2021 T2 Week 10 Part 1
Formal Verification and seL4
@GernotHeiser
Copyright Notice

These slides are distributed under the Creative Commons Attribution 3.0 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/3.0/legalcode
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 and formal verification aim to establish correctness of
• mechanism design
• mechanism implementation
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>
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
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:**
- 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

**Theorem proving:**
- Can deal with large (even infinite) state spaces
- Can prove functional correctness against a spec
- Very labour-intensive

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

RISK ASSESSMENT —
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

The Linux kernel today faces an unprecedented safety crisis. Much like when
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 way.

Does it run Linux? "We’re pleased to say that it does. Recently, we have a para-virtualized ver-
echeményeképpen pedig egy olyan megozöttosagot kapnak a szorvtől, amely e
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]

Translation correctness
[PLDI’13]

Worst-case execution time
[RTSS’11, RTAS’16]

Integrity

Abstract Model

C Implementation

Binary code

Availability

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

World’s fastest microkernel!
Functional Correctness
Proving Functional Correctness

Abstract Model
4.9 kLOC Isabelle

Executable Model
13 kLOC Isabelle

Refinement: all possible implementation behaviours are captured by the model

Implementation
5.7 kLOC Haskell

Formalised C
(Isabelle)

Formal C Semantics

Implementation
8.7 kLOC C

Cparser
How do these proofs work?

"Forward simulation":
Prove state correspondence of abstract and concrete levels

\[ \sigma \xrightarrow{\text{operation}} \sigma' \]

\[ S \xrightarrow{\text{state relation}} S' \]

prove!
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

Bugs found:

- 16 in (shallow) testing
- 460 in verification
  - 160 in C,
  - 150 in design,
  - 150 in spec

Can prove further properties on abstract level!
Binary Correctness
Binary Verification: Translation Validation

C Source → Formalised C

Formal C Semantics → Rewrite Rules

Proof

Compiler

Binary Code

Proof

Symbol Tables

Formal ISA Spec

Target of functional correctness proof

Graph Language

Proof

SMT Solver

Graph Language

Proof

De-compiler

Formalised Binary
Security Enforcement
Isolation Goes Deep

Kernel data partitioned like user data
Integrity: Control Write Access

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!

Event-based kernel always operates on behalf of well-defined user:
• Prove kernel only modifies data if presented write cap
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

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

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

Violation not observable by High!


Confidentiality Proof Challenge

**Spec**

```c
bool a();

bool b() {
    int secret;
}
```

**Implementation**

```c
bool a() {
    return !secret;
}
```

**Solution:**

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

Infoflow is a 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

MMU model finished by recent PhD

Present research!
Present Status

32b Arm
- Confid.
- Integrity
- Availab.

Abstract Model
- Proof
- C
- Proof
- Binary

64b x86
- Confid.
- Integrity
- Availab.

Abstract Model
- Proof
- C
- Proof
- Binary

64b RISC-V
- Confid.
- Integrity
- Availab.

Abstract Model
- Proof
- C
- Proof
- Binary
### Common Criteria?

<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>
<tr>
<td>sel4</td>
<td>Formal</td>
<td>Formal</td>
<td>Formal</td>
<td>Formal</td>
</tr>
</tbody>
</table>
WCET Analysis
WCET Analysis

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

- Loop bounds
- Infeasible path info

Accurate & sound model of pipeline, caches

Challenge: minimise pessimism – establish tight bounds/models

Pessimism! Scalability!
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!
Cost of Verification
## Verification Cost Breakdown

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

[Reusable!]

---

**Abstract Spec**

**Executable Spec**

**C Implementation**

---

**Proof**
Why So Hard for 9,000 LOC?

seL4 call graph
Verification Cost

Confidentiality
- Proof
- 3.4 py

Integrity
- Proof
- 0.6 py, 4 months

Availability
- Proof
- 0 py, by construction

Abstract Model
- Proof
- 11.5 py, 4.5 years

C Implementation
- Proof
- 2 py, 1.5 years
  Mostly for tools
- 2 py, 1 year
  Mostly for tools

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

Cost ($/SLOC)

Assurance

L4
Pistachio
$100–150

Fast!

Green Hills
INTEGRITY
$1000

Slow!

Slav! Fast!

Revolution!

© Gernot Heiser 2019 – CC Attribution License