

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



- Performance
- Reliability
- **Correctness**



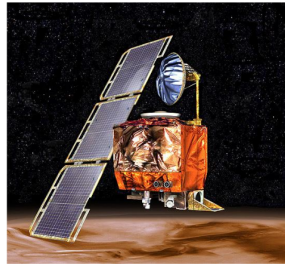
Standard Motivating Slides for Verification



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...

Report: Prius hybrids dogged by software woes - May. 16, 200...

File Edit View Go Bookmarks Tools Help

http://money.cnn.com

Search Postings Getting Started Latest Headlines Overview (Java 2 Platf...

The Internet home of: FORTUNE Money BUSINESS 2.0 FORTUNE

CNNMoney.com Autos in partnership with edmunds.com

HOME NEWS MARKETS TECHNOLOGY JOBS & ECONOMY PERSONAL FIN

New Cars Certified Cars Used Cars Car Reviews T

SAVE | EMAIL | PRINT

Prius hybrids dogged by software

Report: Internal computer woes reportedly cause autos to stall or shut down at highway speeds.

May 16, 2005, 1:15 PM EDT

NEW YORK (CNN/Money) - A software problem is causing some Toyota Prius gas-electric hybrid cars to stall or shut down while driving at highway speeds, according to a published report.

The *Wall Street Journal* reports that the problem involves Priuses from the 2004 model year and some early 2005 models.

RESEARCH A CAR

Get invoice and market prices, specs, reviews and photos

- Sport • Sedans
- SUVs • Luxury

Pick Category

Go

Check latest incentives

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



Australian Government
Department of Communications,
Information Technology and the Arts
Australian Research Council

NICTA Members



The University of Sydney



Queensland University of Technology

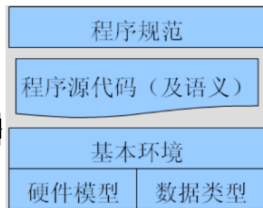
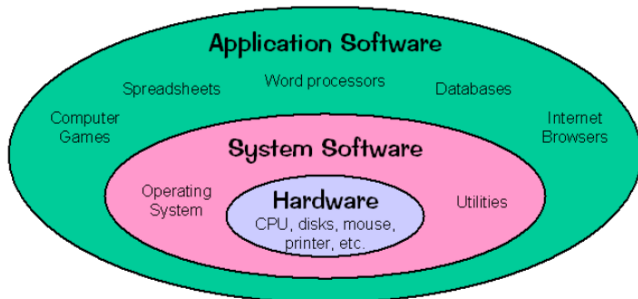


NICTA Partners

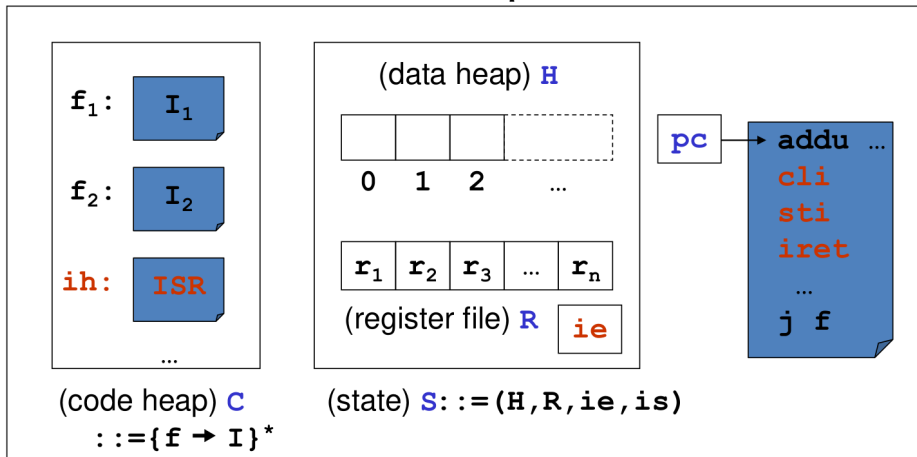
Basic Idea

- **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



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

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

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
-