android Bootcamp 2016

Verified Boot and Encryption

Thursday January 21, 2016

Agenda

State of Play

Attack!

Verified Boot enhancements

Keymaster enhancements

Other enhancements

Remaining attacks

State of Play (Android 6.0)

Verified Boot

- Mandatory on all but slow devices
- May fall back to logging mode when errors detected

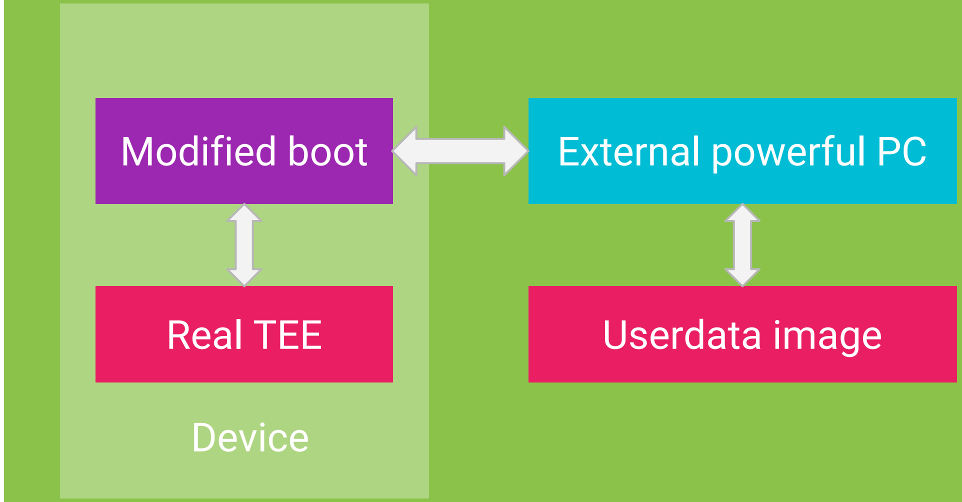
Encryption

- Mandatory on all but slow devices
- Keys tied to Keymaster
- Keymaster ties keys to root of trust through Verified Boot

Common attack

Assumption—attacker can read and modify contents of eMMC freely.

1. Replace boot image. Since verified boot not enforcing, the attacker can replace boot image so long as it claims to be signed by same OEM.
2. Install service that calls into Trusted Execution Environment (TEE) to sign password-derived hashes.
3. Write off-device app to produce such hashes and test the returned signed hashes.
4. Can try 10 passwords/second.



Source: Oliver Kunz—https://ch.linkedin.com/in/kunzoliver

Defense - strong password

- 10/second is 864,000/day
- An 8-digit PIN would take 2 months to break on average. A reasonable password should be more secure.
- Almost no users are going to do this (although fingerprint sensors make this marginally more likely)

Verified Boot Enhancements in N

Step 1

- Measure verified boot failure rates
- Add forward error correction to verified boot
- Verified boot always in enforcing mode

Step 2

- Add versioning information to root of trust for all partitions

Keymaster Enhancements

Step 1

- Tie in root of trust version information
- On version update, upgrade keys
- Do not decrypt on downgrade

Step 2

- Rate limit attempts

Step 3

- SELinux key restrictions

Other Enhancements

Step 1

- Monthly updates
- Easy updates via A/B leading to high rate of takeup of monthly updates

Remaining Attacks

Kernel compromise of device after power cycle and ‘chip off’

- Use compromise to call into TEE to brute force password
- Current kernel: rollback protection and regular updates
- Rate limited to 1 try per 10 seconds

Kernel compromise of locked live device (i.e. key is in memory)

Memory freeze attacks

TEE compromise

Direct hardware attacks

- Still effective, but all are hard!

THANK YOU

OEM asks

- Boot loader changes
  - Provide OS version and patch level to TEE.
  - Don’t boot when locked and boot partition doesn’t pass verification.
  - Request consent when mounting a possibly corrupted system partition.
- Partition format
  - All verified partitions must include a footer that includes OS version and patch level.
  - The crypto footer for all encrypted partitions still using full-disk encryption must include OS version and patch level.