Formal Security Analysis of Widevine through the W3C EME Standard

Stéphanie Delaune[1], Joseph Lallemand[1], **Gwendal Patat**[2], Florian Roudot[1], and Mohamed Sabt[1]

[1]Univ Rennes, CNRS, IRISA, France
[2]Fraunhofer SIT | ATHENE, Germany

August 16th 2024

Over-the-Top (OTT) Platforms

NETFLIX

prime video

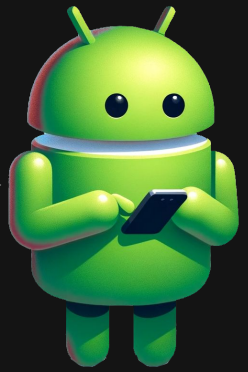
Disney+

OTT Usage

NETFLIX

prime video

Disney+



OTT Attacker Model

NETFLIX

prime video

Disney+

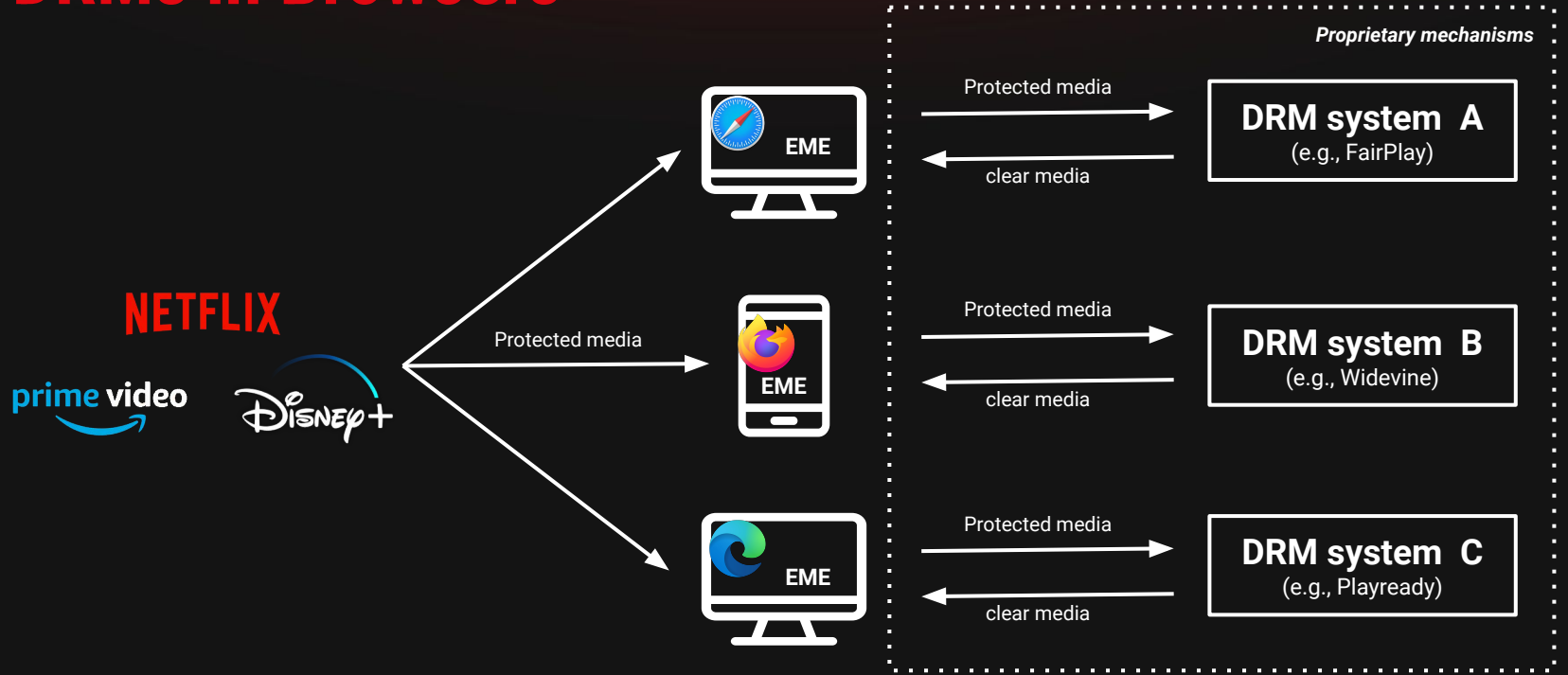
- Legitimate User
- Full Device Control
- *Want to redistribute for free*

Digital Rights Management (DRM)

FairPlay

DRM Principle

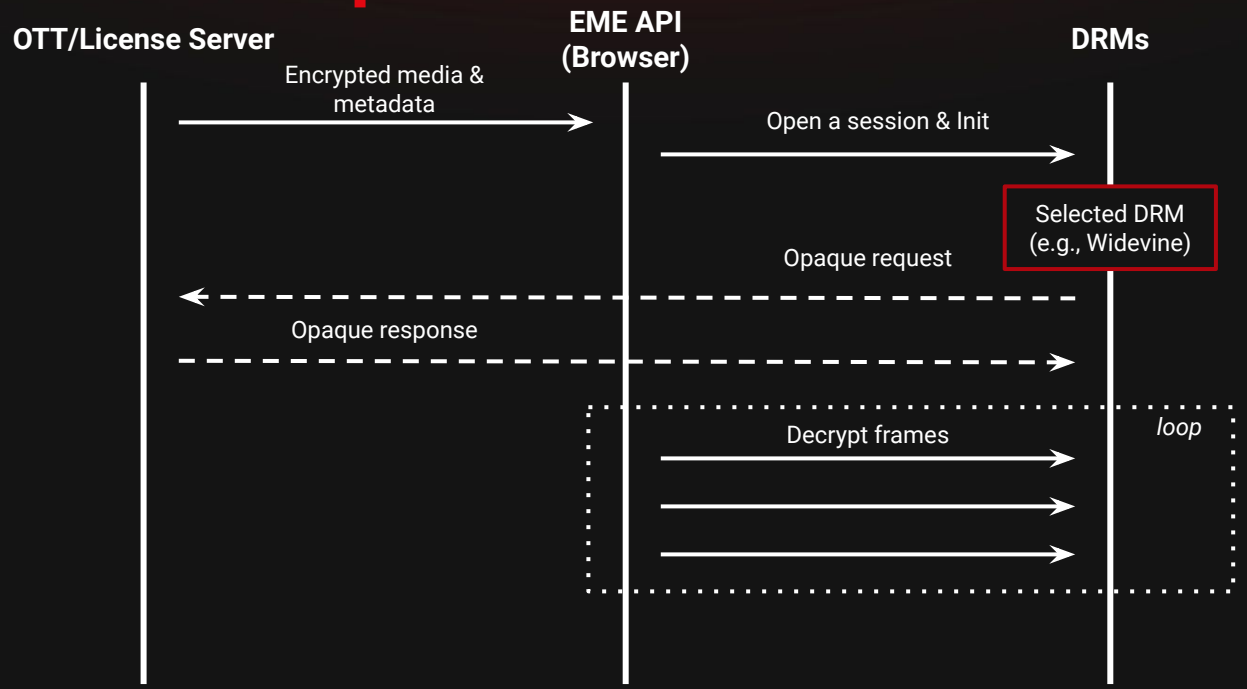
DRMs in Browsers



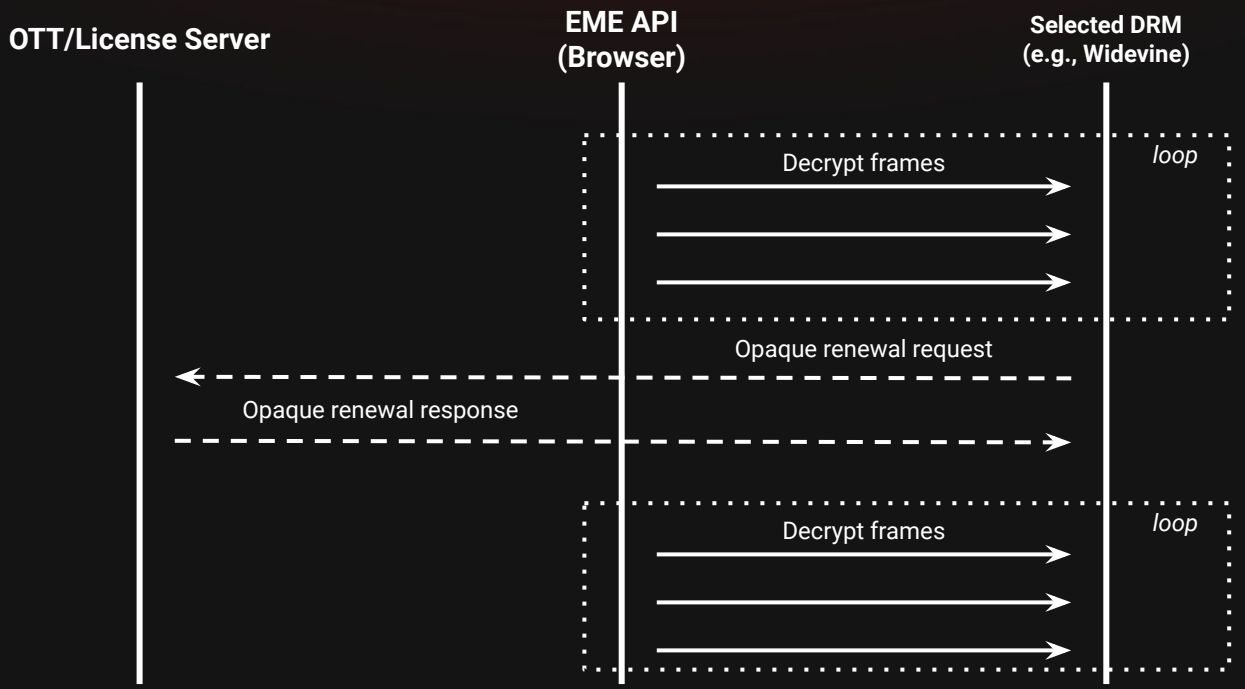
HTML5 Encrypted Media Extension (EME)

- 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

- 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'23*

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 fixed to the EME standard.

Our Generic Goals (1)

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

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.

1. *The TAMARIN Prover for the Symbolic Analysis of Security Protocols. Meier et al., CAV'13.*

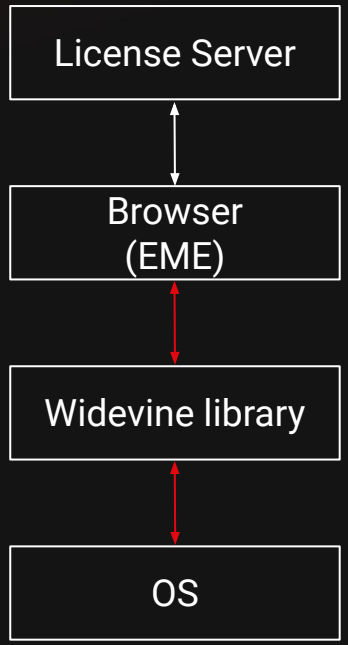
Widevine RE Setup

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

```
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, ∅),
    CDMContentKey(~rID, ~sID, ∅, %1) ]
```

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.

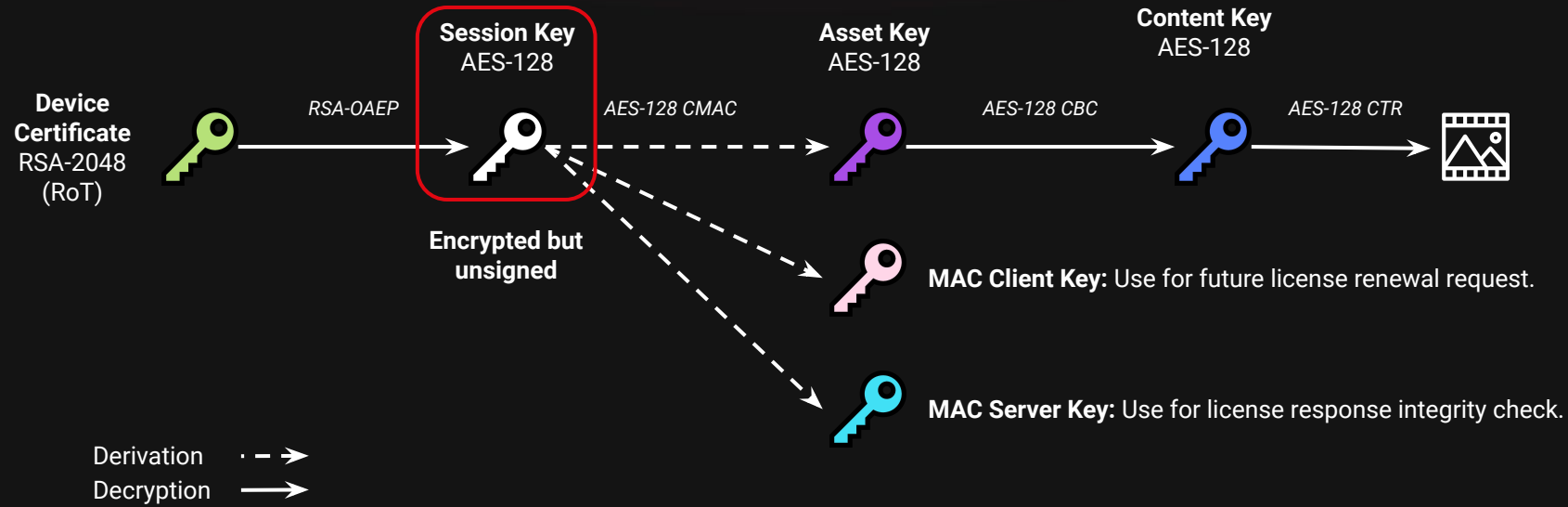
Goal Verification

Failed Goals:

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

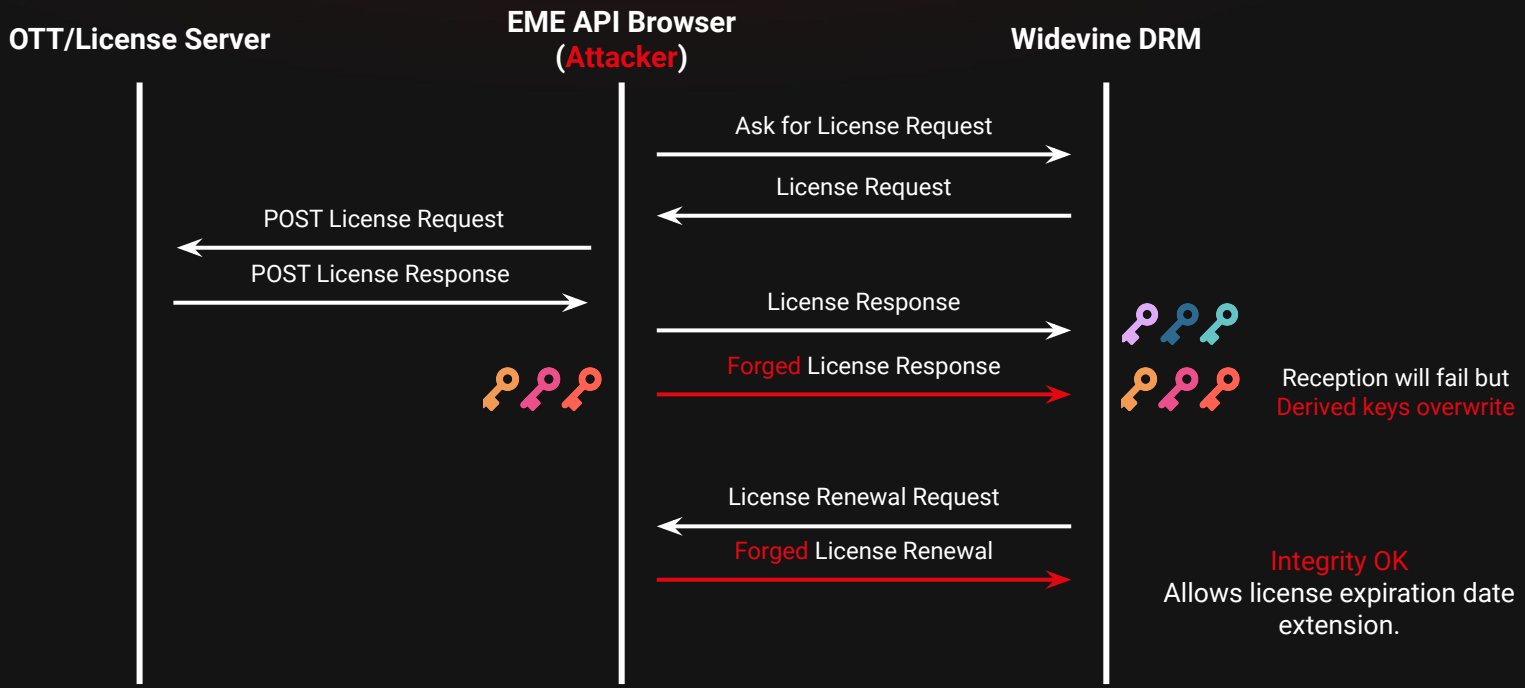
Goal 1	✓
Goal 2	✓
Goal 3	✓
Goal 4	✓
Goal 5	✗
Goal 6	✓
Goal 7	✗

Widevine Key Ladder



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

Widevine EME Key Derivation Attack



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