BKK19-117
SWG Lightning talks

Joakim Bech, Jerome Forissier, Victor Chong, Jens Wiklander, Etienne Carriere
Agenda

- OP-TEE documentation
- Security incidents
- TA ASLR and shared base libraries
- Normal World virtualization support
- AOSP and Keymaster
- SPCI/SPRT
- Device Tree
- Buildroot support
- PKCS#11
- Full BKK19 sessions
OP-TEE documentation

- At the [hacking session](https://github.com/OP-TEE/optee_docs) at YVR18
  - We decided gather all docs, use Sphinx and restructuredText
  - Goal: A single location, avoid duplication and stale information

- What’s left?
  - A couple of docs still at Google drive
  - Keymaster / Gatekeeper OP-TEE architecture missing
  - Recommended OP-TEE configuration for product release

- Source: [https://github.com/OP-TEE/optee_docs](https://github.com/OP-TEE/optee_docs)
- Rendered documentation: [https://optee.readthedocs.io](https://optee.readthedocs.io)
Security vulnerabilities in OP-TEE

- Riscure mini audit in Q3/Q4 2018
- Applied our disclosure policy
  - 90 security embargo for issues with severity “medium/high/critical”
- Resulted in a pull request with 20 commits
  - “Fixes for security potential issues reported by Riscure #2745”

If you want to report an issue, please see:

https://optee.readthedocs.io/general/contact.html#vulnerability-reporting
TA ASLR

- **Address Space Layout Randomization** is a security technique to prevent exploitation of memory corruption vulnerabilities.
- When enabled, TAs are mapped into user space with a random offset.
- OP-TEE 3.5.0 will have a new config flag: CFG_TA_ASRL=y
  - Maximum offset can also be adjusted.
- Disabled by default except for vexpress-qemu_virt and hikey-hikey960
  - Increases memory usage due to more space needed for page tables.
  - Platforms need to tune accordingly.
Shared base libraries for TAs

- Trusted Applications always link against the following base libraries, which are built alongside OP-TEE OS
  - libutee: the GlobalPlatform TEE Internal Core API
  - libutils: a minimal C library
  - libmpa: "big numbers" support, or libmbedtls: "big numbers" and other crypto

- These libraries are normally static archives (*.a)

- OP-TEE 3.5.0 introduces CFG_ULIBS_SHARED to also produce shared objects
  - libutee.so, libutils.so, libmpa.so, libmbedtls.so used at TA link time
  - <UUID>.ta files used at run time (they are signed versions of *.so)

- Shared libraries reduce the amount of space used by TAs in persistent storage, since library code is not duplicated anymore

- They mostly make sense with the introduction of code page sharing (session BKK19-415)
Normal World virtualization support

- OP-TEE 3.5.0 supports virtualization in Normal World via `CFG_VIRTUALIZATION=y`
- This is still experimental
- Patches for XEN are being reviewed (v4 at https://www.mail-archive.com/xen-devel@lists.xenproject.org/msg40025.html)
- Documentation: https://optee.readthedocs.io/architecture/virtualization.html
AOSP and Keymaster

- Keymaster now part of OP-TEE AOSP build by default
  - Upstreaming of CA (normal world code) ongoing
  - Refactoring (converting PTA to TA) ongoing
  - Several compatibility issues with vold reported

- Established quarterly release process
  - In sync with OP-TEE releases, e.g.
    - https://github.com/linaro-swg/optee_android_manifest/tree/optee_kmgk_3.3.0
    - https://github.com/linaro-swg/optee_android_manifest/tree/optee_kmgk_3.4.0
  - *Only* support current latest AOSP + OP-TEE version

- Weekly CI builds
  - http://snapshots.linaro.org/android - under android-hikey{960}-optee-*
  - Experimental!

- Added support for a hikey960 build, but not stable
  - Adb over usb does NOT work, although adb over tcp can be workaround, but..
  - Wifi errors
  - A couple of users reported screen/monitor issues and console noise

- Eliminated root permission dependency
  - Run xtest as shell or system user
Isolation using virtualization in the Secure world

- The white paper “Isolation using virtualization in the Secure world” is available for download at
  https://developer.arm.com/products/architecture/security-architectures
- The Armv8.4 architecture introduces Secure EL2 extension
  - Enables virtualization in the secure world
  - That is, sandboxing of the Trusted OS or Secure Partition
- Secure Partition Client Interface specification
  - Latest version is Alpha2
  - Patched versions of OP-TEE has been used with both Alpha1 and Alpha2
  - Standardizes the communication between the Trusted OS and its driver in normal world
  - Can be used even without virtualization
- Secure Partition runtime specification
  - Latest version is Alpha0
Device Tree

- Up to 3.3.0 OP-TEE used DTB to share configurations with the non-secure world
  - Enabled from CFG_DT=y
  - Expects to find the DTB loaded in memory prior OP-TEE boot
  - OP-TEE gets main memory location(s) and console, and gets or adds PSCI configuration
  - OP-TEE adds few resources information for the benefit of the non-secure world

- Alternate use recently merged: Add nodes as overlay fragments
  - Enabled from CFG_EXTERNAL_DTB_OVERLAY=y
  - Allows non-secure to merge a main DT with fragments provided by OP-TEE

- Alternate use recently merged: built-in DTB and in-tree DTS files
  - Enabled from CFG_EMBED_DTB=y
  - OP-TEE core image contains a DTB image inside a read-only (pageable) section
  - Platform and drivers get secure configuration from it
  - DTB can be built from in-tree DTS files (CFG_EMBED_DTB_SOURCE_FILE)
Buildroot support

- **https://buildroot.org**, Make Embedded Linux Easy
- Contribution [1] in Buildroot to support OP-TEE packages
- OP-TEE mandates changes in Buildroot packaging of TF-A
  - Contribution to build TF-A for OP-TEE support [2], under review
  - [2] also proposes changes to support Armv7-A targets and a bit of debug
- Defconfig and runtime test over Qemu/Armv7-A emulations, under review
  - [2] introduces regression runtime test, as per Buildroot team request
- Many thanks to the Buildroot team for their patience and help

[1] [http://patchwork.ozlabs.org/patch/1033415 to 1033419 patch series](http://patchwork.ozlabs.org/patch/1033415 to 1033419 patch series)
[2] [http://patchwork.ozlabs.org/patch/1052227 to 1052231 patch series](http://patchwork.ozlabs.org/patch/1052227 to 1052231 patch series)
PKCS#11

- OP-TEE/PKCS#11 was presented at HKG18 [1] as a initiative
  1 year later... a basework on private topic branches and a bunch of code to be reviewed
- Topic branch sks from [2], [3], [4] stores the on-going work latest state
  - PKCS#11 support for login, session and persistent object support
  - Reduce set of cryptography: AES flavors, RSA flavors, few HMAC
- Plan: get this work reviewed, matured and integrated into OP-TEE
- What’s next?
  - DH, DSA, Elliptic curves. Would also like certificate support
  - Maturity of the trusted application, regression tests
- Thanks to contributors for fixes and improvements (Gabor, Rouven)
  - Gabor opened a ssh shell with RSA keys handled by OP-TEE through pkcs11-tools

Security sessions at BKK19

- **BKK215 - TPM in TEE (Joakim Bech)**
  - Tuesday, April 2 - 12:00pm - 12:50pm
  - Session Room 2 (Lotus 3-4)

- **BKK415 - Sharing code pages (Jens Wiklander)**
  - Thursday, April 4 - 12:00pm - 12:25pm
  - Keynote Room (World Ballroom BC)

- **Keymaster internals**
  - Cancelled, since the speaker couldn’t attend BKK19.

- **BKK19-419 Debugging with OP-TEE (Sumit Garg)**
  - Thursday April 4 - 12:30pm - 12:55pm
  - Keynote Room (World Ballroom BC)
Thank you
Join Linaro to accelerate deployment of your Arm-based solutions through collaboration

contactus@linaro.org