stairCASE Measurement Architecture

Perry Alexander

August 13, 2018

1 Architecture

1.1 Ground Station

- seL4 instance running on ODROID
- User Virtual Platform (UVP) on seL4 VMM
- Linux instance on seL4 VM
- User AM as Linux process
- UxAS as Linux process
- Platform AM as CAmkES component
- Attestation Manager (seL4AM)

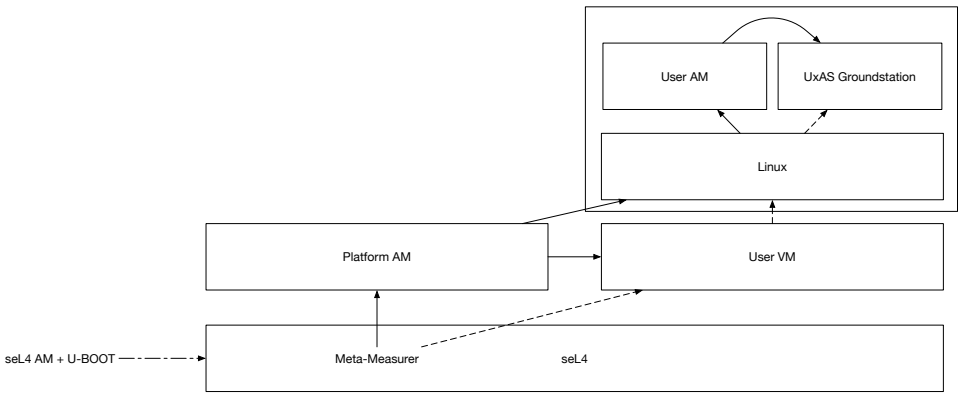

Figure 1: Measurement & Attestatin Architecture

1.2 Mission board

- Mission AM as dictated by mission board designers

1.3 Roots of Trust

- RoT for Measurement - UBOOT
- RoT for Reporting - place key
- RoT for Storage - ??

2 Places

- Mission AM - Appraisal only. Makes requests of ground station AMs and appraises results. No mutual attestation at this time, but could add later if desirable.
- seL4 AM - Hashes the seL4 instance at startup and performs runtime integrity measurement. This may conflate with what U-BOOT currently does. Note that UBOOT performs a signature check and does not currently measure the seL4 imagage. Potentially the root of trust for measurement.
- Platform AM - Hashes the UVP VM at startup and performs runtime integrity measurement. Is hashed as a part of the seL4IM measurement. Consider meta-measurer runnning as CAmkES component to ensure integrity. seLAM might do this as well.
- UVP AM - Hashes the UxAS instance at startup and performs runtime integrity measurement. Is hashed as a part of the Platform measurement. Serves as the interface to the attestation platform.

3 Boot Measurement Story

1. UVP Linux VM hashes and starts UVP AM.
2. UVP Linux VM hashes and starts UxAS groundstation. Makes UVP AM aware of UxAS. UVP AM measures UxAS.

1. UBOOT starts seL4 AM and seL4. seL4 AM measures seL4 image and stores in TrustZone. seL4 AM is made aware of seL4. seL4 AM may be a part of UBOOT. UBOOT has a built-in SHA-256 capability.
2. seL4 starts and measures Platform AM as CAmkES component.
3. seL4 measures and starts User Virtual Platform (UVP) consisting of Linux VM and a RAMdisk.
   (a) Hashes and starts the Linux kernel as VM
   (b) Hashes and mounts RAMDisk

sel4 Makes the Platform AM CAmkES component aware of UVP and RAMDisk.

4. UVP Linux VM hashes and starts UVP AM from a RAMDisk image.
5. UVP Linux VM hashes and starts UxAS groundstation from a RAMDisk image. Makes UVP AM aware of UxAS executing.
6. UVP AM measures UxAS and begins accepting attestation requests from Mission AM

4 Runtime Measurement Story

1. seL4 AM measures sel4 instance
2. seL4 AM measures Platform AM (speculative)
3. Platform AM measures UVP VM and UVP AM
4. UVP AM measures UxAS groundstation and serves as interface to mission platform AM

5 Appraisal Story

- Mission board is aware of the UVP AM and sends requests to it.
- UVP AM is aware of Platform AM and seL4IM and sends requests to them as required by Mission Board requests
- Two kinds of attestation requests
  - Shallow attestation requests invoke UVP AM to measure the application and local platform
  - Deep attestation requests invoke UVP AM to make requests of Platform AM and seL4IM

6 APDT terms

$$\mathsf{seL4Meas} = @_{\mathsf{seL4AM}}\,(\mathsf{n}_1\,;\,\mathsf{USM\ seL4Hash}\ \epsilon\,;\,\mathsf{KIM}_{\mathsf{platformAM}}\ \mathsf{pkim}\ \epsilon\,;\,\mathsf{SIG})$$

$$\mathsf{platformMeas} = @_{\mathsf{platformAM}}\,(\mathsf{n}_2\,;\,\mathsf{USM\ seL4Meas\ n}_1\,;\,\mathsf{KIM}_{\mathsf{userAM}}\ \mathsf{ukim}\ \epsilon\,;\,\mathsf{SIG})$$

7 Open Questions

- RoT for Storage - where can we put measurements and keys that provides confidentiality and integrity?

  - TrustZone proto-TPM - Need to jack with TrustZone. Possibly store first measurement here and use CAmkES component for the rest.
  - CAmkES component - Need to store measurements prior to seL4 start
- Hosting and running KIMs - what will our KIMs be and how will they function?
  - LKIM for UVP AM

8 Odds and Ends

- UBOOT can hash images
- UBOOT runs through TrustZone in some way that we need to understand
- seL4 VMM can start with 2 VMs
  - one is an OS Kernel
  - one is typically a RAM Disk
- New boot structure
  - start the kernel
  - mount the RAMDisk
  - start the user apps from the ramdisk