Mobile Trusted Computing

Jan-Erik Ekberg

Nokia Research Center, Helsinki
Email: jan-erik.ekberg@nokia.com

Abstract

Trusted Computing (TC) denotes a set of security-related hardware and software mechanisms that makes a computing device work in a consistent manner, even in the presence of external attacks. For personal computers, TC typically is interpreted to be a software architecture designed around the Trusted Platform Module (TPM), a hardware chip residing on the motherboard and implemented according to the specifications of the Trusted Computing Group [7]. In embedded devices, the state of-the art in terms of hardware security and operating systems is significantly different from what is present on personal computers. So to stimulate the take-up of TCG technology on handsets as well, the recently approved Mobile Trusted Module (MTM) specification [8] defines new interfaces and adaptation options that match the requirements of the handset business ecosystem, as well as the hardware in use in the embedded domain.

The lecture will provide an overview of a few hardware security architectures in handsets - namely Texas Instruments' M-shield [6] and ARM TrustZone [1] - for introducing the problem domain. The main focus of the talk is the MTM specification - first presenting its main functional concepts [3], such as secure boot and key storage and binding. We will then examine an adaptation of the specification to one of the hardware architectures first described. Examples of security services that can be provided with MTM will also be discussed [10]. Finally, we will look at real-world MTM measurements from a legacy handset [4], as well as a few alternative approaches for achieving hardware-assisted security for applications in embedded devices [2][5].

REFERENCES

[1] ARM 1176 JZFS Technical reference manual. Retrieved April 27, 2009, from http://infocenter.arm.com/help/topic/com.arm.doc.ddi0301g/ DDI0301G arm1176jzfs r0p7 trm.pdf

[2] Ekberg J-E.& Asokan N. & Kostiainen K. & Rantala A. On-Board Credentials Platform Design and Implementation, Nokia Research Center Technical Report NRC-TR-2008-01. Retrieved April 27, 2009, from http://research.nokia.com/files/NRCTR2008001.pdf

[3] Mobile Trusted Module (MTM) - an introduction, Nokia Research Center, Technical report NRC-2007-015. Retrieved April 27, 2009, from http://research.nokia.com/

[4] Ekberg J-E & Sven Bugiel: Trust in a Small Package - Minimized MRTM Software Implementation for Mobile Secure Environments, to be published in Proceedings of the 2009 ACM workshop on Scalable Trusted Computing, Nov 13, 2009.

[5] Kostiainen K & Ekberg J-E. & Asokan N.. & Rantala A. On-board Credentials with Open Provisioning. Proceedings of ASIACCS09, ACM Symposium on Information, Computer & Communication Security

[6] Sundaresan H. OMAP platform security features, July 2003. Texas Instruments white paper. Retrieved April 27, 2009, from http://focus.ti.com/pdfs/vf/wireless/platformsecuritywp.pdf

[7] Trusted Computing Group (2008A). TPM Specification, version 1.2 Revision 103. Retrieved April 27, 2009, from https://www.trustedcomputinggroup.org/specs/TPM/

[8] Trusted Computing Group. Mobile Trusted Module Specification, Version 1.0 Revision 1. Retrieved April 27, 2009, from https://www.trustedcomputinggroup.org/specs/mobilephone

[9] Trusted Computing Group. Mobile Trusted Module Reference Architecture, Version 1. 0. Retrieved April 27, 2009, from https://www.trustedcomputinggroup.org/specs/mobilephone

[10] Winter J: Trusted computing building blocks for embedded Linux-based ARM TrustZone platforms. Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing.