

Enabling the New World of Pay-TV

The Service Provider's Guide to
3-Dimensional Content Security



Enabling the New World of Pay-TV

The Service Provider's Guide to 3-Dimensional Content Security

Rising consumer demand for access to pay-TV on an “anywhere, anytime” basis is challenging service providers to adopt unified content security strategies that will support the seamless 3-screen experience customers are looking for.

This means service providers must not only be able to securely deliver content to multiple devices; they need to be able to support all types of protection that content owners require across different types of networks. Simply put, it's a matter of finding a platform that delivers protection to any screen over any network to meet any threat.

Such a 3-Dimensional Content Security solution must be able to draw from a range of security techniques including encryption, conditional access (CA), digital rights management (DRM), forensic watermarking and other protection schemes. The platform must be able to dynamically apply the appropriate layers of security to each individual content stream no matter what network and device any given customer might be using.

There are many functional details within each of these dimensions that must be considered as pay-TV operators seek to implement an all-encompassing security solution. The solution must not only be 3-dimensional in scope; it must be responsive to all requirements in each dimension. Service providers need to understand the content security requirements from a network perspective, device perspective and content owner perspective to ensure the value of their network today and in the future.

Undeniable Demand

Service providers have long understood they would eventually need to provide customers ubiquitous three-screen access to content. But the complexities of providing content protection that meets content owners' requirements across all networks and devices dampened enthusiasm for pursuing converged media services strategies – especially when there was uncertainty about how important such services would be to consumers.

Now, however, the right content security solution must be found, because evidence from all corners of the globe confirms that consumers want this kind of service. Even at this stage, when 3-screen access can be a cumbersome and costly undertaking for individual users, ever more people are using the Internet and mobile 3G networks to access content that was once available only via the TV or on music CDs.

For example, a study issued in August 2007 by online ad network Advertising.com found that 62 percent of American consumers now watch video of some kind online. According to the Consumer Internet Barometer published in October 2007 by The Conference Board and TNS, 16 percent of U.S. Internet households watch TV broadcasts online, more than double the number registered six months earlier. On the mobile side, researcher iSuppli Corp. in a study reported in July 2007 predicted

3-Dimensional Content Security:

- Multiple Networks
- Multiple Screens
- Multiple Layers of Protection

the market for premium mobile content would more than double in the next four years, going from about \$20 billion in 2007 to over \$44 billion in 2011.

The desire for content portability within the home has been widely documented as well. In November 2007, IMS Research projected that more than 36 million IP-enabled video devices that aren't set-tops, including game consoles, IP-to-TV digital media adapters, Media Center PCs and proprietary systems like the SlingBox SlingCatcher, would ship worldwide in 2007. By 2012 over 200 million such devices will ship worldwide, according to the study.

These are trends no wireline or cable service provider can afford to ignore. Service convergence has become a market-driven imperative representing an upside opportunity for service providers to expand revenues and differentiate service offerings. And there is a downside risk as well associated with consumers going to other sources that offer them ready access to content wherever they happen to be.

Fortunately, it's now possible to meet the security requirements that are essential to delivering a consumer-friendly cross-platform service. The key to finding the right solution is to make sure all the bases are covered in the network, device and protection dimensions.

Network Dimension: The IP Standards-Based Imperative

Several trends point to the challenges that must be met in the network dimension by a unified content security system:

- Network operators of every description are seeking to extend the reach of their services by using a variety of networks beyond their legacy infrastructures.
- Users accessing those services do not want to go through separate sign-up and authentication processes whenever they're on a different network.
- As service providers seek to extend market reach by using multiple networks, hardware-based security works against the goal of ubiquitous reach by imposing limits on the variety of devices that can be used to access content.
- Service providers are expanding their business models to support wholesale services for third parties that want to deliver content over their networks, which means a service provider's core content security solution must be able to co-exist with third-party security solutions.

These developments indicate the need for a unified content security system based on IP core technology that operates in software mode without requiring use of dedicated hardware.

There's no tougher testing environment for ensuring robust security than the Internet, where every solution must run a gauntlet of professional and underground hackers on a continuous basis. That's why software-based IP security technologies have emerged as the gold standard for securing everything from Web-based banking and financial transactions to high-value video in broadband and IPTV service applications.

IP functionalities support the PKI (Public Key Infrastructure) mode of encryption to provide a high standard of security that eliminates the need for smart cards. Leveraging the inherent two-way nature of IP connectivity, this type of protection can deliver an industrial-strength content security system that addresses all the requirements essential to delivering cross-platform security cost effectively.

Standards Drive for IP Unification:

- *Common Technologies across Networks*
- *Streamlining User Experience*
- *Leverage Internet Proven Security*

An IP-based platform eliminates the need for multiple CA or encryption vendors. Reliance on legacy solutions not only imposes burdensome inefficiencies on service providers, it creates a less-than-optimal experience for users who must sign in and be authenticated every time they move into a different security environment. Moreover, a software-based IP content security solution eliminates the need for smart cards or embedded smart card microprocessors. In a retail distribution environment for network devices, only a software-based solution that's at least as hacker proof as any hardware-based system can overcome the limitations imposed by having to insert smart cards into every device that an operator wants to authorize for receipt of protected content.

Equally important, a software-based IP content security solution provides a means for maintaining high-level security over time through downloadable updates to devices. When compared to smart cards, this presents a much more responsive and less costly mechanism for addressing security breaches or new threats. And such a protection system lowers the costs of set-tops and other devices by eliminating the need for CA-specific hardware. In order to maximize this benefit, software security should be designed to employ very "thin" client software on all devices to limit the impact on processor and memory resources.

The central role of IP extends well beyond content security. The benefits of an IP-centric delivery system are increasingly seen in the newest international standards for content delivery. Pivotal organizations such as the Digital Video Broadcast Project (DVB) have baked into their most recent work standardized means of delivering and securing content using IP protocols across diverse network types, merging legacy MPEG-2 delivery with IP infrastructures and IP centric clients. And DVB has provided a very flexible series of Simulcrypt standards to accommodate co-existence of multiple stream types and security platforms within a given deployment. An example would be a pay-TV operator with a legacy encryption system is implementing a cross-platform security solution for a converged service.

Cable operators that want to extend their network reach over DSL and mobile infrastructures can implement a single solution that is competitive with any IP-based TV delivery system. Satellite service providers, seeking to enable broadband, video-on-demand and mobile service components through tie-ins with terrestrial networks can now use a single system to realize these ambitions. And telephone companies using a combination of MPEG-2 RF-based and IPTV-based platforms can apply a single content protection solution as well.



Device Dimension: Securing Multiple Screens

To enable the seamless experience that consumers expect, service providers must ensure any cross-platform security solution they choose can be applied to the largest possible population of set-tops, PC, handhelds and other devices. The more devices any given content security system can support, the more compelling the user experience can become.

Multi-Device Solutions Must:

- Have Broad CE Support
- Allow Multi-Network Connectivity
- Secure Experiences Beyond the TV

A software-based content security approach is essential to providing protection across whatever types of device consumers use to view content. Once this is understood, there is much more to consider to be sure that the reach, flexibility and robustness of the protection regimes are appropriate. The most appropriate solutions are likely to require only lightweight integration of content security between set-tops, games consoles and mobile architectures, yet have sufficient ability to scale.

A software-based system uses DRM techniques to set different business rules depending on what the subscriber has paid for, what use policies have been defined by content providers, the type of device used and other parameters. Service providers must make the subscriber experience as seamless as possible with no repetitive requirements to sign in or take other annoying steps to view content on a particular device. Therefore any given DRM system must be integrated with the application layer software in the device.

Service providers should also make sure the content security platform can protect a device that moves into different networking or non-networking environments. For example, if a mobile user is viewing content on a handheld through a Wi-Fi link in the home and wants to continue viewing as he or she moves into the mobile service domain, the content protection must flow seamlessly from one environment to the next. Or, if a user who is accessing TV content from the service provider via a link from the set-top to a laptop wants to download that content for continued viewing on a trip, the protection system must be sufficiently flexible and secure to support that option.

Tied to the last use case, another important point for service providers to recognize in evaluating solutions is whether the platform provides adequate protection to the PC, which is an especially challenging requirement that few solutions fully address. Now that the PC has become a widely-used platform for viewing entertainment content, service providers don't want to lose potential viewers of TV programming just because they happen to be using their PCs. But to win licensing support from suppliers of high-value content for a TV-to-PC service extension, protection must be more assured than with today's web protection schemes.



This is especially important if the content is decrypted for viewing on the PC the way it is on the TV, it can be stored, transferred and viewed in the clear at any time after the initial decryption. The best way to prevent this from happening is to ensure that the content is always maintained in a protected form and that decryption keys are delivered with each viewing. An appropriate regime of business rules would dictate if the user is specifically authorized to store the content outside of the service provider network – in place shifted form or offline.

Security Dimension: Multiple Layers of Protection as a Business Enabler

The need to support portability for high-value content is one of several requirements that call for additional security capabilities beyond encryption to address multiple types of threats. Service providers must be able to apply these various layers of content security on an as-needed basis, depending on type of content and content owner requirements, and evolve the layers of protection as business needs and types of threat evolve. Pay-TV content protection solutions have evolved from analog scrambling to digital encryption, from analog copy protection to High-bandwidth Digital Content Protection (HDCP), and are continuing to generate new technologies and techniques to address the challenges of piracy.

Protection Layers Must Include:

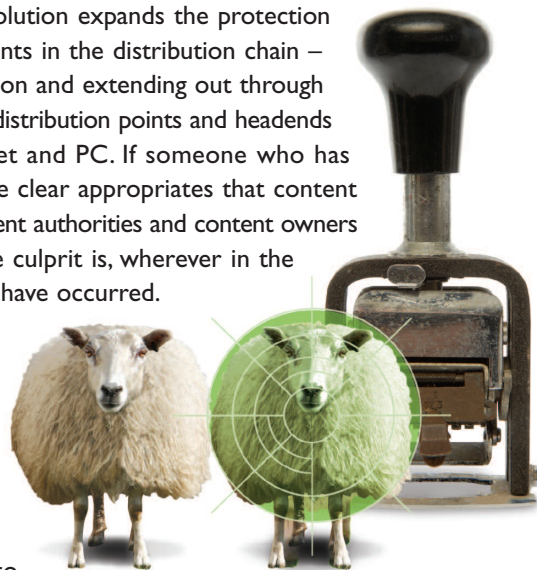
- Encryption/DRM
- Forensic Watermarking
- Clone Detection

One crucial additional protection layer entails use of user-specific forensic watermarking technology to help pinpoint the origin of pirated content. Forensic watermarking is an invisible serialization code embedded into content at various points in the distribution stream to identify the last point at which a pirated piece of content was decrypted. This has high appeal as a defense against piracy because, even if an encryption code is broken or an “in-the-clear” copy of a movie has been obtained and distributed illegally, the indelible, invisible watermark code can be used to identify where the theft occurred.

A comprehensive watermarking solution expands the protection perimeter by encompassing all points in the distribution chain – starting with the production location and extending out through post-production, aggregation, core distribution points and headends all the way to the set-top, handset and PC. If someone who has access to protected content in the clear appropriates that content for unauthorized use, law enforcement authorities and content owners need to be able to know who the culprit is, wherever in the distribution chain the breach may have occurred.

For service providers to win the support of motion picture studios and broadcasters for distribution of high-value assets, such as early release movies, a watermark must be inserted at the point of consumption in order to

trace piracy to the specific individual and not just the pay-TV operator. Content owners are assured of protection that extends beyond the digital network with solid legal evidence, and it serves as a deterrent for illegal behavior.



Beyond watermarking security, there's also a need to protect against a common type of service theft in pay TV services known as "cloning." Illegal devices designed to emulate brand models provide a way for people to access content without paying for it, leading to subscription fee losses in the tens of millions of dollars annually.

To overcome such tactics, the content security system must be able to detect even the most cleverly designed client device clones. It must be able to read regularly generated data from each device to detect operational differences between real and cloned devices, such as differences in channel viewing patterns or differences in the timing of requests for keys. And it must ensure the device is connected to the correct physical network at the appropriate location.

Conclusion

At a time when many network operators still believe a multi-network, multi-device content distribution strategy requires deployment of different protection systems for each network and device environment, a 3-Dimensional Content Security solution offers significant benefits for a true competitive edge.

For the first time, network service providers can proceed with service models that fully address both the ease-of-use and accessibility requirements of customers and the protection requirements of content suppliers across all platforms. Putting a 3-Dimensional Content Security solution to work, service providers can introduce new revenue-generating business models and assure the loyalty of customers in a tumultuous service environment. And they can do it cost effectively, knowing that no matter what security threats might emerge they can address all situations from a single software-based system that extends the reach of security updates to every device used by their customers.

As the IP revolution continues to sweep the digital entertainment market, there's no better way for service providers to prepare for future opportunities and all the challenges that come with meeting the needs of customers and content providers alike.