SECURITY AND SAVINGS: GOING DIGITAL AND GETTING BOTH

Alec Main
Cloakware Corporation

Abstract

Achieving cost savings while converting the analog television ecosystem to digital continues to be a difficult problem. The revenue opportunities available through the conversion of the analog bandwidth to digital are well identified, but with the continued prevalence of analog legacy systems, the path to conversion is a significant challenge. How can the industry leverage the potential revenues of digital bandwidth, while continuing to provide service to those who may not want or need the digital experience?

This paper examines a cost effective path to conversion which proposes developing a basic service set-top box (STB) that would include replacing hardware-based security solutions with a lower cost tamper-resistant software solution. This change would allow subsidized digital STB roll-out and electronic provisioning of basic services, while enforcing the rights of content providers and owners.

INTRODUCTION

The move from analog to digital networks allows cable operators to offer more services to more customers than ever before. With digital cable, multiple service operators (MSOs) can offer a host of new services such as video-on-demand, interactive television and commercial-free CD-quality music, giving subscribers greater choice, quality and control.

Taking the network all-digital frees up bandwidth to offer these new, exciting services. While subscribers report good satisfaction from digital services, the challenge for cable operators is switching over the installed base of analog users. Those reluctant to switch – who could represent the next potential wave of adopters – complain about too few digital channels, while some subscribers have no intention of switching. In the meantime, the base of subscribers who do upgrade from analog to digital can experience reduced quality on analog channels due excessive conversion (i.e., analog to digital to analog).

Consider the following broad categories of cable subscribers:

1) Premium service subscribers using digital services on a set-top box with a smart card and two-way modem.
2) Potential new digital subscribers considering upgrading to a digital STB.
3) Basic service subscribers using analog services, who may never switch to digital.

Until all of the basic subscribers switch over to the digital service, the MSO must continue to provide analog services as well as digital. The fastest way to accomplish the digital conversion – and to reap the benefits – is to entice subscribers to make the leap by lowering the price of the STB to such a point that it is easy for consumers to switch – say, $35 – or at least, to a point where an MSO can economically subsidize the box.

In order to achieve a cost-effective box, we propose boxes without smart cards or CableCARDs™ that are targeted at the basic

service subscriber. Security will be handled by secure software which is lower cost compared to hardware. The set-top box would have a unidirectional cable modem, analog TV output (converted from digital input) and use a standard remote control. There would be no hard drive or personal video recorder (PVR) capabilities and no additional outputs for home networking. It would be compatible with existing TVs and VCRs.

This paper presents the challenges and benefits of going digital using secure software:

- Dealing with currently accepted piracy levels during the transition
- Reducing the manufacturing and on-going support costs
- Realizing additional benefits of a software approach including electronic provisioning
- Making the software secure
- Dealing with legacy CAS systems

It concludes that a software-based solution is cost effective, while continuing to prevent subscription fraud.

GOING DIGITAL

Analog services tie up a significant percentage of bandwidth. Once the analog services are no longer required, bandwidth is freed up for additional premium service offerings.

However, making the switch requires some planning. Many MSOs have already moved some channels to digital, but the network infrastructure must be set to handle all-digital. The switchover must be well communicated and coordinated to ensure minimal disruption of service. The actual adding of the STB to the subscriber's premises should be very simple.

The next issue is whether to scramble basic services – the goal being electronic provisioning and eliminating truck rolls to activate or deactivate subscribers. To answer this question, we need to consider existing piracy and subsidy strategies.

A certain level of subscription fraud is tolerated today. Many subscribers have a splitter in their basement and feed multiple TVs on one subscription.

Going all-digital – whether the basic service is scrambled or not – requires a STB per TV. If the low-cost STB is not available through retail channels, then the MSO needs to consider piracy in conjunction with their subsidy strategy.

The low-end STB has a one-way cable modem and an analog output. It provides only basic services and the keys for delivering premium services are never downloaded to the box. The threat against such a box is low. However, by not addressing existing piracy, a market for grey market hacked devices will develop. A strategy is needed to consider subsidizing one or even two low-cost boxes per home, plus providing additional boxes for sale. Subscriptions can charge for multiple TVs at a reasonable price – but not so high as to stimulate a grey market. Most subscribers will want to stay legitimate given reasonable options.

Under this scenario, users would need to upgrade to another box for premium services. The basic STB could still support the Open Cable Applications Platform (OCAP), but offer a limited set of capabilities (e.g. no interactive functions). The MSO may want to consider giving subscribers the option of the

basic box, with a credit on a premium box when taking the network all-digital.

Proper planning and a strategy to address existing piracy must be in place prior to making the transition to an all-digital network in order for subscribers to legitimately obtain the services they want.

SAVINGS

How can we get the price down low enough to enable the transition to all-digital input for the basic service subscriber? We propose cutting manufacturing costs by replacing the security hardware with secure software. Software can deliver identical functionality to hardware with other added benefits.

Cost savings are realized by eliminating the CableCARD, as well as the reader within the STB. A CableCARD is a PCMCIA-like card with a smart card slot or smart-card functionality embedded. While these prices are expected to drop, they are currently very expensive. The cost of the card is covered by the MSO, and may be recouped by a small incremental monthly charge. If these cards are hacked, which is likely if satellite TV is any indication, then they need to be replaced periodically by the MSO. By eliminating these cards on a basic STB, the MSO saves initial and recurring costs, while minimizing the threat – it is very difficult for a basic services box to be upgraded via hacks to full service.

The additional major cost savings comes from using a basic unidirectional cable modem over a bidirectional DOCSIS® modem. By running the secure software in a Linux® environment, there are no additional operating system costs.

There will, however, be additional costs for the CPU and memory, but it's money better spent: this is the more practical place to add cost, since these processors support a wider variety of software and applications. The CPU could also support Open Cable Application Platform (OCAP) and this know-how can be leveraged on premium boxes where more functionality is CPU intensive, such as DTCP-IP (Digital Transport Copy Protection mechanism for use on IP networks) and PVR functions. Also, expect some additional cost for hardening the software running on the box.

The last additional cost relates to the legacy conditional access system (CAS) in place on the MSO's network. This cost is discussed later in this paper. We believe that the savings will be greater by moving to a secure software implementation, plus there are added benefits to a secure software approach.

BENEFITS OF SOFTWARE SECURITY

In consumer electronics, cost reductions typically involve the replacement of soft parts with hard parts. Integration is usually the name of the game.

Security is an exception.

Conditional access security is provided by an external component such as a smart card. The smart card is not integrated because it needs to be specific to an MSO, but also because it needs to be renewed periodically.

Software security can also be renewed, but at significantly lower cost. In addition, it is much harder to remove software from a closed box, hack it and then insert it into other boxes. Smart cards arguably help create a pirate network because of the ease of removal and distribution.

Secure software – or more specifically a secured software-oriented STB – has other benefits:

1) New revenue opportunities – operators can create new service bundles based on the ability of subscribers to download new technologies and features, even for low-end STB owners.

2) Increased flexibility – operators can meet different standards as they emerge.

3) Increased renewability – new security countermeasures can be deployed quickly and as frequently as required to the entire existing installed base faster, reducing subscription fraud and piracy. Software can be renewed selectively, proactively, or reactively.

4) Ability to upgrade – subscribers don't have to buy a new set-top box to benefit from new technologies and new features that can be downloaded.

All of these benefits can be achieved without the use of smart cards and the added costs of replacing them.

SECURITY

The rewards of the secure software-oriented STB extend well beyond reductions in cost to the MSO, but what kind of new risks are introduced to the MSO and how are they best mitigated? Any discussion on software security should include a description of the threat model. The STB scenario is called a "hostile user threat", where the legitimate user of the system may want to hack it for the purposes of subscription fraud, piracy or theft of services.

Do we even need to protect the box? Certainly the threat is not as severe as in a PC environment where the hostile user has complete control of the CPU and applications that are loaded. However, software protection steps are needed as the box will likely run a known operating system like Linux for cost savings. Regardless, tools exist to attack most computer systems, so some level of protection is prudent.

Can we just encrypt the data? Data confidentiality is only one component of the solution. The software also needs protection. Content protection standards, such as DTCP-IP, CPRM (Content Protection for Renewable Media) and HDCP (High-bandwidth Digital Content Protection), all recognize the need for software robustness.[1] The requirement for software protection is mandated by these standards.

In this case, the primary goal is to prevent subscription fraud. Since this box is for basic services only, the simplest mechanism is to make sure the box does not have the content descrambling keys or functionality required for premium services. We assume some scrambling is performed on the content and the goal is to decrypt only the appropriate channels.

Secondly, the attacker can always convert the analog output to digital (known as the "analog hole"), whereas our security goal is to prevent siphoning-off of the digital content. Again, a basic service box reduces this risk since premium content is never descrambled or available on the internal busses in the clear.

Lastly, we want to prevent the box from being used for other purposes – a form of subscription fraud common with high-end media devices such as Xbox®[2]. Since this is a basic service box with limited outputs, such threat of service is also low risk.

Since we have control of the operating system installation and software upgrades, we can consider numerous techniques to harden the system. First let's look at how software is attacked. A software attack follows this general framework:

1) Analysis – Classic reverse engineering and analysis of the software and protocols to identify vulnerabilities. This can be static analysis when the code is not running, such as disassembly and decompilation, or dynamic tracing of the executing code using debuggers and emulators. There are some more advanced and powerful forms of analysis such as collaborative and differential analysis, which we will discuss later.

2) Tampering – Modifying the code and/or data such that it performs according to the attacker's objectives.

3) Automation – The creation of scripts or code to apply the tampering attack to multiple copies of the application. These are also known as "class attacks" or "global breaks". In some cases, the tampered application must be distributed, which is less desirable from an attacker's perspective as it is more detectable and prosecutable under legal measures.

4) Distribution – Once the automated attack is created, it must be distributed in an effective, confidential means. Often bulletin boards, Internet Relay Chat (IRC) and peer-to-peer networks (P2P) are used for this purpose.

The first goal is to make analysis and tampering difficult, time-consuming and/or expensive. The obvious approach to prevent static analysis is to encrypt the binary. However, there are many techniques to extract these decrypted executables from memory. However, there are also techniques that prevent static analysis such as control flow flattening which introduces pointer aliasing that can only be resolved at runtime. There are specific decompilation and disassembly prevention techniques that target these tools. Note that while very powerful disassembly tools exist, most low-level code written in C or C++ is very difficult to decompile with only a few tools available. Software protection is about using multiple layers of defense and all these techniques should be considered.

Runtime analysis of a system can be prevented or made very expensive by the use of anti-debugger and anti-emulation techniques. A range of techniques unto themselves, these can be effective on platforms where the operating system and applications are known in advance – such as with our basic STB. In this case, the code can be tied to the platform via node locking and loading of new applications controlled by secure code signing techniques. Advanced just-in-time decryption (or self-modifying code) techniques also raise the bar against dynamic analysis. Authentication of components on the machine and encryption of communication channels with protocol not subject to replay attacks also prevent analysis. In addition, data transformation techniques can be used to hide and randomize data values even when operated on within main memory. White-box cryptography refers to specific cryptographic implementations designed to prevent key extraction even when the operation can be viewed by an attacker.

Static tampering is prevented with binary encryption techniques, as well as by introducing data dependencies in the code to change an easy branch jamming attack into tampering – increasing the effort required and involving multiple changes to the code. An important technique to prevent tampering is code signing, but the code signing mechanism itself will be subject to attack and so must also be suitably hardened. Integrity

verification of applications should be done statically (on-disk) as well as in-memory to prevent dynamic tampering attacks.

Prevention of automated attacks is best achieved by deploying code and data diversity such that a successful attack will only work for a sub-set of users. Diversity of code is a result of most software protection techniques outlined above. It is similar to having different keys (diversity of data) for different users. Diversity of code recognizes that attacks will be on the software in addition to the data. Automated attacks are also mitigated by software renewability, which can be made low cost – if designed in upfront. Conversely with hardware based security, renewability is a major cost. Software can be renewed selectively, proactively, or reactively – depending on the strategy and the attacks to the specific system.

Diversity is a prerequisite for successful renewability; otherwise attackers will perform differential analysis. This is a powerful attack used to quickly determine the changes made to software upgrades and shorten the time to successful hack.

LEGACY CONDITIONAL ACCESS

In North America, the vast majority of conditional access systems for cable are provided by Motorola or Scientific-Atlanta. In order to integrate a software based low-end STB, there are three options:

1) License the CAS system from Motorola or Scientific-Atlanta (e.g. as done by Digeo[3] and others)

2) Utilize Sony Passage[4] to run an additional CAS over top the legacy CAS.

3) Roll-over to a new CAS during the all-digital transition.

The disadvantage of Sony Passage is that the MSO must make changes to their head end. The Sony Passage system consumes 2% to 10% additional bandwidth, but this will be amply compensated for by going all-digital. There are a number of new players[5] providing software-based CAS that can work with Sony Passage or independently.

CONCLUSION

This paper has described a secure and cost effective path to migrate analog cable users to digital services.

For the basic service subscriber, we can achieve a cost-effective box without smart cards or CableCARDs. The set-top box would have a unidirectional cable modem, analog TV output (converted from digital input), and would be compatible with existing TVs and VCRs.

Secure software can effectively address the challenges of going digital and provide additional benefits. These challenges include legacy conditional access systems, dealing with piracy and reducing overall cost.

Proper planning and a strategy to address existing piracy must both be in place prior to making the transition to an all-digital network.

The other benefits of implementing a low cost STB employing secure software include new revenue opportunities, increased flexibility, increased renewability, and a cheaper upgrade path.

All of these benefits can be achieved without the use of smart cards and the added costs of replacing them.

We conclude that a software-based solution is cost effective, while continuing to prevent subscription fraud.

TRADEMARKS

CableCARD is a trademark of Cable Television Laboratories, Inc.

DOCSIS (Data Over Cable Service Interface Specification) is a registered trademark of Cable Television Laboratories, Inc.

Linux is a registered trademark of Linus Torvalds.

Passage is a trademark of Sony Corporation.

Xbox is a registered trademark of Microsoft Corporation.

END NOTES

1) See: Hitachi, Ltd., Intel Corporation, Matsushita Electric Industrial, Co., Ltd., Sony Corporation, Toshiba Corporation; "5C Digital Transmission Content Protection, White Paper"; July 14, 1998; http://www.dtcp.com/data/wp_spec.pdf

2) See: xbox hackz Website; http://www.xboxhackz.com/; 2002

3) See: Digeo Inc. Website ; http://www..digeo.com; 2004

4) See: Sony Passage Website; http://www.sonypassage.com; 2004

5) See: Latens Systems Ltd. Website; http://www.latens.co.uk/html/cable.html; 2004.

REFERENCES

1) Bar-Haim, Pam and Wald, Stephanie, NDS Ltd.; "The NDS Guide To Digital Set-Top Boxes: Third Edition"; 2002. See: http://www.broadcastpapers.com/data/NDSGuideSetTopBoxIndex.htm

ABOUT THE AUTHOR

Alec Main (alec.main@cloakware.com) is Cloakware's Chief Technology Officer.

He has spoken at key forums and conferences including Copy Protection Technical Working Group (CPTWG), Media Summit, RSA, the Intel Developer Forum, Information Highways, and Certicom – PKCS.