

# On The Softer Side

RTOSes: Linux Update

## Opinion: Linux Can Be Used in the Military

Bob Morris, Vice President, Sales and Marketing  
LynuxWorks

There has been lively debate recently regarding the use of Linux military applications. One proprietary (OS) vendor has boldly claimed, “Every principle of security is being violated to enable Linux to spread through our defense systems. This must not be allowed to continue.” Sweeping generalizations such as this have certainly fueled the fear, uncertainty and doubt (FUD) surrounding the use of Linux in the military.

Taking these self-serving and short-sighted statements aside, the embedded software and military industries must determine the real issues of using Linux in the military. Linux from an operational point of view is very similar to other robust OSes such as Solaris, UNIX or LynxOS because it is open, standards-based and POSIX-conformant and capable of running tens of thousands of different off-the-shelf applications. What is different in other embedded OSes that is not found in Linux? Most importantly, can Linux be run in a secure network-centric environment without compromising security?

The real center of controversy is the fact that the Linux source code is open for all to see. Consequently, proprietary OS vendors claim that the openness of Linux creates vulnerability dangers because programmers can insert malicious code that could potentially create a security breach. One of the many values of Linux, however, is the fact that the Linux source code has tens of thousands of programmers reviewing it to identify this type of insertion. Vendors

that preach “security through obscurity” believe it is better that a single company with only a handful of people be able to view the source code and look for the insertion of malicious code. These vendors would have us believe that trusted programmers inserting malicious code and hiding it from their internal reviewers is not a possibility.

Proprietary OS vendors also state that Linux cannot be certified to Common Criteria level EAL-7. While this is accurate, let’s not ignore the fact that there are *no* COTS OSes certified to EAL-7. In fact, no COTS OS is certified higher than EAL-4. Therefore, Linux is no worse off than other OSes on the market today. Nonetheless, Linux opponents and naysayers continue to spread FUD that Linux cannot run in a secure network and that only a proprietary operating system can be trusted.

Green Hills Software, LynuxWorks and Wind River Systems are three embedded software vendors currently working toward achieving EAL-7 in their new OSes with an EAL-7 separation kernel that should be certifiable. None, however, are available today.

So until the availability of an EAL-7 OS, what should the military do? Wait and, in the meantime, select a proprietary OS and be tied to a single vendor? Unfortunately, the military has painstakingly realized that being tied to a single OS can be cost prohibitive and lead to long product delays because applications cannot be easily ported among incompatible proprietary OSes. Therefore, the military is trying to reduce costs and improve time to deployment through “spiral development” and the use of open

standards. With Linux, the military can choose from multiple vendors whose products are compatible.

Most importantly, since Linux uses open standards and is POSIX-based, it can be used in an EAL-7 environment by having the Linux OS run in a secure partition on an EAL-7-certified kernel. To achieve this, a Linux application could be isolated from other applications, and data and information control would be managed by the EAL-7-certified kernel. This separation is extremely important because the key element in security is keeping unauthorized people from viewing information that they don’t have security privileges to access. If Linux is running in a partition of an EAL-7-certified kernel, it could be completely isolated from all other applications running in other partitions on the same certified kernel.

Vendors will always try to get an unfair advantage if allowed. The military has smartly decided to move away from proprietary solutions and toward open standards so that future hardware and software upgrades can be made seamlessly. Also, open standards require vendors to be competitive in their offerings. As a result, Linux is seen as a threat to proprietary OS vendors because it will jeopardize their profits, not our military’s ability to fight. Linux will work in a secure network-centric battlefield and LynuxWorks is one of the vendors that will provide the tools to make that happen. ■■

LynuxWorks  
San Jose, CA.  
(408) 979-3900.  
[www.lynuxworks.com].

From the Editor's files



*The controversy surrounding the use of Linux in military applications is heating up. Here are several points of view from companies in-the-know.*

*COTS Journal encourages and will continue to air meaningful opposing points of view.*

*—Ed.*