Hypervisor development with ARM Virtualization Extensions

A master thesis project at the SICS Security Lab

Background

Complex embedded systems are being used more and more and can be found nearly everywhere in our modern life. Unfortunately, security issues are often ignored during development of such systems.
Virtualization techniques allow one to add a secondary layer of software to existing systems, which can be used to provide the missing security services such as isolation and monitoring.
SICS is currently working on a virtualization solution, a hypervisor, for secure embedded systems. With this master thesis we would like to extend the existing version of our hypervisor for ARM to take advantage of the newly introduced Virtualization Extensions (ARM-VE).

Objectives

In the current revision of the ARM architecture a number of functions have been introduced to ease OS and hypervisor development. The most important ones are:

- Addition of a virtual interrupt controller
- CPU privilege levels have been increased from two to three (user, privileged and hypervisor)
- Memory management hardware has been extended with a 2nd translation layer (intermediate physical).

In this thesis we would like to examine the effect of these enhancements on (1) security, (2) performance and (3) footprint (code size and run-time characteristics). For comparison, we will use the SICS Thin Hypervisor for ARM.

In total, the thesis consists of the following items:

1. Analyse security and performance aspects of ARM-VE,
2. Enhance the existing SICS Thin Hypervisor for ARM to support ARM-VE. Measure performance and compare it to the original version of the hypervisor. Analyse the effects of ARM-VE on code density and design simplicity
3. Provide a written report.

Implementation will be carried out on a simulated ARM Cortex-A15 model provided by Imperas.

Competence

We are looking for **one or two** bright MSc students in **Lund or Kista (Stockholm)** who meet the following requirements:

1. Basic knowledge in C and assembly (advanced knowledge is a plus)
2. Knowledge in modern CPU architecture, preferably ARM and MIPS.
3. Knowledge in operating system architectures
4. Good spoken and written English

Applications

Applications should include a brief personal letter, your CV with your education, professional experience and specific skills and recent grades. In your application, make sure to give examples of previous programming or other projects that you consider relevant for the position. Candidates are encouraged to send in their application as soon as possible, in paper form or via e-mail. Suitable applicants will be interviewed as applications are received.

About SICS

SICS Swedish ICT is a leading research institute for applied information and communication technology in Sweden. We are a non-profit-distributing organization with main offices in Kista outside Stockholm and smaller offices in Uppsala and Lund. SICS employs approx. 140 researchers, including 45 PhDs, and hosts another 30 researchers from KTH, consultants and students working on their Master Thesis.

Contact

Arash Vahidi (arash@sics.se)
SICS, Ideon Science Park - β2
Scheelevägen 17
SE-223 70 Lund, Sweden

Contact:
Arash Vahidi, arash@sics.se, +46 (0)70-7731545
https://www.sics.se/groups/security-lab-sec