LYNX
SOFTWARE TECHNOLOGIES

The Opportunity For Unikernels In Mission Critical Systems

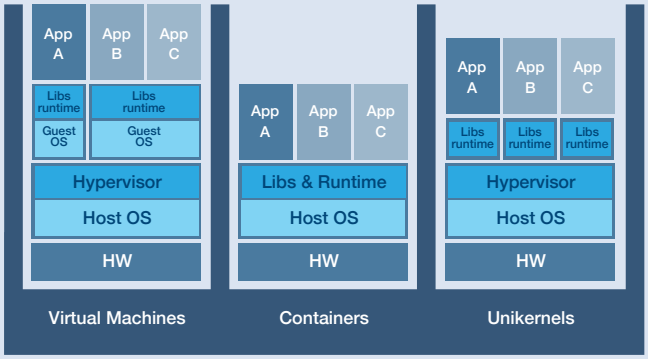
Background

Virtualization technology, whereby multiple operating systems can be run on shared hardware, is extremely well understood if somewhat inefficient in its use of resources. Just a few decades ago, everyone used virtual machines (VM) to host and manage the infrastructure. More recently, industries have shifted towards using containers and their associated infrastructure, including such as Docker and Kubernetes.

Containers try to achieve the same concept as virtual machines but eliminate duplication of effort between machines. Containers are easy to run on development machines and the deployment process itself is also much simpler since one just uploads pre-built containers to a container repository and production systems can pull the updated version. The container-based approach has its downsides. The software has to be adapted for usage in containers (containerized), and this can get tricky, especially with legacy codebases. Containers have many more configurations for resource allocation and interoperability capabilities, so it is quite easy to misconfigure them.

The next logical step in the progression from VMs to containers is unikernels, which try to push the concepts of containers even further.

Unikernels are effectively a set of pre-built binary libraries. Unikernels do not handle resource allocation. The hypervisor handles direct hardware interoperation. The unikernel architecture concept aims to deliver the security strengths of VM level partitioning with the speed and footprint size benefits attributed to containers. While this diagram shows a general approach, the use of the LynxSecure Separation Kernel hypervisor removes use of an underlying HostOS, a proven point of vulnerability.



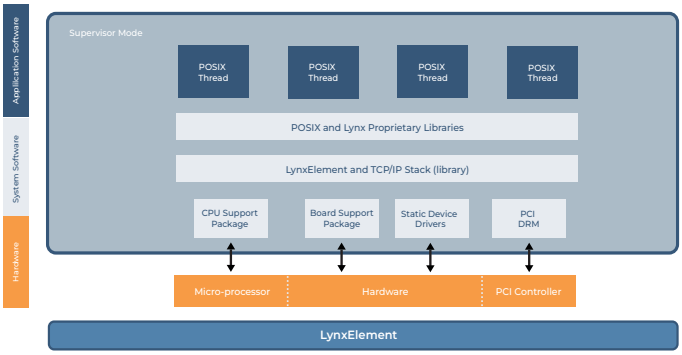
Unikernels have even less overhead than containers and are more streamlined giving the potential for enhanced performance. Furthermore, by eliminating the use of a multi-user, multiple address space kernel, security is drastically improved.

Unikernels are not new. There are, however, a number of issues associated with unikernels which have limited their applications until now. These include;

- Debugging. Since a unikernel has no OS running whatsoever, the approach of directly connecting to its shell and investigating does not work
- Producing unikernel images is complicated and requires deep knowledge on the subject
- Current application frameworks have to adapt and produce documentation on usage in unikernels
- The lack of a safety certifiable/certified unikernel for mission critical applications

Introducing LynxElement™; The unikernel from Lynx Software Technologies

Lynx has taken the approach of basing its unikernel product, LynxElement, on its commercially proven LynxOS-178 real time operating system. There is a focus on maintaining compatibility wherever possible between the unikernel and the standalone LynxOS-178 product to enable customers to freely transport applications between each environment. More specifically FACE and POSIX APIs are supported.



LynxElement runs on LynxSecure. Multiple unikernels can share a CPU core. All applications run in user mode. This is a major advantage when compared to operating systems that use kernel mode. Kernel mode (also referred to as privileged mode) provides a program direct and unrestricted access to all system resources. Software in user mode is is not allowed to access system resources directly. The Lynx filesystem, LynxFS, is supported. It also includes a thread-based scheduler, more specifically a priority-preemptive scheduler with POSIX semantics. Floating point is supported in the unikernel.

The networking stack for LynxElement supports two types of drivers

- Drivers for physical devices (Serial, Ethernet)
- Virtual drivers for serial ports and Ethernet

As mentioned previously, the driver model is compatible with LynxOS-178, which enables driver APIs to be preserved. There is no dynamic device driver support. This eliminates it as an attack vector. Instead, all drivers are linked statically.

LynxElement is initially offered for Intel and Arm architectures.

From an application development perspective, Lynx provides a Linux-based cross development that incorporates a GCC 11 compiler. C/C++ run-times are supported, with uClibC++ as the C++ run-time support.

LynxElement is provided as part of the LYNX MOSA.ic portfolio of products.

Example Use Case

The initial interest for LynxElement is centered on security since

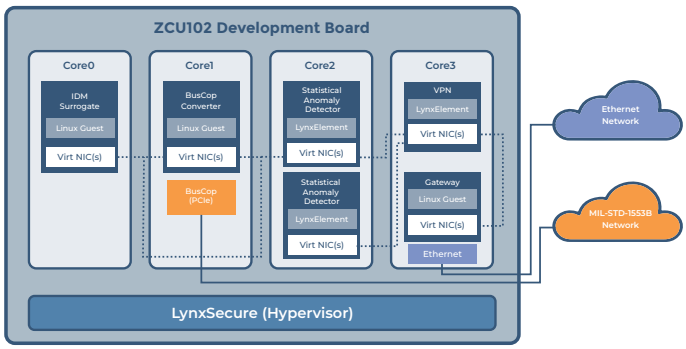
a) This approach drastically reduces the attack surface

b) These types of applications do not demand guaranteed timing requirements and safety certification artifacts

As an example, LynxElement can be used to run security components like IDS and VPNs. Statistical anomaly detectors can be deployed by an Enterprise on networks to monitor IP and 1553 traffic. Use of a data diode and filter on the unikernel would enable a customer to replace a Linux VM, which saves memory space and drastically reduces the attack space.

Summary

Lynx certainly believes that we are entering the time where



unikernels are ready for broader deployment. Lynx's announcement of LynxElement the industry's first commercial unikernel, provides for compatibility with POSIX interfaces and is founded on technology with a proven safety pedigree. Ultimately this means cost and project risk reductions for systems that need to be taken through certification standards such as DO-178C DALA, ISO26262 and IEC61508.

This technology offers a number of benefits to customers including

- Increased system density
- Improved performance
- Better security
- Smaller memory footprint

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