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

IPTV Security: Protecting High-Value Digital Contents David Ramirez

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. A valid subscriber could take digital content and use peer-to-peer networks to distribute the high-quality content to a large audience, eliminating the need for those viewers to pay for the content or maintain any subscription to commercial TV services. All the technology pieces are available for this situation to arise.

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.

On IPTV, a different environment is presented as the signal is being sent using normal IP protocols and intruders could connect via the web and manipulate the middleware or broadcast servers. It is also possible to change the data within the content repository before it has been encrypted by the DRM software. An intruder could manipulate a particular movie or content and cause the IPTV provider to broadcast inappropriate or unauthorized content.

Content has to pass through different intermediaries before it is sent to subscribers. There are three main sections of the journey between the content providers and the subscriber:

1. There is an initial path between the content owner (or its agent) and the service provider operating the IPTV service. This can be via satellite, Internet or magnetic media. Any of these can provide an opportunity for unauthorized modification of the content. In some cases encryption is used, but there can be cases where this protection is broken, in particular if there are no appropriate mechanisms to update and manage the keys.
2. Content is then stored by the service provider at the content database, allowing an opportunity for unauthorized access by intruders or employees who could modify the contents. Disgruntled employees could have access to the database and modify the content either by editing or replacing the files.
3. The last stage is the transport between the regional head end and the STB. If there are no appropriate protections, the content could be modified or new content released to the subscribers. Intruders could attempt to insert broadcast traffic to be received by STBs, trying to have STBs displaying the fake content to subscribers.