Why Safety Requires Security

… and How to Achieve It

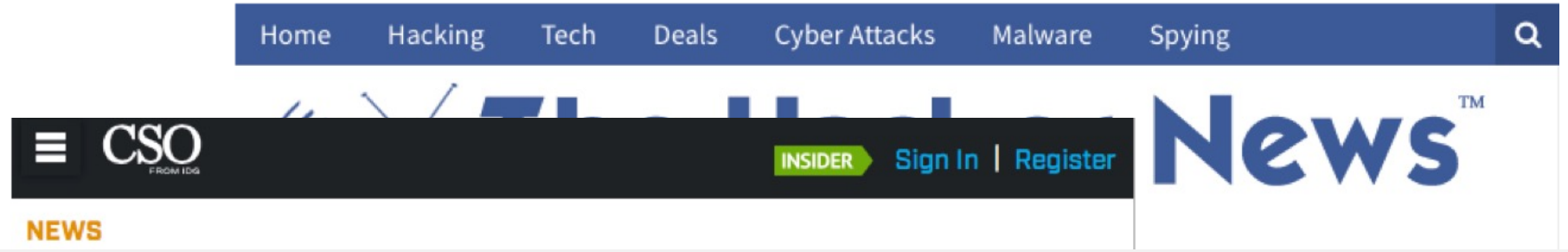
Gernot Heiser | gernot.heiser@data61.csiro.au | @GernotHeiser
Trustworthy Systems | Data61

Cyber Security for Medical and Health Care, Hong Kong, Dec'17

https://trustworthy.systems

CSIRO

Why Does Security Matter?



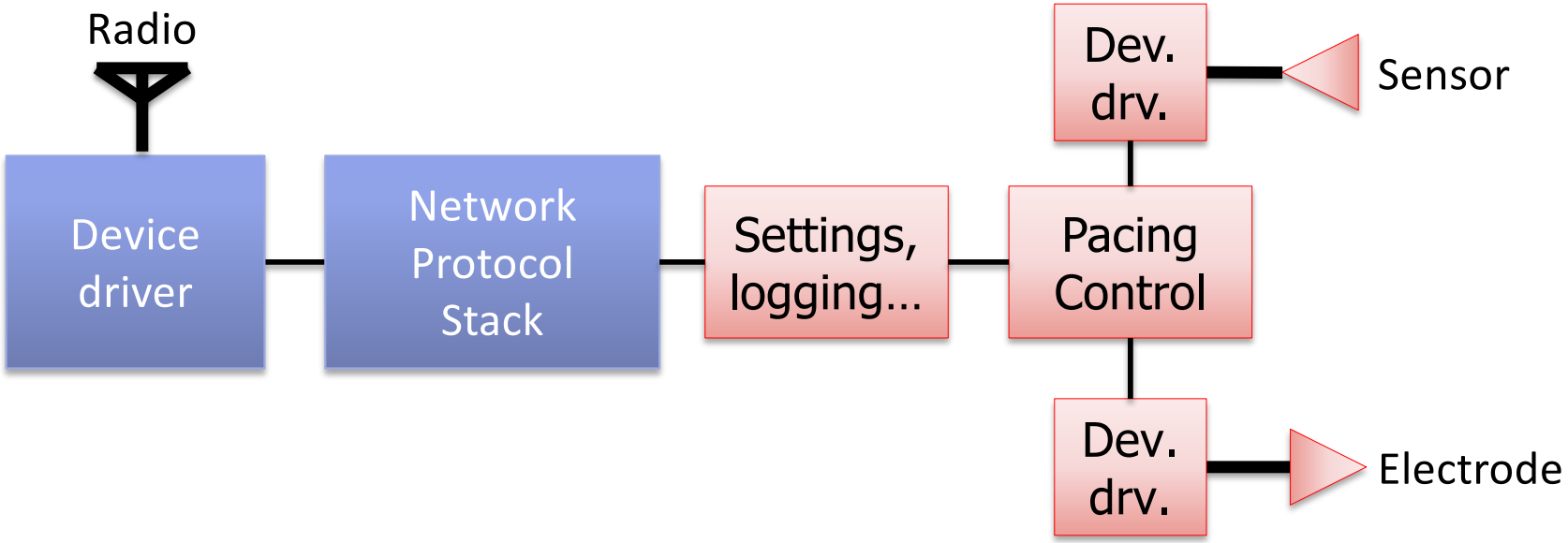
NEWS FEATURES HOW TO OPINION/Q&A CONTACT US NEWSLETTER

Chances are that it happens again soon. In a study published in May, security researchers Billy Rios and Jonathan Butts revealed that they'd found more than 8,000 known security vulnerabilities in four different pacemaker programmer systems from four different manufacturers. These programmer systems are used to alter the behavior of the pacemaker.

What's Behind?

Networking for:

- Day-to-day patient monitoring
- Adjusting settings by physician
- Maintenance (software upgrades)



Challenge of Networking

Networking creates remote attack opportunities

Attack vectors:

- **Insecure protocols**
- **Reusing crypto keys**
- **Software vulnerabilities**

Clinical device: WiFi/Bluetooth, Windows/Linux

'No one is
CT scann
machine
launchpa
attack.'

—ANTHONY JAM

intosec ISLAND

Front Page | Blog Posts | Resources | Media | Whitepapers | Visit Sec

Why Windows is a Bad Idea for Medical Devices

Tuesday, July 12, 2011

Contributed By:
Danny Lieberman

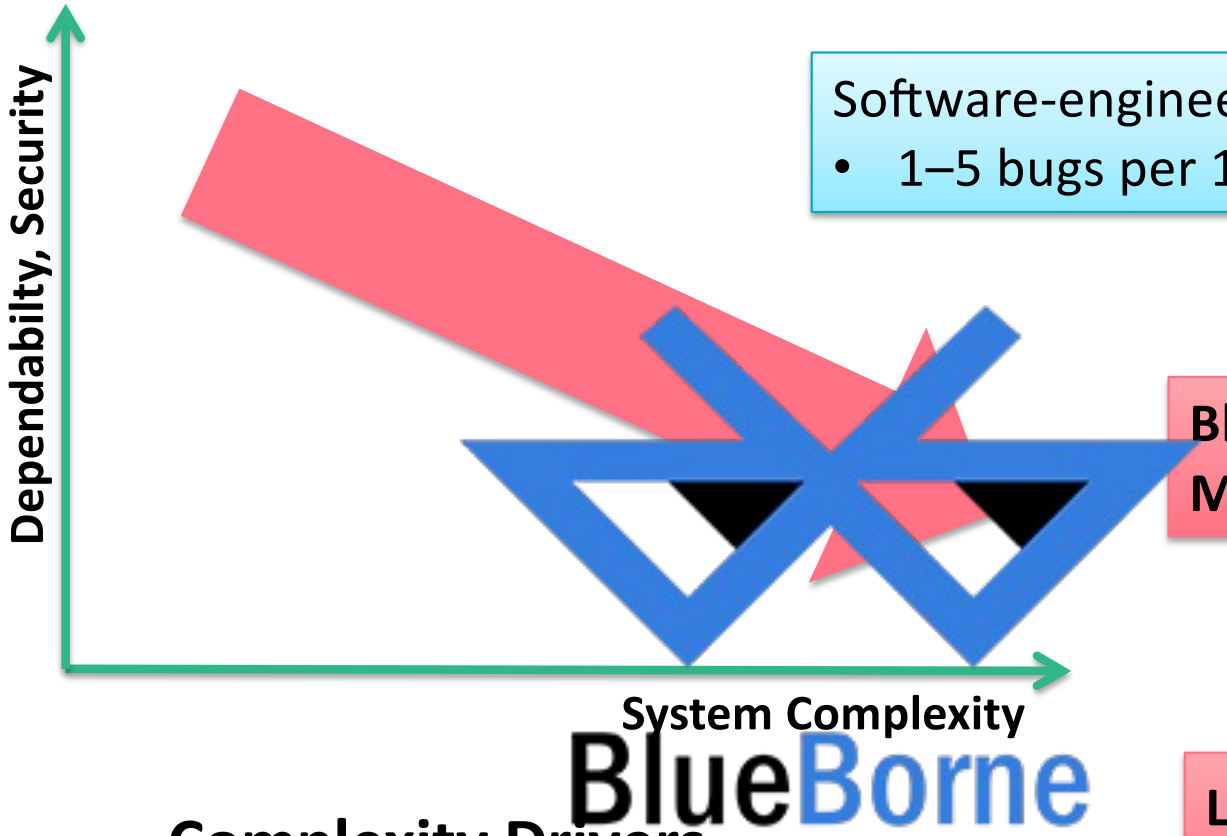
I'm getting some push back on LinkedIn on my articles o
medical devices that are installed in hospitals – read mo
medical devices here and here.

Scott Caldwell tells us that the FDA doesn't rule "out" or
Windows Embedded.

Having said that, Microsoft has very clear language in th
Embedded products:

*"The Products are not fault-tolerant and are not designed, manufactured or
performance in which the failure of a Product could lead to death, serious pe
environmental damage ("High Risk Activities")."*

Software Vulnerabilities



Software-engineering rule of thumb:

- 1–5 bugs per 1,000 lines of ***quality*** code

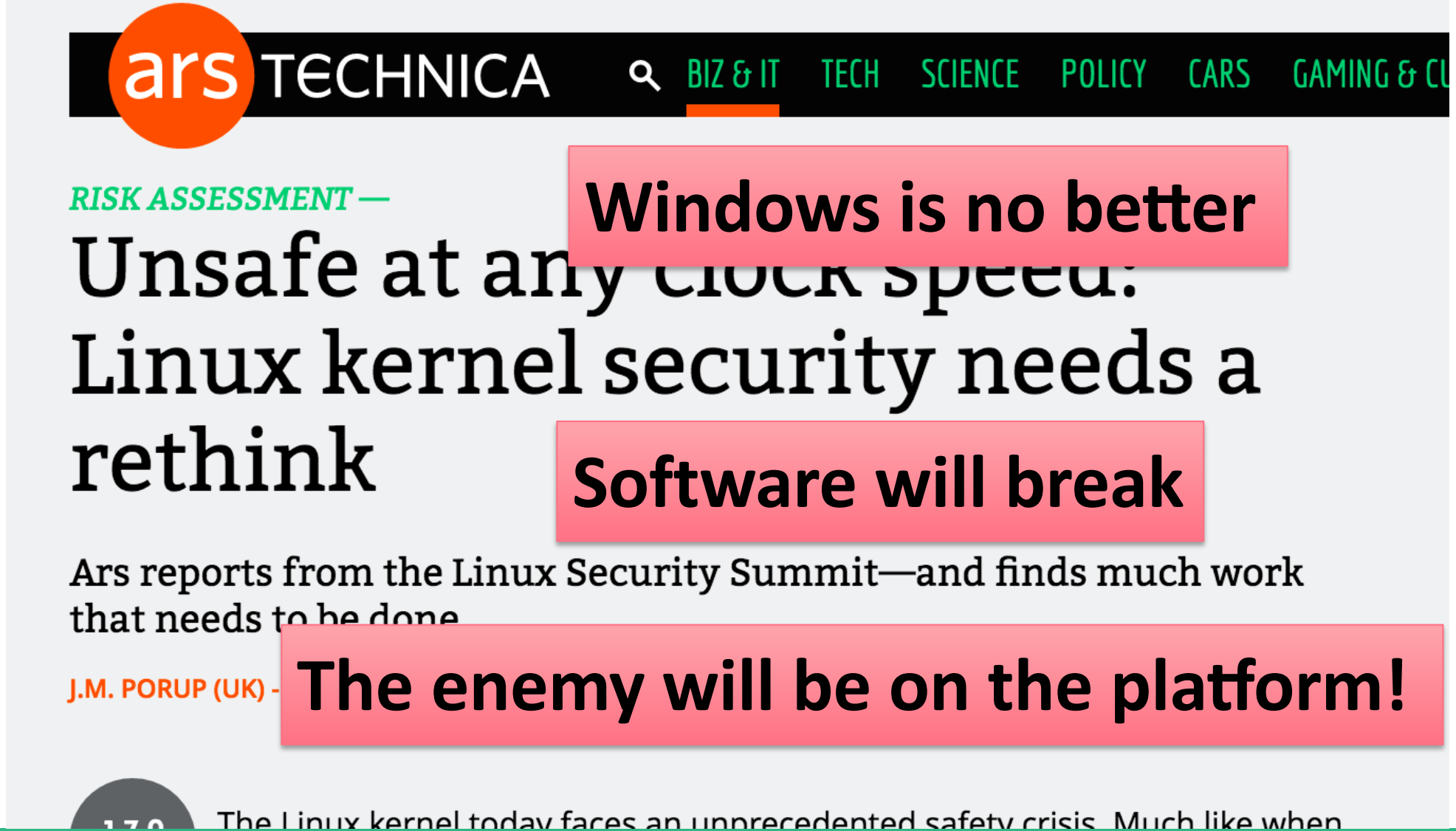
Bluetooth protocol stack:
Multiple 100,000 lines

Linux/Windows kernel:
Tens of millions of lines

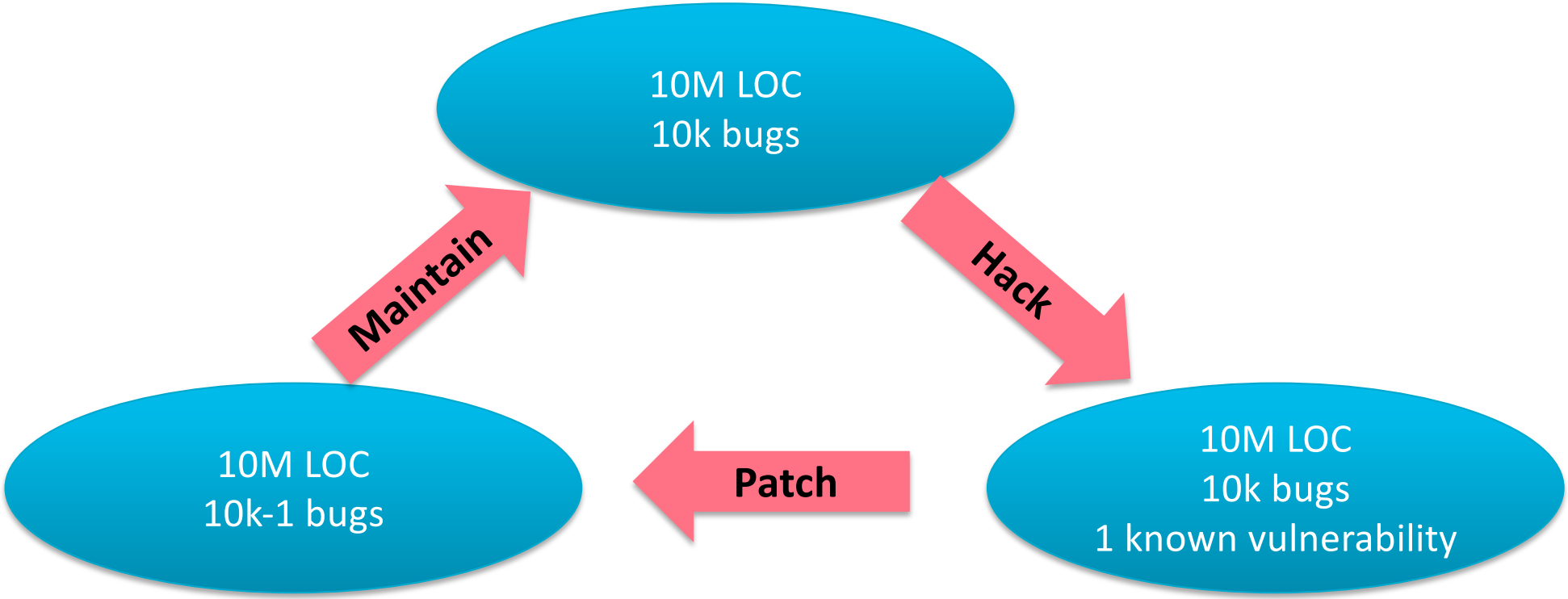
Complexity Drivers

- Features/functionality
- Legacy reuse

Linux “Security”

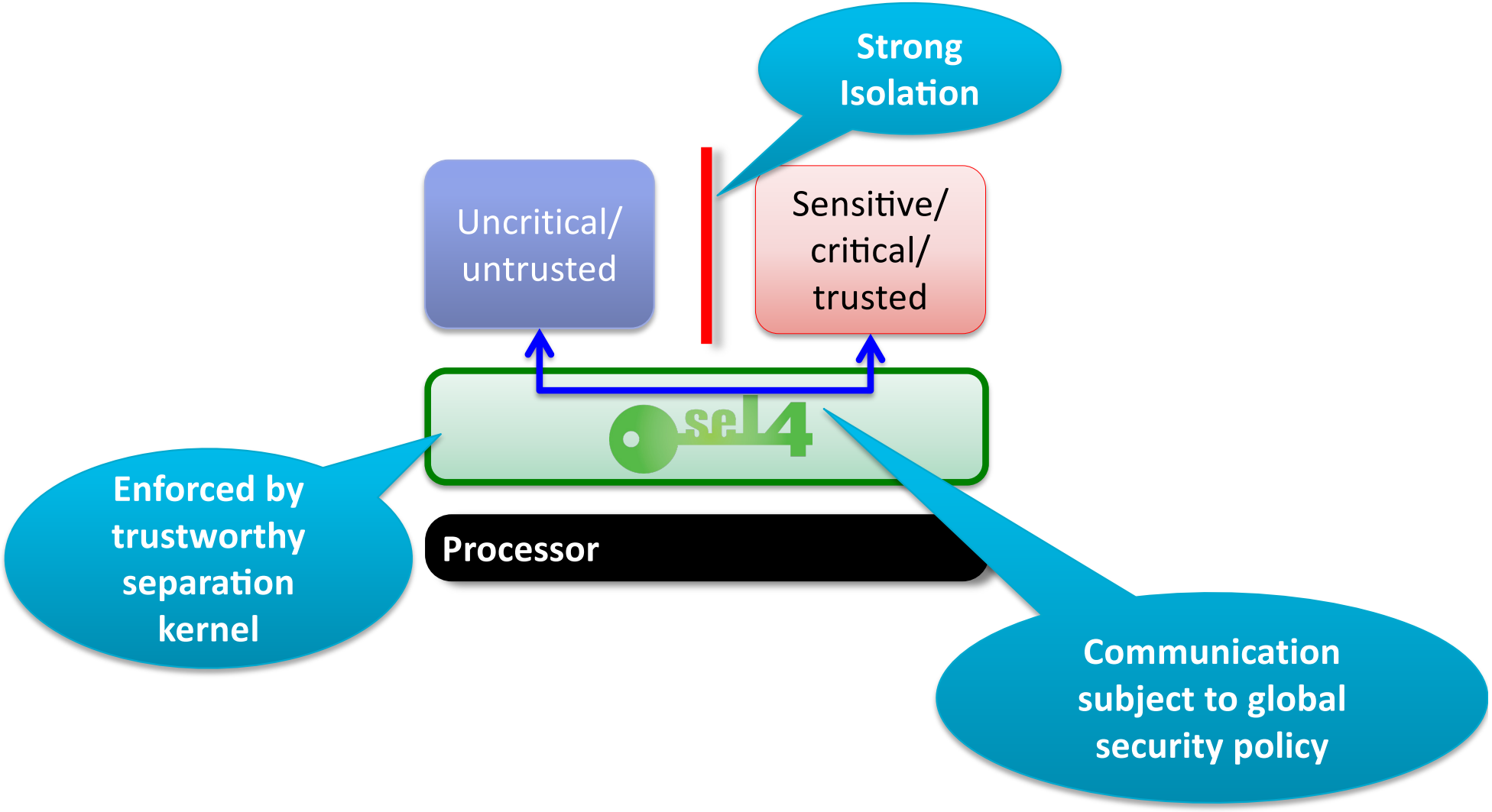


OK, So Let's Patch Regularly



Patch-and-Pray: A losing proposition

Fundamental Security Requirement: Isolation



Trustworthiness: Can We Rely on Isolation?

A system is **trustworthy** if and only if:

- it behaves **exactly** as it is specified,
- in a **timely** manner, and
- while ensuring **secure** execution

***Claim*:**

A system must be considered *untrustworthy* unless *proved* otherwise!

Corollary [with apologies to Dijkstra]:

Testing, code inspection, etc. can only show *lack of trustworthiness*!

seL4 Provably Secure Operating System

~10,000 lines of C and ASM code

Small attack surface,
Amenable to full verification

Non-kernel code can only access resources and communication channels if explicitly authorised with a per-object access token (capability)

Kernel can confine damage from attacks in unprivileged code

Small,

fast,

capability-based,

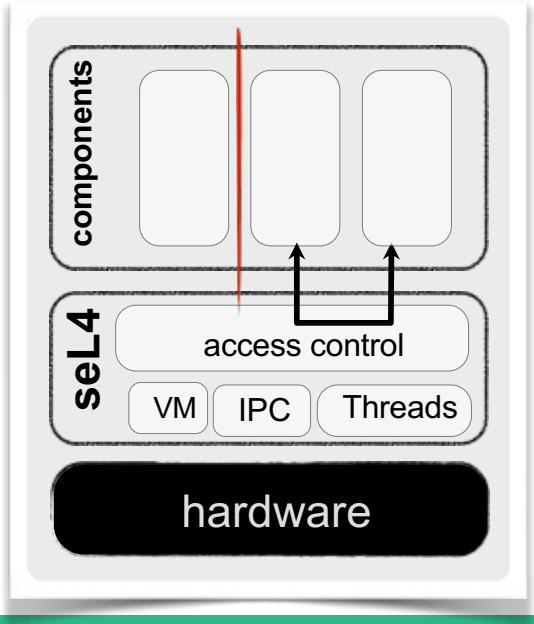
operating system kernel

World's fastest (5–10X faster) operating system designed for security and safety

Suitable for real-world deployment

Code that runs in privileged mode of the hardware

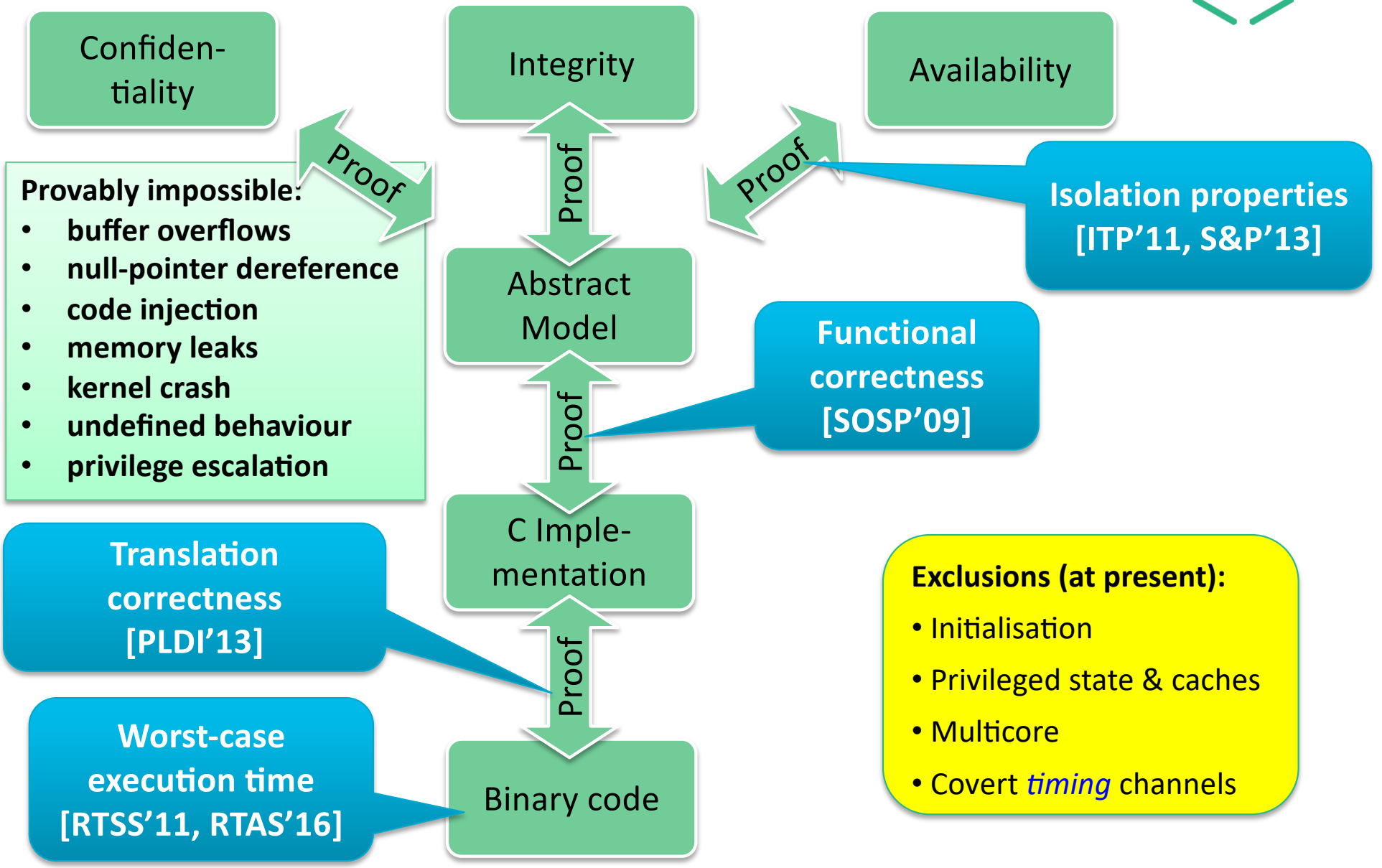
Most critical part



Unprivileged mode

Privileged mode

Proving Trustworthiness of seL4



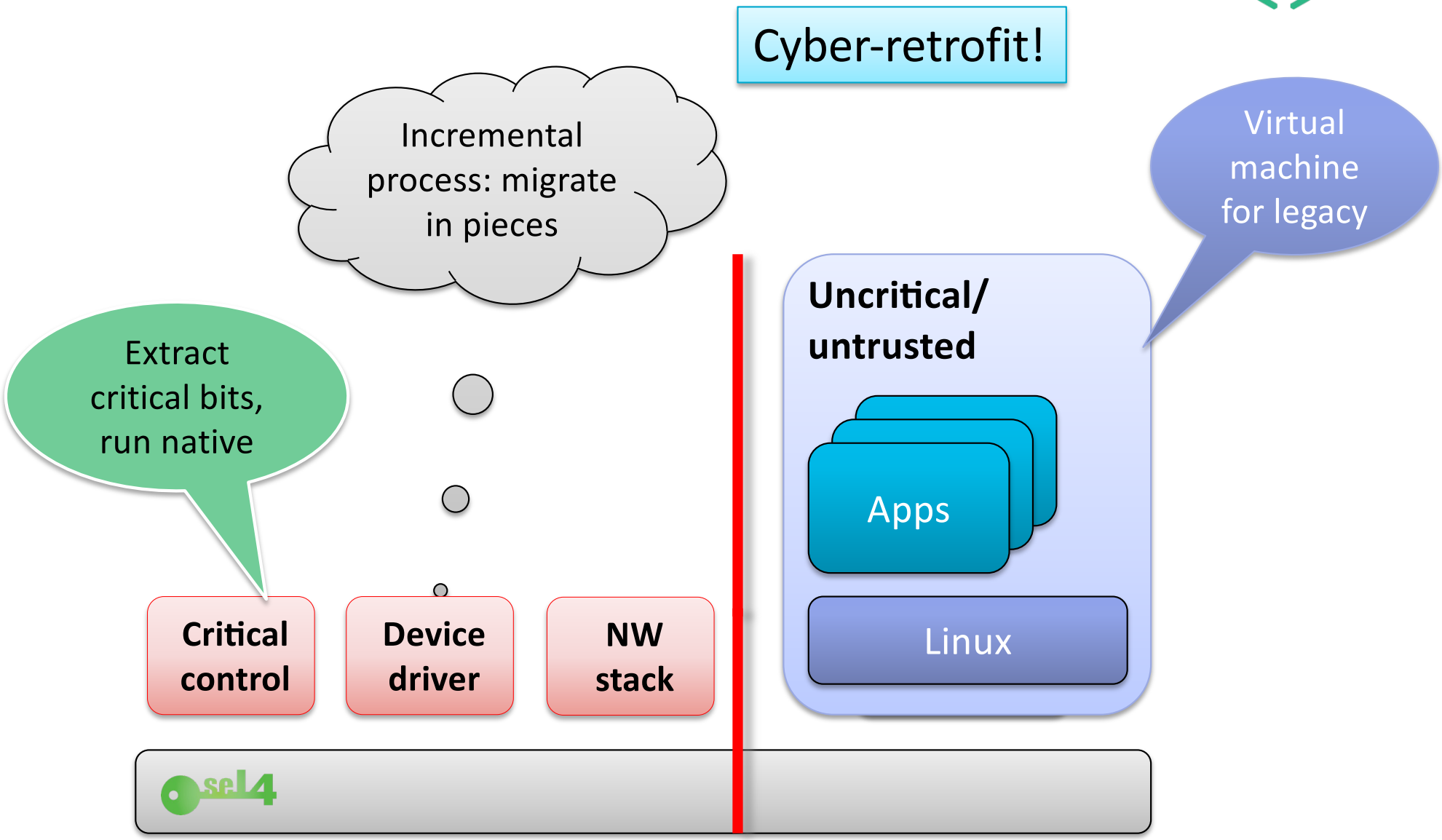
How Does seL4 Compare?

"World's most verified kernel"

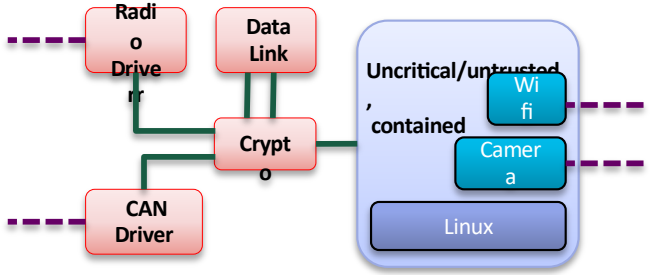
"Software you can depend on, data access you can trust"

Feature	seL4 Open Source!	Others (RTOSes, hypervisors, separation kernels)
Performance	Fast	5-10X slower
Functional Correctness	Guaranteed (Proved)	No Guarantee
Isolation	Guaranteed (Proved)	No Guarantee
Worst-case latency bounds	Sound and Complete	Estimates only
Storage Side Channel Freedom	Guaranteed (Proved)	No Guarantee
Timing Channel Prevention	Low overhead	None or High Overhead
Mixed Criticality Support	Fully supported, High Utilisation	Limited, resource-wastive

Security by Architecture

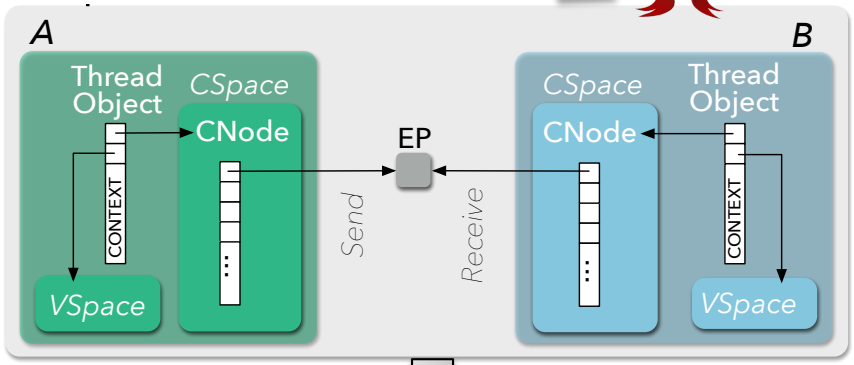


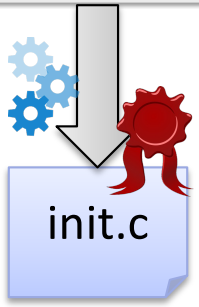
Enforcing the Architecture

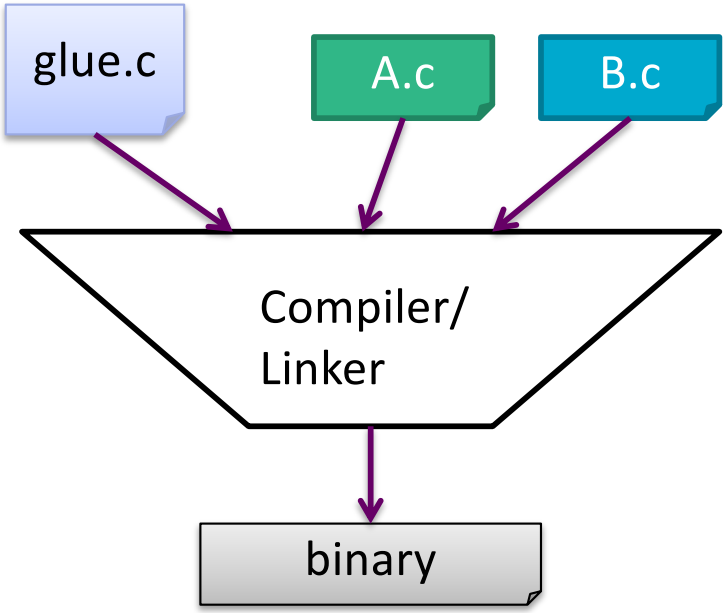


Architecture specification language

Low-level access rights







Real-World Use: DARPA HACMS

Boeing Unmanned Little Bird

Retrofit existing system!

US Army Autonomous Trucks

SMACCMcopter Research Vehicle

Develop technology

TARDEC GVR-Bot

Military-Grade Security

Cross-Domain Desktop Compositor

Multi-level secure terminal

- Successful defence trial in AU
- Evaluated in US, UK, CA
- Formal security evaluation soon

Pen10.com.au crypto communication device undergoing formal security evaluation in UK


DATA
61
Thank you!
Security is no excuse for poor performance!
Gernot Heiser | gernot.heiser@data61.csiro.au | @GernotHeiser
December 2017
http://sel4.systems
seL4
CSIRO