Multi-DRM in an HTML5 World

Perspectives, Do’s and Don’ts
Digital Media @Frost_Sullivan: Research Coverage

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

• DRM 102
• Browsers, Apps and DRM
• Pros and Cons of Various Approaches
• Implications of the Time Axis
• Conclusions

• Not Covering:
  • How DRM actually works
  • DRM for physical media (AACS, etc.) or bouquet broadcasts
  • Details and specifics of the standards themselves
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
Elements of A DRM System

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

- Authentication and User-Specific Encryption
- Content-Specific Encryption
- Rights Definition & Restrictions Enforcement
- Revocation and Renewal
- Output Control and Link Protection
- Forensics & traitor tracing
- Interface to billing and tracking
- Key & license management

Source: Frost & Sullivan Analysis, Verimatrix
Built-in DRM v/s Premium DRM: A Wide Spectrum

**Most likely to be built-in**

**Crypto Core**
- Trust anchors
- Key delivery
- Entitlement transfer
- Decryption

**Complete DRM Client**
- Time/location management
- Output control
- Richness of entitlement
- Entitlement enforcement
- Revocation & renewal

**Full Secure Player**
- Authentication
- Integrity verification
- Intelligent failure
- Watermarking
- Forensics & traitor tracing

The cryptographic core is the *necessary* heart of the protection system.

Higher-end DRMs will include more and more value added features. Depending on your service, you may need to push up this spectrum for *sufficient* protection.

Source: Frost & Sullivan
Multi-DRM server infrastructure provides consistency, scalability and future-proof fragmentation management for the service provider.

Source: Frost & Sullivan
HTML5 and its Implications

- Plug-in support is being dropped, so Flash and SmoothStreaming not available through browsers (apps can still support it)
- HTML5, with EME, was designed to allow any DRM to be consistently accessed from any browser with the goal of interoperability.
- Reality is that browsers are being implemented with only one DRM system
  - Chrome: Widevine; Safari: FairPlay; Edge: PlayReady
- Multi-DRM is a server-side abstraction of underlying complexity
  - Systems are not mostly but not fully interoperable
  - DASH/HLS; also encryption modes are still fragmented
  - Security level of DRM core implementation can differ across devices
  - Entitlement languages vary from system to system
  - Standards, versions and business requirements change over time
- Apps are the new middleware; browsers promise simplicity. Is there middle ground?

Source: Frost & Sullivan
The Client Dilemma: Browser v/s App

Browser

- Simplicity
- Discoverability
- Reach/Portability

Apps

- Roadmap Control
- Flexibility of DRM
- Feature Breadth/Depth

Source: Frost & Sullivan
The Client Dilemma: One Level Deeper

**Cons:**
- Operator has little influence over consumer choice of browser/DRM
- Standards/technology change at their own cadence
- UX options are constrained
- Updates are outside control of operator

**Cons:**
- Higher complexity upfront
- More effort to attract and retain viewers
- App version management creates overhead

**Source:** Frost & Sullivan
The Time Axis and the Update Chain

Planned Update Triggers:
- Proactive improvements in system
- New business models or improved content options
- Stronger or wider content protection requirements
- Algorithm-level compromises

Forced Update Triggers:
- Newly discovered vulnerabilities or loopholes
- Leak of systemic secrets
- Implementation-specific compromises

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Browser Scenario</th>
<th>App with Downloaded DRM Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop crypto core update</td>
<td>At DRM vendor’s discretion; content owners can influence</td>
<td>By DRM vendor; but operator can influence/replace</td>
</tr>
<tr>
<td>Integrate update in platforms</td>
<td>Relies on browser developers, OS developers and OEMs</td>
<td>In-house or under contract by operator</td>
</tr>
<tr>
<td>Distribute updated components to all current users</td>
<td>Relies on app store update features and/or evangelism</td>
<td>Can be accelerated by in-app messaging or other UX method</td>
</tr>
<tr>
<td>Achieving 90% dissemination</td>
<td>More variable</td>
<td>More deterministic</td>
</tr>
<tr>
<td>Fallback Options</td>
<td>Accept leakage, server-side management, transition to apps, and/or bricking</td>
<td>Wide range of possibilities at operator’s discretion</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan
## All Things Considered, What’s the Answer? It Depends.

<table>
<thead>
<tr>
<th></th>
<th>Suitability of browser-only</th>
<th>Impact from client diversity</th>
<th>Features needed beyond crypto core</th>
<th>Sensitivity to hacks</th>
<th>Impact of default DRM limitations **</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Service</strong></td>
<td><img src="DRM" alt="Basic Service" /></td>
<td><img src="DRM" alt="Basic Service" /></td>
<td><img src="DRM" alt="Basic Service" /></td>
<td><img src="DRM" alt="Basic Service" /></td>
<td><img src="DRM" alt="Basic Service" /></td>
</tr>
<tr>
<td>(checkbox DRM)</td>
<td><img src="DRM" alt="Basic Service" /></td>
<td><img src="DRM" alt="Basic Service" /></td>
<td><img src="DRM" alt="Basic Service" /></td>
<td><img src="DRM" alt="Basic Service" /></td>
<td><img src="DRM" alt="Basic Service" /></td>
</tr>
<tr>
<td><strong>Controlled Service</strong></td>
<td><img src="DRM" alt="Controlled Service" /></td>
<td><img src="DRM" alt="Controlled Service" /></td>
<td><img src="DRM" alt="Controlled Service" /></td>
<td><img src="DRM" alt="Controlled Service" /></td>
<td><img src="DRM" alt="Controlled Service" /></td>
</tr>
<tr>
<td>(e.g. OTT broadcasting)</td>
<td><img src="DRM" alt="Controlled Service" /></td>
<td><img src="DRM" alt="Controlled Service" /></td>
<td><img src="DRM" alt="Controlled Service" /></td>
<td><img src="DRM" alt="Controlled Service" /></td>
<td><img src="DRM" alt="Controlled Service" /></td>
</tr>
<tr>
<td><strong>Premium Service</strong></td>
<td><img src="DRM" alt="Premium Service" /></td>
<td><img src="DRM" alt="Premium Service" /></td>
<td><img src="DRM" alt="Premium Service" /></td>
<td><img src="DRM" alt="Premium Service" /></td>
<td><img src="DRM" alt="Premium Service" /></td>
</tr>
</tbody>
</table>

### Notes:

- Unlike CAS, switching DRM strategies is relatively easy if planned well. A robust multi-DRM backend goes a long way in enabling downstream agility.
- **In general. For specific devices, this may vary.
- More sophisticated the service, more important the ability to choose DRM. Apps are typically necessary to leverage non-default DRM options.

Source: Frost & Sullivan
Not to Forget: Content is at Risk in the Network Also

- Hackers will attack the weakest link, and that may not be the client
- Cybersecurity-style exploits on content repositories are a convenient way to siphon off large volumes of content
  - Larson Studios exploit last month
  - Netflix 4K content leak
  - Sony network infiltration
- Hijacking of OTT broadcast networks is also a threat
  - C-Span interrupted by foreign channel earlier this year
  - France’s TV5Monde saw similar interruptions in 2015
- IP-fication creates new opportunities but also opens up new risks
- “Holistic Security” gaining steam as a discipline
  - Cybersecurity for broadcast engineering has unique challenges
  - Leading CAS vendors are establishing consulting practices as well as product suites to help fill these gaps

Source: Frost & Sullivan and Cisco Systems
## Wrapping it Up: Do’s and Don’ts

<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Embrace multi-DRM</td>
<td>□ Simplistically favor “free” as natural default</td>
</tr>
<tr>
<td>□ Keep consistency, reach and longevity at the center of architecture choices</td>
<td>□ Assume that secure today = secure tomorrow</td>
</tr>
<tr>
<td>□ Judge level of control needed, and work to retain it</td>
<td>□ Feel devoid of choice</td>
</tr>
<tr>
<td>□ Pursue hybrid, agile strategies</td>
<td>□ Forget to account for the time axis</td>
</tr>
</tbody>
</table>

Tomorrow’s must-have will exceed today’s state-of-the-art. Default/native DRM will not be universally viable for premium services. Apps v/s browser decisions depend on specific service and target device.

Source: Frost & Sullivan
Questions?
Resources

- DRM & HTML5 101:

- Global Content Protection Market, Forecast to 2021
  [link](https://www.frost.com/c/10107/sublib/display-report.do?id=K12B-01-00-00-00)

- Global DRM Market, Forecast to 2020
  [link](http://www.frost.com/sublib/display-report.do?id=NF18-01-00-00-00)

- Thoughts on Multi-DRM (blog post)
  [link](http://www.frost.com/reg/blog-display.do?id=7749999)

- Multi-Faceted/Holistic Security for Content:

- DRM: Native v/s Downloadable and Aspects of Control