
# Provable Isolation

## Scientia Professor Gernot Heiser

### NICTA and UNSW

Australian Government
Department of Broadband, Communications and the Digital Economy
Australian Research Council

NICTA Funding and Supporting Members and Partners

# The Need for Strong Intra-Platform Isolation

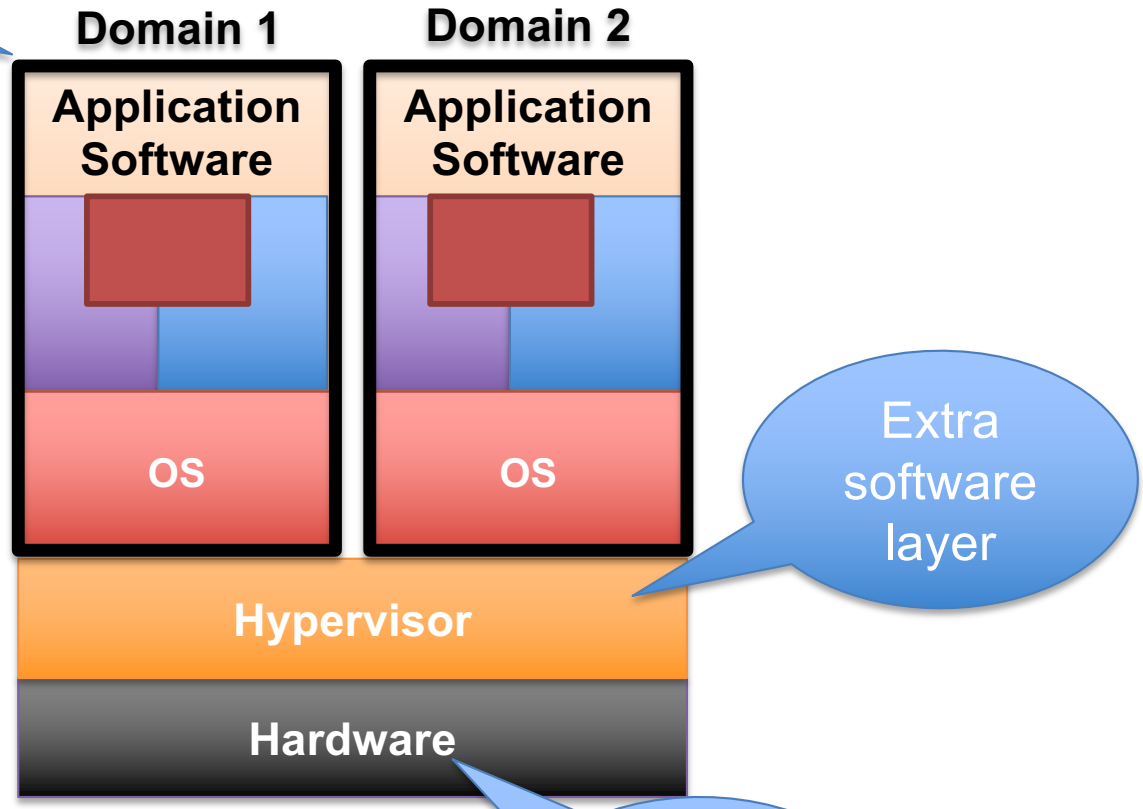
NICTA

- … where air-gap isolation is infeasible


# Intra-Platform Isolation Mediated by Software

NICTA

Multiple virtual machines



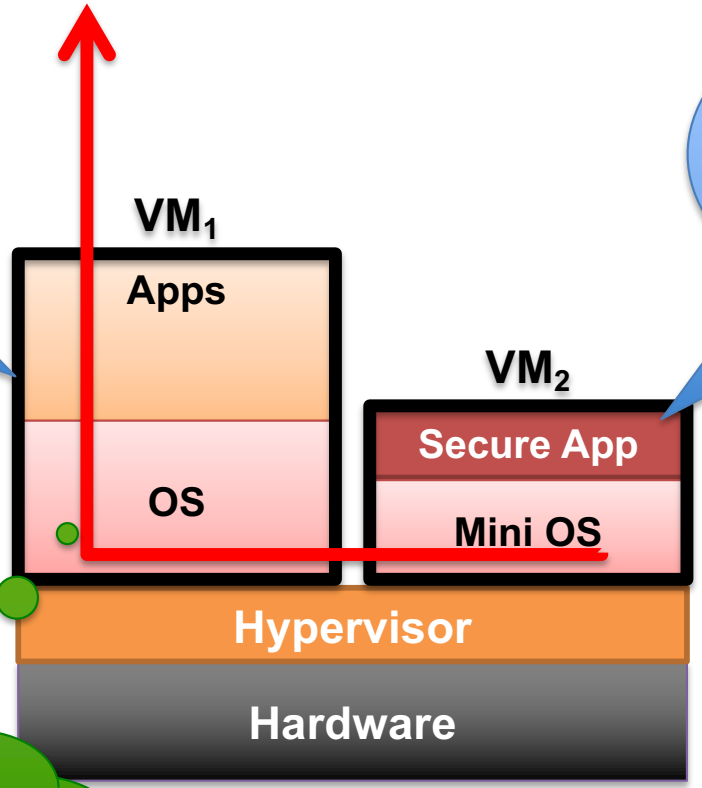

Cross-Domain Solution

# Intra-Platform Isolation Mediated by Software

NICTA

Standard smartphone OS + apps

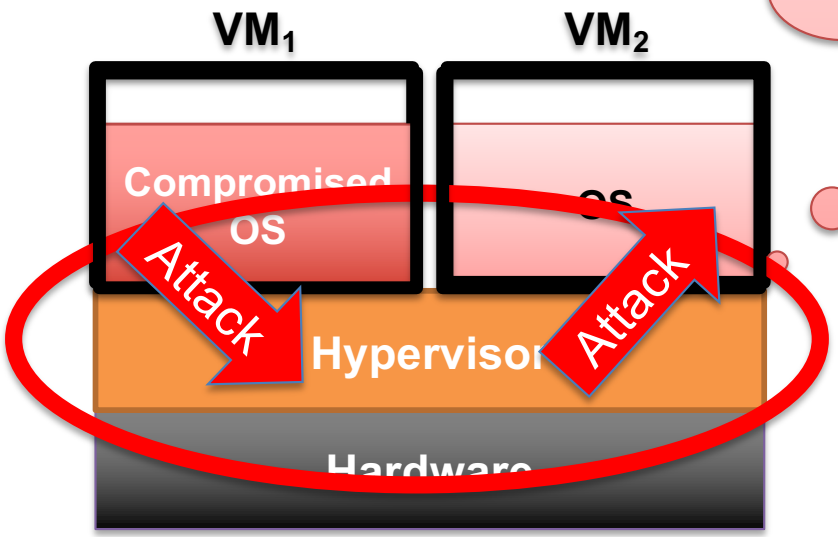
Minimal secure environment, protected by hypervsior




Secure comms on COTS phone

Data encrypted and securely sent through standard environment

# Isolation Software: Hypervisor




How trustworthy *is* this software?

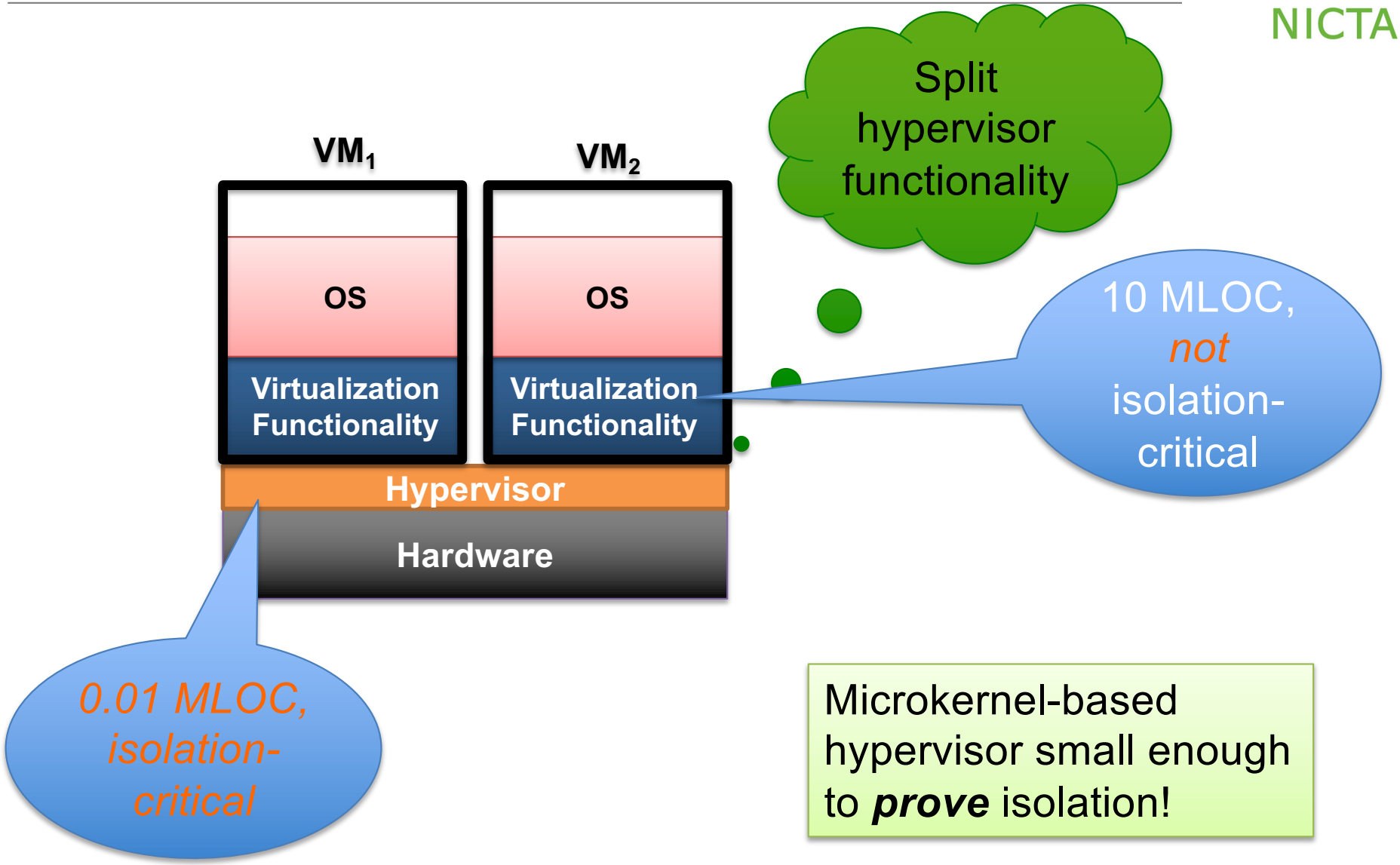
Hardware-enforced isolation mediated by software (hypervisor)

Typical hypervisor:
1 million lines of code

Typical bug density:
1 / 1000 lines of code

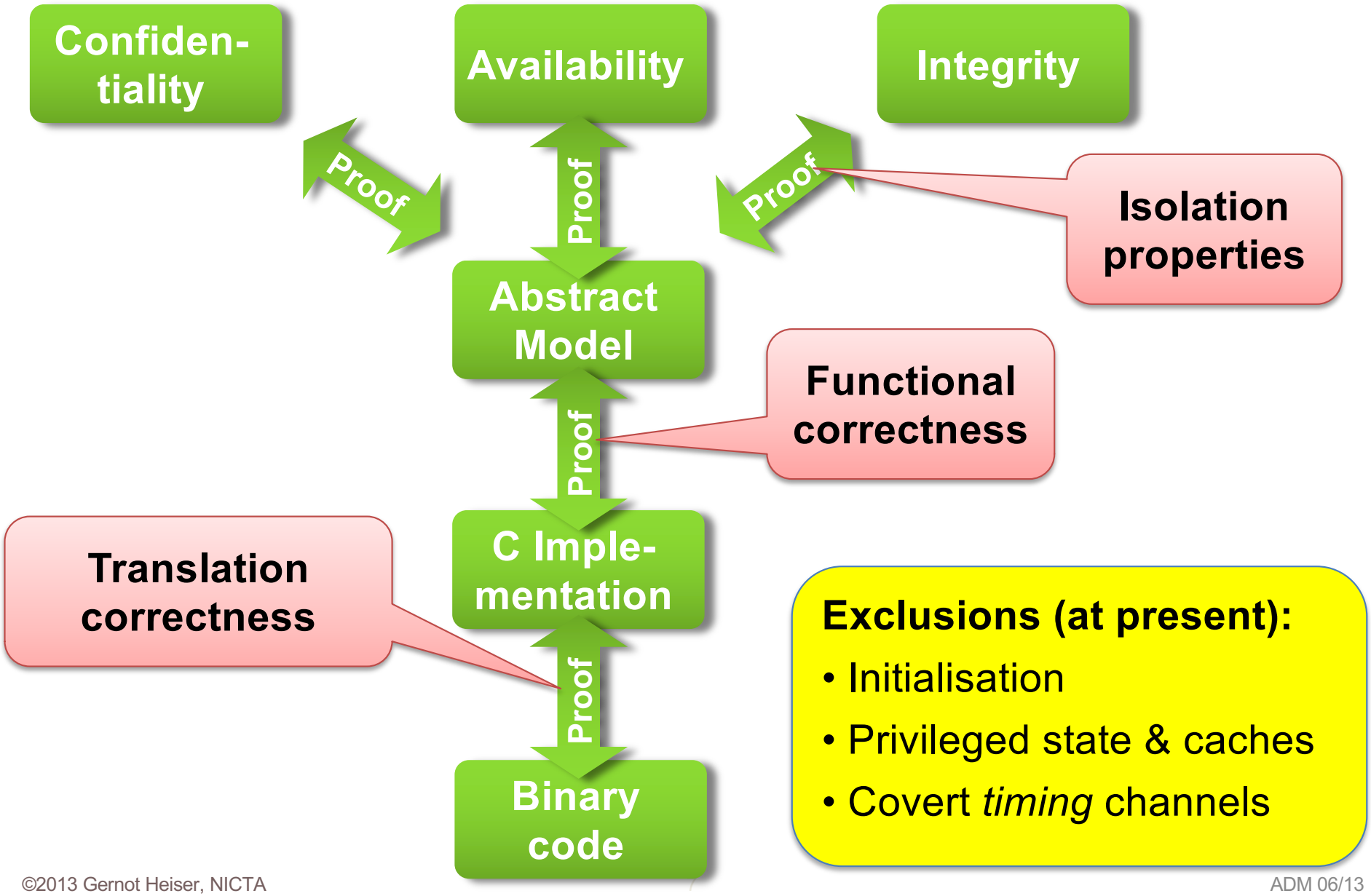
# Decrease Attack Surface: Microkernels

NICTA




Microkernel-based hypervisor small enough to ***prove*** isolation!

# NICTA's seL4: Mathematical *Proof* of Isolation



MIT Technology Review

# 10 BREAKTHROUGH TECHNOLOGIES 2011



## Crash-Proof Code

*Making critical software safer*



WILLIAM BULKELEY

*May/June 2011*

# NICTA's seL4 Microkernel: Unique Assurance


First and only operating-system with functional-correctness proof: operation is always according to specification

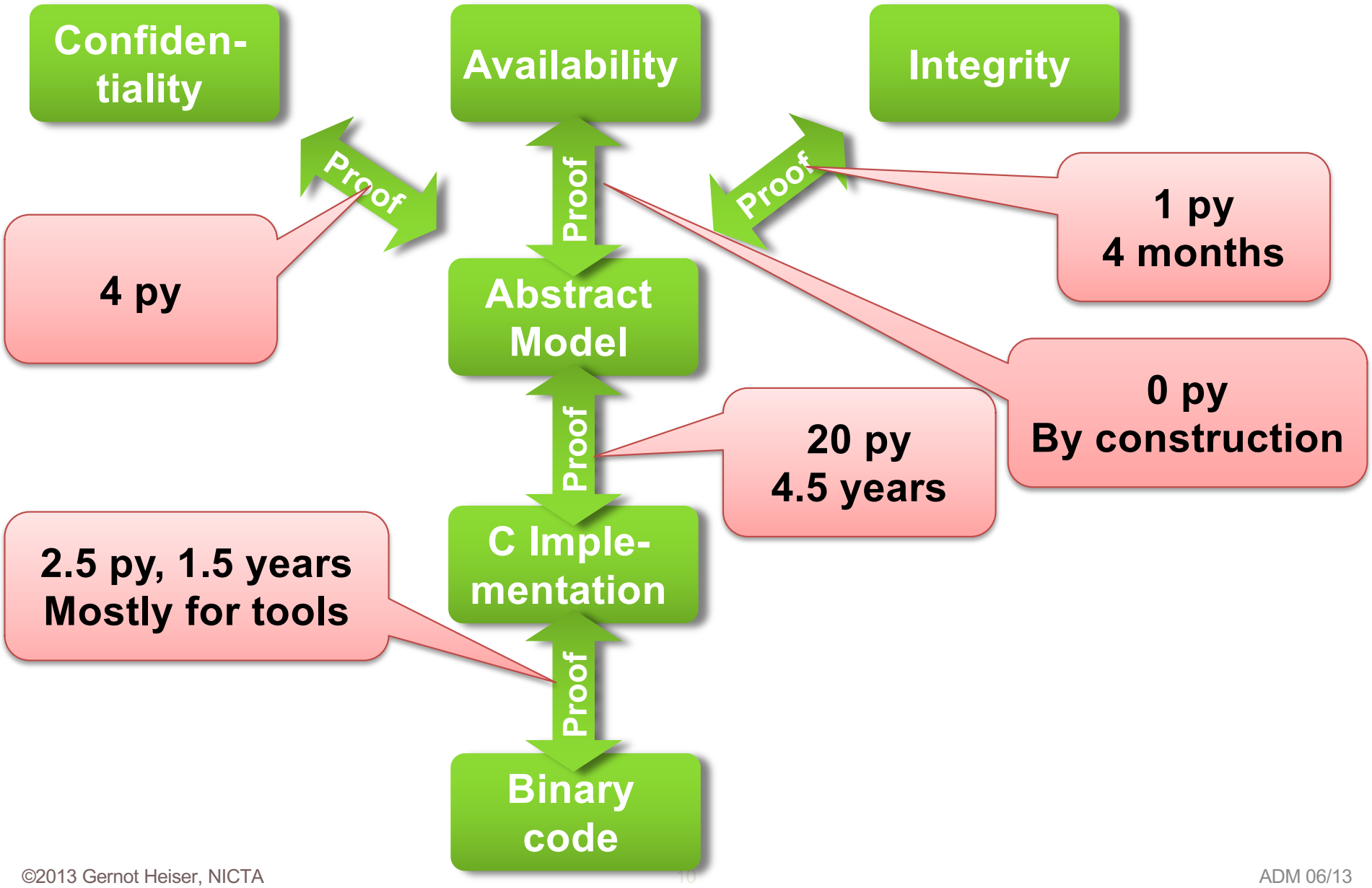
Predecessor deployed on 2 billion devices

First and only operating-system with *proof* of integrity and confidentiality enforcement – at the level of binary code!

World's fastest microkernel on ARM architecture

First and only protected-mode operating-system with complete and sound timing analysis

# seL4: Proof Chain from Requirements to Binary



# Next Step: Full System Assurance

NICTA

**DARPA HACMS Project:**

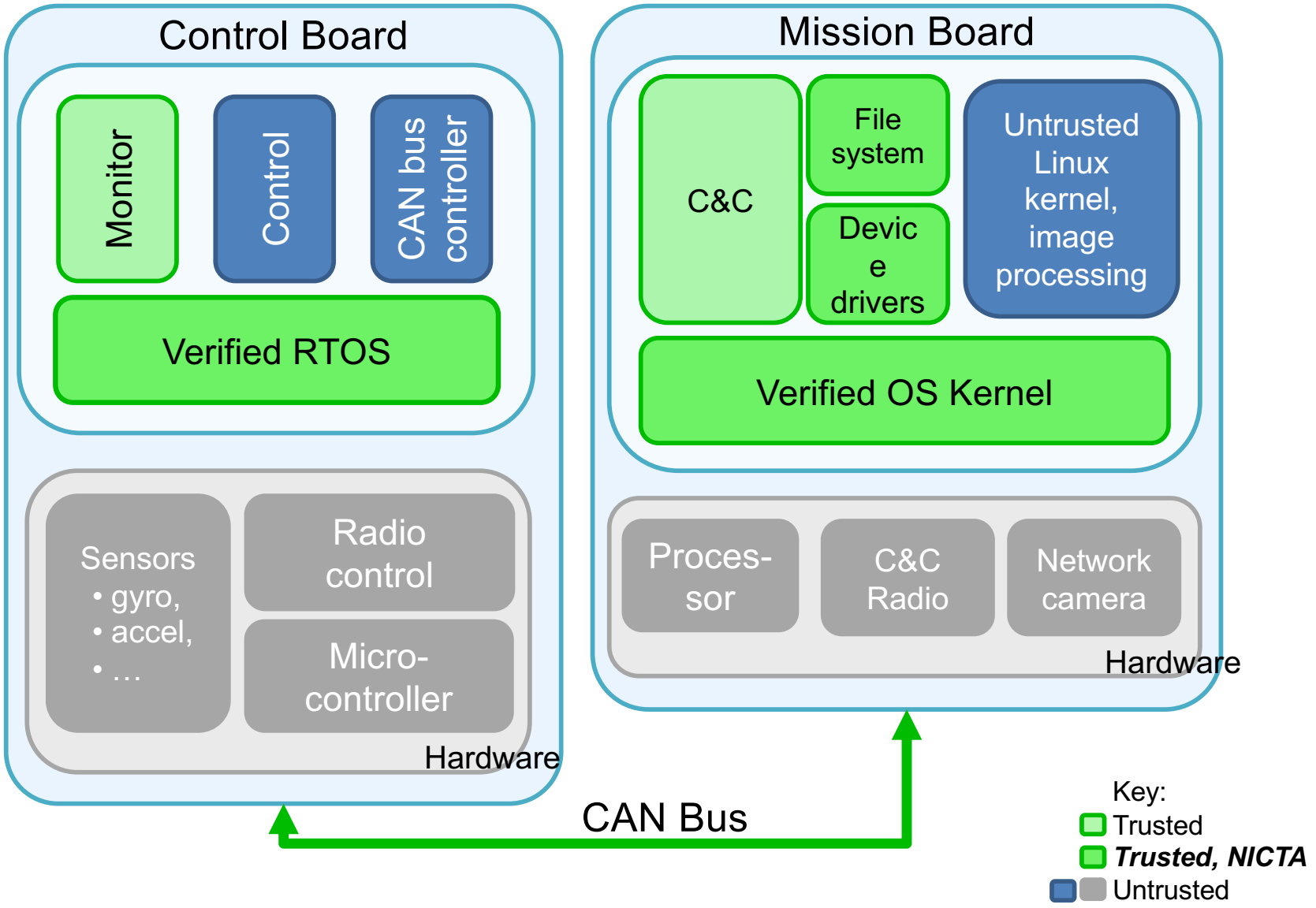
- Provable vehicle safety
- "Red Team" must not be able to divert vehicle
- $18.5M project

ArduCopter
Research Vehicle

Boeing Unmanned
Little Bird (AH-6)
Deployment Vehicle

NICTA Rockwell Collins BOEING galois University of Minnesota

# System Structure



# Provable Isolation is Possible!


Coming to a theatre near you!

google: “NICTA trustworthy systems”

mailto: gernot@nicta.com.au