Many Remote Attack Vectors

Physical

Short-Range Wireless

Long-Range Wireless

Entertainment

SCADA Systems

Source: Laing O'Rourke

Source: Dept. of Energy

Medical Devices

Source: www.seekingalpha.com

Source: www.medtechbusiness.com

Computer Peripherals

Source: HP

Source: www.buy.com

Source: www.bagit.com

Distribution Statement A - Approved for Public Release, Distribution Unlimited
Control Systems
Air gaps & obscurity

Forget the myth of the air gap – the control system that is completely isolated is history.
-- Stefan Woronka, 2011
Siemens Director of Industrial Security Services

Cyber Systems

• Anti-virus scanning, intrusion detection systems, patching infrastructure
This approach cannot solve the problem.
  • Not convergent with the threat
  • Focused on known vulnerabilities; can miss zero-day exploits
  • Can introduce new vulnerabilities and privilege escalation opportunities

Trying to adopt cyber approaches, but technology is not a good fit:
  • Resource constraints, real-time deadlines
  • Extreme cost pressures
  • Patches may have to go through lengthy verification & validation processes
  • Patches could require recalls

We need a fundamentally different approach

1/3 of the vulnerabilities are in security software!
Cyber Resilient Embedded Systems

The HACMS program created technology for the construction of high-assurance cyber-physical systems

Cyber-physical systems are relatively easy to remotely take over and reprogram using cyber attacks.

Capability Objectives:
- High-assurance operating systems and control systems
- Suite of program synthesizers and formal-methods tools
- Assured-integration tools and analysis workbench

Accomplishments:
- High assurance components ported to ULB and US Army TARDEC Autonomous Mobility Appliqué System Joint Capability Technology Demonstration (AMAS JCTD)
- Red Team completed end-of-phase III assessments; no security flaws in demonstration platforms after full access to code

SAE is developing a Formal Methods Academy to transition HACMS technologies to the automotive industry
HACMS Program Structure

**Architectural-Level**
Rockwell Collins, University of Minnesota
Compositional Reasoning

**Application-Level Software**
Galois, CMU, Draper Labs, MIT, Oxford, Princeton, SpiralGen, University of Illinois, University of Pennsylvania
Generate from Specification, Correct by Construction, Software Verification, Robust Algorithms

**Low-Level Software**
Data61 (NICTA), Yale
Verified OS Kernels

**Ground Vehicle**
HRL
Integrate on TARDEC Autonomous Systems

**Air Vehicle**
Boeing
Integrate on Unmanned Little Bird

**Penetration Testing**
AIS

Distribution Statement A - Approved for Public Release, Distribution Unlimited
HACMS cyber retrofit

- Several prototypes of securing existing systems developed using this approach
- Host existing software load image in a seL4 virtual machine
- Study software architecture and partition into a set of virtual machines
- Determine which virtual machines need guest operating system services
- Re-implement security critical software components

Leveraging proven seL4 protections to maintain integrity of the virtual machines
seL4 ecosystem SBIR effort

Build out the open-source ecosystem of secure software components around the seL4 operating system microkernel

- Develop US-based expertise in supporting seL4
- Develop high assurance components for seL4
- Demonstrate prototype seL4-based systems
- Remove roadblocks form seL4 adoption
seL4 SBIR highlights

• Syracuse Assured Boat Loader Executive (SABLE) adapted to seL4
• Genode application framework ported to seL4
• Real-time profile of DDS ported to seL4
• Multi-level secure helmet vision system prototype
• Formally verified network stack
• RISC-V (Draper ISP) implementation
seL4 Community of Excellence

- Provide stable US-based releases of seL4 system
- Deliver US-based support to integrators using seL4
- Deliver training to seL4 users
- Manage a seL4 technology roadmap

Mimic Linux distribution model. Make seL4 a viable candidate technology for use on high-integrity systems