Formal Verification of a Tiny Separation Kernel

Oliver Schwarz
oliver@sics.se

To watch the animated prezi-presentation, please follow this link:

Formal Verification of a Tiny Separation Kernel

speaker: Oliver Schwarz

Oliver@sics.se
"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrified weak that NSA can frequently find ways around it."

-- Edward Snowden
keep critical software isolated
paravirtualized

Separation Kernel

ARM v7
(without virtualization support)
Formal Verification of a Tiny Separation Kernel

Intro

Conclusion

School

More

Verification
Imagine you were the manager of a catholic school who wants to separate boys and girls...

There are a couple of things to think about ...
access control
cleaning up when switching contexts
hide management data
every difference leaks

- delaying the teacher
- changing the teachers mood
interference

- Angry boys
  - Angry teacher
    - Suffering girls
- No class
  - Relaxed teacher
    - Lucky girls
non-interference

- angry boys
  - angry teacher
    - relaxed teacher
      - relaxed teacher
        - lucky girls
  - no class
    - relaxed teacher
      - relaxed teacher
        - lucky girls
Formal Verification of a Tiny Separation Kernel
Partitions should be physically indistinguishable from distributed systems. (1981)

John Rushby
system to be verified

guest 1
message handler
send
buffer
release

guest 2
message handler

Hypervisor

ARM v7 MMU

lifter

3

1

2
Binary Analysis Platform

- check \{pre\} code \{post\}
  - lift binary
  - compute weakest precondition
  - check \text{pre}(v) \rightarrow \text{wp (code, post(v))} for all bitvectors v
    [using SAT solver]
- discover counterexample
H O L

- interactive theorem prover
- open source
- based on Standard ML
- Cambridge ARM model
  (monadic operational semantics)
- enhanced by MMU
Security during user mode execution
Non-Exfiltration

mem [ P | Am | Im ]
reg [ Ar | Ir ]
...

mem [ P | Am' | Im ]
reg [ Ar' | Ir ]
...
Non-Infiltration

mem [ P | Am | . ]
reg [ Ar | . ]
...

mem [ P | Am' | . ]
reg [ Ar' | . ]
...

mem [ P | Am | . ]
reg [ Ar | . ]
...

mem [ P | Am' | . ]
reg [ Ar' | . ]
...
restoring of control flags

bugs found

determining last guest instruction
Formal Verification of a Tiny Separation Kernel

Intro

Conclusion

More

Verification

School
more: timing

remember the tactic of delaying the teacher?

That can be an issue in our setting as well!
more: functionality

run Linux with dynamic memory management
more: devices

DMA devices in a context of secure virtualization
even more

soft reboot

cortex M separation kernel

secure boot

platform support
Formal Verification of a Tiny Separation Kernel

Intro

Conclusion

More

Verification

School
The Provably Secure Execution Platforms for Embedded Systems (PROSPER) project aims to build the next generation framework for fully verified, secure hypervisors for embedded systems. It thus focuses on:

- **Isolation through Virtualization**
  One of our central assets is our hypervisor, a provably secure execution platform for embedded devices (such as mobile phones) based on a virtualization core. The hypervisor supports Linux as a guest and is available as open source.

- **Formal Verification**
  We developed a prototype toolset for formal specification and verification of different versions of the hypervisor, within the context of an ARM architecture.

This project is funded by the Swedish Foundation for Strategic Research (Stiftelsen för Strategisk Forskning - SSF).

---

**SICS Security Seminar**

In this year’s security seminar at SICS (“Securing infrastructures, the Smart GRID and the Things”), Kista, 8th of April 2014) Oliver Schwarz will talk about formal verification within the PROSPER project.

**PROSPER in media**

In the context of a *Crosstalks* debate Mads Dam talked with KTH News about our project. Subsequently, Elektroniktidningen, IDG and others reported about PROSPER.

**Verification talk online**

On February 28th Mads Dam was invited to speak at the *Inova* seminar *"méthodes formelles et sécurité"* in Rennes, France. The 1-hour talk with the title "Formal verification of information flow security for a simple ARM-based separation kernel" is available online.
Read about it ...

**Formal Verification of Information Flow Security for a Simple ARM-Based Separation Kernel**
Mads Dam, Roberto Guanciale, Narges Khakpour, Hamed Nemati and Oliver Schwarz
ACM Conference on Computer & Communications Security (CCS’13).

**Machine Assisted Proof of ARMv7 Instruction Level Isolation Properties**
Narges Khakpour, Oliver Schwarz and Mads Dam
Certified Programs and proofs (CPP’13).

**Machine Code Verification of a Tiny ARM Hypervisor**
Mads Dam, Roberto Guanciale, Hamed Nemati
TrustED 2013.
Formal Verification of a Tiny Separation Kernel

1. Binary level
2. Communication
3. Bisimulation
4. Incl. system

Conclusion

More

Verification

Intro

School

Oliver@sicss.se