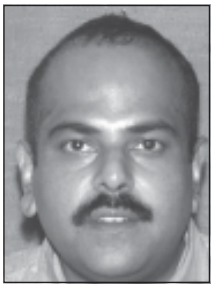
NEXT GENERATION MULTI-NETWORK DIGITAL TV SECURITY

By Naveen Kumar
Sales Director, SAARC Nations for Verimatrix Inc


NAVEEN KUMAR

CABLE TV DIGITALIZATION IN INDIA

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

अगली पीढ़ी वाले मल्टी–नेटवर्क डिजिटल टीवी की सुरक्षा

लेखक नवीन कुमार वेरीमैट्रिक्स इंक के लिए सार्क देशों के विक्रय निदेशक हैं

भारत में केबल टीवी का डिजिटलीकरण

भारत में केबल टीवी नेटवर्कों की आगामी डिजिटलीकरण विश्व में अपनी तरह के सबसे बड़े उपक्रमों में से एक है। यह ऑपरेटरों और तकनीकी विक्रताओं को ऐसी चुनौतियां व अवसर प्रदान कर रहा है जो कि भारत के टेलीविजन इतिहास में पहले कभी नहीं देखने को मिली। डिजिटल टीवी डिलिवरी तकनीकी उपभोक्ता व राजस्व विकास के लिए संभावनाओं को प्रस्तुत करने के साथ–साथ नयी सामग्री व राजस्व सुरक्षा चुनौती भी प्रदान करता है। यह लेख इन चुनौतियों पर ध्यान डाल रहा है और कंडिशनल एक्सेस (सीए) व डिजिटल राइट्स मैनेजमेंट (डीआरएम) से संबंधित कुछ उपाय पर विचार–विमर्श करेगा।

डिजिटल टीवी सुरक्षा–डिजिटल पे–टीवी की आधारशिला

सभी पे–टीवी ऑपरेटरों को सुरक्षित मुद्रीकरण सामग्री संबंधी मौलिक उद्देश्यों की हिस्सेदारी करनी पड़ती है और खासकर सेवा व सामग्री को गैर कानूनी एक्सेस यानि 'पाइरेसी' से बचाना होता है। उनकी विशेष रूप से इच्छा होती है कि वे अपनी वीडियो सेवाओं को (जो कि उनकी सेवा का राजस्व स्रोत है) विभिन्न तरह के खतरे जैसे इसकी सेवा की चोरी, स्मार्ट कार्ड की पाइरेसी, नकली उपकरण आदि से बचाना है। अब जबकि भारत में पे–टीवी की डिजिटल डिलिवरी की तैयारी चल रही है तो ऑपरेटरों को सभी तरह के खतरे को संबोधित करने वाले मॉडल को विकसित करना होगा।

एकओर एनालॉग केबल टीवी सिस्टम में सुरक्षा का प्राथमिक केंद्रबिंदु सेवा की चोरी रोकना था तो जब आप डिजिटल टीवी सेवाओं को प्रस्तुत कर रहे हैं तो खतरे का मॉडल अलग और अधिक चुनौतीपूर्ण होगा। इसलिए जबकि भारतीय केबल टीवी ऑपरेटर एनालॉग से डिजिटल स्थानांतरण की ओर जा रहे हैं तो उन्हें तकनीकी मामले को संबोधित करने के लिए सक्रिय योजना होनी चाहिए। अंत में दीर्घकाल में सेवा (राजस्व) जरूरतों से निबटने की क्षमता का त्याग

MULTI-NETWORK SECURITY

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.

किये बिना एक ऐसी सुरक्षा नीति व तकनीकी पॉथ का चुनाव करना होगा जो कि खर्च को न्यूनतम करे। सुरक्षा तकनीकी का चुनाव भारतीय केबल टीवी ऑपरेटरों के प्रतिस्पर्धी भविष्य और वित्तीय प्रदर्शन दोनों के लिए महत्वपूर्ण व मौलिक है।

डिजिटल टीवी सुरक्षा संबंधी बातें

हालांकि भारतीय केबल ऑपरेटर, एनालॉग से डिजिटल संक्रमण के लिए विचार व योजनाएं बना रहे हैं, साथ ही यह उन्हें डिजिटल टीवी सुरक्षा प्रदायकों द्वारा कार्य के समांतर पर परिमाण पर भी विचार करने की बात करता है। डिजिटल टीवी सुरक्षा से जुड़े कुछ लोग इस तरह भी विचार कर रहे हैंः

- एमपीईजी**2** या एमपीईजी**4** वीडियो फॉरमेट का चुनाव करें।
- सिर्फ स्टैंडर्ड डेफिनिशन (एसडी) सेवा ही ऑफर किया जाए या प्रारंभ से हाई डेफिनिशन (एचडी) शामिल किया जाए।
- प्रसारण नेटवर्क के प्रबंध के लिए हाईब्रिड आईपी आधारित उपाय शामिल किया जाए।
- स्वयं सीई उपकरणों को बंद करने के लिए अप्रबंधित नेटवर्क के ऊपर ओवर द टॉप (ओटीटी) आईपी सेवा को शामिल किया जाए।

छोटे या बड़े सभी भारतीय केबल टीवी ऑपरेटरों को एहसास होना चाहिए कि नये व्यपाार मॉडल और उनकी प्रतिस्पर्धात्मकता बढ़ाने के लिए लोचशील व प्रभावशाली डिजिटल टीवी सुरक्षा संरचना आवश्यक हो सकता है। इसलिए समग्र सुरक्षा उपाय की पसंद महत्वपूर्ण रणनीतिक निर्णय है। यह विचार राजस्व सुरक्षा के व्यापक अवधारणा के लिए पारंपरिक सामग्री संरक्षण से सुरक्षा तकनीकी के परिप्रेक्ष्य की ओर स्थानांतरण की बात कहता है।

कई पे–टीवी सुरक्षा कारक हैं (कम से कम वित्तीय नहीं) जिसपर विचार किये जाने की जरूरत है, जैसे,

- प्रारंभिक खरीदी मूल्य (सीएपीईएक्स)
- संचालन मूल्य (ओपीईएक्स)
- अनसुलझे सुरक्षा उल्लंघन की लागत (राजस्व की हानि)
- एसटीबी प्रमाणीकरण लागत और नेतृत्व समय
- एसटीबी (एसटीबी विक्रेताओं के बीच प्रतिस्पर्धा) की पसंद व उपलब्धता।
- लाइसेंस प्रीमियम सामग्री के लिए योग्यता (विश्वनीय सीए/डीआरएम विक्रेता)

सामग्री मालिकों की चिंताएं

क्वालिटी (प्रीमियम) सामग्री की लाइसेंसिंग सफल पे–टीवी उद्यमियों की आधारशिला है। मूवी स्टूडियोज और अन्य सामग्री प्रदायकों के बड़े

MULTI-NETWORK SECURITY

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.

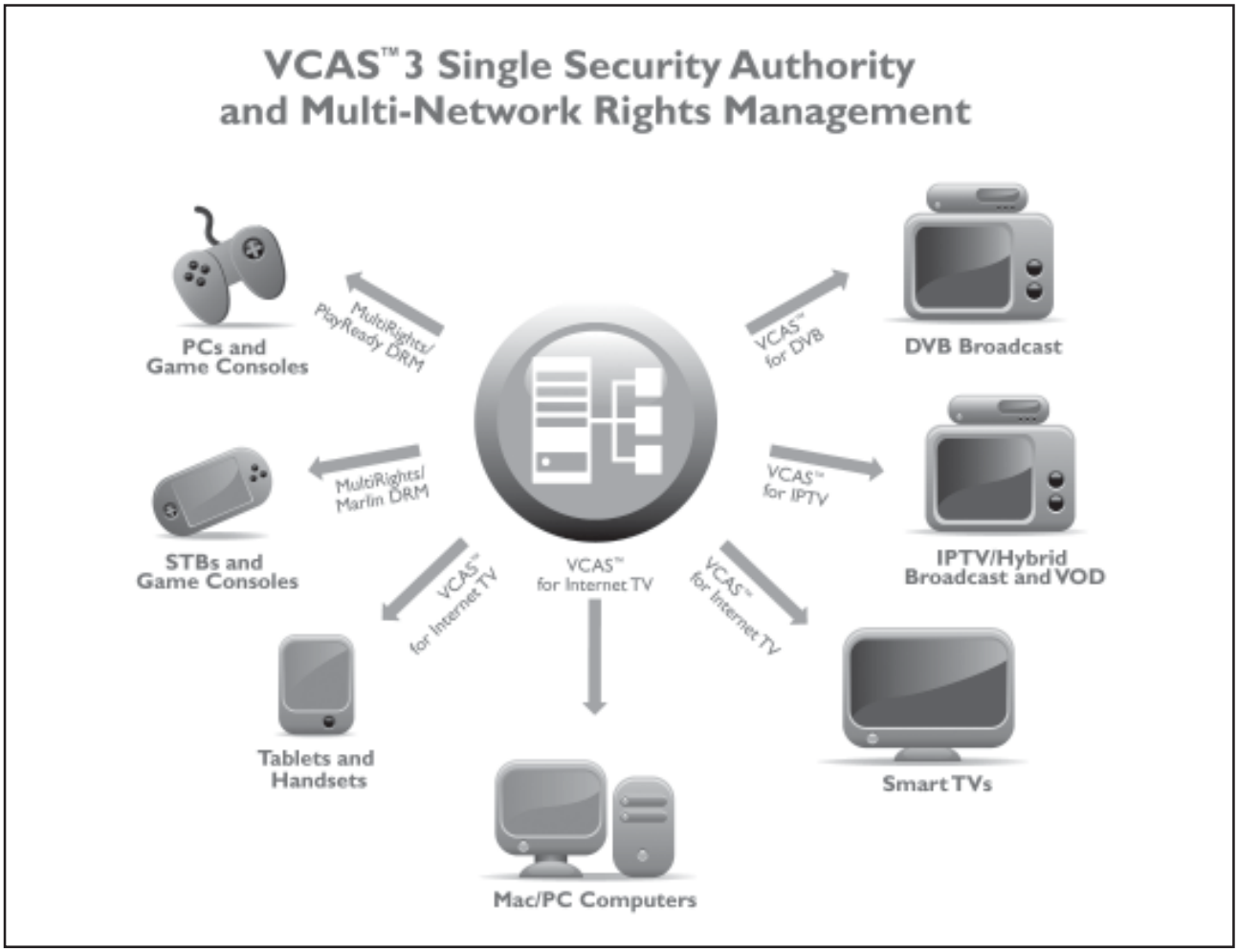
Content providers focus on enforcing digital rights through a combination of technological and legal processes. Rights owners and pay-TV operators alike expect digital TV security vendors to address the evolving challenges through a set of technologies and tools that encompass complete revenue security, 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

पैमाने पर पाइरेसी (जो कि उनके उत्पादों की संभावित जीवनकाल राजस्व की क्षमता को कमजोर कर सकता है) प्रमुख चिंता का विषय है। इसके अतिरिक्त एचडी सामग्री के लिए वाणिज्यिक दांव एसडी की तुलना में काफी अधिक है– और दुनिया के कुछ हिस्सो में 3डी को मिश्रण के रूप में शामिल किया गया है।

सामग्री प्रदाता, तकनीकी व वैधानिक उपायों के संयोजन के माध्यम से डिजिटल अधिकारों को लागू करने पर ध्यान केंद्रित कर रहे हैं। अधिकार धारक व पे–टीवी ऑपरेटर समान रूप से डिजिटल टीवी सुरक्षा विक्रेताओं से उम्मीद कर रहे हैं कि वे निर्धारित प्रोद्योगिकी और उपकरण की सहायता से उभरती चुनौतियों को संबोधित करें, जो कि सामग्री निर्माण, भंडारण, वितरण और खपत के दौरान और नेटवर्क से परे भी पूर्ण राजस्व सुरक्षा धरना, पूर्ण राजस्व सुरक्षा प्रदान करे।

इस संबंध में डिजिटल संक्रमण की योजना बना रहे भारतीय



MULTI-NETWORK SECURITY

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 card-less 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

केबल टीवी ऑपरेटरों द्वारा जाने माने और सामग्री प्रदाताओं द्वारा किये गये भरोसे से सुरक्षा विक्रेताओं के चुनाव का लाभ होगा। यहां सिर्फ एकमात्र कसौटी है जो कि वास्तव में मायने रखती है वह है विश्वभर में पे–टीवी ऑपरेटरों की सफल तैनाती का रिकॉर्ड।

डिजिटल टीवी सुरक्षा–एक संक्षिप्त इतिहास

जब 90 के दशक के मध्य में यूरोप में पहली बार डिजिटल टीवी प्रस्तुत की गयी तो सभी प्रसारक नेटवर्कों की प्रकृति एक समान थी यानि उनके पास एसटीवी से हेडएंड तक चैनल रिटर्न की व्यवस्था नहीं थी। तकनीकी दृष्टिकोण को 'पे–टीवी रहस्य' (जैसे उपभोक्ता एंटाइटेलमेंट व डिक्रिप्शन कुंजी) प्रदान किये जाने वाले स्मार्ट कार्ड को उपभोक्ताओं को एसटीवी के साथ प्रदान किया जाता था। सेवा प्रदायकों को अपनी सुरक्षा उपायों को मजबूत बनाने की जरूरत थी जो कि नेटवर्क व सेट टॉप के बीच भौतिक कनेक्शन पर निर्भर नहीं करे। यह स्मार्ट कार्ड आधारित कंडिशनल एक्सेस सिस्टम के लिए सबसे उपयुक्त थी।

दुर्भाग्य से हैकर ने शीघ्र ही सभी प्रमुख सीए सिस्टम के साथ छोड़छाड़ शुरू कर दी और अब यह विरासत सीए विक्रेताओं के बीच आम बात है कि वे प्रत्येक तीन या इतने ही वर्षों में इस्तेमाल किये जा रहे स्मार्ट कार्ड को बदलने की सिफारिश करें।

सेट टॉप बॉक्स की सुरक्षा व विकास

आज पूरा डिजिटल टीवी वातावरण बदल गया है। केबल ऑपरेटर अभी भी सेट टॉप बॉक्स का इस्तेमाल कर रहे हैं, लेकिन आज बॉक्स में कहीं अधिक प्रसंस्करण शक्ति है (इलेक्ट्रॉनिक कार्यक्रम गाइड का प्रदर्शन और परिष्कृत इंटरेक्टिव आवेदनों के संचालन के साथ–साथ वीडियो डिक्रिप्शन व डि–कंप्रेशन के लिए), जो कि पर्सनल कंप्यूटर का प्रतिद्वंदी है। ये प्रायः टू–वे कनेक्टिविटी के साथ आते हैं और ऑपरेटर, वीडियो–ऑन–डिमांड और इंटेरिक्टिव सेवाओं को ऑफर करने के क्रम में ब्रॉडबैंड क्षमता शामिल कर रहे हैं।

वस्तुतः आधुनिक सेट टॉप बॉक्स, अपने सीपीयू में शामिल सुरक्षा विशेषताओं व सॉफ्टवेयर के संयोजन का इस्तेमाल करके सुरक्षा कार्य कलापों को पूरी तरह संभालने में सक्षम है। स्मार्ट कार्ड वैसे ऑपरेटरों के लिए अभी भी व्यवहार्य तकनीक का प्रतिनिधित्व करते हैं जो कि इस तरह के दृष्टिकोण को पसंद करते हैं, लेकिन कार्ड रहित सुरक्षा निश्चित रूप से अगला कदम होगा।

कार्ड–रहित सुरक्षा

आधुनिक सेट टॉप बॉक्स की कार्ड रहित सुरक्षा में एम्बेडेड सुरक्षा सुविधाओं के साथ समझने में अत्यधिक कठिन, सॉफ्टवेयर आधारित सुरक्षा मॉड्यूल या परिष्कृत सिस्टम–ऑन–ए–चिप (एसओएस) के साथ बेहद कम लागत वाला बॉक्स शामिल हो सकता है जो कि आज सबसे

MULTI-NETWORK SECURITY

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

मजबूत और अभेद्य पे–टीवी सुरक्षा को संभव बनाता है। सुरक्षा मॉड्यूल सॉफ्टवेयर पर आधारित है लेकिन यह काफी सुरक्षित वातावरण में रहता है जो कि स्मार्ट कार्ड के पाइरेट्स द्वारा पारंपरिक रूप से इस्तेमाल किये जाने वाले उपकरणों से भेदा नहीं जा सकता।

सुरक्षित एसओसी उपाय नियंत्रण शब्द हिस्सेदारी 'पाइरेसी समस्या' को भी हल करता है। कुछ विरासत प्रणालियों में कंट्रोल वर्ड (सामग्री स्क्रैंबलिंग कुंजी) को स्मार्ट कार्ड और सेट टॉप वीडियो/ऑडियो डिस्क्रैंबलर के बीच स्पष्ट रूप से पास किया जाता है। पाइरेट्स ने कुंजी को बीच में रोकने का तरीका ढूंढ निकाला और इंटरनेट के ऊपर अन्य (भुगतान नहीं करने वाले) उपभोक्ताओं के साथ इसकी हिस्सेदारी करने लगे और इस तरह से पे टीवी सेवाओं की कई अन्य के द्वारा चोरी के लिए इनमें से एक हैक्ड बॉक्स का इस्तेमाल सर्वर के रूप में किया जा सकता है। सुरक्षित एसओसी वातावरण में कुंजी कभी भी सुरक्षित क्षेत्र के बाहर कभी उजागर नहीं होता और इस तरह कंट्रोल वर्ड शेयरिंग के खतरे से छुटकारा मिल जाता है।

कार्ड–रहित सुरक्षा के लाभ

तेजी से बदल रहे खतरे के परिदृश्य में सुरक्षा सब सिस्टम के नवीकरण की क्षमता का विशिष्ट लाभ है और व्यापार संभावनायें, सॉफ्टवेयर आधारित सुरक्षा को आकर्षक विकल्प बनाते हैं। सामग्री की सुरक्षा पाइरेट्स व जालसाजों के खिलाफ हथियारों की होड़ है, इसलिए सुरक्षा का नवीकरण होना चाहिए। आधुनिक सुरक्षित एसओएस तकनीकी के साथ सॉफ्टवेयर आधारित सुरक्षा लोचशील नवीकरण विकल्प प्रदान करते हुए केबल ऑपरेटरों को एक कदम आगे बने रहने की अनुमति देते हैं।

सॉफ्टवेयर आधारित व कार्ड रहित सुरक्षा मिलकर सीएपीईएक्स व ओपीईएक्स खर्च को घटाते हुए स्वामित्व प्रोफाइल के कुल लागत को और अधिक अनुकूल बनाता है। ओवर–द–एयर–अपडेट की सहायता से खतरे का मुकाबला किया जा सकता है।

सही डिजिटल टीवी सुरक्षा का चुनाव करना

भारतीय केबल ऑपरेटरों के लिए अनिवार्य है कि वे ऐसी सुरक्षा तंत्र का चुनाव करे जो कि तत्काल एनालॉग से डिजिटल संक्रमण में मदद करने के साथ–साथ भविष्य के लिए मजबूत आधारशिला भी रखे–ऐसा भविष्य जिसमें पीसी व मैक को डिलिवरी, गेम्स कॉनसोल्स, स्मार्ट फोन, टैबलेट्स व अन्य मोबाइल उपकरण शामिल हो सकता है।

आकांक्षी केबल ऑपरेटरों को अंततः सीए/डीआरएम सिस्टम को लागू करने का प्रयास करना चाहिए जो कि अनेक नेटवर्कों के लिए कई स्क्रीनों तक पहुंच के लिए निर्धारित सेवाओं के लिए एकीकृत राजस्व सुरक्षा प्लेटफार्म के रूप में सेवा करे। वे ऐसा उपाय चाहते हैं जो कि एन्क्रिप्शन कंडिशनल एक्सेस, डिजिटल राइट्स मैनेजमेंट के लिए सबसे अच्छा हो, और वीडियो वॉटर मार्ककिंग तकनीकी जिससे कि प्रत्येक सेवा

MULTI-NETWORK SECURITY

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. ■

के लिए उपयुक्त सुरक्षा को नेटवर्क द्वारा कौन से डिलिवरी नेटवर्क का इस्तेमाल किया गया है, इसकी चिंता किये बिना और इसे एक्सेस करने के लिए किस तरह के सब्सक्राइबर उपकरण का इस्तेमाल किया जा रहा है, इसकी चिंता किये बिना गतिशील तरीके से लागू करे। वस्तुतः एकीकृत सुरक्षा हेडएंड से भिन्न डीआरएम सिस्टम के लिए अधिकार व उपभोक्ता प्रबंधन को संभालना अंतिम उद्देश्य है।

सौभाग्य से भारतीय केबल ऑपरेटर अब उपभोक्ताओं के अनुभव के लिए जटिलता शामिल करना या सुरक्षा से समझौता किये बिना पारंपरिक सीए सिस्टम वाले सिंगल नेटवर्क से बच सकते हैं। वस्तुतः एक कार्ड रहित सिस्टम, नयी मल्टी स्क्रीन सर्विस मॉडलों के लिए आवश्यक सुरक्षा का नया स्तर प्रदान करता है जो कि विरासत सिस्टम के साथ प्राप्त करना वस्तुतः असंभव है। एकीकृत डिजिटल टीवी सुरक्षा प्रणाली ऐसे केबल ऑपरेटरों के लिए महत्वपूर्ण घटक है जो कि अपने अनुबंधों व सेवा संरक्षण दायित्वों को पूरा करने के लिए अपनी सेवा प्रोफाइल में विस्तार करने की ओर देख रहे हैं। बहु–स्तरीय सुरक्षा प्रदान करने वाला एक एकल सुरक्षा अधिकार नये बिजनेस मॉडल को उभरने व फलने फूलने का अवसर देगा। वेरीमैट्रिक्स वीडिया कंटेंट अथॉरिटी सिस्टम (वीसीएएस) द्वारा इसका उदाहरण दिया गया है।

एक उभरती पे–टीवी नेटवर्क पर राजस्व सुरक्षित करने के लिए नये खोज की जरूरत है जो कि पारंपरिक डीवीबी सीए से परे जाए। वीसीएएस**3** मल्टी नेटवर्क प्लेटफार्म के हिस्से के रूप में डीवीबी के लिए वीसीएएस, वन वे और डीवीबी–आईपी हाईब्रिड नेटवर्कों के लिए पूर्ण विशेषताओं वाला सुरक्षा उपाय है। एकीकृत समाधान में कार्ड आधारित और कार्ड रहित दोनों विशेषताओं के साथ पीसी/मैक, टैबलेट्स व स्मार्ट फोन के साथ वीसीएएस संरक्षित मल्टी स्क्रीन सेवा के साथ इसे जोड़ा जा सकता है जिसे एकीकृत वीसीएएस**3** मल्टी नेटवर्क सुरक्षा अथॉरिटी द्वारा सक्षम बनाया जाता है। ■

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. ■

लेखक के विषय में

लेखक नवीन कुमार वेरीमैट्रिक्स इंक के लिए सार्क देशों के विक्रय निदेशक हैं और पिछले दो दशकों से 'ब्रॉडकास्ट और केबल टीवी उद्योग' के साथ वरिष्ठतम रूप से जुड़े हुए हैं।

*उन्होंने अपने **20** साल के विस्तृत कैरियर में विभिन्न भूमिकाओं व क्षमताओं के साथ पहले उद्यमी के रूप में और फिर बिजनेस इंडिया टेलीविजन और जनरल इंस्ट्रूमेंट–मोटारोला के लिए काम किया है जहां उन्होंने अपना ध्यान प्रसारण व केबल उद्योग के लिए ई**2**ई उपाय लाने की ओर केंद्रित किया। इसके बाद उन्होंने वेरीमैट्रिक्स में शामिल होने से पहले इरडेटो में शामिल होकर खास रूप से पेटीवी उद्योग की ओर ध्यान केंद्रित किया।* ■