Simplifying "TV Everywhere:"

Principles for

a Robust Online

Video Entitlement System

Presented at the 2009SCTE Cable-Tec Expo®

Jim Brandt
Lead Developer
Synacor
40 La Riviere Drive
Suite 300
Buffalo, NY 14202
(716) 362-3496 (Phone)
716 - 332 – 0081 (Fax)
jbrandt@synacor.com
and
Jim Turner
Former VP,
Product Management
Synacor

Principles for a Robust Online Video Entitlement System

Video Market Trends

Without question, the popularity of online video of all types (including professional and user-generated content) is growing at a rapid rate. Nielsen's Online VideoCensus for May '09 indicates that online video consumption has ramped-up considerably over the past year as reflected in both the total number of US viewers (now ~134M, up 13%) and video streams (~10B per month, up 35%). Additionally, the average time spent viewing video online has jumped 49% to 189 minutes per month and according to the latest Pew Internet and American Life survey, 62% of Internet users view video online, up from 33% just three years ago.

Along with this overall growth, viewers are now consuming full-length, professionally produced programs online more than ever before. The Pew study reports 35% of Internet users have watched a TV show or movie online. Hulu, with its wide collection of current, full-length TV episodes from ABC, Fox and NBC along with a limited selection of feature films, has risen to become the No. 2-ranked video site (trailing only YouTube's break-away UGC popularity). These metrics clearly indicate strong demand and rapidly changing behavior patterns toward online video consumption.

Strong online growth figures notwithstanding, it's worth pausing to consider the relative magnitude of the emerging online video market as compared to traditional broadcast and subscription-based TV services. Concurrent with strong growth in online viewing, Nielsen also reports that Americans now consume more than 153 hours of traditional TV viewing per month, supporting a thriving $80B US television advertising market. As such, 98% of video viewing still takes place in front of the TV.

One reason for this disparity may be the fact that (legitimate) online video consumption has thus far excluded a substantial category of premium content – full-length programs from cable networks as well as live news and sports programming – due to exclusive distribution arrangements and lucrative associated subscription revenues enjoyed by cable programmers and operators.

Consumer demand and cross-platform technology advances (including broadband proliferation, advanced codecs, declining distribution costs and maturity of IP platform services) have made it clear that this content will find its way online, satisfying viewers' desires to watch their favorite cable programs on their own schedule on a device and media form-factor that is most convenient. Simultaneously, programmers and operators alike seek to manage consumption and to promote greater audience loyalty to their programs while discouraging unauthorized distribution through piracy (either via BitTorrent or black-market DVD sales).

Motivation for Entitlement-based Online Services

To grant programmers and operators access to latent consumer demand for their products online without eroding existing revenue streams, will require a system that simultaneously protects and enhances the existing distribution agreements that make up the foundation of the cable industry. This system must preserve control over programmers' content and substantial revenue streams resulting from subscription fees consumers pay to access the programming.

By tying access to premium online video content to existing subscription offerings, operators add value to those products (thus reducing subscriber churn and encouraging up-sell), while simultaneously positioning themselves proactively in the emerging online video market and reinforcing their aggregation and distribution roles to consumers. Additionally, as consumer viewing habits continue to include Web components, supplemental revenue streams will emerge through online video and display advertising.

While ubiquitous online access to premium content may at first glance appear to by-pass and marginalize existing service provider revenues (thus motivating a 'wait-and-see' approach), two points argue strongly in favor of a strategy of MSOs taking a leadership position in this space.

First, if trends in digital music and print media are to be taken as an indication of future video consumption trends, there is strong precedent that consumption will increasingly flow online, regardless. MSOs may either adopt proactive strategies which leverage their incumbent relationships with programmers, advertisers and technology vendors or risk 'playing defense' as third-parties (e.g., Microsoft, Google, Facebook) work aggressively to capture their share of television advertising and subscription market as it migrates online.

Further, while the move online will undoubtedly provide increased convenience and choice to consumers, there will still be a valuable role to play in aggregating, curating and promoting quality content in this new media. Though the 'mechanics' of online video and metadata management will diverge substantially from traditional HFC broadcast and VOD models, MSOs are uniquely positioned (via direct billing relationships with subscribers, leverage with programmers, broadband network leadership, and strong video provider branding) to influence online video consumption patterns.

The Mechanics of Entitlement

Online subscriber *authentication* and *authorization* of *entitled* content represents the first-step in implementing a robust online strategy not only within the context of the MSO's own video portal but also through integration and co-branding with programmer's sites and embeddable video players supporting syndication to third-party sites.

Regardless of the depth, sophistication and convenience of any particular portal, a larger monetizable market exists for content which is accessible across the Internet – within the context of complementary sites and services. The viral distribution capabilities of social networks speak to this point.

So long as access to premium online video is coupled to robust authentication, authorization and analytics mechanisms which reinforce subscription payments, MSOs will be well positioned to encourage wide distribution and consumption growth across the Internet without ceding control or cannibalizing existing subscription revenues. In other words, if premium online video sites are able to confirm that a user is paying to receive the programs and networks on their TV service, rights should be extended to viewing ”anywhere and everywhere” online as well on TV.

“Authentication” in this context entails securely identifying a user on the Web, typically via username/password and/or by IP/MAC address. “Authorization” refers to the process of mapping an authenticated user to a set of consumption policies. Within the context of an online video “entitlement” system, these policies will consist of rules that define access rights for particular pieces of content based on subscription package offerings.

The process of entitlement becomes, at its simplest, a request to an MSO subscriber database by a Website asking if the user who is visiting the site should be allowed to access certain content or pages on that site. If the response is “yes,” the user is allowed to view the content; if the answer is “no,” he or she could be given options to re-authenticate or subscribe to the services (up-sell).

While the basic authentication and authorization transactions outlined above may seem trivial, several deployment challenges arise as you move from proof-of-concept on a small scale to nationwide deployment across dozens of programmer libraries and operator networks. Each operator (and in many cases each division within a larger operator) has its own way of packaging and identifying channels within subscription tiers. Similarly, each operator maintains its own subscriber database with associated authentication mechanisms – typically used for single sign-on (SSO) across multiple Web offerings.

In the absence of a common technical solution for securely accessing these databases, normalizing content naming schemes, and delivering authorization responses to third-party partners (such as programmer direct-to-consumer sites), the industry will be burdened with an N^2 *problem* of separately integrating each operator with each programmer and third-party site.

Even more importantly, any proposed system will be successful only if it satisfies the user by proving simple and consistent to use. When all these considerations

are taken into account, the need for a simple, scalable, secure, and unified system for entitlement is clear.

Principles of Proposed Solution

Within the past decade, the cable industry has garnered substantial experience in working with third-party vendors to provide authentication and entitlement systems for Web and video content providers. The experience and knowledge that has been gained by the industry at large will be necessary to create and operate a system of this complexity while balancing the needs of the viewer, programmer and operator.

It is important to note that to date, authentication has been focused on providing access to services which are unique to that customer (e.g.. e-mail), and generally are not location specific. If someone were to obtain a customer's username and password, it would compromise that one person's information, but generally would not affect other customers.

This approach differs from the model to which cable system operators have become accustomed. In the cable world, video authentication historically has been explicitly tied to a device like a set-top unit, and has not granted rights or access to an individual user. This new entitlement world has at its core a shift from device-centric access to individual access entitlement.

With that in mind, below are a collection of principles that should be incorporated into the emerging online video authentication and entitlement system.

1. **Invest in robust user authentication and identity management.**

   It is tempting to look for quick and simple ways to provide authentication for users – some have suggested simple IP/MAC address checks, for example. However, these approaches expose a number of limitations and vulnerabilities.

   From a business perspective, requiring that a consumer purchase both video and broadband services from the same provider may provide compelling incentives for the up-sell of bundled services. However, if adopted, this strategy would be better implemented as a configurable policy of an entitlement rules-engine rather than as a fundamental assumption required to bootstrap the authentication process.

   Further, the proliferation and popularity of mobile broadband and WiFi Internet access has created an expectation for corresponding mobility in online media services, as well. Imagine, for example, the market impact that would result if Apple's iTunes music service were only accessible from behind a particular telco's DSL modem.

Rather than coupling user authentication and identity management to a particular hardware device or access network, a solution should be provided which securely prompts an individual for authentication credentials and verifies them either directly against the operator's backend or a secure, managed local cache.

Fortunately, most MSOs have already invested in robust identity management infrastructure in support of existing Web, e-mail and bundled premium content offerings. These systems are typically based on LDAP/X.500 or RDBMS backends, with interfaces exposed and managed via Web Services.

2. **Provide a clear distinction between authentication and authorization functions.**

   Whereas authentication is focused specifically upon identifying a particular user, authorization involves retrieving a set of content policies and mapping them to access requests. As agility in provisioning, enforcing and updating these policies will be a key competitive consideration for the operator, a system should be established which provides an open framework for entering, storing and extending entitlement policy as a set of rules.

   Fundamental to this process in the context of online video is the ability to retrieve and normalize various service offerings, packages and tiers, thus providing a common schema across programmers and operators, alike.

   Finally, a high-performance entitlement engine should be implemented which services authentication/authorization requests, applies appropriate rules, issues responses and enables associated management and monitoring capabilities.

3. **Insist upon open-standards and avoid proprietary, closed systems.**

   Fortunately, a number of open protocols and standards have been developed over the past ten years that are directly applicable to the authentication/authorization problem. These include:

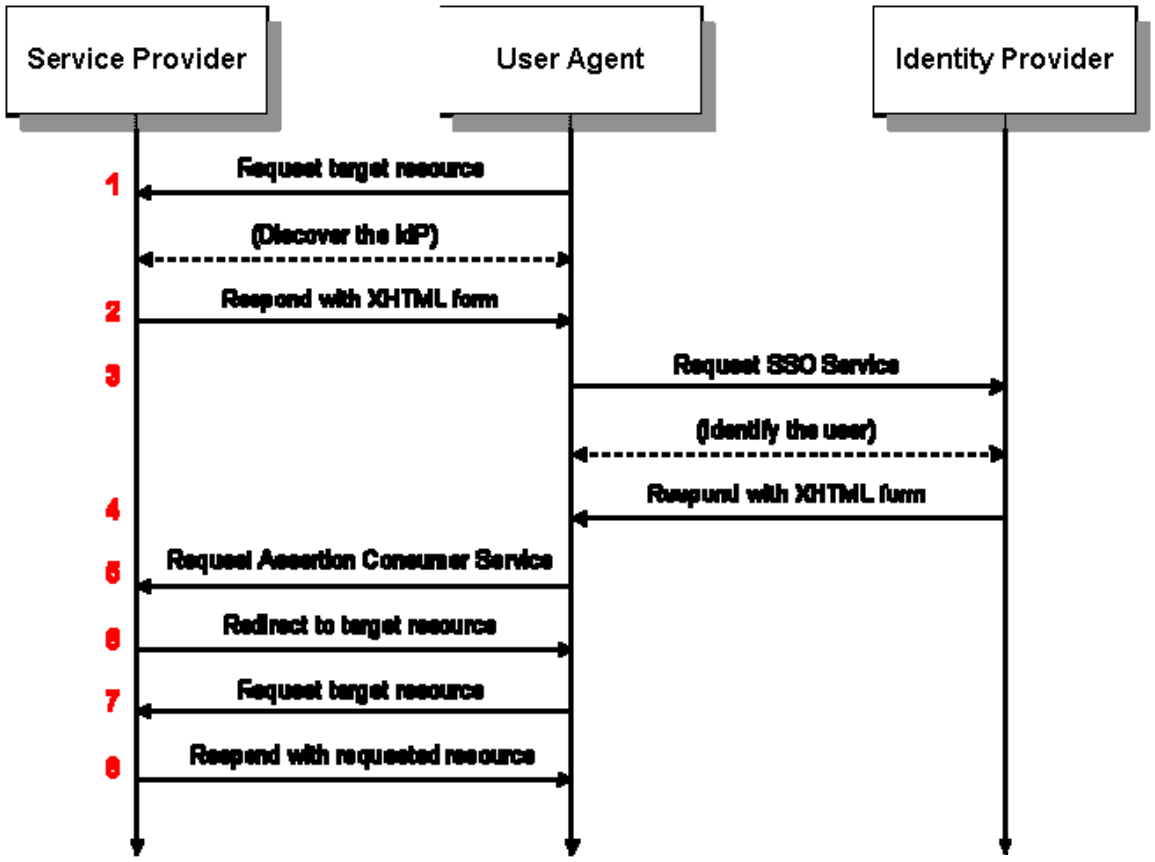
   - *HTTP*: hypertext transport, providing basic plumbing for the Web
   - *SOAP*: simple object access, with messaging semantics
   - *SAML*: security assertions, with bindings to both SOAP and HTTP
   - *XML*: extensible metadata, providing a common data format across systems
   - *XML Schema*: mechanism for specifying structure and content of documents

- *XML Signature*: mechanism used to establish sender identity
- *XML Encryption*: mechanism used to obfuscate and protect document content
- *RESTful Web Services*: lightweight approach B2B APIs via HTTP/XML

Of the technologies outlined above, SAML, the Security Assertion Markup Language, is particularly applicable and central to the problem of providing a robust, secure and scalable identity management and content entitlement framework spanning multiple parties and roles.

While originally developed by the OASIS Security Services Technology Committee as a solution to the SSO problem, SAML defines a concept of *assertions*, consisting of a secure, open mechanism for specifying and communicating entitlement rights.

Key logical roles in the SAML model include: the consumer's User Agent (Web browser), a Service Provider (Website offering premium content) and an authoritative Identity Provider (offering authentication and authorization of entitled content based on programmer and operator business policies). These roles and associated message sequencing are outlined in the diagram that follows.



Keep in mind that much of the 'heavy lifting' associated with deploying a SAML-based entitlement system involves integrating this infrastructure with existing subscriber and product databases and implementing a rules-management and execution engine to service authorization requests.

4. **Balance users' ease-of-access to content with robust policy management to reinforce subscription value.**

   Two key principles -- usability and robustness -- define the core of the issue. If a user is required to explicitly sign-in every time they attempt to access entitled content, or to visit their operators' site to get permission to see content on others' sites, or if the entitlement system is so easily hacked that content rights can be freely passed around, the system is doomed to fail. Therefore, to facilitate widespread adoption and high-volume usage while enforcing subscription policies, the system should have a number of characteristics:

   - The system should consist of a "network" of sites that share a common interface and mechanism for identifying and authenticating users

   - It should allow the user to become authenticated (i.e., enter their operators' subscription credentials) just once and at any site or point they first attempt to use the system to gain access.

   - When the user is initially authenticated, the system should use whatever heuristics are available to make the process simple for the user and at the same time secure. For example, the system should try to detect the broadband service and geo-location of a user and offer an intelligent suggestion of which operator the user has for TV service.

   - The authorization process should be implemented based on configurable business rules. For example, the operator may allow the subscriber to authorize three devices (PC, mobile, etc) upon which they can receive entitled content. This may include a home PC, a laptop, and perhaps allow temporary authorizations from work or other locations.

   - To protect these authorizations, the system should incorporate anti-fraud techniques and detection. Examples of anti-fraud techniques included limitations based on concurrent access, frequency of access, and IP variations.

- Parental controls may also be integrated into the entitlement rules engine to enforce additional, user-managed policies.

5. **Content management, discovery and delivery services should be separable from user authentication and content authorization functions.**

   Allowing for a clean demarcation between content and the management, presentation and functions of metadata does more than simply respect system architectural *modularity* and *separation-of-concerns* best-practices. It also allows programmers, operators and authorized third-parties flexibility in striking content deals and tweaking product offerings.

   In some cases, operators may choose to ingest, manage, deliver and track content from programmers, thus providing an end-to-end video portal solution. In other cases, programmers may prefer to manage and deliver their own content, via embeddable, syndicated video players. Finally, achieving maximal marketing and distribution reach in the current Internet market necessitates a third-party syndication strategy for social networking sites, personal blogs, fan pages, etc.

   The authorization process at its simplest is a “yes” or “no” response to the question asked by a participating Website about whether this user is allowed to see certain content. How that permission is used is determined by the inquiring Website and the business rules agreed upon by the operators and programmers.

   For example, a positive entitlement assertion might add more content links to an integrated video player page. Alternatively, it may enable a specific video playback technology for high-quality playback instead of a lower-resolution short clip player. In another approach, entire sections of a Website may be hidden to non-entitled users in a walled-garden model.

   So long as the entitlement framework is separable from other content management functions, each of these models may easily be supported via one, unified, reusable solution.

6. **Allow maximum flexibility in the definition and application of entitlement rules.**

   Each operator and programmer will have a set of business rules defined by the contractual agreement they have created, and these rules will be codified and enforced by the entitlement system. The domain of these rules may extend to multiple, complementary dimensions beyond product packaging or service tier validation. Examples may include:

- Geo-location restrictions
- Temporal windowing
- Video quality levels
- Website white/black listing
- Device-specific policies (iPhone, Android, Boxee, PS3)
- Access network policies (WiFi, 3G, MAC/IP)

As previously noted, these rules will also incorporate definitions of how each operator's tiers and packages are translated into specific network or content entitlements.

The entitlement system must provide a mechanism to define, edit, store, review, execute and monitor these business rules. It should also include the ability to experiment and make changes to rules on a permanent or temporary basis; for example, to allow a "free online video weekend" trial to all users.

7. **Provide attribution and branding for both the programmer and operator.**

   Regardless of where and how entitled content is viewed, an important aspect of reinforcing and promoting the fundamental business relationship between programmers and operators includes ensuring that proper attribution and branding are provided to the user. This should include appropriate programmer branding on the operator's site and/or syndicated player, and vice versa.

8. **Respect and protect the privacy policies of all parties.**

   The authentication process must provide appropriate security and privacy protections, specifically preventing *personally identifiable information* (PII) from being passed to unauthorized parties. The framework proposed here achieves this by leveraging mature Web security technologies including SSL/TLS transport security for HTTP, XML Signatures verifying a message originator, and XML Encryption ensuring message integrity and privacy. Additionally, backend and entitlement administration interfaces must be protected via strong user authentication and group management policies.

   Where business rules and privacy policies allow, the authentication process may also provide information to personalize or customize the website user's experience. SAML supports this via extensible *attribute statements*.

9. **Streamline the entitlement integration process to encourage adoption.**

To encourage wide adoption of the framework, the integration of the front end mechanism that requests authentication when required and performs the necessary authorization requests must be simple and easy to implement. This is best accomplished using open and standardized protocols and frameworks like SAML as discussed above. Furthermore, the approach should allow for flexibility within the context of those standards and permit a variety of technical implementations that conform to the standards and pass the defined data and requests in a uniform manner.

In support of this open standard approach, it is critical to develop a body of documentation and support materials that are readily accessible and can grow and develop by the community of users implementing the system.

10. **Provide accurate reporting and usage metrics to both programmers and operators.**

Core to the business and usage development of the entitlement system as well as to driving consumer usage and acceptance is the availability of metrics and analytics to the participants in the system.

Since the authentication, authorization, and entitlement process does not provide the flow of content that is consumed, the metrics supporting specific asset consumption, advertising, etc. will need to be tracked and reporting through separate systems. However, the entitlement system should provide key metrics around the access and usage of the various inherent mechanisms. These would include:

- Number of authentication requests by source; operator; successful completions; failed completions; redirects to up-sell; or informational pages, etc.
- Number of authorization requests by source; operator; session lengths; number of sites per session; repeat requests; authorization failures, etc.
- Correlated data such as geographic mapping of requests; number of accesses per household, etc.

Conclusion

The demand for consumption of full length entitled content is high and continues to grow. Without a robust entitlement system in place, both programmers and operators face lost opportunity and potential long term impact to their businesses as users find other ways to seek out and consume their desired programming.

The ultimate goal of this or any similar system is to drive consumer usage and consumption of content, which will build additional engagement for the programmers' content and new value for the operators' subscription services. The principles presented here leverage the industry's experience in providing authenticated content to online users and attempt to lay a foundation for the creation of an open, secure, and consumer-friendly entitlement system.

While it might be tempting to some to move slowly, exploding consumer demand and the opportunity to direct consumer usage in a manner that supports both the programmers' and operators' goals calls for focused and determined efforts to implement a robust entitlement system quickly.