ökko

VIDEO CONTENT PROTECTION OVERVIEW FOR FRONTEND DEVELOPERS

Alexey Golubev, CTO, Okko

DATE: 5.03.19

ökko

CONTENT PROTECTION BASICS

The Pirate Bay

NO PIRACY
346
REGENCY

ökko

Why Content Protection?

1. Legal digital content distributed online should be protected by Digital Rights Management (DRM) system
2. DRM is studio-approved content protection ecosystem
3. Content is encrypted and user obtains decryption key after purchase
4. Protection guidelines are defined by licensors
5. Technical capabilities are dependent on hardware/software platform

ökko

Protected video files

1. Multi-bitrate video tracks support for adaptive streaming
    1. Each video track is MP4 H.264 or H.265
    2. H.265 and other codecs should be supported on platform
2. Multi-audio tracks, subtitles, Trickplay tracks (<<, >>)
3. Video content encrypted with AES-128

ökko

Adaptive Streaming

ökko

Encrypted content

1. Video content encrypted with AES-128
2. Can be decrypted with the key

DRM protected content - all of the above and…

3. Secret key storage (keybox)
4. License = key + rules
5. License request outside player
6. Protected and robust infrastructure

ökko

DRM Licenses

1. **License** = Key to decrypt content + Distribution rules
2. Different content can be distributed by different rules
3. **TVOD: DTO**
   - “forever” license window: 5-10 years
4. **TVOD: Rent**
   - license window: 30 days
   - playback window: 2 days
5. **SVOD: Subscription**
   - renewable license window

ökko

Online & Offline Protected Playback

1. Encrypted asset is not stored on the device
2. Requires short-term license storage on device
3. Invalidate license right after playback

1. Encrypted asset should be stored on the device
2. License should be stored on the device
3. Invalidate license by internal timer or when online
4. Supported only on devices with secure clock!

100R-6522901/A120
PC-45/5572A/RN-25
DIP54
H2/447-500
T15
2537377Z0

ökko

Software & Hardware DRM

1. **CDM** – Content Decryption Module
2. **Software-based CDM** (i.e. in some web browsers):
    1. Native software library integrated to browser platform
    2. Obfuscated and signed
    3. Accessible through library API via plugin or HTML5 (MSE and EME)
3. **Hardware CDM** (on CE devices, smartphones, etc.):
    1. Integrated to device firmware and hardware during manufacturing process
    2. API to access high-level platform DRM methods

DRM via Software (Secure)

Decryption/decoding processes occur in user-space: player app pushes frames to screen

DRM via Software TEE (More Secure)

Decrypted/decoded frames pass through user-space: player app pushes frames to screen

DRM via Hardware TEE (Most Secure)

Decrypted/decoded frames securely pass directly to screen

ökko SOFTWARE & HARDWARE DRM

	Software CDM	Hardware Assisted CDM: HW key storage + SW video path	Hardware CDM: HW key storage + HW video path
SD	Approved	Approved	Approved
HD (720p) & FullHD (1080p)	Partially Approved	Approved	Approved
UltraHD (4K)	Restricted	Restricted	Approved
	Desktop Browsers	Android & iOS Browsers: Chrome on Android & Safari on iOS	CE Devices: SmartTVs, STBs, Android & iOS native apps

YOU CAN NOT PLAY ULTRA HD
CONTENT IN BROWSERS
SAD :(

DIGITAL RIGHTS MANAGEMENT SYSTEMS

ökko

Classic DRM

1. Widevine Classic
   - Multibitrate WVM-file format (single file)
2. PlayReady Smooth Streaming
   - ISM-manifest + multibitrate binaries (ismv)
3. Adobe Flash Access
   - F4M-manifest + multibitrate binaries (f4f)
4. Verimatrix, Securemedia, Marlin, NagraVision, Irdeto and others

ökko

Modular DRM (1)

Based on open industry standards:

1. **DASH** – Dynamic Adaptive Streaming over HTTP

   http://dashif.org/

2. **CENC** – Common Encryption ISO/IEC 23001-7:2012

   http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=60397

3. **MSE** – Media Source Extensions

   https://www.w3.org/TR/media-source/

4. **EME** – Encrypted Media Extensions

   https://www.w3.org/TR/encrypted-media/

   https://www.html5rocks.com/en/tutorials/eme/basics/

5. **CDM** – Content Decryption Module

ökko

Modular DRM (2)

1. **ClearKey** – encryption with predefined key.
   Supported by any browser. Good for testing.
2. **pssh-box** – unique DRM system identifier
3. **AES-128** based – single binary encryption
4. Single DASH manifest with multiple DRM metadata

ökko

Modular DRM Systems

1. Microsoft PlayReady
2. Google Widevine
3. Apple FairPlay
4. Adobe Primetime

ökko

Distribution by Platforms

PlayReady

Fairplay

Widevine

ökko

BORING?

ökko

YOUR USER REQUIREMENTS INCLUDE FOUR HUNDRED FEATURES.
DO YOU REALIZE THAT NO HUMAN WOULD BE ABLE TO USE A PRODUCT WITH THAT LEVEL OF COMPLEXITY?
GOOD POINT. I'D BETTER ADD "EASY TO USE" TO THE LIST.
www.dilbert.com scottadams@aol.com
4/14/01 © 2001 United Feature Syndicate, Inc.

ökko
BACK
END
VS
FRONT
END

ökko

DRM Component Flow

ökko

DRM Component Flow

ökko

PLAYER WITH DRM: BROWSERS

ökko

Media Source Extensions aka MSE

Extends **`HTMLMediaElement`** to allow JavaScript to generate media streams for playback by dynamically constructing media streams for **`<audio>`** and **`<video>`**

https://www.w3.org/TR/media-source/#examples

ökko

MSE

MediaSource
SourceBuffer
SourceBuffer
SourceBuffer
Media Source API
HTML Media Element
Track Buffer
Track Buffer
Track Buffer
Track Buffer
Track Buffer
Video Decoder
Audio Decoder
Audio Decoder
Video Decoder
Audio Decoder
Audio Device
Video Tag Display Region

ökko

Encrypted Media Extensions aka EME

Extends **`HTMLMediaElement`** providing APIs to control playback of encrypted content by selecting content protection mechanisms, control license/key exchange, and execute custom license management algorithms

https://w3c.github.io/encrypted-media/#examples

ökko

EME

CDN
License Server
Web Server may handle requests or send them directly to License Server.
Web Server
Get License
License
Get License
License
Application
encrypted
requestMedia-KeySystemAccess()
createMediaKeys()
createSession()
generateRequest()
message
update()
createSession()
generateRequest()
message
update()
Dashed lines show an optional additional session (includes dotted lines) or additional round trip.
Net
Media Stack
MediaKeySession
MediaKeySession
Browser
Generate Reouest
License Request
Provide License
Generate Request
License Request
Provide License
Decrypt Frame
Frame
CDM implementations may return decrypted frames or render them directly
Content Decryption Module
CDM may use or defer to platform capabilities
Frame
Platform
Legend
Content
Encrypted Key
Other Command/Event
Optional

ökko

Browser DRM Support

HTML5 Browsers	PlayReady	Widevine Modular	FairPlay
Chrome (35+)			
Firefox (47+)			
Opera (31+)			
Internet Explorer (11)			
Microsoft Edge			
Safari			

ökko

Detecting EME and requestMediaKeySystemAccess support

```
var hasEMESupport = function() {
  var eme = "MediaKeys" in window || "WebKitMediaKeys" in window || "MSMediaKeys" in window;
  if (eme) {
    return true;
  }
  return false;
}
```

```
var hasRMKSASupport = function() {
  var requestMediaKeySystemAccess = "requestMediaKeySystemAccess" in window.navigator;
  if (requestMediaKeySystemAccess) {
    return true;
  }
  return false;
}
```

Detecting EME and requestMediaKeySystemAccess support

```
var config = [{
  "initDataTypes": ["cenc"],
  "audioCapabilities": [{
    "contentType": "audio/mp4;codecs=\"mp4a.40.2\""
  }],
  "videoCapabilities": [{
    "contentType": "video/mp4;codecs=\"avc1.42E01E\""
  }]
}];
try {
  navigator.
  requestMediaKeySystemAccess("com.widevine.alpha", config).
  then(function(mediaKeySystemAccess) {
    console.log('widevine support ok');
  }).catch(function(e) {
    console.log('no widevine support');
    console.log(e);
  });
} catch (e) {
  console.log('no widevine support');
  console.log(e);
}
```

ökko

ALMOST NO REASON TO REINVENT THE WHEEL

ökko

Paid Solutions

1. **Bitmovin**

   https://bitmovin.com/video-player/

2. **Brightcove**

   https://www.brightcove.com/en/player

3. **PRESTOplay**

   https://castlabs.com/products/prestoplay-browser/

4. **NexPlayer**

   https://www.nexplayersdk.com/

5. **THEOPlayer**

   https://www.theoplayer.com/

ökko

Open Source Players

1. **Shaka Player** – by Google
   http://g.co/shakainfo
2. **DashJS** – by Dash Industry Forum
   https://github.com/Dash-Industry-Forum/dash.js
3. **VideoJS** – sponsored by Brightcove
   1. Basic – https://github.com/videojs/http-streaming
   2. EME plugin – https://github.com/videojs/videojs-contrib-eme
4. **RxPlayer** – by Canal+
   https://github.com/canalplus/rx-player

ökko

Players DRM Support

	ClearKey	PlayReady	Widevine	FairPlay
Shaka Player	Yes	Yes	Yes	In progress
DashJS	Yes	Yes	Yes	—
VideoJS	Yes	IE11 only	Unknown	Yes
RxPlayer	Yes	Yes	Yes	—

ökko

Shaka Player: DRM Support Matrix

Browser	Widevine	PlayReady	FairPlay	ClearKey
Chrome	Yes	—	—	Yes
Firefox	Yes	—	—	Yes
Edge	—	Yes	—	—
IE11	—	Yes	—	—
Safari	—	—	In progress	—
Opera	untested	—	—	untested
Chromecast	Yes	Yes	—	untested
Samsung Tizen	Yes	Yes	—	untested

ökko

PLAYER WITH DRM: CE DEVICES

ökko

SmartTV DRM Support

Smart TVs	PlayReady	Widevine Modular	Widevine Classic	FairPlay
Samsung (Tizen) 2017-2018+				
Samsung (Tizen) 2015-217				
Samsung (Orsay) 2010-2015			70%	
LG (webOS & Netcast)				
Smart TV Alliance (LG, Philips, Toshiba, Panasonic)				
Android TV				

ökko

Other CE DRM Support

Set-top Boxes & Casting	PlayReady	Widevine Modular	FairPlay
Chromecast			
Android TV			
Apple TV			
Game Consoles			
Xbox One / 360			
PlayStation 3 / 4			

AND SO YOU CODE...

ökko

Proprietary Player API Nightmare

Samsung Maple

```
media: {
  playerClasses: ['Samsung', 'SamsungSef']
}
```

Samsung+Shaka

```
media: {
  playerClasses: ['HTML', 'HTMLShaka']
}
```

Samsung Tizen

```
media: {
  playerClasses: ['SamsungAVPlayTizen']
}
```

LG Netcast

```
media: {
  playerClasses: function () {
    return ['LG'].concat(Platform.isWebosInNetcastMode() ? 'LGWebos' : 'LGNetcast')
  }
}
```

LG WebOS

```
media: {
  playerClasses: ['HTML', 'HTMLWebos', 'HTMLShakaWebos']
},
```

XBox

```
media: {
  playerClasses: ['HTML', 'HTMLEdge']
}
```

Playstation

```
media: {
  playerClasses: ['Playstation']
}
```

Panasonic, Netrange

```
media: {
  playerClasses: ['HTML']
}
```

Sony, HiSense

```
media: {
  playerClasses: ['HTML', 'HTMLWebInitiator']
}
```

Philips

```
media: {
  playerClasses: function () {
    return Platform.generation > Platform.GENERATIONS.G_2015 ? ['HTML'] : ['CEHTML', 'CEHTMLCAD']
  }
}
```

ökko

Proprietary Player API Nightmare

WHERE ARE MSE AND EME?

ökko

Samsung SmartTV

1. Tizen 3.0 & 4.0 (since 2017)
2. MSE 2015-2016 / EME 2016
3. DASH + CENC + WV & PlayReady
4. Full specification:

   https://developer.samsung.com/tv/develop/specifications/media-specifications

ökko

LG SmartTV

webOS TV Developer

1. WebOS TV 4.0 (since 2016)
2. MSE 2016 / EME 2015
3. DASH + CENC + Widevine & PlayReady
4. Full specification

   http://webostv.developer.lge.com/discover/webos-tv-platform/supported-media-formats/
5. DRM Implementation

   http://webostv.developer.lge.com/develop/app-developer-guide/playing-drm-content/

ELIMINATE
DRM
DefectiveByDesign.org

ökko

Defective by Design

On July 6, 2017, the W3C greenlighted DRM for the Web.

CANCEL
NETFLIX

The motive for DRM schemes is to increase profits for those who impose them, but their profit is a side issue when millions of people's freedom is at stake; desire for profit, though not wrong in itself, cannot justify denying the public control over its technology. Defending freedom means thwarting DRM
– Richard Stallman, President of the Free Software Foundation

https://www.defectivebydesign.org/

ökko

Defective by Design

Firefox still suggests EME/CDM free copy to download

Chrome since v57 disable availability to exclude EME/CDM

CONCLUSIONS

ökko

Conclusions

1. Understand standards: DASH, MSE, EME, etc.
2. Don’t reinvent the wheel
3. Use open source (Shaka, RxPlayer, etc.)
4. Avoid proprietary APIs
5. Study Smart TV vendor documentation
6. Defeat fragmentation nightmare
7. Enjoy the coding!

THANK YOU

BACKUP

DRM proxy

1. Content provider’s backend component
2. Controls internal business logic using optional client data
3. Can replace policies and some request parameters
4. Creates signed requests and sends to license server to get license
5. Can extract status codes from license responses
6. Check heartbeat-requests

Robustness rules

1. Compliance and robustness rules for:
    1. Content distributor
    2. Hardware product
2. Defines mandatory rules to implement and integrate DRM solution
3. Device security and trust level depends on DRM implementation (software vs platform)

Live stream specifics

1. Mpeg-ts chunks
2. Key rotation
3. DVR (Digital video recorder) window
4. Very sensitive to playlist format and time synchronization

ökko

CENC Encryption schemes

1. **CENC AES-CTR** or **cenc**: CENC Protection Scheme using AES 128-bit keys in Counter Mode (AES-128 CTR),
2. **CENC AES-CBC** or **cbc1**: CENC Protection Scheme using AES 128-bit keys in Cipher-block chaining mode (AES-128 CBC),
3. **CENC AES-CTR Pattern** or **cens**: CENC Protection Scheme using AES 128-bit keys in Counter Mode (AES-128 CTR) using pattern of unencrypted/encrypted bytes,
4. **CENC AES-CBC Pattern** or **cbcs**: CENC Protection Scheme using AES 128-bit keys in Cipher-block chaining mode (AES-128 CBC) using pattern of unencrypted/encrypted bytes

ökko

More topics to cover

1. License acquisition flow
2. License wrapping for EME to integrate user data

ökko OLD SMART TV FRAGMENTATION

Supported DRMs

	Streaming protocol	Widevine classic	Smooth Streaming	DASH				Test content playback result
	DRM	Widevine classic	Playready	Playready	Widevine	Prime	FairPlay	
Samsung	Orsay 2013	Yes	Yes	Supported OIPF Rely / MPEG2 Sony / AES-128				N/A
	Orsay 2014	Yes	Yes	Supported OIPF Rely / MPEG2 Sony / AES-128				Yes
	Tizen 2015	Yes	Yes	Yes	No	No	No	Yes
	Tizen 2016	Yes	Yes	Yes	No	No	No	N/A
LG	NC 2014	Yes	Yes	No	No	No	No	Particularly
	WebOS 2014	Yes	Yes	Yes	No	No	No	Yes
	NC 2015	Yes	Yes	Yes	No	No	No	N/A
	WebOS 2015	Yes	Yes	Yes	No	No	No	N/A
	SS 2016	Yes	Yes	Yes	No	No	No	N/A
	WebOS 2016	Yes	Yes	Yes	No	No	No	N/A
Sony	2013	No	Yes	No	No	No	No	No
	2014	No	Yes	Yes	No	No	No	
	Android 2015	No	Yes	Yes	N/A	N/A	No	
	Android 2016	No	Yes	Yes	N/A	N/A	No	N/A
Philips	2012	Yes	Yes	No	No	No	No	No
	2013	Yes	Yes	No	No	No	No	No
	2014	Yes	Yes	No	No	No	No	No
	Android 2015	Yes	Yes	No	N/A	N/A	No	N/A
	Android 2016	Yes	Yes	No	Yes	N/A	No	N/A
PS	PlayStation 3	No	Yes	Yes	No	No	No	
	PlayStation 4	No	Yes	Yes	No	No	No	