LynxSecure

Software security driven by an embedded hypervisor

With the introduction of the LynxSecure separation kernel and embedded hypervisor, Lynx Software Technologies once again raises the bar when it comes to superior embedded software security and safety.

Highest standards for safety- and security-critical applications

The military and avionics industries rigidly mandate high security for safety-critical software environments, operating systems and development tools. Meanwhile, military networks increasingly need to interface with the civilian IT infrastructure, exposing them to program bugs, design flaws and other vulnerabilities.

LynxSecure addresses this issue on all fronts by providing a robust environment within which multiple secure and nonsecure operating systems can perform simultaneously—with no compromise of security, reliability or data.

LynxSecure expands on the proven real-time capabilities of the LynxOS® real-time operating system (RTOS) with time-space partitioning and operating-system virtualization.

The LynxSecure separation kernel is a robust virtual machine monitor that is certifiable to (a) Common Criteria EAL-7 security certifi cation (Evaluated Assurance Level 7), which is a level of certifi cation unattained by any known operating system to date; and (b) DO-178B level A, the highest level of FAA certifi cation for safety-critical avionics applications.

MILS architecture conformance for building secure systems

LynxSecure conforms to the Multiple Independent Levels of Security/Safety (MILS) architecture, with strict adherence to data isolation, damage limitation and information-flow policies identified in this architecture. Unlike a traditional security kernel that performs all trusted functions for a secure operating system, a separation kernel's primary security function is to partition data and resources of a system and to control information flow between partitions.

Partitions and information-flow policies are defined by the kernel's configuration. This provides a robust foundation for the creation of multi-level secure systems.

Virtualization of guest operating systems

The use of hypervisors and virtualization technology allows one operating system (and its applications) to run within the environment of another kernel, in effect allowing multiple dissimilar operating systems to share a single physical hardware platform. Virtualization technology allows for significant cost savings through hardware consolidation, while retaining the ability to leverage the ecosystem of applications that belong to different operating system domains into a single system.

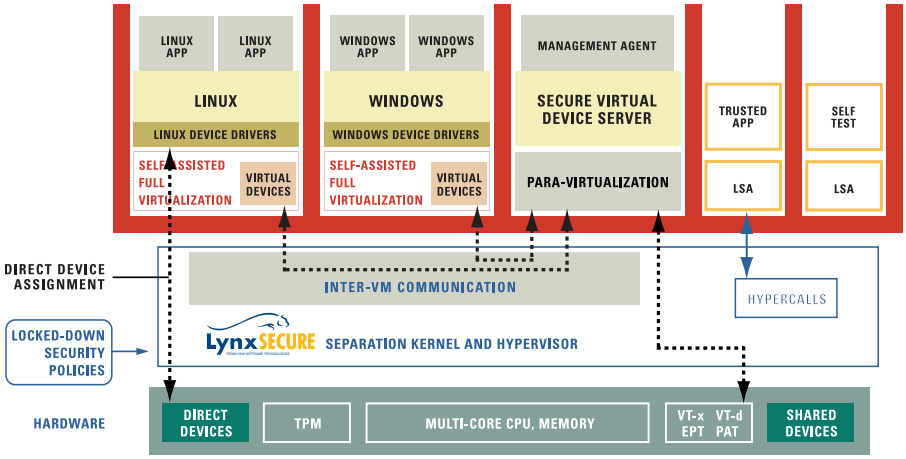
To achieve virtualization, LynxSecure uses a hypervisor to create a virtualization layer that maps physical system resources to each guest operating system. Each guest operating system is assigned certain dedicated resources, such as memory, CPU time and I/O peripherals. "Co-operative virtualization" provides superior performance for the guest operating systems—such as Linux®, LynxOS-SE and LynxOS-178.

LynxSecure Advantages

- Optimal security and safety—the only operating system designed to support both CC EAL-7 and DO-178B level A
- Real time—time-space partitioned separation kernel for superior determinism and performance
- Hypervisor and virtualization technology—supports multiple heterogeneous operating system environments on the same physical hardware including Intel® VT
- Highly scalable—supports Symmetric MultiProcessing (SMP) and 64-bit addressing for high-end scalability
- Support for open standards—100% binary compatibility for Linux or POSIX-based software applications allows them to migrate to a highly robust, secure environment
- Faster time to market—enables developers to begin early development for secure applications

LYNX SOFTWARE TECHNOLOGIES

100% application binary-compatibility with the non-virtualized instance of the operating system is preserved. LynxSecure isolates each virtual instance by providing hardware protection to every partition with its own virtual addressing space. In addition, it guarantees resource availability, such as memory and processor-execution resources, to each partition, so that no software can fully consume the scheduled memory or time resources of other partitions. LynxSecure supports simultaneous use of system interfaces, including multiple instances of the same or different operating systems in different partitions.



Flexible scheduling policy

LynxSecure's fixed-cyclic ARINC 653-based scheduler manages CPU time to prevent starvation in any partition. LynxSecure also allows dynamic scheduling policies to maintain maximum flexibility in developing diverse secure applications using OS virtualization.

Highly scalable technology

LynxSecure provides a scalable solution ranging from deeply embedded systems to high-end workstations and servers for the design of applications in embedded avionics products, weapons systems, C4ISR data systems as well as critical infrastructure control systems.

The LynxSecure separation kernel provides the essential components for a complete scalable, multithreaded and secure architecture:

- multithreaded small-footprint run-time environment for secure application development
- multiprocess, multithreaded environment through virtualized Red Hat®, Linux, LynxOS or LynxOS-SE operating systems
- symmetric multiprocessing (SMP) for optimal resource utilization and load balancing
- Microsoft® Windows® support in full virtualization mode
- high-end scalability and memory support through 64-bit execution mode and addressing capabilities

Support for open standards

Like all Lynx Software Technologies operating systems, LynxSecure is based on open standards. LynxSecure provides a seamless migration path for Lynx Software Technologies customers whose Linux and POSIX®-based applications can now run on virtualized Red Hat Linux, and LynxOS family environments within LynxSecure partitions.

The LynxSecure separation kernel provides a high-assurance run-time environment: a small-footprint flexible API based on open standards (POSIX), that allows for the development and certification of secure applications to CC EAL-7.

1.800.255.5969

Lynx Software Technologies, Inc.
855 Embedded Way
San José, CA 95138-1018
408.979.3900
408.979.3920 fax
inside@lynx.com
www.lynx.com

Lynx Software Technologies UK
400 Thames Valley Park Drive
Thames Valley Park
Reading, RG6 1PT
United Kingdom
+44 208 906 9506
+44 208 906 2338 fax
inside@lynx.com

Lynx Software Technologies Europe
38 Avenue Pierre Curie
78210 Saint-Cyr-l'École
France
(33) 1 30 85 06 00
(33) 1 30 85 06 06 fax
inside@lynx.com

©2012 Lynx Software Technologies, Inc. Lynx Software Technologies and the Lynx Software Technologies logo are trademarks, and LynxOS and BlueCat are registered trademarks of Lynx Software Technologies, 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.