11th Seminar within the Framework of the Swedish IT Security Network for PhD students (SWITS 2011)

Oliver Schwarz

“DMA Virtualization and Hypervisor Verification”

ABSTRACT

Computer systems get more and more complex. This applies even to embedded systems. While commodity operating systems generally fail to provide sufficient security for the software they are running, virtualization arises as one approach to assure isolation between trusted and non-trusted software. Those parties, in virtualization commonly called guests, can be separated from each other by means of the Memory Management Unit (MMU). Recent research work has shown successfully that virtualization can be used to secure computer systems. However, embedded systems are often not covered by those approaches. A special threat to all virtualized systems is the presence of Direct Memory Access (DMA) functionality. DMA allows fast copying between peripherals and memory or within memory and became essential in modern architectures. Unfortunately it provides a way for attackers to circumvent the MMU. Many solutions to this problem are present today, yet nearly all of them demand special hardware support as for example the presence of an IOMMU. However, this is not always provided, especially not on embedded platforms. The presentation will describe an approach for securing DMA on ARMv5 processors. The main contribution consists in a solution purely based on software. No additional hardware is needed. Instead the protection of the DMA controller is realized with means of a standard ARM MMU only.

Furthermore the presentation will give some first impressions on verifying this solution with formal methods, more precisely theorem proving. While modern operating systems are just too complex for verification, software providing virtualization, so called hypervisors, are thinner and thus an interesting target for proving correctness. However, compared to software on application level they evoke new challenges and questions in respect to verification.