Less-Insecure Network Edge Virtualization with Low Size, Weight and Power

Platform Security Summit 2019 (10/02/2019)

Piotr Król

3MDEB

About me

Piotr Król
Founder & Embedded Systems Consultant

- open-source firmware
- platform security
- trusted computing

- @pietrushnic
- piotr.krol@3mdeb.com
- linkedin.com/in/krolpiotr
- facebook.com/piotr.krol.756859

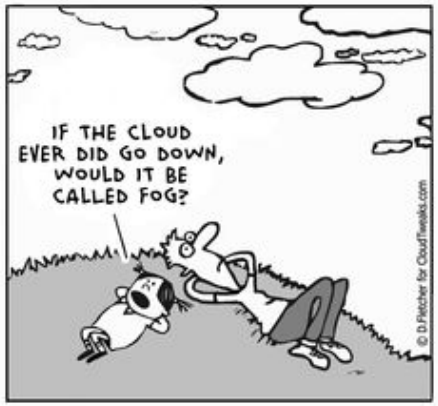
CC-BY-4.0 | Piotr Król

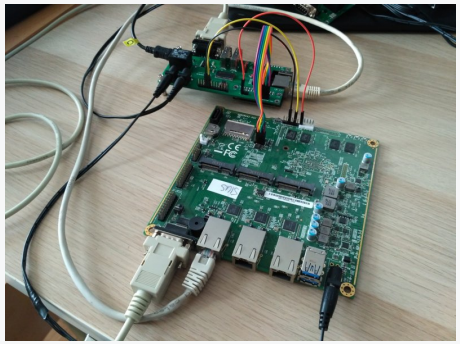
Agenda

- Problem statement, goals and motivation
- TPM 2.0 in open-source
- PC Engines hardware and firmware
- SRTM: coreboot and GRUB2
- DRTM: TrenchBoot
- PCRs and measurements
- OPNsense and NDVM performance
- Demo
- Where to go from here?

CC-BY-4.0 | Piotr Król

Problem statement





- Edge/Fog Computing and IoT Gateways hype will increase the amount of network appliance devices.
- Vulnerability in network appliance software may lead to malicious firmware modification, which can be undetected over the whole life cycle of the device.
- Toolbox for reestablishing trust in firmware is almost empty and not easy to use.

https://www.wired.com/2013/09/nsa-router-hacking/ https://i.pinimg.com/236x/8e/77/77/8e7777e3cd4759eeb20da17969881a48--fog-computing-tech-humor.jpg

CC-BY-4.0 | Piotr Król

How we can build less-insecure system?

- Use virtualization to isolate system components
  - strong, hardware-supported isolation
- Implement narrow interfaces
  - devices disaggregation
- Open-source software stack
  - on every stage of platform operation
  - in each device controller
- Reproducible builds
- Modern hardware features
  - firmware storage security
  - secure launch (aka late launch or secure startup)
  - IOMMU
- Trusted Platform Module

CC-BY-4.0 | Piotr Król

Goal and Motivation

How many solutions are shipped with those features working out-of-the-box?

How open those solutions are?

Goal

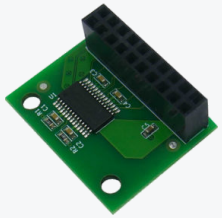
Create less-insecure virtual network appliance

Motivation

- Need for secure network appliance which measurements can be attested
- Creation TrenchBoot implementation for AMD platforms
- Build solid ecosystem for Edge Computing "era"
- Building foundation for secure remote updates

CC-BY-4.0 | Piotr Król

TPM status in open-source



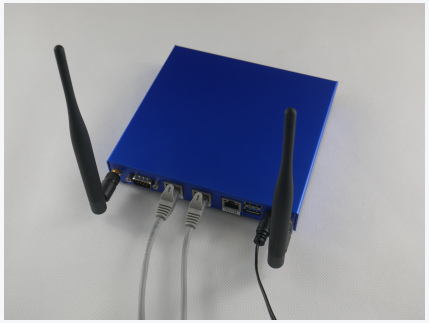
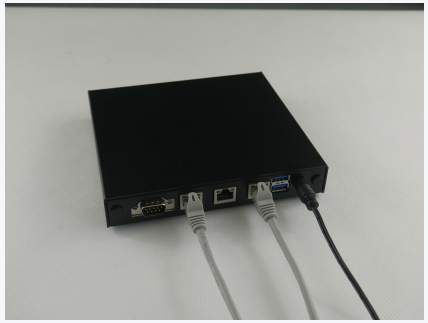
- Trusted Platform Modules are plug-and-play modules
- TPM enables SRTM and DRTM fundamental for platform integrity
- TPM 1.2 are common and well supported, but new designs should use 2.0
- Recent advancement in open-source TPM 2.0 support
  - tpm2-software (TSS, PKCS#11, OpenSSL Engine)
    `https://github.com/tpm2-software`
  - TPM Genie mitigation in Linux kernel
    `https://github.com/nccgroup/TPMGenie`
  - FreeBSD Secure Boot support
    `https://papers.freebsd.org/2019/bsdcan/stanek-improving_security_of_the_freebsd_boot_process/`
- TPM 2.0 is mandatory for Edge Computing and IoT Gateways (AWS, Azure)

CC-BY-4.0 | Piotr Król

PC Engines apu2

- Made by open-minded Swiss company
- Frequently OEMed used as base for other products by other vendors



CC-BY-4.0 | Piotr Król

PC Engines apu2

- AMD Embedded G series GX-412TC, 1 GHz quad Jaguar core with 64 bit
- AES-NI
- SKINIT for DRTM
- 4GB DDR3-1333 DRAM with ECC
- SD, USB, mSATA, SATA
- 2x mPICe (one with SIM socket)
- 3 Gigabit Ethernet channels using Intel i210AT / i211AT NICs depending on the model
- 6-10W@12V DC
- Lot of buses (RS232, LPC, GPIO, I2C)

CC-BY-4.0 | Piotr Król

PC Engines open-source firmware

- There are already thousands of devices in the field
- Each can be leveraged as a less-insecure network appliance
- Reasonable community that cares about open-source firmware
- regular monthly firmware releases (for last 27 months)
- reproducible builds
- signed hashes provided
    - QubesOS-like key chain
    - `3mdeb master->3mdeb open-source firmware->PC Engines release key`

CC-BY-4.0 | Piotr Król

coreboot (SRTM)

- SPI image is build using the coreboot build system
- SRTM (or rather S-CRTM) implemented based on vboot library
- coreboot measures all boot stages and payload (GRUB2)
- SPI image can be build using the following repository
  - https://github.com/pcengines/coreboot/tree/pcengines_trenchboot
  - Use `config.pcengines_apu2.tb`
- Features
  - measured boot
  - verified boot (booting unsigned code result triggers recovery mode)
  - firmware updates
  - signed SPI images

CC-BY-4.0 | Piotr Król

Read-only SPI region

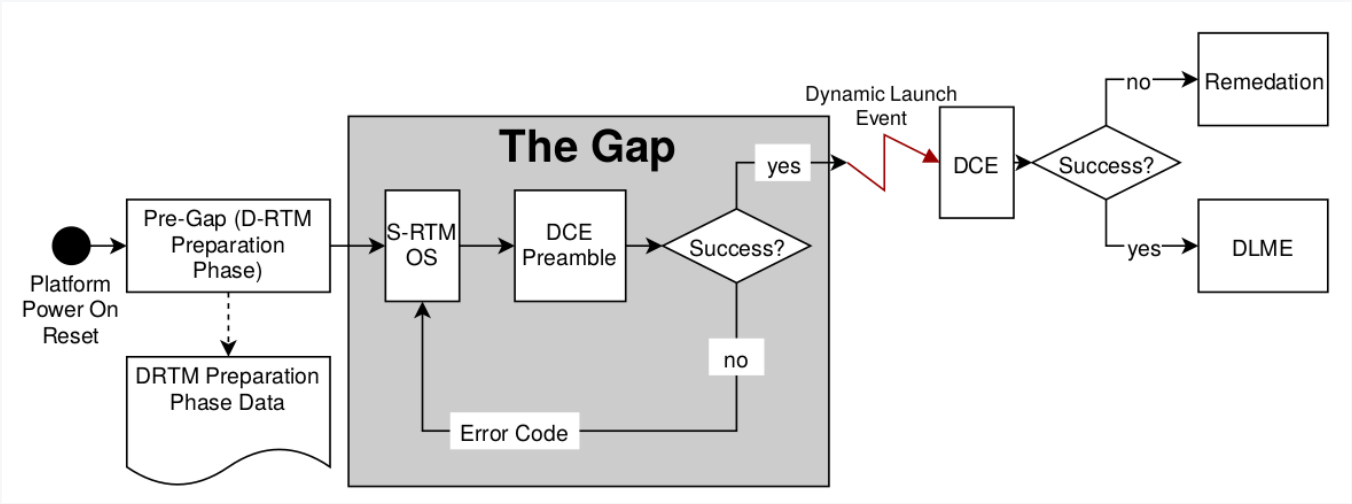
1	0	X	Lock-Down	until the next power-down, power-up cycle.(1)
1	1	X	One Time Program(2)	Status Register is permanently protected and can not be written to.

Note:
1. When SRP1, SRP0 = (1, 0), a power-down, power-up cycle will change SRP1, SRP0 to (0, 0) state. 2. This feature is available upon special order. Please contact Winbond for details.

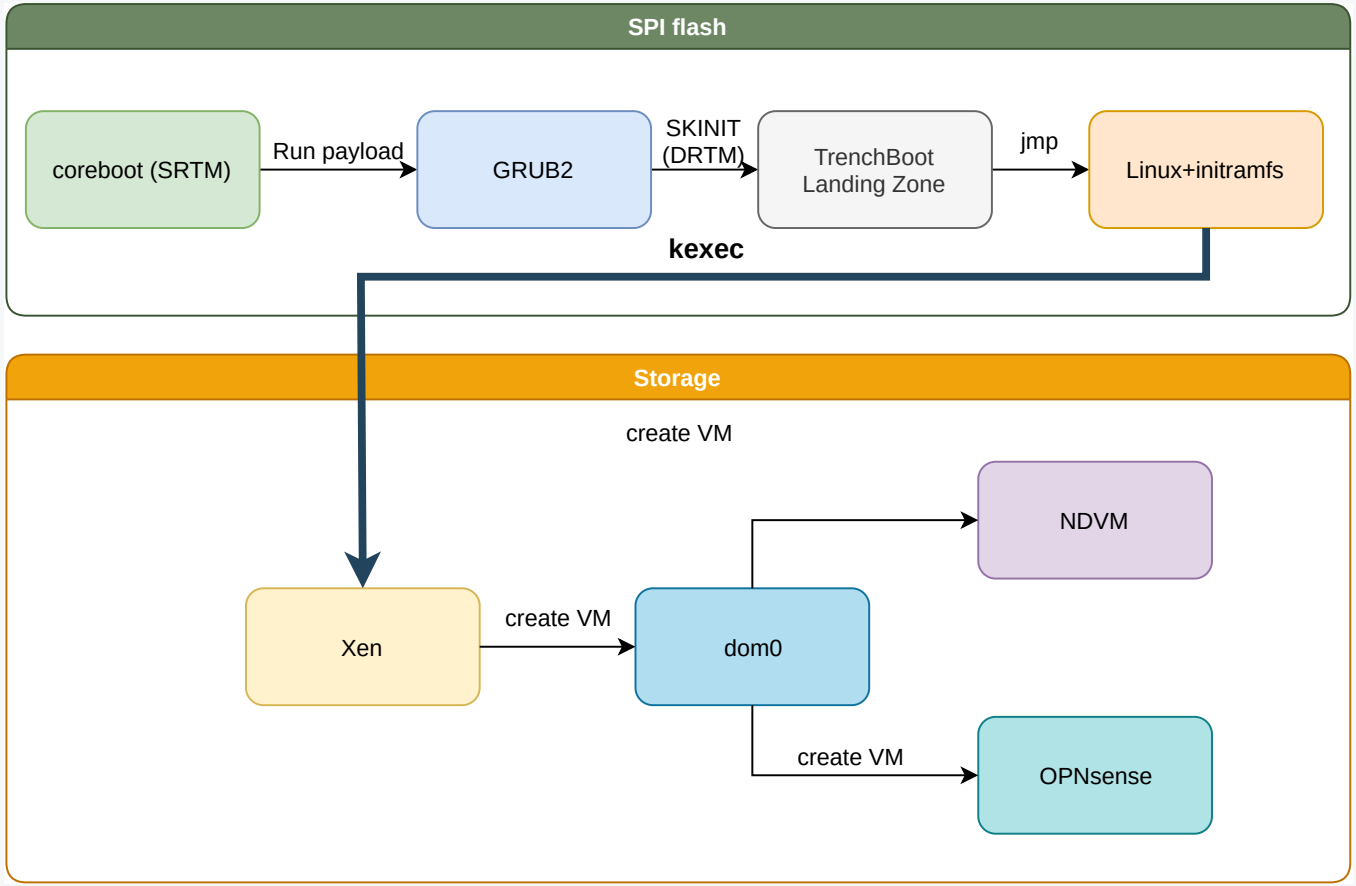
- Required for SRTM implementation
- Default Winbond chip for PC Engines apu2 doesn't have that feature
- Adesto AT25SF641 which provide features w/o "special order"
- Flashrom - A utility for identifying, reading, writing, verifying and erasing flash chips
- PC Engines fork of flashrom was extended to support Adesto chip and OTP feature
- https://github.com/pcengines/flashrom

CC-BY-4.0 | Piotr Król

- Open-source ecosystem-wide framework for launch integrity
- Main goal is to enable out-of-the-box support for TCG D-RTM in open-source ecosystem
- Currently targeting Intel and AMD implementation design is prepared to handle other solutions
- Note that the AMD TrenchBoot implementation is completely open-source. This is not possible with Intel.

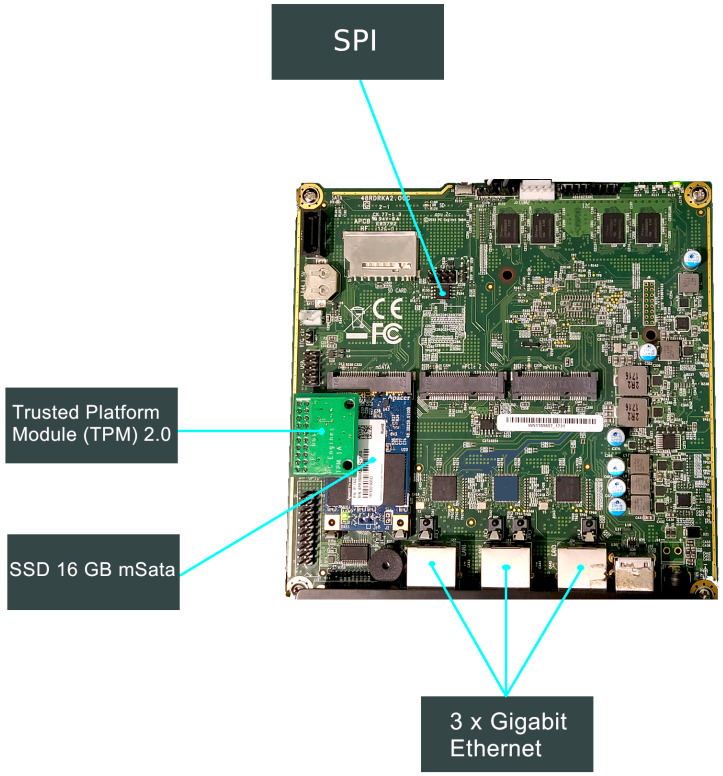


coreboot, TrenchBoot, and hypervisor



CC-BY-4.0 | Piotr Król

Hardware platform



CC-BY-4.0 | Piotr Król

coreboot TCPA measurements

- Visible during coreboot boot

```
PCR-2 a16bc92eb28ae11c13ad6d9c2ad0632dc9909983f4b17663dbf388eb756ddf9c SHA256 [FMAP: COREBOOT CBFS: bootblock]
PCR-2 8035cc56c197087c79504d98bd7c5841a8c7886b8236ee14d862f191d95d8dad SHA256 [FMAP: COREBOOT CBFS: fallback/romstage]
PCR-0 62571891215b4efc1ceab744ce59dd0b66ea6f73 SHA1 [VBOOT: boot mode]
PCR-1 a66c8c2cda246d332d0c2025b6266e1e23c89410051002f46bfad1c9265f43d0 SHA256 [VBOOT: GBB HWID]
PCR-2 957757f20415ecd1c6f7e5acbaaafc9ac4cc858ec2df1913958b1e0655daf45a SHA256 [FMAP: COREBOOT CBFS: fallback/ramstage]
PCR-2 6c1d20616d91442b61de89de6bf81f0ee8e929919c9284061e00d004de893994 SHA256 [FMAP: COREBOOT CBFS: spd.bin]
PCR-3 585721d9e083591b90d1df05178d87124a73602d88c4ab8258793d8658ab5061 SHA256 [PSPDIR]
PCR-2 1f58561c980dd7c6d3c3cb6a845894cf674dc754b9215b54b85057b25ed3c1ea SHA256 [FMAP: COREBOOT CBFS: AGESA]
PCR-2 1f58561c980dd7c6d3c3cb6a845894cf674dc754b9215b54b85057b25ed3c1ea SHA256 [FMAP: COREBOOT CBFS: AGESA]
PCR-2 1f58561c980dd7c6d3c3cb6a845894cf674dc754b9215b54b85057b25ed3c1ea SHA256 [FMAP: COREBOOT CBFS: AGESA]
PCR-2 1f58561c980dd7c6d3c3cb6a845894cf674dc754b9215b54b85057b25ed3c1ea SHA256 [FMAP: COREBOOT CBFS: AGESA]
PCR-2 1f58561c980dd7c6d3c3cb6a845894cf674dc754b9215b54b85057b25ed3c1ea SHA256 [FMAP: COREBOOT CBFS: AGESA]
PCR-2 1f58561c980dd7c6d3c3cb6a845894cf674dc754b9215b54b85057b25ed3c1ea SHA256 [FMAP: COREBOOT CBFS: AGESA]
PCR-2 1f58561c980dd7c6d3c3cb6a845894cf674dc754b9215b54b85057b25ed3c1ea SHA256 [FMAP: COREBOOT CBFS: AGESA]
PCR-2 5b6d4566a1b3157a6f437c320be95fe85eb371eab63fcd4520b0e763572f4683 SHA256 [FMAP: COREBOOT CBFS: fallback/dsdt.aml]
PCR-2 6c1d20616d91442b61de89de6bf81f0ee8e929919c9284061e00d004de893994 SHA256 [FMAP: COREBOOT CBFS: spd.bin]
PCR-2 19d059948d4188fca951dd7297defe02d68a221dd78a9188515c69904c82c8fd SHA256 [FMAP: COREBOOT CBFS: fallback/payload]
```


CC-BY-4.0 | Piotr Król

Measurement

- Obtained in Xen dom0

```
sha1 :
  0  : 1e745033ad915853b44c9439116f311dd85011c8
  1  : 0000000000000000000000000000000000000000
  2  : 0000000000000000000000000000000000000000
  3  : 0000000000000000000000000000000000000000
  4  : 0000000000000000000000000000000000000000
  5  : 0000000000000000000000000000000000000000
  6  : 0000000000000000000000000000000000000000
  7  : 0000000000000000000000000000000000000000
  8  : 0000000000000000000000000000000000000000
  9  : 0000000000000000000000000000000000000000
  10 : 0000000000000000000000000000000000000000
  11 : 0000000000000000000000000000000000000000
  12 : 0000000000000000000000000000000000000000
  13 : 0000000000000000000000000000000000000000
  14 : 0000000000000000000000000000000000000000
  15 : 0000000000000000000000000000000000000000
  16 : 0000000000000000000000000000000000000000
  17 : 169a4fe87b0df8470670339ba78ba05ea6fb9489
  18 : 3d9f3514b22efe39c15094110f109e9ab06d5daf
  19 : 0000000000000000000000000000000000000000
  20 : 0000000000000000000000000000000000000000
  21 : 0000000000000000000000000000000000000000
  22 : 0000000000000000000000000000000000000000
  23 : 0000000000000000000000000000000000000000
```


CC-BY-4.0 | Piotr Król

Measurement

- Obtained in Xen dom0

```
sha256 :
  0  : 0000000000000000000000000000000000000000000000000000000000000000
  1  : d965b906c85450d5aad254368b53f043480e811b590ce37a524331d2b9135368
  2  : 6e6e3d56aa878cd7f8ae745104d589f299938cd4009c3c79ea9cad2701690b12
  3  : f80ac628144ea6ac2743d9a48715e8f1ecb7458925d1d2a1b9e4bf5011ae1f5b
  4  : 0000000000000000000000000000000000000000000000000000000000000000
  5  : 0000000000000000000000000000000000000000000000000000000000000000
  6  : 0000000000000000000000000000000000000000000000000000000000000000
  7  : 0000000000000000000000000000000000000000000000000000000000000000
  8  : 0000000000000000000000000000000000000000000000000000000000000000
  9  : 0000000000000000000000000000000000000000000000000000000000000000
  10 : 0000000000000000000000000000000000000000000000000000000000000000
  11 : 0000000000000000000000000000000000000000000000000000000000000000
  12 : 0000000000000000000000000000000000000000000000000000000000000000
  13 : 0000000000000000000000000000000000000000000000000000000000000000
  14 : 0000000000000000000000000000000000000000000000000000000000000000
  15 : 0000000000000000000000000000000000000000000000000000000000000000
  16 : 0000000000000000000000000000000000000000000000000000000000000000
  17 : 0d7bc289be9cdfec68e69665de67bdbd92aaa860a8bf4db49803991600dba2a6
  18 : 0000000000000000000000000000000000000000000000000000000000000000
  19 : 0000000000000000000000000000000000000000000000000000000000000000
  20 : 0000000000000000000000000000000000000000000000000000000000000000
  21 : 0000000000000000000000000000000000000000000000000000000000000000
  22 : 0000000000000000000000000000000000000000000000000000000000000000
  23 : 0000000000000000000000000000000000000000000000000000000000000000
```


CC-BY-4.0 | Piotr Król

SRT measurements

SHA-1

- **PCR0** - extended by vboot logic with boot mode (normal, dev, recovery, keyblock)

SHA-256

- **PCR1** - extended by vboot logic and represent hardware ID
- **PCR2** - used by coreboot to extend measurements of all loaded and/or executed components from CBFS'es, either read-only or read-write parts
- **PCR3** - used by coreboot to extend measurements of variable and runtime data that might change across boots (MRC cache, CMOS configuration, etc.)
- **PCR4-16** - not used

CC-BY-4.0 | Piotr Król

DRT measurements

SHA-1

- **PCR17** - extended by TrenchBoot Landing Zone code and measures LZ, Linux+u-root
- **PCR18** - command line used for booting Linux+u-root

SHA-256

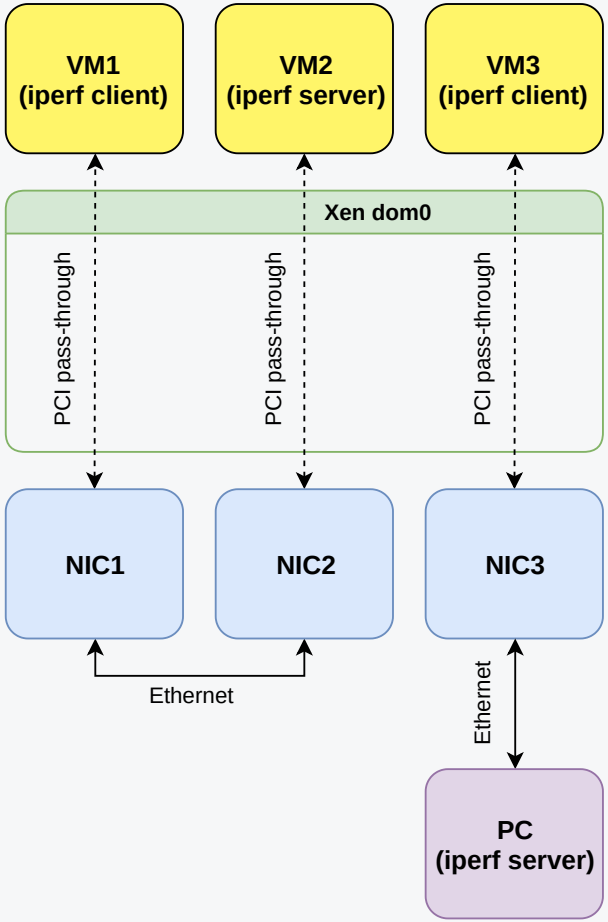
- **PCR17** - extended natively by AMD SKINIT instruction

CC-BY-4.0 | Piotr Król

- pfSense fork since 2015
- BSD 2-Clause “Simplified” license
- different UI
- IPS/IDS based on Suricata included
- weekly security updates

CC-BY-4.0 | Piotr Król

Performance tests setup



CC-BY-4.0 | Piotr Król

Performance tests results

- VM1 client (VM to VM test)

```
(...)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-120.00 sec  13.1 GBytes   940 Mbits/sec  575             sender
[  5]   0.00-120.04 sec  13.1 GBytes   939 Mbits/sec                  receiver
```

- VM2 server (VM to VM test)

```
(...)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-120.00 sec  13.1 GBytes   940 Mbits/sec  575             sender
[  5]   0.00-120.04 sec  13.1 GBytes   939 Mbits/sec                  receiver
```

- VM3 client (VM to PC test)

```
(...)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-120.00 sec  13.1 GBytes   940 Mbits/sec  575             sender
[  5]   0.00-120.04 sec  13.1 GBytes   939 Mbits/sec                  receiver
```


CC-BY-4.0 | Piotr Król

Demo time

CC-BY-4.0 | Piotr Król

What we can do with that?

- Security
  - reproducible builds of whole software stack
  - only firmware signed by trusted party can be used
  - possibility of reestablishing trust without reboot
  - remote attestation
- Multifunction network appliance with clean isolation
- Simplified configuration reproducibility and migration
- Multiple levels of management
  - direct connection with firewall VM for network management
  - orchestration through hypervisor
- With additional VMs sky is the limit (or rather hardware performance)
- All of that without losing trust in your network appliance
- And even if that will happen you detect and can reestablish it

CC-BY-4.0 | Piotr Król

Where to go from here?

- https://trenchboot.github.io
- https://github.com/TrenchBoot
- https://groups.google.com/forum/#!forum/trenchboot-devel

CC-BY-4.0 | Piotr Król

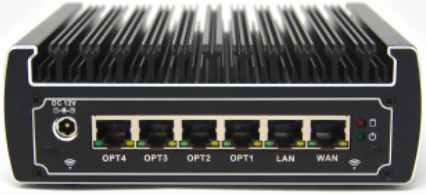
Marketing pitch

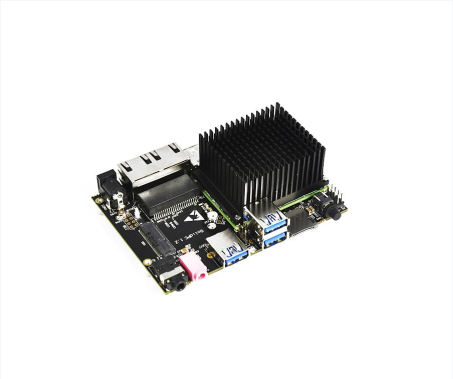
- 3mdeb is based in Gdańsk, Poland
- Over 4 years we worked with 50 customers from 21 countries

CC-BY-4.0 | Piotr Król

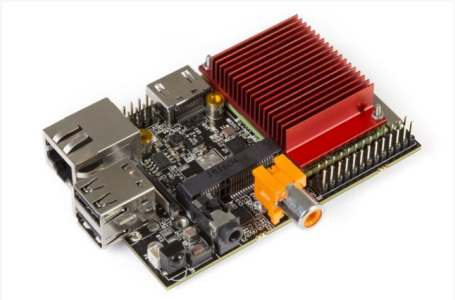
Example engagements

- Open-source firmware implementation and maintenance





- IoT Gateways and Edge/Fog Computing devices



CC-BY-4.0 | Piotr Król

Open-source hardware

- 3mdeb inside

- community projects manufactured by 3mdeb

CC-BY-4.0 | Piotr Król

Marketing pitch

- Examples engagements
  - From hardware bring-up to complete Board Support Package (BSP)
  - x86 firmware (BIOS/UEFI/coreboot) development, debugging and optimization
  - AWS and Microsoft IoT Cloud integration
  - firmware and embedded systems maintenance
- Desired partnership
  - hardware makers and OEMs
  - open-source firmware promoters
- Hiring
  - we always look for people motivated to open firmware ecosystem and promote open solutions on the edge
  - Interested? Please send CV
- If you looking for commercial support feel free to visit our website or contact us:
  - https://3mdeb.com
  - contact@3mdeb.com

CC-BY-4.0 | Piotr Król

Q&A

CC-BY-4.0 | Piotr Król

Backup

CC-BY-4.0 | Piotr Król

Hardware platforms limitations

- TPM2.0 over LPC
  - TPM Genie and sniffing issues
  - Patches to Linux kernel under review
- SPI header
  - anyone with recovery dongle and working firmware

CC-BY-4.0 | Piotr Król

coreboot future improvements

- C environment bootblock for apu2
  - we cannot use vboot before romstage
  - everything up to romstage has to be locked by RO flag
- Recovery mode
  - currently, there is not enough space
  - we deployed commercial solutions with SRTM, firmware A/B, and recovery mode
- TPM2.0 logs are stored in TCPA (TPM1.2 log)
  - TPM2 logs are different than TCPA logs, implement correct TPM2 log format and differentiate from TCPA log API
- minimize the read-only locked code by moving raminit code to read-write partitions
- save TPM2 measurements in TPM2 log area in a format compliant with TCG (coreboot)
- implement TrenchBoot support for the direct secure launch of Xen
- use SHA256 sums for all PCRs in TrenchBoot and coreboot

Start trusting Your BIOS SRTM with vboot, TPM and permanent flash protection, Michał Żygowski, OSFC 2019

CC-BY-4.0 | Piotr Król