e-Government Threats

ATTACK

government server

citizen terminal

©2013 Gernot Heiser, NICTA
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

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

Disadvantages:
• increased attack surface

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

Disadvantages:
• increased attack surface
### Attack Surface

<table>
<thead>
<tr>
<th>Component</th>
<th>Total size</th>
<th>Critical part</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>1 MLOC</td>
<td>1 MLOC</td>
<td>100s</td>
</tr>
<tr>
<td>Web server, database, application</td>
<td>10 MLOC</td>
<td>1 MLOC</td>
<td>100s</td>
</tr>
<tr>
<td>Operating System</td>
<td>10 MLOC</td>
<td>10 MLOC</td>
<td>1000s</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>1 MLOC</td>
<td>1 MLOC</td>
<td>100s</td>
</tr>
</tbody>
</table>
Virtualization Attacks: Server-to-Server

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

Target may not even know about co-location!
Virtualization Attacks: Side Channels

Information leakage through hardware/hypervisor

Demonstrated theft of encryption keys

Without affecting “correct” hypervisor operation!
Decrease Attack Surface: Microkernels

Split hypervisor functionality

10 MLOC, not isolation-critical

0.01 MLOC, isolation-critical
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!

- Standard smartphone OS + apps
- Minimal secure environment, protected by hypervisor
- Data encrypted and securely sent through standard environment

©2013 Gernot Heiser, NICTA
Recommendations

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