Cable TV Digitalization in India
Digital TV Security Considerations in the Post-Smart Card Era

by Steve Christian, VP, Marketing, Verimatrix

The digitalization of cable TV networks in India is one of the largest undertakings of its kind anywhere. Decisions to rollout HD or SD and the type of set-top boxes are accompanied by decisions on what security system to deploy. The security architecture must be capable of supporting the analogue-to-digital transition as well as future delivery to a variety of devices. Most traditional smartcard security systems have now been compromised. Best protection of digital rights and paid-TV service delivery is provided by cardless systems, which have a sophisticated System-on-a-Chip (SOC) with renewable software. Such secure systems ensures robust and impenetrable access control, which can be applied to multiple screens (TV, PC, phone), across multiple networks.

Steve Christian, VP, Marketing, Verimatrix.

Steve Christian has a wealth of experience in the digital media and Internet technology space and is a speaker on media technology and business trends at industry events around the globe. At Verimatrix he is responsible for product strategy, marketing programs and management of brand equity.

Prior to joining Verimatrix, Mr. Christian was VP Marketing at streaming media specialist Nine Systems and has also run his own "virtual VP" technology marketing consultancy, helping the growth of a variety of software, wireless and Internet security ventures. His background includes product and services management at Wind River, ST Microelectronics and Raytheon.

Mr. Christian has a 1st class degree in Physics from the University of Bristol and an MBA from the Open University in the UK.

The ongoing digitalization process of cable TV networks in India is one of the largest undertakings of its kind anywhere. It is presenting operators and technology vendors with challenges and opportunities unheard of in the history of Indian television. Digital TV delivery technologies, while offering opportunities for subscriber and revenue growth for service providers, also present new security challenges in order to comply with programming licensing obligations. This article will look at these challenges and discuss important considerations and solution related to conditional access (CA) and digital rights management (DRM) technologies and their potential impact on cable TV operations and financials.

Content security – The cornerstone of Pay-TV

Pay-TV operators share a fundamental goal: to securely monetize content and – specifically – to protect content and services from unauthorized access, a.k.a. 'piracy.' They have a particular desire to secure their video services – their service revenue streams - from various threats, such as theft of service, smart card piracy, device cloning, etc. As pay-TV moves to digital delivery in India, operators must prepare to address ever-evolving threat models, which now also include content redistribution over the Internet.

While security in analog cable TV systems is primarily focused on preventing theft of service, the threat models are different and more challenging for digital TV services. Therefore, as Indian cable TV operators plan their transition to digital, they must proactively address a unique set of technology and business issues. Ultimately, the objective is to choose a security policy and technology path that minimizes costs without sacrificing the ability to meet evolving service (revenue) requirements in the long run. The choice of security technology is critical to operators' future competitiveness and financial performance.

Digital TV Service considerations

While Indian cable operators plan for the transition from analogue to digital, it is important to consider key service issues such as:

- Choosing appropriate digital video compression formats (MPEG-2 or MPEG-4 with others on the horizon).
- Whether to offer just standard definition (SD) services only or include high definition (HD) quality from the outset.
- Potential of adding hybrid broadcast-IP services, with on-demand video delivered over IP.
- Offering over-the-top (OTT) services over unmanaged networks to off-the-shelf CE devices such as smart phones and tablets.
- Impact of industry standardization initiatives such as MPEG-DASH.

Digital TV Security Considerations

Indian cable operators, whether small or large, should realize that a flexible and

effective digital TV security architecture is the essential enabler of innovative business models to improve the competitive position versus satellite-based broadcasters and pure OTT operators. Choosing the overall security solution is therefore a critical strategic decision. This process should also expand the perspective of the security technology consideration from traditional single network content protection to the broader concept of multi-network revenue security.

There are many pay-TV security factors, not least financial, which need to be considered, such as:

- Initial purchase cost (CAPEX)
- Operational cost (OPEX)
- Cost of an unresolved security breach (ongoing loss of revenue)
- Cost to overcome a security breach (security renewal)
- Set-top box (STB) certification cost and delivery lead time
- Choice and availability of STBs (competition among STB vendors)
- Ability to license premium content (trusted CA/DRM vendor and technology).

Content owners' concerns

Licensing of quality ("premium") content is the cornerstone of a successful pay-TV enterprise. For movie studios and other content providers the threat of large-scale piracy, which could undermine the lifetime revenue potential of their products, is a major concern. Moreover, the commercial stakes for HD content are significantly higher than those of SD.

Content providers focus on enforcing digital rights through a combination of technological and legal processes. Rights owners and pay-TV operators alike expect content security vendors to address the evolving challenges through a set of technologies and tools that encompass complete revenue security, from content creation to storage, delivery and consumption – and beyond the network too!

Therefore, Indian operators planning for the digital transition will benefit from choosing security technology that is well respected and trusted by the content providers. There is only one criterion that truly matters: a successful long term track record of protecting pay-TV deployments around the world.

Digital TV security - A brief history

When digital TV was first introduced in the mid '90s, broadcast networks were "one-way" in nature, i.e. there wasn't any return channel from the STB to the broadcast center. The technology approach was to protect the "pay-TV secrets," such as subscriber entitlements and decryption keys, in a "smart card" provided to the subscriber together with the STB. Operators required a robust security solution that did not depend on a return channel, which was well-suited – at the time – for smart card-based CA systems.

Unfortunately, "hackers" soon compromised all major CA systems, and it is now common practice among legacy CA vendors to recommend replacement of the deployed smart cards every three years or so. This is a financial burden that has become widely accepted by operators although there are now technology alternatives that provide financial advantages too.

Evolution of Set-Top Boxes and security

Today the entire digital TV environment has changed. Cable operators still use set-tops, but today's boxes have far more processing power (for video decryption and decompression, and for displaying electronic program guides and running sophisticated interactive applications), rivaling that of personal computers. They also often come with IP connectivity so operators can add broadband capability and offer Video-on-Demand and interactive services.

In fact, modern set-tops are perfectly capable of accommodating sophisticated client security using a combination of software and hardware features embedded in their CPUs without relying on external smart cards. Cardless security is thus ushering in the post-smart card era.

Cardless security for the post-smartcard era
The cardless security of modern STBs can either consist of a very low-cost box with a highly obfuscated, software-based security module, or a sophisticated System-on-a-Chip (SOC) with embedded security features that enables the most robust and impenetrable pay-TV security possible today. In the latter case, the security module is software-based but resides in a highly secure environment that cannot be penetrated by the tools traditionally used by 'card pirates.'

The secure SOC solution also solves the 'control word sharing' piracy problem. In legacy systems, the Control Word (content descrambling key) is passed "in the clear" between the smart card and the STB video/audio descrambler. Pirates found ways to intercept the key and distribute it to illicit "subscribers" over the Internet. Thus one hacked box is as a "server" for many viewers who effectively steal pay-TV services. In the secure SOC environment, the key is never exposed in the clear outside the secure area, and hence the control word sharing menace is overcome.

Advantages of cardless security

Renewability of security subsystems is a distinct advantage in times of fast changing threats and business opportunities, making cardless security an attractive option. Content security is a proverbial "arms race" against pirates, so the security must be renewable. Software-based security, in combination with state-of-the-art secure SOC technology, offers flexible renewability options allowing operators to stay a step ahead.

Cardless security in combination with secure SOCs combines lower CAPEX and OPEX costs and results in a more favorable Total Cost of Ownership profile. Threats can be countered by over-the-air updates.

Making the right Digital TV security choice

For Indian cable operators it is imperative to choose a security architecture that supports both the immediate analogue-to-digital transition while also laying a sound foundation for the future, which no doubt will include delivery to PCs and Macs, games consoles, smart phones and tablets.

Aspiring operators should strive to implement a CA/DRM system that can ultimately serve as a unified revenue security platform for services destined for multiple screens across multiple networks. They need a solution that can draw on the best of encryption, conditional access, digital rights management and video watermarking techniques. The solution should dynamically apply appropriate security for each service, regardless of delivery network, and irrespective of the type of subscriber device accessing it. In fact, harmonized multi-screen services rights and subscriber management from a unified security head-end is the ultimate objective.

Fortunately, Indian cable operators can now escape traditional CA system single-network limitations without compromising security or adding complications to the consumer's experience. A well-crafted cardless system offers a security level that is essential to new multi-screen service models, otherwise impossible to achieve with legacy systems.

Conclusion

A unified, digital TV security system is a vital ingredient for operators looking to expand their service profiles, to meet contractual and service protection obligations. A single security authority, offering multi-layered protection, allows new business models to emerge and flourish. ●