DRM in the Age of HTML5

From Alphabet Soup to Nirvana….. Right?
Digital Media @Frost_Sullivan: Research Coverage

- Marketing Process Optimization
- Dynamic Publishing
- Digital Asset Management & Enterprise Content Management
- Animation & CAE Software
- Encoding & Transcoding
- Broadcast & Cinematography Cameras
- Media Asset Management
- Nonlinear Editing
- Video Switchers
- Video & Ad Insertion Servers
- IRDs
- Broadcast Scheduling Systems
- IP Video Network Management
- Online Video Platforms & Analytics
- Online Video Platforms
- Enterprise Search
- Online Video & Web Analytics
- Marketing Automation
- Enterprise Search
- Online Video & Web Analytics
- Digital Signage
- Video Enabled Consumer Devices
- 3D Technologies
- Multi-Platform Delivery & CDNs
- Multi-Platform Delivery & CDNs
- Pay TV Platforms
- Multi-Platform Delivery & CDNs
- Multi-Platform Delivery & CDNs
- Content Protection, Entitlement & Rights Management
- Content Protection, Entitlement & Rights Management
- Content Protection, Entitlement & Rights Management
- Pay TV Platforms
- Content Protection, Entitlement & Rights Management
- Pay TV Platforms
- Content Protection, Entitlement & Rights Management
- Pay TV Platforms
- Content Protection, Entitlement & Rights Management
- Pay TV Platforms
- Content Protection, Entitlement & Rights Management
- Pay TV Platforms
@Avni_FS @Frost_Sullivan: Research Coverage

Digital Media Value Chain:

- Lecture Capture & Video Webcasting
- Marketing Automation
- Enterprise Search
- Online Video & Web Analytics
- Multi-Platform Delivery & CDNs
- Digital Signage
- Video Enabled Consumer Devices
- 3D Technologies

Acquisition:
- Marketing Process Optimization
- Dynamic Publishing
- Animation & CAE Software
- Encoding & Transcoding

Middleware and Workflow:
- Digital Asset Management & Enterprise Content Management
- Content Protection, Entitlement & Rights Management
- Nonlinear Editing
- Video Switchers
- Video & Ad Insertion Servers
- IRDs
- Broadcast Scheduling Systems
- IP Video Network Management
- Pay TV Platforms
- Online Video Platforms & Analytics

Delivery:
- Multi-Platform Delivery & CDNs
- Pay TV Platforms
- Online Video Platforms & Analytics
- Multi-Platform Delivery & CDNs

Storage:
- Content Protection, Entitlement & Rights Management
- Media Asset Management
- Media Asset Management
- Media Asset Management
- Media Asset Management
- Media Asset Management

Enterprise Media and Entertainment:
- Pay TV Platforms
- Online Video Platforms & Analytics
- Multi-Platform Delivery & CDNs

Broadcast & Cinematography Cameras
- Encoding & Transcoding
- Animation Software

Marketing Automation
- Dynamic Publishing
- Animation & CAE Software
- Encoding & Transcoding
Outline

• DRM 101
• Motivations for interoperable secure playback
• Disruptions, options and solutions
• Conclusions

• Not Covering:
  • How DRM actually works
  • DRM for physical media (AACS, etc.) or bouquet broadcasts
  • Details and specifics of the standards themselves
How Do ~You~ Define DRM?
Definitions

- **DRM**: A mathematical core, in a wrapper of trust, bringing protected content business models to life
- **DRM vendor**: A trusted business partner
- **Piracy**: Imperfectly controlled distribution of content, resulting in loss of (retail, subscription, transaction, ad,...) revenue to service provider & content owner
- **Monetization**: Generating revenue through content and the use of content
- **User**: The instrument of monetization. Not to be confused with pirate.
  - Ideally we don’t want to alienate or inconvenience them (or force them to choose a certain browser, or brick their devices, or have them arrested, or....)

Source: Frost & Sullivan
OTT Content Protection: Many Forms

- Open streaming, with player tied to web page
- Stream encryption
- Digital Rights Management
- Watermarking and Fingerprinting

- DRM is a business of trust
  - Defining characteristics of trust are robustness and resilience
  - Encryption/decryption is one feature
  - Controlled output is one feature
  - Enforcement of user-specific, time-variant policy is one feature
  - Data reporting for analytics is one feature

Source: Frost & Sullivan
Elements of A DRM System

Many server-side and client-side features come together to enable protection and monetization.

<table>
<thead>
<tr>
<th>Authentication and User-Specific Encryption</th>
<th>Content-Specific Encryption</th>
<th>Rights Definition &amp; Restrictions Enforcement</th>
<th>Revocation and Renewal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Control and Link Protection</td>
<td>Forensics &amp; traitor tracing</td>
<td>Interface to billing and tracking</td>
<td>Key &amp; license management</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan Analysis, Verimatrix
Robustness Rules: DRM’s Raison d’Etre

• How robust a DRM client is against hacking at the time of shipping or installation, and how resilient it will be to compromise over time
• Crux of specifications is difficulty of extracting private key, content keys and decrypted compressed content by pirates
• DRM vendors win trust of copyright owners and pass on select obligations to device, player and server developers
• Each studio negotiates agreements with individual service providers; generally norms are consistent
• Service providers in turn rely on app developers, CE device manufacturers and DRM value added resellers to meet these obligations. Their goal is to run a profitable, popular service:
  • Maximize device reach but optimize development and maintenance costs/complexity
  • Achieve consistent, pleasant user experience across all devices and screens: managed experiences on unmanaged platforms
  • Avoid penalties associated with breaches or non-compliance

Source: Frost & Sullivan
Outline

- DRM 101
- Motivations for interoperable secure playback
- Disruptions, options and solutions
- Conclusions
Motivation: Growth in OTT Plus Rise in Device Fragmentation Creates Intolerable Complexity

- OTT services are a competitive imperative for all content companies
- Massive shift away from PC-based streaming to device-based consumption; soaring online video consumption
- 8 classes (and growing) of PCs and connected video devices
  - Over 200 vendors, each with 2-20 models
  - Different OSs (e.g. Android, Android, Android, Android, and others)
  - Different security tools, APIs, threat surfaces…. 
  - HLS/HDS/Silverlight/DASH; TEE/Software; Counter mode v/s CBC mode v/s pattern encryption
- Building secure players is a huge challenge
  - Even if DRM core is free, secure player is not
  - ABR_profiles * encryption_formats * streaming_formats * DRM_System(s) * consistent_UX = Intolerable_Complexity
  - Ideally, goal is to enable enough interoperability across streaming and DRM implementations that OTT players can be made DRM-agnostic

Source: Frost & Sullivan
Motivation: Robustness Requirements (and Implementation Costs) Grow As Content Resolution Grows

Level of restriction has some variance depending on value of content and preference of copyright owners. Below figure shows general norms.

Source: Frost & Sullivan
Silos Give Way to Standards (sort of)

- “Interoperable DRM” aspired to since ~2000AD
- Intermediate Progress: HbbTV, Ultraviolet,….
- Business priorities, immature technology and lack of intolerable pain slowed progress
- Come 2015, Significant Achievements:
  - Media Source Extensions, Encrypted Media Extensions in HTML 5
  - Common Encryption in DASH
  - CDMi Interface for browsers
Cross-platform commercial video apps are enabled by the Encrypted Media Extensions and Media Source Extensions to HTML5.

The Media Source Extensions are the W3C HTML5 application correlate to the MPEG DASH media presentation specification.

The Encrypted Media Extensions are the W3C HTML5 application correlate to the MPEG CENC multi-DRM specification and work with DASH.

Combined these four specifications enable interoperability and the mobility of experience for commercial video distributed over the Internet.
The Underlying Plumbing

HTML/JavaScript Application

Browser

Content Decryption Module

Digital Rights Management

Trusted Execution Environment

Player

Client

Core

Source: John Simmons @ Microsoft Corporation
You Can Doesn’t Mean You May (or vice-versa)

- Parallels to CAS:
  - Content key **exchanged** via unregulated license transaction
  - Content key **utilized** via standardized algorithms and protocols

- Standards-compliant DRM core is irrelevant unless the service provider is allowed to use it for a given content title and resolution on that device.

- DRM core and DRM client are two distinct entities
  - DRM Core: Decryption, decompression & output protection enforcement
    - Still has to be built device by device.
    - Standardized TEEs can help, but not much.
    - Cannot, alone, meet robustness and compliance obligations
  - DRM Client: Authentication, license transactions, revocation & SRMs, anti-jailbreak, forensics, analytics, etc.
  - Secure Player: Adds UX, ad insertion, overlays, controls, rendering etc. around DRM client

Source: Frost & Sullivan
# The Media Playback Ecosystem: Types of Stakeholders

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRM Cores</td>
<td>PlayReady, Widevine, Marlin, VCAS, PrimeTime, …</td>
</tr>
<tr>
<td>Multi-DRM Solution</td>
<td>Verimatrix, Ericsson, CastLabs, Inka Networks, Neulion, BuyDRM, EZ DRM, Other CAS vendors, …</td>
</tr>
<tr>
<td>Players</td>
<td>VisualOn, InsideSecure, HASPlayer, DASH JS Player, Device-native players, most OVPs, …</td>
</tr>
<tr>
<td>Browsers</td>
<td>Google, Microsoft, Apple, Mozilla, some others</td>
</tr>
<tr>
<td>CE Device Vendors</td>
<td>Samsung, Apple, Microsoft, Sony, Panasonic, Google, Technicolor …</td>
</tr>
<tr>
<td>Silicon Vendors</td>
<td>ARM, Intel, Broadcom, Qualcomm, Sigma, ST Micro, …</td>
</tr>
</tbody>
</table>
Robustness Requirements Revisited

The most common fail-safe option is to deliver a lower resolution stream if an acceptable hardware-secured DRM core is not available.

Software Client

Hardware-Assisted Security

Full Hardware Decrypt/Decode

SD

720p

1080p

HD+

4K

Source: Frost & Sullivan
Outline

• DRM 101
• Motivations for interoperable secure playback
• Disruptions, options and solutions
• Conclusions
The End of Plug-Ins and the Age of DASH

• Support for plug-ins in browsers is dropping, driven by rising complexity and development of alternative standards
  • Google dropping support for NPAPI in Chrome
  • Microsoft ending support for ActiveX in IE
• Consequence: Flash and SmoothStreaming may/will not be available through browsers moving forward
  • Apps can still support it
• With DRM being a cost center for most vendors, transition guidance and backward compatibility can be afterthoughts
  • Problematic consequences for developers and manufacturers
• Most secure player vendors reporting that as of 2015, use of DASH is under 5% and plug-ins or apps are still the preferred solution for secure content delivery.
Interoperability was designed to allow any DRM to be consistently accessed from any browser, so long as DRM was implemented. Reality is that browsers are being implemented with only one DRM system, though in standards-compliant fashion:
- Chrome: Widevine
- Safari: FairPlay
- Edge: PlayReady
- Firefox: Primetime

Security level of DRM core implementation can differ across devices. Operators will thus need to prepare to license and implement several DRM systems, although this is still less complex than implementing and maintaining a portfolio of device-specific apps. Businesses wishing to work with a specific DRM system at a specific level will need to be smart about how they leverage HTML5.

Source: Frost & Sullivan
## Apps v/s Browsers: Pros and Cons

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Native Apps:</strong> Higher control, but high cost and complexity</td>
<td><strong>Cons</strong></td>
</tr>
<tr>
<td>• Easier to make secure</td>
<td>• Expensive to build – consistently – across all devices</td>
</tr>
<tr>
<td>• Usually richer, more fluid experiences</td>
<td>• Cumbersome to develop and deploy upgrades over time</td>
</tr>
<tr>
<td>• By and large, freedom to choose your own DRM system</td>
<td></td>
</tr>
<tr>
<td><strong>Browser-based Rendering:</strong> Simplicity, but at a price</td>
<td></td>
</tr>
<tr>
<td>• Rely on standards to specify features</td>
<td>• Rely on browsers to (imperfectly?) implement features</td>
</tr>
<tr>
<td>• Smaller support matrix compared to individual devices</td>
<td>• Bound to user’s choice of browser.</td>
</tr>
<tr>
<td>• Upgrade app everywhere just by rewriting a web page</td>
<td>• Restricted, as of now, to using the one DRM called by the specific browser</td>
</tr>
</tbody>
</table>

**Hosted Web Apps can provide best of both worlds:**
- Update one web page, then low overhead to change all app instances
- Allows one consistent browser to be encapsulated across all app ports
- As an example, Edge powers Manifold JS project, Cordova extensions
- More flexibility, and predictability, in which DRM system will be used
- Still relies on underlying DRM system to be natively integrated in device.

Source: Frost & Sullivan
Recommended Best Practices

• Browser vendors: Make it easy for secure player vendors to wrap your browser into a hosted web app targeting a wide ranges of devices and platforms.
• SoC vendors/CE manufacturers: Aim to natively integrate two DRM cores with a full hardware video path. One is unlikely to be competitive enough; more than two is likely to be too expensive.
• Service providers: Plan to support 3-5 DRM systems in your operations center. Seriously consider a reliable multi-DRM solution which pushes this complexity under its hood.
• DRM vendors: The TEE isn’t infallible, so hardening of core and client will still be required. A renewability strategy is crucial.
• Player developers: For now, we believe hosted web apps offer the best balance between portability, consistency, rights to render highest quality content, and excellence of user experience.

Source: Frost & Sullivan
Outline

• DRM 101
• Motivations for interoperable secure playback
• Disruptions, options and solutions
• Conclusions
Conclusions

• Standardization sorely needed to solve the expense and complexity of consistent secure playback in fragmented PC/device ecosystem
  • MSE, EME and CENC enable huge strides forward
• Can I v/s May I: The complexity of DRM is in secure decryption and playback, but what ultimately defines DRM is trust. Theoretically, interoperability is great. But, trust is hard to standardize.
  • There is, we believe, some misplaced confidence in the level of ubiquity current standards will provide, at least in the short term.
  • Multi-rights solutions are strongly recommended for most operators
• Failure is an option: You can deny service or use a lower resolution
  • Onus is on OEMs, browser developers and app developers to collectively ensure that the highest possible resolution of content can be delivered and played back on a given device.
  • Supporting two DRM systems, not just one, is recommended for device vendors and silicon vendors
• Change is coming, and will make things better. But overhauls to workflows will be needed, so plan and prepare now.

Source: Frost & Sullivan
## Acknowledgements (Selected)

- Adobe Systems
- Arxan Technologies
- CastLabs
- Ericsson
- Fraunhofer Fokus
- Microsoft
- Ooyala
- VisualOn
- Verimatrix
- Wowza
Stay in Touch

http://www.frost.com/AvniRambhia

@Avni_FS

http://www.linkedin.com/groups/Ask-Frost-Sullivan-Digital-Media-1787024/about

http://www.slideshare.net/FrostandSullivan

http://www.slideshare.net/FrostandSullivan
Resources

- Common encryption standards and their business implications
  - https://www.youtube.com/watch?v=14YnkW6ZsI0
- Migrating from Silverlight to HTML5 and DASH
  - http://blogs.windows.com/msedgedev/2015/07/02/moving-to-html5-premium-media/
- Multi-rights DRM in action
- Role of TEE in DRM Standardization
For Additional Information

Avni Rambhia
Principal, Digital Media
avni.rambhia@frost.com

Anisha Vinny
Sr. Research Analyst, Digital Media
anisha.vinny@frost.com