The SICS Hypervisor project for ARM project

Arash Vahidi
SICS Security Lab (SEC)
What is this all about?

● Embedded systems are getting more and more complex,

● **Security** issues are becoming critical,

● Virtualization technologies may be used as a security **enabler**.
What is a hypervisor?

And a few words about the SICS hypervisor...
Virtualization?
Virtualization?

Type 2

- VMware
- Virtual PC
- VirtualBox
- Hypervisor
- Host OS
- Hardware

Applications

OS

OS
Virtualization?

Type 1

OS

Hypervisor

Hardware

Type 2

OS

Hypervisor

Host OS

Hardware
Uses of hypervisors (1)
Uses of hypervisors (2)

- OS: ~15 MLOC
- Hypervisor: ~6 KLOC
- Hardware:
  - UART
  - Ethernet
  - Flash
  - EEPROM
Uses of hypervisors (3)
Uses of hypervisors (4)
Uses of hypervisors (5)
Hypervisor requirements.

or

Can I use this in my current project?
Virtualization requirements (1)

Bad
- Microchip PIC12/16/18
- Motorola 68K
- Intel 8051
- Atmel AVR

Good
- Motorola 68K10
- AMD64 (x86-64)
- Intel x86
- MIPS32
- MIPS64

Best
Virtualization requirements (2)

<table>
<thead>
<tr>
<th>Bad</th>
<th>Good</th>
<th>Best</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARMv4 (ARM7)</td>
<td>ARMv5 (ARM9)</td>
<td>ARMv8 e.g. Cortex-A57</td>
</tr>
<tr>
<td>???</td>
<td>ARMv6 (ARM11)</td>
<td>Cortex-A15</td>
</tr>
<tr>
<td>ARMv7 profiles R &amp; M</td>
<td>ARMv7 profile A e.g. Cortex-A8</td>
<td></td>
</tr>
</tbody>
</table>

SICS hypervisor primary targets
So there is no free lunch...

What are the costs of virtualization?
Performance degradation?

- Virtualization introduces an overhead
- Virtualization does affect your real-time performance slightly (added latency)
- Depending on the system and the application, this overhead can be significant or negligible
- SICS hypervisor: a 2-20% increase of running time was measured in various applications
Hypervisor footprint?

- Unless for very small systems, the added footprint of a hypervisor is negligible.

- SICS hypervisor: a 8-32KB code, 4KB - 1MB memory on ARM.

- ARM Virtualization Extensions can significantly reduce these numbers (i.e. Cortex-A15 and newer).
Code complexity?

- The hypervisor itself is tiny (few KLOC, we have seen as little as 600 LOC in research versions).
- The guest OS can be run on top of the hypervisor without any modification. This could however result in very poor performance.
- With some changes to the guest OS, one may increase the performance significantly.
  - For a 2.6 Linux kernel, these modifications can be as little as 800 LOC. Newer kernel versions may require even less changes!
How about MIPS, PPC, XYZ?

- Hypervisors are inherently platform dependent
- However, we have done our best to make the SICS hypervisor easy to port
  - ARM
  - MIPS in progress
- Talk to me if you are working with other architectures
THE END
Questions?