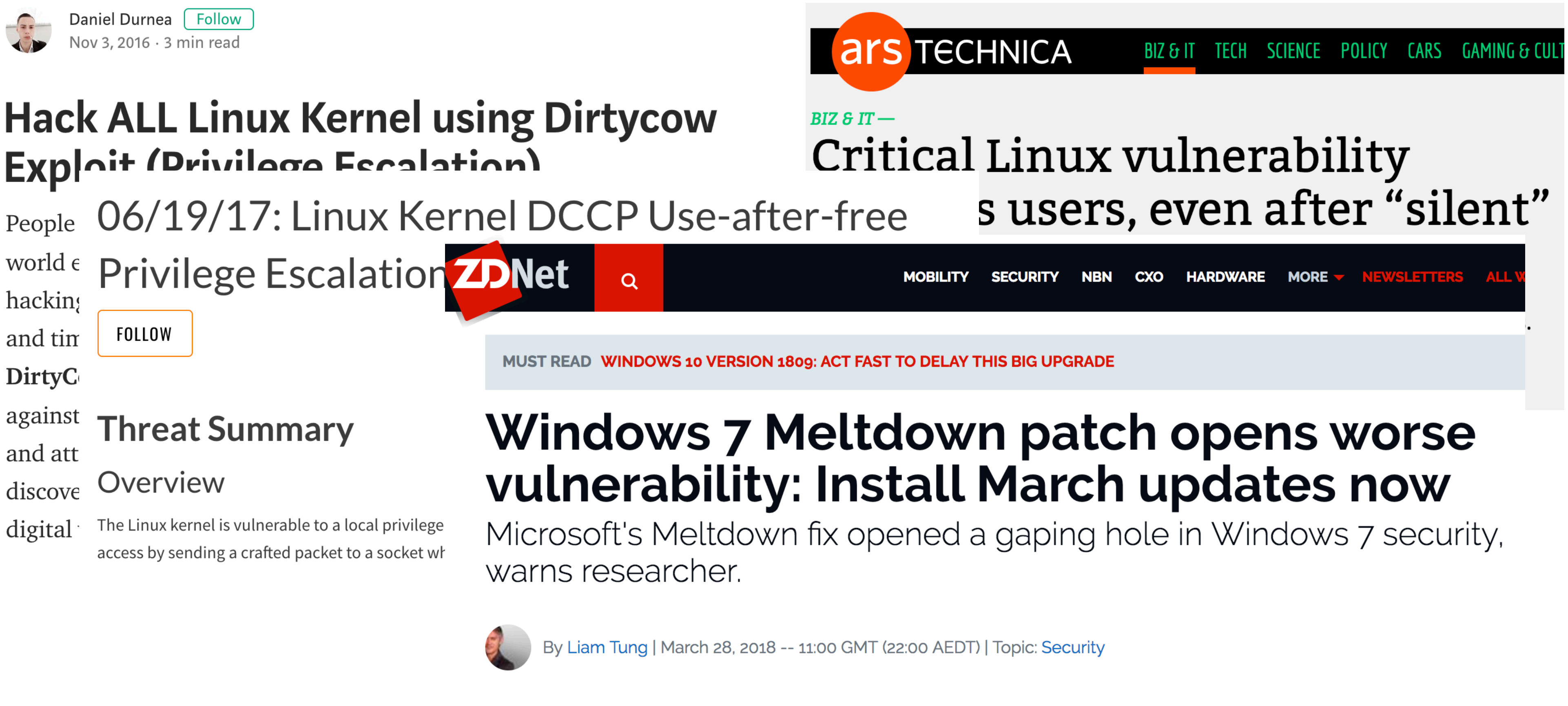
The Jury Is In: Monolithic OS Design is Flawed

Microkernel-based Designs Improve Security

Simon Biggs, Damon Lee, Gernot Heiser
gernot.heiser@data61.csiro.au | @GernotHeiser

https://trustworthy.systems

We’ve Seen It So Many Times…



Hack ALL Linux Kernel using Dirtycow Exploit (Privilege Escalation)

People
world e
hacking
and tim
DirtyC
against
and att
discove
digital

06/19/17: Linux Kernel DCCP Use-after-free Privilege Escalation

Threat Summary

Overview

The Linux kernel is vulnerable to a local privilege
access by sending a crafted packet to a socket wh

Critical Linux vulnerability
s users, even after “silent”

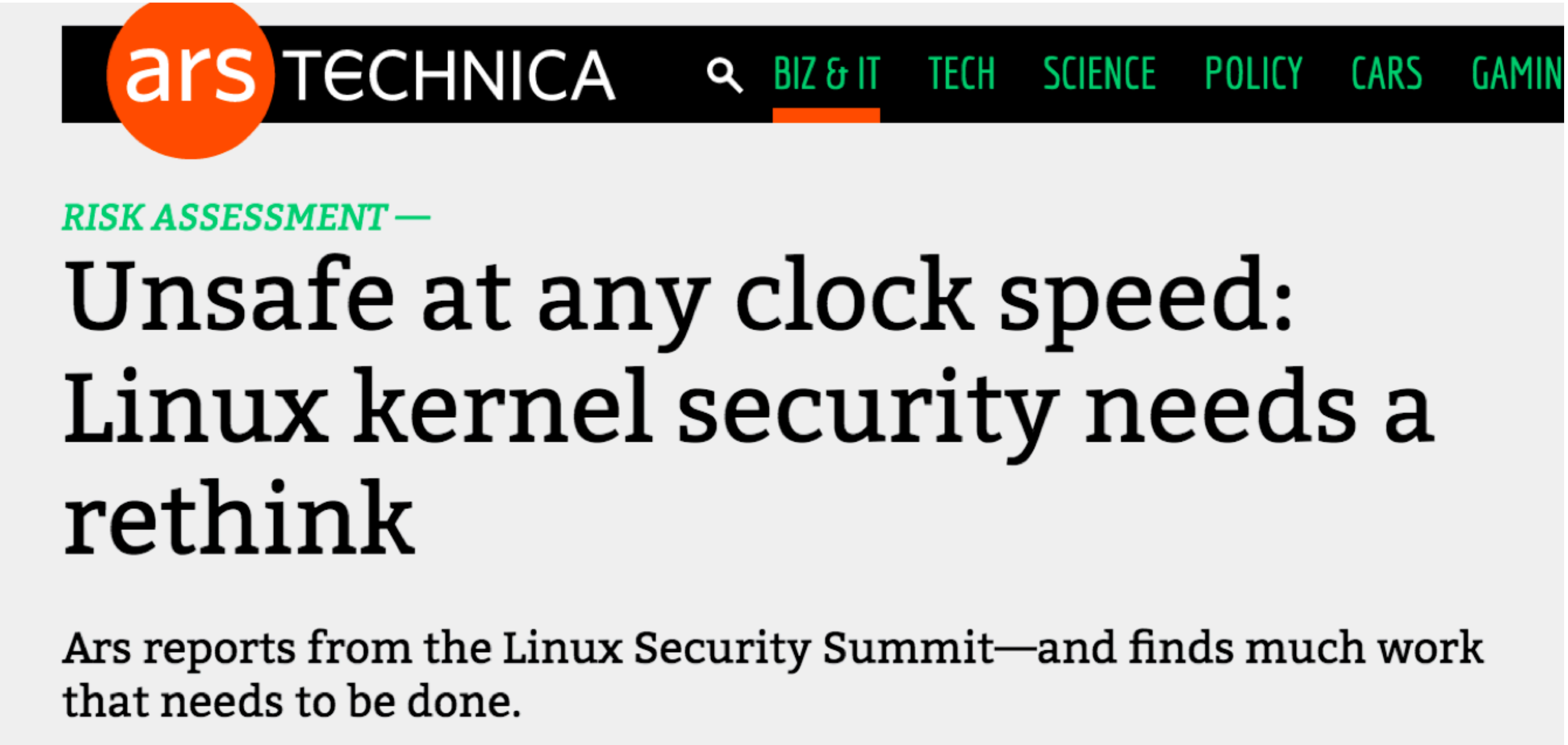
MUST READ WINDOWS 10 VERSION 1809: ACT FAST TO DELAY THIS BIG UPGRADE

Windows 7 Meltdown patch opens worse vulnerability: Install March updates now

Microsoft's Meltdown fix opened a gaping hole in Windows 7 security, warns researcher.

By Liam Tung | March 28, 2018 -- 11:00 GMT (22:00 AEDT) | Topic: Security

Linux “Security”



RISK ASSESSMENT —

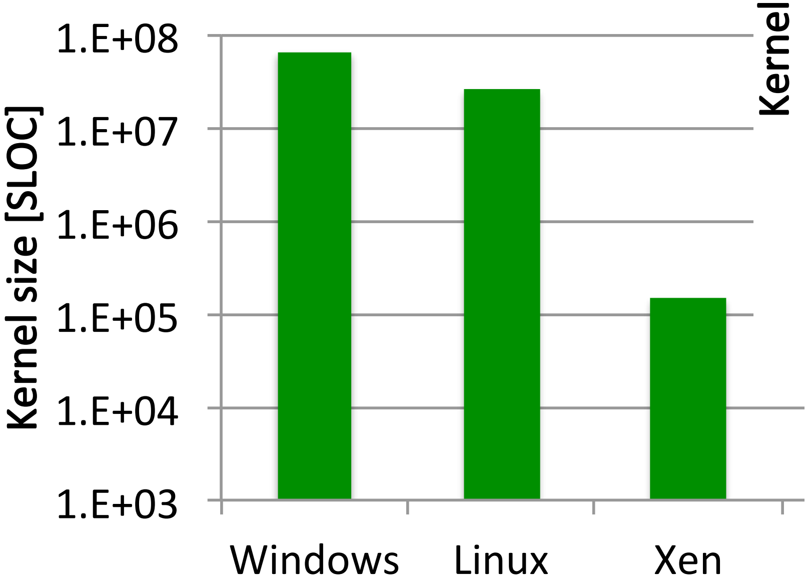
Unsafe at any clock speed: Linux kernel security needs a rethink

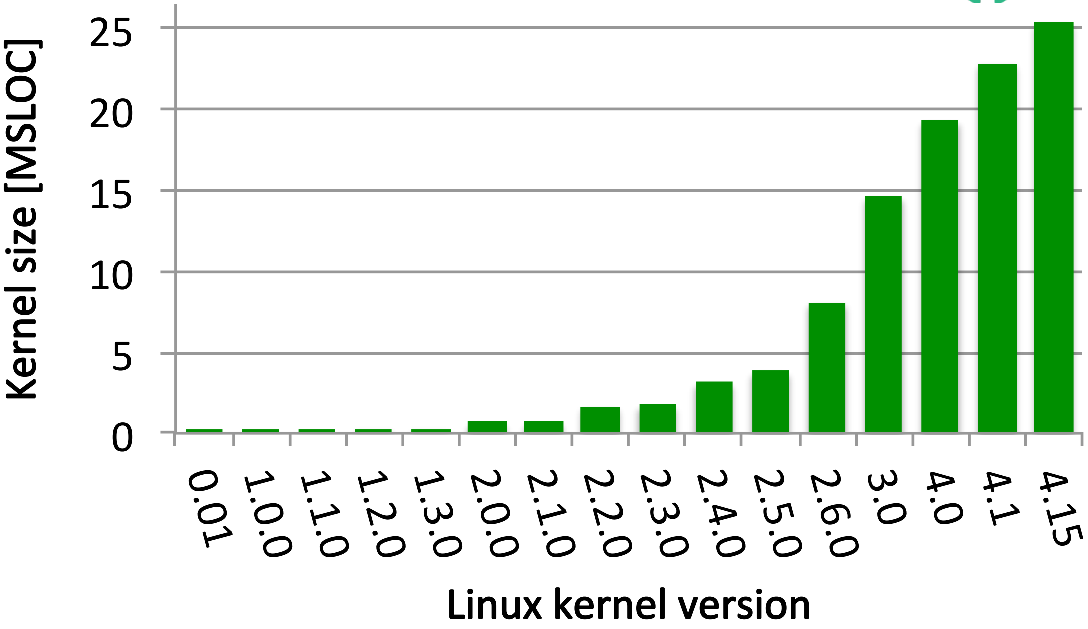
Ars reports from the Linux Security Summit—and finds much work that needs to be done.

Insecure by Design

"Quality" code:

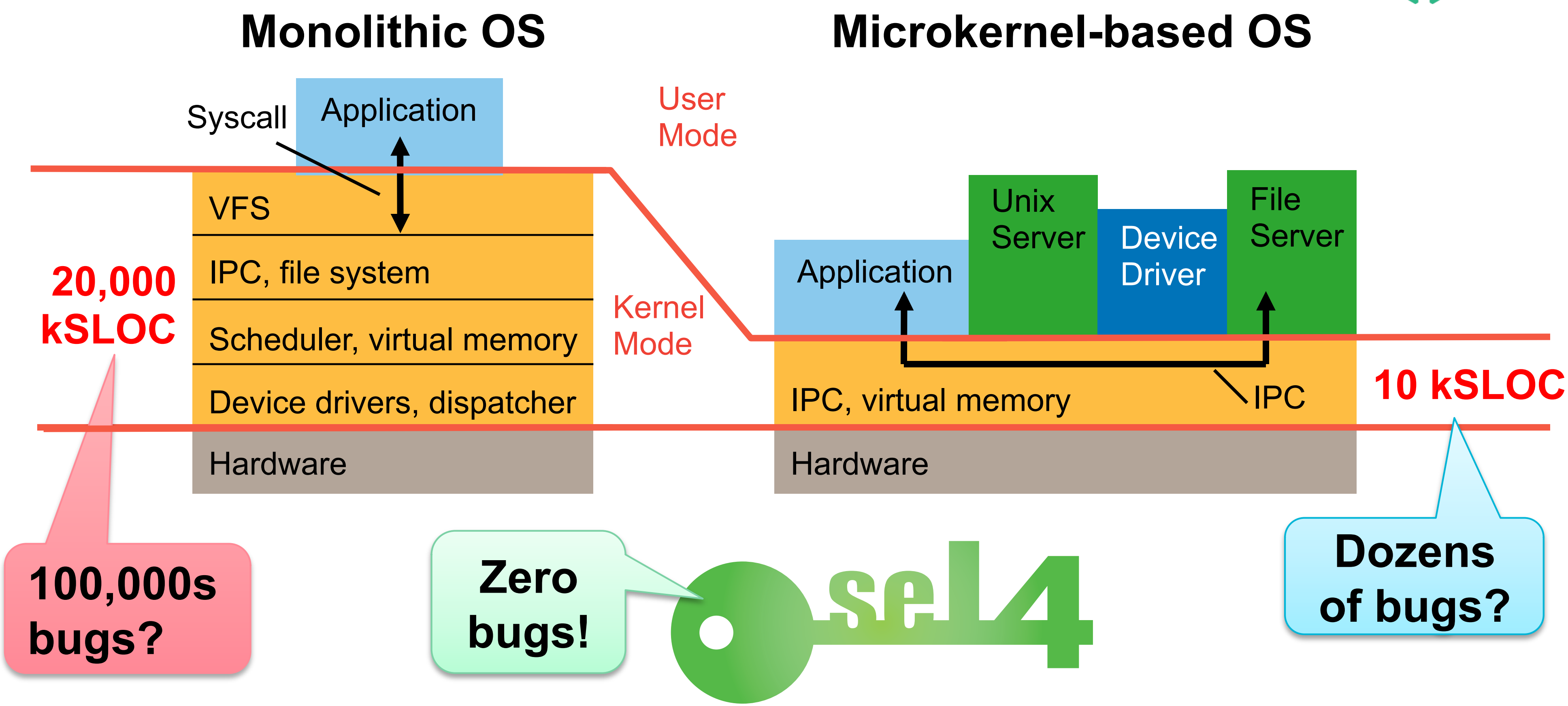
1–5 bugs/kSLOC





Large Kernels =
Disaster waiting to happen!

Alternative: Microkernels



Quantify OS-Design Security Impact

Approach:

- Examine all ***critical*** Linux CVEs (vulnerabilities & exploits database)
- For each establish how microkernel-based design would change impact

Finding:

- Almost all vulnerabilities eliminated or reduced in criticality

Approach

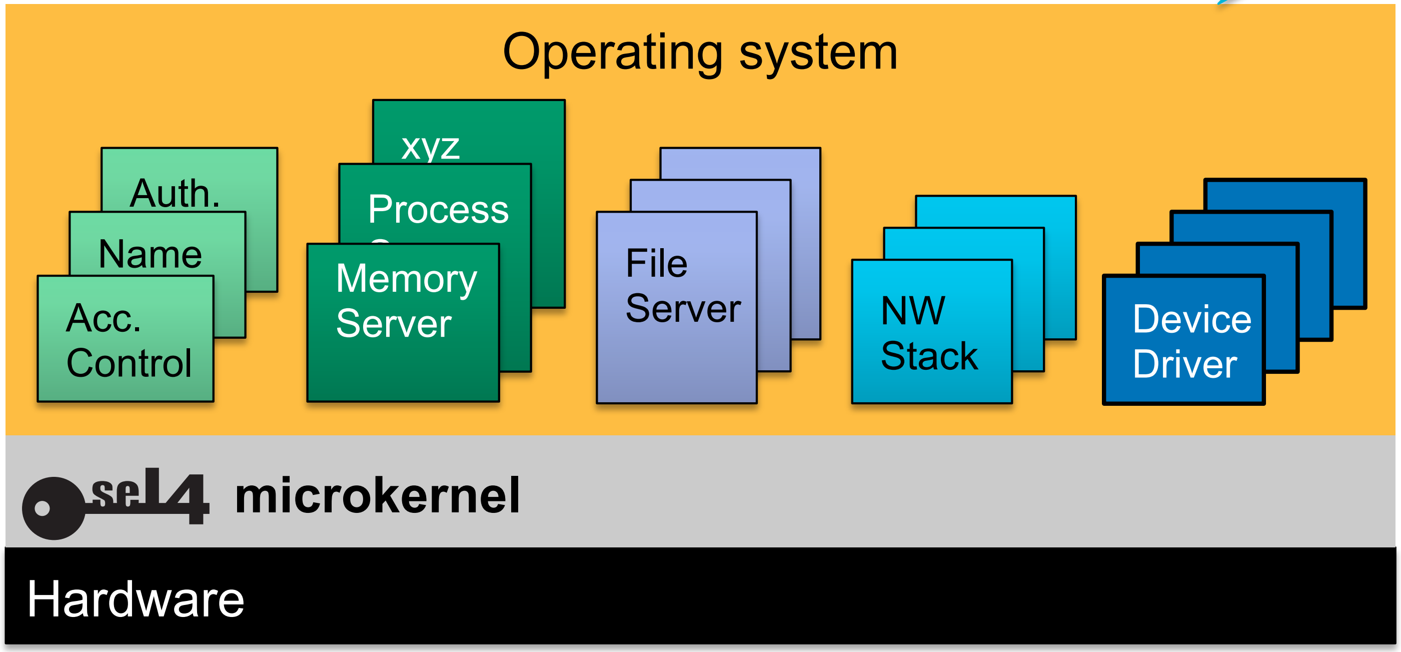
Analyse all *Critical* Linux CVEs

- All critical CVEs to November'17
- Critical:
  - easy to exploit
  - high impact
  - no defence available
  - confirmed

Hypothetical seL4-based OS

OS structured in *isolated* components, minimal inter-component dependencies, *least privilege*

Functionality comparable to Linux



Operating system

Auth.

Name

Acc. Control

xyz

Process

Memory Server

File Server

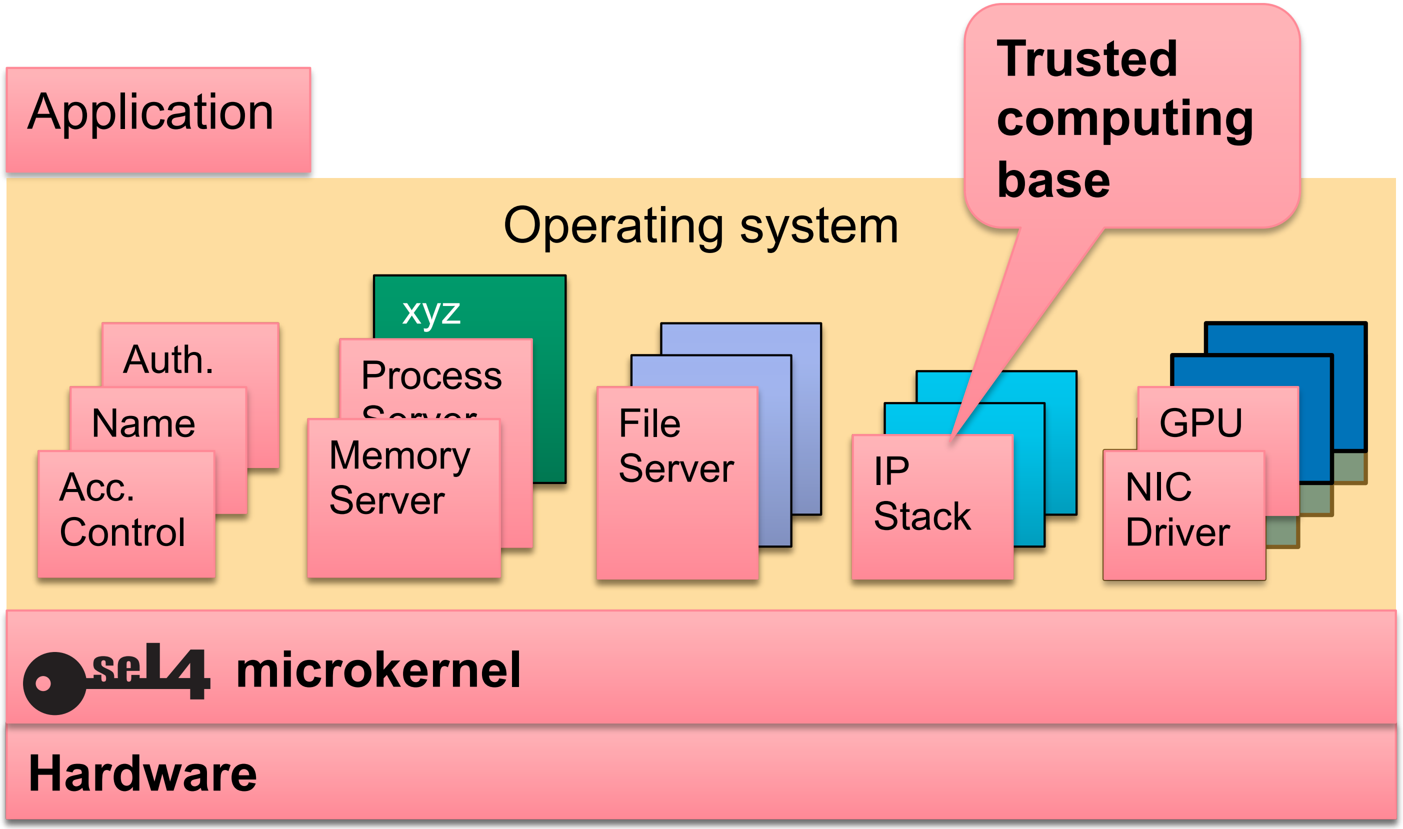
NW Stack

Device Driver

seL4 microkernel

Hardware

Hypothetical Security-Critical App

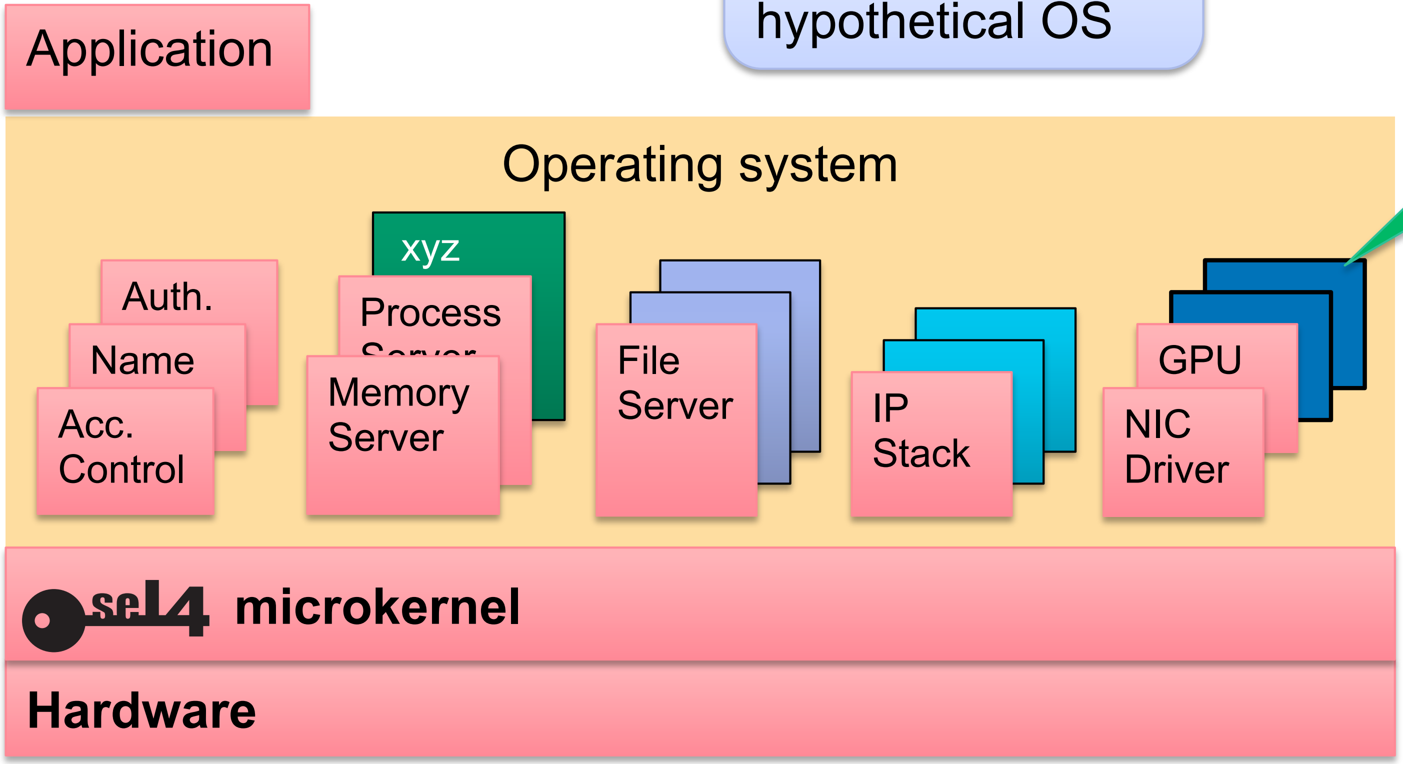


App requires:

- IP networking
- File storage
- Display output

Analysing CVEs

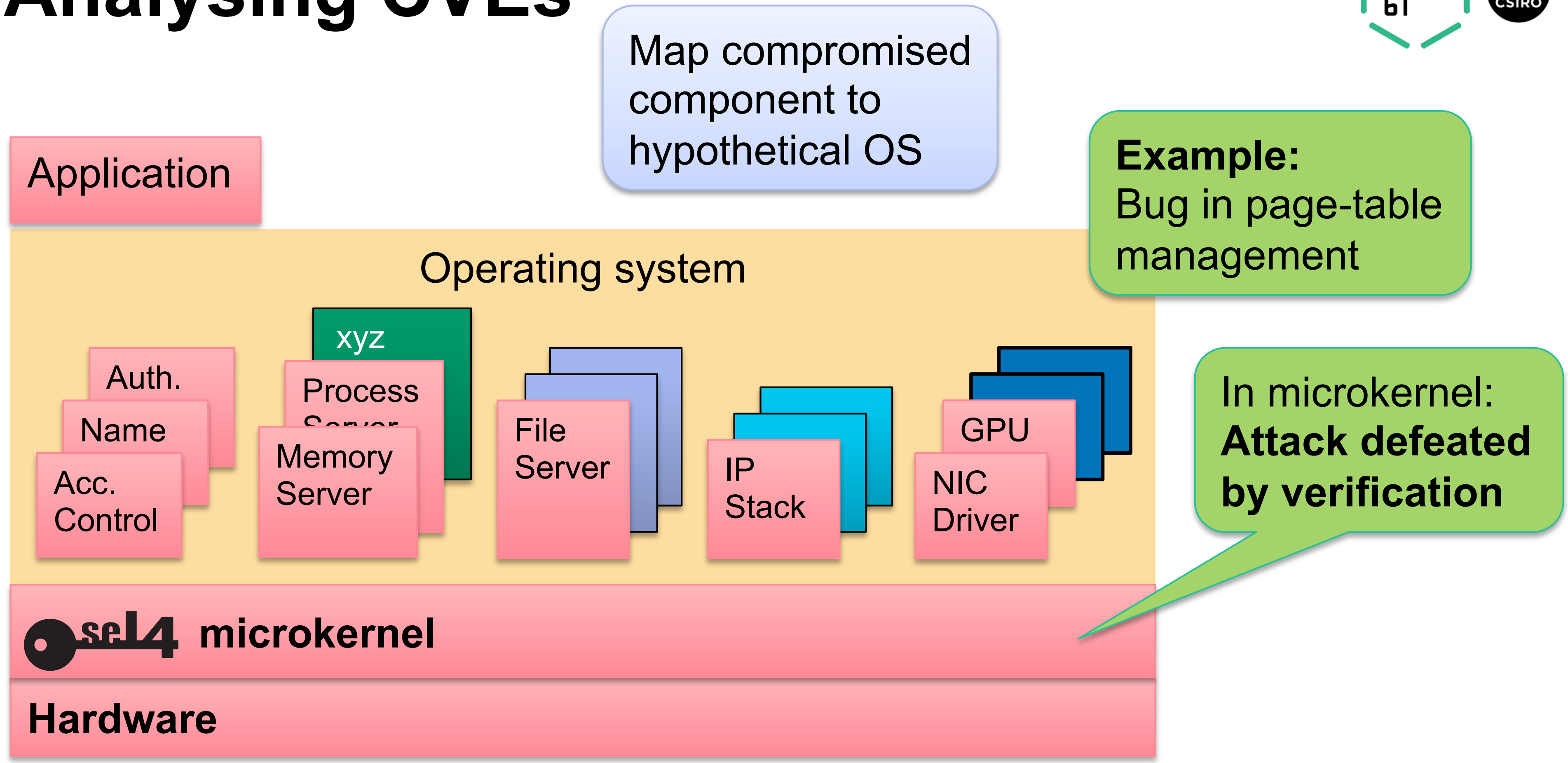
Map compromised component to hypothetical OS



Not in TCB: **Attack defeated**

Example: USB driver bug

Analysing CVEs

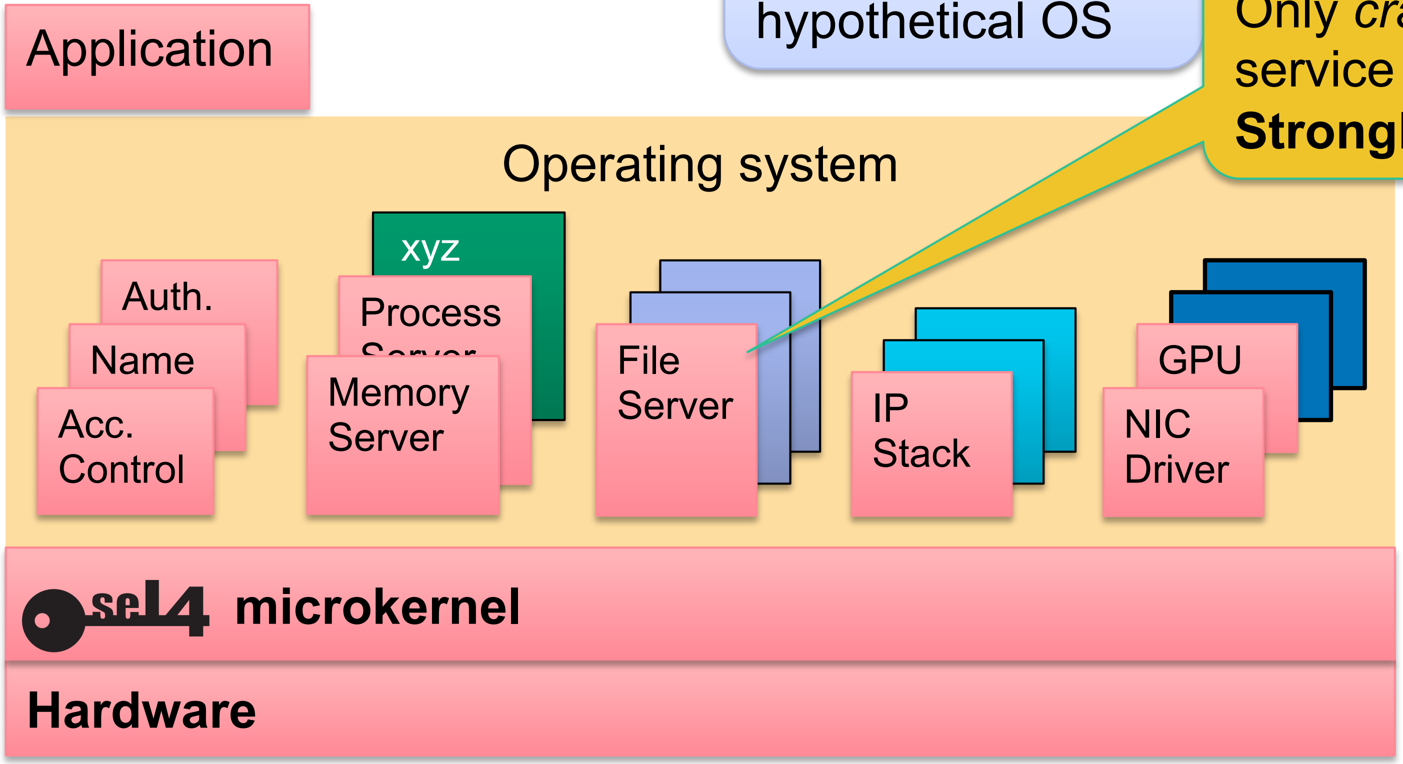


Map compromised component to hypothetical OS

Example:
Bug in page-table management

In microkernel:
Attack defeated by verification

Analysing CVEs



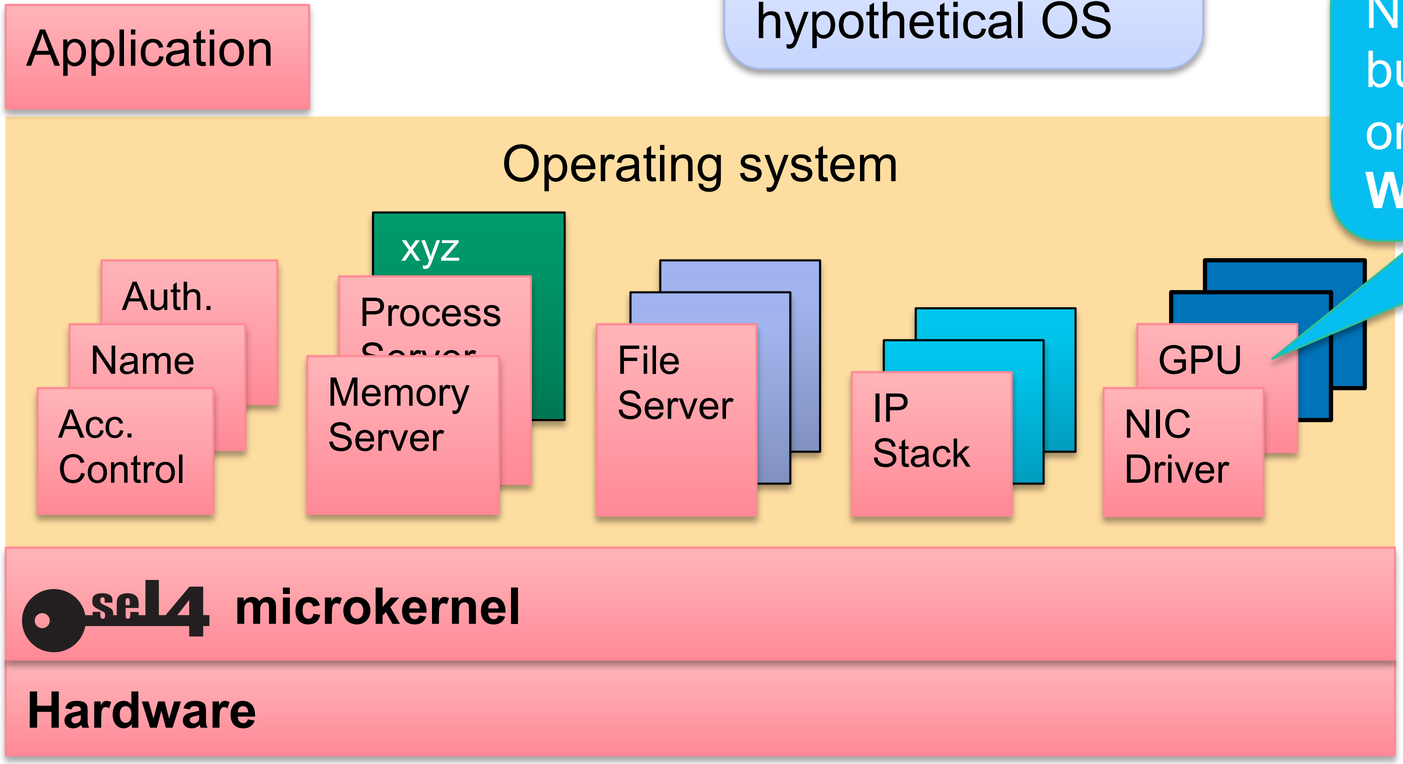
Map compromised component to hypothetical OS

Only *crash* essential service (availability): **Strongly mitigated**

Example: File system compromised

Analysing CVEs

Map compromised component to hypothetical OS

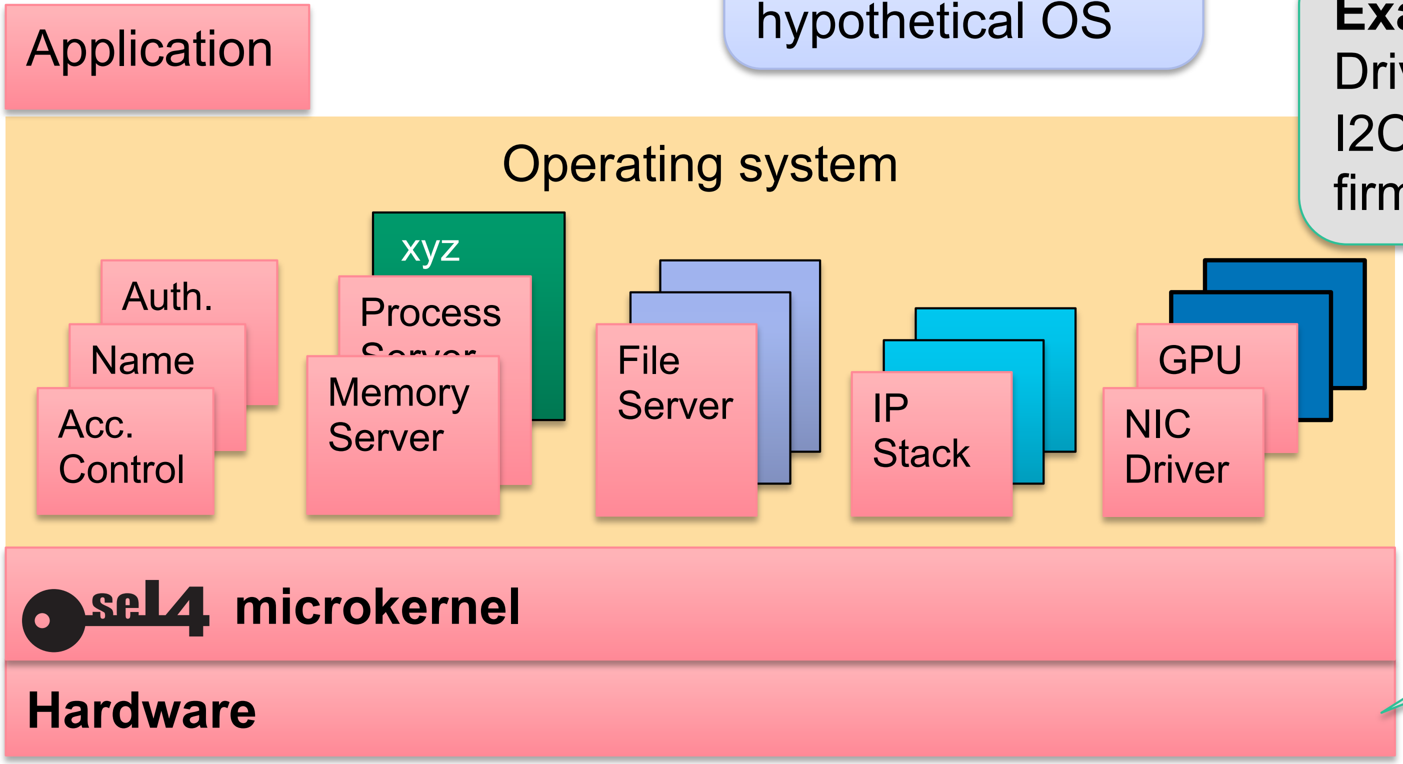


No full compromise, but violates integrity or confidentiality: **Weakly mitigated**

Example: GPU compromised

Analysing CVEs

Map compromised component to hypothetical OS



Application

Operating system

xyz

Auth.

Name

Acc. Control

Process Server

Memory Server

File Server

IP Stack

GPU

NIC Driver

seL4 microkernel

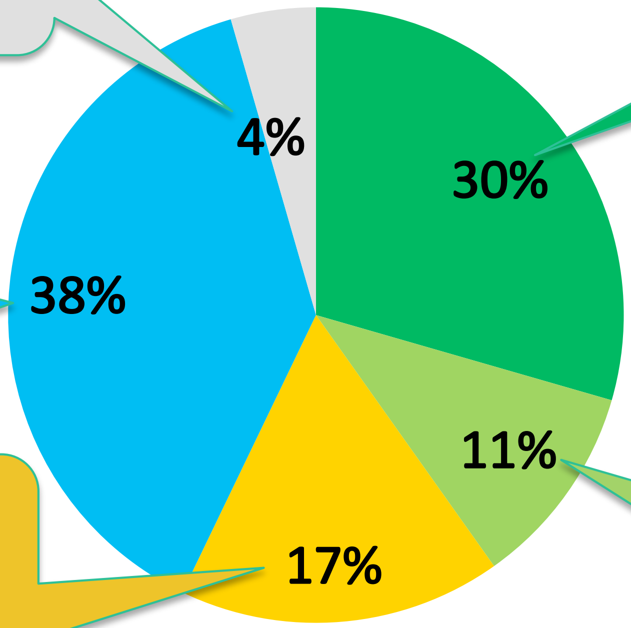
Hardware

Example:
Driver exploit hijacks I2C bus, allowing firmware reflush

Still full system compromise:
No effect

Results

All Critical Linux CVEs to 2017



Still full system compromise: **No effect**

Not in TCB: **Attack defeated**

No full compromise, but violates integrity or confidentiality: **Weakly mitigated**

- 41% eliminated
- 58% low severity
- 96% not *critical*

Only *crash* essential service (availability): **Strongly mitigated**

In microkernel: **Attack defeated by verification**

Summary

OS structure matters!

- Microkernels definitely improve security
- Monolithic OS design is fundamentally *flawed from security point of view*

Use of a monolithic OS in security- or safety-critical scenarios is professional malpractice!

Thank You

Simon Biggs, Damon Lee, Gernot Heiser

gernot.heiser@data61.csiro.au | @GernotHeiser

https://trustworthy.systems