The upcoming digitalization of cable TV networks in India is one of the largest undertakings of its kind in the world. It presents operators and technology vendors with challenges and opportunities like never before in the history of television in India. Digital TV delivery technologies, while offering opportunities for subscriber and revenue growth, also present new content and revenue security challenges. This article will look at these challenges and discuss some solutions related to conditional access (CA) and digital rights management (DRM).

DIGITAL TV SECURITY – THE CORNERSTONE OF DIGITAL PAY-TV

All pay-TV operators share the fundamental objective 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 – that is, their service revenue streams - from various types of 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.

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

DIGITAL TV SECURITY CONSIDERATIONS

While Indian cable operators consider and plan for the transition from analog to digital, it behooves them to consider in parallel the value brought by digital TV security providers. Related to digital TV security are also considerations such as:

- Choosing MPEG-2 or MPEG-4 video formats.
- Offering standard definition (SD) services only, or including high definition (HD) from the outset.
- Adding hybrid IP-based solutions to managed broadcast networks.
- Adding over-the-top (OTT) IP services over unmanaged networks to off-the-shelf CE devices.

Indian cable TV operators, whether small or large, should realize that a flexible and effective digital TV security architecture can be an essential enabler of innovative business models and improve their competitiveness. The choice of the overall security solution is therefore a critical strategic decision. This consideration also shifts the perspective of the security technology from traditional content protection to the broader concept of 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 unresolved security breach (loss of revenue)
- Cost to overcome a security breach (security renewal)
- STB certification cost and lead time
- Choice and availability of STBs (competition among STB vendors)
- Ability to license premium content (trusted CA/DRM vendor)

CONTENT OWNERS’ CONCERNS

Licensing of quality (“premium”) content is the cornerstone of a successful pay-TV enterprise.

MULTI-NETWORK SECURITY

किये विना एक ऐसी मुद्दा नीति व तकनीकी पंजी का चुनाव करना होगा जो कि कार्य को पूर्व सत्ताम में। मुद्दा कलाकारों का सुनाव महात्म जयपुर के प्रतिद्वंद्वी भविष्य और विलोम पद्धति दोनों के लिए महत्वपूर्ण व मौलिक हो।

डिजिटल टीवी मुद्दा संबंधी बातें

हालाँकि भारतीय केन्द्र ऑपरेटर, एनालॉग से डिजिटल मंडल के लिए विवाद व वोजनांक बना रहे हैं, साथ ही वह उन्हें डिजिटल टीवी गुरुत्व प्रदान करने, कार्य के मापदंड पर परीक्षा पर भी बिवाद करने की वात करता है। डिजिटल टीवी मुद्दा जुड़े कुछ लंग इस तरह भी विवाद कर रहे हैं:

- एपीएसजी2 या एपीएसजी4 वीडियो सार्वजनिक का बुनाव कर।
- सिफर स्टैंडर्ड डिस्कार्ड, (एसडी) ग्राफ हो ओएम किया जाए या प्रारंभ में साइड डिस्कार्ड एएसडी तीन आयोजन किया जाए।
- प्रयोग नेटवर्क के प्रमुख के लिए हाईडिल आईडेआई आयोजन उपयोग किया जाए।
- चयन और उपयोग की बंट करने के लिए अतिक्रमण नेटवर्क के उपर ओवर द टीप (ओवरटी) आईडेआई वेब को अभियोजन किया जाए।

होटल या बड़े महत्वाना भारतीय केन्द्र टीवी ऑपरेटरों के एहसास होना चाहिए कि नये व्यवहार गोट्स और उनकी प्रतिपादकता विभाजन के लिए लोकप्रिय व प्रभावशाली डिजिटल टीवी मुद्दा गंभीर आवश्यक हो मुक्त है। इसलिए स्मार्ट उपयोग की परंपरा महत्वपूर्ण गैरहसिलक निर्णय है। यह विवाद राजनीतिक गुरुत्व के लिए प्रतिपादक मूल्य में गुरुत्व तकनीकी के परिचय की ओर श्रद्धांजलि की वात करता है।

कई पे-टीवी मुद्दा जोता है (क्रम में क्रम विवाद नहीं) निम्नप्रद विवाद किये जाने की जरूरत है, जैसे,

- प्राथमिक वर्गीकरण (प्राथमिक)
- संचालन मृत्यु (प्राथमिक)
- अनुगमन गुरुत्व उल्लंघन की लागत (राजनीति की हालानी)
- एपीएसजी प्रणाली कारण लागत और नेतृत्व सरकार
- एपीएसजी (एपीएसजी विकल्पों के बीच प्रविष्टियां) की परंपरा और उपलब्धता।
- लाइसेंस प्राप्तिमें कारणों के लिए योग्यता (विवर्तनीय, सीए/डीआरएफ विकल्प)

सामग्री मानिकों की विनिमय

क्लासिक (प्रतिपाद) सामग्री की विलोकन मामले पे-टीवी उद्यमों की आवाजाहिता है। पूरी दृष्टिकोण और अन्य सामग्री पुरानी के बांटे
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 – and 3D has been added to the mix in some parts of the world.

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

In this respect, Indian cable TV operators planning for the digital transition will benefit from...
choosing a security vendor that is well known among, and trusted by, the content providers. There is only one criterion that truly matters: a successful track record of pay-TV operator deployments around the world.

DIGITAL TV SECURITY – A BRIEF HISTORY

When digital TV was first introduced in Europe in the mid ’90s, all broadcast networks were one-way in nature, i.e. they had no return channel from the STB to the head-end. 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. 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 conditional access systems.

Unfortunately, “hackers” soon compromised all major CA systems, and it is now common practice among the legacy CA vendors to recommend replacement of the deployed smart cards every three years or so.

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, as well as for displaying electronic program guides and running sophisticated interactive applications), rivaling that of personal computers. They also often come with two-way connectivity, and operators are adding broadband capability in order to offer Video-on-Demand and interactive services.

In fact, modern set-tops are perfectly capable of handling security functions using a combination of software and security features embedded in their CPUs. Smart cards still represent a viable technology for operators that prefer such an approach, but cardless security is definitely the next step up.

CARD-LESS SECURITY

The card-less security of modern set-tops 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. The security module is software-based but resides in a highly secure environment that cannot be penetrated by the tools traditionally used by smart card pirates.

The secure SOC solution also solves the “control word sharing” piracy problem. In some legacy systems, the Control Word (content scrambling key) is passed in the clear between the smart card and the set-top video/audio descrambler. Pirates have found ways to intercept the key and share it with other (non-paying) subscribers over the Internet, and thus one hacked box can be used as a “server” for many others to 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 threat is overcome.

ADVANTAGES OF CARD-LESS SECURITY

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

Software-based and card-less security combines lower CAPEX and OPEX costs into 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 analog-to-digital transition while also laying a sound foundation for the future – a future that may include delivery to PCs and Macs, games consoles, smart phones, tablets and other mobile devices.

Aspiring cable operators ultimately should strive to implement a CA/DRM system that can serve as a unified revenue security platform for services destined to reach multiple screens across multiple networks. They will want a solution that can draw on the best of encryption, conditional access, digital rights management and video watermarking.
techniques to dynamically apply whatever types of security are appropriate to each service, no matter which delivery network is used, and no matter what type of subscriber device is used to access it. In fact, handling rights and subscriber management for different DRM systems from a unified security head-end is the ultimate objective.

Fortunately, Indian cable operators can now escape traditional CA system single-network restrictions without compromising security or adding complications to the consumer’s experience. In fact, a card-less system can provide new levels of security essential to new multi-screen service models that would be virtually impossible to achieve with legacy systems.

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. This is exemplified by the Verimatrix Video Content Authority System (VCAS™).

To secure revenue on an evolving pay-TV network, innovation is required that goes beyond traditional DVB CA. Part of the VCAS™ 3 multi-network platform, VCAS for DVB is a full featured security solution for one-way and DVB-IP hybrid networks. Featuring both card based and cardless security in a unified solution, it can be combined with VCAS protected multi-screen services to PC/Macs, tablets and smart phones, enabled by the unified VCAS 3 multi-network security authority.

**ABOUT AUTHOR**

The author Naveen Kumar is the Sales Director, SAARC Nations for Verimatrix Inc and a veteran associated with the “Broadcast and Cable TV Industry” for last two decades. He has worked in various roles and capacities spanning his 20 year career both as an entrepreneur and later moving to working for companies like Business India Television and General Instrument-Motorola where he focused in bringing in E2E solutions for the Broadcast & Cable industry. He subsequently moved on to focus primarily on the Pay TV industry by moving on to Irdeto, prior to joining Verimatrix.

**ABOUT VERIMATRIX**

Verimatrix is a leading provider of pay TV content protection solutions. Its solutions are designed for the world’s leading broadcast and cable service providers and digital TV operators who deliver video content to a wide variety of IP-based devices. The Verimatrix solutions enable service providers to preserve revenue streams and protect the value of their content in a multi-device world.

**MULTI-NETWORK SECURITY**

Verimatrix is a leading provider of pay TV content protection solutions. Its solutions are designed for the world’s leading broadcast and cable service providers and digital TV operators who deliver video content to a wide variety of IP-based devices. The Verimatrix solutions enable service providers to preserve revenue streams and protect the value of their content in a multi-device world.

Verimatrix is a leading provider of pay TV content protection solutions. Its solutions are designed for the world’s leading broadcast and cable service providers and digital TV operators who deliver video content to a wide variety of IP-based devices. The Verimatrix solutions enable service providers to preserve revenue streams and protect the value of their content in a multi-device world.

Verimatrix is a leading provider of pay TV content protection solutions. Its solutions are designed for the world’s leading broadcast and cable service providers and digital TV operators who deliver video content to a wide variety of IP-based devices. The Verimatrix solutions enable service providers to preserve revenue streams and protect the value of their content in a multi-device world.