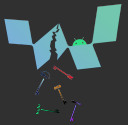
WideLeak: How Over-the-Top Platforms Fail in Android

Gwendal Patat, Mohamed Sabt, Pierre-Alain Fouque

University of Rennes, CNRS, IRISA

June 30th, 2022



Over-the-Top Platforms

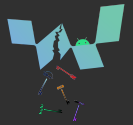
NETFLIX

prime video

Disney+

OCS HBO

CANAL+



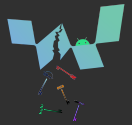
NETFLIX

prime video

Disney+

OCS HBO

CANAL+



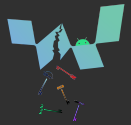
NETFLIX

prime video

Disney+

OCS HBO

CANAL+



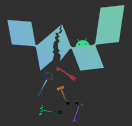
NETFLIX

prime video

Disney+

OCS HBO

CANAL+



Attacker Model

Capabilities

- Legitimate User Access
- Full Device Control

Goal

- Redistribution of media

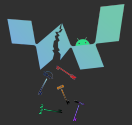
Some DRM Solutions

Microsoft PlayReady

FairPlay

WIDEVINE

Figure: Example of DRM Systems



Generic DRM Usage

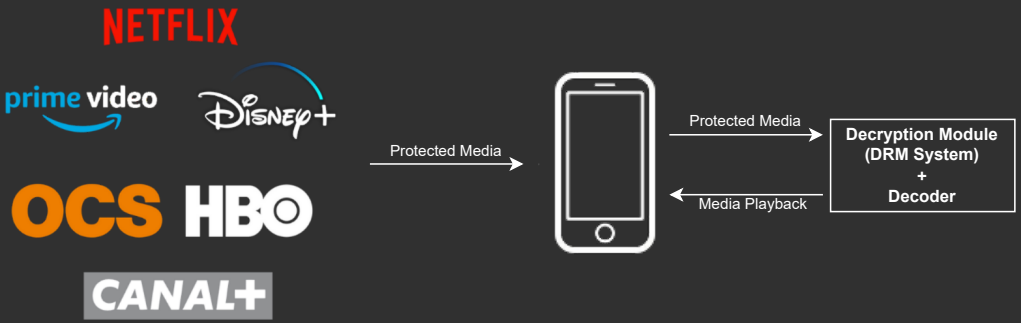
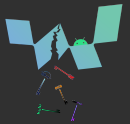


Figure: OTTs and DRMs.



Modern DRM

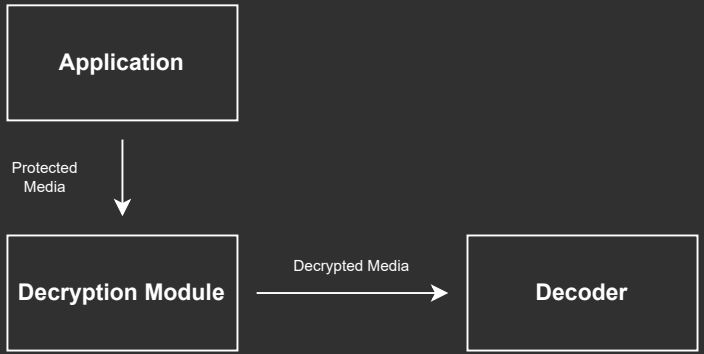
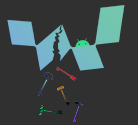


Figure: Decryption Module and decoder are outside of the application.



Modern DRM

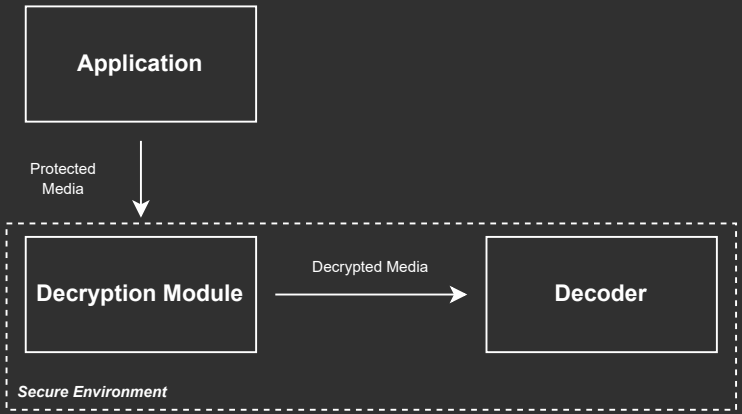
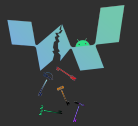
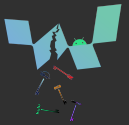


Figure: Both Decryption Module and Decoder are in a secure environment.




WIDEVINE



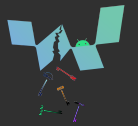
Widevine

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).
- L3: Media decryption and playback software-only solution.



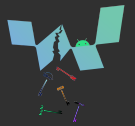
Widevine

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).
- L3: Media decryption and playback software-only solution.



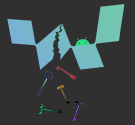
Widevine

General

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

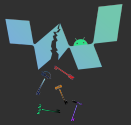
Levels

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



Our Contributions

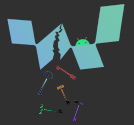
- Inspect the Widevine ecosystem in Android.
- Monitoring and reverse engineering of Widevine cryptographic operations.
- Empirical study on OTTs usage of Widevine regarding DRM guidelines.
- Unfixable Proof-of-Concept for Media recovery in legacy devices.[1]



[1] https://github.com/Avalonswanderer/widevine13_Android_PoC

Our Contributions

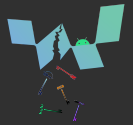
- Inspect the Widevine ecosystem in Android.
- Monitoring and reverse engineering of Widevine cryptographic operations.
- Empirical study on OTTs usage of Widevine regarding DRM guidelines.
- Unfixable Proof-of-Concept for Media recovery in legacy devices.[1]



[1] https://github.com/Avalonswanderer/widevine13_Android_PoC

Our Contributions

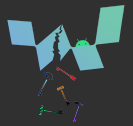
- Inspect the Widevine ecosystem in Android.
- Monitoring and reverse engineering of Widevine cryptographic operations.
- Empirical study on OTTs usage of Widevine regarding DRM guidelines.
- Unfixable Proof-of-Concept for Media recovery in legacy devices.[1]



[1] https://github.com/Avalonswanderer/widevine13_Android_PoC

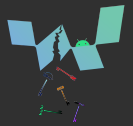
Our Contributions

- Inspect the Widevine ecosystem in Android.
- Monitoring and reverse engineering of Widevine cryptographic operations.
- Empirical study on OTTs usage of Widevine regarding DRM guidelines.
- Unfixable Proof-of-Concept for Media recovery in legacy devices.[1]



[1] https://github.com/Avalonswanderer/widevinel3_Android_PoC

Widevine and Android



DRM in Android

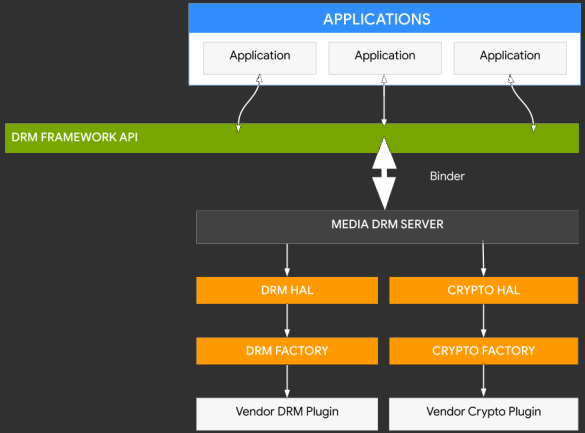
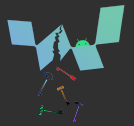


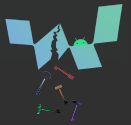
Figure: DRM Framework before Android 11 (src: source.android.com)



Widevine Monitoring

- Python tool based on Frida[2].
- Attached to the **Media DRM Server** 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.

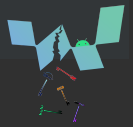


[2] https://frida.re/

Widevine Monitoring

- Python tool based on Frida[2].
- Attached to the **Media DRM Server** 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.



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

Simplified Key Ladder

Figure: Widevine under Android

Simplified Key Ladder

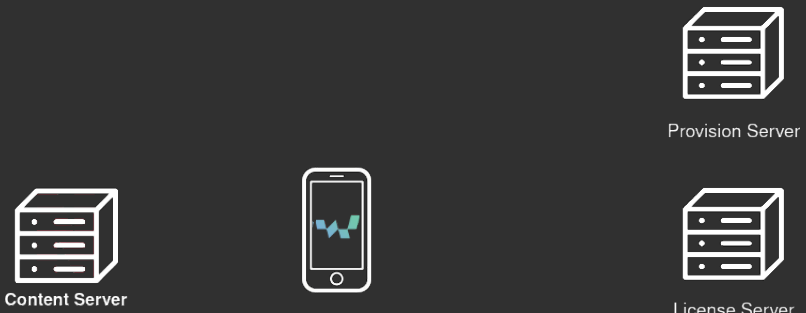


Figure: Widevine under Android

Simplified Key Ladder

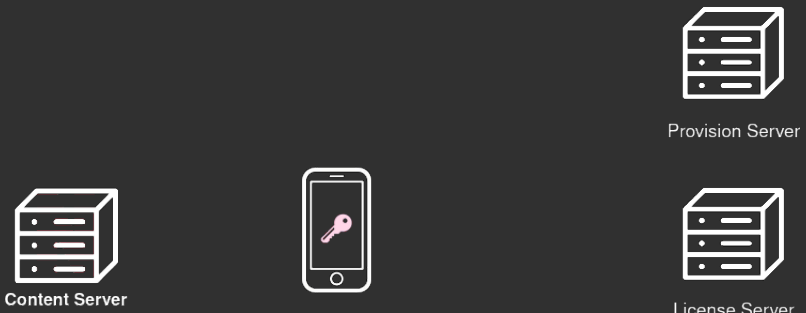


Figure: Widevine Root-of-Trust: Keybox

Simplified Key Ladder

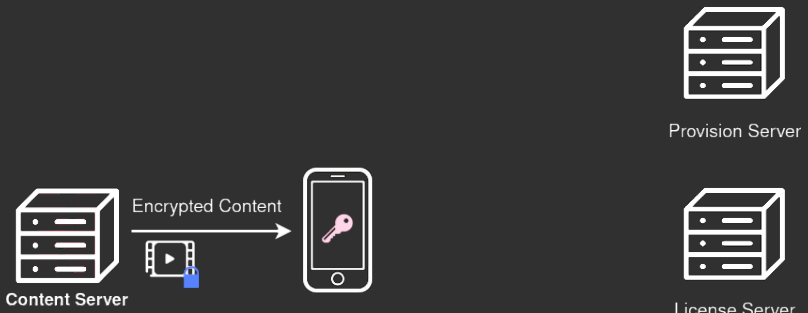


Figure: Encrypted Media Reception

Simplified Key Ladder

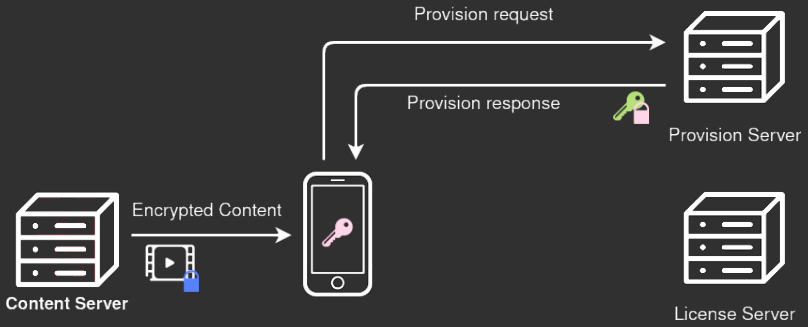


Figure: Widevine Provision Key

Simplified Key Ladder

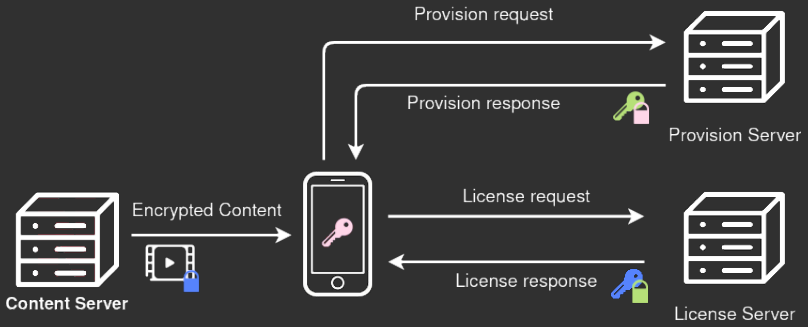
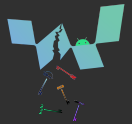
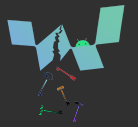


Figure: Widevine Content Key(s)



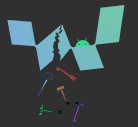
Widevine Guidelines

- *Recommended:* Audio and video encrypted with different Content Keys.
- *Minimum:* only the video is protected or same Content key as for the audio.
- Do not support devices no longer receiving security updates.



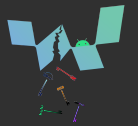
Widevine Guidelines

- *Recommended:* Audio and video encrypted with different Content Keys.
- *Minimum:* only the video is protected or same Content key as for the audio.
- Do not support devices no longer receiving security updates.



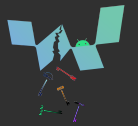
Widevine Guidelines

- *Recommended:* Audio and video encrypted with different Content Keys.
- *Minimum:* only the video is protected or same Content key as for the audio.
- Do not support devices no longer receiving security updates.

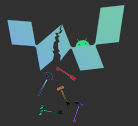


Widevine Guidelines

- *Recommended:* Audio and video encrypted with different Content Keys.
- *Minimum:* only the video is protected or same Content key as for the audio.
- Do not support devices no longer receiving security updates.



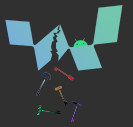
Is Widevine used at all by OTTs?



Do OTT apps use Widevine?

10 premium OTT apps based on
Google Play Store popularity and **regional bank account restrictions**.

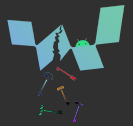
- Netflix (1,000M+)
- Disney+ (100M+)
- Amazon Prime Video (100M+)
- Hulu (50M+)
- HBO Max (10M+)
- Starz (10M+)
- myCANAL (10M+)
- Showtime (5M+)
- OCS (1M+)
- Salto (1M+)



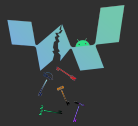
Do OTT apps use Widevine?

10 premium OTT apps based on
Google Play Store popularity and **regional bank account restrictions**.

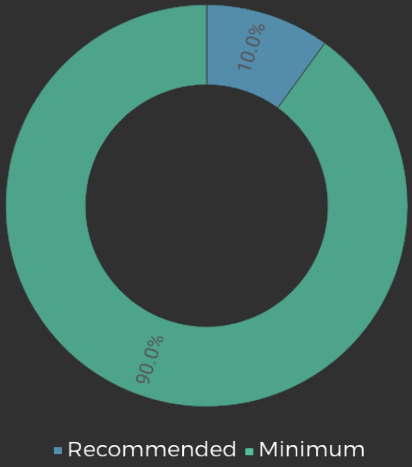
- Netflix (1,000M+)
- Disney+ (100M+)
- Amazon Prime Video (100M+)
- Hulu (50M+)
- HBO Max (10M+)
- Starz (10M+)
- myCANAL (10M+)
- Showtime (5M+)
- OCS (1M+)
- Salto (1M+)



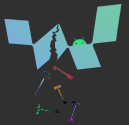
What about assets protection?



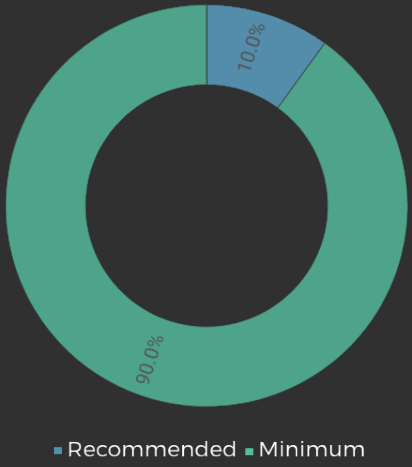
Assets Protection



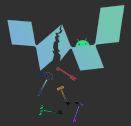
- 100% of OTTs protected their video assets.
- 30% of OTTs send their audio files in clear.
- Only one OTT uses different content keys for audio/video.



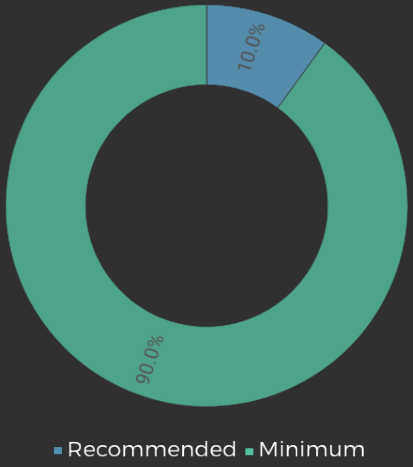
Assets Protection



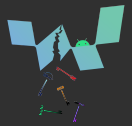
- 100% of OTTs protected their video assets.
- 30% of OTTs send their audio files in clear.
- Only one OTT uses different content keys for audio/video.



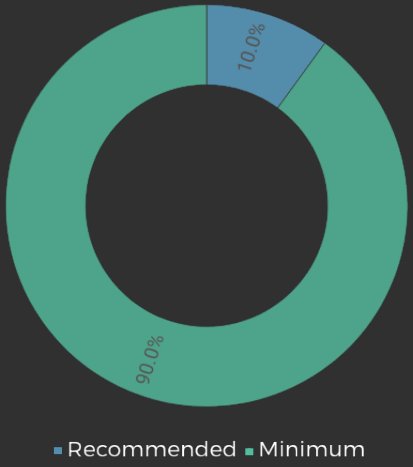
Assets Protection



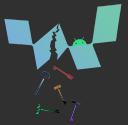
- 100% of OTTs protected their video assets.
- 30% of OTTs send their audio files in clear.
- Only one OTT uses different content keys for audio/video.



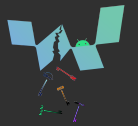
Assets Protection



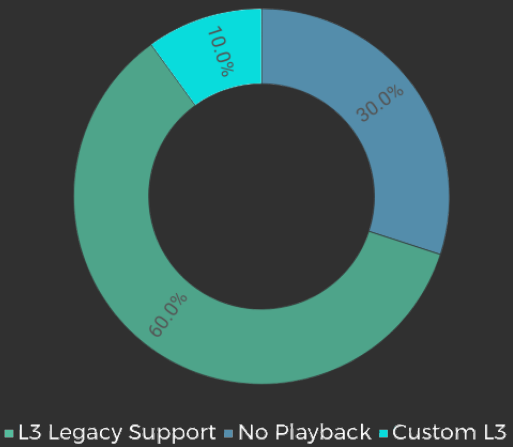
- 100% of OTTs protected their video assets.
- 30% of OTTs send their audio files in clear.
- Only one OTT uses different content keys for audio/video.



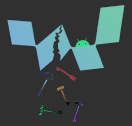
Are discontinued phones still supported?



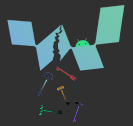
L3 Legacy Phone Support

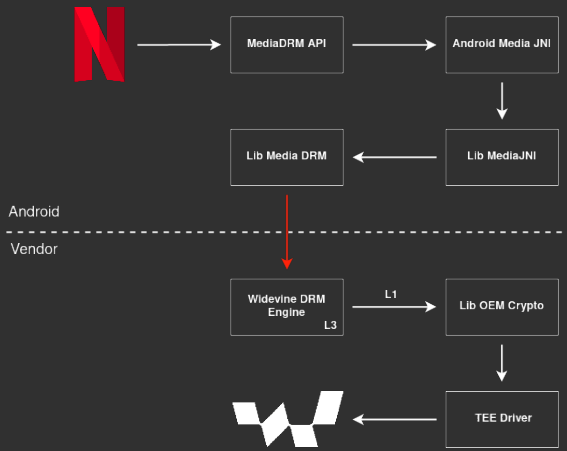


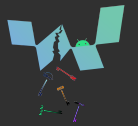
- Most OTTs chose to ignore revocation recommendations of Widevine and to send media to L3 devices.

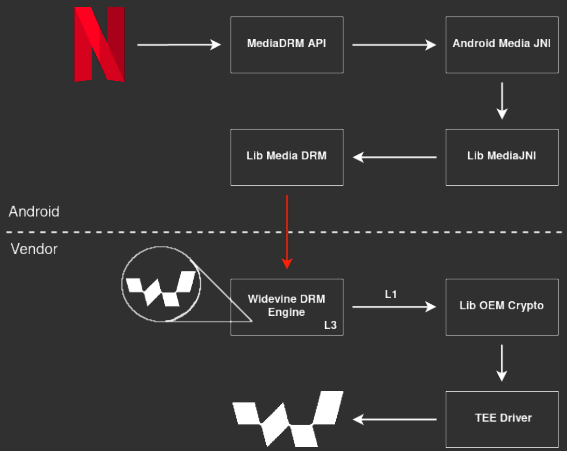


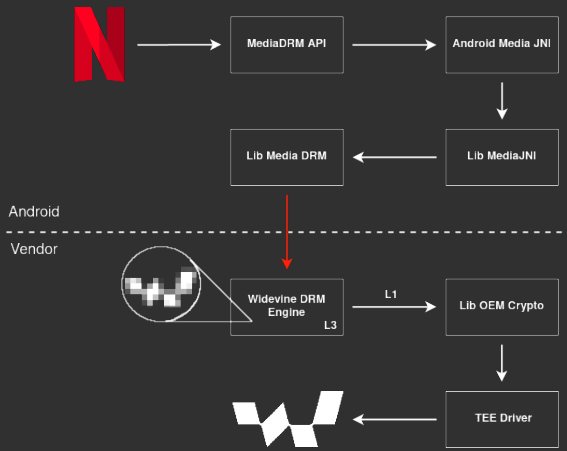
Android L3 RoT Recovery



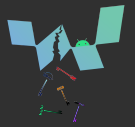

MediaDRM API
Android Media JNI
Lib Media DRM
Lib MediaJNI
Android
Vendor
Widevine DRM Engine
L3
L1
Lib OEM Crypto
TEE Driver



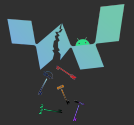

MediaDRM API
Android Media JNI
Lib Media DRM
Lib MediaJNI
Android
Vendor
Widevine DRM Engine
L3
L1
Lib OEM Crypto
TEE Driver


MediaDRM API
Android Media JNI
Lib Media DRM
Lib MediaJNI
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** in `munmap` calls.



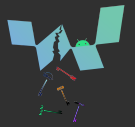
Reversing the obfuscation **can easily be avoided** thanks to an **insecure memory deallocation** in `munmap` calls.



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**

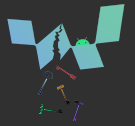
Table: Widevine Keybox



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**

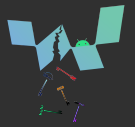
Table: Widevine Keybox



Widevine KeyBox: RoT structure

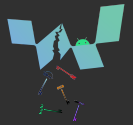
Field	Description	Size (bits)
Device ID	Internal Device ID	256
Device Key	128-bit RoT AES key	128
Provisioning Token	Used by provision requests	576
Magic Number	'kbox' (0x6b626f78)	32
CRC32	CRC32 validating the keybox integrity	32
Total		**1024**

Table: Widevine Keybox



Our Keybox

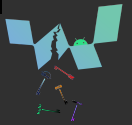
00000000	4f 63 6a 44 68 77 71 57	44 4b 61 6b 45 4a 70 7a	OcjDhwqW	DKakEJpz
00000010	5a 6a 6a 49 78 75 79 68	52 4b 43 6c 45 6c 70 00	ZjjIxuyh	RKClElp0
00000020				
00000030	00 00 00 02 00 00 11 5d	22 13 9f e5 9a 2d c4 a4	000•00•]	"•xxx-xx
00000040	c5 f9 10 e3 58 4f 76 b8	53 4d 9b f4 2e bd a4 25	xx•xOvx	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
```

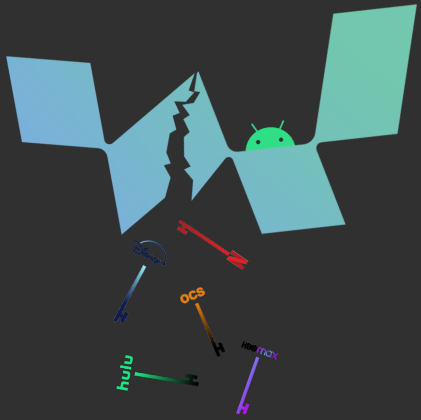


Can it be fix?

Yes!

Can it be fix?

Just kidding, it cannot.



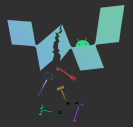
Takeaways

OTT Apps and Widevine:

- OTT apps do not fully protect their assets regarding Widevine guidelines.
- Large support of outdated devices.

Widevine DRM:

- Reverse engineering of the Widevine cryptographic key ladder.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.
- Disclosure to Google in June 2021 and discussion with multiple OTTs.
  - CVE-2021-0639.[3]
  - Android Security Bulletin August 2021.[4]



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

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

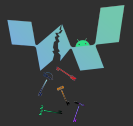
Takeaways

OTT Apps and Widevine:

- OTT apps do not fully protect their assets regarding Widevine guidelines.
- Large support of outdated devices.

Widevine DRM:

- Reverse engineering of the Widevine cryptographic key ladder.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.
- Disclosure to Google in June 2021 and discussion with multiple OTTs.
  - CVE-2021-0639.[3]
  - Android Security Bulletin August 2021.[4]



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

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

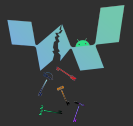
Takeaways

OTT Apps and Widevine:

- OTT apps do not fully protect their assets regarding Widevine guidelines.
- Large support of outdated devices.

Widevine DRM:

- Reverse engineering of the Widevine cryptographic key ladder.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.
- Disclosure to Google in June 2021 and discussion with multiple OTTs.
  - CVE-2021-0639.[3]
  - Android Security Bulletin August 2021.[4]



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

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

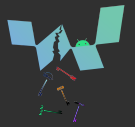
Takeaways

OTT Apps and Widevine:

- OTT apps do not fully protect their assets regarding Widevine guidelines.
- Large support of outdated devices.

Widevine DRM:

- Reverse engineering of the Widevine cryptographic key ladder.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.
- Disclosure to Google in June 2021 and discussion with multiple OTTs.
  - CVE-2021-0639.[3]
  - Android Security Bulletin August 2021.[4]



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

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

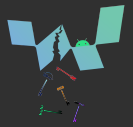
Takeaways

OTT Apps and Widevine:

- OTT apps do not fully protect their assets regarding Widevine guidelines.
- Large support of outdated devices.

Widevine DRM:

- Reverse engineering of the Widevine cryptographic key ladder.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.
- Disclosure to Google in June 2021 and discussion with multiple OTTs.
  - CVE-2021-0639.[3]
  - Android Security Bulletin August 2021.[4]



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

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

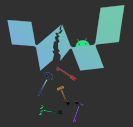
Takeaways

OTT Apps and Widevine:

- OTT apps do not fully protect their assets regarding Widevine guidelines.
- Large support of outdated devices.

Widevine DRM:

- Reverse engineering of the Widevine cryptographic key ladder.
- The obfuscated software-only scheme can be broken trivially due to simple mistakes.
  - with no fix possible for discontinued phones.
- Disclosure to Google in June 2021 and discussion with multiple OTTs.
  - CVE-2021-0639.[3]
  - Android Security Bulletin August 2021.[4]



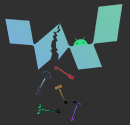
[3] https://www.cve.org/CVERecord?id=CVE-2021-0639

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

Thanks for your attention

@ gwendal.patat@irisa.fr
@avalonswanderer
Avalonswanderer

Paper Preprint[5]



[8] https://people.irisa.fr/Gwendal.Patat/assets/publications/wideleak.pdf