seL4 Microkernel Solutions

Engineering Design Services

Extreme security is reachable

Many product developers want strong security in their products, but get stressed about implementing it when technology is added to the system. DornerWorks provides guidance on your product with seL4 and safety/security so you understand/prevent risks.

DornerWorks has won a Small Business Innovation Research (SBIR) contract, from US DARPA, to fund development around seL4. With this contract, DornerWorks has expanded the seL4 ecosystem with new tools, like GDB support on ARM, and with new drivers, like Ethernet on the Xilinx ZC702 development board. DornerWorks is looking for more opportunities to add to this ecosystem to simplify development around seL4.

Get your freedom in 3 Easy Steps:

1. *Discuss:* Schedule a discussion with our engineering team
2. *Develop:* We'll collaborate with you to create your product
3. *Deliver:* We'll work with you to launch your product to market

With DornerWorks and seL4, You get:

- A Quick Start Package is available so that you can get started quickly on your standout product solution
- With our proven expertise in seL4 and CAmkES we'll customize your seL4 solution to give you innovative and high-quality results, including for such things as:
  - New drivers
  - Porting to new platforms
  - CAmkES configuration
  - Application development
- We're a US-based company with an experienced and consistent staff so you can develop your solution with us without worry of export controls
- We provide a customer-focused approach to guide your project towards safety or security certifications

seL4 Applications

- Since seL4 is formally proven, it lends itself well to be used for the following security based applications:
  - Security Gateways
  - Secure Mobile OS
  - Secure embedded OS
- seL4 has a Virtual Machine Manager (VMM) mode and has proven isolation, so it is great for the following applications:
  - Virtualization Solutions
- Others…

Call us to learn more

technology engineering so you can focus

write sales@dornerworks.com
call 616-245-8369
click www.dornerworks.com

3445 Lake Eastbrook Blvd SE
Grand Rapids, MI 49546
USA

seL4 Background

Security and Safety-Critical Systems

seL4 is an open source, formally verified microkernel that is a member of the L4 family of high-performance microkernels. The seL4 verification uses a formal mathematical proof that is a full code-level correctness proof. This proof is used in the theorem prover Isabell/HOL to prove the correctness of the code. All this means that the implementation is proved to be bug-free, in other words, the kernel level code is free from buffer overflows, null pointer exceptions, use-after-free, etc. There is another proof that shows that the binary code is a correct translation of the source code. Your system is not automatically safe and secure by using seL4, but the proof can be used to ease both safety and security certifications.

Small Size

seL4 has a very small footprint of ~8,700 lines of C code and ~600 lines of assembly code. This is because the seL4 microkernel has an intentionally limited feature set. Most typical OS features are delegated to user-mode applications, including device drivers, network protocol stack, and file systems. These applications are granted privileges to interact with the devices and features based on passed capabilities.

Specifics

- Supports ARM Cortex-A8, A9, A15 & A53 processors
- Supports Intel x86 and x64 platforms
- Model based development framework, CAmkES
- VMM mode to virtualize Guest Operating Systems

seL4
Security. Performance. Proof.

seL4 Microkernel Solutions

Virtualized Driver

A customer had a virtualized environment using seL4 as the VMM. They were running Linux VMs with built-in ramdisks for file systems, but needed persistent storage. They knew they could give a single VM direct access to the hard disk, but that creates a problem when more than a single VM needs persistent storage. The customer knew that an alternative method would be difficult, but they needed some extra help and guidance. DornerWorks was able to provide a solution with our expertise in seL4 and CAmkES:

- Added a new driver to camkes-vm to allow access from Virtual Machines (VM) to partitions on a hard drive.
- Software development
    - Low-Level IDE driver for x86 platform
    - Virtualized partitions
    - Virtio-blk driver to communicate with Linux VMs
    - Configured via CAmkES
    - Modifications to Linux VM configurations

For more information:
seL4.world

DORNERWORKS
technology engineering so you can focus

write sales@dornerworks.com
call 616-245-8369
click www.dornerworks.com

3445 Lake Eastbrook Blvd SE
Grand Rapids, MI 49546
USA