

Hardware Virtualization puts a new spin on Secure Systems

Real-time determinism and military security don't have to be separate realities. A combination of a secure separation kernel and an embedded hypervisor enables whole new levels of system security.



Author: Robert Day, LynuxWorks, Inc.

As more military embedded systems get connected to the outside world, particularly to the open Internet, the more vulnerable they become to the seemingly unstoppable waves of cyber attacks. Gone are the days of dedicated and discrete embedded systems, and in their place the embedded systems look more and more like the PCs and workstations that sit in our offices and homes, which in turn means that the software that runs on these devices will need similar characteristics to desktop systems.

There are two serious issues with this trend. The traditional desktop operating systems, software stacks and applications are not built with either real-time performance or security in mind, and are now being used in systems that require the determinism of a Real-Time Operating System (RTOS). And when they are connected to outside world, they need protection from cyber attack that has plainly been lacking in our desktop world.

A possible solution to these issues is to use an embedded version of a desktop OS, like embedded Linux® or Windows® CE. However, although both are more real-time and possibly more secure than their desktop counterparts, neither have been built with either real-time determinism or military security in mind, and only go so far to solving these issues. An interesting, elegant and ultimately more suitable solution is to use the combina-

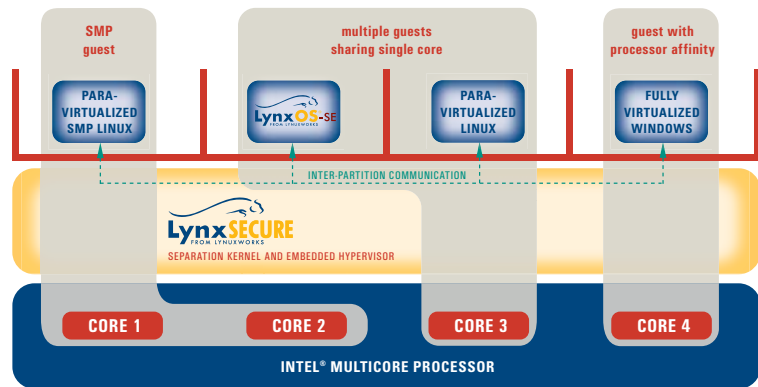


Figure 1: Multicore processors, which often also have hardware virtualization support, are the best way to maintain near-native performance of all of the secure domains.

tion of a secure separation kernel and an embedded hypervisor combined with today's modern multicore processors.

Separation-Kernel Technology

The separation kernel is a technology developed for use in secure military systems that provides an underlying real-time platform with multiple secure domains housing software applications that cannot interfere with each other. When combined with an embedded hypervisor, each of the domains can securely host different "guest" operating systems and the applications that they support. This secure virtualization system provides security and trust by containing the operating systems and applications from

one another and enforcing strict security policies with any desired communication between the domains.

Because the underlying separation kernel has real-time scheduling policies, real-time applications and operating systems can run in a domain providing the performance normally offered by an RTOS. The desktop functionality and connection to the outside world can be hosted in another domain, using a more traditional desktop OS like Windows or Linux. Any cyber attacks will be contained to this domain and cannot spread to the critical functions or hamper the performance of the real-time domain. Also, because the desktop operating system is being run in

a virtual environment, any contamination is not just contained, but it can also be cleaned up by either rebooting or re-provisioning the desktop system without stopping or resetting the real-time part of the system.

Leveraging Multicore Processors

Software virtualization can be used across single-core processors, but when running larger desktop operating systems that are used to having full control of a processor, multicore parts that often also have hardware virtualization support are the best way to maintain near-native performance of all of the secure domains (Figure 1). The LynxSecure separation kernel and hypervisor from LynuxWorks™ offers support for both real-time and desktop guest operating systems and supports multicore Intel® processors with hardware virtualization, and gives a secure foundation for building trusted embedded systems.

An example program using this separation kernel and hypervisor technology is the U.S. Navy's Common Display System (CDS). CDS is a survivable and configurable high-assurance workstation providing an operator access to multiple shipboard applications simultaneously. This family of console displays is to be integrated into the ships that comprise the DDG 1000 Zumwalt class of next-generation destroyers (Figure 2) as well as the modernization of the Aegis class of guided missile destroyers. The CDS project is part of the U.S. Navy Open Architecture Computing Environment initiative.

In the CDS, LynxSecure provides an environment in which multiple guest



Figure 2: The Common Display System (CDS) aboard the DDG 1000 Zumwalt class of next-generation destroyers will make use of virtualization using separation kernel and hypervisor technology.

operating systems running at different security levels (Secret, Top Secret and Unclassified) execute at the same time without compromising security, reliability or data integrity. This is critical because military systems such as the CDS display console system require adherence to rigid high-assurance security requirements. Program plans include evaluation of LynxSecure to EAL-7 per the Common Criteria and the Separation Kernel Protection Profile (SKPP).



Robert Day is Vice President, Marketing at LynuxWorks, Inc. and has more than 20 years of experience in the embedded industry. Based in San José, California, Robert is a graduate of the University of Brighton, England, where he earned a Bachelor of Science degree in computer science.



1.800.255.5969



LynuxWorks, Inc.
855 Embedded Way
San José, CA 95138-1018
408.979.3900
408.979.3920 fax
www.lynuxworks.com

LynuxWorks Europe
50 Broadway
London SW1H 0RG
United Kingdom
+44 208 906 9506
+44 208 906 2338 fax

©2011 LynuxWorks, Inc. LynuxWorks and the LynuxWorks logo are trademarks, and LynxOS is a registered trademark of LynuxWorks, Inc. Linux is a registered trademark of Linus Torvalds. All other trademarks are the trademarks and registered trademarks of their respective owners.

All rights reserved. Printed in the USA.