IPTV Security
Protecting High-Value Digital Contents

David Ramirez
Alcatel-Lucent, UK
IPTV Security
I would like to take this opportunity to give special thanks to Luis Eduardo Niño for taking a chance and trying my ideas, even if they were based more on hope and ambition than on experience.

Also, I would like to give special thanks to Ramon Alonso Jaramillo for seeing beyond the obvious and allowing me to learn, and to Carlos Mario Toro and John Cuervo who guided my work and shared my enthusiasm for security.
This page intentionally left blank
Contents

Preface xv
About the Author xvii

1 Introduction to IPTV 1
1.1 Introduction 1
1.2 General Threats to IPTV Deployments 3
  1.2.1 Access Fraud 4
  1.2.2 Unauthorized Broadcasting 5
  1.2.3 Access Interruption 5
  1.2.4 Content Corruption 6

2 Principles Supporting IPTV 9
2.1 History of Video and Television 9
  2.1.1 Television 10
2.2 Viewing Experience of Video 15
  2.2.1 Line Scanning 15
  2.2.2 Video Resolution 15
  2.2.3 Number of Pictures per Second 16
  2.2.4 Aspect Ratio 16
  2.2.5 Video Compression Method 16
2.3 Video Compression 16
  2.3.1 MPEG-2 17
  2.3.2 H.263 18
  2.3.3 MPEG-4 18
2.4 TCP/IP Principles 19
  2.4.1 Addresses 19
  2.4.2 Routing 20
    2.4.2.1 IP Packet 20
2.5 Summary 21
References 22
Bibliography 22
# Contents

3 **IPTV Architecture** 23

3.1 High-level Architecture 23

  3.1.1 Service Types 25

3.2 Functional Architecture for the IPTV Service 25

  3.2.1 Content Provision 26

  3.2.2 Content Delivery 26

  3.2.3 IPTV Control 26

  3.2.4 Subscriber Functions 26

  3.2.5 Security 27

3.3 Detailed IPTV Architecture 28

  3.3.1 Head End (IPTV Service Provider) 28

    3.3.1.1 Critical Elements of the Head End 29

    3.3.1.2 Content Input 30

    3.3.1.3 MPEG Video Encoder 32

    3.3.1.4 IP Encapsulator 33

    3.3.1.5 Video Transcoder 34

    3.3.1.6 Content Management Server 34

    3.3.1.7 Video Repository 35

    3.3.1.8 Digital Rights Management 36

    3.3.1.9 Video Streaming Server 37

    3.3.1.10 Subscriber Interaction 37

  3.3.2 Transport and Aggregation Network (IPTV Network Provider) 40

    3.3.2.1 RP and RTSP 49

    3.3.2.2 RTSP 49

    3.3.2.3 Ismacryp 51

    3.3.2.4 PIM 52

    3.3.2.5 MSDP 53

    3.3.2.6 DSM-CC 53

    3.3.2.7 Internet Service Provider 53

    3.3.2.8 DSLAM 53

  3.3.3 Home End (Subscriber) 57

    3.3.3.1 Set Top Box 58

3.4 Summary 61

References 62

4 **Intellectual Property** 63

4.1 Introduction 63

4.2 Supporting Technology 73

  4.2.1 Symmetric Key Cryptography 73

  4.2.2 Asymmetric Key Cryptography 74

  4.2.3 Hybrid Encryption 74

  4.2.4 Hash – Digest 74

  4.2.5 Commonly Used Algorithms 75

  4.2.6 Public Key Infrastructure and ITU-T Recommendation X.509 76

  4.2.7 Operation of PKI 80

  4.2.8 Secure Socket Layer and Transport Layer Security 81

4.3 General Mechanisms for Content Protection 82

  4.3.1 CPS 82

  4.3.2 CAS 83

  4.3.3 DRM 83
4.4 Operation of DRM on IPTV

4.4.1 DRM Applied to VOD

4.4.2 DRM Applied to Broadcast TV

4.4.3 Smart Cards and DRM

4.4.4 Storage Protection

4.4.4.1 VCPS

4.4.4.2 CPRM/CPPM (CPSA)

4.4.5 Open DRMs

4.4.5.1 SDMI

4.4.5.2 OMA DRM

4.4.5.3 DMP

4.4.5.4 MPEG21

4.4.5.5 MPEG21 REL Data Model

4.4.5.6 DVB-CPCM

4.4.5.7 DVB-CBMS

4.4.5.8 PERM

4.4.5.9 DCAS

4.4.5.10 DReaM

4.4.5.11 OpenIPMP

4.4.5.12 OpenCA

4.4.5.13 PachyDRM

4.4.6 Interoperability Proposals

4.4.6.1 Coral

4.4.6.2 DMP

4.4.6.3 SmartRight

4.4.6.4 SVP

4.4.6.5 OpenCP

4.4.6.6 OMArlin

4.5 Watermarking and Fingerprinting

4.5.1 History

4.5.2 Steganography Techniques

4.5.3 Watermarking and Fingerprinting Principles

4.5.4 Typical Attacks

4.5.5 Forensic Use of Digital Fingerprints

4.6 WWW? (What Went Wrong?)

4.6.1 Introduction

4.6.2 Satellite Television

4.6.3 DVD Protection

4.6.4 AACS on Blue-Ray and HD-DVD

4.6.5 Videos Over the Web

4.7 Authentication

4.8 Summary

References

Bibliography
5.4.2.3 STB Platform SW 148
5.4.2.4 DVR/PVR 148
5.4.2.5 STB Credentials 149
5.4.2.6 Digital Certificate (Software Provider) 150
5.4.2.7 STB Digital Certificate 150
5.4.2.8 Public Keys (Used for Digital Certificates) 151

5.4.3 STB User Storage 151
5.4.3.1 Downloaded Content 151
5.4.3.2 User-created Content 152
5.4.3.3 STB Smart Card 152
5.4.3.4 STB Credentials 152
5.4.3.5 STB Digital Certificate 153
5.4.3.6 STB High-definition Output Interface 153
5.4.3.7 DVI 154

5.4.4 Residential Gateway 154

5.4.5 DSLAM 154
5.4.5.1 Audience Metering Information 154
5.4.5.2 Fraud Control Information 155
5.4.5.3 IP Filters 155

5.4.6 Broadcast/Multicast TV VLAN Service 156
5.4.6.1 Decryption Keys 156
5.4.6.2 CWMP 157
5.4.6.3 NTP/SNTP 157

5.4.7 Broadcast/Multicast TV Application 158
5.4.7.1 MPEG-2 and MPEG-4 Video Stream 158
5.4.7.2 DSM-CC 158

5.4.8 Middleware Application 158
5.4.8.1 EPG 158
5.4.8.2 Menus 159
5.4.8.3 Subscriber Credentials 159
5.4.8.4 Purchasing Information 160
5.4.8.5 Digital Certificates (Content Provider) 161
5.4.8.6 Parental Controls 161
5.4.8.7 PVR/DVR Application 162
5.4.8.8 User-sourced Content 162

5.4.9 Application Management 163
5.4.9.1 IPTV Usage Information 163
5.4.9.2 IPTV Billing Information 164

5.5 Conclusion 165

6 Countering the Threats 167
6.1 Securing the Basis 167
6.1.1 Hardening Operating Systems 167
6.1.2 Business Continuity 172
6.1.3 Intrusion Detection/Intrusion Prevention 173
6.1.4 Network Firewalls 174
6.1.5 Fraud Prevention 175
6.1.6 DRM–CAS 176

6.2 Head End (IPTV Service Provider) 176
6.2.1 Critical Elements of the Head End 176
6.2.2 Content Input 177
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2.2.1.1 The SAML Process</td>
<td>218</td>
</tr>
<tr>
<td>A2.2.1.2 Reviewing Existing Standards</td>
<td>220</td>
</tr>
<tr>
<td>A2.3 Applicability to an IPTV Security Environment</td>
<td>220</td>
</tr>
<tr>
<td>A2.3.1 Internal Applications</td>
<td>220</td>
</tr>
<tr>
<td>A2.3.2 Set Top Box Security</td>
<td>221</td>
</tr>
<tr>
<td>A2.4 Video on Demand</td>
<td>221</td>
</tr>
</tbody>
</table>

### Appendix 3 Barbarians at the Gate

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3.1 Barbarians at the Gate</td>
<td>223</td>
</tr>
<tr>
<td>A3.2 How to Break an IPTV Environment</td>
<td>224</td>
</tr>
<tr>
<td>A3.3 Network Under Siege</td>
<td>224</td>
</tr>
<tr>
<td>A3.3.1 Confidentiality</td>
<td>224</td>
</tr>
<tr>
<td>A3.3.2 Integrity</td>
<td>225</td>
</tr>
<tr>
<td>A3.3.3 Availability</td>
<td>225</td>
</tr>
<tr>
<td>A3.4 Countermeasures</td>
<td>225</td>
</tr>
<tr>
<td>A3.4.1 Set Top Box</td>
<td>225</td>
</tr>
<tr>
<td>A3.4.2 DSLAM</td>
<td>226</td>
</tr>
<tr>
<td>A3.4.3 Routing</td>
<td>227</td>
</tr>
<tr>
<td>A3.4.4 User Segregation</td>
<td>228</td>
</tr>
<tr>
<td>A3.4.5 Quality of Service</td>
<td>228</td>
</tr>
<tr>
<td>A3.4.6 Virtual Networks and Virtual Circuits</td>
<td>229</td>
</tr>
<tr>
<td>A3.5 Conclusion</td>
<td>229</td>
</tr>
</tbody>
</table>

### Index

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>231</td>
</tr>
</tbody>
</table>
This page intentionally left blank
Preface

Paraphrasing the famous quote from Karl Marx, I would say that television is the opium of the masses. If we have any doubts, we just need to look at the number of people glued to the TV every day. I fully understand this inclination. When I was young I spent most of my time looking at the world through the TV. Many images and sounds that now as an adult I try to revisit in person. For many of us, black-and-white TV is still a memory (not just a scary story or an urban myth!). We lived with just a few TV channels that started in the morning and by late afternoon were finished. Only in recent years have we had access to cable packages with hundreds of channels and basically any topic we may want to see.

For many years, TV has been a central mechanism for sharing culture. Although books, music and radio are helpful in bringing an insight into other worlds, audiovisual messages are more powerful and gain more attention from the audience. TV is also cheaper than live performances, and the audience is constantly growing as the number of TV sets per family increases. In many countries, TV channels are closely controlled by the political power, which ensures that only acceptable contents are presented to the public. New technologies may change this environment, allowing subscribers to choose what they see and select from different sources worldwide.

Being a TV fan, it was very interesting to get involved in the topic of IPTV. It was almost by accident that I was requested to write a chapter for an IPTV book in 2005. I had to jump head first into the subject and learn as much as I could about IPTV. One of the conclusions from my initial research on the topic was that information was limited, mostly linked with specific products, and some information lacked structure. This is a common situation with new technologies – there are very clever people developing the technology and they have little time to share all the details with the world.

I expanded the topic of IPTV in my MSc dissertation and, as a result of this additional research, concluded that writing a book on the specific aspects of security could be a positive contribution for those interested in the subject. The writing process became a very interesting journey as I was faced with the challenge of structuring in a coherent way a number of separate areas that span different knowledge domains. I tried to replicate my learning process in the book, bringing together all the diverse subjects that form IPTV in a single document that would allow the reader quickly to gain insight into the components and interactions within IPTV environments.
In general, most of the information available on the subject was either related to particular products or was work in progress expected to become a standard in the future. The book intends to provide detailed information about the different elements that comprise the IPTV environment, filling in some of the gaps left by available information.

The most exciting part of exploring IPTV is realizing how subscribers will have the power to control most aspects of their viewing experience. It may not start with the death of television as we know it, but in years to come subscribers will be able to choose exactly when and what type of content they want to access. Today we have a few IPTV deployments worldwide, and these are slowly gathering momentum. This technology will definitely become an alternative to satellite and cable.

Moreover, as we have seen with many other technologies, the first versions do have security vulnerabilities. More specifically, IPTV is a highly complex environment that brings together technologies from many different vendors, and this increases the potential for security problems. The journey of exploring the security of the IPTV environment clearly shows that there are hundreds of potential points of failure. Many components can become the weakest link and allow intruders to have access to digital assets or components within the IPTV environment.

Hopefully, this book will help security professionals gain a broader picture of the challenges and tools available to secure the environment and ensure that security incidents are reduced and controlled.
David Ramirez
Senior Manager
Alcatel-Lucent Services

David Ramirez has been involved with information security for the past 13 years. He began his career as a networking specialist and then joined a consulting company managing information risk management practice where he was involved in risk assessments for more than 80 companies. His next move was to a risk management company in the UK, as part of their new information security division. In that role, Ramirez was responsible for developing the methodologies for the practice, including penetration testing, ISO 17799 compliance and disaster recovery. He was involved in security projects for banks and other financial institutions around the world. The projects focused on security awareness, disaster recovery and business continuity, security policies, security architecture, managed security services and compliance with international standards.

Ramirez is a member of Alcatel-Lucent’s security consulting practice. His responsibilities include innovation and technology, thought leadership and knowledge sharing.
1

Introduction to IPTV

1.1 Introduction

Television is one of the inventions that has shaped the way society and culture has evolved in the past 60 years. Back in 1940, the first commercial television broadcast started a revolution, showing people of all ages how others lived outside their towns and cities. Television had a powerful effect, shrinking the world and creating a unified view of how things were.

In 1969, ARPANET was created, and a new stage in communications started. Then, in 1983, the core protocol of ARPANET went from NCP (Network Control Protocol) to TCP/IP (Transfer Control Protocol/Internet Protocol) and the Internet was born.

Both the TV and the Internet have revolutionized the way we live. We now have TV channels providing information 24 hours a day, and the Internet facilitating both communication and commerce. Several common areas between the two have finally drawn the technologies into merging, creating IPTV (Internet Protocol Television).

There are some differences between IPTV and IP video. Although the two terms are very similar, there is a clear distinction in the way the market is using the two. IPTV can be used to refer to commercial offerings by service providers with very close access to the subscriber and offers a number of TV channels with a similar look and feel to standard television. IP video is more common within websites and portals, offering downloadable contents and, in some cases, even TV shows and movies downloaded on demand. If it has a number of channels and acceptable quality, it would be called IPTV.

IPTV is a new technology that enables much more flexibility to manage contents and facilitates direct interaction with the sources of content, improving the feedback and future planning. The customer experience is greatly improved by allowing more control over the type of contents immediately available, as well as two-way communication with content providers.

A few years ago, another new technology shocked the entertainment industry – the infamous Napster enabled people to share music and movies in an unprecedented way. With
this technology it was not just the case of a neighbor lending a VHS tape with an old movie. With Napster, people shared prerelease albums and videos, creating significant losses for the music industry and movie studios.

Napster was eventually shut down in 2001, but several peer-to-peer (P2P) networks appeared and the phenomenon grew dramatically, reaching millions of users worldwide. Checking e-mule would confirm an average user base of 600–900 million users worldwide.

At the same time, several providers have started to offer legal downloads to the general public. Anyone can buy music and video files. The entertainment industry has added digital rights management (DRM) capabilities to the files and applications used to reproduce the contents, which enables a sustainable model for sales of digital content. Recently, some online stores have even removed DRM to calm the complaints from their subscribers related to fair use of the contents. Users feel that, once they have paid for content, they should be able to enjoy it on any device, and DRM is blocking that fair use possibility.

The recently born IPTV industry will need to address the same issues that once affected the digital media distributors. Customers tend to share information, and over the years there have been a number of very clever pieces of software that enable people to share information and content. A recent example of the phenomenon is Freenet, a reportedly headless network of nodes, storing encrypted sections of content and sending it to anyone who requests a particular piece of data. With Freenet it is very difficult to find who is sharing illegal material, and hence the enforcement of intellectual property rights and copyright restrictions becomes more difficult.

One of the main risks faced by the industry is the rise of thousands of ‘home-made stations’ willing to broadcast DRM-protected contents. One example of the technology that will come in the future is VideoLAN. This software enables multimedia streaming of MPEG-2, MPEG-4, DVDs, satellite and terrestrial TV on a high-bandwidth network broadcast or unicast. If Freenet and VideoLAN meet, then there will be thousands of encrypted stations broadcasting content outside any control of regulators.

However, the IPTV industry not only has DRM and content protection issues, customers are used to an always-on service with consistent quality. IPTV would have to maintain high levels of availability to convince subscribers that this is a viable option.

With a worldwide trend in privacy protection laws, all the information sent and received from the customer must be protected from third parties trying to capture information. The wireless LAN/WAN markets are a prime example that bad publicity happens to good people. IT managers are not purchasing the technology because of fear, uncertainty and doubt around the potential risks of deploying wireless networks.

Many problems that have affected the cable and satellite industry in the past will gradually migrate to the IPTV service providers, with the increased impact of IPTV providing a two-way communication that includes logical paths connecting TVs to the Internet, and with that environment come computer worms and viruses. IPTV service providers must ensure that subscribers are not able to attack the servers providing contents, and also protect subscribers from the Internet and other subscribers. Most importantly, the shared infrastructure with other services has to be protected.

All those risks and threats must be addressed to achieve a profitable business model. The following chapters of this book will cover some of the basic measures required to implement IPTV security.

Chapter 1 will cover an initial reference to threats to IPTV infrastructures, including known attacks and effects on the IPTV solution.
Chapter 2 will cover references to the IPTV architecture, operation, elements and known requirements. This will provide the novice with background to understand the technology.

Chapter 3, under the title of Intellectual Property, will cover the requirements that content owners have placed on service providers to protect contents from unauthorized access.

Chapter 4 provides a technical overview of the threats faced by IPTV and how these can affect the infrastructure and applications.

Chapter 5 is based on the International Telecommunications Union (ITU) X.805, a standard that covers end-to-end security for communication networks.

Chapter 6 will provide a summary of the technology, threats and countermeasures.

The material found in this book will allow readers to understand the basic concepts supporting IPTV and existing threats to the IPTV environment, and will provide a structured approach to defining what countermeasures are relevant and required for the appropriate protection of the IPTV environment.

1.2 General Threats to IPTV Deployments

IPTV market growth and adoption is benefiting from the increased bandwidth available as part of new broadband services on a number of different technologies. DSL, cable, mobile phones and WiMax are just a few examples of the type of technologies now offering enough bandwidth for acceptable service levels and customer experience.

It is important to remember that the IPTV business model is based on the general public being able to access intellectual property owned by third parties and being distributed by service providers. Both content owners and service providers derive their revenues from the secure operation of the service. If content were disclosed in digital form and full quality, then the potential revenue would be greatly reduced. The symbiotic relationship between content owners and service providers depends on the use of technological mechanisms to reduce the risk of unauthorized release of the digital media. Most cases include the use of DRM and other security solutions to ensure control over the distribution and access.

What are the threats, risks and vulnerabilities that the industry is trying to overcome?

There are two main areas of concern:

1. The underlying communication technology used to send the content to the subscribers. This is composed of the networking equipment and communication equipment linking the display to the source of data.
2. The second area is the IPTV-related equipment. This is a series of elements designed to operate the IPTV service and provide access and information to enable the service to operate.

Compared with traditional voice/data networks or cable TV infrastructure, threats to an IPTV environment are far more severe. The whole environment can be affected by a single computer worm. IPTV environments are formed by homogeneous hardware and software platforms. In most cases, one or two operating systems would be used for all the set top boxes deployed, but, if a computer worm were to affect the network, then a minimum of 50% of all set top boxes (and subscribers) would be out of service for a period of time. Carriers also need to ensure that quality of service is protected to comply with customer’s expectations and service level agreements (SLA).
Those two main areas of concern can be translated into specific threats and risks to the IPTV service.

### 1.2.1 Access Fraud

Access fraud is one of the oldest forms of fraud within premium/paid TV. This situation happens when an individual circumvents the conventional access mechanisms to gain unauthorized access to TV contents without paying a subscription or increasing the access granted.

An example of the type of threats faced by IPTV vendors comes from the satellite TV industry. For years they have been fighting access fraud. The widespread nature of fraud has caused, during recent years, some satellite TV companies to start taking legal action against defendants for unauthorized access to TV content. A whole industry was developed around the provisioning of modified access cards allowing unlimited access to TV packages and eroding the revenue of satellite TV vendors.

The experience of the satellite TV industry shows that fraudsters go to great lengths to break the existing security measures. This includes cracking the smart card protection used for the set top boxes and distributing cloned ‘free access’ cards. Even though the satellite TV providers modified the cards, fraudsters have managed to find alternative ways to break the safeguards incorporated in the new releases, and this cycle is repeated constantly.

Now that video technology has entered the IP world, the level of threats has escalated – vulnerabilities that have been solved in other, more mature technologies are still part of the new IPTV systems. There is a recent example of a major TV provider stopping their online content distribution owing to security vulnerabilities being found and exploited on the digital rights management technology protecting the content. There could be numerous vulnerabilities discovered on IPTV systems while the infrastructure reaches a higher maturity level. It is important to ensure that the underlying platform has the state of the art in relation to security mechanisms and procedures. This will add protection layers to the environment and will limit the effect of vulnerabilities discovered.

Another relevant example is the constant battle between cable operators and users. In many cases, cable modems have been modified to uncap the access to the network. This situation is presented when someone has access to the configuration function of the cable modem via the software interface or, in some cases, even access to hardware components within the cable modem and the bandwidth and other restrictions are removed. There are sites on the Internet where modified cable modems are offered, as well as kits and instructions to modify the configuration and remove the bandwidth limitations.

IPTV is transferred not only to set top boxes but also to computers and handheld devices. This facilitates the process of breaking the security of contents. Intruders could manipulate or modify the behavior of their IPTV client and extract the content in digital form ready to be copied or broadcast. Simple software modifications introduced by hackers allow them to break the encryption system and other security measures, or even capture and redistribute the contents using peer-to-peer networks.

The main fact related to access fraud is that, in order for an IPTV system to work, end-users have to be provided with the encrypted content, encryption algorithm and the encryption keys. Anyone familiar with these technologies will tell you that you have lost the game at that point as you no longer have control over the content. Historically, these
types of environment show that eventually someone will be able to break the protections and release the content.

Access fraud is reduced greatly by the implementation of different technologies intended to block any attempt at unauthorized access, for example:

- The STB has a DRM client needing to liaise with the DRM application to receive the valid keys for the content. Any third party with access to the content will not be able to decrypt the information as no valid keys have been issued for them.
- Communication with the middleware servers is protected using SSL, and STBs can be authenticated, ensuring that only valid systems are accessing the content.
- DSLAMs are able to validate that only valid subscribers are able to connect to the network and communicate with the middleware servers. The physical line used for access to the network is mapped with the MAC and IP address used by the subscriber and is validated to ensure authorized access. The DSLAM will block any access between systems, avoiding peer-to-peer connections that may result in hacking incidents or unauthorized access to content.

1.2.2 Unauthorized Broadcasting

IPTV contents are distributed in digital format, simplifying the work of any individual with an interest in copying or broadcasting the contents. One of the arguments in the campaign against movie piracy is that bootleg DVDs tend to be recordings made at the cinema by people using handheld cameras. However, with digital content broadcast as part of an IPTV service there is no difference between pirate and original content.

A major impact on the satellite TV industry has been fraudsters selling modified ‘all access’ smart cards based on modifications to valid smart cards and receivers. If fraudsters are successful at the same type of attack within an IPTV environment, they will be able to create ‘all access’ IPTV set top boxes or cards. As a result, the IPTV industry faces an entirely new threat – with broadcasting stations residing on every home PC, hackers would be able to redistribute the broadcast stream to other computers all over the world. There are some known cases where individuals have offered redistribution of sport events, charging interested people a small fraction of the commercial cost of accessing the content.

Taking as an example the widespread effect of peer-to-peer networks and how easy it is to use one of these environments to distribute large amounts of data, it is technically feasible to set up a peer-to-peer network used to distribute broadcast IPTV content. One single source could be used to deliver contents to nonpaying viewers around the world. This is a clear danger to the business model followed by content owners and service providers.

1.2.3 Access Interruption

Television is a service that people take for granted – the public expects to click the button and get something on the screen. If an intruder were able to damage the infrastructure or
one of the service components, then customers would loose access to their services, causing a loss of confidence in the service. Cable operators offer a pretty much reliable service, and customers would compare the reliability of IPTV networks against other solutions.

Security and reliability must be built into the architecture to ensure that the service is always available and any interruptions are quickly solved.

The way most IPTV solutions are deployed creates a number of risks, especially from fast-replicating attacks such as the ones from worms and viruses. A worm capable of attacking the set top boxes could bring down several hundred thousand boxes in seconds and, properly coded, would cause an outage of weeks while technical support people recovered the boxes to their original state. Similar attacks could be launched against web-based middleware servers, leaving all viewers without access to their electronic programming guide.

STBs tend to have the same operating system within a particular service provider. If the central server were infected by a worm or virus, it would be a matter of seconds before all STBs were infected, easily bringing the service down.

The major weaknesses within the IPTV environment, related to access interruption, are as follows:

- Middleware servers, even if deployed in a high-availability environment, are a single point of failure. If vulnerability were exploited on the servers, then intruders could shut down the middleware servers.
- Denial of service is also a major risk within the middleware servers. If there are no appropriate mechanisms, intruders could send a number of invalid requests to the middleware server, blocking access by valid users.
- DSLAMs tend to have the same operating system. If an intruder is capable of affecting the configuration of a number of DSLAMs, then thousands of users would be left without service. An additional problem is that some DSLAMs tend to be deployed in rural areas with limited access by support personnel, and recovering service may take from several hours to several days.
- STBs tend to run known operating systems, and a worm exploiting vulnerability on those systems could shut down all STBs simultaneously, even disabling the STB permanently until a technician has physical access to the system.
- Residential gateways present the same type of risk. A massive attack could shut down all RGs and leave customers without access.
- There are similar risks within the IPTV core components. For example, if an intruder were to disable the broadcast server or video-on-demand server at the regional head end, thousands of subscribers would loose access to the server. This is valid for the DRM and other IPTV components at the head end. In general, the whole infrastructure should be designed following an approach of high availability.

1.2.4 Content Corruption

The resources and funding required to broadcast over-the-air fake signals are so large that this is something usually left for military use. There are no frequent cases of people starting their own TV station and blasting their message to large regions of a city or even across cities. Cable operators have to their advantage that any modification to the signal requires physical access and can be easily tracked.