

Security and certification necessary for mission-critical software

BY JOHN McHALE

SANTA BARBARA, Calif.—Speakers at the third annual Green Hills Embedded Software Summit last month touted security and certification as necessary for software used in military applications such as the F/A-22 fighter-bomber and the F-35 Joint Strike Fighter.

The increased use of commercial off-the-shelf (COTS) technology has created the need for assurance that these systems will not fail, they say.

“Once upon a time before the need for commercial off-the-shelf (COTS), custom products were the norm for the military and assurance was required,” says Robert Williamson, assistant vice president of corporate development at Science Applications International Corp. (SAIC).

The correct way for the U.S. Department of Defense (DOD) and prime contractors to use commercial technologies is to fund partner vendors to achieve necessary DOD capabilities, says Ben Calloni, research program manager of advanced development at Lockheed Martin Corp. in Bethesda, Md.

Funding partners should make long-term business sense to the vendor, be commercially sustainable through sales of product, meet specific needs of more than one program, and DOD assumes no ownership; intellectual property rights are retained by the vendor, Calloni says.

“Certified COTS technology vs. DOD-proprietary “equals 84 percent savings,” he says.

The key is to ensure that an independent body evaluates the products.

“Product evaluation is the business of building secure products,” Williamson says. Evaluators should understand the security technology, design issues, read code, and testing—evaluation should be an enabling technology.

The benefit of using evaluation is to help customers create a security specification for types of information technology (IT), Williamson says. Customers can identify the appropriate assurance requirements rather than create a request for proposal for a custom government product, he added.

Software companies such as Green Hills, Wind River Systems in Alameda, Calif., and LynuxWorks in San Jose, Calif., are working toward certification under the Common Criteria Evaluation and Validation Scheme (CCEVS), which is the U.S. version of an International standard—ISO 15048.

The National Information Assurance Partnership (NIAP) is performing evaluations of code. NIAP is a U.S. Government initiative to meet the security testing needs of IT consumers

and producers. It is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under PL 100-235 (Computer Security Act of 1987).

The Common Criteria is a “common language and structure for expressing IT security requirements in a manner that allows those requirements to be used to evaluate allegedly conforming products,” Calloni says, adding that he sees companies someday possibly using the fact that their code is certified as a defense in court.

Software vendors are obtaining this high-level of assurance through Multilevel Security (MLS), which is about enabling application-level processes to enforce the policy semantics specific to an organization, Calloni says. MLS does this by distributing high-confidence, trusted enforcement mechanisms across several layers.

The MILS architecture is a layered architecture concept that helps compose system properties from trusted components, Calloni says. Layered functionality and assurance comes with four conceptual layers: separation kernel and hardware (single node); distributed communication (multiple nodes); middleware services (single node); and trusted applications as required on one node.

Common Criteria Testing Laboratories executes valuation activities, and NIAP representatives provide evaluation oversight, Calloni says. Currently the governing bodies are only issuing guidelines for evaluation and assurance not for import/export controls, Calloni says.

Williamson explained that the Common Criteria comprises several criteria: a metric for documenting design, implementation, maintenance, and testing; a methodology to physically install and test a product against documented design and guidance; a meta-language as a methodology to create comparable security for IT products and systems; and a method to compare security functions and assurances between commercial products of like technologies.

There are two main risks to mitigate—those without a security feature and those for which an implemented security feature is unreliable, Williamson says.

The Common Criteria describes assurances based on three components, product development environment, operating environment, and independent evaluation, Williamson says.

The Common Criteria has seven levels of evaluation; one is the least secure and sev-

en is the most. The one that companies like Green Hills are pursuing is the Evaluation Assurance Level 6-plus (EAL6+), which deals with code for life-threatening, classified environments.

During the evaluation process 100 percent of products evaluated are improved, 30 percent improve security by eliminating exploitable flaws, 40 percent directly improve security by adding or extending security features, and 100 percent have needed to modify documentation to remove ambiguities conflicts and or clarify security functions, Williamson says.

Green Hills engineers demonstrated their version of MLS, the Padded Cell, at the conference.

The Green Hills real-time operating system (RTOS), Integrity, has Padded Cell technology to enable people who have Windows and Linux applications that are not mission critical to run on top of Integrity, says Jeff Hall, regional field application engineer at Green Hills.

The padded cell enables Linux and Windows functions, but keeps them from touching hardware or the real-time functions of Integrity. If a virus infects an application in Windows, Integrity will shut Windows down while still running Linux and protecting the real-time applications from the virus.

Dan O’Dowd, the Green Hills chief executive officer, expressed concern that the continued push toward open-source systems like Linux will create problems not only for securing software for critical applications but for the embedded job market in the U.S.

“New embedded manufacturing jobs are moving offshore and if I don’t speak up now CEO jobs will move offshore,” O’Dowd says.

The only way to keep jobs in the U.S. is to enable American engineers to do something the engineers overseas cannot—write software programs that never fail and that no hacker can break into, O’Dowd says.

Airplanes crashes have yet to be traced to software because the software does not fail, O’Dowd says. Software for critical applications such as airplanes will not come from overseas for this reason, he added.

Green Hills charges more for its product because it does not fail and because it pays for high-end engineering talent necessary to write reliable code, O’Dowd says.

There is an unlimited supply of programmers in India, China, and Russia who have Linux and Eclipse skills but not ones who can write code for real-time operating systems (RTOSs) such as Integrity, O’Dowd says. ●