CMP
United Business Media

ELECTRONIC ENGINEERING
EETIMES
The industry newspaper for engineers and technical management

WWW.EET.COM APRIL 19, 2004

Linux: unfit for national security?

OS among those not suited for defense apps, experts say

By Charles J. Murray

Chicago — Days after an embedded-industry CEO stirred up a firestorm by charging that Linux poses a threat to U.S. security, two prominent computing-security experts said last week that some developers are already inappropriately using Linux in critical security applications where it isn't suitable.

Purdue University professor Eugene Spafford and Cynthia Irvine of the Naval Postgraduate School warned that the highest-level, but little-understood, security concerns are sometimes ignored during the development of control systems for tanks, bombs, missiles and defense aircraft. Linux, Windows and Solaris operating systems should not be used in such applications, Spafford said.

"An awful lot of decisions involving national-defense implications are being made on the basis of price and personal bias, and not upon sound evaluation of the underlying tools and software," said Spafford, who is executive director of the largest U.S. academic research center on information security, the Center for Education and Research in Information Assurance and Security, as well as an adviser to President Bush. "And it's happening in places where it should not be happening."

'Decisions involving national defense are being made on the basis of price and personal bias.'
Purdue's Spafford

'People have heard Linux is secure and are starting to use it in tanks, bombs and planes.'
Green Hills' O'Dowd

Although Spafford said that virtually no developers would attempt to use Windows in such high-security applications, many are already employing Linux, believing it is sufficiently secure.

"I don't want to single out Linux alone, because it is not the only [operating] system with problems," he said. "But it certainly has one problem, and that is that there are many elements of unknown provenance in it."

"Software subversion," in which adversaries add a few lines of code that can cause a major system to malfunction, is a concern of security experts, said Irvine, a professor of computer science and an expert on information warfare at the Naval Postgraduate School in Monterey, Calif. In such applications, she said, developers need to use "high-assurance" operating systems with the smarts to prove that subverting code doesn't exist. Linux, she said, is not one of them.

"There are definitely places within the national critical infrastructure where we should be concerned and should be looking at higher-assurance systems to protect us from adversarial attack," Irvine said.

Spafford added that he "would be scared to death" to be near a power plant or defense aircraft that employed any of the "general-use operating systems," such as Linux, for the highest levels of safety-critical control.

Comments by Spafford and Irvine stood in sharp contrast to those of many embedded-industry members who vehemently argued last week that Linux is inherently secure. Makers of Linux-based tools and software, and even some Linux competitors, went on record to declare that Linux's development process, which involves the scrutiny of thousands of individuals, makes it almost impossible for "adversarial code" to sneak through. Their comments came on the heels of assertions about "the Linux threat" made a week earlier by Dan O'Dowd, chief executive officer of Green

Hills Software Inc. (Santa Barbara, Calif.).

“The open-source community doesn’t just take whatever someone contributes,” noted Bill Weinberg, strategic-marketing director of MontaVista Software Inc. (Sunnyvale, Calif.). “These contributions aren’t like a message in a bottle.”

“It [Linux] poses no more of a threat than any other operating system in the world,” said Neil Henderson, general manager of Mentor Graphics Corp.’s Embedded Systems Division (Wilsonville, Ore.), a maker of hardware and software design solutions.

Speaking at the Net-Centric Operations Industry Forum in McLean, Va., O’Dowd of Green Hills said that Linux violates every principle of security, and charged that Linux suppliers MontaVista Software and LynuxWorks Inc. are using offshore software developers in such locales as Moscow and Beijing, a practice he described as a security threat.

Executives from both those companies, as well as others in the embedded industry, blasted O’Dowd’s comments as a form of FUD (a claim that causes “fear, uncertainty and doubt” about Linux).

‘Plays on paranoia’

“The way it was stated is exaggerated, and it plays on the paranoia about terrorism and even communism,” said Inder Singh, CEO of LynuxWorks (San Jose, Calif.). Singh added, however, that if suppliers are creating a piece of security-related software, “it should be done in the U.S., by U.S. citizens.” Singh said that is how LynuxWorks develops its own security-related software.

O’Dowd has since reiterated and even amplified his comments about Linux’s security shortcomings. He told *EE Times* last week that in the past few months he has spoken to developers working on control systems for tanks and other high-security systems, and has seen individuals who are planning to use Linux and are unaware of what he describes as its security lacks.

“What concerns me is that people have heard Linux is secure and they are starting to use it in tanks and bombs and planes,” O’Dowd said. “We’ve known this for months, and it scares me. If we don’t tell them soon about the security problems, they will get so far down the road in the development process that they won’t be able to change.”

O’Dowd cited Green Hills’ Integrity real-time operating system, along with LynuxWorks’ LynxOS-178 and Wind River Systems’ VxWorks AE653 RTOSes, as secure solutions.

Foreign risk

Industry executives, however, bristled last week at the suggestion that such operating systems could solve the subversion problem, arguing that O’Dowd was using the subject to focus attention on his own company’s product.

“It’s ridiculous,” said Henderson of Mentor Graphics. “Is he saying that he has no foreign employees? He has no one who could subvert his code? He makes compilers that are used by the military. What’s to stop one of his employees from putting a backdoor into the code that’s generated by the compiler?”

Security experts Spafford and Irvine, however, said the oft-cited “many eyes” concept of open-source software development is not a sufficient form of assurance for national-security-level applications. “A subtle flaw could be included in the system and missed by all those eyes, because they may not have the training or motivation to look for the right problems,” Spafford said.

Spafford, an IEEE Fellow who has testified before Congress on matters of national information security, urged the programming community to get past issues of cost, corporate politics and technological “religion” when dealing with matters of national security.

“The problem occurs when a vendor decides to adopt software because of cost or because of familiarity to their current programmers,” he said. “They end up making a decision that involves risk, and they don’t have the appropriate background to make that decision.”

Irvine said that to head off catastrophes, high-security applications need software that can’t be corrupted. “The Linux people feel that Linux is very flexible, so they can do many things with it,” she said. “But one of the things you can’t do with it is demonstrate the absence of subversive artifice in the system.”

Spafford added that the embedded community needs to have rational discourse on the subject. “The question is why people are so up in arms about this Linux story,” he said. “Do they want a system with flaws in it to be used in national defense?”

Lessons of ‘Farewell Dossier’

A cautionary tale of code corruption from CIA annals

To illustrate the risks associated with subversive software, Cynthia Irvine, a professor of computer science and an expert on information warfare at the Naval Postgraduate School, points to a Cold War example.

During the 1970s and early ’80s, Soviet spies were having a field day stealing technology secrets from the United States and other Western nations. In early 1982, the CIA slipped a so-called Trojan horse into code subsequently stolen by Soviet spies as part of a program called Line X. The situation was one of many detailed in a report called the “Farewell Dossier.” “Farewell” was a Russian engineer assigned to evaluate stolen technologies; he also was a French spy who turned over everything to French intelligence officials, who subsequently compiled the dossier and handed it to the CIA.

Line X operatives obtained the buggy software and deployed it on a Trans Siberian gas pipeline. The bug eventually caused a 3-kiloton blast considered the most monumental non-nuclear explosion and fire ever seen from space.

Gus Weiss, an economist who helped devise the plan, wrote about the caper in a 1996 edition of *Studies in Intelligence*, a periodic journal published by the CIA (*cia.gov/csi/studies/96unclass/farewell.htm*). — *Charles J. Murray*