Android and trusted execution environments | Program | Android Security Symposium 2015

Jan-Erik Ekberg

Trustonic Inc, Helsinki, Finland

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 Android, but also in OS security aspects such as SEAndroid. Jan-Erik received his doctorate in Computer Science from Aalto University.

Over the last years, third-party provisionable Trusted Execution Environments (TEEs) have seen increasing market presence, one estimate is that 0.5B handsets have been shipped with one, at least 350M of these are Android handsets. Interface standards in the field are also maturing.

My talk will focus on the deployed TEE ecosystem with an Android perspective - outlining what a TEE architecturally is, which components and services it typically contains and which processing / processor services form the fundament of the TEE security argument. I will briefly touch on recent platform alternatives for TEE development and research, as well as which directions in which we see TEEs evolving in the near future. I will round up by motivating TEE usefulness through a few selected use-cases like mobile payments and identity, as well as a few architecture and application results we have recently reached in the new domain of TEEs in servers (Cloud), primarily in collaboration with Aalto University, Helsinki.

Get the slides here.

Source: https://usmile.at/symposium/program/2015/ekberg