INTEGRATED SOFTWARE AND HARDWARE SECURITY: THE NEXT STEP IN SET-TOP BOX CONTENT AND REVENUE PROTECTION

By Ben Jun, Vice President and CTO, of Cryptography Research, Inc. and Petr Peterka, CTO, Verimatrix

As the volume of set-top boxes (STBs) shipped continues to increase, hacking STBs remains a primary activity for pirates. While the last 25 years have shown advances in content protection technology, many consider the necessary next step in STB-based pay TV to be hardware security cores, which serve as vaults inside the STB chipsets/system-on-chips (SoCs) performing highly sensitive content protection functions. Concentrating all security sensitive functions of the STB chipsets in a hardware security core nucleus makes it very hard for pirates to accomplish their nefarious mission. In this article, we will explore the benefits of a hardware security core solution, and offer operators guidance on how to incorporate such a solution into their content protection strategies.

एकीकृत सॉफ्टवेयर और हार्डवेयर सिक्यूरिटीः सेट टॉप बॉक्स कंटेंट में अगला चरण और राजस्व सुरक्षा

लेखकः बेन जुन, उप-प्रधान व सीटीओ, क्रिप्टोग्राफी रिसर्च इंक और पेट्र पिटिरका, सीटीओ, वेरिमेट्रीक्स

सेट टॉप बॉक्स (एसटीबी) के वॉल्यूम के आयात के लगातार बढ़ने के साथ पाइरेट्स के लिए प्राथमिक गतिविधि हैक किये गये एसटीबी हैं। एक ओर पिछले **25** वर्ष में हमें कंटेंट प्रोटेक्शन तकनीकी में प्रगति देखने को मिली है, कई इसे हार्डवेयर सिक्यूरिटी कोर के लिए एसटीबी आधारित पे टीवी में आवश्यक मान रहे हैं, जो कि एसटीबी चिपसेट्स/सिस्टम ऑन चिप्स (एसओसी) के भीतर वॉल्ट के रूप में अत्यधिक संवेदनशील कंटेंट संरक्षण कार्य का प्रदर्शन करता है। हार्डवेयर सिक्यूरिटी में एसटीबी चिपसेट के सभी सुरक्षा संवेदनशील कार्यों पर ध्यान केंद्रित करते हुए कोर नाभिक पाइरेट के लिए उनके नापाक मिशन को अंजाम देना मुश्किल बना देती है। इस लेख में हम हार्डवेयर सिक्यूरिटी कोर समाधान के लाभ का पता लगायेंगे और ऑपरेटरों के लिए यह दिशा-निर्देश देंगे कि उनके कंटेंट प्रोटक्शन रणनीति में इस उपाय को कैसे शामिल किया जाए।

INTEGRATED STB SECURITY

EXPLORING THE BENEFITS OF A HARDWARE SECURITY CORE SOLUTION

As the sophistication of STB chipset technology has evolved, all major chip manufacturers have introduced some form of security hardware subsystem to provide CW encryption and other protection techniques in the security logic of their products. The varying levels of sophistication offered, and the increasing challenge of parallel integration efforts, have created an opportunity in the industry for a specialized hardware core that provides a common approach and state-of-the-art protection across device families.

The hardware security core approach brings significant security and architectural advantages.

A hardware security core that includes strong countermeasures against glitching, SPA, DPA, and other invasive and non-invasive attacks, can help achieve a hardware security level on the STB chipset that improves on today's most advanced smart card chips. As a part of advancing the overall industry approach, focusing hardening effort on the STB chipset rather than a separate security module removes the obvious physical and electrical attack points inherent in removable hardware and the buses that interface this hardware to the STB itself.

With careful design of the STB security software in conjunction with the hardware security cores, the content decryption keys (CWs) and other critical security data do not pass through external card interfaces or through easily probed register interfaces. Instead, the CWs are passed directly inside the chipset to the descramblers. With security processing tightly integrated with the video decryption and decoding processes, the resulting security against CW sharing and related attacks is greatly improved compared with traditional approaches.

Furthermore, by providing key management protection integrated with the hardware security core, it becomes very hard for pirates to follow or modify the device security processing. In an increasingly hybrid network environment where entitlement decisions can be migrated to secure head-end environments, the hardware security core provides a strong environment in which to process device and message authentication, including challenge-response functions to help improve the integrity of runtime tamper resistance.

Two additional advantages are achieved by the separation of the hardware security core from the rest of the STB environment:

हार्डवेयर सुरक्षा कोर समाधान के लाभों की तलाश

एसटीबी चिपसेट तकनीकी के परिष्करण का विकास हुआ तो सभी प्रमुख चिप उत्पादकों ने किसी भी रूप में अपने उत्पादों के सिक्यूरिटी लॉजिक में सीडब्लू एन्क्रिप्शन और अन्य सुरक्षा तकनीकी प्रदान करने के लिए सिक्यूरिटी हार्डवेयर सब सिस्टम प्रस्तुत किया। परिष्कार पेशकश के अलग स्तर और समानंतर एकीकरण प्रयासों की बढ़ती चुनौतियां विशिष्ट हार्डवेयर कोर के लिए उद्योग में अवसरों का निर्माण किया जो कि समस्त परिवार उपकरण को अत्यधिक सुरक्षा और एक आम दृष्टिकोण प्रदान करते हैं।

हार्डवेयर सुरक्षा कोर दृष्टिकोण उल्लेखनीय सुरक्षा और आर्किटेक्चर फायदा लाता है।

हार्डवेयर सिक्यूरिटी कोर जिसमें कि ग्लीचिंग, एसपीए, डीपीए और अन्य आक्रमक व गैर-आक्रमक अटैक के विरूद्ध मजवूत काउंटर उपाय शामिल हैं, एसटीबी चिपसेट पर हार्डवेयर सुरक्षा स्तर को प्राप्त करने में सहायता कर सकता है जो कि आज के अधिकांश स्मार्ट कार्ड चिप में सुधार करेगा। समग्र उद्योग दृष्टिकोण को आगे बढ़ाने के भाग के रूप में एसटीबी चिपसेट सख्त प्रयासों पर केंद्रित होगा न कि अलग सिक्यूरिटी मॉड्यूल स्पष्ट फीजिकल और इलेक्ट्रीकल एटैक प्वाइंट को हटाता है जो कि रिमूवल हार्डवेयर और बसों में शामिल होता है जो कि इस हार्डवेयर को खुद एसटीबी में इंटरफेस करेगा।

हार्डवेयर सिक्यूरिटी कोर के साथ सहयोग में एसटीबी सिक्यूरिटी सॉफ्टवेयर के सावधानीपूर्वक डिजाइन के साथ कंटेंट डि-क्रिप्शन की (सीडब्लू) और अन्य जटिल सिक्यूरिटी डेटा इस बाहरी कार्ड इंटरफेस या आसानी से रजिस्टर इंटरफेस के जांच के माध्यम से पास नहीं होगी। इसके स्थान पर सीडब्लू सीधे चिपसेट के भीतर पास होकर डिस्क्रैंबल होगा। वीडियो डिक्रिप्शन और डि-कोडिंग प्रोसेस के साथ मजबूती से एकीकृत सिक्यूरिटी प्रोसेसिंग के साथ सीडब्लू शेयरिंग के विरूद्ध सुरक्षा परिणाम और संबंधित अटैक, पारंपरिक तरीकों के साथ तुलना में काफी सुधार करता है।

इसके अलावा हार्डवेयर सुरक्षा कोर के साथ एकीकृत प्रमुख मैनजमेंट सुरक्षा प्रदान करके यह पाइरेट के लिए काफी मुश्किल होता है कि वे उपकरण सुरक्षा प्रोसेसिंग में सुधार करें या पालन करें। एक बढ़ते हुए हाईब्रिड नेटवर्क वातावरण में जहां कि एंटाइटिल निर्णय को सुरक्षित हाई एंड वातावरण में माईग्रेट किया जा सकता है, हार्डवेयर सिक्यूरिटी कोर एक मजबूत वातावरण प्रदान करता है जहां कि डिवाइस और संदेश प्रमाणीकरण को प्रोसेस करता है जिसमें कि चुनौती प्रतिक्रिया फंक्सन शामिल होता है जिससे कि रनटाइम टैंपर प्रतिरोध की अखंडता को बेहतर बनाने में सहायता हो।

शेष एसटीबी वातावरण से हार्डवेयर सिक्यूरिटी कोर के पृथक्करण द्वारा दो अतिरिक्त लाभ प्राप्त किया जा सकता हैः

INTEGRATED STB SECURITY

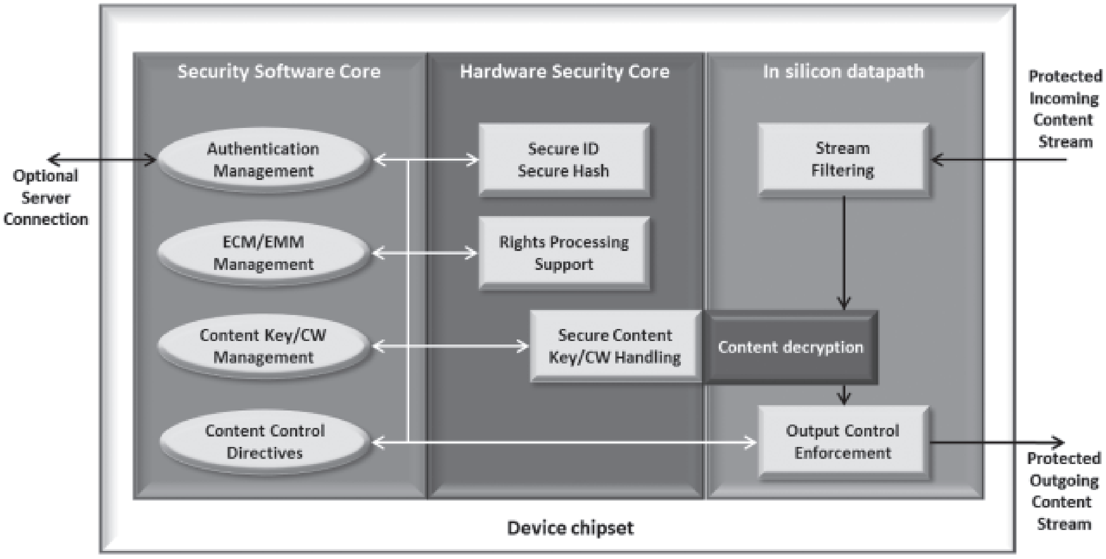

Figure 2: Hardware security core in the STB chipset.

(1) Less scope for malicious or compromised software/firmware in the STB to be able to interfere with content protection, and

(2) Any update to the STB software or firmware would not require the STB maker, operator, etc. to re-certify the overall STB security.

The former improves security and allows for open platforms such as Android and third-party apps, while the latter saves time and effort thus improving time to market.

Moreover, in a world where operators attempt to differentiate their services by offering compelling content, including high-value titles in HD quality and increasingly in early release windows, having inadequate STB security results in higher content acquisition costs, lost revenue and/or less compelling content.

HARDWARE SECURITY CORES REQUIRE INTEGRATED SOFTWARE

While a hardware security core provides the silicon-level capabilities to enable effective security, it needs to be combined with software capabilities to provide an end-to-end system of highly resistant key management. A hardware security core is therefore an essential element of a conditional (CA) solution, not a replacement for one.

One particularly compelling approach is cardless CA systems for broadcast networks – an approach that is increasingly a standard

(1) एसटीबी में दुर्भावनापूर्ण या कंप्रोमाइज्ड सॉफ्टवेयर/फर्मवेयर के कंटेंट प्रोटेक्शन के साथ हस्तक्षेप की कम संभावना है, और

(2) एसटीबी सॉफ्टवेयर या फर्मवेयर में किसी अपडेट के लिए एसटीबी मेकर, ऑपरेटरों आदि को अपने पूरे एसटीबी सुरक्षा को फिर से सर्टिफाई कराने की जरूरत नहीं होगी।

पहला जहां सुरक्षा में सुधार करता है और एन्ड्रायड व थर्ड पार्टी ऐप जैसे ओपन प्लेटफार्म के लिए अनुमति देता है जबकि दूसरा वाला समय व प्रयास को बचाता है जिससे मार्केट के लिए समय में सुधार किया जाए।

इसके अलावा एक विश्व में जहां कि ऑपरेटर बाध्यकारी कंटेंट ऑफर करके अपनी सेवा को अलग करने का प्रयास करता है, जिसमें शामिल है एचडी क्वालिटी में हाई वैल्यू टाइटिल और फिल्म को पहले रिलिज करना, यदि एसटीबी सुरक्षा अपर्याप्त होगी तो अधिग्रहण मूल्य अधिक होगा, राजस्व नुकसान या फिर उतने बाध्यकारी कार्यक्रम नहीं होने के रूप में हो सकता है।

हार्डवेयर सिक्यूरिटी कोर के लिए एकीकृत सॉफ्टवेयर की जरूरत

एकओर हार्डवेयर सिक्यूरिटी कोर प्रभावी सुरक्षा को सक्षम बनाने के लिए सिलिकॉन लेवल क्षमताओं को प्रदान करता है, इसे सॉफ्टवेयर क्षमताओं के साथ एकीकृत करने की जरूरत है जिससे कि उच्च प्रतिरोधी की मैनेजमेंट के एंड टू एंड सिस्टम को प्रदान किया जाए। इसलिए एक हार्डवेयर सिक्यूरिटी कोर कंडिशनल (सीए) सॉल्यूशन का आवश्यक तत्व है, जिसके लिए रिप्लेसमेंट नहीं।

प्रसारण नेटवर्क के लिए एक विशेष रूप से बाध्यकारी तरीका कार्डलेस सीए दृष्टिकोण है–एक ऐसा तरीका जो कि लगातार स्टैंडर्ड

requirement. The attractive approach here is to maximize the utilization of hardware within the STB chipset by the security/CA subsystem. This potent combination delivers the cost-effectiveness and flexibility of software combined with the highest levels of security offered by hardware.

Additionally, in IP video delivery networks, where STB clients have long been based on cardless architectures, utilization of a hardware security core in the STB chipset can address concerns regarding potential CW sharing and cloning attacks. In such architectures the security software is responsible for requesting keys, receiving and storing incoming messages, synchronizing descrambling, and managing the user interface, but removed from direct handling of the video decryption keys themselves or the decrypted media stream.

CARDLESS SECURITY SCENARIOS

Example 1: Software-based security for one-way networks – Using a pure software CA for one-way broadcast operation is intriguing. Compared with external devices like smart cards, software is cost efficient to deploy in the field and to update over time.

However, the logic of pay-TV content security is well known to pirates and this makes the control paths somewhat vulnerable to analysis and potential alteration. Certainly, if software runs in an unprotected STB host environment, skilled hackers can figure out how to short-circuit the access entitlement logic and/or extract CWs.

By integrating the security implementation with the support of a hardware security core, the potential for hackers to use emulators and rogue devices to manipulate the content access decision and extract CWs is greatly reduced. Hardware security cores can therefore play a significant role in enabling the use of cardless CA for mainstream one-way broadcast operation.

Example 2: Hybrid broadcast – broadband support – Flexible hardware security cores will support the different scrambling and rights processing schemes used for DVB broadcasting, IPTV live-TV streaming and on-demand delivery. The same core can then be used to harden both the broadcast CA and the on-demand and streaming digital rights management (DRM) system clients of hybrid STBs and home-gateways providing a very compact solution supporting picture-in-picture, recording one

जरूरत बनती जा रही है। यहां पर आकर्षक तरीका है सिक्यूरिटी/सीए सबसिस्टम की सहायता से एसटीबी चिपसेट के भीतर हार्डवेयर के इस्तेमाल को अधिकतम करना। यह शक्तिशाली संयोजन हार्डवेयर द्वारा ऑफर किये गये सुरक्षा के उच्चतम स्तर के साथ लागत प्रभावशीलता और सॉफ्टवेयर के लचीली संयोग को डिलिवर करेगा।

आईपी वीडियो डिलिवरी नेटवर्क में इसके अलावा, जहां कि एसटीबी ग्राहक काफी लंबे समय से कार्डलेस आर्किटेक्चर, एसटीबी चिपसेट में हार्डवेयर सिक्यूरिटी कोर का इस्तेमाल संभावित सीडब्लू शेयरिंग और क्लोनिंग एटैक से संबधित चिंता को संबोधित करता है। इस तरह की संरचना में सिक्यूरिटी सॉफ्टवेर रिक्वेस्टिंग की, आने वाले संदेश को रिसीव व स्टोर करना, सिंक्रोनाइजिंग डिस्क्रैंबलिंग और यूजर इंटरफेस के देखरेख के लिए जिम्मेवारी होती है, लेकिन वीडियो डि–क्रिप्शन खुद या डि–क्रिप्टेड मीडिया स्ट्रीम के सीधे हैंडलिंग से हटा देता है।

कार्डलेस सिक्यूरिटी परिदृश्य

उदाहरण 1ः वन वे नेटवर्क के लिए सॉफ्टवेयर आधारित सिक्यूरिटी–वन वे ब्रॉडकास्ट ऑपरेशन के लिए प्योर सॉफ्टवेयर का इस्तेमाल करना लुभावना है, जब हम इसकी तुलना स्मार्ट कार्ड, जैसे बाहरी उपकरणों के साथ करते हैं तो सॉफ्टवेयर को फिल्ड में लगाना किफायती है और समय के साथ अपडेट होता रहता है।

हालांकि पे टीवी कंटेंट सिख्यूरिटी की लॉजिक पाइरेट्स के लिए जानी मानी है और यह विश्लेषण व संभावित परिवर्तन के कंट्रोलपथ को कुछ हद तक कमजोर बना देती है। निश्चित रूप से यदि सॉफ्टवेयर को किसी असुरक्षित एसटीबी होस्ट वातावरण में संचालित किया जाए तो प्रशिक्षित हैकर इस बात का पता लगा सकते हैं कि एक्सेस इनटाइटेलमेंट लॉजिक और/या एक्स्ट्रेक्ट सीडब्लू को किस तरह शर्ट सर्किट किया जाए।

हार्डवेयर सिक्यूरिटी कोर के समर्थन के साथ सिक्युरिटी प्रस्तुतिकरण को एकीकृत करके हैकरों के लिए एमुलेटर और rogue devices के इस्तेमाल की संभावना कंटेंट एक्सेस निर्णय में हेराफेरी कर सकता है और निकाला सीडब्लू काफी घट जाता है। इसलिए हार्डवेयर सिक्यूरिटी कोर वन वे ब्रॉडकास्ट ऑपरेशन को बरकरार रखने के लिए कार्डलेस सीए के इस्तेमाल में सक्षम बनाने में अहम भूमिका निभाता है।

उदाहरण 2ःहाईब्रिड ब्रॉडकास्ट–ब्रॉडबैंड समर्थन–डीवीबी ब्रॉडकास्टिंग, आईपीटीवी लाइव–टीवी स्ट्रीमिंग और ऑन डिमांड डिलिवरी के लिए इस्तेमाल भिन्न स्क्रैंबलिंग और सही प्रोसेसिंग योजना फ्लेक्सिबल हार्डवेयर सिक्यूरिटी कोर का समर्थन करता है। इसी कोर का फिर इस्तेमाल ब्रॉडकास्ट सीए और ऑन डिमांड व स्ट्रीमिंग डिजिटल राइट्स मैनेजमेंट (डीआरएम) और होम गेटवे दोनों में करते हुए काफी कॉम्पैक्ट उपाय सर्पोटिंग पिक्चर–इन–पिक्चर, एक कार्यक्रम की रिकॉडिंग करता है जबकि अन्य व अन्य कई

programme while viewing another and multi-room even if the content is received from different networks.

Example 3: Two-way pay-TV networks – When distributing pay-TV content via two-way networks, the STBs authenticate themselves to a head-end CA/DRM server. The server becomes the point of decision making for individual STB and content entitlements, and provides the information necessary for accessing the content after entitlement verification.

While two-way communication offers more control options than one-way distribution – including positive acknowledgement of updates and integrity checks – it does not completely eliminate the threat of CW sharing attacks and potential client emulation. If pirates are able to hack a STB/device using a sophisticated form of logic attack (for example DPA), or otherwise appear as authentic for the CA/DRM server, they might obtain access to the compressed digital content as well as CW information that can be used for CW sharing.

कंट्रोलरूम देखता है बावजूद इसके कि कंटेंट भिन्न नेटवर्क से रिसीव हो रहा है।

उदाहरण 3ः टू वे पे टीवी नेटवर्क–जब हम टू वे नेटवर्क की सहायता से पे टीवी कंटेंट का वितरण करते हैं तो एसटीबी खुद को सीए/डीआरएम सर्वर हेडएंड को प्रमाणीकृत करता है। सर्वर व्यक्तिगत एसटीबी और कंटेंट हकों के लिए निर्णय लेने वाला बिंदु बनता है और प्रमाणीकृत की जांच के बाद कंटेंट को एक्सेस करने के लिए आवश्यक सूचना प्रदान करता है।

हालांकि टू वे संचार, वन वे वितरण के मुकावले अधिक नियंत्रण ऑफर करता है–इसमें अपडेट की सकारात्मक अभिस्वीकृति और अखंडता की जांच शामिल रहती है–यह पूरी तरह सीडब्लू शेयरिंग एटैक और संभावित क्लाइंट अनुकरण को पूरी तरह समाप्त नहीं करता है। यदि पाइरेट लॉजिक एटैक (उदाहरण के लिए डीपीए) के परिष्कृत फार्म या सी/डीआरएम सर्वर के लिए अन्यथा प्रमाणीकृत का इस्तेमाल करके एसटीबी/उपकरण को हैक करने में सक्षम हो जाते हैं तो वे संभवतः कंप्रेस्ड डिजिटल कंटेंट के साथ–साथ सीडब्लू सूचनाओं को भी एक्सेस कर सकते हैं जिसका इस्तेमाल सीडब्लू शेयरिंग के लिए किया जाता है।

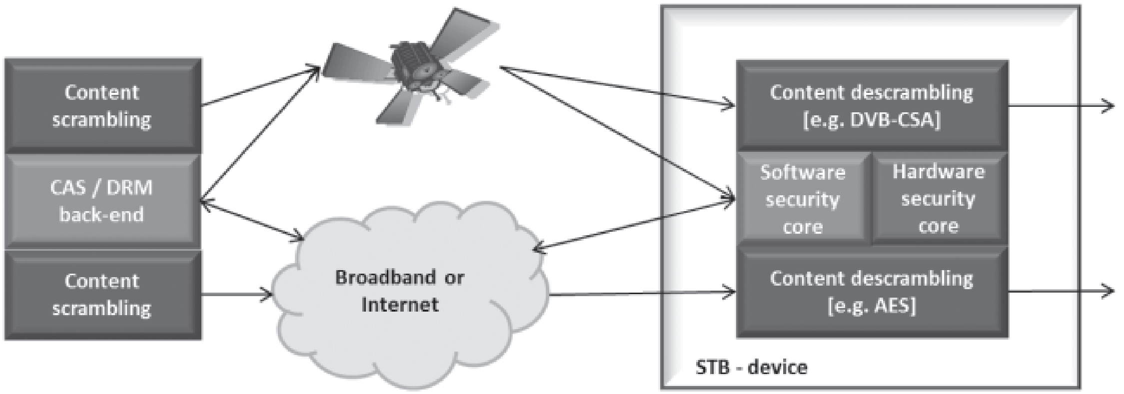

Figure 3: Example of hybrid broadband and IP delivery using a unified security platform

Device authentication performed in conjunction with head-end servers, including HW supported challenge/response mechanisms becomes significantly stronger when performed in conjunction with a hardware security core.

Example 4: Parallel CA "double-hull" security – Combining hardware security core mechanisms with security techniques from other technology environments can achieve a strong composite 'seat belt + airbag' effect. If the card, security app or hardware security core is penetrated, hackers would still need to break the other protection(s) to compromise overall security.

उपकरण प्रमाणीकरण का प्रदर्शन हेडएंड सर्वर के साथ मिलकर किया जाता है जिसमें शामिल एचडब्लू समर्थित चुनौती/प्रतिक्रिया तंत्र काफी मजबूत हो जाती हैं जब इसका प्रदर्शन हार्डवेयर सिक्यूरिटी कोर के साथ मिलकर किया जाता है।

उदाहरण 4ःसमानांतर सीए 'डबल–पतवार' सुरक्षा– अन्य तकनीकी वातावरण से सिक्यूरिटी तकनीकी के साथ हार्डवेयर सुरक्षा कोर तंत्र के मेल को 'सीट बेल्ट + एयरबैग प्रभाव को एक मजबूत मिश्रण से प्राप्त किया जा सकता है। यदि कार्ड, सिक्यूरिटी ऐप या हार्डवेयर सिक्यूरिटी कोर को भेदा जाता है तो हैकर को अभी भी संपूर्ण सुरक्षा के साथ समझौते के लिए अन्य सुरक्षा को तोड़ने की जरूरत है।

Note that such double configuration is different from Simulcrypt. Normal Simulcrypt assumes the receiver device to have a single security module that processes a single CA/DRM only, while parallel CA configuration assumes the receiver device to have several security modules configured in a way that forces pirates to break them all to exploit the system.

Example 5: Cloud based OTT content distribution service – A cloud-based content distributor's security app can be installed on operator client devices that have hardware security cores inside. The OTT content can then be encrypted in a way that requires both the security app and the hardware security core to provide separate CWs for content decryption.

Such a scheme provides the cloud operator complete end-to-end protection of the content as well as control over the number of devices receiving the content, while the local operator maintains the role as the primary TV provider to the subscribers.

EVOLVING STB CONTENT PROTECTION REQUIREMENTS

Hardware security cores in STB chipsets represent the next step in STB content protection.

Their first and foremost contribution is significant increase of robustness where it is now needed: inside the STB chipsets. Leaving minimal room for piracy benefit all stakeholders along the value chain.

Additional advantages include offering operators flexibility to optimize content presentation and monetization via advanced system software, cost efficiency as no external smart cards or CAMs are required, reduced risk of premature STB replacements due to piracy, and increased likelihood of obtaining content within early release windows at favorable terms.

STB and chipset makers also benefit from less content protection-related constraints, which means more freedom for innovation.

And finally, CA/DRM system vendors are able to offer a larger security repertoire including improved security against control word sharing, 'double hull' security shell, etc. to gain and retain operator customers. These improved system products offer operators more features in STBs and support hybrid delivery, OTT delivery, cloud delivery and multi-screen/TV Everywhere — serving as the foundation of STB content and revenue protection. ■

नोट करें कि इस तरह का दोहरा कॉनफिगुरेशन सिमूलक्रिप्ट से भिन्न है। सामान्य सिमूलक्रिप्ट एक सामान्य सुरक्षा मॉड्यूल के लिए रिसीवर उपकरण मानता है जो कि सिंगल सीए/डीआरएम को ही प्रोसेस करता है, जबकि समानांतर सीए कॉफिगुरेशन मानता है कि रिसीवर उपकरणों में कई सिक्यूरिटी मॉडयूल लगा हुआ है जो कि पाइरेट को सिस्टम का शोषण करने के लिए सभी को ब्रेक करने को बाध्य करता है।

उदाहरण 5ः एक क्लाउड आधारित कंटेंट डिस्ट्रीब्यूटर के सिक्यूरिटी ऐप को ऑपरेटर क्लाइंट उपकरणों पर इंस्टॉल किया जा सकता है जिसमें कि हार्डवेयर सिक्यूरिटी अंदर होता है। इसके बाद ओटीटी कंटेंट इस तरीके से एन्क्रिप्टेड किया जाता है जिसके कंटेंट डिक्रिप्शन के लिए अलग सीडब्लू प्रदान करने के लिए सिक्यूरिटी ऐप व हार्डवेयर सिक्यूरिटी कोर दोनों की जरूरत होती है।

इस तरह की स्कीम ऑपरेटरों को कंटेंट रिसीव करने वाले कई उपकरणों के ऊपर नियंत्रण के साथ साथ कंटेंट के पूर्ण एंड टू एंड सुरक्षा प्रदान करता है, जबकि स्थानीय ऑपरेटर उपभोक्ताओं को प्राथमिक टीवी प्रदायक की भूमिका को बरकरार रखते हैं।

विकसित एसटीबी कंटेंट सुरक्षा जरूरत

एसटीबी चिपसेट में हार्डवेयर सिक्यूरिटी कोर एसटीबी कंटेंट सुरक्षा में अगला कदम है। पहला और सबसे महत्वपूर्ण योगदान मजबूती में उल्लेखनीय बढ़ोतरी है जहां कि इसे अब एसटीबी चिपसेट के भीतर होने की जरूरत है। जिससे पाइरेसी की संभावना एक ओर बहुत कम रह जाती है वहीं वैल्यू चेन से जुड़े सभी हितधारकों के लिए लाभदायक होता है।

अतिरिक्त लाभ में परिष्कृत सिस्टम सॉफ्टवेयर की सहायता से कंटेंट प्रस्तुतिकरण और मुद्रीकरण अनुकूलन की लोचशीलता ऑपरेटर को ऑफर करता है, यह किफायती है क्योंकि किसी बाहरी स्मार्ट कार्ड या सीएएम की जरूरत नहीं होती, पाइरेसी के चलते समय से पहले एसटीबी रिप्लेसमेंट के खतरे को घटाता है और अनुकूल शर्तों पर अर्ली रिलीज विंडो के भीतर कंटेंट प्राप्त करने की संभावना को बढ़ाता है।

एसटीबी और चिपसेट निर्माता भी कंटेंट संरक्षण से संबंधित कम बाधाओं से लाभान्वित होंगे, इसका मतलब है खोज के लिए अधिक स्वतंत्रता।

और अंत में सी/डीआरएम सिस्टम विक्रेता एक बड़ी सुरक्षा प्रदर्शनों की सूची की पेशकश करने में सक्षम होंगे, जिसमें शामिल है कंट्रोल वर्ड शेयरिंग के खिलाफ बेहतर सुरक्षा, 'दोहरे पतवार' सुरक्षा कवच आदि ऑपरेटर उपभोक्ताओं को हासिल और बनाये रखता है। ये परिष्कृत सिस्टम प्रोडक्ट, एसटीबी में और विशेषताओं को ऑफर करते हैं और हाईब्रिड डिलिवरी, ओटीटी डिलिवरी, क्लाउड डिलिवरी और मल्टी स्क्रीन/टीवी सभी जगह ऑफर करते हुए एसटीबी कंटेंट और राजस्व सुरक्षा के नींव के रूप में सेवा देते हैं। ■