第 1 讲：Advanced OS Overview

第六节：Tendency of OS – Correctness

陈渝

清华大学计算机系

yuchen@tsinghua.edu.cn

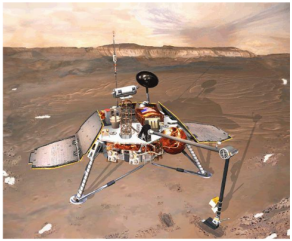
2020 年 2 月 15 日

Tendency

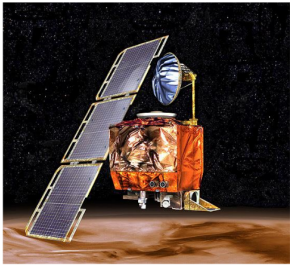
- Performance
- Reliability
- **Correctness**

Standard Motivating Slides for Verification

Ariane 5



Mars Polar Lander

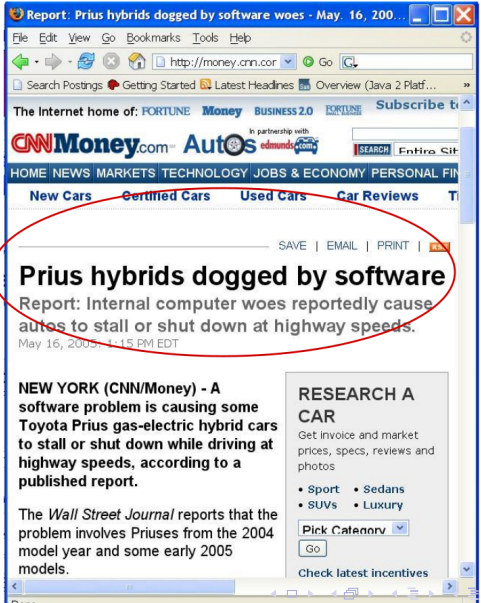


Mars climate orbiter

Standard Motivating Slides for Verification

Photo from edmunds.com

Toyota recalled its 160,000 Prius cars in Oct 2005, because of bugs in the software controlling the hybrid gas-electric engine system…



NICTA

seL4

Formal Verification of an OS Kernel

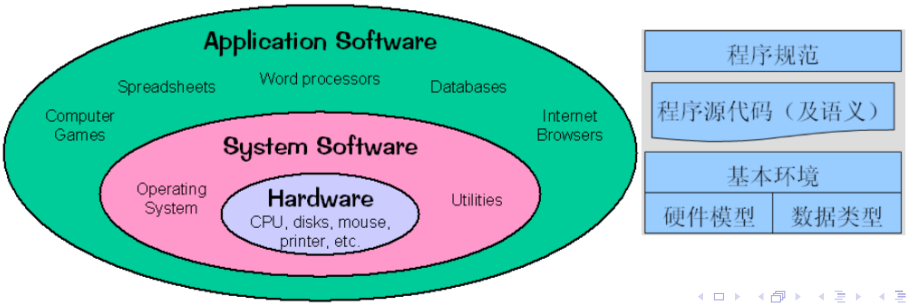
Gerwin Klein
June Andronick
Dhammika Elkaduwe
Michael Norrish

Kevin Elphinstone
David Cock
Kai Engelhardt
Thomas Sewell
Simon Winwood

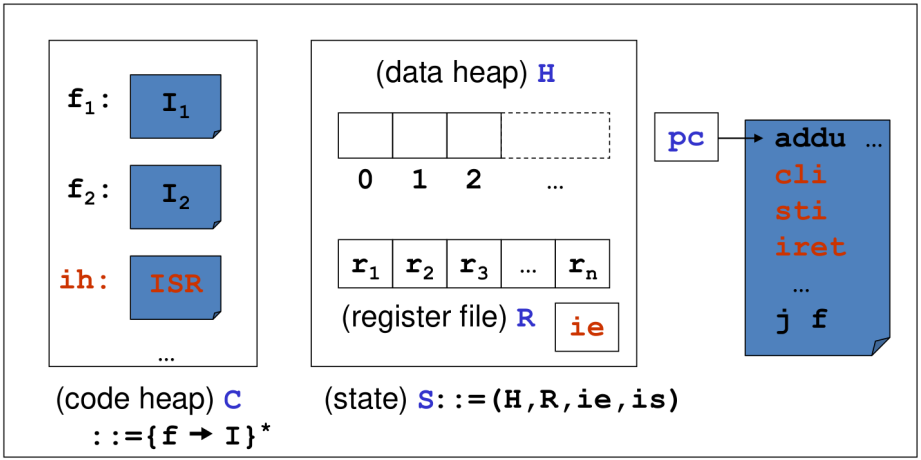
Gernot Heiser
Philip Derrin
Rafal Kolanski
Harvey Tuch

Basic Idea

- Certified Software: Problem Definition
  - Hardware
    - processors, memory, storage, devices, ...
  - Software
    - bootloader, device drivers, OS, runtime, applications, ...
  - Need a mathematical proof showing that as long as the hardware works, the software always work according to its specification



Abstract Interrupt Machine



(program) P ::=(C,S,pc)

Challenges of AIM

- Components come from different sources
  - Manually written assembly
  - C/C++
  - Type safe languages(Java, C#)
  - Go, Rust
  - DSL
- Many different features
  - Code loading

Challenges of AIM

- Components come from different sources
  - Manually written assembly
  - C/C++
  - Type safe languages(Java, C#)
  - Go, Rust
  - DSL
- Many different features
  - Code loading
  - Control abstractions
    - jmp (goto)/functions
    - exceptions/interrupts
    - process/threads

Challenges of AIM

- Components come from different sources
  - Manually written assembly
  - C/C++
  - Type safe languages(Java, C#)
  - Go, Rust
  - DSL
- Many different features
  - Code loading
  - Control abstractions
    - jmp (goto)/functions
    - exceptions/interrupts
    - process/threads
  - Memory update
    - type-preserving update
    - type-changing update
    - pointer arithmetic

Challenges of AIM

- Components come from different sources
  - Manually written assembly
  - C/C++
  - Type safe languages(Java, C#)
  - Go, Rust
  - DSL
- Many different features
  - Code loading
  - Control abstractions
    - jmp (goto)/functions
    - exceptions/interrupts
    - process/threads
  - Memory update
    - type-preserving update
    - type-changing update
    - pointer arithmetic
  - Device drivers and I/O
  - Hardware ...

Some Conclusions

- AIM machine
  - low-level
  - can implement interrupt handlers and thread libraries
- A program logic
  - following local reasoning in separation logic
  - modeling cli/sti, switch, block/unblock in terms of memory ownership transfer
  - can certify different implementation of locks and C.V.s

CONCLUSION

OS is an interesting research area.

《儒效篇》–荀子

不闻不若闻之，闻之不若见之，见之不若知之，知之不若行之；学至于行之而止矣。

- Find problems
- Analysis
- Practice
- Write paper

Thanks

Some materials are from:

- cop5611 course from Andy Wang, Florida State University
- CS-502 course from WPI
- Compiler/Program Research Group in TH
- OS papers/slides on our course topics
- ……