

Formal Security Analysis of Widevine through the W3C EME Standard

Stéphanie Delaune¹, JosephALLEmand¹, Gwendal Patat²,
Florian Roudot¹, and Mohamed Sabt¹

¹Univ Rennes, CNRS, IRISA, France

²Fraunhofer SIT | ATHENE, Germany

August 16th 2024



Université
de Rennes



UMR

IRISA



Fraunhofer
SIT



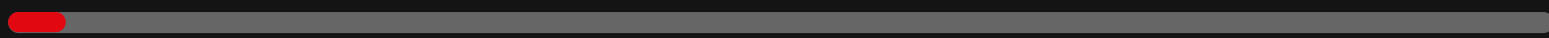
ATHENE
National Research Center
for Applied Cybersecurity

| Over-the-Top (OTT) Platforms

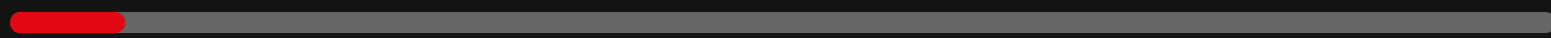
NETFLIX

prime video

Disney+



I OTT Usage



OTT Attacker Model



- Legitimate User
- Full Device Control
- *Want to redistribute for free*



| Digital Rights Management (DRM)

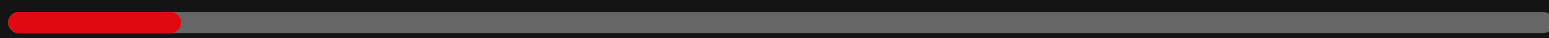


Microsoft PlayReady®



WIDEVINE

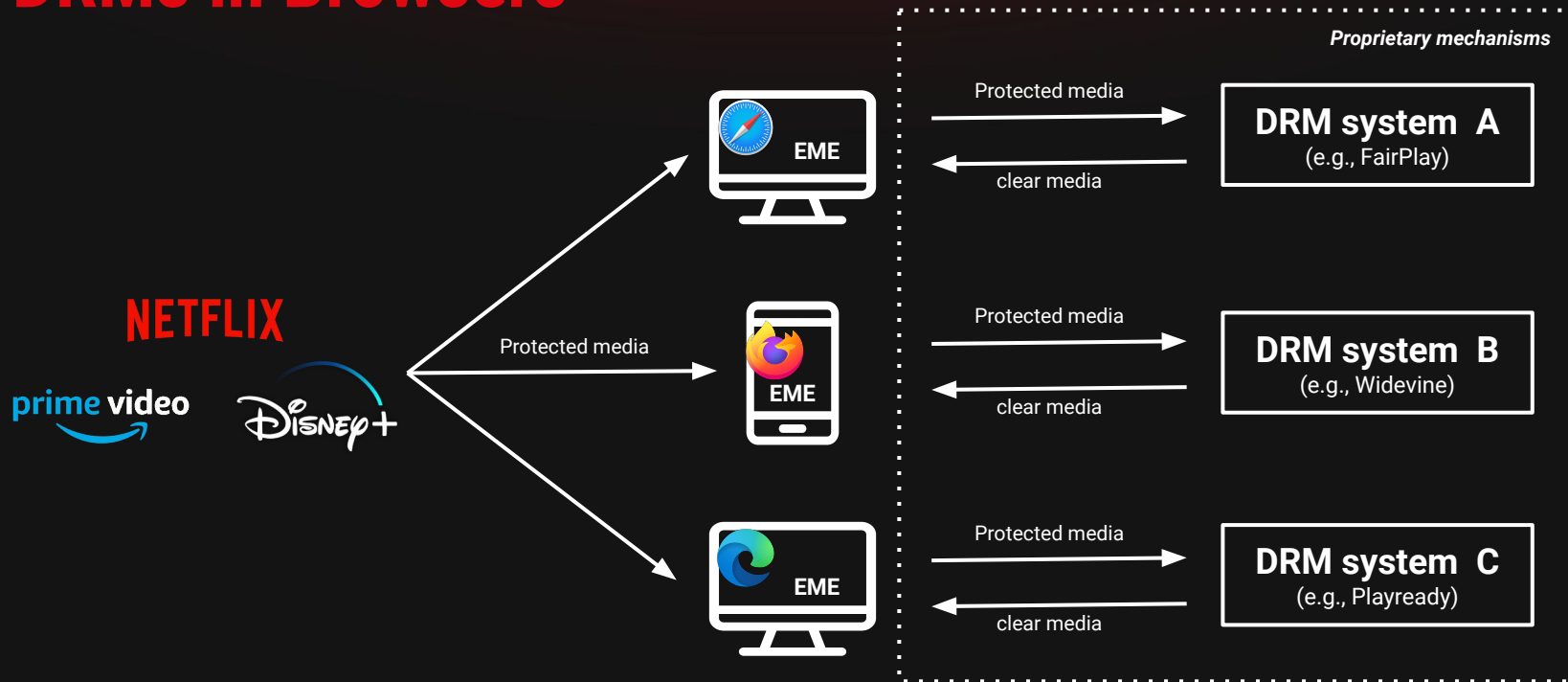
FairPlay



| DRM Principle



| DRMs in Browsers

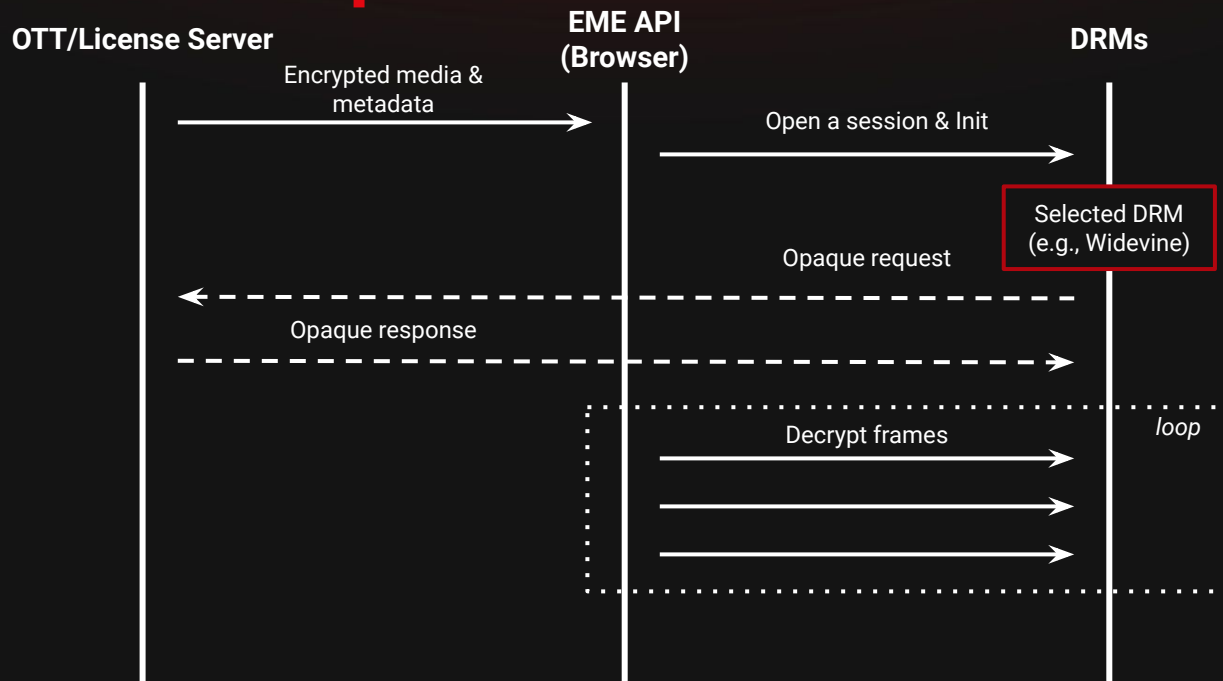


| HTML5 Encrypted Media Extension (EME)

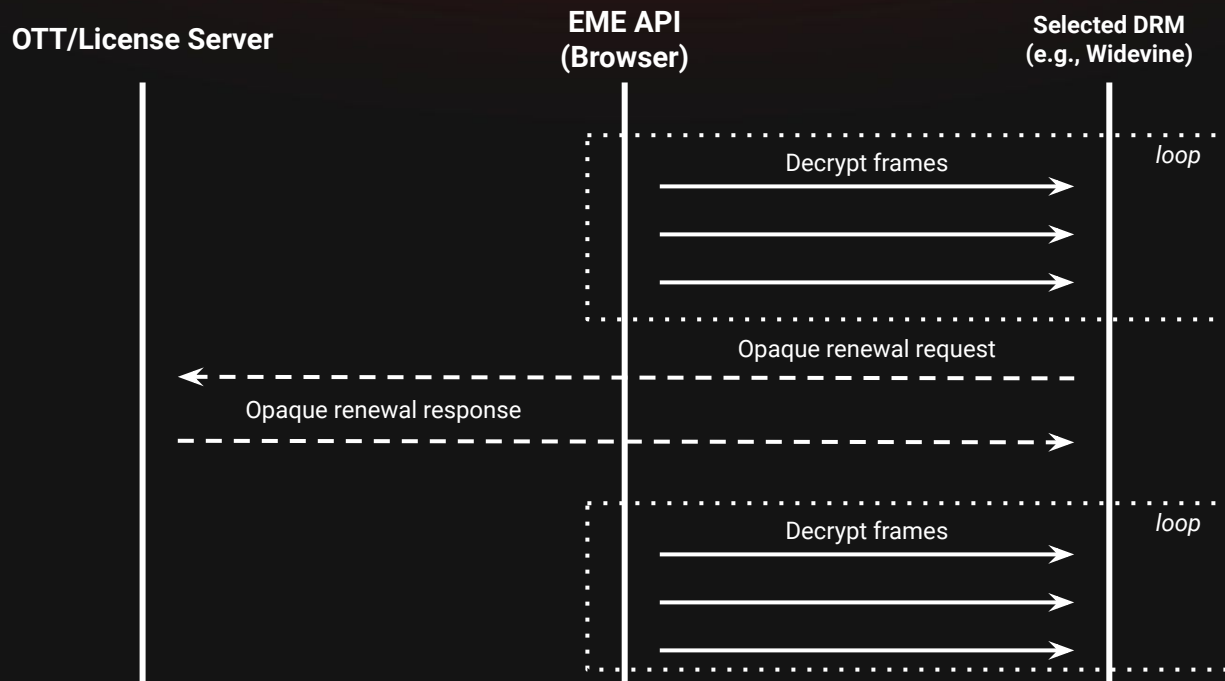
W3C[®]

- API Extension to HTML5.
- Standard for DRM systems since 2013.
- Implemented in all major browsers (both mobile and desktop).

EME License Acquisition



EME License Renewal

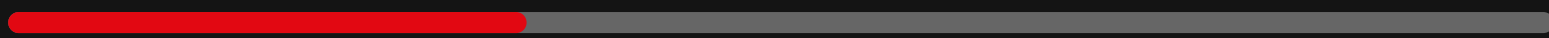


| Widevine



WIDEVINE

- Owned by Google since 2011.
- One of the most deployed DRM.
- Closed-source → Opaque.



What about the security of this opacity?

EME Security Concerns:

- Focused on users security and privacy as a web application. -> *Nice*.¹
- **But** nothing concerning protected media security.



1. Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME. Patat et al., PETS'22



I Our Contributions

Generic Security Goals for Media consumption:

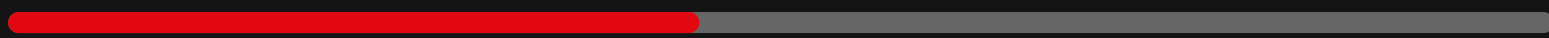
- Applicable for all media DRM systems based on the EME API.

Formal Security Analysis of these goals on the Widevine DRM:

- Definition of goals and rules based on our observations.
- Found a vulnerability within the Widevine EME instance.
- Proposed a fix to the EME standard.

I Our Generic Goals (1)

As an OTT, you want to **protect** your media, and
control its distribution, and consumption.



I Our Generic Goals (2)

General:

- **Confidentiality** of the decryption key, therefore the media itself.

Acquisition:

- **Integrity** and **authenticity** of initial licenses.
- **Freshness** of initial licenses.
- **Enforcing** expiration time of initial licenses.

Renewal:

- **Integrity** and **authenticity** of renewal licenses.
- **Freshness** of renewal licenses.
- **Enforcing** expiration time of renewal licenses.

| TAMARIN Prover



- Symbolic Protocol Verification tool.¹
- Suitable to model stateful protocols such as APIs based on ordered events.

Needs rules to be verified.

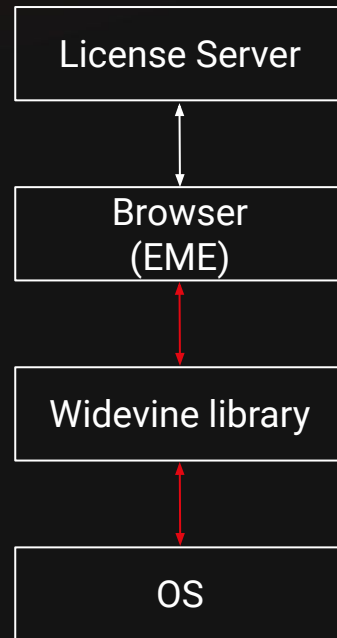
I Widevine RE Setup

Setup:

- Using Widevine Test License Server for Vendor Integration.
- Instrumented Widevine library with **custom EME hooks**.

Capabilities:

- **Observe** and **tamper** with every API calls from EME to the Widevine DRM.
- **Tamper with syscalls** made by the Widevine library.



Widevine Reverse Engineering <-> TAMARIN rules

```

08 01 12 CF 0B 0A 8E 0B 08 01 12 F2 09 0A B2 02 ...I...Z...ö...
08 02 12 11 61 A5 6C 92 C7 74 D0 C0 DF 45 B8 33 ...äwI'çtðABE.3
E4 39 1B BA 0A 18 98 E6 BD FC 05 22 8E 02 30 82 ä9.º.~æ%u."Z.0.
01 0A 02 82 01 01 00 D9 28 9C 12 75 94 FA B9 A0 ....Ü(æ.u'Ü'
73 7E 05 EC 2E 3D B2 08 B6 83 73 40 06 BA B9 11 s~.i.=+0fse.º'.
45 42 41 E4 15 FB 21 2B E6 C0 78 2E 79 EC E0 8D EBAA.Ü!+æAk.yiä.
9E 74 87 AF D2 E1 18 F4 94 30 59 B9 FD 68 9A 9E Zt+Öä.ö'OV'yhsZ
16 C5 A3 77 90 89 D5 56 7F 6A 93 B1 9C 3E 4F AE .ÄEW.%OV.j"±æ>O0
91 20 EB 86 7A 54 57 B4 42 E2 DE 25 F0 CC 1B BE ' etzTW'BâP%öi.%
0E 9E DF 0E 1C 5A 3F 23 51 AD 27 04 1C 60 4C 8A .ZB..Z7#Q-'...'LŠ
49 97 79 6F EE B1 8F D0 C0 F9 53 D2 EA 50 4A 68 I-yoi+DÄÜSÖâPJh
FD ED 7F ED C0 C3 58 74 FB 7F 68 FF 25 22 41 13 yi.iÄÄxÜ.hyz*A.
04 9B 76 DB E0 64 74 E2 3E BE D4 87 7E C0 1C 4B .vÜadtâ>%0+~A.K
07 38 18 94 3F 76 CB C9 6E 6B A8 82 D3 1D FA C0 .B."?vEËnk".Ö.ÜÄ
8E 62 BA 45 E6 42 2B F0 7C 8B 55 F8 C1 94 EC 13 Žb°EaB+ð|UoÄ'i.
11 01 C1 C6 0D E3 F7 35 1A 9D 4D 58 7B 77 6F B4 .ÄE.ä+5..MX{wo'
32 8E 01 9E 3A 8B 89 63 53 EA C8 45 47 9A 73 1A ZZ.Z:~kcSËËËGss.
CF BE 58 93 47 6E D2 43 21 D7 AF F1 11 B8 DD 78 IxX"GnÖC!xIn.Ÿx
CB 51 FA A6 87 0C E5 8A D3 F3 7D CF 63 68 91 51 IQü|t.äSöjIch'Q
A9 2B E8 B3 B3 98 BF 02 D3 01 00 01 28 99 9D 01 @+ä""Z.....(M'.
48 01 12 80 02 6B 3B 6C 6C 54 2D ED 10 DC 0D 5A H..ë.kjllt-i.U.Z
3F 84 BB A2 49 87 B7 2A BE 45 F5 16 42 2E 9C 30 ?..«CI+~*MEö.B.æ0
EE 20 CE D4 BC 84 67 4B E7 48 EC BE 51 ED FA 46 i IÖ%.gKçHiWQiUF
77 F3 AC 19 7F 28 49 60 8F 9F 67 AD 5C B2 D9 DC wö~..(I'.Yg-^ÜÜ
AF 38 A9 34 A4 D7 78 D9 2F 5F 4A 22 35 48 9A 16 B04=xxÜ/_5HŠ.
0D B7 06 36 DF D6 0C 77 AA 05 56 F0 14 9D F3 36 ..6BÖ.w%.Vä..ö6
9A 7F BD E1 F3 0A AF 7A 6E 1C 49 82 7B 56 EC 41 Š.%áo.~zn.I,{ViA
F4 32 1A F5 93 69 72 96 B0 52 30 0A 04 1A 23 0E ö2.ö"ir-~RO...#.
7F 47 C3 B5 7E BC 07 3E 62 A3 C2 7B A6 30 F6 C8 .GÄu-%.>bEÄ{!0oE
BF 81 7B 7B BB 71 CA 2F 1F 71 F7 D0 0D 59 23 87 ž.{x+qE/.q+D.Y#š
3D BC CA B0 DC 0C 0C 18 6D 04 F3 57 15 89 B7 52 =KË°Ü...m.öW.%R
FA DE D3 F8 2C 01 04 3D 96 49 B6 8D 01 75 AA C2 ÜPöo...=-I¶..U°Ä
6E 6E 57 E1 C2 76 76 28 7C A9 23 ED B1 A8 B5 A4 æÜsâny.Ööü.tun

```

rule **CDMGenerateRequest**:

```

let request = <~rID, ~keyID, %t,
                enc(clientID, ~kPrivacy),
                aenc(~kPrivacy, pk(~kOTT)), ~n>
signReq = sign(request, kDevice)

```

in

```

[ In(%t), In(~keyID), Fr(~rID), Fr(~n), Fr(~kPrivacy),
  !OTTKey(~kOTT), !CDMSession(~sID, kDevice, clientID)]

```

```

- [ GTime(%t), LCDMGenR(~requestID, ~sID, %t) ] ->

```

```

[ Out(<request, signReq>), CDMNonce(~n, ~sID),
  !CDMState(~rID, ~sID, ~kOTT, request, %t),

```

```

  CDMKeys(~rID, ~sID, 0),

```

```

  CDMContentKey(~rID, ~sID, 0, %1) ]

```

I Modeling Challenges

Widevine:

- Lot of cryptographic keys involved.
- Nonces and timestamps use for freshness and license expiration.

TAMARIN:

- No built-in support for modeling time; only event ordering.
- Timestamps are crucial for certain security goals, requiring a novel explicit time model in TAMARIN -> **global clock** within event.

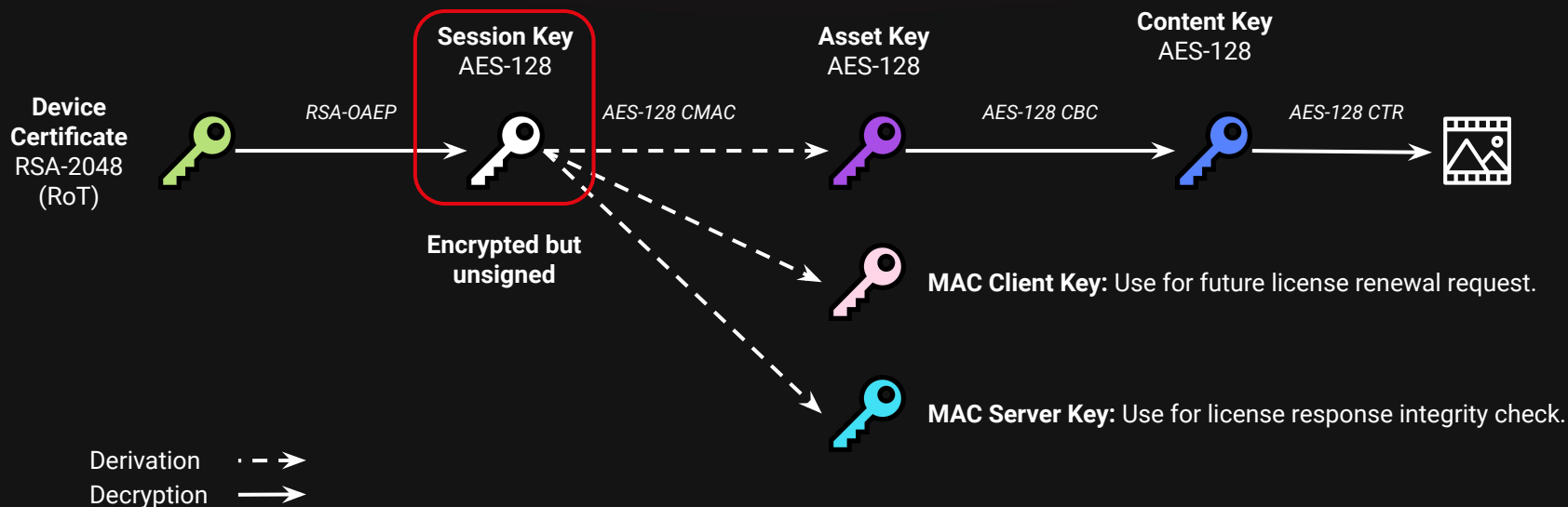
I Goal Verification

Failed Goals:

- Integrity and authenticity of renewal licenses.
- Enforcing expiration time of renewal licenses.

Goal 1	✓
Goal 2	✓
Goal 3	✓
Goal 4	✓
Goal 5	✗
Goal 6	✓
Goal 7	✗

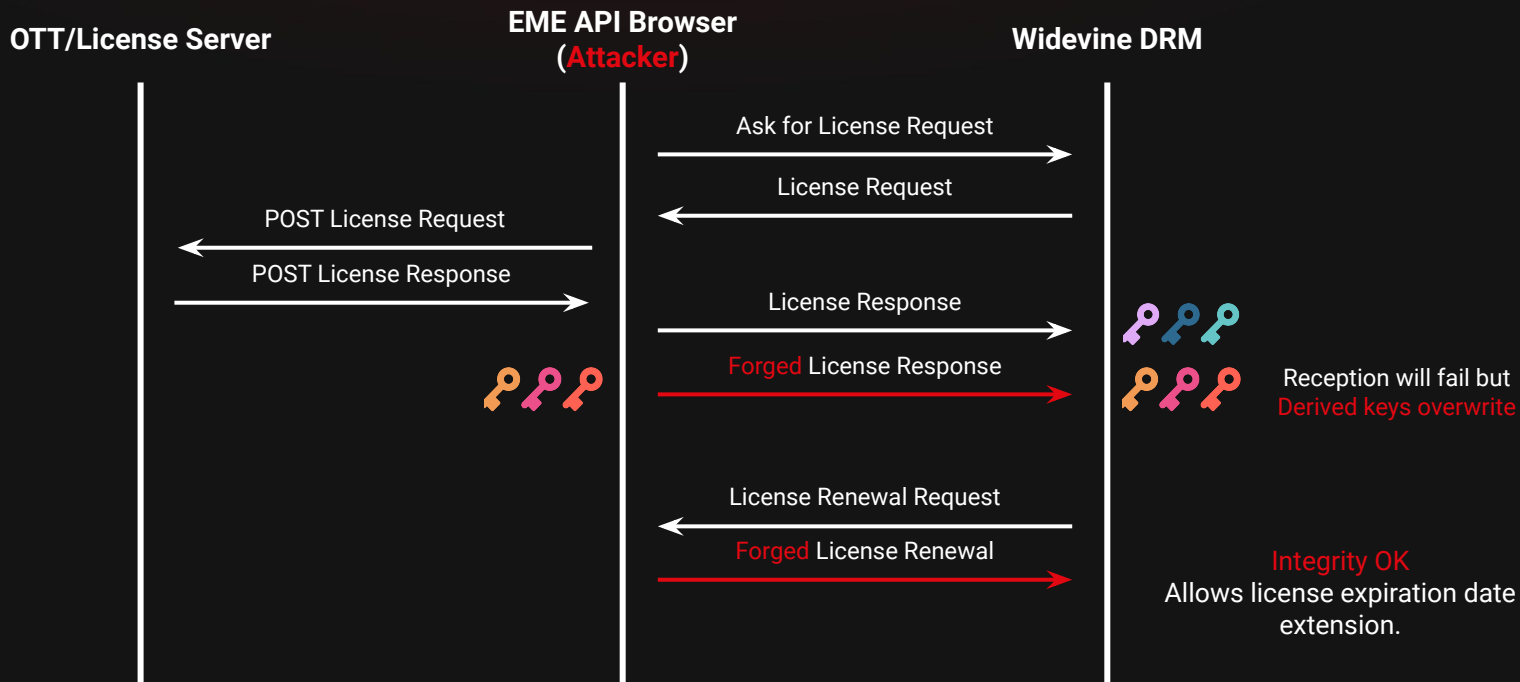
Widevine Key Ladder



A problem due to Session Key **processed
before** license authenticity check



Widevine EME Key Derivation Attack



I Protocol Fixe

Modification 1: EME Specification

- Bind opened CDM session to a read-only OTT certificate with the *setServerCertificate* API call (originally define for privacy purposes).

Modification 2: Full License Signature

- Require the Session Key to *be signed along side the request* by the server certificate's private key.

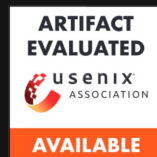
| Takeaways

Security Impacts:

- Widevine EME protocol flaw allowing for infinite media consumption.
- Definition of DRM generic goals for media security.

PoC model:

- Our TAMARIN Model can be found on our github.¹



Responsible Disclosure:

- Widevine contacted on March 2024.
- EME contacted on February 2024, and discussed in the media WG meeting.²
 - will follow on the suggested patch and modify the standard accordingly.



1. https://github.com/Avalonswanderer/eme_widevine_formal_verification
2. <https://www.w3.org/2024/02/13-mediawg-minutes.html#t04>

Thank you

Do you have any questions?

✉ gwendal.patat@sit.fraunhofer.de

🌐 avalonswanderer.github.io

✂ @avalonswanderer

🐙 Avalonswanderer

