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.
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 core, 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:
(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.
INTEGRATED STB SECURITY

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 homegateways providing a very compact solution supporting picture-in-picture, recording one
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.

InTEGRATED STB SECURITY

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.

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

उपरकरण प्रामाणिकता का प्रदान हेडेंड सर्वेंट के साथ मिलकर किया जाता है जिसमें आमतौर पर एडवर्डस-समर्थित नूतनी/क्यारिकल्टांश तंत्र का प्रयोग होता है। इसका प्रदान हाइडेंड हिजिटल कोर के साथ मिलकर किया जाता है।

उपरकरण 45 समानांतर सीए ‘ओल-टवर’ सुरक्षा - अन्य तकनीकी वातावरण में सिक्सुरिटी तकनीकी के साथ हाइडेंड ग्राफिक कोर के मेद को ‘प्रों-ब्रेन्ड + एयरवेग प्रमाण’ का एक मजबूत मिलकर प्राकृतिक रूप से प्राप्त किया जा सकता है। उपरकरण का ‘एएस’ छत्रांकित सिक्सुरिटी कोर को भंडा किया जाता है तो हैकर को अपनी भी संग्रहण गुणवत्ता के साथ समय-कालीन से बनाया जा सकता 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.