SFO15-105: Core Development Lightning Talks

Core Dev Team

Presented by
Core Dev Team

Date
Monday 21 September 2015

Event
SFO15
Intro

Each of the core development teams will give a 10 minute overview on current happenings
KWG

Click to edit master text body
KWG: Upstream kernel

Arnd Bergmann, Linus Walleij & Mark Brown

- arm-soc tree
- Subsystems
  - Too many for one slide!
- Not just KWG, many other maintainers in other groups
KWG: ARM64

Dave Long & Takahiro Akashi

- kexec
- kprobes
- kdump
- Live patching
KWG: CoreSight

Mathieu Poirier & Chunyan Zhang

- ETMv4 & QC replicator support added
- Perf integration
- Ftrace integration
  - Currently on hold → may not be feasible
- Work on trace decode library started
  - Session on Thursday
KWG: u-boot for AArch64

Linus Walleij

- Semihosting commands for FVP
- Reference hardware support implemented on Juno
- Support for HiKey implemented very quickly by Peter Griffin
KWG: Other tasks

- kselftest (Bamvor Zhang Jian)
  - Working with kernelci.org team to get kselftest running well on kernelci.org
- Y2038 (Arnd Bergmann, John Stultz)
  - Many assignees helping out with addressing Y2038 issues
- dm-crypt (Baolin Wang)
- KAsan (Linus Walleij)
- Kernel reloaded (Linus Walleij, Baolin Wang, Takahiro Akashi)
  - Session on Wednesday
SWG

Click to edit master text body
SWG (1/4): Completed since HKG-15

- Added LPAE support
- 64bit-support in TEE core (S-EL1)
- Published optee_test on GitHub
- Repo + Makefiles instead of shell-scripts
SWG (2/4): Completed since HKG-15

- New hardware supported in OP-TEE:
  - Hikey
  - MT8173
  - TI Dra7xxx
- Secure Storage enhancements (AES-GCM)
- Elliptic Curve Cryptography (ECC)
- Enabled ARMv8 crypto extensions
SWG (3/4): Ongoing, next steps

- Linux kernel generic TEE driver (v5)
- Secure Storage enhancements (SFO15-503)
  - To-do: Rollback, TA storage separation, RPMB
- Widevine / OEMCrypto
- GP Internal core API v1.0 -> v1.1
- PAN (Privileged Access Never) to LSK
- SMMU secure services
SWG (4/4): Ongoing, next steps

- Trusted Applications as signed ELF-files
- Multi-core TA support
- OP-TEE on Hikey + AOSP
- Trusted UI
- Open Source Security Project!
PMWG: Focus Areas

- EAS, cpuidle, cpufreq
- Runtime PM, generic power domains (genpd)
- Tools
PMWG: Upstream Maintainers

- Daniel Lezcano (cpuidle, clockevents)
- Ulf Hansson (genpd and MMC)
- Kevin Hilman (genpd, OMAP PM)
- Viresh Kumar (cpufreq)
PMWG: Since HKG15

- Rationalisation of cpu capacity and load calculations in the scheduler: merged
- sched-DVFS: RFCv3 reviewed at LPC, plans for v4 include
  - changes to cpufreq locking
  - provide interface for other scheduling classes to influence OPP
PMWG: Since HKG15 (cont’d)

- Fix constraints in genpd to improve fine grained power management
- Extending genpd to manage CPU clusters: RFCv2 and LPC discussions
PMWG: Current Focus

- Benchmarking, tuning and reviewing outstanding EAS patches
  - Goto status update session on Wednesday, 10:10
  - Goto technical deep-dive session on Thursday, 12:10
  - Go watch a demo at Demo Friday

- Remove constraints on effective use of runtime PM/genpd subsystems
  - Goto session on Monday, 16:10

- Improving CI setup with dedicated mini-lab
  - Goto related session on Friday, 11:15
VIRT: Three Technologies

KVM/ARM

QUEMU

Xen™
VIRT: KVM/ARM - since HKG15

- ARMv8 Guest Migration
- Live Migration (Dirty Page Tracking)
- GICv3 in-kernel emulation support
- ARMv8 Guest Debugging Support
- Platform Device Assignment (VFIO)
- VHOST Support
- Architected Timers IRQ Active Series
- Lazy VFP switching
- Backported all fixes to stable kernels
VIRT: KVM/ARM - current focus

- Feature parity with x86
- Performance Monitors (PMU Support)
- Performance and Latency Investigations
- ARMv8.1 VHE support
- PCIe Passthrough (VFIO)
- PCIe hotplug
VIRT: QEMU - since HKG15

- Linaro is Top 2 author, committer, and reviewer company for QEMU
  - Peter Maydell being the top author and committer!
- ACPI and PCI support on ARM
- Improved command line handling improving ARM QEMU user experience
- Improved CI setup
- GIC and virt board support for TrustZone (secure side)
VIRT: QEMU - current focus

- QEMU Multi-Threaded System Emulation
  - This is huge: go to the session Tuesday @10:10
- TrustZone:
  - ARMv8 (64 bit) CPU TrustZone
  - Split Address Space support
  - Work out security states in DT reporting
  - Add secure devices and run OP-TEE
- In-kernel KVM GICv3 patch review
- GICv3 Emulation
- Upstream QEMU Android Emulator support
VIRT: Xen - since HKG15 and now

- UEFI support for Xen added and upstreamed by LEG
- Main VIRT focus: Xen ACPI support on ARM
- Design Document written by Linaro under review
- Patch series on list:
  - Requires rework
  - Upstreaming
VIRT: Office hours

Thanks

Office hours on Thursday @ 4pm