

# Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME

Gwendal Patat, Mohamed Sabt, Pierre-Alain Fouque

Univ Rennes, CNRS, IRISA

July 13, 2023



# Over-the-Top (OTT) Platforms



Figure: Example of Famous OTTs<sup>1</sup>

<sup>1</sup>All logos are trademarks of their respective companies.



# Digital Right Management (DRM) Systems



WIDEVINE

FairPlay

Figure: Major DRM systems<sup>2</sup>

<sup>2</sup>All logos are trademarks of their respective companies.

<sup>2</sup>Google Widevine. *Widevine*. <https://widevine.com/>. 2023.

<sup>2</sup>Apple. *Apple FairPlay*. <https://developer.apple.com/streaming/fps/>. 2023.

<sup>2</sup>Microsoft. *Microsoft PlayReady*. <https://www.microsoft.com/playready/>. 2023.



# Generic DRM Usage



Figure: OTTs and DRMs.



# Generic DRM Usage



Figure: OTTs and DRMs.



# Generic DRM Usage

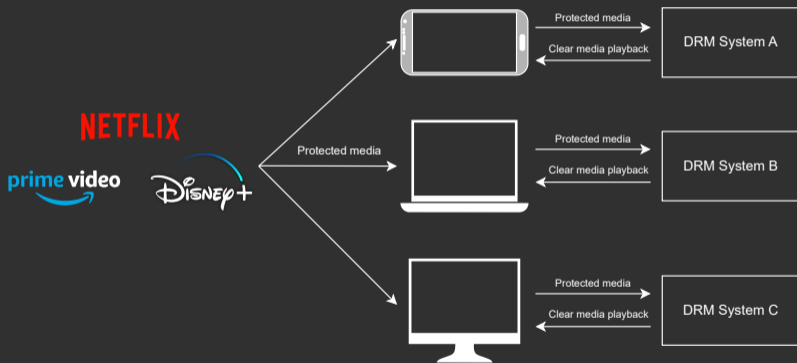


Figure: OTTs and DRMs.



# Generic DRM Usage

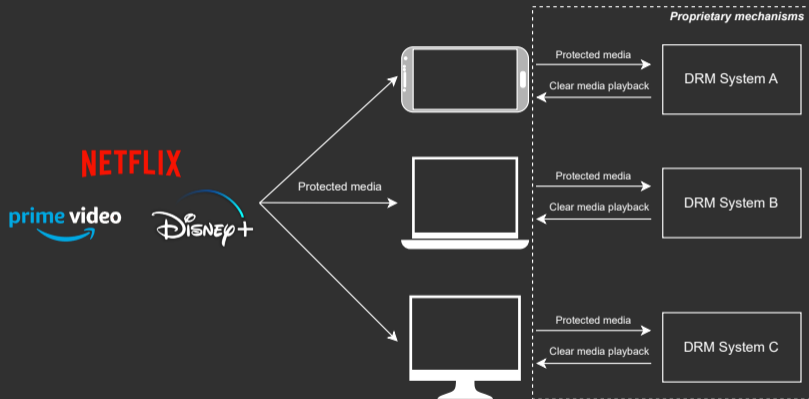


Figure: OTTs and DRMs.



# Generic DRM Usage

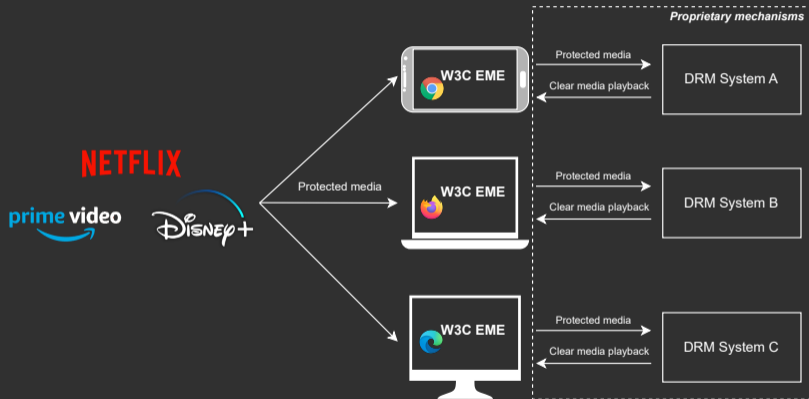


Figure: OTTs and DRMs.





# Encrypted Media Extension (EME)

## EME API

- Defined by the W3C to standardized DRM APIs<sup>3</sup>.
- Define security and privacy guidelines for DRMs.
- Supported in all major web browsers<sup>4</sup>.



<sup>3</sup>David Dorwin et al. *Encrypted Media Extensions*. <https://www.w3.org/TR/encrypted-media/>.

<sup>4</sup>Can I Use. *Encrypted Media Extensions*. <https://caniuse.com/eme>. 2023.



# Encrypted Media Extension (EME)

## EME API

- Defined by the W3C to standardized DRM APIs<sup>3</sup>.
- Define security and privacy guidelines for DRMs.
- Supported in all major web browsers<sup>4</sup>.



<sup>3</sup>Dorwin et al., *Encrypted Media Extensions*.

<sup>4</sup>Can I Use, *Encrypted Media Extensions*.



# Encrypted Media Extension (EME)

## EME API

- Defined by the W3C to standardized DRM APIs<sup>3</sup>.
- Define security and privacy guidelines for DRMs.
- Supported in all major web browsers<sup>4</sup>.



<sup>3</sup>Dorwin et al., *Encrypted Media Extensions*.

<sup>4</sup>Can I Use, *Encrypted Media Extensions*.



# EME Actors

## Actors:

- **User-Agent:** Web Browser EME compatible (e.g., Chrome, Firefox).
- **CDM:** Content Decryption Module, client-side implementation of the DRM (e.g., Widevine, PlayReady).
- **License Server:** Providing content decryption keys (aka licenses), compatible with the DRM system.



# EME Actors

## Actors:

- **User-Agent:** Web Browser EME compatible (e.g., Chrome, Firefox).
- **CDM:** Content Decryption Module, client-side implementation of the DRM (e.g., Widevine, PlayReady).
- **License Server:** Providing content decryption keys (aka licenses), compatible with the DRM system.



# EME Actors

## Actors:

- **User-Agent:** Web Browser EME compatible (e.g., Chrome, Firefox).
- **CDM:** Content Decryption Module, client-side implementation of the DRM (e.g., Widevine, PlayReady).
- **License Server:** Providing content decryption keys (aka licenses), compatible with the DRM system.



# EME Actors

## Actors:

- **User-Agent:** Web Browser EME compatible (e.g., Chrome, Firefox).
- **CDM:** Content Decryption Module, client-side implementation of the DRM (e.g., Widevine, PlayReady).
- **License Server:** Providing content decryption keys (aka licenses), compatible with the DRM system.



# EME Workflow

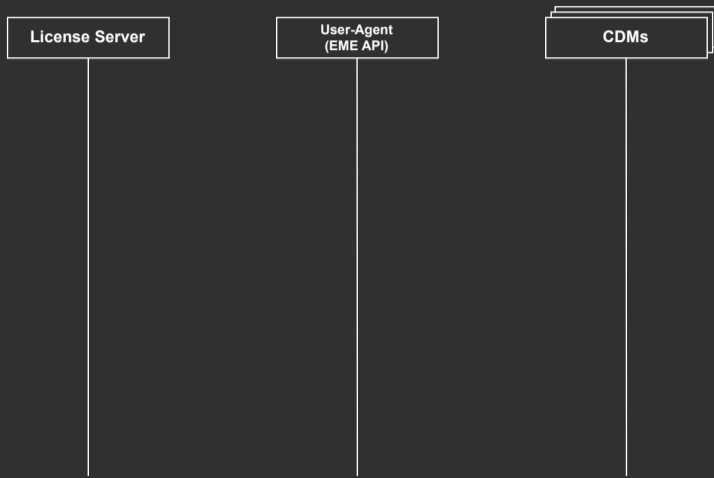


Figure: EME Workflow License Acquisition.





# EME Workflow

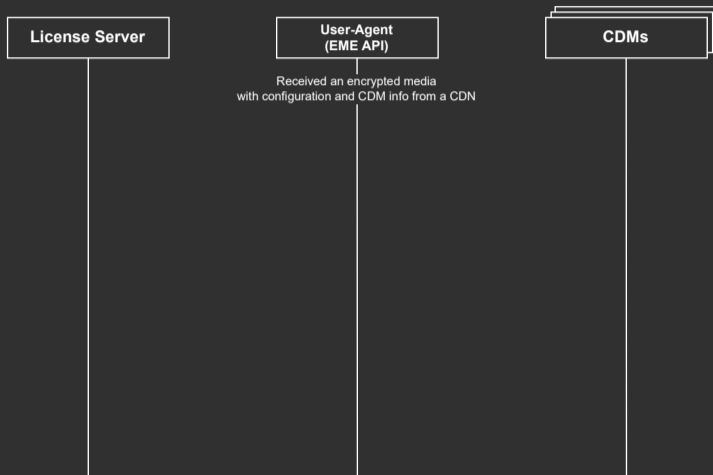


Figure: EME Workflow License Acquisition.



# EME Workflow



Figure: EME Workflow License Acquisition.



# EME Workflow



Figure: EME Workflow License Acquisition.



# EME Workflow

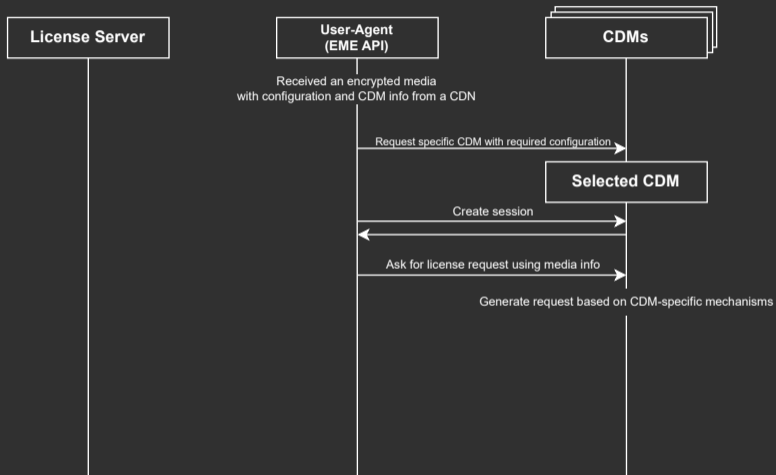


Figure: EME Workflow License Acquisition.



# EME Workflow

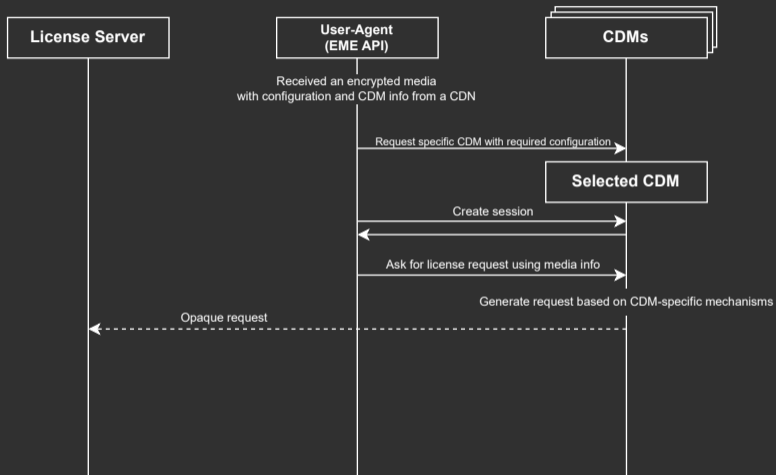


Figure: EME Workflow License Acquisition.



# EME Workflow

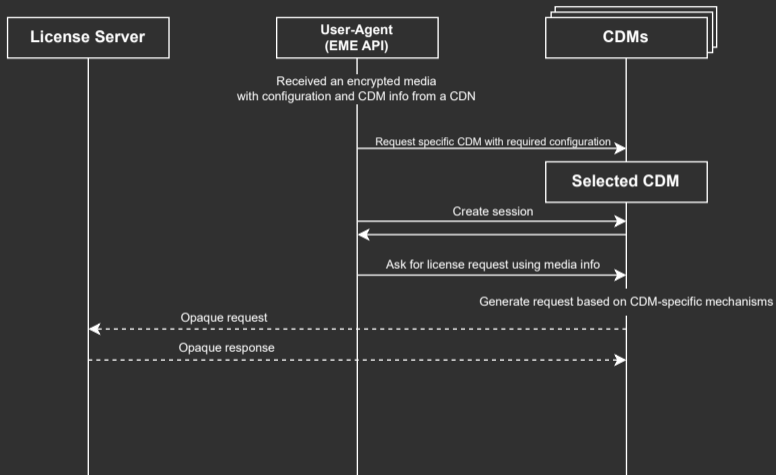


Figure: EME Workflow License Acquisition.



# EME Workflow

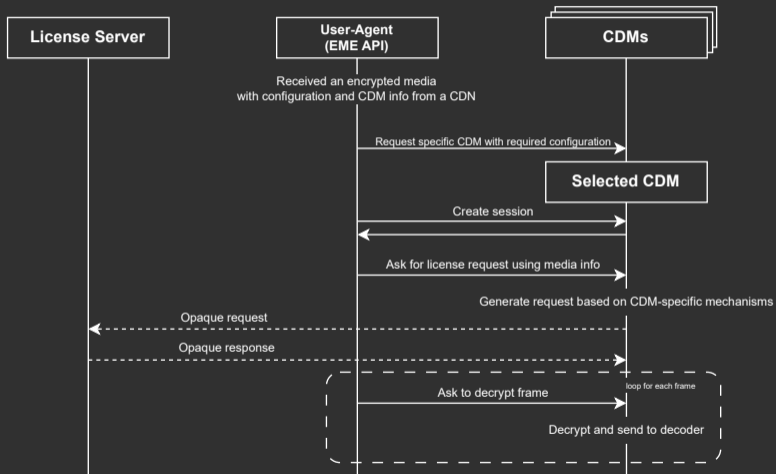


Figure: EME Workflow License Acquisition.



# Additional Workflow

In addition to license acquisition, EME defines also license renewal:

- Purpose : Extend decryption keys lifetime.
- Another Opaque Request/Response exchange with the license server.





# Additional Workflow

In addition to license acquisition, EME defines also license renewal:

- Purpose : Extend decryption keys lifetime.
- Another Opaque Request/Response exchange with the license server.



# Additional Workflow

In addition to license acquisition, EME defines also license renewal:

- Purpose : Extend decryption keys lifetime.
- Another Opaque Request/Response exchange with the license server.



# EME Privacy Concerns

**EME raised privacy concerns on opaque systems.**

## Stateless Tracking

- Distinctive Identifier.
- Distinctive Permanent Identifier (e.g., Hardware-related, and/or not trivially removable).

They should not appear in clear.



# EME Privacy Concerns

**EME raised privacy concerns on opaque systems.**

## Stateless Tracking

- Distinctive Identifier.
- Distinctive Permanent Identifier (e.g., Hardware-related, and/or not trivially removable).

They should not appear in clear.



# EME Privacy Concerns

**EME raised privacy concerns on opaque systems.**

## Stateless Tracking

- Distinctive Identifier.
- Distinctive Permanent Identifier (e.g., Hardware-related, and/or not trivially removable).

They should not appear in clear.



# Widevine



## General

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



# Widevine



## General

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



# Widevine



## General

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





# Widevine



## General

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



# Motivation & Contributions

Does DRM opaque systems bring privacy issues within browsers?

## Contributions

- Reverse opaque messages of EME when defined by Widevine.
- Analyze Widevine-based EME browser implementations regarding EME privacy guidelines.
- Explore the amount of privacy leakage resulting from non-compliance.



# Motivation & Contributions

Does DRM opaque systems bring privacy issues within browsers?

## Contributions

- Reverse opaque messages of EME when defined by Widevine.
- Analyze Widevine-based EME browser implementations regarding EME privacy guidelines.
- Explore the amount of privacy leakage resulting from non-compliance.



# Motivation & Contributions

Does DRM opaque systems bring privacy issues within browsers?

## Contributions

- Reverse opaque messages of EME when defined by Widevine.
- Analyze Widevine-based EME browser implementations regarding EME privacy guidelines.
- Explore the amount of privacy leakage resulting from non-compliance.



# Motivation & Contributions

Does DRM opaque systems bring privacy issues within browsers?

## Contributions

- Reverse opaque messages of EME when defined by Widevine.
- Analyze Widevine-based EME browser implementations regarding EME privacy guidelines.
- Explore the amount of privacy leakage resulting from non-compliance.



# EME & Widevine



# EME Widevine Messages

<i>Widevine Protocol</i>	<i>EME API</i>	<i>Message Content</i>
License Request	generateRequest	Request ID Content Key ID(s) Client ID
License Response	update	Request ID Content Key(s) TTLs License Policy
Renewal Request	MediaKeyMessageEvent	Request ID Client ID
Renewal Response	update	Request ID Updated TTLs Updated License Policy

**Table:** Content of Widevine Messages for License Acquisition and Renewal.



# EME Widevine Messages

<i>Widevine Protocol</i>	<i>EME API</i>	<i>Message Content</i>
License Request	generateRequest	Request ID Content Key ID(s) Client ID
License Response	update	Request ID Content Key(s) TTLs License Policy
Renewal Request	MediaKeyMessageEvent	Request ID Client ID
Renewal Response	update	Request ID Updated TTLs Updated License Policy

**Table:** Content of Widevine Messages for License Acquisition and Renewal.





# Widevine Client ID

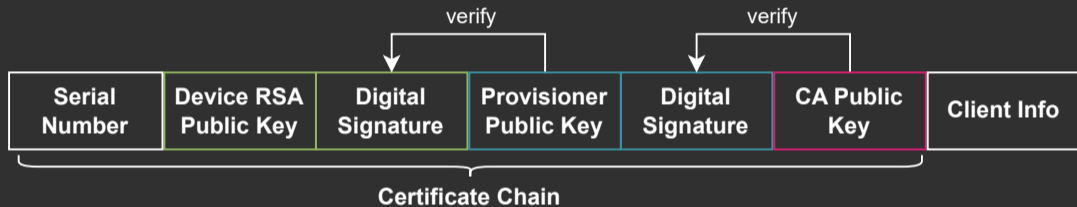


Figure: Client ID Fields.

Used by the CDM for key provisioning and device revocation.



# Widevine Client ID

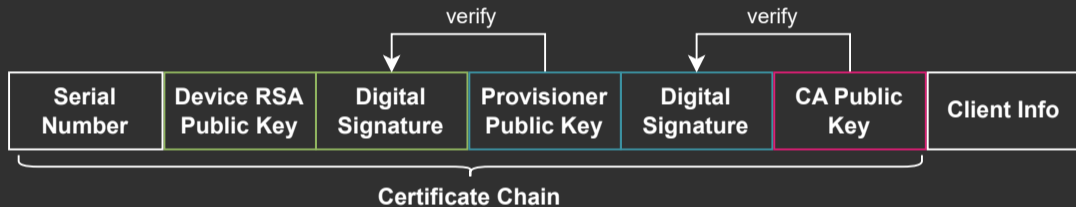


Figure: Client ID Fields.

Used by the CDM for key provisioning and device revocation.



# Widevine Client Info

Structure with multiple attributes:

- **For Desktop:** OS Name, CPU Architecture, Widevine version.
- **For Android Mobile:** CPU, Device Build info, Widevine build and version, etc...

Sounds distinctive...



# Widevine Client Info

Structure with multiple attributes:

- **For Desktop:** OS Name, CPU Architecture, Widevine version.
- **For Android Mobile:** CPU, Device Build info, Widevine build and version, etc...

Sounds distinctive...



# Privacy Protection: Privacy Mode and VMP

## Privacy Mode

- Encrypt the embedded Client ID.
- **Need to be enable by the browser** or forced by VMP.

## Verified Media Path (VMP)

- Integrity checks of Widevine binaries and decoding chain.
- Available on Windows and macOS.



# Privacy Protection: Privacy Mode and VMP

## Privacy Mode

- Encrypt the embedded Client ID.
- **Need to be enable by the browser** or forced by VMP.

## Verified Media Path (VMP)

- Integrity checks of Widevine binaries and decoding chain.
- Available on Windows and macOS.



# User-Agent Implementations



# Research Questions

Is the Privacy Mode used by web browsers?

And does it protect *all occurrences* of the Client ID in the Widevine workflow?





# Research Questions

Is the Privacy Mode used by web browsers?

And does it protect **all occurrences** of the Client ID in the Widevine workflow?



# Browser Selection

Two distinct groups based on popularity<sup>5</sup>:  
*Chromium-based* and *Firefox-based* browsers.

## ■ Chromium-based:

- Chrome
- Edge
- Opera
- Samsung Internet Browser
- Brave

## ■ Firefox-based:


- Firefox
- Firefox Focus
- Ghostery

Note: We excluded iOS and Safari on macOS, due to Apple using its own CDM FairPlay.

---

<sup>5</sup>Stat Counter. *Desktop Browser Market Share Worldwide.*

<https://gs.statcounter.com/browser-market-share/desktop/worldwide/2022>. 2022; Stat Counter. *Mobile Tablet Android Version Market Share Worldwide.*

<https://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide.2022>. 

# Browser Selection

Two distinct groups based on popularity<sup>5</sup>:  
*Chromium-based* and *Firefox-based* browsers.

## ■ Chromium-based:

- Chrome
- Edge
- Opera
- Samsung Internet Browser
- Brave

## ■ Firefox-based:


- Firefox
- Firefox Focus
- Ghostery

Note: We excluded iOS and Safari on macOS, due to Apple using its own CDM FairPlay.

---

<sup>5</sup>Stat Counter. *Desktop Browser Market Share Worldwide.*

<https://gs.statcounter.com/browser-market-share/desktop/worldwide/2022>. 2022; Stat Counter. *Mobile Tablet Android Version Market Share Worldwide.*

<https://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide.2022>. 

# Browser Selection

Two distinct groups based on popularity<sup>5</sup>:  
*Chromium-based* and *Firefox-based* browsers.

## ■ Chromium-based:

- Chrome
- Edge
- Opera
- Samsung Internet Browser
- Brave

## ■ Firefox-based:

- Firefox
- Firefox Focus
- Ghostery


Note: We excluded iOS and Safari on macOS, due to Apple using its own CDM FairPlay.

---

<sup>5</sup>Stat Counter. *Desktop Browser Market Share Worldwide.*

<https://gs.statcounter.com/browser-market-share/desktop/worldwide/2022>. 2022; Stat Counter.

*Mobile Tablet Android Version Market Share Worldwide.*

<https://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide.2022>. 

# Browser Selection

Two distinct groups based on popularity<sup>5</sup>:  
*Chromium-based* and *Firefox-based* browsers.

## ■ Chromium-based:

- Chrome
- Edge
- Opera
- Samsung Internet Browser
- Brave

## ■ Firefox-based:

- Firefox
- Firefox Focus
- Ghostery


Note: We excluded iOS and Safari on macOS, due to Apple using its own CDM FairPlay.

---

<sup>5</sup>Stat Counter. *Desktop Browser Market Share Worldwide*.

<https://gs.statcounter.com/browser-market-share/desktop/worldwide/2022>. 2022; Stat Counter.

*Mobile Tablet Android Version Market Share Worldwide*.

<https://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide.2022>. 

# Implementation Results

Browsers	Acquisition		Renewal	
	VMP	non-VMP	VMP	non-VMP
<b>Desktop</b>				
<b>Chromium Family</b>				
Chrome	●	○	○	○
Edge	●	○	○	○
Opera	●	○	○	○
Brave	●	○	○	○
<b>Firefox Family</b>				
Firefox	●	○	○	○

● EME compliant.

○ Do not respect EME privacy recommendations.

**Table:** Results for Implementation Questions per Browsers.

Browsers	Acquisition	Renewal
<b>Android Mobile</b>		
<b>Chromium Family</b>		
Chrome	●	●
Samsung	●	●
Edge	●	●
Opera	●	●
Brave	N/A	N/A
<b>Firefox Family</b>		
Firefox	○	○
Firefox Focus	○	○
Ghostery	○	○



# Implementation Results

Browsers	Acquisition		Renewal	
	VMP	non-VMP	VMP	non-VMP
<b>Desktop</b>				
<b>Chromium Family</b>				
Chrome	●	○	○	○
Edge	●	○	○	○
Opera	●	○	○	○
Brave	●	○	○	○
<b>Firefox Family</b>				
Firefox	●	○	○	○

● EME compliant.

○ Do not respect EME privacy recommendations.

**Table:** Results for Implementation Questions per Browsers.

Browsers	Acquisition	Renewal
<b>Android Mobile</b>		
<b>Chromium Family</b>		
Chrome	●	●
Samsung	●	●
Edge	●	●
Opera	●	●
Brave	N/A	N/A
<b>Firefox Family</b>		
Firefox	○	○
Firefox Focus	○	○
Ghostery	○	○



# Result Takeaways

On Desktop:

- Client IDs are **always in clear** in Renewal Request. Browsers only rely on VMP, therefore the opaque CDM, to enforce Privacy Mode.

On Android:

- Client IDs are **always in clear in the Firefox family**.





# Result Takeaways

On Desktop:

- Client IDs are **always in clear** in Renewal Request. Browsers only rely on VMP, therefore the opaque CDM, to enforce Privacy Mode.

On Android:

- Client IDs are **always in clear in the Firefox family**.



# Widevine EME Privacy Issues

“What is the privacy impact of this gap?”



# Widevine EME Privacy Issues

“What is the privacy impact of this gap?”



# Statement

Any web server sending you a JS file can make you execute EME and generate Widevine requests to **gather your Client ID**.

A Client ID that is in clear within Android Firefox family and on desktop.



# Statement

Any web server sending you a JS file can make you execute EME and generate Widevine requests to **gather your Client ID**.

A Client ID that is in clear within Android Firefox family and on desktop.



# Client ID Certificate

What about the Client ID certificate chain?



# Client ID Certificate Fingerprints (1)

We used our own curious website sending an EME script to gather Client ID in a fully automated way on:

## Desktop



159,923 Client IDs from macOS Big Sur, Windows 10/11, and Linux VMs.

## Android Mobile



317 physical devices, 18,101 emulated ones.

What about fingerprint properties?



# Client ID Certificate Fingerprints (1)

We used our own curious website sending an EME script to gather Client ID in a fully automated way on:

## Desktop



159,923 Client IDs from macOS Big Sur, Windows 10/11, and Linux VMs.

## Android Mobile



317 physical devices, 18,101 emulated ones.

What about fingerprint properties?





## Client ID Certificate Fingerprints (2)

### For Desktop:

- **Uniqueness:** Not unique due to certificate chain as a *whitebox within CDM binaries*.
- **Stability:** Linked to a version of the Widevine binary.

### For Android Mobile:

- **Uniqueness:** *Unique for all devices*, due to per device certificate provisioning.
- **Stability:** *Strong stability* tested on a 2 years period.



## Client ID Certificate Fingerprints (2)

### For Desktop:

- **Uniqueness:** Not unique due to certificate chain as a *whitebox within CDM binaries*.
- **Stability:** Linked to a version of the Widevine binary.

### For Android Mobile:

- **Uniqueness:** *Unique for all devices*, due to per device certificate provisioning.
- **Stability:** *Strong stability* tested on a 2 years period.





# Client Info Augmented User-Agent

```
Cert Serial Number: XXXXXXXXXXXXeb24ab4d9025ae96f928bc7cf3169f965946XXXXXXXXXXXXXXXXXX
Client Info:
  Application Name: org.mozilla.firefox
  Package Cert Hash: p4tipRZbRJSy/q2edqKA0i2Tf+5iUa70WZRGsuoxmwQ=
  Company Name: Google
  Model Name: Pixel 6
  Architecture Name: arm64-v8a
  Device Name: oriole
  Product Name: oriole
  Build Info: google/oriole/oriole:12/SD1A.210817.015.A4/7697517:user/release-keys
  Widevine CDM Version: 16.1.0
  OEM Crypto Build Info: OEMCrypto Level3 Code 22594 May 28 2021 16:59:07
  OEM Crypto SPL: 0
```

Figure: Client Info of a Google Pixel 6.



# Client Info Augmented User-Agent

When the Client ID appears in clear:

Client Info can be used as a **never-lying enhanced User-Agent HTTP Header** as it cannot be modified/influenced by the browser.

Especially a problem considering current initiatives<sup>6</sup>.

---

<sup>6</sup>Google. *User-Agent reduction*. <https://developer.chrome.com/docs/privacy-sandbox/user-agent-reduction/>



# Client Info Augmented User-Agent

When the Client ID appears in clear:

Client Info can be used as a **never-lying enhanced User-Agent HTTP Header** as it cannot be modified/influenced by the browser.

Especially a problem considering current initiatives<sup>6</sup>.

---

<sup>6</sup>Google. *User-Agent reduction*. <https://developer.chrome.com/docs/privacy-sandbox/user-agent/>, 2022.



# Takeaways

## EME Widevine Privacy Leakage:

- Widevine opaque messages bring real privacy risks:
  - *Unique* and *stable* fingerprints for Android.
  - *Never-lying* User-Agent for Desktop and Android.
  - *Stateful* tracking with persistent sessions (more details in the paper).

## Responsible Disclosure:

- Disclosure to Mozilla in December 2022.
  - Rewarded by their Bug Bounty program and Hall of Fame.
  - Now patched since Firefox 109.0a1.
- Disclosure to the Widevine team.



# Takeaways

## EME Widevine Privacy Leakage:

- Widevine opaque messages bring real privacy risks:
  - *Unique* and *stable* fingerprints for Android.
  - *Never-lying* User-Agent for Desktop and Android.
  - *Stateful* tracking with persistent sessions (more details in the paper).

## Responsible Disclosure:

- Disclosure to Mozilla in December 2022.
  - Rewarded by their Bug Bounty program and Hall of Fame.
  - Now patched since Firefox 109.0a1.
- Disclosure to the Widevine team.





# Takeaways

## EME Widevine Privacy Leakage:

- Widevine opaque messages bring real privacy risks:
  - *Unique* and *stable* fingerprints for Android.
  - *Never-lying* User-Agent for Desktop and Android.
  - *Stateful* tracking with persistent sessions (more details in the paper).

## Responsible Disclosure:

- Disclosure to Mozilla in December 2022.
  - Rewarded by their Bug Bounty program and Hall of Fame.
  - Now patched since Firefox 109.0a1.
- Disclosure to the Widevine team.



# Takeaways

## EME Widevine Privacy Leakage:

- Widevine opaque messages bring real privacy risks:
  - *Unique* and *stable* fingerprints for Android.
  - *Never-lying* User-Agent for Desktop and Android.
  - *Stateful* tracking with persistent sessions (more details in the paper).

## Responsible Disclosure:

- Disclosure to Mozilla in December 2022.
  - Rewarded by their Bug Bounty program and Hall of Fame.
  - Now patched since Firefox 109.0a1.
- Disclosure to the Widevine team.



# Takeaways

## EME Widevine Privacy Leakage:

- Widevine opaque messages bring real privacy risks:
  - *Unique* and *stable* fingerprints for Android.
  - *Never-lying* User-Agent for Desktop and Android.
  - *Stateful* tracking with persistent sessions (more details in the paper).

## Responsible Disclosure:

- Disclosure to Mozilla in December 2022.
  - Rewarded by their Bug Bounty program and Hall of Fame.
  - Now patched since Firefox 109.0a1.
- Disclosure to the Widevine team.



# Takeaways

## EME Widevine Privacy Leakage:

- Widevine opaque messages bring real privacy risks:
  - *Unique* and *stable* fingerprints for Android.
  - *Never-lying* User-Agent for Desktop and Android.
  - *Stateful* tracking with persistent sessions (more details in the paper).

## Responsible Disclosure:

- Disclosure to Mozilla in December 2022.
  - Rewarded by their Bug Bounty program and Hall of Fame.
  - Now *patched since Firefox 109.0a1*.
- Disclosure to the Widevine team.





Paper link!










# Thanks for your attention

@ gwendal.patat@irisa.fr

@avalonswanderer

Avalonswanderer

# Bibliography I

-  Apple. *Apple FairPlay*. <https://developer.apple.com/streaming/fps/>. 2023.
-  Can I Use. *Encrypted Media Extensions*. <https://caniuse.com/eme>. 2023.
-  Counter, Stat. *Desktop Browser Market Share Worldwide*.  
<https://gs.statcounter.com/browser-market-share/desktop/worldwide/2022>. 2022.
-  —. *Mobile Tablet Android Version Market Share Worldwide*.  
<https://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide>. 2022.
-  Dorwin, David et al. *Encrypted Media Extensions*.  
<https://www.w3.org/TR/encrypted-media/>. 2019.
-  Google. *User-Agent reduction*.  
<https://developer.chrome.com/docs/privacy-sandbox/user-agent/>. 2022.
-  Google Widevine. *Widevine*. <https://widevine.com/>. 2023.

# Bibliography II



Microsoft. *Microsoft PlayReady*. <https://www.microsoft.com/playready/>. 2023.