Less-Insecure Network Edge Virtualization with Low Size, Weight and Power: APU2, TPM 2.0 and AMD SKINIT DRTM with TrenchBoot, OpenEmbedded meta-virtualization and pfSense

Piotr Król[1], Krystian Hebel[2], and Łukasz Wcisło[3]

[1] 3mdeb Embedded Systems Consulting, Gdansk, Poland
piotr.krol@3mdeb.com
[2] 3mdeb Embedded Systems Consulting, Gdansk, Poland
krystian.hebel@3mdeb.com
[3] 3mdeb Embedded Systems Consulting, Gdansk, Poland
lukasz.wcislo@3mdeb.com

Abstract

For the last several years hypervisors have acquired a key role in platform security by leveraging a reduction of the possible attack surface. Meanwhile one could observe an increasing range of TPM's usability. And that open-source is a growing part of all the code delivered around the World.

In this talk, we want to show a process of how all those pieces can work together. Using a simple and well-known platform we will process a secure boot using Static Root of Trust for Measurement with coreboot, move to Dynamic Root of Trust for Measurement by SKINIT in TrenchBoot, and use all of that to provide a complete Chain of Trust for Xen hypervisor, which will handle a virtual firewall with no physical NICs.

Everything will be built from upstream OE meta-virtualization and meta-measured. Then we will provide power and performance benchmarks for virtualization overhead.

Finally, we are going to discuss why something that complex can still be very practical and we will explain the value behind that stack.