Lightning Talks

Qubes OS and 3mdeb mini-summit 2019

Piotr Król

3MDEB

DRTM/TrenchBoot

- We are moving slowly forward with TrenchBoot for PC Engines (AMD G-series based firewall)
    - Krystian can tell more about status
    - it is worth to mention that we enabled AMD IOMMU for PC Engines and tested that on Xen
- Is there any interested from Qubes OS side about open DRTM?
- What about potential of modern AMD based platform with open DRTM implementation?
- Any opinions about TrenchBoot effort are welcome

HCL

- We see value in reporting as much PCs as possible from our company and ecosystem
  - do you think it is acceptable to automate that?
  - can we do that under "3mdeb Embedded Systems Consulting" name?
  - how name is selected? manual edit to HCL report?
- Are there any plans to anonymize HCL reports?
  - as mentioned some reports may consider fragile information about the system
- What is your opinion about long term maintenance of such list?
  - we see some problems related to that in coreboot community
- Can we leverage information from HCL in areas of firmware?
  - reporting about firmware quality
  - warn about out of date firmware
  - suggest better open alternative

fwupd

- Do you know the project, if yes what is your take on that?
- Richard improve features and want to add security checks as well as robust explanation to particular firmware components
- System76 conspiracy theory

Business deployments

- Do you work on wider deployments for business?
- Is there any value for regular company?
  - minimization of IT administration problems
  - less problems with malicious software
- We see some potential customers and we would like to preform small beta deployment (15-20 workstations)

Hardware crypto keys

- Nitrkey
- Yubikey

Suggested conferences

- Any conferences that you prefer?
- Any particular topics that you think are interesting recently, that we maybe missing?
- What are the best conferences to talk about Qubes OS and lower layers?

Q&A