Hardware Isolation for Trusted Execution

Jan-Erik Ekberg
Trustonic
Ruoholahdenkatu 8 C
Helsinki, Finland
jan-erik.ekberg@trustonic.com

ABSTRACT

For more than a decade, Trusted Execution Environments (TEEs), found primarily in mobile phone and tablets, have been used to implement operator and third-party secure services like payment clients, electronic identities, rights management and device-local attestation.

For many years, ARM TrustZone-A™ (TZA) primitives were more or less the only available hardware mechanism to build a TEE, but recently alternative hardware security solutions have emerged for the same general purpose --- some are more tailored to the upcoming Internet of Things (IoT) device market whereas we also now have hardware that potentially can bring TEEs into the cloud infrastructure.

In my talk I will introduce the contemporary TEE as is being deployed in today's devices, but one focal point of the presentation is on a functional comparison between the hardware support provided by TZA and the recently released and deployed Intel SGX™ and ARM TrustZone-M™ architectures. Each solution has its relative strengths and drawbacks that reflects its main deployment purpose, and as a result, the software stack that completes the TEE environment will have to significantly adapt to each individual hardware platform.

The final part of the talk will present a few conducted tests and research prototypes where we have gone beyond the TEE as it typically is set up today -- e.g. exploring problems emerging in a cloud environment with migrating workloads as well as policy enforcement in IoT devices.

Short Bio

Jan-Erik Ekberg is Director of Advanced Development at Trustonic. His background is in the telecom industry, where he worked for 18 years at Nokia Research Center. His primary interests are with issues related to platform security, TPMs and TEEs, but he has also background in (securing) network protocols and telecom systems, as well with short-range communication technologies like NFC, BT-LE and WLAN. In his latest role his main focus is in trusted execution environments for mobile devices as well as IoT endpoints and servers. Jan-Erik received his doctorate in Computer Science from Aalto University.

.

SPSM'16, October 24, 2016, Vienna, Austria.
ACM ISBN 978-1-4503-4564-4/16/10.
DOI: http://dx.doi.org/10.1145/2994459.2994460