HKG18-204: Cross team component discussion on the impact of security vulnerabilities

Joakim Bech and David Rusling
Timeline

- **Nov -17**: Linaro learns about the attacks.
- **Dec -17**: Spectre & Meltdown goes public (one week sooner than initially planned).
- **Jan -18**: OP-TEE Security Advisories (+mail), Initial deck from Linaro.
- **Feb -18**: Spectre & Meltdown at 96Boards OpenHours.
- **Mar -18**: OP-TEE 3.0.0 with Meltdown and Spectre v2.
- **Q2-Q4 -18**: This session!

**Blog posts**
- **Blog post #1**: Spectre v1 investigation, Red Hat scanner tool.
- **Blog post #2**: Linaro Security Update Portal.

**Events**
- **Nov 23**: Spectre & Meltdown.
- **Dec 3**: Optimizations?
- **Jan 9**: Backporting?
- **Jan 11**: 96Boards OpenHours.
- **Mar 20**: Linaro disclosure policy?
- **Mar 21**: Themed hacking session.

**Dates**
- **Nov 23**: Dec -17
- **Dec 3**: Jan -18
- **Jan 9**: Jan -18
- **Jan 11**: Jan -18
- **Mar 20**: Mar -18
- **Mar 21**: Mar -18
Topics for discussion

● Tooling
  ○ Toolchains - static analysis
  ○ Specific tools developed just for Meltdown & Spectre
    ■ Red Hat scanner tool (by Nick Clifton)
    ■ Other tools?
    ■ Should Linaro get involved in the development of this type of tooling?

● Disclosure policy
  ○ Linaro has a “Responsible disclosure policy” for OP-TEE.
  ○ Make the OP-TEE policy more generic? I.e, some kind of “Linaro security disclosure policy”?
  ○ Should Linaro create → linaro.org/security-advisories?

● Backporting
  ○ What strategy?
  ○ What has been done so far?

● Linaro Security Update Portal
  ○ Is it useful?
  ○ How can we make it better?
Current status

- In general, the Linaro Security Update Portal contains all current information about all projects Linaro are involved in.

- OP-TEE
  - Meltdown (“KPTI”) & Spectre v2 (branch invalidation) have been patched.
  - Spectre v2 - needs some improvements related to branch invalidation, ongoing.
  - Spectre v1 - have not been able to find any vulnerable areas.

- Linux kernel
  - KPTI - in mainline for x86
  - Backport initiative - Speculative execution security fixes (LSK-43)
    - arm64 KPTI backport to v4.14 (LSK-40), v4.9 (LSK-41), v4.4 (LSK-42)
    - Initial arm64 v1/v2 workaround backports v4.14 (LSK-44), v4.4 (LSK-45)
    - 32bit ARM branch predictor hardening v4.14 backport (LSK-47), v4.9 (LSK-48), v4.4 (LSK-49)

- UEFI
  - Patch series for unmapping the kernel during runtime service calls
Thank You

#HKG18

HKG18 keynotes and videos on: connect.linaro.org
For further information: www.linaro.org