Title of talk: Run-time / memory protection on future mobile processors

About the Speaker: Jan Erik Ekberg is CTO, Mobile Security at Huawei Finland. His background is partly in the telecom industry, where he worked for 18 years at Nokia Research Center, and partly in developing secure mobile device platforms (7 years in Trustonic Inc and DarkMatter Llc). His primary interests are with issues related to platform security architectures, TEEs, TPM, mandatory access control mechanisms and protecting mobile software against run-time attacks. He also has a background in (securing) network protocols and telecom systems, as well as with securing and standardizing short-range communication technologies like NFC, BT-LE and WLAN. In his latest role his main focus is in securing the Huawei mobile device platform at the hardware and system software levels. Jan-Erik received his doctorate in Computer Science from Aalto University, and is currently also serving as a part-time Adjunct Professor in the System Security Group in his alma mater.

Abstract: The next few years will bring us several new hardware-assisted micro-architectural security features in consumer devices. Future ARM processors come with support for pointer integrity (PAuth, ARMv8.3A), Branch Target Protection (BTI, ARMv8.5A), also available in ARMv8M-class controllers, and memory tagging (MTE, ARMv8.5A). I will present these features, as well as explore academic contributions in this domain, done in collaboration between Aalto Systems Security Group, and Huawei Technologies (Finland). I will round off the presentation by discussing future options, where

the combination of microarchitecture and software design may achieve memory protection against run-time attacks at an even higher granularity.