2022 T2 Week 10 Part 1

Formal Verification and seL4

@GernotHeiser
Copyright Notice

These slides are distributed under the Creative Commons Attribution 4.0 International (CC BY 4.0) License

• You are free:
  • to share—to copy, distribute and transmit the work
  • to remix—to adapt the work

• under the following conditions:
  • Attribution: You must attribute the work (but not in any way that suggests that the author endorses you or your use of the work) as follows:
    “Courtesy of Gernot Heiser, UNSW Sydney”

The complete license text can be found at http://creativecommons.org/licenses/by/4.0/legalcode
Today’s Lecture

• Assurance and verification
  • Common Criteria
  • Formal verification

• seL4
  • Functional correctness
  • Translation correctness
  • Security enforcement
  • Verification limitations
  • WCET analysis
  • Cost of verification

• Security impact of OS design
Assurance and Verification
Refresher: Assurance and Formal Verification

• **Assurance:**
  • systematic evaluation and testing
  • essentially an intensive and onerous form of quality assurance

• **Formal verification:**
  • mathematical proof

• **Certification:** independent examination
  • confirming that the assurance or verification was done right
Assurance: Substantiating Trust

• Specification
  • Unambiguous description of desired behaviour

• System design
  • Justification that it meets specification

• Implementation
  • Justification that it implements the design

• Maintenance
  • Justifies that system use meets assumptions

Informal (English) or formal (maths)
Compelling argument or formal proof
Code inspection, rigorous testing, proof
Common Criteria

• **Common Criteria for IT Security Evaluation** [ISO/IEC 15408, 99]
  • ISO standard, for general use
  • Evaluates QA used to ensure systems meet their requirements
  • Developed out of the famous US DOD “Orange Book”: *Trusted Computer System Evaluation Criteria* [1985]

• Terminology:
  • **Target of evaluation** (TOE): Evaluated system
  • **Security target** (ST): Defines requirements
  • **Protection profile** (PP): Standardised ST template
  • **Evaluation assurance level** (EAL): Defines thoroughness of evaluation
    • PPs have maximum EAL they can be used for
## CC: Evaluation Assurance Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Requirements</th>
<th>Specification</th>
<th>Design</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAL1</td>
<td>not evaluated</td>
<td>Informal</td>
<td>not eval</td>
<td>not evaluated</td>
</tr>
<tr>
<td>EAL2</td>
<td>not evaluated</td>
<td>Informal</td>
<td>Informal</td>
<td>not evaluated</td>
</tr>
<tr>
<td>EAL3</td>
<td>not evaluated</td>
<td>Informal</td>
<td>Informal</td>
<td>not evaluated</td>
</tr>
<tr>
<td>EAL4</td>
<td>not evaluated</td>
<td>Informal</td>
<td>Informal</td>
<td>not evaluated</td>
</tr>
<tr>
<td>EAL5</td>
<td>not evaluated</td>
<td>Semi-Formal</td>
<td>Semi-Formal</td>
<td>Informal</td>
</tr>
<tr>
<td>EAL6</td>
<td>Formal</td>
<td>Semi-Formal</td>
<td>Semi-Formal</td>
<td>Informal</td>
</tr>
<tr>
<td>EAL7</td>
<td>Formal</td>
<td>Formal</td>
<td>Formal</td>
<td>Informal</td>
</tr>
</tbody>
</table>

**Thoroughness, cost**
Common Criteria: Protection Profiles (PPs)

- **Controlled Access PP** (CAPP)
  - standard OS security, up to EAL3
- **Single Level Operating System PP**
  - superset of CAPP, up to EAL4+
- **Labelled Security PP** (LSPP)
  - MAC for COTS OSes
- **Multi-Level Operating System PP**
  - superset of CAPP, LSPP, up to EAL4+
- **Separation Kernel Protection Profile** (SKPP)
  - strict partitioning, for EAL6-7
COTS OS Certifications

• EAL3:
  • 2010 Mac OS X (10.6)

• EAL4:
  • 2003: Windows 2000
  • 2005: SuSE Enterprise Linux
  • 2006: Solaris 10 (EAL4+)
    • against CAPP (an EAL3 PP!)
  • 2007: Red Hat Linux (EAL4+)

• EAL6:
  • 2008: Green Hills INTEGRITY-178B (EAL6+)
    • against SKPP, relatively simple PPC-based hardware platform in TOE

• EAL7:
  • 2019: Prove & Run PROVENCORE

Get regularly hacked!
SKPP on Commodity Hardware

- SKPP: OS provides only separation
- One Box One Wire (OB1) Project
  - Use INTEGRITY-178B to isolate VMs on commodity desktop hardware
  - Leverage existing INTEGRITY certification
    - by “porting” it to commodity platform

Conclusion [NSA, March 2010]:
- SKPP validation for commodity hardware platforms infeasible due to their complexity
- SKPP has limited relevance for these platforms

NSA subsequently dis-endorsed SKPP, discontinued certifying ≥EAL5
Common Criteria Limitations

- Very expensive
  - rule of thumb: EAL6+ costs $1K/LOC [Green Hills] design-implementation-evaluation-certification
- Too much focus on development process
  - rather than the product that was delivered
- Lower EALs of little practical use for OSes
  - c.f. COTS OS EAL4 certifications
- Commercial Licensed Evaluation Facilities licenses rarely revoked
  - Leads to potential “race to the bottom” [Anderson & Fuloria, 2009]
Formal Verification

• Prove properties about a mathematical model of a system

Model checking / abstract interpretation:
• Systematic exploration of system state space
  - Cannot generally prove code correct
    • Proves specific properties
  - Generally have to
    • over-approximate (false positives), or
    • under-approximate (false negatives, unsound)
  - Suffers state-space explosion
    ✓ Automatic
    ✓ May scale to large code bases

Recent work automatically proved functional correctness of simple systems using SMT solvers [Hyperkernel, SOSP’17]

Theorem proving:
• Proofs about state spaces
  ✓ Can deal with large (even infinite) state spaces
  ✓ Can prove functional correctness against a spec
  ✓ Very labour-intensive
Theorem Proving

“Forward simulation”: Prove state correspondence of abstract and concrete levels

\[ \sigma \rightarrow \sigma' \]

\[ s \rightarrow s' \]

state relation

operation
Model Checking and Linux: A Sad Story

- Static analysis of Linux source [Chou & al, 2001]
  - Found high density of bugs, especially in device drivers
- Re-analysis 10 years later [Palix & al, 2011]

Disappointing rate of improvement for bugs that are automatically detectable!
And the Result?

Unsafe at any clock speed: Linux kernel security needs a rethink

Ars reports from the Linux Security Summit—and finds much work that needs to be done.

J.M. PORUP (UK) - 9/27/2016, 10:57 PM
August 2009

A NICTA bejelentette a világ első, formális módszerekkel igazolt,

New Scientist
Saturday 29/8/2009
Page: 21
Section: General News
Region: National
Type: Magazines Science / Technology
Size: 196.31 sq.cms.
Published: -----S-

The ultimate way to keep your computer safe from harm

FLAWS in the code, or “kernel”, that sits at the heart of modern computers leave them prone to occasional malfunction and vulnerable to attack by worms and viruses. So the development of a secure general-purpose microkernel could pave the just mathematics, and you can reason about them mathematically,” says Klein.

His team formulated a model with more than 200,000 logical steps which allowed them to prove that the program would always behave as its
Crash-Proof Code

Making critical software safer

WILLIAM BULKELEY
May/June 2011
## Proving Security and Safety (Armv6/7)

### Confidentiality
- Isolation properties [ITP’11, S&P’13]
- Functional correctness [SOSP’09]

### Integrity
- Abstract Model
- C Implementation
- Binary code

### Availability
- Still most comprehensive verification

### Exclusions (at present, Armv7):
- Kernel initialisation not yet verified
- MMU & caches modelled abstractly
- Multicore not yet verified
- Covert \textit{timing} channels not precluded

---

2019 ACM SIGOPS Hall-of-Fame Award

1999 ACM SIGOPS Hall-of-Fame Award

Still only verified capability-based OS
Security Is No Excuse For Bad Performance!

Latency (in cycles) of a round-trip cross-address-space IPC on x64

<table>
<thead>
<tr>
<th>Source</th>
<th>seL4</th>
<th>Fiasco.OC</th>
<th>Zircon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mi et al, 2019</td>
<td>986</td>
<td>2717</td>
<td>8157</td>
</tr>
<tr>
<td>seL4.systems, Jul’22</td>
<td>763</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Sources:
- Zeyu Mi, Dingji Li, Zihan Yang, Xinran Wang, Haibo Chen: “SkyBridge: Fast and Secure Inter-Process Communication for Microkernels”, EuroSys, April 2020
- seL4 Performance, [https://sel4.systems/About/Performance/](https://sel4.systems/About/Performance/), accessed 2022-07-31

World’s fastest microkernel!

Within 10% of hardware limit!
Functional Correctness
Proving Functional Correctness

Abstract Model
4.9 kLOC Isabelle

Refinement: all possible implementation behaviours are captured by the model

Executable Model
13 kLOC Isabelle

Proof
117,000 lop

Implementation
5.7 kLOC Haskell

Proof
50,000 lop

Formalised C
(Isabelle)

Cparser

Implementation
8.7 kLOC C

 Formal C Semantics
Functional Correctness Summary

Kinds of properties proved

- Behaviour of C code is fully captured by abstract model
- Behaviour of C code is fully captured by executable model
- Kernel never fails, behaviour is always well-defined
  - assertions never fail
  - will never de-reference null pointer
  - will never access array out of bounds
  - cannot be subverted by misformed input
- All syscalls terminate, reclaiming memory is safe, ...
- Well typed references, aligned objects, kernel always mapped...
- Access control is decidable

Can prove further properties on abstract level!

Bugs found:

- 16 in (shallow) testing
- 460 in verification
  - 150 in spec,
  - 150 in design,
  - 160 in C
Translation Correctness
Binary Verification: Translation Validation

- **C Source** → **Formalised C** via **Formal C Semantics**
- **Compiler** → **Symbol Tables** → **Binary Code**
- **Formalised Binary** → **Graph Language** → **SMT Solver** → **De-compiler**
- **Target of functional correctness proof**

**Proof** steps:
- **Rewrite Rules**
- **SMT Solver**

**Diagram nodes**:
- **Graph Language**
- **Formalised Binary**
- **Graph Language**
- **Formal ISA Spec**
Security Enforcement
Isolation Goes Deep

Kernel data partitioned like user data
To prove:
Low has no write capabilities to High objects
⇒ no action of Low will modify High state
Specifically, kernel does not modify on Low’s behalf!
Availability: Ensuring Resource Access

Strict separation of kernel resources
⇒ Low cannot deny High access to resources

Nothing to do, implied by other properties!
Confidentiality: Control Information Flow

Non-interference proof:
- Evolution of Low does not depend on High state
- Also shows absence of covert storage channels

To prove:
Low has no read capabilities to High objects
⇒ no action will reveal High state to Low
Confidentiality Proof Challenge

Spec
bool a();

Implementation
bool a() {
    return !secret;
}

Solution:
• Remove non-determinism where it affects confidentiality
• Eg: scheduler strictly round-robin

Non-determinism breaks confidentiality under refinement!

Infoflow is very strong property, requiring restrictions rarely met in real world
Limitations
Verification Assumptions

1. Hardware behaves as expected
   • Formalised hardware-software contract (ISA)
   • Hardware implementation free of bugs, Trojans, …

2. Spec matches expectations
   • Can only prove “security” if specify what “security” means
   • Spec may not be what we think it is

3. Proof checker is correct
   • Isabel/HOL checking core that validates proofs against logic

With binary verification do not need to trust C compiler!
Present Verification Limitations

- Not verified boot code
  - Assume it leaves kernel in safe state
- Caches/MMU presently modeled at high level / axiomised
- Not proved any temporal properties
  - Presently not proved scheduler observes priorities, properties needed for RT
  - WCET analysis applies only to dated ARM11/A8 cores
  - No proofs about timing channels (yet)

Present research!
Present Status

32b Arm
- Confid.
- Integrity
- Availab.
  - Proof
  - Abstract Model
    - Proof
    - C
    - Proof
    - Binary

64b x86
- Confid.
- Integrity
- Availab.
  - Proof
  - Abstract Model
    - Proof
    - C
    - Proof
    - Binary

64b RISC-V
- Confid.
- Integrity
- Availab.
  - Proof
  - Abstract Model
    - Proof
    - C
    - Proof
    - Binary

64b Arm in progress
### Common Criteria?

<table>
<thead>
<tr>
<th>EAL Level</th>
<th>Requirements</th>
<th>Specification</th>
<th>Design</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAL1</td>
<td>not evaluated</td>
<td>Informal</td>
<td>not eval</td>
<td>not evaluated</td>
</tr>
<tr>
<td>EAL2</td>
<td>not evaluated</td>
<td>Informal</td>
<td>Informal</td>
<td>not evaluated</td>
</tr>
<tr>
<td>EAL3</td>
<td>not evaluated</td>
<td>Informal</td>
<td>Informal</td>
<td>not evaluated</td>
</tr>
<tr>
<td>EAL4</td>
<td>not evaluated</td>
<td>Informal</td>
<td>Informal</td>
<td>not evaluated</td>
</tr>
<tr>
<td>EAL5</td>
<td>not evaluated</td>
<td>Semi-Formal</td>
<td>Semi-Formal</td>
<td>Informal</td>
</tr>
<tr>
<td>EAL6</td>
<td>Formal</td>
<td>Semi-Formal</td>
<td>Semi-Formal</td>
<td>Informal</td>
</tr>
<tr>
<td>EAL7</td>
<td>Formal</td>
<td>Formal</td>
<td>Formal</td>
<td>Informal</td>
</tr>
<tr>
<td></td>
<td>Formal</td>
<td>Formal</td>
<td>Formal</td>
<td>Formal</td>
</tr>
</tbody>
</table>

**seL4**
WCET Analysis
WCET Analysis

Program binary → Control-flow graph → Micro-architecture model → Analysis tool → Integer linear equations → ILP solver → WCET

Accurate & sound model of pipeline, caches

Challenge: minimise pessimism – establish tight bounds/models

Pessimism!
Loop Bounds & Infeasible Paths

Tight loop bounds and infeasible path refutations infeasible to obtain from binary – lack of semantic information, especially pointer aliasing analysis.

Idea:
• prove on C level
• transfer to binary using translation-validation toolchain

Result: High-assurance & tight bounds!
WCET Analysis on ARM11

WCET presently limited by verification practicalities
- without regard to verification achieved 50 µs
- 10 µs seem achievable
- BCET ~ 1µs
- [Blackham‘11, ‘12] [Sewell’16]

Problem: Latency information no longer published by Arm!

Pessimism mostly due to under-specified hardware
Cost of Verification
## Verification Cost Breakdown

<table>
<thead>
<tr>
<th>Verification</th>
<th>Cost (py)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Haskell design</td>
<td>2</td>
</tr>
<tr>
<td>C implementation</td>
<td>0.15</td>
</tr>
<tr>
<td>Debugging/Testing</td>
<td>0.15</td>
</tr>
<tr>
<td>Abstract spec refinement</td>
<td>8</td>
</tr>
<tr>
<td>Executable spec refinement</td>
<td>3</td>
</tr>
<tr>
<td>Fastpath verification</td>
<td>0.4</td>
</tr>
<tr>
<td>Formal frameworks</td>
<td>9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>24</strong></td>
</tr>
<tr>
<td>Non-reusable verification</td>
<td>11.5</td>
</tr>
<tr>
<td>Traditional engineering</td>
<td>4–6</td>
</tr>
</tbody>
</table>

**Reusable!**

### Proof Relationships
- Abstract Spec
- Executable Spec
- C Implementation
Why So Hard for 9,000 LOC?

seL4 call graph
Verification Cost

- Confidentiality: 3.4 years
- Integrity: 0.6 years, 4 months
- Availability: 0 years, by construction

Abstract Model

- C Implementation: 11.5 years, 4.5 years
- Binary code: 2 years, 1 year
  - Mostly for tools

Design + implementation + verification = $400/LOC
**Microkernel Life-Cycle Cost in Context**

- Revolution!
- L4 Pistachio: $100–150
- Green Hills INTEGRITY: $1000
- Fast!
- Slow!

<table>
<thead>
<tr>
<th>Assurance</th>
<th>Cost ($/SLOC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slow</td>
<td>100</td>
</tr>
<tr>
<td>Fast!</td>
<td>250</td>
</tr>
<tr>
<td>Fast!</td>
<td>500</td>
</tr>
<tr>
<td>Fast!</td>
<td>750</td>
</tr>
<tr>
<td>Fast!</td>
<td>1000</td>
</tr>
</tbody>
</table>
Security Impact of OS Design
Quantifying OS-Design Security Impact

Approach:

• Examine all critical Linux CVEs (vulnerabilities & exploits database)
  • easy to exploit
  • high impact
  • no defence available
  • confirmed

• For each establish how microkernel-based design would change impact

115 critical Linux CVEs to Nov’17
Hypothetical seL4-based OS

OS structured in *isolated* components, minimal inter-component dependencies, *least privilege*

Functionality comparable to Linux
Hypothetical Security-Critical App

App requires:
- IP networking
- File storage
- Display output
All Critical Linux CVEs to 2017

- **Not in TCB:** Attack defeated
  - 41% eliminated
  - 58% low severity
  - 96% not critical

- **In microkernel:** Attack defeated by verification

- **Still full system compromise:** No effect

- **No full compromise, but violates integrity or confidentiality:** Weakly mitigated

- **Only crash essential service (availability):** Strongly mitigated

- 38% eliminated
  - 30% not critical
  - 17% low severity
  - 11% moderate severity
  - 4% high severity
Conclusion: OS Structure Matters

- Microkernels definitely improve security
- Microkernel verification improves further
- Monolithic OS design is fundamentally flawed from security point of view

Use of a monolithic OS in security- or safety-critical scenarios is professional malpractice!

[Biggs et al., APSys’18]