility of serving systems ranging from the isolated single host to the densely clustered fabric of modern high performance configurations.

Approved for public release March 14, 2003
P.A. #ASC-03-0672