design® news
Reed Business Information.
07.19.04
INSIDE THE WORLD OF DESIGN ENGINEERS
www.designnews.com

RANT
Really Opinionated People

DAN O'DOWD
CEO
GREEN HILLS SOFTWARE INC.

No Defense for Linux

INADEQUATE SECURITY POSES NATIONAL SECURITY THREAT

LINUX IS BEING DESIGNED INTO FUTURE

U.S. defense systems, including the Army's Future Combat System (FCS), the Land Warrior, and the Global Information Grid, which will connect future military systems into one network. This spread of Linux into defense systems is cause for serious concern. Linux security is inadequate for defense use.

The operating system used in defense is the foundation of its overall integrity. The operating system controls all of a system's functions, communications, and security; if it is compromised, an enemy can spy on, disable, or commandeer the entire system.

The Linux operating system is developed by an open source process. With the knowledge that Linux is going to control our most advanced defense systems, foreign intelligence agencies and terrorists can easily infiltrate the Linux community to contribute subversive software. The risk is particularly acute since many Linux contributors are based in countries from which the U.S. would never purchase commercial defense software. Some embedded Linux providers even outsource their development to China and Russia.

It would be incredibly naive to believe that other countries and terrorist organizations would not exploit an easy opportunity to sabotage our military or critical infrastructure systems when we have been doing the same to them for more than 20 years!

Linux in the defense environment is the classic Trojan horse scenario—a gift of "free" software is being brought inside our critical defenses. If we proceed with allowing Linux to run these defense systems without demanding proof that it contains no subversive or dangerous code waiting to emerge after we bring it inside, then we invite the fate of Troy.

One of the greatest misconceptions about Linux is that the free availability of its source code ensures that the "many eyes" with access to it will surely find any attempt at sabotage. Yet, despite the "many eyes," new security vulnerabilities are found in Linux every week in addition to dozens of other bugs. Many of these flaws have eluded detection for years. It is ridiculous to claim that the open source process can eradicate all of the cleverly hidden intentional bugs when it can't find thousands of unintentional bugs left lying around in the source code.

Linux is being selected for defense systems because of the perception that it is more secure than Windows. However, this conventional wisdom is unsupported by quantitative data. In fact, the U.S. National Institute of Standards and Technology (NIST) security vulnerabilities database lists more vulnerabilities for Linux than Windows in the last ten years. In addition, under the internationally recognized Common Criteria for IT Security Evaluation (ISO 15408), Windows has been certified to Evaluation Assurance Level 4 (EAL 4), a higher level of security than the EAL 2 that Linux has achieved.

Even if Linux were as secure as Windows, Windows is the wrong benchmark. Defense systems should be held to a higher standard.

The Federal Aviation Administration (FAA) requires software that runs commercial (and many military) aircraft be approved as part of a DO-178B certification. DO-178B Level A is the highest safety standard for software design, development, documentation, and testing. It is required for any software whose failure could cause or contribute to the catastrophic loss of an aircraft.

Several operating systems have been DO-178B Level A certified. Until Linux is certified to DO-178B Level A, our soldiers, sailors, airmen and marines should not be asked to trust their lives with it. ■

O'Dowd is CEO of Green Hills Software.