Air Force SBIR/STTR

Innovation

Air Force SBIR/STTR Innovation Story

SBIR Topic Number:
OSD07-I05

SBIR Title:
Autonomic Kernel Protections to Reduce Attack Susceptibility

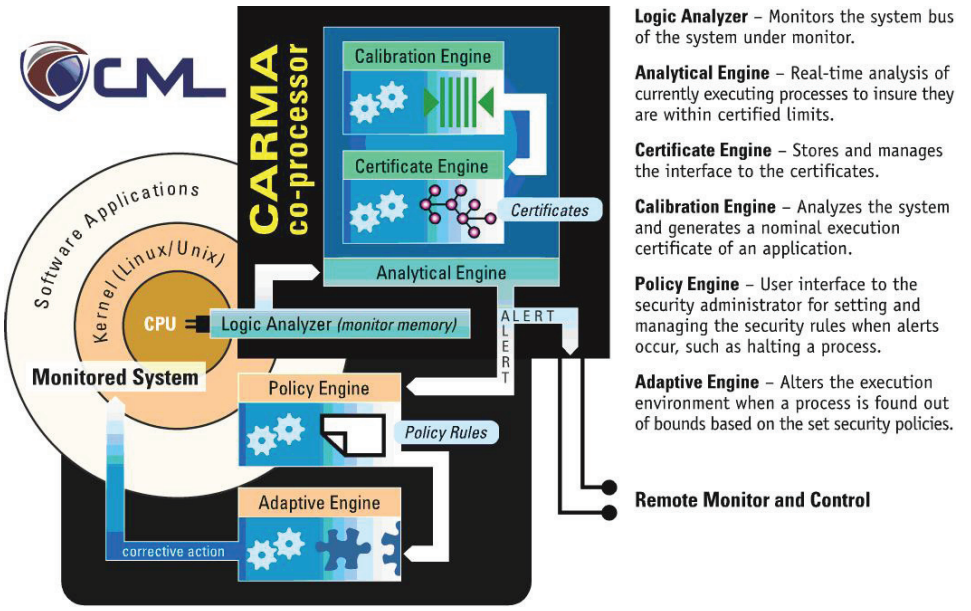
Contract Number:
FA8650-08-C-1460

SBIR Company Name:
Computer Measurement Laboratory, Inc., Meridian, ID

Sponsoring Office:
Office of the Secretary of Defense, Washington, DC

Technical Project Office:
AFRL Sensors Directorate, Wright-Patterson AFB, OH

This Air Force SBIR/STTR Innovation Story is an example of Air Force supported SBIR/STTR technology that met topic requirements and has outstanding potential for Air Force and DoD.



Computer Measurement Laboratory (CML) Attack Recognition Management Architecture (CARMA™)

Dynamic Kernel Monitoring for Attack Detection and Mitigation

- The Department of Defense needs to develop advanced self-monitoring and self-healing techniques for Linux kernel software protection technology
- Computer Measurement Laboratory, Inc., (CML) designed an engineering methodology for software process control developed around an 8-Lane PCI Express (PCIe) card, which is the initial release of an extensive family of software process control systems
- Through use of the CML Attack Recognition Management Architecture (CARMA™), which represents a proof-of-concept in the PCIe card environment, software processes can be monitored during their execution by a hardware-based control system
- The savings for the full utilization of the software/system process control would extend the lives of legacy systems and significantly reduce the lifecycle costs

01-19OCT10/OSD073-I05

Air Force Requirement

The Global Information Grid (GIG) requires software security that extends to the end-nodes of the network. Software applications that are vulnerable to malicious alteration, piracy, and reverse engineering can result in the compromise of command, control, and communication channels. The Anti-Tamper Software Protection Initiative (AT-SPI) Technology Office is performing research and development in kernel-mode software protection as a means to protect applications by making them less accessible (i.e., more out-of-band) to the attackers.

The Department of Defense (DoD) needs to develop advanced self-monitoring and self-healing techniques for kernel software protection technology.

SBIR Technology

Computer Measurement Laboratory, Inc., (CML) developed an engineering methodology for software process control. If a software system has been compromised, its normal activity profile will change. Processes may then be instituted to restore the system to a nominal state. CML has leveraged dynamic measurement technology to develop an engineering approach to software process control. The objective of this approach is to break the traditional software vulnerability cycle. Through the use of software process control, a software system may be monitored, in real time, for evidence that it has been compromised.

The process control system was developed around an 8-Lane PCI Express (PCIe) card. The PCIe card is the initial release of an extensive family of software process control systems. The FPGA on this card contains all of the components required to implement CML's Attack Recognition Management Architecture (CARMA™). In this context, the complete execution-monitoring environment for the entire monitored system resides on the card. The card is equipped with its own Ethernet port that provides a secure communication channel for interacting with the monitoring system from a single security server. This technology can be readily integrated into the current servers and desktop systems in use today.

The objective of the ongoing Phase II program enhancement is to migrate software process monitoring technology to the embedded systems design and development environment. Using the embedded CARMA technology, software processes can be monitored during their execution by a hardware-based control system. Their operation is continuously compared against a standard execution model. If a process deviates from its normal or standard execution model, the CARMA system can move to alter the executing code to return it to a normal execution mode. CARMA is implemented as a hardware coprocessor. This coprocessor is capable of monitoring the execution of all software running on the host computer, including the operating system kernel itself.

There are three essential components in the CARMA system:
- The Analytical Engine runs on the coprocessor system. It receives telemetry from the host central processing units (CPUs) via a logic analyzer.
- The Calibration Engine is used to build a model of standard or certified behavior for a software system that is to be monitored. It will compare the currently executing software process against a standard model or certificate of normal process operation.
- The Certificate Librarian maintains the Software Process Control (SPC) certificates for all certified programs.

Potential Application

The CARMA system represents a proof-of-concept in the PCIe card environment. It lays the foundation for the design of future computer architectures that provide for the continuous monitoring of software. As more software systems come under the control of continuous process monitoring, the cyber threat to future systems will begin to diminish.

The implementation of this technology has the potential of revolutionizing every aspect of software and system lifecycle cost and functionality. It provides a way to bring out-of-control systems back under control while also providing mechanisms to completely understand how things break down and how to fix them. The savings for the full utilization of the software/system process control would extend the lives of legacy systems and significantly reduce the lifecycle costs.

Company Impact

"CML is pioneering real-time software measurement technologies for security and reliability of software applications," states CML co-founder Rick Hoover. "Our company had the opportunity to pursue this technology innovation because of the federal funding. With the assistance of SBIR contracts, we have solidly launched our company and have been able to hire additional employees."

U.S. AIR FORCE

SBIR/STTR

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

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