Protecting *e*-Government Against Attacks

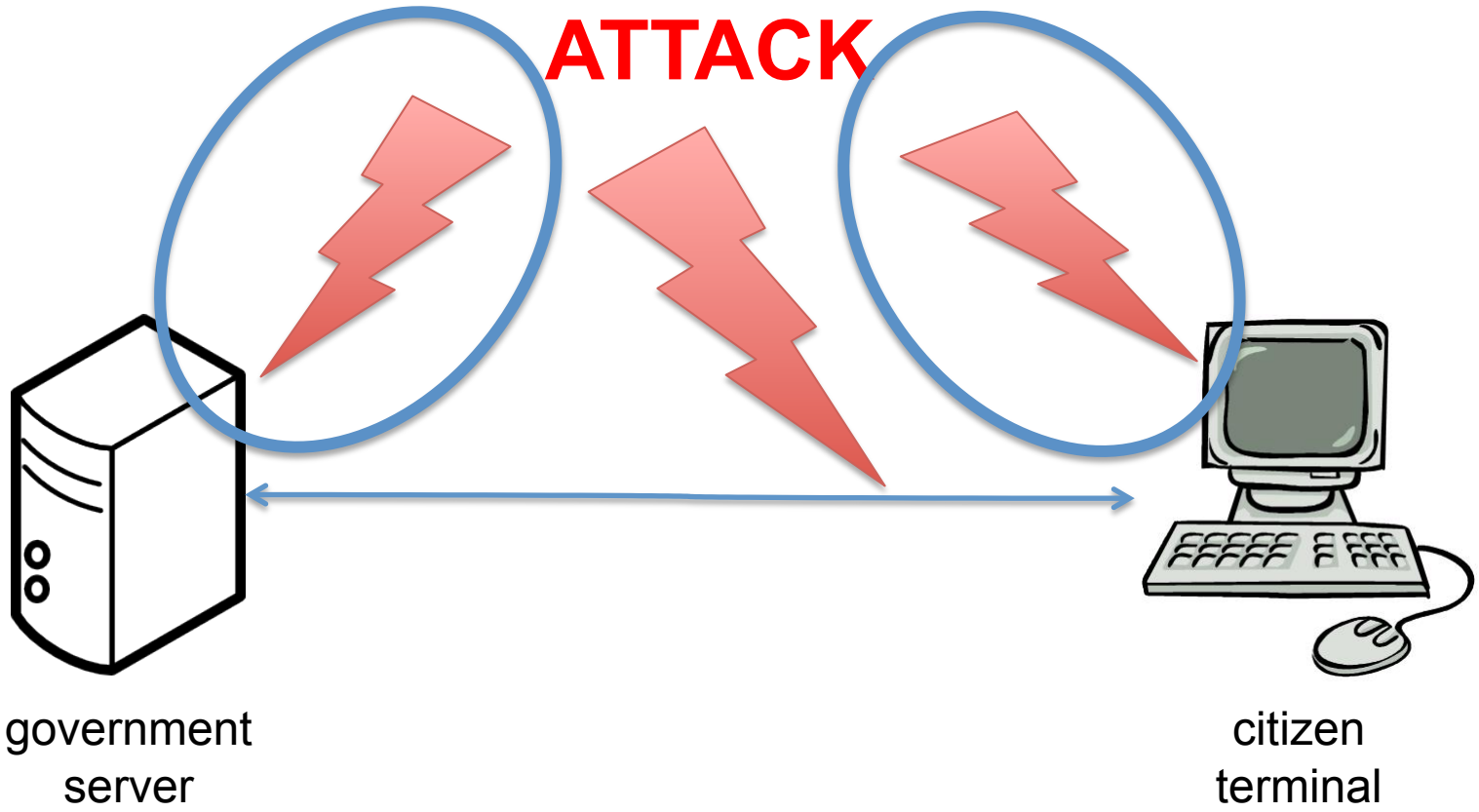
Gernot Heiser

NICTA and University of New South Wales

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

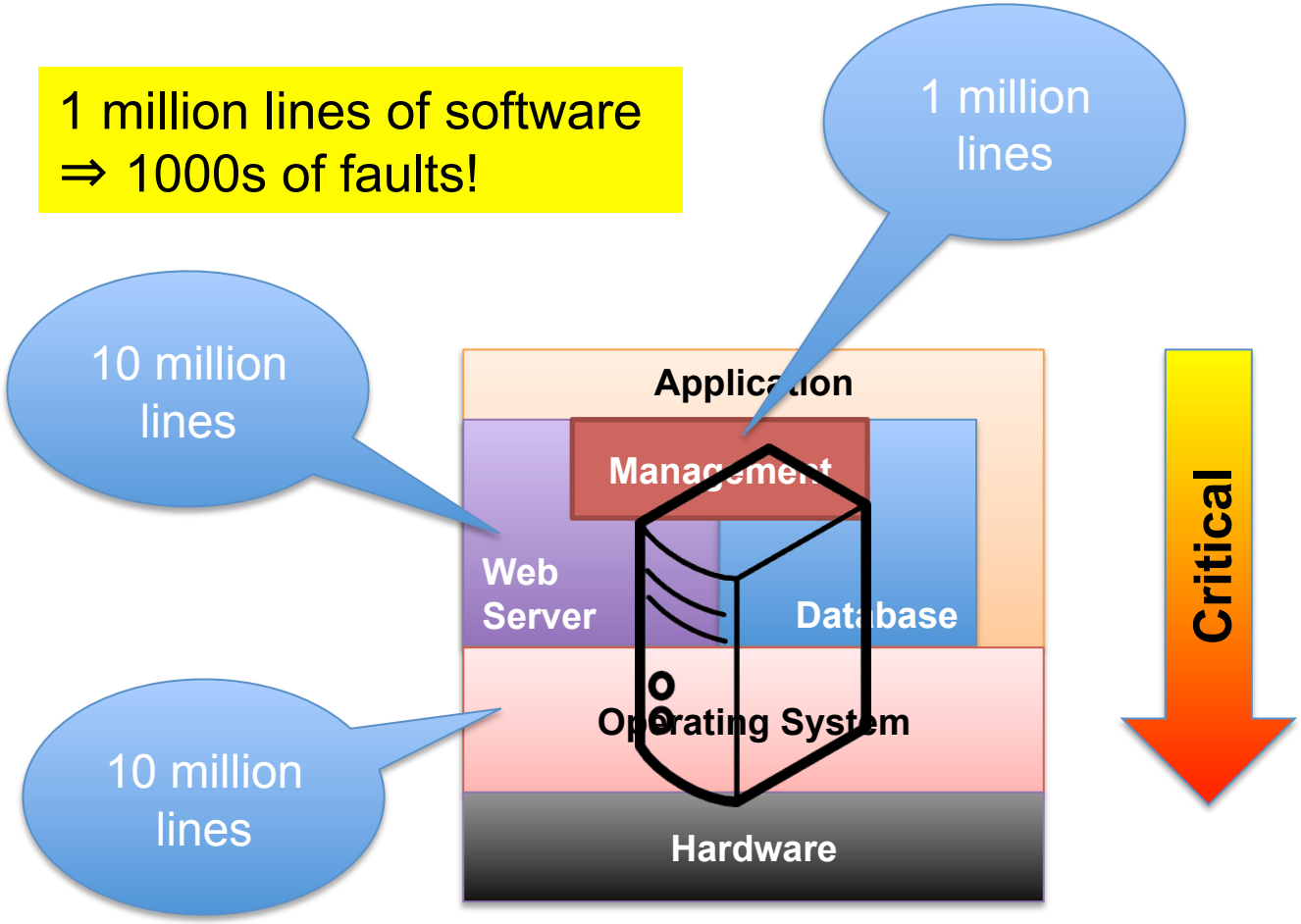
NICTA Funding and Supporting Members and Partners

e-Government Threats



Software Complexity and Attack Surface

1 million lines of software
⇒ 1000s of faults!

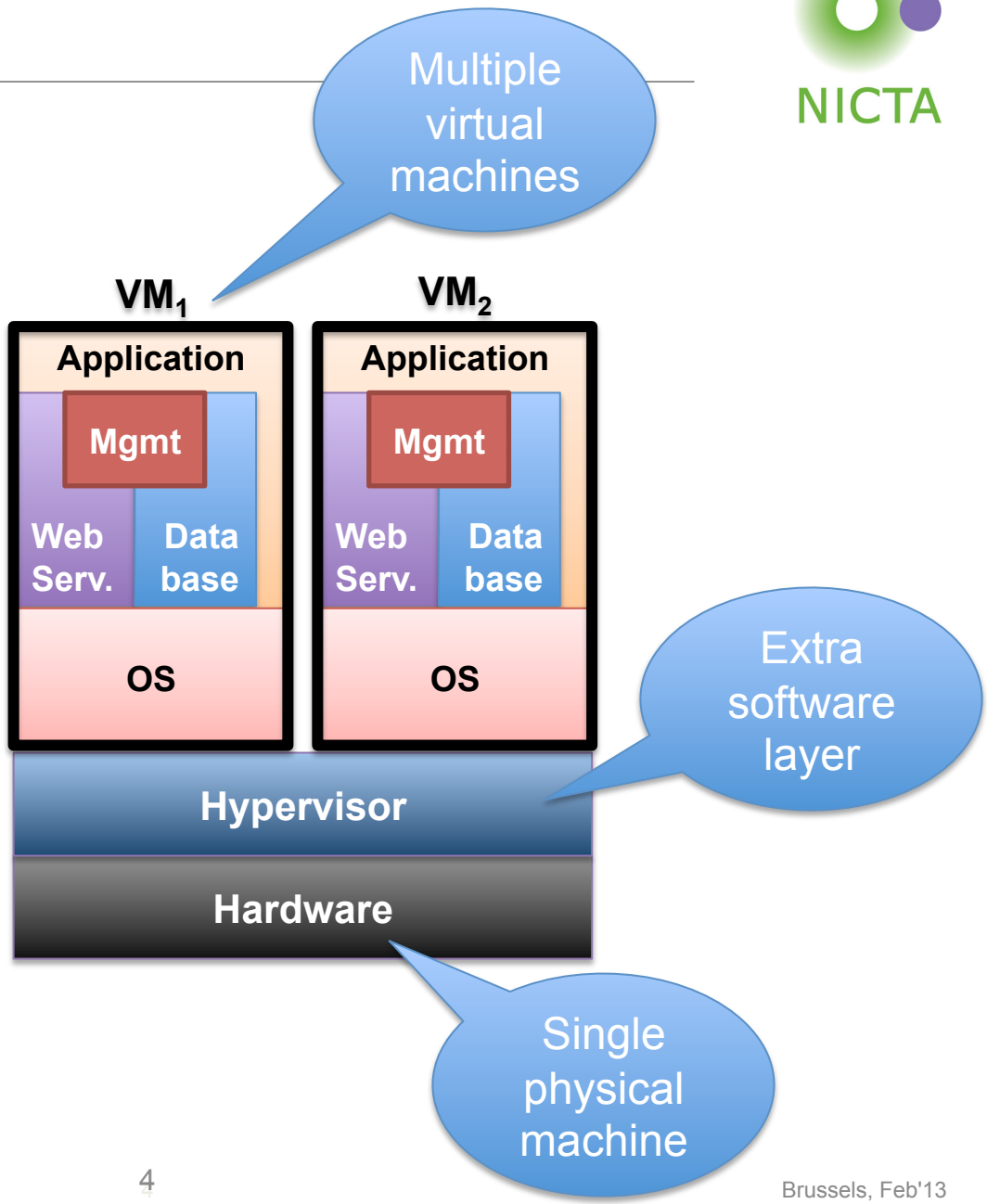


In security-critical software,
>10% of faults become vulnerabilities

Virtualization

Advantages:
- server consolidation
- reduced management cost
- improved utilisation
- reduced energy use

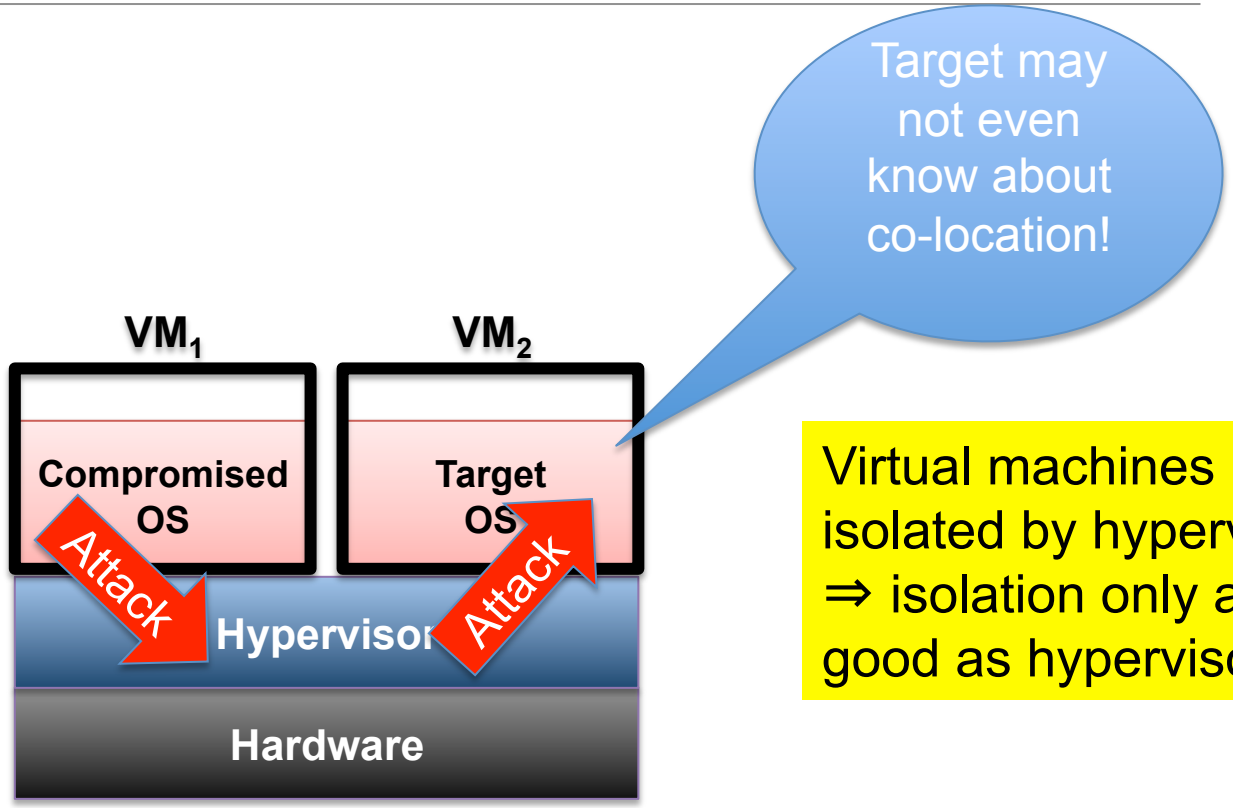
Disadvantages:
- increased attack surface



Attack Surface

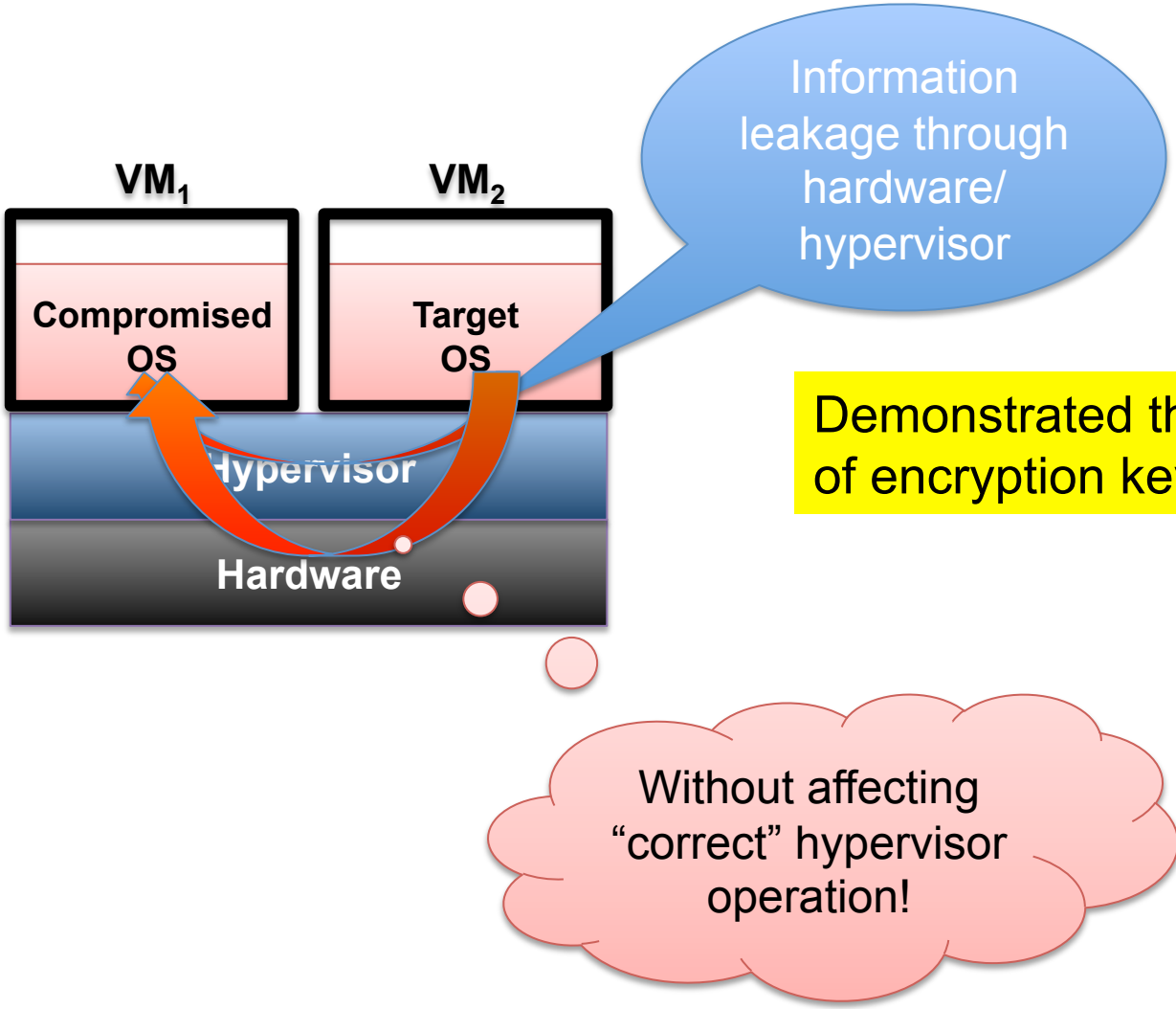
Component	Total size	Critical part	Vulnerabilities
Management	1 MLOC	1 MLOC	100s
Web server, database, application	10 MLOC	1 MLOC	100s
Operating System	10 MLOC	10 MLOC	1000s
Hypervisor	1 MLOC	1 MLOC	100s

Virtualization Attacks: Server-to-Server

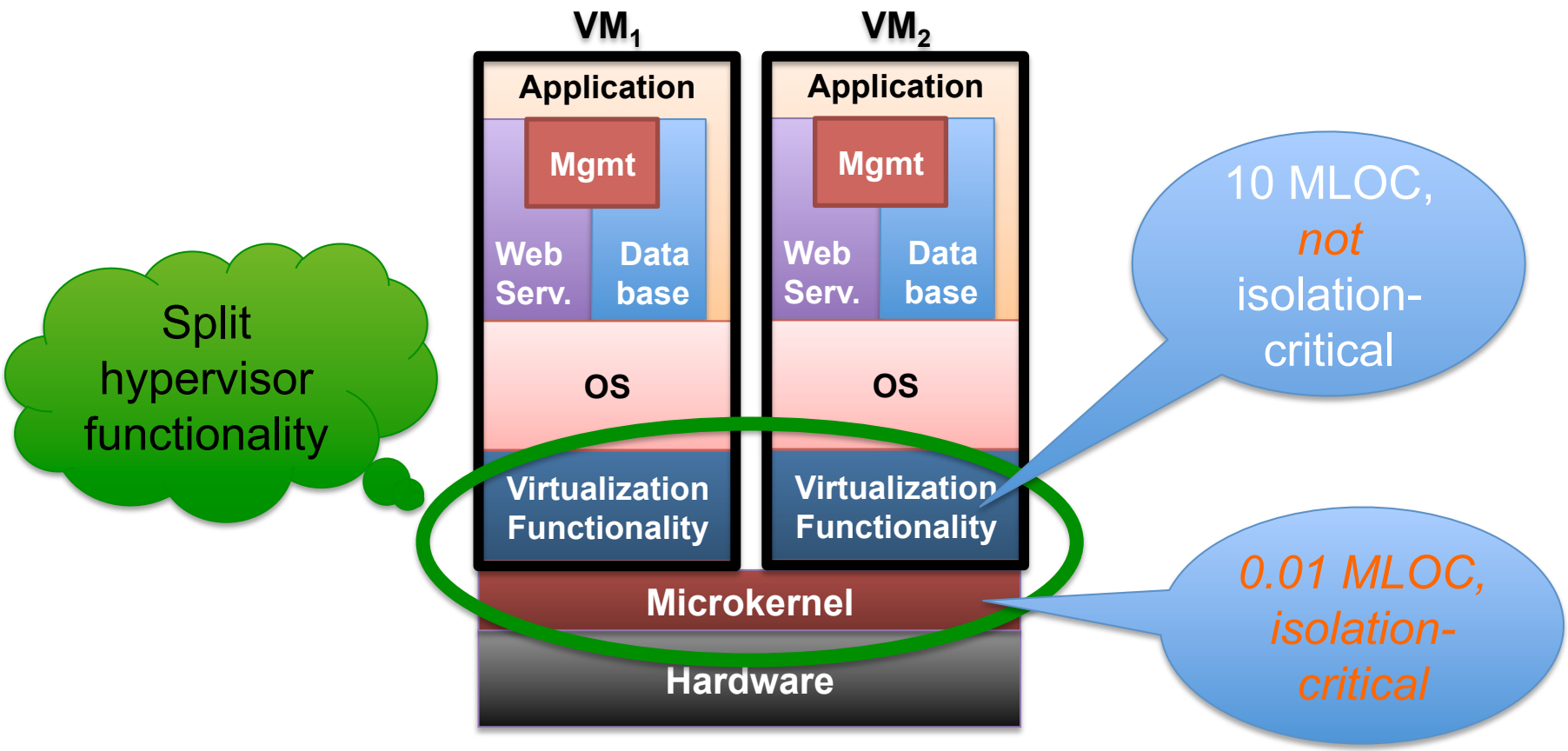


Virtual machines isolated by hypervisor ⇒ isolation only as good as hypervisor

Virtualization Attacks: Side Channels



Decrease Attack Surface: Microkernels



Microkernels

Track record:

- OKL4 microkernel deployed on > 1.5 billion mobile devices
- Developed by NICTA, marketed by Open Kernel Labs

Unparalleled security potential:

- 10,000 lines ⇒ minimal vulnerabilities
- Small enough to *prove* absence of faults

NICTA's seL4 microkernel:

First and only operating-system with *proof* that operation is always according to specification

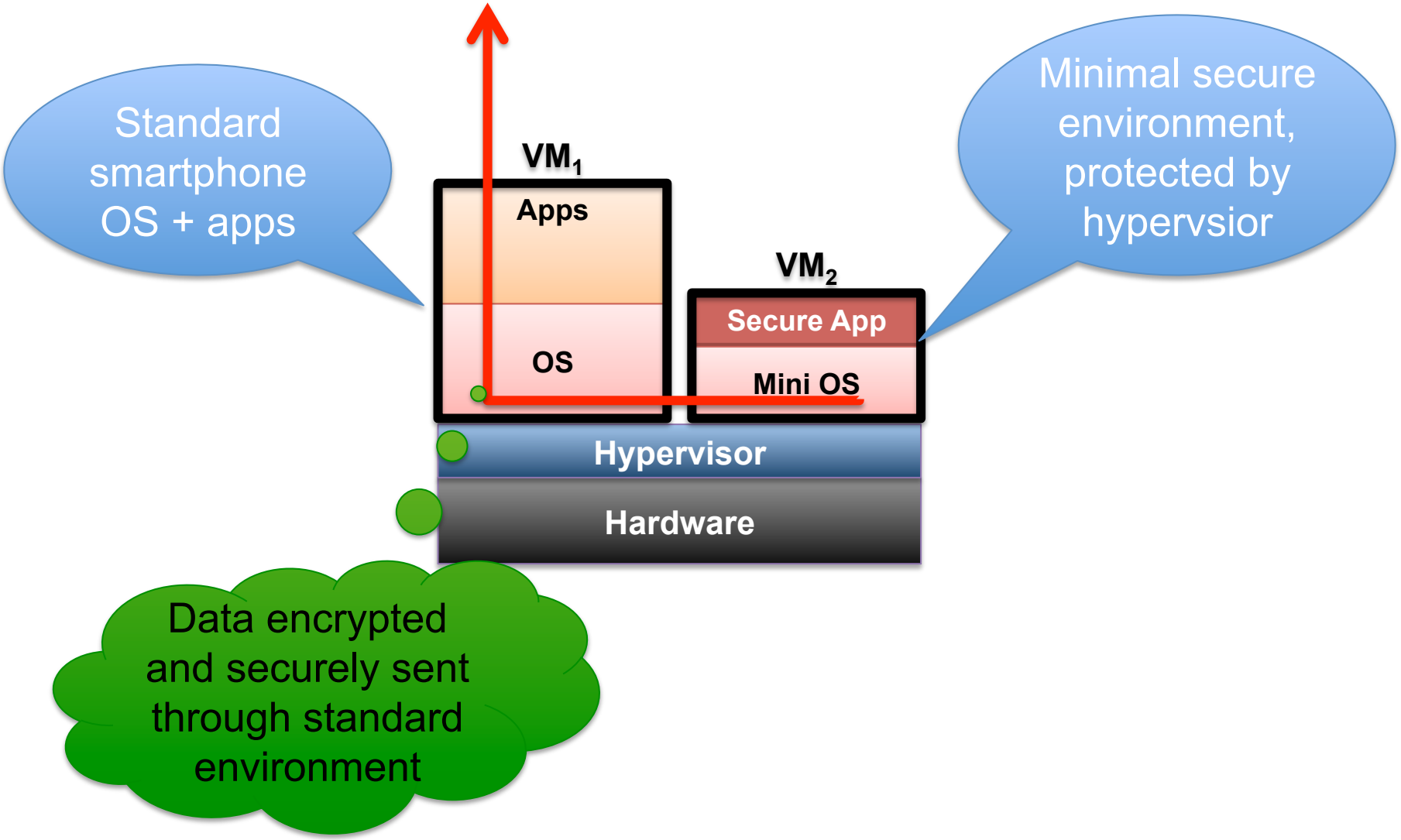
… and as fast as *any* microkernel!

Terminals

Bigger challenge than servers

- Live in uncontrolled environments
- Run large amounts of untrusted software
- Large percentage infected by malware
- Cannot be trusted to keep secrets!

Protecting Terminals – With Virtualization!



Recommendations

NICTA

1. Require *provably* secure virtualization technology (after transition period)
   - provide incentive to industry for delivering secure products

2. Fund development of open-source *provably* secure virtualization technology (equivalent to seL4)
   - avoid private monopoly for critical infrastructure

3. Require certified secure communication functionality on terminals accessing e-government services (after transition period)
   - provide incentive to industry for delivering secure products