

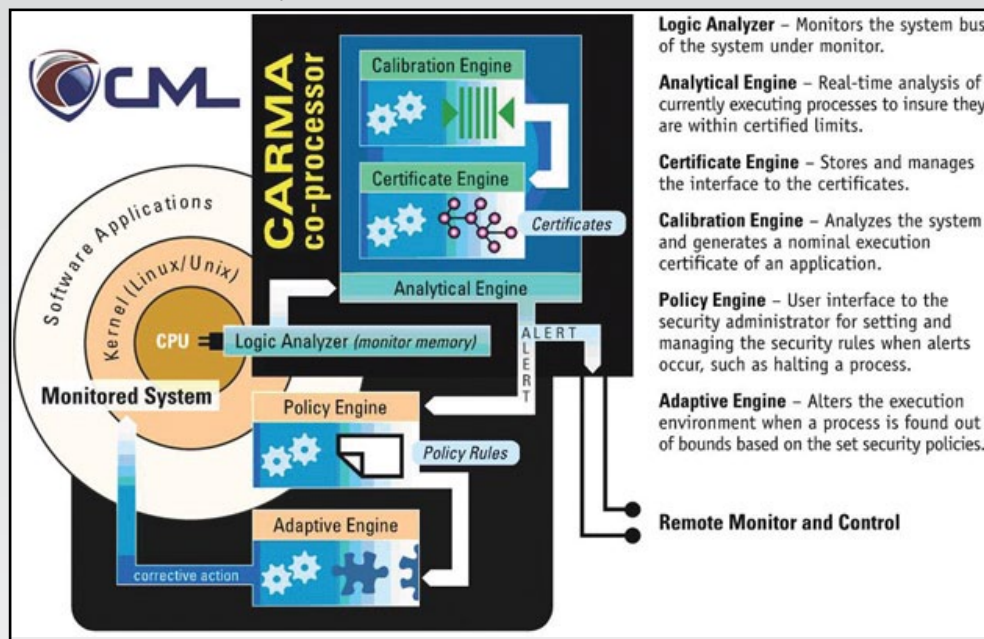
Engineering Methodology Designed to Monitor Software Security

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.

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.

system may be monitored, in real time, for evidence that it has been compromised.

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.



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

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.

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

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