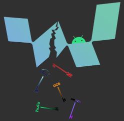
Exploring Widevine for Fun and Profit

Gwendal Patat, Mohamed Sabt, Pierre-Alain Fouque

Univ Rennes, CNRS, IRISA

May 26th, 2022



Over-the-Top Platforms

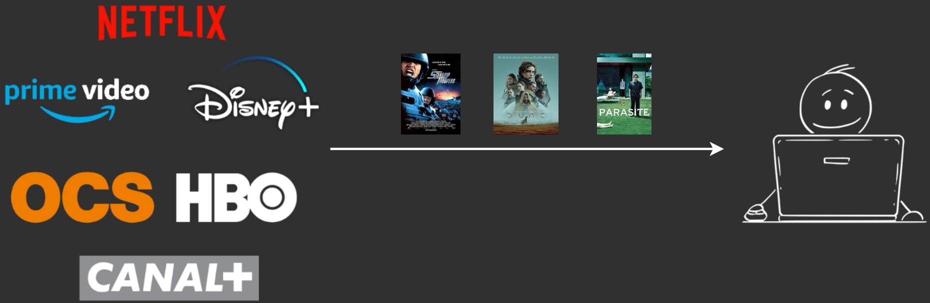
NETFLIX
prime video
Disney+
OCS
HBO
CANAL+

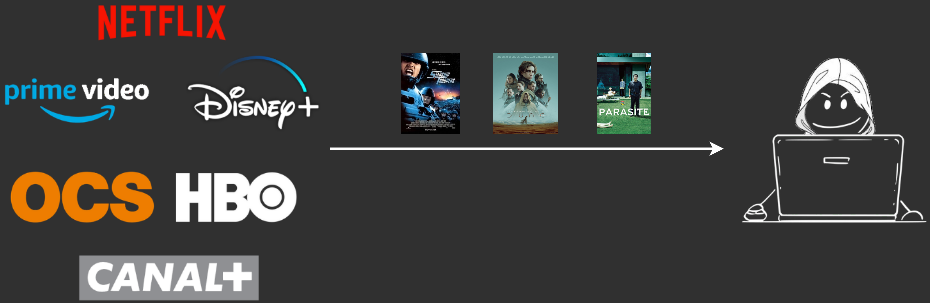
NETFLIX

prime video Disney+

OCS HBO

CANAL+


NETFLIX
prime video
Disney+
OCS
HBO
CANAL+
PARASITE


NETFLIX
prime video
Disney+
OCS
HBO
CANAL+
PARASITE

Attacker Model

Capabilities

- Legitimate User Access
- Full Device Control

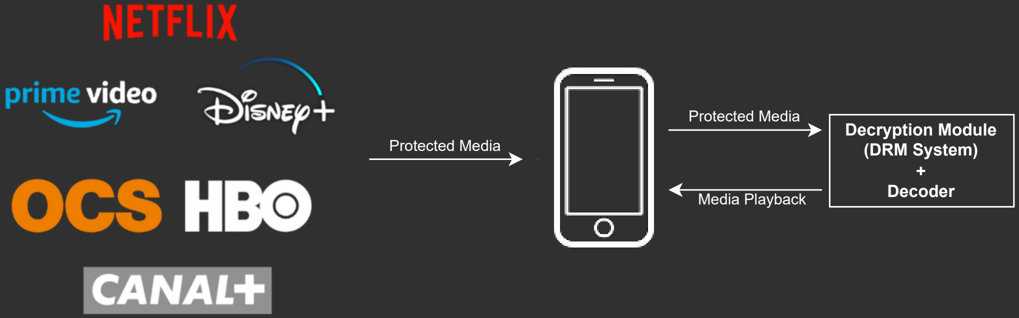
Goal

- Redistribution of media

Some DRM Solutions

Figure – Example of DRM Systems

Generic DRM Usage



Protected Media

Protected Media

Decryption Module (DRM System) + Decoder

Media Playback

Figure – OTTs and DRMs.

Old DRM

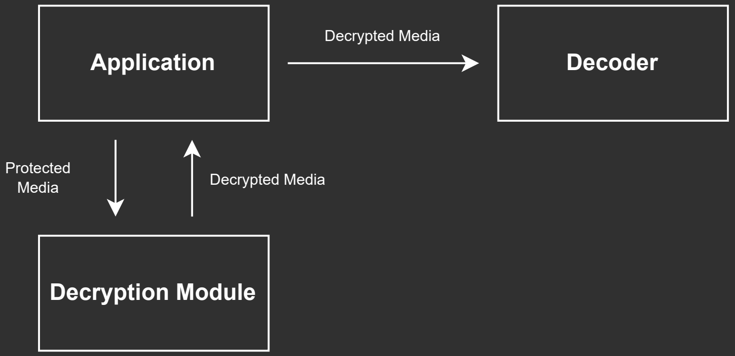


Figure – Decryption Module outside the OTT App.

Modern DRM

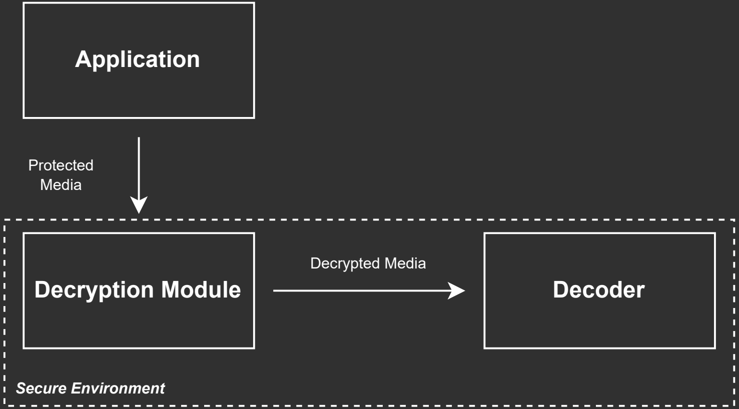


Figure – Both Decryption Module and Decoder in a secure environment.

WIDEVINE

Widevine

General

- Closed-source.
- Owned by Google since 2011.
- One of the most deployed DRM (Android TV, Smartphone, Browser, ...).

Levels

- L1 : Media decryption and playback in secure environment (e,g,. TEE).
- L2 : Only media decryption in secure environment.
- L3 : Media decryption and playback software-only solution.

Widevine

General

- Closed-source.
- Owned by Google since 2011.
- One of the most deployed DRM (Android TV, Smartphone, Browser, ...).

Levels

- L1 : Media decryption and playback in secure environment (e,g,. TEE).
- L2 : Only media decryption in secure environment.
- L3 : Media decryption and playback software-only solution.

Our Contributions

- RE of Widevine components in the Android ecosystem.
- Description of Widevine as a protocol.
- The WideXtractor tool[1] for Widevine monitoring.
- Proof-of-Concept[2] for Widevine Key ladder mimicking.
- L3 Root-of-trust recovery on Android.

[1] https://github.com/Avalonswanderer/wideXtractor

[2] https://github.com/Avalonswanderer/widevine_key_ladder

Our Contributions

- RE of Widevine components in the Android ecosystem.
- Description of Widevine as a protocol.
- The WideXtractor tool[1] for Widevine monitoring.
- Proof-of-Concept[2] for Widevine Key ladder mimicking.
- L3 Root-of-trust recovery on Android.

[1] https://github.com/Avalonswanderer/wideXtractor

[2] https://github.com/Avalonswanderer/widevine_key_ladder

Our Contributions

- RE of Widevine components in the Android ecosystem.
- Description of Widevine as a protocol.
- The WideXtractor tool[1] for Widevine monitoring.
- Proof-of-Concept[2] for Widevine Key ladder mimicking.
- L3 Root-of-trust recovery on Android.

[1] `https://github.com/Avalonswanderer/wideXtractor`

[2] `https://github.com/Avalonswanderer/widevine_key_ladder`

Our Contributions

- RE of Widevine components in the Android ecosystem.
- Description of Widevine as a protocol.
- The WideXtractor tool[1] for Widevine monitoring.
- Proof-of-Concept[2] for Widevine Key ladder mimicking.
- L3 Root-of-trust recovery on Android.

[1] `https://github.com/Avalonswanderer/wideXtractor`

[2] `https://github.com/Avalonswanderer/widevine_key_ladder`

Our Contributions

- RE of Widevine components in the Android ecosystem.
- Description of Widevine as a protocol.
- The WideXtractor tool[1] for Widevine monitoring.
- Proof-of-Concept[2] for Widevine Key ladder mimicking.
- L3 Root-of-trust recovery on Android.

[1] https://github.com/Avalonswanderer/wideXtractor

[2] https://github.com/Avalonswanderer/widevine_key_ladder

Widevine and Android

Widevine in Android (1)

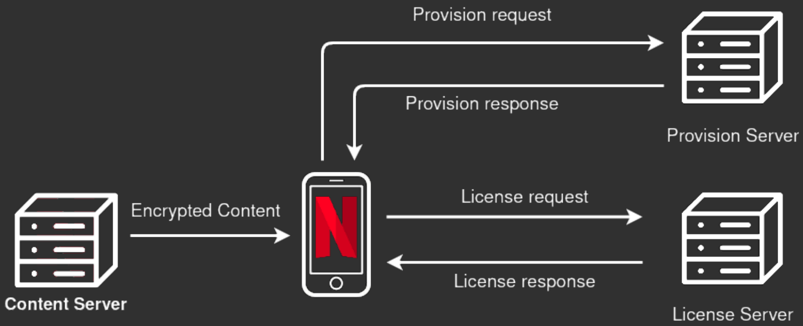


Figure – DRM under Android

Widevine in Android (2)

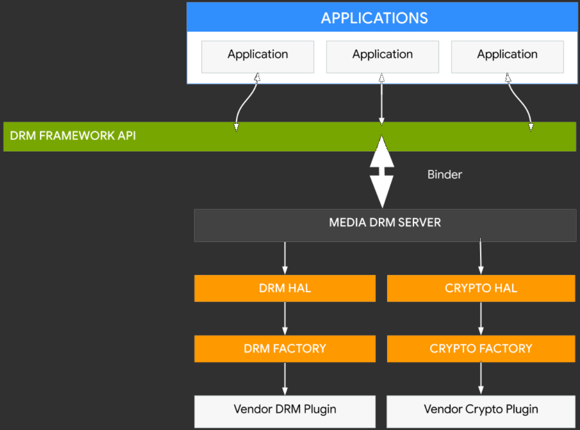


Figure – DRM Framework before Android 11 (src : source.android.com)

Widevine in Android (3)

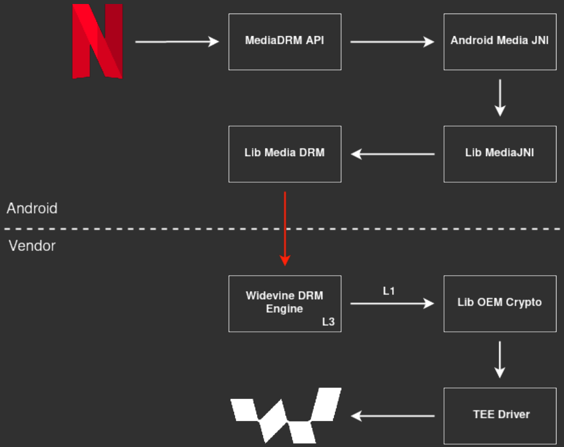


Figure – Android DRM Ecosystem with Widevine

WideXtractor

- Python tool based on Frida[3].
- Attached to the **Widevine DRM Engine** for L1 and L3 compatibility.
- Avoid Apps anti-debug techniques.

- Monitor the control flow of Widevine execution.
- Log parameters and return values.
- Dump buffers linked to provisioning for analysis.

[3] https://frida.re/

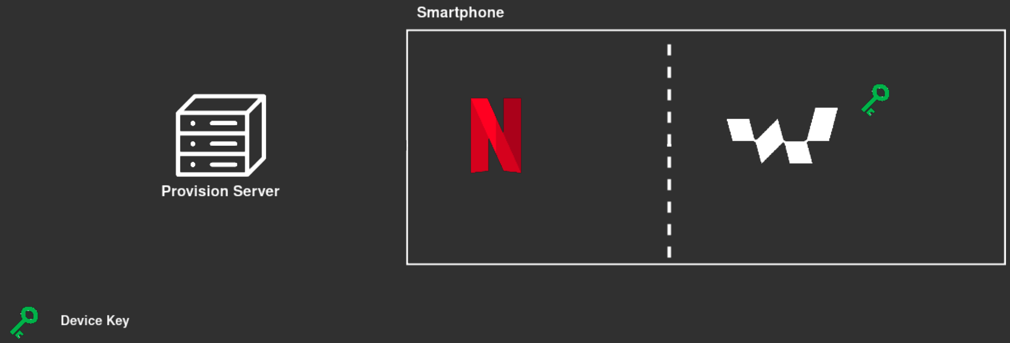
WideXtractor

- Python tool based on Frida[3].
- Attached to the **Widevine DRM Engine** for L1 and L3 compatibility.
- Avoid Apps anti-debug techniques.

- Monitor the control flow of Widevine execution.
- Log parameters and return values.
- Dump buffers linked to provisioning for analysis.

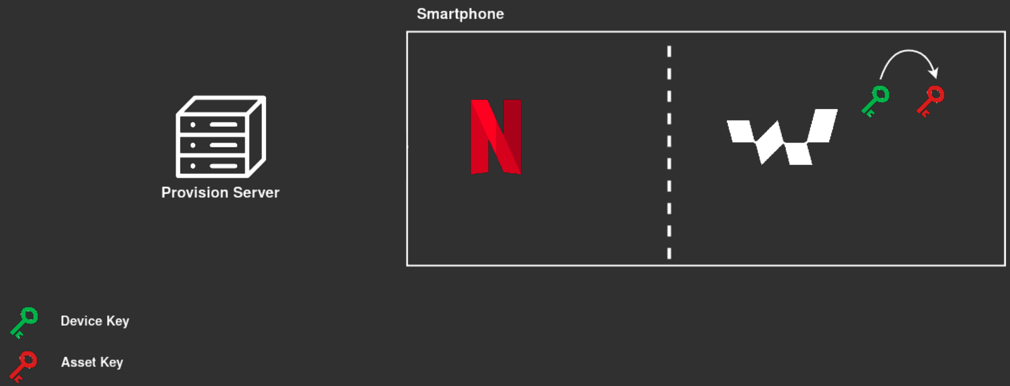
[3] `https://frida.re/`

Step 1 : Provisioning



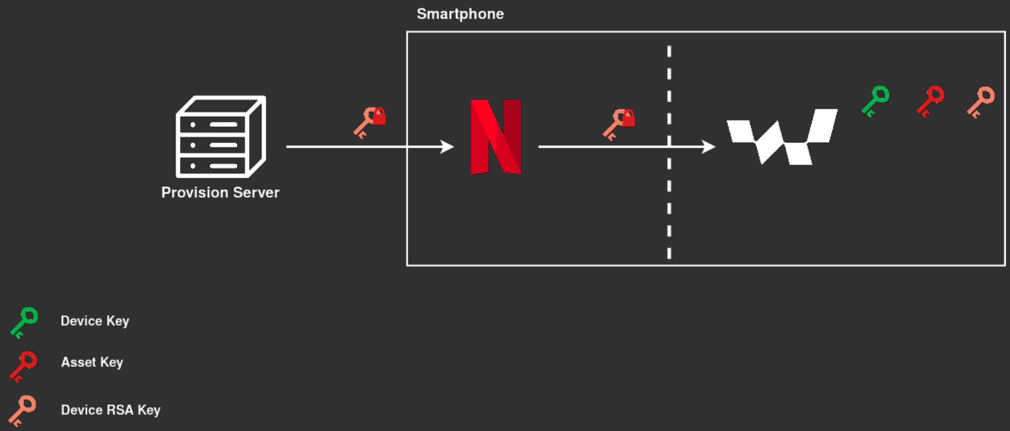
Initial State.

Step 1 : Certificate Provisioning



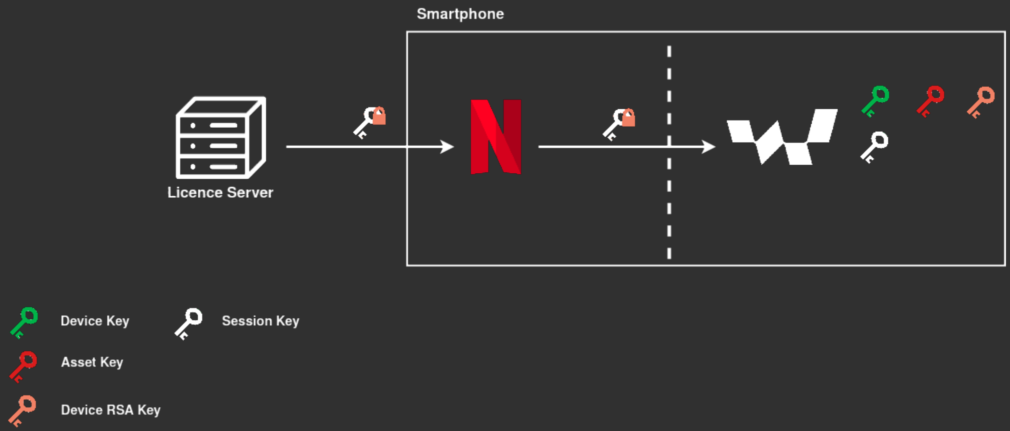
Asset Key Derivation.

Step 1 : Certificate Provisioning



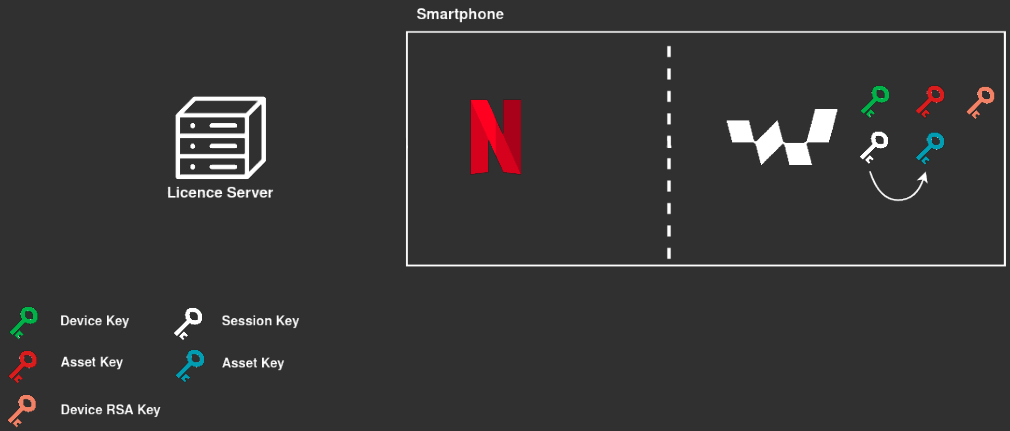
RSA Key reception.

Step 2 : License Acquisition



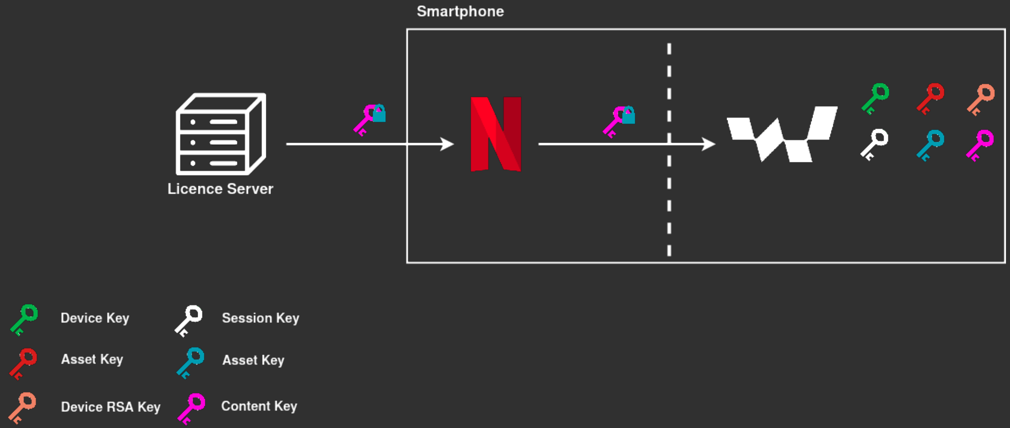
Session Key reception.

Step 2 : License Acquisition



New Asset Key Derivation.

Step 2 : License Acquisition



Smartphone

Licence Server

Device Key

Asset Key

Device RSA Key

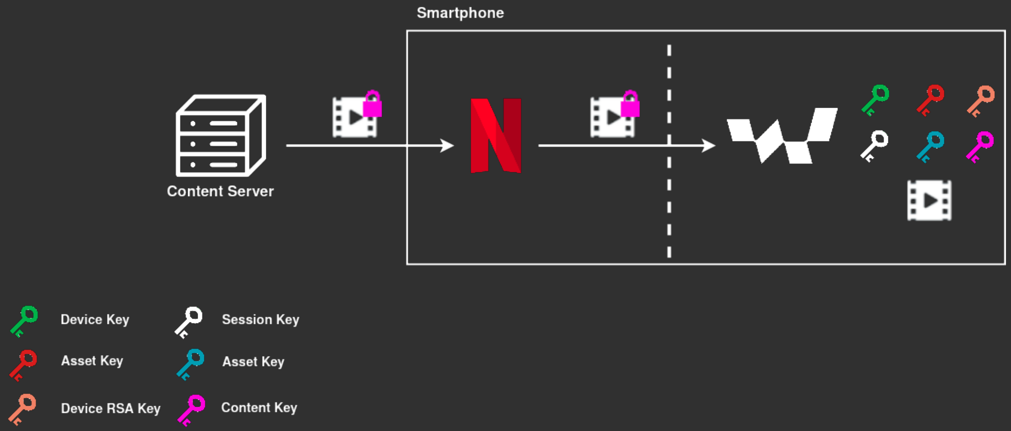
Session Key

Asset Key

Content Key

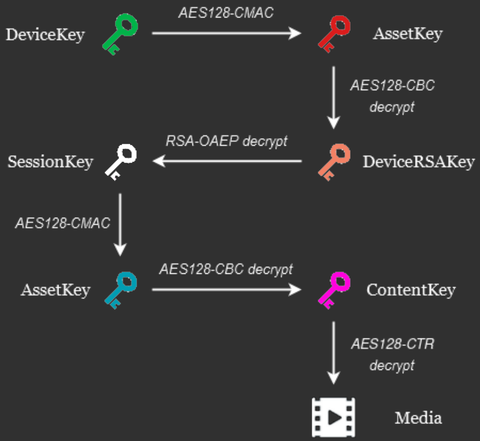
Content Key reception.

Step 3 : Media Decryption



Media decryption.

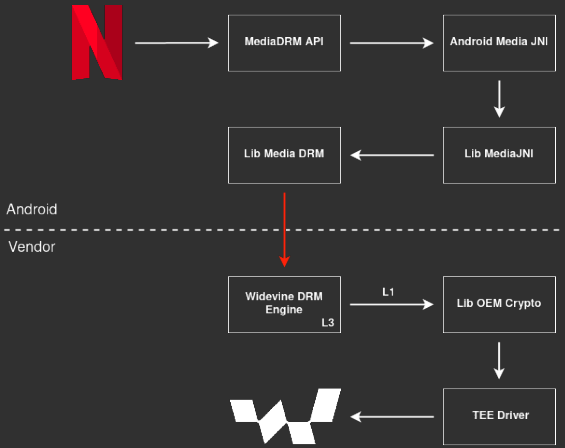
Crypto Key Ladder



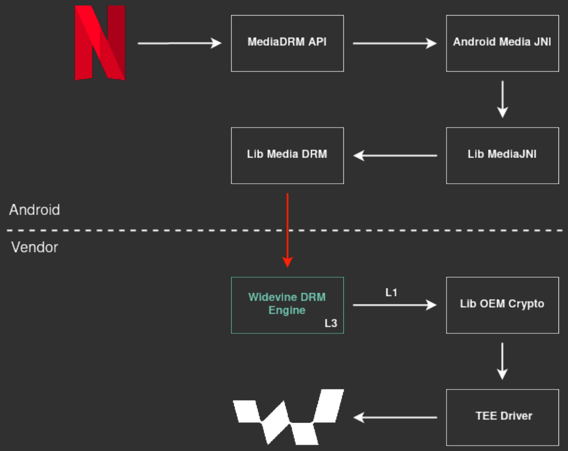
DeviceKey
AES128-CMAC
AssetKey
AES128-CBC decrypt
DeviceRSAKey
RSA-OAEP decrypt
SessionKey
AES128-CMAC
AssetKey
AES128-CBC decrypt
ContentKey
AES128-CTR decrypt
Media

Figure – Widevine Crypto Key Ladder

Android L3 RoT Recovery


MediaDRM API
Android Media JNI
Lib MediaJNI
Lib Media DRM
Android
Vendor
Widevine DRM Engine
L3
L1
Lib OEM Crypto
TEE Driver

L3 Root-of-Trust Recovery



MediaDRM API

Android Media JNI

Lib MediaJNI

Lib Media DRM

Android

Vendor

Widevine DRM Engine

L3

L1

Lib OEM Crypto

TEE Driver

Reversing the obfuscation **can easily be avoided** thanks to an **insecure memory deallocation** with *munmap*.

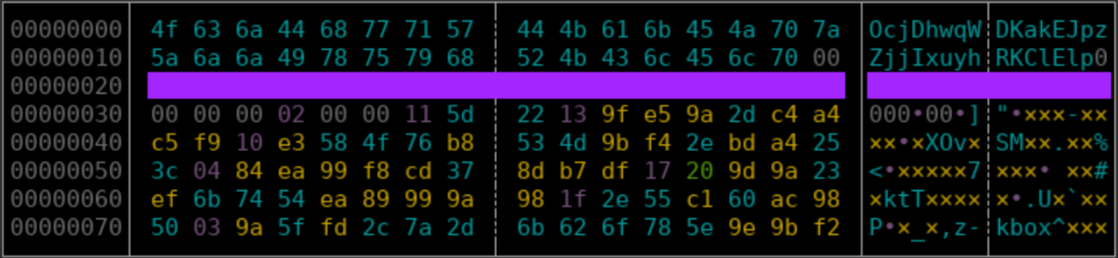
Reversing the obfuscation **can easily be avoided** thanks to an **insecure memory deallocation** with *munmap*.

Widevine KeyBox : RoT structure

Field	**Description**	**Size (bits)**
Device ID	Internal Device ID	256
Device Key	128-bit RoT AES key	128
Provisioning Token	Used by provision requests	576
Magic Number	‘kbox’ (0x6b626f78)	32
CRC32	CRC32 validating the keybox integrity	32
Total		**1024**

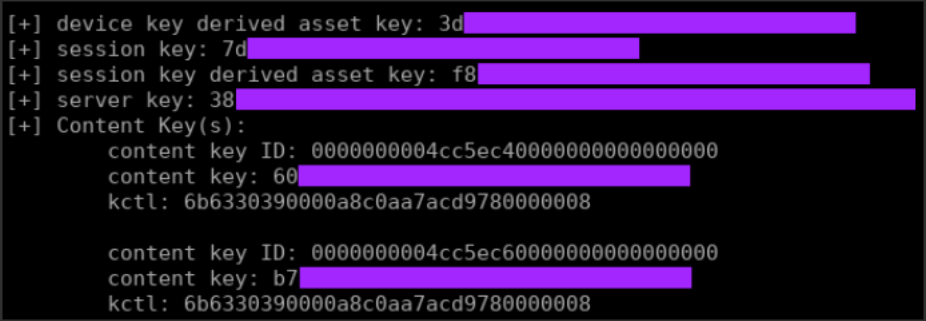
Table – Widevine Keybox

Our Keybox



```
00000000  4f 63 6a 44 68 77 71 57  44 4b 61 6b 45 4a 70 7a  OcjDhwqW┊DKakEJpz
00000010  5a 6a 6a 49 78 75 79 68  52 4b 43 6c 45 6c 70 00  ZjjIxuyh┊RKClElp0
00000020  [redacted]
00000030  00 00 00 02 00 00 11 5d  22 13 9f e5 9a 2d c4 a4  000•00•]┊"•xxx-xx
00000040  c5 f9 10 e3 58 4f 76 b8  53 4d 9b f4 2e bd a4 25  xx•xXOvx┊SMxx.xx%
00000050  3c 04 84 ea 99 f8 cd 37  8d b7 df 17 20 9d 9a 23  <•xxxxx7┊xxx• xx#
00000060  ef 6b 74 54 ea 89 99 9a  98 1f 2e 55 c1 60 ac 98  xktTxxxx┊x•.Ux`xx
00000070  50 03 9a 5f fd 2c 7a 2d  6b 62 6f 78 5e 9e 9b f2  P•x_x,z-┊kbox^xxx
```

Key Ladder Mimicking



```
[+] device key derived asset key: 3d[redacted]
[+] session key: 7d[redacted]
[+] session key derived asset key: f8[redacted]
[+] server key: 38[redacted]
[+] Content Key(s):
        content key ID: 0000000004cc5ec40000000000000000
        content key: 60[redacted]
        kctl: 6b6330390000a8c0aa7acd9780000008

        content key ID: 0000000004cc5ec60000000000000000
        content key: b7[redacted]
        kctl: 6b6330390000a8c0aa7acd9780000008
```

Responsible Disclosure

- Disclosure to Google in June 2021.
  - CVE-2021-0639.[4]
  - Android Security Bulletin August 2021.[5]

[4] https://www.cve.org/CVERecord?id=CVE-2021-0639

[5] https://source.android.com/security/bulletin/2021-08-01#widevine

Takeaways

Widevine DRM :

- Full reverse of the Widevine protocol.
- Complete crypto key ladder for media consumption.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.

Takeaways

Widevine DRM :

- Full reverse of the Widevine protocol.
- Complete crypto key ladder for media consumption.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
    - with no fix possible for discontinued phones.

Takeaways

Widevine DRM :

- Full reverse of the Widevine protocol.
- Complete crypto key ladder for media consumption.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.

Takeaways

Widevine DRM :

- Full reverse of the Widevine protocol.
- Complete crypto key ladder for media consumption.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.

https ://people.irisa.fr/Gwendal.Patat/widevine-l3-android/

Thanks for your attention

@ gwendal.patat@irisa.fr

@avalonswanderer

Avalonswanderer