

The Advantages of Software-Based Content Security in a Multi-Device, Multi-Service Pay-TV World

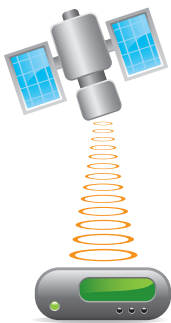


The Advantages of Software-Based Content Security in a Multi-Device, Multi-Service Pay-TV World

Executive Summary

Video has evolved from a simple service watched on conventional television to a complex offering of services watched “anything, anywhere, anytime.” Hardware-based security solutions, or smart cards, were developed in a period when video was watched exclusively on television sets, using set-top boxes. Today, however, video is increasingly watched on PCs and mobile devices, as well as televisions, and service providers need a content security solution that can adapt to support all of these platforms.

Software-based security solutions have emerged as a compelling option that offers the flexibility to support set-tops, PCs and mobile devices. While hardware-based solutions are suitable for set-tops, they are impractical for PCs and inapplicable to the diverse range of mobile devices. In the event that the security system is compromised, hardware-based security requires the distribution of new hardware tokens to subscribers, an expensive and time-consuming process, whereas new software can be routinely updated to preempt security challenges. Software-based security has become the choice of the vast majority of IPTV deployments, representing the new wave of pay-TV service providers. For these reasons, software-based security should be the first choice for the evolving multi-device, multi-service, converged service world.



Cable set-tops already have extensive two-way connections and satellite operators are adding Internet connection to set-tops for video-on-demand and interactive services

The Evolution to Multi-Device, Multi-Service, Converged Video

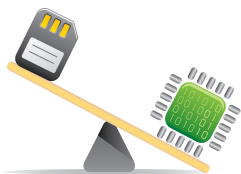
Until fairly recently, “video” meant one thing: TV received terrestrially from over-the-air broadcasters, or via cable or satellite. Pay-TV services, delivered via cable or satellite, relied on set-tops, which tuned in the appropriate channels, converted the signals to the right frequency for television receivers, and (perhaps most importantly) provided endpoint security for the video signals. This endpoint security, called conditional access (CA), tried to ensure that only those subscribers who were entitled to receive the video content could actually view it.

Hardware-based security systems excelled in this environment, since hardware (the set-top) was required in order to watch pay content. Satellite systems introduced an additional constraint in that the transmission system was inherently one-way - from

the satellite to the receiver. Satellite service providers needed a robust security solution that did not depend on a physical connection between the network and set-tops, which was well-suited for smart card-based systems. Set-tops were useless without a valid smart card, and in the worst case, if the entire security system was compromised, the smart cards had to be replaced by subscribers in the field.

Jump forward to today, however, and the entire video environment has changed. Cable and satellite service providers still use set-tops of course, but those boxes have far more intelligence and much better connectivity than those of the past. Cable set-tops now have extensive two-way connections, and satellite operators are adding Internet connections to their set-tops in order to offer Video-on-Demand and interactive services. And, IPTV services, usually offered by telcos, have entered markets around the world and leverage IP set-tops that inherently have high-speed two-way connectivity.

These set-tops can do much more than their predecessors. Their processing power (for video decryption and decompression, as well as for displaying electronic program guides and running sophisticated interactive applications) rivals that of personal computers. They can do in software what used to require dedicated hardware, and it is that power that shifts the balance in favor of software-based security for set-tops.



New generation set-top boxes now use software to perform advanced functions, which used to require dedicated hardware. This processing power has shifted the balance in favor of software-based content security.

Video is delivered to personal computers in numbers that were unimaginable only a few years ago. A survey by Integrated Media Measurement released in July 2008 found that a significant percentage of the audience (as much as 20% in some cases) has completely replaced watching shows on television with watching them online. This shift from television to online viewing has been confirmed by many other studies.

There are service providers whose video service heavily relies upon PCs: IOL Netcom, a service provider focusing on video services delivery in the exploding Indian market, believes that PCs represent the preferred viewing platform for many of their new subscribers. And, of course, there are “over the top” services such as Hulu, Joost, Dailymotion and YouTube, streaming millions of videos to PCs every day.

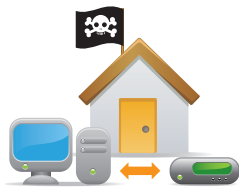
Finally, adoption of mobile video is exploding in markets around the world, most strongly in Asia. A service provider may supply a video channel to set-tops, PCs and

mobile devices simultaneously. Content providers demand that all of these clients provide similar content protection. In a “watch anything, anywhere, anytime” world, service providers are challenged to simultaneously preserve customer convenience and provide adequate security.

Surpassing Hardware-Based Content Security in a Multi-Device, Multi-Service World

As discussed earlier, hardware-based security was developed for a world of set-tops with limited intelligence and little or no two-way connectivity. Hardware-based systems use physical tokens, generally smart cards, with built-in microprocessors and many layers of protection to keep their security schemes from being compromised. They can work in a completely standalone mode, needing no communication back to a central server in order to maintain their security. In addition, they do not rely on the intelligence of the host device (the set-top) in order to function—the set-top can be fairly dumb, but robust security can still be maintained.

However, the strengths of hardware-based security have become weaknesses in today’s world. Piracy has become a sophisticated business, where analysis and reverse engineering of removable tokens or cracking their communication with the host CPU has evolved very rapidly. The vast majority of modern set-tops are perfectly capable of handling security functions using a combination of software and security features embedded in their CPUs, so the extra hardware cost required to support physical tokens is not necessary. If the security of a hardware-based system is compromised, all of the tokens have to be revoked and reissued. Operators must launch a program of informing subscribers about the change, educate them as to how to replace their old tokens with new ones, distribute potentially millions of new tokens, and handle the myriad of customer service calls and complaints that will arise as a result of the change. The costs, in terms of money, time and customer satisfaction, are enormous.



Content security must extend from the home to PCs and mobile devices. Hardware-based security is generally impractical for cost, upgradability and customer satisfaction reasons.

Securing video on PCs presents more challenges for hardware-based security. Very few PCs have smart card readers, so implementing security requires either an external smart card reader connected via USB, or a memory stick-like device connected to a USB port (usually called a “dongle”). Neither of these devices are popular with PC users, especially notebook computer users who have to carry them along whenever they travel. Not only are they clumsy, but these devices represent a security risk, in that the flow of data to and from the security device can be intercepted at the USB port.

Similarly, mobile devices are not generally engineered for hardware-based security. Other than the SIM card slots in GSM phones (SIMs are essentially smart cards), there is no way whatsoever to attach an external device to a mobile device for decryption. Hardware devices are not generally a solution, because they will add to costs in an era where every penny counts. So, hardware-based security independent of a mobile operator SIM simply is not a viable solution for mobile applications.

The bottom line is this: It is impossible to deploy a hardware-based solution across a multi-device, multi-service subscriber base. Even if it was technically possible to do so, it is impractical for cost, upgradability and customer satisfaction reasons.

The Basics of Software-Based Content Security

If hardware-based security will not cut it in a multi-device, multi-service environment, what will? The solution is software-based security. A software-based security system takes advantage of the intelligence of the client and high-speed two-way communications to provide a high level of security. Here is how it works:

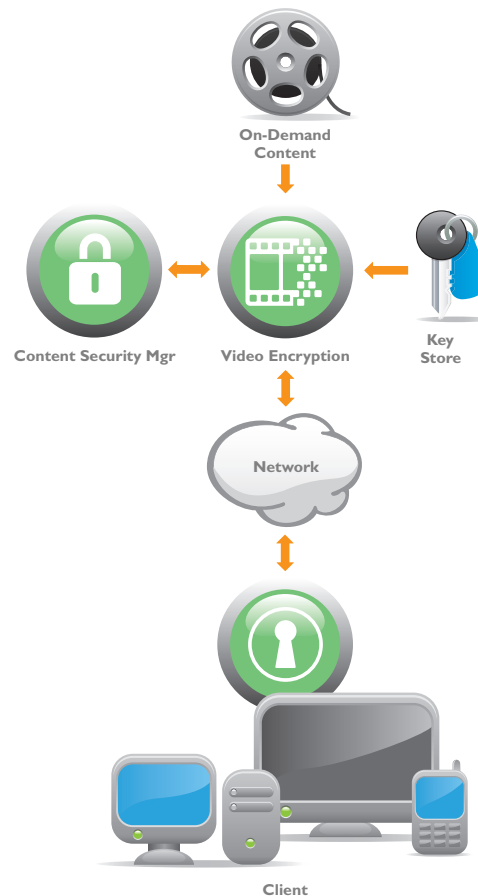


Figure 1: Basic Software-based Content Security Architecture for Video-on-Demand Services

- Digital content (video and audio) is encrypted at the head-end and transmitted to a client, which can be a set-top, PC or mobile device. High-level Public Key encryption is used, along with a number of techniques that can be employed, such as AES. By using a publicly-known encryption technique, the security of the system can be tested and verified, and “holes” in the technique can be discovered and closed quickly through standardized mechanisms.
- The client device decrypts the video as a function of the client’s secret key. The client has more than enough processing power and memory to handle the key calculations and decryption.
- The client’s key can be revoked by the server at the head end at any time, if necessary, making it impossible for the client to decrypt the video. No truck rolls are necessary, and the client device cannot be connected to the network in order to receive the content without being subject to revocation messages.



Advantages of software-based security:

- *No hardware changes required for any client device*
- *Devices are secured without intervention from subscriber*
- *Individual services are instantaneously revoked due to a breach*
- *Head-end is able to revoke services if the security system is hacked*
- *No complicated or expensive programs in the event of a mass revocation*

Why Software-Based Security is Ideal for Today’s Video Services Environment

The above is a very brief description of what is, obviously, a far more complex process. However, from the subscriber’s point of view that complexity is completely invisible. That is one of the reasons why software-based security is the right solution for today’s video services environment. Consider these points:

- No hardware changes are required to set-tops, PCs or mobile devices in order to implement software-based security. In fact, many set-tops that were built to support hardware-based security can also support software-based security.
- Individual clients can be secured without user intervention. The software security client can be installed at the factory, in the service provider’s warehouse, at retail locations, or can even be downloaded when the subscriber first connects the device to the network. In every case, the subscriber does not need to know, or care, about the kind of security being implemented.

- Individual clients can be revoked instantaneously. As soon as the head-end is either instructed to change or cut off service to a client, or detects that security on a client has been compromised (through identifying a cloned client), that client's security can be revoked and access to the content terminated. The user cannot bypass security through a hardware hack.
- Should the security system be challenged, or even as a routine pre-emptive measure, the head-end can revoke all of the clients and issue new client software, electronically and invisibly to users. The client download will usually take only a few seconds, and can be done overnight or whenever the user next logs onto the system.
- With software, in the event of a mass revocation, there is no complicated consumer education program, no physical distribution of smart cards or other physical tokens, and no customer service burden.

The Power of Software-Based Security in a Multi-Device, Multi-Service Environment

There are two key components of security in today's environment: Conditional access (CA), which has been discussed in detail, and digital rights management (DRM). CA determines whether or not a given user or device has access to particular content, and DRM determines what the user or device can do with the content. In a multi-device, multi-service environment, the CA and DRM systems may not necessarily come from the same vendor, but it is essential that they work together, transparently to the end user.

Different devices often use different DRM systems, and the service provider needs to support native DRM systems on the devices that they support. Only software-based security solutions have the ability to interface and harmonize with multiple DRM schemes, which enables a unified approach to all types of devices from a single head-end. For example, a mobile phone with Open Mobile Alliance (OMA) DRM would be authenticated to play specific content in parallel with other software-base secured clients, like the set-top or PC.

The overall impact of this type of approach for a pay-TV operator is to support the widest variety of devices and services in a manner that provides great subscriber transparency.

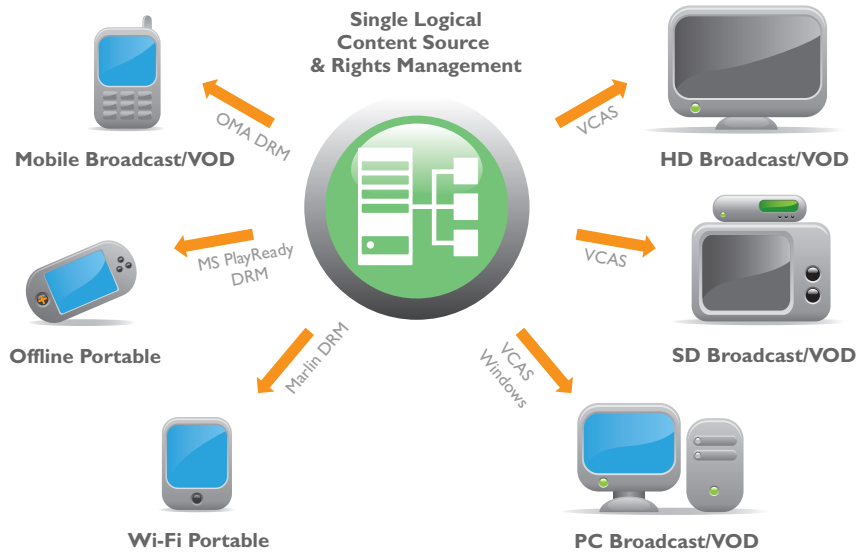


Figure 2: The Challenge of Securing the Multi-Device Environment

The IPTV Industry Solidly Supports Software-Based Security

Obviously, there is room for both hardware- and software-based security solutions in the market; each service provider has to make its own decision on the approach to adopt, based on its own situation and needs. However, the tide of industry support has turned decisively toward software-based solutions. The vast majority of IPTV service providers have adopted software-based security solutions. These operators, that have to support a multi-device, multi-service environment in order to offer triple-play and quadruple-play packages, have gone with software-based security, for all the reasons outlined above.

Some of the largest IPTV operators in Europe, including Belgacom, KPN, Neuf Cegetel and TeliaSonera, have adopted software-based security. Asian service providers using software-based security include KT, NTT and OCN Shanghai Cable. In the U.S., major independent telcos such as Consolidated Communications and Pioneer Telephone have also adopted software-based security. Norilsk in Russia is a user of software-based security, as are many other operators worldwide.

In the past five years, IPTV has grown from a handful of deployments by a few pioneering telcos and ISPs to an established part of the pay-TV landscape with services spanning the globe from Australia to the Ukraine.

-ABI Research, May 2008

*DCAS = Downloadable
Conditional Access System*

*In January 2007, the Federal
Communications Commission
(FCC) ruled that a DCAS
system would satisfy the
separable security mandate
currently required for all U.S.
video delivery set-top boxes.*

Software-Based Content Security is an Advantage in an Era of Emerging Standards

Software-based security systems are the best way to go in an era of emerging security standards. In the cable industry, U.S. operators are committed to move to a Downloadable Conditional Access System, or DCAS, which will provide a software-based security system to replace the hardware-based security integrated into existing cable set-tops. While the key stimulus for this is regulatory, the operators themselves recognize the key commercial and operational advantages of the new landscape and are moving to implementation in parallel with many IP-related upgrades to their delivery systems.

Three worldwide initiatives, the Coral Consortium, the Marlin Development Community and the Open Mobile Alliance, are working to bring interoperability to DRM systems, and have attracted members from industry leaders in both hardware- and software-based security. However, there is an enormous difference as to how these emerging standards will be implemented in the field. Hardware-based security systems will require a mass replacement of security tokens in the field, but software-based systems will require only that new software be downloaded to clients. As the standards evolve, service providers will have the choice of waiting for other opportunities to upgrade hardware-based security systems in the field, or simply pushing updated software to clients. One entails significant costs and time, and the other can be done at low cost and virtually immediately.

Conclusion

Hardware-based security was the right solution when it was developed, but it cannot deal with the new world of set-tops, PCs and mobile devices, all receiving video services from the same service providers. Hardware-based security is expensive and painful to update in the field whenever security is compromised, and it is simply not practical for PCs and mobile phones.

That is why software-based security is the right solution for today. It works transparently with set-tops, PCs and mobile phones. It provides an equal level of security to the best of the hardware solutions. When necessary, it can be updated “on the fly,” in seconds, virtually invisibly to subscribers. For today’s service providers, with their mix of devices and services, software-based security is the answer.



*Software-based security
should be the first choice for
the evolving multi-device,
multi-service, converged
service world.*