Android Widevine on OP-TEE

David Brown
Agenda

- Motivations
- How not to do it
- OP-TEE
- General solutions
- Overview of Widevine
Motivation
Motivation

- Software playback
- Red arrow, bad!
- Creators sad, no HD
Agenda

- Motivations
- **How not to do it**
- OP-TEE
- General solutions
- Overview of Widevine
How not to do it?

- Plaintext video passes through userspace
- Find exploit in player, or many other things
- Root makes it trivial to get

- Notice the key is also in userspace
- This is bad
Can we do better?
Can we do better?

- Less is accessible
- Plaintext still in userspace
- Creators still sad
All plaintext in kernel?

Media player

license manager

Net

decryption

secret key

Video Driver

Kernel

Media Server

License Server

key info
encrypted data
plaintext

hw codec
All plaintext in kernel?

- Better, no plaintext in userspace
- Key still there
- Kernel is vulnerable
Key in kernel

- key info
- wrapped key info
- encrypted data
- plaintext
Key in kernel

- All key/plaintext now in kernel
- Content protected from userspace
- Kernel exploits possible
- Creators still sad
OP-TEE

- ARM® TrustZone®
  - Trustable through boot into secure OS
  - Runs alongside Kernel
- GlobalPlatform TEE Specification
  - OP-TEE is our implementation
  - Allows trusted apps, and clients
OP-TEE

REE

TEE

Client

Client

Kernel

OP-TEE OS

TA

TA

TA

TA

TA
DRM in TEE

- key info
- wrapped key info
- encrypted data
- plaintext

Media Server
License Server

Media player
license manager

Net
Video Driver

Kernel

OP-TEE
Media TA

decryption

keybox
secret key

hw codec
DRM in TEE

- Almost there, key is in TEE
- Plaintext video still available at end
- Providers **still** sad
One more thing

- We need a weird buffer
  - Accessible to secure side
  - Not readable by unsecure (even kernel)
  - Accessible by HW decoder

- SMAF
  - Secure memory allocator
  - TEE can decode into this memory
  - HW can play it back

- It’s tricky to get right, only certain HW should have access
Agenda

- Motivations
- How not to do it
- OP-TEE
- General solution
- Overview of Widevine
Keybox

1. Keypair

- key info
- wrapped key info
- encrypted data
- plaintext

Media Server
License Server

OP-TEE
Media TA

Kernel

Decryption

keybox
secret key

Media player
license manager

Video Driver

Net

hw codec
Keybox

1. Keypair
2. Install
Content Key

3. Content Key

- key info
- wrapped key info
- encrypted data
- plaintext

Media Player
License Manager

Net
Video Driver
Kernel

Decryption

OP-TEE
Media TA

keybox
secret key

License Server
Media Server

Linaro Connect
Las Vegas 2016

Engineers and Devices Working Together
Agenda

- Motivations
- How not to do it
- OP-TEE
- General solution
- Overview of Widevine
Widevine

- CDM (content decryption module) for Android
- Specifics are for partners only
- Plugin based, we implement oemcrypto.so using our client lib and TA
Status

- Working on HiKey board
- OP-TEE available for Android AOSP
- We have a liboemcrypto.so and TA for Widevine CDM
- Several security things missing
  - No trusted boot chain, TEE could be modified (HiKey issue)
  - SMAF not yet supported (patches in progress)
    https://lkml.org/lkml/2016/9/7/133
  - No HW video playback, buffers still need to be visible to software (HiKey work in progress)
Thank You

#LAS16
For further information: www.linaro.org
LAS16 keynotes and videos on: connect.linaro.org