LynxSECURE

Separation Kernel Hypervisor offering military-grade security & aviation-grade safety

Arm v8-A & Intel® 64

LynxSecure is a real-time development platform that leverages multi-core CPU hardware virtualization features to enhance OEM embedded solutions with accelerated performance and security property enforcement.

It is primarily targeted to raise the assurance of systems that perform critical computing functions in regulated environments. Common use cases include; separating critical apps from internet omains, isolating security functions from application domains, verifying and filtering inter domain communication. LynxSecure lives underneath applications and operating systems, runs completely transparent and cannot be tampered with. The software can be embedded into a broad class of devices from embedded to IT platforms.

The technology was designed to satisfy high assurance computing requirements in support of the NIST, NSA Common Criteria, and NERC CIP evaluation processes which are used to regulate military and industrial computing environments.
Key markets include:

- Industrial
- Automotive
- Medical
- Defense
- Aerospace
- Cyber

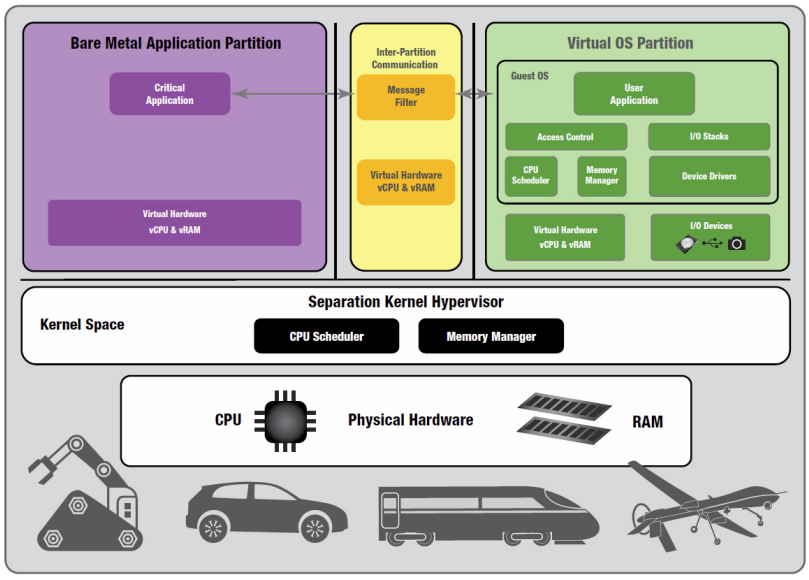

Figure 1: Platform integrity through isolated domains

Platform Integrity with LynxSecure

The LynxSecure SDK offers advanced resource, scheduling, and security controls that exceed traditional operating systems and micro-kernel offerings. These granular controls allow developers to explicitly define how a computing platform executes with traceable evidence from specification to instantiation, establishing platform integrity for the following design patterns:

- Safety & Security Domain Isolation
- Trusted Execution Environments
- Reference Monitor Plug-ins
- E.g. Firewalls, IDS, Encryption, Guards

Network Integrity with LSA.connect

LSA.connect is a LynxSecure SDK expansion that allows developers to create computing devices with multiple independent cryptographic channels that can tunnel over a common IP network and create nested encrypted enclaves. The expansion includes cryptographic modules that can be layered inbetween network interfaces to encrypt data in motion generated by applications before exposing the data to public network interfaces. The LSA.connect components remain transparent to applications and are interoperable with any LynxSecure supported guest operating system, and works with any IP supported network interface. LynxSecure protects the crypto modules from exposed network interfaces or internal application domains, providing an architecture vastly superior to kernel integrated software VPNs that can be bypassed by malware or users. LSA.connect provides robust network integrity between a wide range of devices from IT infrastructure to OT process controllers running in safety critical environments.

LynxSecure Advantages

- **Safety and Security Application Partitioning**
- **Trusted Application Protection**
- **Multi-channel Network Isolation**
- **Multi-core Processing**
- **Hardware Virtualization Support**
- **Platform Consolidation**
- **Real-time Execution Control**
- **High Assurance Safety and Security Certification Design Artifact Support**

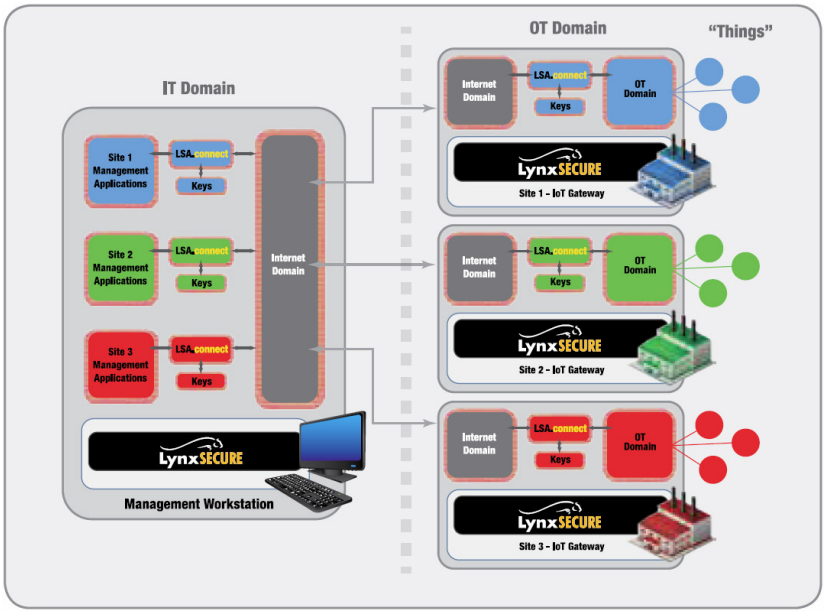

Figure 2: Network integrity using multi-channel secure communications

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, automotive systems, and critical infrastructure control systems.

Virtualization of guest operating systems

The use of hypervisors and virtualization technology allows multiple types of 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 platform.

Least privilege architecture for building secure systems

LynxSecure upholds the principles of least privilege featuring limited kernel space functionality, lightweight simple design, and explicit granular authorization of all system control functions. Unlike traditional OS and hypervisor kernels that include drivers, I/O stacks, and application APIs, the LynxSecure separation kernel exports all I/O and application support in user space. Instead LynxSecure limits its kernel space functionality to resource partitioning, controlling data flow between partitions, and mediate access to system state change functions. This provides a robust foundation for the development of high assurance systems.

The LynxSecure separation kernel provides the foundational safety and security properties to host scalable, high performance, and completely secure architectures.

Kernel:

- Isolate memory
- Isolate DMA & I/O interfaces
- Isolate privileged CPU instructions
- Isolate TPM interface
- Isolate storage interfaces
- Isolate application space from system service space
- Isolate system service space from kernel space
- Monitor inter VM/vCPU communication
- Monitor system Start/Stop/Restart services
- Support custom shared memory interfaces
- Support Multi-core, SMP, AMP processing
- Support real-time CPU scheduling
- Support I/O device sharing
- Full Virtualization Support – Eg. Windows, Linux, LynxOS

SDK:

- Define virtual machines – CPUs, schedules, memory, I/O interfaces
- Define virtual machine communication permissions
- Provide bare-metal libraries for system service and Inter-VM communications
- Provide Linux drivers for accelerated communication and message interfaces for Linux guest VMs
- Optional bare-metal crypto modules for virtual in-line encryption network and storage services

Supported Architectures

LynxSecure is available for:

- **Intel 64 architecture supporting Xeon®, Core™, and Atom® processors**
- **Arm v8-A architecture supporting reference SoCs from Xilinx and NXP**

LYNX SOFTWARE TECHNOLOGIES

1.800.255.5969

Lynx Software Technologies, Inc.
855 Embedded Way
San Jose, CA 95138-1018
+1 (800) 255-5969
+1 (408) 979-3900
+1 (408) 9793-920 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 (0) 118 965 3827
+44 (0) 118 965 3840 fax

Lynx Software Technologies France
38 Avenue Pierre Curie
78210 Saint-Cyr-l'École
France
+33 (0) 1 30 85 06 00
+33 (0) 130 85 06 06 fax