Xen and the Art of Certification

Nathan Studer and Robert VanVossen
Xen Developer Summit 2014
Certification – Why?

B787-2139 by MilborneOne is licensed under http://creativecommons.org/licenses/by-sa/3.0/deed.en
Certification – Why?

A problem has been detected and Windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xfd3094c2, 0x00000001, 0xfbfe7617, 0x00000000)

*** SPCMDCON.SYS – Address Fbfe7617 base at Fbfe5000, Date/Stamp 3d6dd67c
Earning Trust

- Assurance standards $\neq$ “No Bugs” standards
- Demonstrate that your software can be trusted
- This trust is required for Medical, Automotive, and Aviation applications
Importance

- Server flaws do not usually cause direct personal harm.
- Flaws in safety-critical systems can kill
  - Car: Controlled Fireball
  - Plane: Passenger Carrying Missile
  - Robotic Surgery: Tamed Terminator
Overview

- DornerWorks Work
- Certification
- Certifying Core Xen
- Patch Examples
- Beyond Core Xen
- Cost
- Conclusion
- Questions
DornerWorks Work

- Started with the ARINC653 scheduler
- Continued with support by Navy Small Business Innovative Research (SBIR) topics
  - Rockwell Collins
  - Leanna Rierson – Designated Engineering Representative (DER)
  - Accuvant
Main Goals

- Demonstrate Xen on Embedded Platforms
- Understand what certifying Xen to DO-178 Design Assurance Level (DAL)-A and Common Criteria (CC) Evaluation Assurance Level (EAL) 6+ would take
- Begin the certification process
- Do some Formal Methods Analysis on Xen
Overview

- DornerWorks Work
- Certification
  - Certifying Core Xen
  - Patch Example
  - Beyond Core Xen
- Cost
- Conclusion
- Questions
What is certification

- Requires things that everyone knows should be done, but tend to skip. (e.g. Documentation)
- Enforces good practices. (e.g. design and test independence)
- Interesting Verification Activities
- Prevent certification loopholes. (e.g. tool qualification)
Tool Qualification

- What if the automated tool introduces an error?
What is Required?

- What does each level require
  - DAL-E: The software must exist.
  - DAL-D: High-Level Documentation/Tests
  - DAL-C: Low-Level Documentation/Unit Tests, Statement Coverage, and Code/Data Coupling Analysis
  - DAL-B: Branch Coverage
  - DAL-A: Source to Object Analysis and MC/DC Coverage

- DO-178 D-A closely related to ASIL A-D[1]
Example Applications

- **DAL-E: Infotainment**
  - Failure is a minor inconvenience

- **DAL-D/C: Instruments**
  - Failure can be mitigated by operator

- **DAL-B/A: Engine Control**
  - Failure could kill someone without warning
Certification Metrics[2]

- With Certification Experience
  - DAL-A: 0.67 hour / SLOC
  - DAL-B: 0.40 hour / SLOC
  - DAL-C: 0.20 hour / SLOC
  - DAL-D: 0.13 hour / SLOC
  - DAL-E: 0.11 hour / SLOC

- Without Certification Experience: Multiply by 3-4
Certification Metrics In Pictures

- Rate: $100/hr
- Two Examples:
  - 30K SLOC: ~Xen ARM
  - 1 Million SLOC: Small Linux Kernel?
Example Certification Cost – 30K SLOC

Cost to Certify 30K SLOC versus DAL

Cost ($) vs DAL

- $- $500,000.00
- $500,000.00 $1,000,000.00
- $1,000,000.00 $1,500,000.00
- $1,500,000.00 $2,000,000.00

With Experience

Without Experience

E D C

Xen Developer Summit
2014

Xen and the Art of Certification
Example Certification Cost – 30K SLOC

Cost to Certify 30K SLOC versus DAL

Cost ($) vs. DAL

- $10,000,000.00
- $8,000,000.00
- $6,000,000.00
- $4,000,000.00
- $2,000,000.00

With Experience vs. Without Experience

E, D, C, B, A
Example Certification Cost – 1M SLOC

Cost to Certify 1M SLOC versus DAL

- $10,000,000.00
- $20,000,000.00
- $30,000,000.00
- $40,000,000.00
- $50,000,000.00
- $60,000,000.00

DAL

- E
- D
- C

With Experience
Without Experience
Example Certification Cost – 1M SLOC

Cost to Certify 1M SLOC versus DAL

- $50,000,000.00
- $100,000,000.00
- $150,000,000.00
- $200,000,000.00
- $250,000,000.00
- $300,000,000.00

With Experience
Without Experience
Where does the time go?

Breakdown of DO-178 Objectives (DAL-A)

- Planning
- Development
- Verification
- Configuration Management
- Quality Assurance
- Certification
- Source Code
Overview

- DornerWorks Work
- Certification

Certifying Core Xen

- Patch Example
- Beyond Core Xen
- Cost
- Conclusion
- Questions
General Xen Certification Plan

- Create a small subset
- Reverse Engineer Certification Artifacts for any extant features
- Forward Engineer any additional features
Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
Reverse Engineering – What can go wrong? [3]

- Poor reverse engineering justification
- Lack of a well defined Software Lifecycle Plan
- Abstraction and traceability problems
- No Access to original developers
- Complex and poorly documented source code

Commercial Aviation Safety Team (CAST)
Access to Original Developers

“Developing the design, requirements, and test cases for a complex software component, such as an operating system, can be nearly impossible without some access to the original developers.” [3]
Xen Original Developers

- ARM
  - Ian Campbell
  - Ian Jackson
  - Stefano Stabellini
  - Julien Grall

- X86
  - Kier Frasier?
  - ???
Backup Plan

1. Git commit messages.
2. Archived Design Discussions on the mailing list.
Documentation and Comments

“Many reverse engineering efforts start with source code that is complex and poorly documented. The code may contain numerous pointers and complex data structures. The code may also not contain commentary statements, which can make it difficult to understand.” [3]

Reoccurring topic on Slashdot
Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. **Focus on ARM**
Overview

- DornerWorks Work
- Certification
- Certifying Core Xen

**Patch Example**

- Beyond Core Xen
- Cost
- Conclusion
- Questions
Good Patch – Design Details

- David Vrabel – Scalable Event Channels
Hi,

Here is a design for a scalable event channel ABI for Xen. It has a number of benefits over the design currently being proposed by Wei Lui.

* More event channels (>100,000).
* 16 event priorities.
* Reduced memory requirements (only 1 additional page per domU).
* The use of FIFOs for events ensures fairness, whereas it is difficult to reason about the fairness with the current bitmap system.

The PDF version is easier to read and has diagrams and readable maths but the original markdown format document is included below (for ease of commenting).

http://xenbits.xen.org/people/dvrabel/event-channels-A.pdf
## Design Details (DAL-D)

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>1.1</td>
<td>Purpose</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>System Overview</td>
<td>2</td>
</tr>
<tr>
<td>1.3</td>
<td>Design Map</td>
<td>2</td>
</tr>
<tr>
<td>1.4</td>
<td>References</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Design Considerations</td>
<td>3</td>
</tr>
<tr>
<td>2.1</td>
<td>Assumptions</td>
<td>3</td>
</tr>
<tr>
<td>2.2</td>
<td>Constraints</td>
<td>3</td>
</tr>
<tr>
<td>2.3</td>
<td>Risks and Volatile Areas</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Architecture</td>
<td>3</td>
</tr>
<tr>
<td>3.1</td>
<td>Overview</td>
<td>3</td>
</tr>
</tbody>
</table>
Design Details (DAL-D)

4 High Level Design

4.1 Shared Event Data Structure

4.2 Event State Machine

4.3 Event Queues

4.4 Hypercalls

4.4.1 EVTCHNPOp_init

4.4.2 EVTCHNPOp_expand

4.4.3 EVTCHNPOp_set_priority

4.4.4 EVTCHNPOp_set_limit

4.5 Memory Usage

4.5.1 Event Arrays

4.5.2 Control Block
Design Details (DAL-C, B, A)

5 Low Level Design

5.1 Raising an Event ......................................................... 10
5.2 Consuming Events ....................................................... 10
5.3 Masking Events .......................................................... 11
5.4 Unmasking Events ....................................................... 11
Overview

- DornerWorks Work
- Certification
- Certifying Xen
- Patch Example

Beyond Core Xen

- Cost
- Conclusion
- Questions
Xen Helpers

- U-boot or bootloader
- Qemu
- XL and friends
- Dom0
Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM
4. Create a simpler bootloader
Xen Helpers

- U-boot or bootloader
- Qemu
- XL and friends
- Dom0
Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM
4. Create a simpler bootloader
5. Use direct pass-through or PV drivers
Xen Helpers

- U-boot or bootloader
- Qemu

**XL and friends**

- Dom0
Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM
4. Create a simpler bootloader
5. Use direct pass-through or PV drivers
6. Create a simpler toolstack
Xen Helpers

► U-boot or bootloader
► Qemu
► XL and friends
► Dom0
How hard is certifying Linux?

- It’s been done… to DAL-D.
- DAL-C is a big hurdle.
- It must be the “Rate of Change”, right?
Why such a big hurdle?

- DAL-D
  - High-Level Documentation
  - Functional Tests
- Information already exists.
Why such a big hurdle?

- **DAL-C**
  - Statement Coverage
  - Code/Data Coupling Analysis
  - Low-Level Documentation
  - Exhaustive Unit Tests

- Extremely unpopular tasks in the open source community.
Xen Certification Guidelines

1. Create a small subset
2. Use virtualization extensions
3. Focus on ARM
4. Create a simpler bootloader
5. Use direct pass-through or PV drivers
6. Create a simpler toolstack
7. Replace or Offload Linux dom0
Avoiding Linux – Open Source

- Mini-os dom0
- Custom dom0
- FreeRTOS?
Avoiding Linux - Other

- Already Certified dom0 (e.g. VxWorks, GreenHills, etc…)
  - HVM (or PVH) dom0
- Certified service domains
  - Still certifying a subset of Linux
- Unikernels
Overview

- DornerWorks Work
- Certification
- Certifying Core Xen
- Patch Example
- Beyond Core Xen

Cost

- Conclusion
- Questions
Cost

- Certification Packages are expected to be expensive, but not that expensive
- Amortize certification costs, somehow
- Start with something less critical
Overview

- DornerWorks Work
- Certification
- Certifying Xen
- Patch Example
- Beyond Core Xen
- Cost

Conclusion

- Questions
Conclusion

- Certification is a lot of work
- It needs to be done if a Xen guest is ever going to:
  - Fly a plane
  - Drive a Car
  - Perform Orthopedic Surgery
- The Xen developer community has a good framework in place to make it happen
References


Overview

- DornerWorks Work
- Certification
- Certifying Xen
- Patch Example
- Beyond Core Xen
- Cost
- Conclusion

Questions
Questions
Contact Information

- Nathan Studer: nate.studer@gmail.com
- Robert VanVossen: robert.vanvossen@dornerworks.com