A Review of IPTV Threats Based on the Value Chain

Hong Joo Lee
College of Business Administration, Seoul National University
SK Business Hall, #315, Gwanak-ro 599, Gwanak-gu, Seoul 151-742, South Korea
[e-mail: blue1024@snu.ac.kr]

Received February 7, 2009; revised March 25, 2009; accepted April 9, 2009; published April 25, 2009

Abstract

The demand for services using digital technology is constantly increasing as new developments in digital consumer electronics and the Internet are made. This is especially true in terms of the demand for IPTV utilizing high speed Internet networks. Research on IPTV threats is important for facilitating financial transactions via IPTV and preventing illegal use or copying of digital content. Thus, this paper analyzes IPTV threats via the IPTV value chain. That is, the distribution system for IPTV service is analyzed along with the components of the value chain and corresponding IPTV security requirements or security technologies, in order to perform a threat analysis and research suitable for the IPTV service environment. This paper has a greater focus on the value chain of the IPTV business than the approach in previous research, in order to analyze security requirements and technologies that are more applicable to the business environment.

Keywords: IPTV, security threat, value chain, security technology, IPTV service process

This research was supported by the Brain Korea 21 project, the Ministry of Education, Science and Technology, the Korean government.

DOI: 10.3837/tiis.2009.02.003

1. Introduction

Various mechanisms for delivering content have recently been developed along with widely-distributed high speed Internet and digital broadcasting programs. One of these is IPTV, which refers to Internet Protocol Television. This is a consumer electronics product providing various digital services and content by fusing the functions of a TV with those of high-speed Internet.

In particular, the demand for services using digital technology has increased as new developments in digital consumer electronics and the Internet have been made, especially the demand for IPTV utilizing high speed Internet networks. According to the OVUM report [1], this is forecast to exceed 55 million by the end of 2011, an increase of over 1,200% [1]. This increasing demand for IPTV service necessitates careful consideration of the risks involved in using such a service, as the issue could be a decisive factor influencing IPTV business. Research on IPTV risk is especially important for facilitating financial transactions through IPTV and preventing illegal use or copying of digital content.

Thus, this study performs a risk analysis of the IPTV value chain. IPTV is a user-oriented mechanism for delivering digital content and services. This differs from previously used system-oriented information security; therefore, the risk analysis of IPTV considers the requirements arising from distribution of service. That is, the distribution system for IPTV service is analyzed along with the components of the value chain and the corresponding security requirements or applicable technology in order to perform a security analysis and research suitable for the IPTV service environment.

1.1 Research Process

This study followed the process shown in **Fig. 1**.

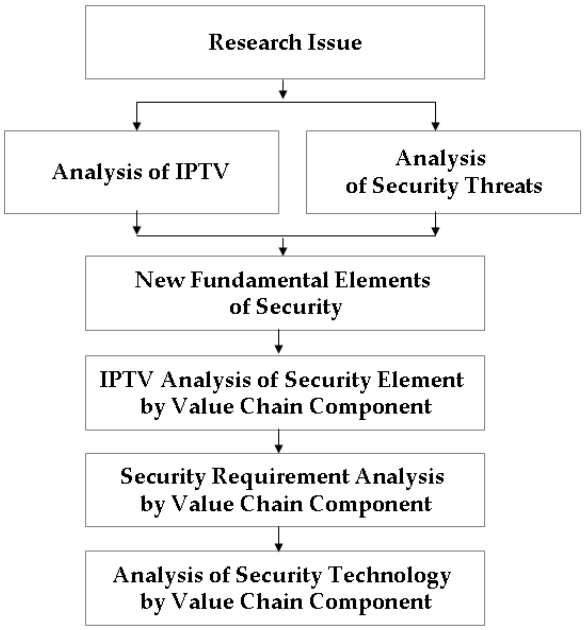

Fig. 1. Research Process

First, the research issue was established. Second, I analyzed the characteristics of IPTV and the security threats were found based on a literature review. Third, I suggested new fundamental elements of security that differ from previous research. Fourth, the threats to IPTV security and the IPTV value chain were analyzed. Fifth, vulnerable points of IPTV security are analyzed with respect to the value chain components. Lastly, security technology was suggested for such vulnerable points.

IPTV is a consumer electronics product that offers user-oriented service. In particular, it provides individualized service with interactive features, as well as the ability to perform financial transactions using a TV. Such services require a particular emphasis on IPTV security.

2. Literature Review

2.1 Internet Protocol Television

As high speed Internet has become widely distributed, the demand for new services, such as products combining the features of TV and Internet, has also increased, and this has led to development of IPTV (Internet Protocol Television). IPTV is an intelligent service that enables simultaneous two-way service via a high speed Internet network and a TV [2].

There exist various definitions of IPTV service, which makes it difficult to establish a single definition. However, IPTV can be tentatively defined as a service that delivers media such as video via a network in real-time, or is used to retransmit stored media [2][3][4][5]. **Table 1** shows various definitions of IPTV established by researchers.

Table 1. Definitions of IPTV

Researcher	Definition
ITU [4]	Multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to provide the required level of QoS/QoE, security, interactivity and reliability.
Gilbert [3]	Digital video content, including television, which is delivered via the Internet Protocol (IP).
William Copper, Graham Lovelace [5]	Delivery of digital television and other audio and video service over broadband data networks using the same basic protocols that support the internet.
Stefano Nicoletti et al [6]	IPTV is the electronic delivery of television and/or video signals to subscribers by dedicated bandwidth allocation with IP.

That is, IPTV refers to the use of IP as a delivery mechanism for video content that can use a public IP-based network, such as the Internet, or a private IP-based network. In this paper, IPTV is defined as the delivery of both digital services and the broadcast of digital content over an IP network. **Table 2** shows the features of IPTV identified in previous research [2][3][5][7].

2.2 IPTV service process according to service type

In this paper, my research about the IPTV value chain involved analysis of IPTV broadcasting service based on previous research. IPTV service is similar to broadcasting service under the

current broadcasting act. In addition, interactive broadcasting service is provided in IPTV, which is regarded as communication involving IPTV and the user. In this paper, my analysis of the IPTV service process according to service type was based on previous research. One type considered was broadcasting and the other was interactive broadcasting.

Table 2. Features of IPTV

Features	Description
Support for interactive service	The two-way capabilities of an IPTV system allow service providers to deliver a whole raft of interactive TV applications. The type of service delivered via an IPTV service can include standard live TV, high definition TV (HDTV), interactive games, and high speed Internet browsing.
Time shifting	IPTV in combination with a digital video recorder permits time shifting of programming content.
Personalization	An end-to-end IPTV system supports bidirectional communications and allows the end user to personalize their TV viewing habits by deciding what they want to watch and when.
Low bandwidth requirements	Instead of delivering every channel to every end user, IPTV technologies allow service providers to only stream the channel that the end user has requested. This attractive feature allows network operators to conserve bandwidth on their networks.
Accessible on multiple devices	Viewing of IPTV content is not limited to televisions. Consumers often use their PCs and mobile devices to access IPs.

(1)Broadcasting service

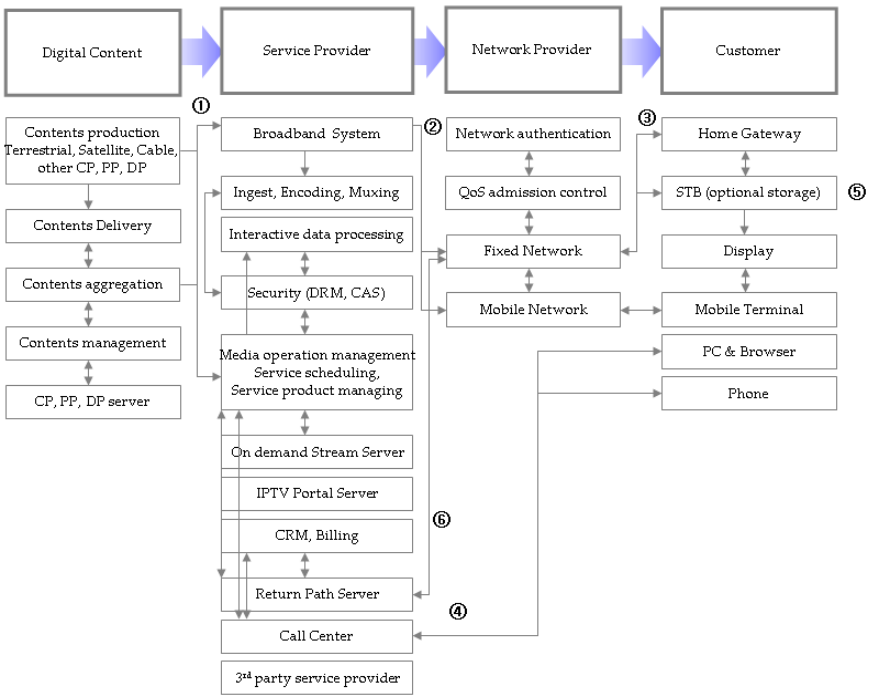

Fig. 2. IPTV Broadcasting Service Process [8]

Fig. 2 shows broadcasting according to the service flow scenarios which include Linear/Broadcast TV, PVR (Personal Video Recorder), PPV (Pay-Per-View), multi-angle [8]. **Table 3** describes each step of the IPTV broadcasting service process [8].

Table 3 IPTV broadcasting service process

Step	Description
①	Broadcasting contents and service scheduling are provided to a baseband system by a contents provider
②	Broadcasting contents are reworked for showing on IPTV and they are sent to a network provider
③	STB (Set-Top-Box) is connected via multicast broadcasting and then STP shows the broadcasting contents
④	The IPTV user can request a new service via STB
⑤	The user can watch the telerecording on IPTV via STB and PVR (Personal Video Recorder)
⑥	The user can buy desired contents such as PPV (Pay Per Viewer)

(2) Interactive broadcasting service

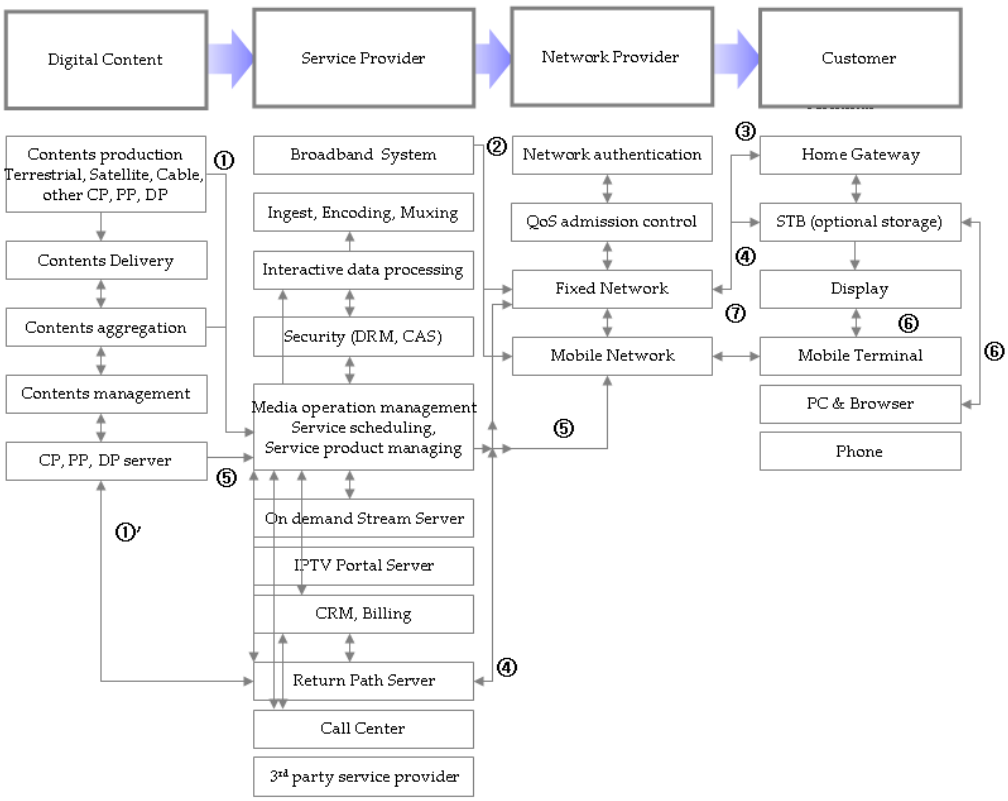

Fig. 3 Interactive Broadcasting Service Process [8]

Fig. 3 shows interactive service according to the service flow scenarios which include TV-Portal, T-Commerce, T-Communication, T-Entertainment, and education [8]. **Table 4**

describes each step of the IPTV broadcasting service process [8].

Table 4. Interactive Service Process

Step	Description
①	Interactive broadcasting contents are provided to a media operation management system by a contents provider
①'	The attributes of contents are considered to provide the service.
②	The contents are reworked for showing on interactive IPTV and they are sent to a network provider
③	STB (Set-Top-Box) is connected via multicast broadcasting and then STP shows the broadcasting contents
④	The IPTV user has communication with service provider. And the user requests the service information from a service provider.
⑤	The attributes of contents are considered to provide the service.
⑥	STB (Set Top Box) provides interactive service to customer via mobile terminal and computer.

2.3 Security Threats

(1) Analysis of Security Threats

In this paper, I define a fourth type of security threat based on previous research. **Fig. 4** shows the types of network security threats

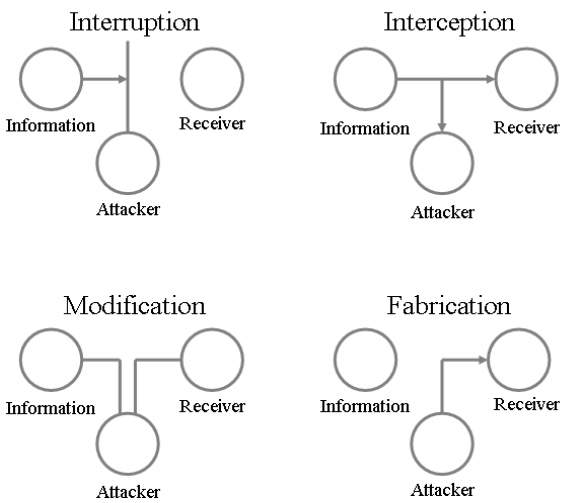

Fig. 4. Network Security Threats [9]

The types of security threats are interruption, interception, modification and fabrication. The descriptions of these are shown in **Table 5**.

Table 5. Types of Network Security Threats [9][10]

Threat Type	Description
Interruption	A system asset is destroyed or becomes unavailable. Examples include destruction of hardware, disabling of the file management system, erasure of a program or data file, and failure of an operating system manager.
Interception	A threat action whereby an unauthorized entity directly accesses sensitive data

	traveling between an authorized source and destination.
Modification	The content of a data transmission is altered, leading to an unauthorized action or result. Examples include changing values of items, altering a program so that it performs incorrectly, and modifying incoming messages.
Fabrication	An unauthorized party inserts counterfeit objects into the system. Examples include insertion of spurious messages or the addition of records to a file.

Jung insisted that threats to the security of a network can be characterized by examining the function of the computer system that is providing information [10]. In general, there is a flow of information from a source to a destination [10].

Thus, I analyzed attack methods from security threats that is associated fundamental elements of security in **Table 6**.

Table 6. Attack Method and Fundamental Element of Security

Threat Type	Attack Method	Fundamental Element of Security
Interruption	Denial of Service [11] Virus, Bomb, Worm [12]	Availability [9]
Interception	Release of message contents, Traffic analysis [13]	Confidentiality [9]
Modification	Modification of message [11][12]	Integrity [9]
Fabrication	Spurious association, Initiation [13] Fabrication of data [14]	Integrity [9]

(2) Security threats model

In order to analyze IPTV security, ITU [4] divides IPTV security elements into five layers. These are: content security threats, service security threats, network security threats, terminal security threats, and subscriber security threats. **Fig. 4** shows the relationships among the security threats.

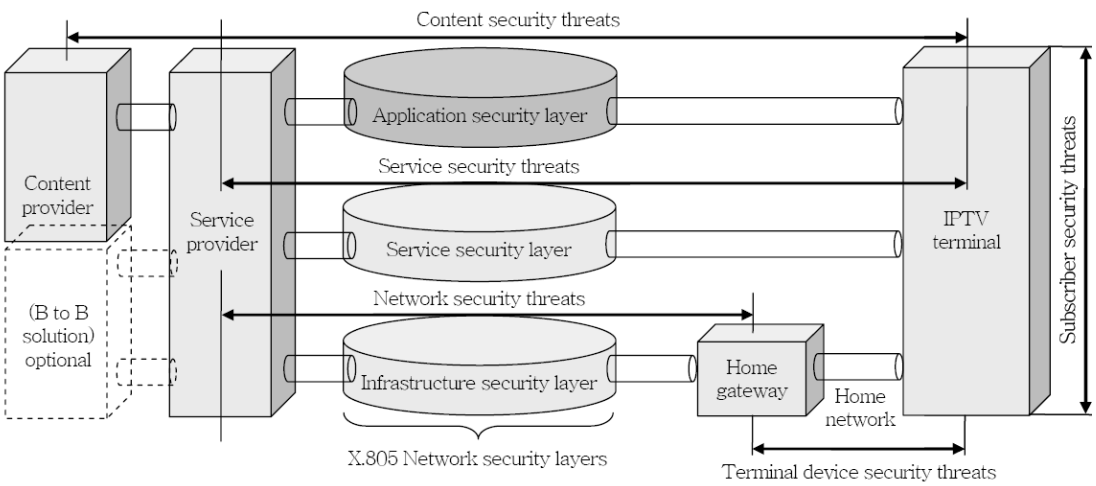

Fig. 4. Security Elements and X.805 Network Security Network [15]

Table 7 describes security threats with respect to the components and targets being protected.

Table 7. Security Threats Attribute of IPTV [16]

Attributes	Description
Content security threats	The target of content security threats is the contents delivered to users by contents providers or service providers. Potential threats include interception, unauthorized viewing, and unauthorized redistribution or reproduction.
Service security threats	Targets of service security threats include the media server, DRM server, CDN (Contents Distribution Network) server, payment server, and management server - resources that belong to service providers. Potential threats include copy-right infringement, masquerading/spoofing, hacking/DoS attacks, and phishing/Trojan horses.
Network security threats	The targets of network security threats include the router switch or network resources, which belong to network operators.
Terminal security threats	The targets of terminal security threats are the resources necessary for the processes through which end users consume contents. These resources belong to terminal devices. Potential threats include tampering with device hardware, illegal access to information, modification of hardware devices (medication of time information to nullify DRM (Digital Rights Management)), and virus attacks.
Subscriber Security threats	The target of subscriber security threats is the personal information of subscribers. Potential threats include illegal copying or release of such information.

2.4 Fundamental Elements of IT Security

This study involved a literature review in order to analyze security threats and their associated requirements for IPTV.

I first reviewed the security dimensions and described the mapping of security dimensions to security threats [15]. In this review, I analyzed security threats and security requirements in value chain of IPTV. A '√' symbol in a table cell indicates that a particular security threat is associated with the corresponding security dimension.

Table 8. Mapping of security dimensions to security threats [15]

Security Dimension	Security Threats				
	Destruction of information /resources	Corruption/modification of information	Theft/removal/loss of information/ resources	Disclosure of information	Interruption of services
Access control	√	√	√	√	
Authentication			√	√	
Non-repudiation	√	√	√	√	√
Data Confidentiality			√	√	
Communication Security			√	√	
Data Integrity	√	√			
Availability	√				√
Privacy				√	

Analyses of security threats and their associated requirements have been presented in several previous papers on information security. For example, Frank [17] argued that integrity, privacy, authentication, and availability are the essential factors relating to information security. Also, Donald G [18] suggested that identification, security auditing, and immunity are the crucial elements of information security.

Table 9 shows the various elements of information security suggested by the literature review.

Table 9. IT Security Elements Analyzed according to Literature Review

	Identification	Integrity	Security Auditing	Privacy	Non-reputation	Authentication	Confidentiality	Authorization	Availability	Immunity
Frank [17]		√		√		√			√	
Marianne Swanson [19]		√				√				
Pauline Bowen [20]		√							√	
GAO [21]		√		√		√		√	√	
Donald G. Firesmith [22]		√		√		√		√	√	
Donald G. Firesmith [18]	√		√							√
Paolo Bellavista [23]		√		√		√		√	√	
Boncella, R, J [24]		√		√		√		√	√	
TERO OJANPERÄ and RISTO MONONEN [25]		√		√		√	√		√	
Longstaff [26]		√				√	√	√	√	
ISO/IEC 1996 [27]		√			√	√	√			
NRC [28]		√			√	√			√	
US OCR [29]									√	
NSA [30]		√								

3. Security Threats to IPTV

3.1 New Fundamental Elements of Security

According to the research results in **Table 9**, many researchers have studied the security elements; Identification, Integrity, Security, Auditing, Privacy, Non-reputation, Immunity Authentication, Confidentiality, Authorization, Availability. However, many researchers have previously suggested only three security elements; Integrity, Confidentiality and Availability [25][26][27] .

In this paper, specially, I researched confidentiality in detail. Confidentiality has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access" [31]. Also, Confidentiality means the protection of information in the system so that unauthorized persons cannot access it. It includes Authentication and Authorization. It is widely thought that this type of protection is of most importance to military and government organizations that need to keep plans and

capabilities secret from potential enemies [32]. Confidentiality also includes privacy issues, which have received an increasing amount of attention in the past few years, thus, confidentiality is also of importance for protecting personal information maintained in automated systems by both government agencies and private-sector organizations [32].
From this researched, I suggested new fundamental elements of security that need more detailed research due to changes in the security environment. These are: Integrity, Privacy,Authenication, Authoritization, Availability(IPAAA) . This paper analyzed all five elements of IT security in detail, based on previous research. **Table 10** shows the new fundamental elements of security and their definitions.

Table 10. Fundamental Elements of Security

Security Element	New Fundamental Element of Security	Definition
Integrity	Integrity	Integrity is a property of data such that information has not been modified, altered or destroyed accidentally or in an unauthorized manner.
Confidentiality	Privacy	Privacy can be defined as an individual's right to determine his/her own communication contacts as well as the right to control the use of his/her personal information by others.
	Authentication	Authentication is the process of verifying a principal's claimed identity; positive verification of the identity of a user, device, or another entity in an information system. This is often a prerequisite for allowing access to system resources.
	Authorization	Authorization is the function of specifying access rights to resources.
Availability	Availability	Availability is a property of data such that information and other necessary systems are accessible and useable on a timely basis as required to perform various tasks.

In **Table 11**, I analyzed new fundanmental element of security. This analysis based on threat type and security dimensions through **Table 6** and **Table 8**.

Table 11. Security dimensions and new fundanmental element of security

Threat Type	Security dimensions	New Fundanmental Element of Security
Interruption	Access Control	Avaliability
Interception	Access Control, Communication Security	Authorization
Modification	Data Confidentiality	Integrity, Privacy
Fabrication	Data Confidentiality, Non-Repudiation	Privacy, Authentication, Authorization

3.2 Analyses of the IPTV Value Chain

The main business assets of IPTV service are the digital contents stored and transported in the IPTV business value chain. Hence, analyses of security threats to IPTV tend be focused on analyzing the value chain rather than the systems required by previous products. The value chain consists of the development of digital content, making the content available through service providers, and distribution of the content to household TVs through networks [4][7]. Therefore, security technology suitable for service is analyzed in order to study the more

plausible security threats. In this paper, based on previous research I show the value chain of IPTV. **Fig. 5** describes the value chain of IPTV service.

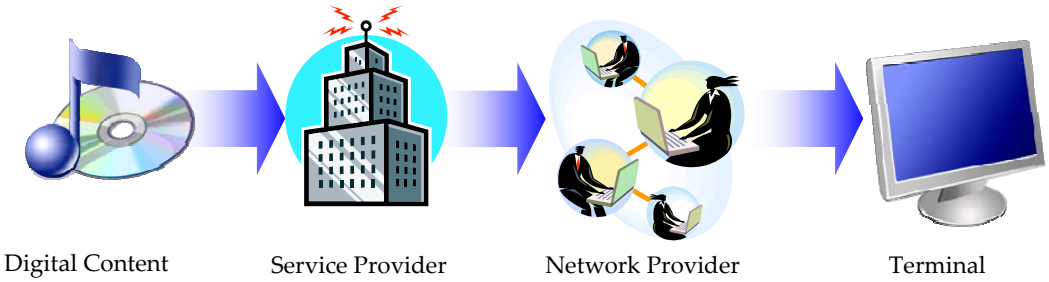

Fig. 5. Value Chain of IPTV

Table 12 describes each component of the IPTV value chain.

Table 12. Value Chain of IPTV

Component	Description
Digital Content	This is the component in which content is created and purchased and amalgamated into a service or channel. The amount of advertising that is placed on the channel and editorial control over the type of content on the channel is determined in this component. The content provider provides a variety of content for IPTV service and uses it.However, the privacy of UGC (User Generated Content) could be infringed.
Service Provider	This is the component in which channel services are aggregated and made available for distribution in the form of a commercial offering. To provide IPTV service, the service provider is responsible for management of customer information , product scheduling, billings and user authentication.
Network Provider	The network provider must transmit the service across a network to the customer. According to the data transmission type the service is divided into broadcast multicast and unicast.
Terminal	This is the component in which users can directly access services and content.

Fig. 6 shows the IPTV service flow. This is a more detailed explanation about IPTV value chain based on the literature review. In this paper, based on the IPTV service flow [8], I analyzed the security threats in each component of the value chain.

4. Threat Points in the IPTV Value Chain

This paper identifies security threats in the IPTV value chain based a review of current literature, as described in **Table 13** [16]. I researched security dimensions by value chain component of IPTV. And I suggested threat of IPTV asset and threat point in each component of the IPTV value chain.

Digital content can be consumed by the end-user via an IPTV terminal device.The content threats are illegal use of content such as unauthorized viewing and unauthorized reproduction. The service provider is responsible for management of customer information, product scheduling, billing and user authentication. The provider threats come from malicious attackers. The attackers can intercept the subscriber's information by methods such as hacking of a user's ID, billing information or ordering information, and analysis of a user's character

via remote control. The network provider transmits the service across a network to the customer. Network security threats to multicast technologies used in IPTV networks include spoofing of multicast TV sources, or illegitimate multicast group members [15].

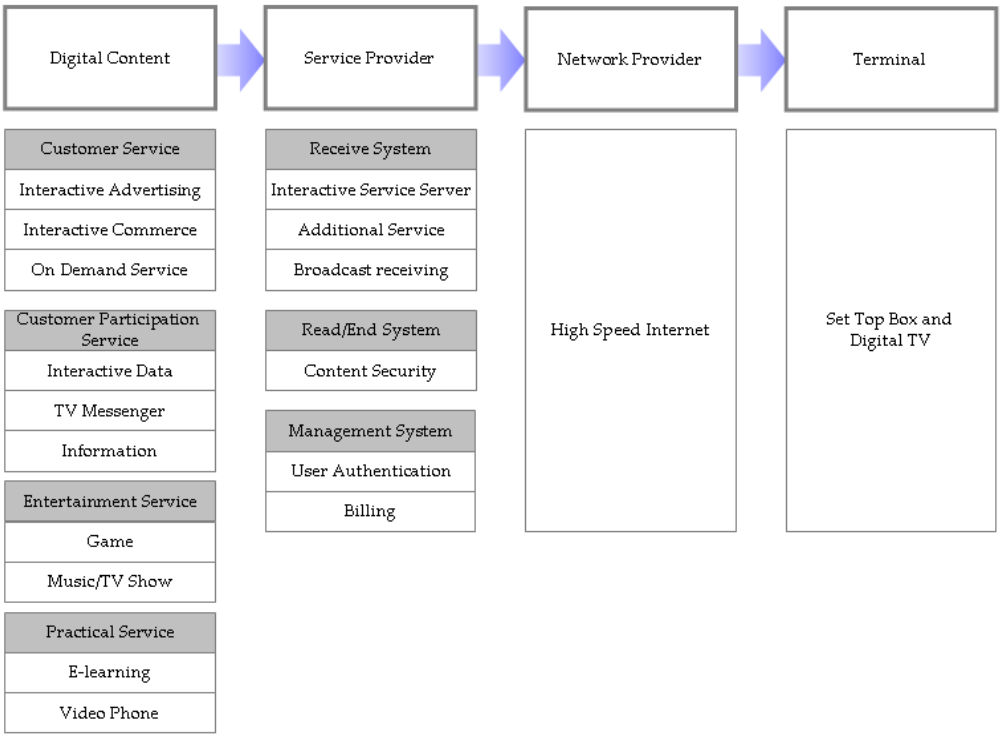

Fig. 6. IPTV Service Flow

Table 13. Security Threats in Different Components of the Value Chain

Value Chain Component	Security Dimension	Threat of IPTV Asset	Threat Point
Digital Content	Data Confidentiality	Accessing illegitimate content	Illegal use of content (Copyright infringement : Unauthorized viewing, Unauthorized reproduction)
Service Provider	Access Control	Circumvention of conditional access system (CAS) enabling access to content	Hacking of a user's ID, billing information or ordering Information, Analysis of a user's character via Remote Control
Network Provider	Access Control, Non-Repudiation	Packet capture on the home network and IP subnet	Unauthorized access and transmission of data (Spoofing of multicast TV sources), Privacy Invasion by Cookie, Message forgery, DDOS
Terminal	Data Confidentiality, Access Control, Non-Repudiation, Communication Security	Capturing the digital certificate from an STB for ordering contents and broadcasting/ redistributing the stream to other subscribers	Protection of copyrighted contents delivered to users (Illegally accessing digital content by tampering with device hardware), User Authentication

The terminal device can be used by the end user to process and store content for the IPTV service. Therefore, the terminal needs to be protected against illegal accessing of digital content via tampering with device hardware, and unauthorized use by subscribers.

In this paper which is based on IT security elements analysis and security threats in different components of the value chain, I suggested the five security elements (IPAAA: Integrity, Privacy, Authentication, Authorization and Availability) in each component of the IPTV value chain and the results are described in **Table 14**.

Table 14. Security Elements of Value Chain Components

Value Chain Component	Security Element (IPAAA)
Digital Contents	Integrity
Service Provider	Authorization, Availability, Privacy
Network Provider	Authentication, Integrity, Availability
Terminal	Authentication, Authorization, Privacy

This study analyzed the security requirements for each component of the value chain based on **Table 13** and **Table 14**. Based on the anlyses, I suggested IPTV security requirements for each component of the value chain in **Table 15**. Moreover, applicable technologies for new fundamental elements of security in each component of the value chain are also suggested.

Table 15. Security Requirements and Security Technology

Value Chain Component	Security Requirements	Security Technology
Digital Content Provider	This component requires security technology that can prevent illegal use of digital content by controlling the ability to access the content and allowing access only to authorized users.	Digital Watermark SHA-1 for hash, AES(Advanced encryption standard)
Service Provider	IPTV services should have the capability to identify legitimate subscribers in order to prevent illegitimate access. Robust authentication and strict authorization schemes are required to prevent illegitimate subscribers from accessing service networks and servers. Also, IPTV services should be able to limit the ability of legitimate subscribers to access content. (e.g. limit the number of times the same user can access the network and prevent uploading and downloading of unallowable data), in order to prevent abuse of network resources.	Digital Certificate, Token, Contents Protection System;VCPS (Video Content Protection System, CPRM (Contents Protection for Recordable Media), DVB-CPCM (Contents Protection and Copy Managnent), DVB-CBMS (Convergence of Broadcast and Mobile Service)
Network Provider	In this component, technology related to multicast or protocol security is required for secure network transmission. In particular, robust authentication is required for data transmission or access requests.	Digital Certification, DHCP (Dynamic Host Configuration Protocol)
Terminal	Preventive measures should be developed to control illegitimate use of digital content previously delivered to users and the release of subscriber information.	EAP-TLS, DCE/Kerberos,Smart Card, Digital Signatures, One Time Password

5. Conclusions and Future Directions

This study reviewed the security requirements for a successful IPTV business. I first analyzed the elements of information security via a literature review. Second, the security weaknesses of each component in the IPTV value chain were reviewed. Third, the security elements required to protect each component in the value chain were studied and, finally, applicable security technology was suggested, based on the analysis of the security elements. I analyzed security technologies used in the IPTV value chain, including Digital Watermark, Digital Certificate, Token, Smartcard, Fingerprint, Digital Certification, EAP-TLS and DCE/Kerberos.

This study had a greater focus on the value chain of the IPTV business than the approach in previous research, in order to analyze security requirements and technologies more applicable to the business environment. However, the analysis of security elements for the value chain may require greater consultation with experts in the field. In addition, detailed analysis should be done on security technology with respect to the form of IPTV services. At the same time, further studies on security technology, based on customer demand for IPTV, should be conducted, which will assist in making IPTV more user-friendly.

References

[1] M. Philpott, “IPTV: challenges and opportunities,” OVUM, 2007.
[2] G. O'Driscoll, “Next Generation IPTV Services and Technologies,” Wiley-Interscience, 2008.
[3] G. Held, “Understanding IPTV,” Taylor & Francis Group, 2007.
[4] ITU-T,“Security Architecture for Systems Providing End-to-end Communications Recommendation X.805,” ITU, 2003.
[5] W. Copper and G. Lovelace, “IPTV Guide,” Informitv and Lovelace Consulting Limited, 2006.
[6] S. Nicoletti et al, “Regulation of the IPTV Value Chain,” OVUM, 2007.
[7] HanaroTelecom, “Business Strategy of IPTV,” in *Proceedings of IPTV Conference,* 2007.
[8] KISA, “A study on Analysis of Privacy Invasion and Protection in IPTV,” KISA, 2007.
[9] J. H. Jeon et al, “Information Security Essential,” Scitech Media, 2009
[10] Bumsuk Jung et al, “Security threats to Internet: a Korean Multi-Industry Investigation,” *Information & Management*, vol.38, pp.487-498, 2001.
[11] A. J. Bayle, “Security in Open system network: a tutorial survey,” *Information Age*, vol.10, no.3, pp.131-145, 1988.
[12] R. K. Rainer, C. A. Snyder, and H. H. Carr, “Risk analysis for information technology,” *Journal of Management Information System*, vol.5, no.1, pp.129-147, 1991.
[13] L. S. Rutledge and L. J. Hoffman, “A survey of issues in computer network security,” *Computer and Security*, pp.296-308, 1986.
[14] C. P. Pfleeger, “Security in Computing,” Prentice Hall, 2006.
[15] ITU, FG IPTV-DOC-0155, “Working Document : IPTV Security Aspects,” ITU, 2007.
[16] J. Y. Park et al, “The Standardization Issue for ITV-T FG IPTV Security Aspects,” *ETRI*, 2007.
[17] F. Stajano, “Security for Ubiquitous Computing,” John Wiley& Sons, 2002.
[18] D. G. Firesmith, “Analyzing Specifying Reusable Security Requirements,” Carnegie Mellon SEI, 2006.
[19] M. Swanson et al, “Security Metrics Guide for Information Technology Systems,” National Institute of Standards and Technology, 2003.
[20] Pauline Bowen et al, “Information Security Guide For Government Executives,” National Institute of Standards and Technology, 2007.
[21] United States Government Accountability Office, “INFORMATION SECURITY-FBI Needs to Address Weaknesses in Critical Network,” United States Government Accountability Office, 2007.

[22] D. G. Firesmith, "Security Use Cases," *Journal of Object Technology*, vol.2, no.3, 2003.
[23] P. Bellavista, "An integrated management environment for network resources and services," *IEEE Journal on Selected Areas in Communications*, vol.18, no.5, 2000.
[24] R. J. Boncella, "Web Services and Web Service Security," in *Proceedings of the Americas Conference in Information Systems*, NY, 2004.
[25] T. Ojanpera and R. Mononen, "Security and Authentication in the Mobile World," *Wireless Personal Communications*, 2002.
[26] T. Longstaff et al, "Security of the Internet," *The Froechlish/Kent Encyclopedia of Telecommunication*, vol.15, pp.231-255, 1997.
[27] International Organization for Standardization, "International Electro technical Commission Informational Technology- open distributed processing," ISO/IEC, 1996.
[28] National Research Council Committee on Information Systems Trustworthiness, "Trust in Cyberspace," National Academy Press, 1999.
[29] U.S .Government office for Civil Rights (OCR)- http://www.hhs.gov/ocr/
[30] National Security Agency, "National Security Research Center Trusted Network Interpretation," NSA, Vol.1.7/31/87 NCSC-TG-005(Red Book), 1987
[31] ISO, "International Organization for Standardization 27001," ISO, 2005
[32] H. F. Tipton and M. Krause, "Information Security Management Handbook," CRC Press LLC, 2008.

Hong Joo Lee is a BK Professor at the College of Business Administration, Seoul National University, Seoul, Korea. He graduated from the School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA. He has also received a Ph.D degree in Industrial System Engineering from Yonsei University, Seoul, Korea. He was a senior researcher at DAEWOO Electronics Corp. And, he has worked at Dankook University as a teaching professor. His research focuses on Ubiquitous Technology and strategic uses of New Technology.