RESEARCH ARTICLE   OPEN ACCESS

Internet Protocol Television (IPTV) and its Security Threats - An Overview

V.Vasanthi[1], M.Chidambaram[2]

Research Scholar[1], Research and Development Center
Bharathiar University, Coimbatore
Assistant Professor[2], Department of Computer Science
Rajah Serfoji Govt. Arts College, Thanjavur
Tamil Nadu - India

ABSTRACT

The digital technologies have completely transformed with the introduction of IPTV which fuses telecommunication and digital television delivery services together. Another revolution is that the user will be capable to have a bidirectional communication, the ability to interact with the service provider and enjoy high quality end-to-end service, for example if the user requests content from the EPG (Electronic Program Guide) which acts as an interface to access the IPTV service, then the desired program is delivered. The IPTV service affords rich multimedia services over a measured IP network. IPTV end users are increasing day by day as it is offering attractive features online with technological advancements. The paper gives an overview of IPTV, its working, offered services and its security threats.

Keywords:- Set-top box (STB), VoD (Video on Demand)

I.   INTRODUCTION

IPTV (Internet Protocol Television) is a technology where the digital television services like video channels and programs are delivered to the television sets or the smart phones through a broadband connection, rather than being delivered through the conventional cable or broadcasts set-up. In simple terms, IPTV is nothing but a video and audio being delivered over an IP network. The user can watch internet TV on computer screen, a television screen (with a set-top box installed) or a mobile device like a cell phone or an iPad. The video streams are encoded as a series of internet protocol packets and those packets travel through the public internet which can be received by any user by having a set-top box (STB) and a subscription for the service. IPTV is a technology that offers revenue generating opportunities for the telecom and service providers. Verizon was the first Telco to offer IPTV as it launched service in Keller Texas in Sept. 2005. There are a lots of IPTV providers as of now. The remaining of the paper is organized as follows: section II

explains the working of IPTV, section III lists the various IPTV service, section IV discusses about the security system, section V focuses on the security issues, section VI deals the various security elements and section VII concludes the paper.

II.   HOW IPTV WORKS

With traditional Television, television services are delivered over a broadcast network or over cable network via satellite. The broadcast is being turned into radio waves and they pass through the air to a roof-top antenna on house. The antenna converts the waves back into electrical signals and the TV set decodes them to make its sound and picture. In IPTV, the videos are encoded as sequence of IP packets and delivered over an IP network.

The audio / video contents that the IPTV Company delivers to its end users are stored in IPTV video servers. The contents like live programs are streamed, but prerecorded programs and movies need to be stored in such a way that

they can be selected and streamed on demand. The IPTV Company should obtain the rights to collect the videos and redistribute the content. A Head end is the physical unit which collects all media streams, encodes /decodes and multicasts it for distribution.

The IPTV head end can be separated as satellite reception, encoding and distribution. The content reception is done with the use of large multi-focal point C-band dish to receive the content signals from the various satellite transmitters. The output received from various receivers will be inserted into an encoding device to deliver to the multicast IP addresses. These streams are encoded either in MPEG2 or MPEG4 (is a compression technique adopted by broadcasters for high definition television) format. After all the received contents are demodulated and multicast IP encoded, encryption is applied to the contents to protect it from unauthorized access.

A. Protocols Used In Iptv

Streaming a video is not like downloading a normal file. Instead, a fragment of a file is downloaded, played and, while it's playing, simultaneously downloads the next part of the file ready to play in a minute. The Internet links almost all the computers in the world as they all agree to communicate with each other using agreed technical procedures called protocols. Streaming employs protocols adapted for concurrent downloading and playing, such as RTP (Real-Time Protocol) and RTSP (Real-Time Streaming Protocol). IGMP (IP Group Membership Protocol) is used for streaming videos from the server and broadcast it to members of a group of clients (many people watching the same TV channel - multicast). The role of the protocols in IPTV is depicted in fig.1.

- HTTP (Hypertext Transfer Protocol) – Browsers use to communicate with the clients and the servers for data transfer.
- RTSP (Real Time Streaming Protocol) – Used to deliver Video on Demand services.
- IGMP (IP Group Membership Protocol) – Used for connecting television with multicast TV programming.
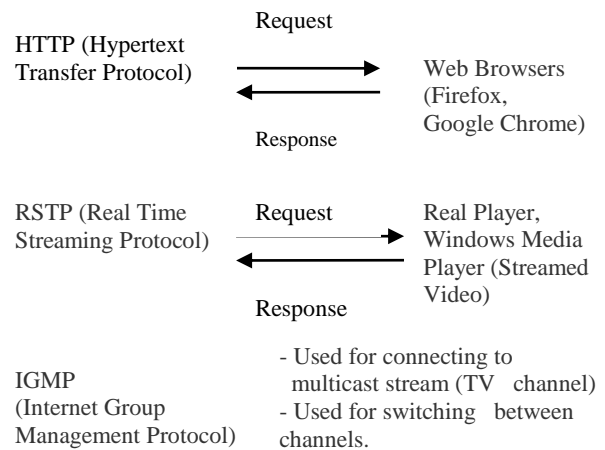

Fig 1. Protocols used in IPTV

B. Iptv Distribution Network

The IPTV Distribution Network covers large area, with sufficient bandwidth and QoS (Quality of service) to the customers for delivering the IPTV content. Fibre Optic Technology has the capability of carrying thousands of audio and video streams. In certain cases service providers install Fibre optic connections to the next closest hub or to the street-end which is termed as Fibre-To-The-Node or Neighbourhood [FTTN] or Fibre-To-The-Curb [FTTC] or directly to home as Fibre-To-The-Home [FTTH]. In common these technologies are collectively known as FTTx. Generally the networks for the IPTV distribution are Fiber to Home (FTTH / FTTx), Ethernet Passive Optical Networks (PONs) or a hybrid network with a Digital Subscriber Line (DSL).

C. Set Top Box Software as a Middleware

Set top box software acts as a middleware that performs many operations on the set top box and also allows watching the video content on TV. It accesses and manages the content stream database on various IP addresses and port numbers [1]. It also manages various details like what package of channels the user can access, subscriber's details, their set top boxes, VoD (Video on demand) etc. In addition, it provides the presentation to the end users in the form of Electronic Program Guide (EPG) which enables the user to view a program as well as to navigate up and down within the subscribed channels.

D. Iptv Viewing Device – The Set Top Box

The Set Top Box is a hardware device that receives packets of streamed videos from the network, encodes MPEG videos and decodes MPEG2 videos, and then displays them as high-quality TV pictures. The set top box works with the middleware to connect the end user's television with the IPTV service provider.

E. Rights Management

The Digital Rights Management (DRM) package is responsible for encryption content. The DRM also ensures how the content is protected and the nature of the content protection. In pay-TV content is protected during transmission from the head-end to the set-top box. This is done by the cable and satellite operators on employing conditional access security systems which restricts the content usage to only authorized user to view the content. IPTV also applies similar rules.

III.   IPTV SERVICES

- Time shift: With IPTV's time shift, the user can watch a week programmes auto recorded.
- Live TV Controller: Watching live TV broadcast by using features like rewind, pause and play.

- Real Movie on Demand: Rewind, fast forward, pause and play the latest hit movies like watching with a DVD player.
- Triple play: Triple play means offering multiple services by a single service provider such as voice (Telephony), data (Internet access) and Television services. Quadruple play adds mobile to the above three. Dual mode GSM plus Wi-Fi cell phones support quadruple play.
- Other things that could be provided with IPTV are Interactive applications like gaming, chatting or transactional applications like TV Shopping.

IPTV supports both live TV (multicasting) and the stored videos (unicasting) services. In case of live TV, the video content is compressed using MPEG2 or MPEG4 codec (A device which encodes and decodes digital media streams) and then sent in the MPEG transport stream via IP multicast. IP multicast is a one-to-many service model that delivers the video content to many users simultaneously i.e, broadcast television, whereas the unicast technology is a one-to-one service model that delivers the video content specifically for each user i.e., VoD service.

IV.   SECURITY

The delivery of television service over IP requires an intelligent network with advanced security that protects the videos. IPTV can be subject to the hackers, threats and vulnerabilities which may lead to customer dissatisfaction. For this reason, providers must enforce complete security in their IPTV networks from the start. The comprehensive security plan for IPTV services must provide multiple layers of security to protect content as well as end-users' home network. The concepts and security strategies used for other IP services can be applied to protect IPTV content delivery network but as IPTV has its own unique set of challenges like unique high bandwidth, real time requirements and a different

set of user expectations from services, a new approach is required.

V. IPTV SECURITY ISSUES

Security problems may arise in home networks, delivery and management networks and content source. The attackers may sometimes take control of the home networks by disrupting the service, spreading worms, virus, Trojan and stealing the content. Problems like middleware problem, weak account and passwords, streaming/ encoding server problem, may arise in delivery and management networks. In content source, problems like finding the backup, discovering the source may occur. A security violation opens up a chance for bandwidth consuming attacks that can degrade the IPTV provider's service and result in user disappointment and possibility of service cancellation.

VI. PRECAUTIONS TO HANDLE SECURITY ISSUES

In order to provide a secure IPTV service, the providers must focus more on security elements like privacy, confidentiality, integrity, availability and interoperability.

- Privacy – Telcom's must store the customer information in a highly protected method and they should also make clear whether the customer premise equipments (CPEs) such as set-top-box, belong to the customer or the service provider [4].
- Confidentiality – Digital Right Management (DRM) must be used, recorded contents should be protected and the system should provide high level of authentication and authorization [4].

- Integrity – Content source security should be enforced, authorized access to the billing system and internal fraud should be detected and avoided.
- Availability – Disruption in IPTV service should be avoided, Denial of service attack and side channel attacks should be disallowed.
- Interoperability – A common standard on IPTV must be adopted so that the change of service provider does not bring any major impact.

VII. CONCLUSIONS

The services offered by IPTV and the digital technologies have been used by people all over the world as it satisfies the edutainment/entertainment needs of the people. The increase in number of service providers and users has witnessed the investments in this industry. To offer better service and retain the subscribers, the IPTV providers have to enforce an intelligent and secured network. This paper has discussed the various security threats that are hurdles for the growth of IPTV. It has been identified that the security elements like privacy, confidentiality, integrity, availability, interoperability are to be addressed for the sustainable growth of the technology.

REFERENCES

[1] http://www.engineersgarage.com
[2] http:// www.explainthatstuff.com/how IPTV works.html
[3] Amal Punchihewa, Ann Malsha De Silva, Yongseng Diao, "*Internet Protocol Television*", Multimedia Research Group, School of Engineering and Advanced Technology, Massey University 2010.
[4] Yen-Ming Chen, Senior Principal Consultant- Foundstone, A division of McAfee, Triple Play; Triple Threats? IPTV Security.
[5] Amy Harris, Greg Ireland, "Enabling IPTV: What Carriers Need to Know to Succeed", IDC White Paper, May 2005.