

Transition

An example of Air Force supported SBIR/STTR technology that has been transitioned into an Air Force or other DoD system or subsystem or used by Air Force test ranges and facilities or maintenance depots.

SBIR Topic Number:

OSD04-SP4

SBIR Title:

Polymorphic Software

Contract Number:

FA8650-06-C-8051

SBIR Company Name:

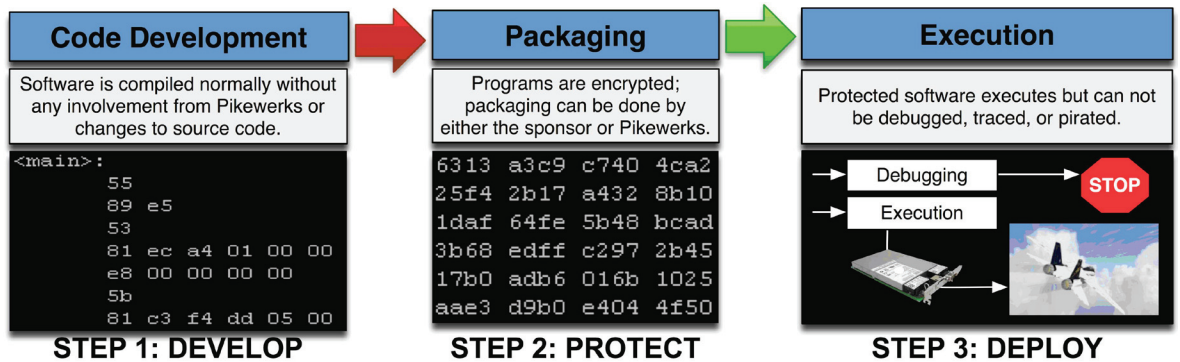
Pikewerks Corporation,
Alexandria, VA

Sponsoring Office:

Office of the Secretary of
Defense, Washington, DC

Technical Project Office:

AFRL Sensors Directorate,
Wright-Patterson AFB, OH



Electronic Armor operates using a 1) develop, 2) protect, and 3) deploy process; no changes to the source code are necessary and protected applications are stored encrypted on disk.

Software Protection by Polymorphic and Metamorphic Transformations

- Software protection to prevent piracy, reverse engineering, and tampering of critical applications from nation-state class adversaries is needed to prevent exploitation and compromise of Department of Defense (DoD) weapon systems
- The kernel-based protections are supplemented by programmable commercial off-the-shelf hardware that stores and executes critical information and data out-of-band to the adversary
- Applications that can be protected include desktop and workstation software applications, real-time embedded system software, high performance computing applications, and sensor systems
- Pikewerks Corporation developed Electronic Armor®, which is an operating system kernel-based software protection technology that prevents piracy, reverse engineering, and tampering of critical software applications on Linux, Windows, VxWorks, Red Hawk Linux, and Solaris
- Electronic Armor has been transitioned to several DoD organizations and prime contractors

Air Force Requirement

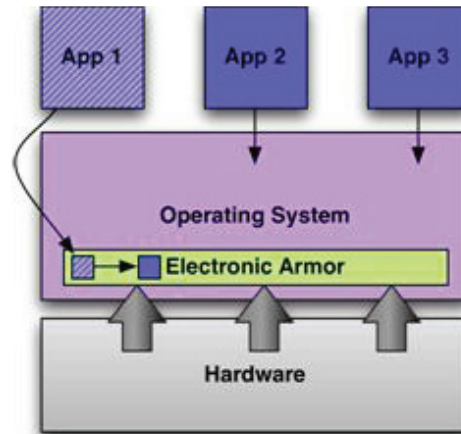
Software protection to prevent piracy, reverse engineering, and tampering of critical applications from nation-state class adversaries is needed to prevent exploitation and compromise of Department of Defense (DoD) weapon systems.

SBIR Technology

Pikewerks Corporation developed Electronic Armor® under this SBIR project, which was sponsored by the Office of the Secretary of Defense and managed by the AFRL Sensors Directorate. Electronic Armor is an operating system kernel-based software protection technology that prevents piracy, reverse engineering, and tampering of critical software applications on Linux, Windows, VxWorks, Red Hawk Linux, and Solaris. The kernel-based protections are supplemented by programmable commercial off-the-shelf hardware that stores and executes critical information and data out-of-band to the adversary.

system software, high performance computing applications, and sensor systems.

Electronic Armor has been transitioned to several DoD organizations and prime contractors. Since many of these systems will be deployed in hostile territory and other areas where adversaries will have access to the computers running the software, Electronic Armor will have a significant impact on the security of those systems.



Electronic Armor interfaces directly with an Operating System to protect application software.



Electronic Armor can ensure the security and integrity of protected applications both at rest on disk and during execution. Depending on the deployment scenario, Electronic Armor supports:

- Debug prevention
- Copy protection
- Input/output file protection
- Secure coprocessors
- Out of band storage and execution
- Out of band attestation
- Secure loading
- Tiered encryption
- Layered defenses
- Integration with other anti-tamper solutions

Company Impact

“Pikewerks Corporation started with two employees in 2005 with its first Office of the Secretary of Defense (OSD)-sponsored Phase I SBIR contract related to the Anti-Tamper Program and Software Protection Initiative (ATSPI) and has grown to 42 employees in 2010,” states Sandra Ring, company founder and president. “The estimated revenue from Electronic Armor sales and follow-on development contracts from the DoD and defense prime contractors account for over \$5 million annually.”

“Pikewerks has significantly contributed to improving the overall cyber security posture of the United States through its dedicated staff and leadership in the software protection and anti-tamper community.”

Transition Impact

Critical information on weapons systems resides largely in the software running on those systems. Electronic Armor protects that software from compromise and exploitation. Applications that can be protected include desktop and workstation software applications, real-time embedded



SBIR/STTR

Air Force SBIR Program
AFRL/XP
1864 4th Street
Wright-Patterson AFB OH 45433

AF SBIR/STTR Program Manager: Augustine Vu
AF CPP Program Manager: Richard Flake
Website: www.sbirsttrmall.com
Comm: (800) 222-0336
Fax: (937) 255-2219
e-mail: afrl.xppn.dl.sbir.hq@wpafb.af.mil

