WHITE PAPER

Security Impacts Of Next-Generation Set-Top Boxes

March 2010

Table of Contents

1. Introduction

Consumer demand for media-rich home entertainment services is driving innovation and new revenue opportunities in the set-top box (STB) industry. Next-generation STBs will become hybrid devices, integrating video content from multiple signal sources such as broadcast television, premium video-on-demand and Internet-based over-the-top video services, providing value-added capabilities like time-shifting, and allowing content to be distributed to a variety of viewing devices including multi-room TV networks, personal computers, portable media players and other mobile devices.

However, systems which allow multiple sources of content access and portability are inherently more susceptible to piracy, and increase the complexity of security requirements. Set-top boxes and their associated conditional access (CA) systems and digital rights management (DRM) technologies are under constant threat from device tampering, software security breaches and hacker attacks that can significantly impact the reputation and bottom line for both STB manufacturers and operators.

2. Set-top box security drivers

The evolution of premium video distribution and content consumption models is driving new security requirements throughout the distribution chain.

Content distribution: content owners, such as movie and television studios, demand protection against the piracy of their intellectual property and require

that content licensees take steps to prevent piracy and to mitigate against damage should a breach occur. These security requirements form part of operator distribution agreements and translate into technical requirements for set-top box suppliers.

Input and output types: new services that combine traditional broadcast and Internet-based content necessitate a STB security architecture capable of integrating both CA and DRM protection mechanisms. Adding PVR/DVR and home media networking capabilities to enable time-shifting and content sharing between devices places additional security requirements to protect links and outputs as new use cases will require content to be passed between various protection systems.

Open platforms: several set-top box OEMs are contemplating or committing their next-generation designs to the Linux operating system which is a broadly available, widely understood open platform. The prevalence of skilled Linux “hackers” along with the large base of free software development and reverse engineering tools makes it critical that the STB manufacturers take extra precautions to protect their systems.

Lifecycle protection: defending against continuous attacks from the hacker community is an ongoing battle for STB makers and operators, and the costs of protecting systems and reacting to breaches are significant. The objective of a sound security strategy is to raise the barriers (in terms of time and money) to a level where the hacker business model is no longer financially viable.

3. Set-top box security trends

As previously stated, set-top box architectures are becoming more sophisticated through the integration of new functions and content protection systems. In this section we will examine the key trends in this area and provide a deeper understanding of the security challenges created through the integration of these technologies.

3.1 HYBRID SET-TOP BOXES

The STB industry is undergoing a rapid shift from supplying standalone cable and satellite STBs to hybrid STBs which incorporate IP-based, over-the-top video services. Traditional cable and satellite service providers are providing IP-based services, such as DirectTV-On-Demand, that are complimentary to their CA-delivered channels. Alternative business models with STBs targeted for retail sales to consumers are also emerging, where the set-top box is not tied to a cable or satellite provider but instead provides access to over-the-top (OTT) video services as an alternative to traditional video services.

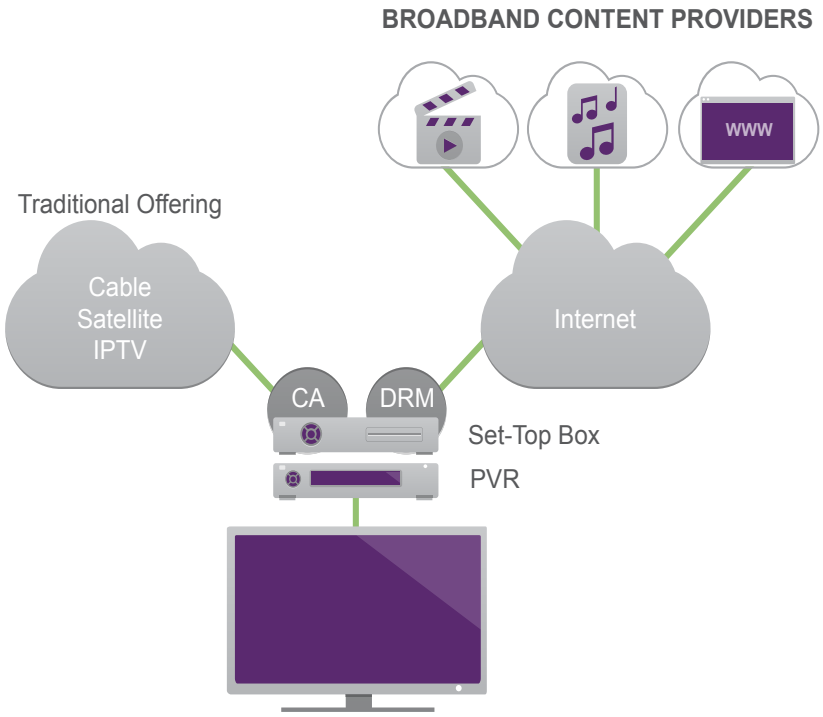

Figure 1. The hybrid STB requires protection for both traditional and Internet-based content

3.1.1 DRM REQUIREMENTS

If the service provider supports DRM-protected content as part of IPTV or premium OTT video, the STB will need to integrate DRM functionality. This is typically accomplished through licensing a common DRM (such as WMDRM-PD(7), OMA DRM 2.0(8), Microsoft PlayReady(9), or Marlin(10)) and integrating the DRM client into the STB and media framework. Along with the effort in integrating the DRM into the STB player architecture, the OEM must also ensure that the DRM implementation meets the compliance and robustness (C&R) rules of the particular DRM.

Compliance and robustness rules describe the level of protection required for encryption keys, device certificates and other assets, as well as how to correctly use and protect the content. DRM licensors stipulate the compliance and robustness rules that must be met as part of their license agreements, with heavy penalties for failure to meet these standards. Penalties for non-conformance by licensees can include contractual liabilities and license revocation, while breaches in the field often result in high costs and disruption from recalls and repairs, not to mention potentially damaging brand erosion to both STB manufacturers and operators.

3.1.2 ATTACK VECTORS

Building a set-top box that meets or exceeds the compliance and robustness rules for a DRM standard can be a daunting challenge. Pirates use an evolving mix of hardware and software hacking techniques to attack the system including using emulator cards, leveraging side channel attacks on processors, attacking hardware/software interfaces, reverse engineering software, tampering with executables, stepping through code using debugging tools, and others techniques. History has shown, that given enough time and money, a hacker can compromise any system.

3.1.3 SERVICE OFFERINGS

The selection of a DRM has significant implications for the manufacturer because it may restrict the types of services that can be offered, such as rental or purchase, and whether the content can be exported or bridged to another DRM system. To support PVR/DVR/future playback capability, the DRM must allow the content to be stored locally in the native DRM format or to be exported or bridged to another local DRM for local storage.

In summary, the hybrid STB model provides opportunities for the STB OEM to enable or offer innovative content services. Doing so requires careful attention to the choice of DRM technologies and system level security required to protect the DRM and content assets.

3.2 SEPARABLE CONDITIONAL ACCESS

Cable and satellite services have been closed networks with limited opportunity for devices such as PCs and consumer electronics devices to access content from these networks. Through specifications such as CableCARD from CableLabs and DVB-CI+, the conditional access system must be contained in a standalone “separable security device” instead of being integrated within the set-top box. In North America, as of July 2007, set-top boxes cannot contain integrated conditional access and in the EU it is mandatory that all TVs contain a Conditional Access Module (CAM) slot.

From a security perspective, the fact that the conditional access is terminated on a PCMCIA card creates some unique security challenges. The CA smart card is responsible for removing the operator-based content protection and encrypting the content into a specified format for transmission over the PCMCIA bus to the host device, such as a STB, digital cable ready TV, or PVR/DVR.

This transcription from conditional access to the interface DRM must be done securely and the security requirements for this operation are specified in the compliance and robustness rules for each standard.

For CableCARD and tru2way™, the C&R rules are found in the Cable tru2way™ Device License Agreement(11), formerly CableCARD Host Interface License Agreement (CHILA). As with other DRM systems, meeting the compliance and robustness rules typically involves protecting device certificates, encryption keys and other secrets while protecting the security code itself from modification or tampering. Non-conformance or breaches in the security may lead to contractual liabilities, device revocation and service disruption.

While separable CA modules address some needs, there are additional market, cost and technical pressures pushing CA systems to a downloadable model where the CA system can be deployed and updated as required without requiring new hardware or a service call by the operator. When software CA is deployed, the CA client on the STB must be adequately protected from software hacking as well.

3.3 DIGITAL HOME NETWORKS

Home networks, wireless access, and portable devices are pushing content beyond the TV to a wide range of network-enabled devices including STBs, digital televisions, digital/personal video recorders, personal computers, portable media players, etc. As consumers demand seamless access to licensed content from any device, STB OEMs have the opportunity to differentiate their products with innovative customer-facing features. However, increased content portability leads to higher security risks as content is now susceptible to piracy on a broader range of devices.

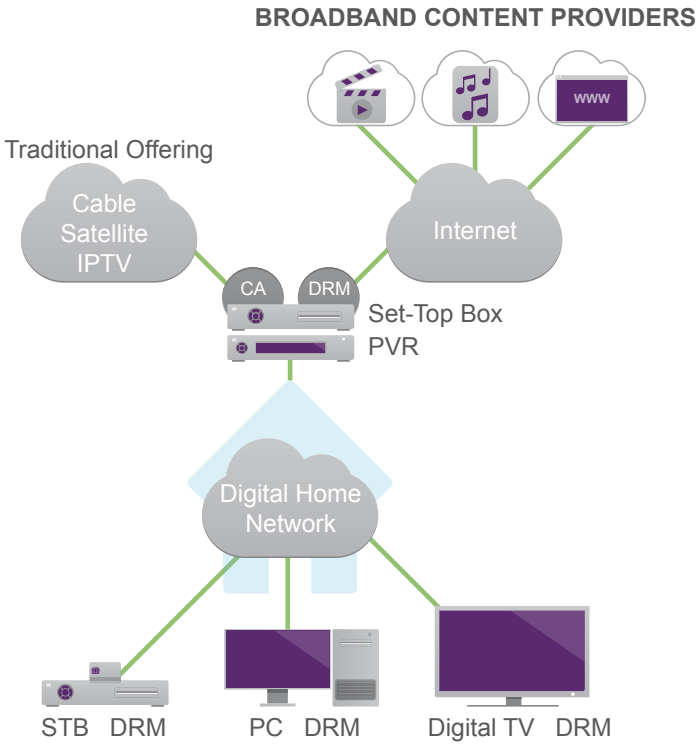

Figure 2. Digital home technologies extend content delivery to a wider range of client devices.

3.3.1 MULTI-ROOM PVR/DVR

While hybrid set-top boxes support the delivery of content from the Internet to the home, digital home-enabled STBs extend this functionality to enable premium content to be distributed to other devices in the home. Set-top box manufacturers must include additional DRM functionality on the home network side of their equipment to support either in-home streaming or the transfer of content between devices. The traditional cable and satellite models have seen tremendous success with the PVR/DVR. With this success, consumers are demanding that the PVR/DVR content be accessible on all of their televisions.

To cost-effectively enable this multi-room PVR/DVR concept, some network operators prefer to distribute a number of small, low cost, “daughter” set-top boxes that can pull the recorded programming from the larger, more expensive “mother” PVR/DVR. If the content is streamed over the home network, the

daughter boxes do not need local content storage or a separate cable card interface and therefore have a significantly lower bill of materials cost. This model also creates new security challenges such that the transmission of the content between the devices must be protected by a “link protection” DRM. Both the mother and daughter set-top boxes need to have integrated DRM functionality and the mother set-top box must be able to securely bridge the locally-protected content to the link protection DRM.

3.3.2 PC INTEROPERABILITY

The PC is often viewed as a security landmine for protected content. Unlike other “embedded” devices, which run on a relatively closed hardware platform, the PC is a completely open system where a user can freely install applications of their choosing, including hacking and debugging utilities.

This is the most difficult environment to secure because the user can easily use compilers, debuggers, memory scrapping utilities, etc. to tamper with or reverse engineer software on the PC. PC software manufacturers must use cutting-edge technologies and techniques to protect their applications from tampering. Many recent and highly publicized premium content attacks such as ACCS(12) and FairUse4WM have occurred on the PC.

For PCs to be successfully integrated into the premium content ecosystem, they must include a player application that supports the DRM technology required to access the content from the STB or other content source. In some cases the operator may want a PC application to terminate and display CA-protected content. In this case the PC may be combined with an Open Cable Unidirectional Receiver (OCUR) or Bi-directional Open Cable Receiver (BOCR) device which is responsible for removing the CA encryption and applying DRM

protection to secure the content as it is transferred over to the PC. On the PC, the complete video processing pipeline must be secure, including decryption, demultiplexing, decoding and hand-off to secure drivers. Also, the content must never pass over a user-accessible bus in compressed form. In these scenarios, the PC application and OCUR/BOCR device will leverage DRM technologies. The OCUR/BOCR device also must be concerned with meeting the compliance and robustness rules with the CableCARD interface, as well as provide secure bridging between the terminated conditional access and the outgoing DRM over the Digital Receiver Interface. If an operator or STB OEM chooses to include the PC in their digital home ecosystem, they must be aware of the security implications of doing so. If the operator or STB manufacturer designs the PC client themselves or leverages a third-party player, they must ensure that the necessary level of software protection is applied. Not adequately protecting their PC application will make the PC an easy target for the hacker community.

3.3.3 OTHER CONSUMER ELECTRONICS DEVICES

Consumers also want to access content on a variety of CE devices. They want to take their premium content with them on their laptop, portable media player or mobile phone. These usage scenarios require that the content remain protected and therefore the devices need to integrate DRM technologies. In some scenarios, the master set-top box will export the protected content to another device using a DRM. If the target device is using the same DRM, the master STB may only need to securely create a new content license for the target device. In some cases the master device may need to provide functionality to transcode and transcript the content from the local DRM to the target DRM. These scenarios must all be done securely, ensuring that the content is not exposed and the content rights are protected against tampering.

In the past, content portability was difficult to achieve due to licensing restrictions of many DRM standards and device support. Emerging DRM standards, such as PlayReady and Marlin, may improve the number of “target devices”. One way to improve interoperability is to leverage a DRM architecture that is agnostic to the specific DRM standard and which allows DRMs to be deployed “on demand” or as required by the service. This future-proofing strategy enables the business models and services to evolve without service calls or equipment replacement.

3.4 DRM STANDARDS AND WORKING GROUPS

A number of different approaches have been taken to facilitate DRM interoperability, with no clear winner or approach to date. There are a number of well known and emerging DRMs, such as OMA DRM2.0, WMDRM-PD, PlayReady and Marlin DRM, that facilitate content purchase and other business models. Additionally, there are several link protection DRMs, such as DTCP-IP and WMDRM-ND, that protect in-home

‘Broadband subscribers have reached 283 million wordwide subscribers expected to reach 570 million in 2011.’ MultiMedia Intelligence

streams. There are also framework technologies that promote in-home DRM interoperability such as Coral(13) and DVB-CPCM(14). The best choice of DRM will depend on the usage scenarios and type of ecosystem to be supported.

The Digital Living Network Alliance(15) (DLNA) aims to reduce this confusion. The DLNA is a consortium of industry-leading consumer electronics (CE) device manufacturers focused on creating guidelines that promote interoperability between devices in the digital home. The first mandate of the DLNA was to enable DLNA-compliant devices to be able to discover one another on the home

network and be able to share personal (non-protected) content such as MP3s, home movies, etc. This work resulted in the DLNA Interoperability Guidelines v1.0. These guidelines were later expanded to include more home and mobile devices and also include link protection to enable the sharing of premium content within the home. The link-protection guidelines state that devices sharing copyright-protected commercial digital content must support DTCP-IP and may support WMDRM-ND. The Content Protection Subcommittee of the DLNA is now focused on developing DLNA Guidelines in the area of DRM interoperability.

With CableLabs' approval(16) of DTCP-IP for protecting cable content and its acceptance by the DLNA and other standards organizations, many STB OEMs are actively integrating this technology into their products. While some manufacturers are using DTCP-IP as part of a proprietary solution to enable interoperability between their own devices, others are embracing DLNA and building DLNA compliance directly into the STB. As the DRM Interoperability Guidelines solidify, many consumer electronics manufacturers hope to see adoption of the guidelines into a wide range of devices, enlarging the ecosystem. Integrating these DRM technologies into the end devices will require that the device manufacturers be aware of the security impacts and be diligent in providing or ensuring that the necessary level of security has been implemented in the products. As the number of content devices increases in the operator's ecosystem, the operator must be increasingly diligent in ensuring that the devices have an adequate level of security. The strength of the ecosystem is limited to the strength of the weakest device.

4. The security challenge

The ultimate security goal of the device manufacturer is to raise the cost of hacking to a level where the hacker's window of opportunity to profit from piracy is diminished, if not entirely eliminated. The evolving STB and digital home devices present new security challenges which must be addressed by the manufacturer. To achieve sustainable device security in the STB ecosystem requires that the security solution addresses four key areas. This section will summarize these areas and describe what can be done by the manufacturer to achieve the necessary level of protection. Only by addressing all four areas can a manufacturer be prepared to safely carry high-value premium content on their devices.

4.1 INITIAL ATTACK RESISTANCE

The security challenges that exist for a set-top box OEM ultimately depend on the services and features they wish to support. The discussion of trends earlier in this document has identified a number of separate security systems that may exist in products. To provide an adequate level of initial attack resistance, each of these security systems must resist attempts to bypass them via reverse engineering or tampering. A vulnerability in any one area will result in the system being compromised.

4.1.1 SUMMARY OF SECURITY SYSTEMS

1. Separable Conditional Access System

Separable conditional access systems may exist as either hardware or software modules. In both cases, the CA system and the interface between the CA system and the device must be protected. In many instances, such as with CableCARD

and DVB-CI+, a DRM-like interface is defined between the module and host system resulting in the need to also meet compliance and robustness rules. Secure bridging is required if the content will be stored locally on the PVR/DVR or streamed over the home network via a link protection DRM.

2. PVR/DVR System

A PVR/DVR-capable STB must securely store recorded content locally in the device. The PVR/DVR sub-system often encrypts content with AES and may store and enforce usage rights associated with the content. Since the PVR/DVR is acting as a local, proprietary DRM, it must be secured in ways similar to what is outlined in DRM compliance and robustness rules. Secure bridging is required if the PVR/DVR content is streamed over Link Protection or exported via DRM to other devices in the home.

3. Over-the-Top Video DRM System

If the set-top box supports premium OTT video services, it will integrate a DRM system that must meet the compliance and robustness rules associated with the DRM standard. Secure bridging is required in situations where OTT content is streamed over link protection or exported via DRM to other devices in the home.

4. Link Protection System

If the STB supports content streaming over the home network via link protection, it will integrate a DRM system such as DTCP-IP or WMDRM-ND and must therefore meet the associated compliance and robustness rules.

5. DRM Export System

If the set-top box supports content sharing over the home network via DRM export, it will integrate a DRM system and must therefore meet the associated compliance and robustness rules.

4.1.2 SECURITY REQUIREMENTS

The security requirements of these set-top box systems can generally fit into three categories: protecting conditional access systems, meeting compliance and robustness rules; and security bridging.

CA Protection

The STB OEM will typically integrate the CA system required by the specific operator for which they are designing the box. If the CA is supplied by a third party, protection of the CA system will be the responsibility of the CA provider. If it is a proprietary CA, the STB OEM must secure it themselves either through their hardware design and/or through software techniques. To protect a software-based (soft CA) client, or the software interfaces of a CA module, OEMs can leverage third-party software security tools to add the necessary tamper resistance to the design.

DEVICE/SYSTEM	PROTECTION REQUIREMENTS		
	CA PROTECTION	COMPLIANCE AND ROBUSTNESS	SECURITY BRIDGING
SEPARABLE H/W AND S/W CA MODULES	●	●	DEPENDS ON SERVICE
PVR/DVR SYSTEM		●	●
OVER THE TOP VIDEO SYSTEM		●	DEPENDS ON SERVICE
LINK PROTECTION SYSTEM		●	●
DRM EXPORT SYSTEM		●	●

Figure 3. System protection requirements matrix

Compliance and Robustness Rules

- STB OEMs can choose to meet the compliance and robustness rules in one of three ways. The OEM can choose to develop technology and in-house software security expertise to protect the STB software and sensitive assets This is the most difficult and time-consuming option and requires that the

OEM has a strong understanding of the compliance and robustness rules, an expert understanding of software hacking methodologies and the necessary development resources to implement the security countermeasures

- For cases where the OEM chooses to integrate a common DRM, --the simplest solution is to use a pre-hardened DRM implementation which includes a DRM porting kit that has been analyzed and secured to meet the compliance and robustness rules. In such secure DRM implementations, DRM security experts have studied the compliance and robustness rules, modeled the attack tree of the code and platform, developed suitable countermeasures and applied (often patented) security techniques to ensure protection of the DRM system
- For cases where a standard porting kit is not available, or where --the OEM has their own software, they can use specialized software security tools to protect the software and assets as required

To help meet their security objectives, many OEMs use conformance and compliance testing services from DRM security consultants who can analyse the implementation and provide an independent compliance conformance report. Engaging such independent experts demonstrates due diligence in meeting the C&R rules and improves confidence in the overall security design.

Secure Bridging

Security bridging is a common requirement that may exist for many set-top box applications. The movement of content between any of the security systems will necessitate the need for secure bridging. This will include secure transcoding, transcription and usage rights mapping between security systems.

In some cases a protection system such as a DRM may have specific file-

type requirements. Transcoding is required if content is to be passed from one protection system to another that does not support the required file format. The source content, for example MPEG2, would be decoded and then reencoded into target file types such as WMV. Because this processing must be done on unencrypted content, the process must be secured to ensure that the content cannot be intercepted and stored or exported.

The method by which content is encrypted may differ between content protection systems. In cases where content is moved between dissimilar systems, the encryption will have to be changed, this is called transcription. Transcryption involves decrypting the content using one content protection system, such as DTCP-IP, and re-encrypting the content using a different content protection system such as WMDRM. Because this process exposes clear content, it must be secured to prevent the interception of unencrypted content.

Rights mapping, like content transcription, is required when content is transmitted between dissimilar content protection systems. Each content protection system typically has its own method of transmitting and specifying the user rights associated with the content. When content is bridged between two systems, the appropriate level of rights and permissions must be maintained. For example, if the source content protection system has content marked as “copy never”, it would be a security issue if the rights were changed to “copy freely” when moved to the destination content protection system. Because different systems have different rights fields or rights objects, the mapping that must take place may be complex and may be defined by the licensing authority of the source content protection system. Since usage rights are being created or modified locally, the process must be secured to ensure that the rights are mapped correctly.

To adequately secure content bridging systems requires strong expertise in software hacking methodologies and the necessary software skills to implement security countermeasures. OEMs can choose to secure their bridging systems on their own, or leverage third-party security tools that are specially designed to achieve the required results and reduce the development effort.

4.2 DIVERSITY

While some set-top box security mechanisms provide initial resistance to attack, once broken the entire installed base is compromised if the STBs are homogeneous because the same attack will work on all systems.

A security approach that leverages software diversity can prevent BORE (Break Once Run Everywhere) attacks, reducing the impact of a successful breach. Software security diversity is a mechanism where the software instances are functionally equivalent but structurally different on different devices.

Using specially designed software development tools, STB OEMs can automate the creation of these diversified software instances to enable diversity to be applied per operator, per STB version, or even for every individual STB. If a hacker manages to successfully attack one device, diversity ensures the attack will be limited in scope, multiplying the effort a hacker needs to be financially successful. Diversity essentially breaks the hacker business model.

4.3 RENEWABILITY

Software diversity can also be used to proactively prevent attacks by regularly updating the security on an operator's installed base of STBs, thus frustrating hacker attempts to crack the system. By occasionally replacing the security system with new diversified instances, attackers are forced to abandon the existing analysis.

4.4 BREACH RESPONSE

It can be argued that, given enough time and resources, any system can be hacked. Under this premise, STB manufacturers should formulate their security strategies with the assumption that the device will be compromised at some point after it has been deployed.

Once that assumption is made, the shortcomings of hardware-only security solutions become obvious. If a hardware-only security system is compromised, it usually necessitates a hardware field upgrade, which can be a very expensive and lengthy process. Even if a software-based fix for the STB can be found, the software update itself will need to be protected against tampering and reverse engineering.

To allow for cost-effective field updates, STB manufacturers are advised to implement security systems that leverage hardware security (if available) combined with a layer of software security. This strategy, with the benefits of diversity, provides a very high level of attack resistance and also enables the operator to respond quickly in the event of a breach.

5. Conclusion

New delivery and consumption models are driving the convergence of traditional video and Internet-based content onto a multitude of viewing platforms within the digital home. The technical and contractual requirements surrounding the protection of premium content on next-generation STBs is increasing the

complexity, time, expense and risk to the design and development of these devices. Trends such as hybrid set-top boxes, multi-room DVRs and separable access security multiply the choices, effort, and risks faced by STB research and development teams.

When developing next-generation STBs, OEMs should formulate and implement security strategies that address the challenges of multi-source, multi-device networked environments. To do so, OEMs must understand the security issues and vulnerabilities associated with managing both CA and DRM protected content in hostile environments where hackers have access to sophisticated reverse engineering and tampering tools. To meet DRM compliance and robustness requirements, OEMs should seek an independent conformance assessment from qualified DRM security experts. Comprehensive STB security designs to prevent content theft should incorporate security mechanisms that provide a strong level of attack resistance, use diversity to prevent automated attacks, and offer efficient security update capabilities.

6. Set-top box security solutions from Irdeto

As the leader in software security for content protection technologies and applications, Irdeto understands the challenges STB OEM's face in meeting the demands of both content providers and consumers. Our advanced protection solutions provide an advantage to developers wanting to reduce time-to-market in a highly competitive market for next-generation STB devices.

Irdeto Security Suite is a set of automated tools that enable STB software developers to secure content protection, DRM bridging and application code against reverse engineering, tampering and automated attacks.

Irdeto's pre-packaged robust DRM solutions provide STB developers with many benefits, including accelerated product development, industry leading security, and confidence in the design.

To help STB makers define an effective security strategy, Irdeto also offers a range of consulting, training and development services to guide manufacturers through all phases of the security development lifecycle, including:

- Security requirements analysis to identify potential threats and weaknesses
- Solution design and implementation to accelerate time-to-market
- Conformance testing to fulfill DRM and other licensing obligations
- Breach mitigation and management to minimize impact and protect against further attacks
- Training to educate STB development teams on all aspects of software and content protection

Many of the world's most widely recognized hardware and software companies rely on Irdeto solutions to protect content, comply with licensing requirements and accelerate their time-to-security. Contact us to find out how we can help you gain a competitive edge in the set-top box market.

SOURCES

(1) www.leichtmanresearch.com/press/091508release.html
(2) www.conference-board.org/economics/consumerBarometer.cfm
(3) www.billingworld.com/articles/telecom-service-synication-oss-bss.html
(4) www.cable-satellite.com/pdf/features/sep-oct_07/37-38-39ott.pdf
(5) www.cable-satellite.com/pdf/features/sept-oct_08/22.pdf
(6) www.ipi.org
(7) www.microsoft.com/windows/windowsmedia/forpros/drm/default.mspx
(8) www.openmobilealliance.org
(9) www.microsoft.com/windows/windowsmedia/forpros/drm/default.mspx
(10) www.marlin-community.com
(11) www.opencable.com/downloads/tru2way_agreement.pdf
(12) www.wikipedia.org/wiki/Advanced_Access_Content_System
(13) www.coral-interop.org/
(14) www.dvb.org
(15) www.dlna.org
(16) www.cablelabs.com/news/pr/2007/07_pr_dtla_082307.html