Qubes Hardware Certification

Qubes OS and 3mdeb mini-summit 2019

Piotr Król

3MDEB

Disclaimer

- Opinions are my own and represent view of my employer
- We do not follow very close Qubes OS development and discussions
- We came from embedded and firmware world - our experience with general-user-facing system is low

Qubes statement (2 years old)

- `we're working hard to make a "reasonably secure laptop" a reality`
  - can we ask what does it mean?
  - what is the progress of that effort?
  - is there any place for Open Source Firmware consulting company?
  - there are many companies trying the same
- `Serious prospective business customers should [contact us] for more information`
  - We would like to understand what that means
  - Feasible?

x86 considered harmful

- Are there any architecture which can be considered not-harmful?
  - ARM
    - poisoned supply chain
    - hard to build general purpose computer for masses
    - UEFI
    - mobile solutions
    - Purism effort around i.MX8
  - OpenPOWER
    - very expensive
    - we are not sure about exact state since we never worked with this architecture
  - RISC-V
    - we think it is very promising
- even if CPU is clear, we have to face tons of other blobs in different system components
  - firmware is everywhere

Blobs

- coreboot
  - do you see any alternatives to open-source boot firmware?
  - BTW it really like your precise naming
- Intel FSP
  - it looks that there are serious plans to open source FSP
  - BootROM in x86
- (CS)ME/IE
  - after many PT revelations lots of interesting things happen
  - any comments on that?

Hardware certification

- Not only hardware vendors are interested in that
  - OEM/ODM
  - Embedded Systems Consulting
- Customers often come to us from Qubes OS website
  - Thank you
  - Qubes OS (hw cert) -> coreboot -> consulting -> 3mdeb
- Qubes certified laptop

UEFI issues

- Are there any real issues with UEFI in light of certification?
- IBVs are not very welcome in current ecosystem
- Does Qubes OS see some implementation problems with UEFI implementation
    - What are the things users complain?
    - Any hard to debug/workaround/fix bugs affecting OS?

Qubes OS and 3mdeb

- Is there a place for Qubes OS and companies like 3mdeb to cooperate?
  - what areas?
  - how we can help each other assuming reasonable resources?
- Discussion

Q&A