Journal of The Korea Society of Computer and Information
Vol. 17 No. 6 , June 2012

2012-17-6-4-7

국내 인터넷기반 방송서비스의 보안 모델 설계

서 희 석*, 김 성 준**, 안 우 영***

A Design on Security Model of Domestic Internet-based Broadcasting Service

Hee-Suk Seo *, Sung-Jun Kim **, Woo-Young Ahn***

요 약

최근 통칭 IPTV라고 불리는 새로운 개념의 텔레비전 서비스가 활성화되고 있다. VoD(Video On Demand)라고 불리는 콘텐츠 제공방식은 시청자들이 보고 싶은 프로그램을 시간에 구애받지 않고 원하는 시간에 볼 수 있게 되었고, 그 외에도 여러 부가서비스들이 제공되어 사업자들이 새로운 방식으로 수익을 창출하게 되었다. 다양한 서비스를 제공 중인 IPTV는 IP를 기본으로 하여 서비스된다. IP와 방송의 융합으로 IP기반의 서비스에서 발생 했던 보안 위협이 IPTV에서도 발생 할 수 있다.

국제 IPTV 보안 권고안은 추상적이라 현장에 바로 적용시키기는 어려움이 많다. 본 논문에서는 표준 모델을 기반으로 서비스가 어떠한 위협에 노출되어 있는지, 서비스를 제공하는 과정에서 수집하는 사용자의 어떠한 개인정보가 노출될 위협에 있는지에 대해 알아보고 이 취약점들을 분석하여 한국형 보안 모델을 설계하였다.

▸ Keyword : IP 방송서비스, 컨텐츠보안, IPTV보안

Abstract

Internet Protocol Television(IPTV) is the use of an IP broadband network to deliver television (cable TV type) services to the end user. Traditional telecommunications service providers as well as alternate service providers and Internet service providers can utilize their IP networks (and broadband consumer access) to deliver broadcast TV, Video on Demand (VOD) and other Internet services to the consumer. As digital technologies progress, illegal copy and redistribution of IPTV

• 제1저자 : 서희석 • 교신저자 : 안우영
• 투고일 : 2012. 03. 20, 심사일 : 2012. 04. 03, 게재확정일 : 2012. 04. 23.
* 한국기술교육대학교 컴퓨터공학부(Dept. of Computer Science, Korea University of Technology and Education)
** 동국대학교 법학 겸임교수, 연세대학교 정보대학원 박사과정(Graduate school of information, Yonsei Univ.)
*** 대전보건대학 바이오정보과(School of Bio-infomation, Daejeon Health Sciences College)
※이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2010-0021951).

content become easier and simpler. Therefore it is required to protect IPTV content or service. In this paper, we analyze the security threats and requirements. We also discuss related issues and solutions for IPTV.

▸ Keyword : IP Broadcasting Service, Contents Security, IPTV Security

I. 서 론

최근 우리나라를 포함하여 전 세계적으로 방송과 통신이 융합된 새로운 방송서비스가 큰 인기를 끌고 있다. 인터넷 망을 이용한 인터넷 방송 서비스로, IPTV는 VOD서비스 등 자신이 원하는 프로그램만 원하는 시간에 골라 볼 수 있다.

국내 유료방송 시장에서도 주요 통신사들이 IPTV 서비스를 본격적으로 제공하기 시작했다. IPTV 사업은 기본적으로 케이블TV와 속성은 유사하지만 자체적으로 콘텐츠를 제작하기 보다는 여러 가지 다양한 커뮤니케이션 및 미디어 서비스를 재구성하여 이를 가입자에게 제공하는 콘텐츠 포털 모델의 특성을 갖고 있다. IPTV 사업은 콘텐츠를 생산하는 가치 모델이기 보다는 콘텐츠 유통을 통해 다양한 경제적 가치를 생산하는 사업 모델에 가깝기 때문이다.[1] IPTV 서비스가 틈새시장을 대상으로 하는 개인화된 미디어 서비스이기 때문에 독자적으로 사업자가 콘텐츠를 기획, 제작, 편성하는 기존의 수직 통합된 가치 사슬을 구성하는 것이 어렵다는 점이다. IPTV 서비스 사업은 자체 제작된 콘텐츠를 기반으로 이를 유통시키는 기존의 방송 모델이 아니라 인터넷 포털과 같이 기존의 다양한 콘텐츠 서비스를 구매하여 이를 재구성하거나 패키징하여 새롭게 판매하는 모델이다.

2008년 IPTV 실시간 방송이 개시된 후, 2010년 11월말 기준 가입자 수가 347만 명을 넘어서고 있고, 현재도 꾸준히 증가하고 있다. [2] IPTV 활성화에 따라 국내 이동통신 사업자들은 방송, 교육, 금융 서비스 등 다양한 부가서비스를 제공하고 있으며 양방향 통신이 가능한 장점을 이용하여 공인인증서, IC카드 기반의 전자금융서비스를 제공하고 있다. [3] IPTV 등의 방송통신 융합서비스는 IP기반 네트워크 기술과 방송기술의 결합을 기반으로 하기 때문에 기존의 인터넷에서 존재하던 보안 위협들이 그대로 IPTV 서비스에 대한 위협이 될 수 있으며, 기존에는 보안상으로 크게 문제가 되지 않던 네트워크 보안 관련 취약점들도 IPTV 방송 서비스와 결합되면서 중대한 문제가 될 수 있다.

따라서 현존하는 프로토콜과 기술들의 연구를 통하여 IPTV에 적용될 수 있는 위협들을 검토하여 해당 피해를 사전에 방지해야 한다. 그리고 이제까지 발견되지 않았던 문제점들이라도 객관적인 지표로 삼을 수 있는 연구 논문의 결과 또는 앞으로 발생할 수 있는 보안 위협들의 타당성을 고려하여 알려진 IPTV 보안 위협에 대한 대응책을 마련하기 위한 보안 모델이 필요하다.

본 논문에서의 2장에서는 IP 방송 서비스 국제 보안 권고안 X.805와 X.1191에 대해 알아보고, 3장에서는 IP 방송 서비스 보안 위협에 대해 알아보고 분석한다. 또한 나아가 4장에서는 이를 바탕으로 구체적인 IPTV의 보안 위협에 대해서 분석하여 한국형 IPTV보안 모델을 제시하고자 한다.

II. 관련 연구

1. X.805 보안 권고안

표 1 X.802.11의 보안 규격
Table 1. Security standard for X.802.11

보안 규격
액세스 제어 보안 규격
인증 보안 규격
비-부인 보안 규격
데이터 기밀 보안 규격
통신 보안 규격
데이터 무결성 보안 규격
가용성 보안 규격
개인 정보 보안 규격

2003년 10월에 권고된 X.805(Security architecture for systems providing end-to-end communications, end-to-end 통신을 제공하는 시스템을 위한 보안 아키텍처)에는 end-to-end 네트워크 보안을 제공하는 네트워크 보안

의 아키텍처가 정의되어 있다.[4] end-to-end 통신 방식은 망을 경유한 양 단말간의 종단 간 통신으로, 교환 기간 신호를 중계하는 방식 중 하나를 말하는데, IPTV에서는 end-to-end를 이용한 QoS(Quality of Service, 서비스 품질) 기술이 필수적으로 요구된다. X.805 권고안에서는 보안 아키텍처, 보안 규격, 보안 계층, 보안 모델, 보안 위협에 대해 기술되어 있다.

2. X.1191 보안 권고안

2009년 02월에 최종 권고된 X.1191은 IPTV 보안을 위한 기본 지침인 권고안으로 IPTV 보안 측면에 대한 기능적 요구 사항, 아키텍처 및 보안 메커니즘 등에 대해 다루고 있다. 기본 지침이 될 권고안인 만큼 특정 보안에 대한 자세한 내용은 다루고 있지 않고, 향후에 권고될 권고안들이 고려해야 할 내용들을 다루고 있다.

○ 콘텐츠 암호화

대부분의 경우, 내용을 전달하는 동안 불법적인 사용을 방지하기 위해 암호화 할 수 있다.

○ 콘텐츠 추적 및 확인

콘텐츠 추적을 제공하는 것은 무단으로 콘텐츠에 액세스하거나 사용한 경우 원본을 식별하고 후속 조사를 용이하게 한다.

○ 워터마킹

워터마킹은 특정 콘텐츠 기능의 변경을 통해 콘텐츠에 대한 정보를 추가하는 과정을 말한다. IPTV 서비스에서 워터마킹은 동영상이나 멀티플렉스 콘텐츠의 오디오 스트림에 직접 숨겨진 정보를 참조할 수 있다.

○ 콘텐츠 라벨링

콘텐츠 라벨링은 콘텐츠의 성격뿐만 아니라 콘텐츠 측면과 콘텐츠 특성 등을 설명하는 내용과 메타데이터를 삽입하거나 연관시키는 과정이다. 콘텐츠 라벨은 콘텐츠 전달 체인의 중간 장치를 통해 이러한 메타 데이터와 함께 쉽게 정렬, 필터, 분류될 수 있다.

○ 서비스 인증

최종 사용자(가입자)가 특정 서비스 제공 업체와 직접적인 관계를 가지고 있는 관리 서비스의 경우 서비스 공급자는 일반적으로 서비스를 시작하기 전에 터미널 장치 최종 사용자(가입자)를 안전한 방법으로 인증할 수 있어야 한다.

○ 서비스 승인

서비스 제공의 목적을 위해 최종 사용자(가입자) 또는 터미널 장치를 인증하는 것은 가입자 규정에 따라 서비스나 콘텐츠를 호스트 해주는 특정 서비스의 액세스 권한을 부여하는 것을 인증하기 위한 서비스 인증 메커니즘으로 사용된다.

○ 단말기 장치 보호를 다루는 보안 메커니즘

터미널 장치 보안 메커니즘은 안전하고 조작이 방지된 비밀 데이터 저장, 서비스 인증, 제어 신호의 암호화, 복호화, 콘텐츠 복호화, 콘텐츠의 메타데이터 복호화, 워터마크 검출, 디지털 출력 포트(인터페이스) 암호화 등과 같은 하드웨어 및 소프트웨어 모두를 기반으로 한 광범위한 기능을 포함한다.

III. 인터넷 기반 방송 서비스 보안 위협

방송통신융합서비스는 콘텐츠 공급자(Content Provider)와 서비스 공급자(Service Provider), 방송통신융합서비스 가입자(Client)로 분류된다. 콘텐츠 공급자는 서비스 공급자에게 콘텐츠를 제공하고 서비스 공급자는 제공받은 콘텐츠를 가입자에게 제공하는 역할을 한다. 이 과정에서 발생할 수 있는 취약점은 다양하다. 사소한 것부터 방송통신융합서비스 서비스 자체를 위협하는 중대한 취약점까지 존재한다. 헤드엔드, 기간사업자망, 홈 네트워크(셋톱박스, 터미널) 등 각 분류마다 구성요소들도 각각의 취약점을 가지고 있다.

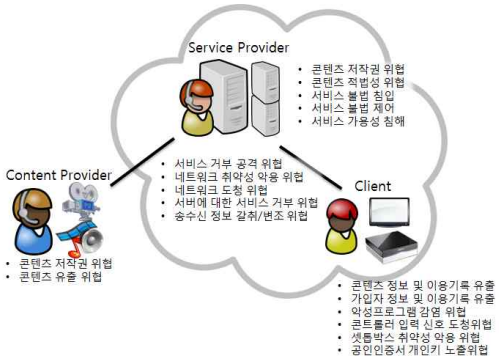

그림 1. IP 방송 서비스 보안위협
Fig. 1 IP Broadcasting Service Security Threats

1. 콘텐츠 공급자의 보안 위협 및 취약점

- 콘텐츠가 서비스되기 이전이나 저작권 등록 전에 외부로의 유출 가능성 존재
- 서비스를 제공을 위해 네트워크에 연결된 콘텐츠 파일이

유출 가능성 존재
- 헤드엔드 내부의 관리자의 패스워드 노출 등으로 인한 유출 위협 존재
- 저작권 보호 메커니즘을 적용하지 않은 콘텐츠는 사후 추적 문제점 존재

2. 서비스 공급자의 보안 위협 및 취약점
- 서비스를 제공 시 저작권이 적용되지 않은 콘텐츠 파일이 유출 가능성 존재
- 저작권 보호 메커니즘을 적용하지 않은 콘텐츠는 사후 추적 취약성 존재
- 인터넷과 직접적인 연결되어 있어, 악성코드에 감염될 경우 콘텐츠 공급자와 가입자 정보 유출이나 대대적인 악성코드 확산에 대한 취약성 존재

3. IPTV 가입자의 보안 위협 및 취약점
- 사용자의 고의적인 셋톱박스의 기술(네트워크, 전송기술 등) 노출, 기기 개조
- 외부로 노출된 기기는 셋톱박스를 공급한 사업자가 기기의 상태 확인 불가
- 사용자는 앱스토어 홈페이지나 저장매체를 통해 불특정한 다수의 애플리케이션이나동영상 등을 설치 및 실행 가능하며 이로 인해 악성코드에 대한 취약성 존재
- 셋톱박스 패스워드, 가입자 개인정보, 결제정보 등 중요 정보가 기기 내부에 저장

4. 악의적 목적 네트워크 침입 위협
- 불필요한 서비스나 포트 사용, 허락받지 않은 프로그램의 실행 등의 취약점 존재
- 이미 알려진 서버 장비 및 기반 기술의 취약성을 이용한 악용 공격 위협 존재
- 공개된 네트워크 프로토콜에 존재하는 취약성 악용 위협 존재
- 외부 망에 접속된 서버들이 웹 서비스 도중 불필요한 서비스 사용 가능성으로 인한 취약점 존재

5. 악의적 서버 접근 위협
- 외부 기기 연결 등을 통한 클라이언트로부터의 불법적인 접근 위협 존재
- 관리자가 해킹, TCP 세션 하이재킹 공격 등 다양한 공격 위협 존재[5]
- 서비스 거부 공격(DoS), 위장 접근, IP 스푸핑 등과 같은 각종 네트워크 공격 가능성 존재
- 서비스 공급자와 가입자는 인터넷으로 연결되어 있어 악성코드에 노출
- TCP SYN, UDP Flooding등 네트워크 프로토콜을 악용한 트래픽 과부하 위협 존재

이처럼 IPTV에는 각각의 구성요소마다 취약점이 존재하고 있다. 그 중 외부로 노출된 셋톱박스로 인해 발생 가능한 보안 위협은 다른 보안 위협보다 훨씬 많고 위협적이다. 하지만 이러한 이유로 IPTV가 가진 취약성은 외부로 노출된 셋톱박스만이라고 할 수는 없다. 콘텐츠를 제공하는 사업자가 보유한 네트워크나 네트워크 장치, 헤드엔드 센터의 디바이스들을 타겟으로 한 DDoS 공격은 치명적인 손실을 입힐 수 있다. DDoS 공격을 받은 서비스 공급자는 정상적인 서비스 제공이 어렵게 되며 이로 인해 정당하게 서비스를 받아야 하는 가입자들에게 서비스를 제공할 수 없게 된다.[5]

서비스 공급자와 가입자 구간 사이에 존재하는 네트워크에도 보안 취약성은 어김없이 존재한다. 불의의 목적을 가진 비가입자가 가입자로 가장하거나 셋톱박스에 잘못된 정보를 전송할 수 있다. 이처럼 네트워크 중간에 콘텐츠를 위조하거나 변조를 통해 셋톱박스로 전송할 수 있는 취약성도 존재하는 것이다.

IV. 인터넷기반 방송서비스 보안 모델

국내 IPTV 사업자는 앞에서 설명한 취약성으로 인한 금전적 피해나 고객의 개인정보 유출 등을 예방하기 위한 보안 메커니즘의 구축은 필수적이다. 이를 위한 각종 대응 방안을 수립 및 계획을 진행하고 있으며, IPTV 보안 기술에 대한 연구도 활발히 진행해 오고 있다. IPTV 기술은 IP 프로토콜을 기반으로 하기 때문에 기존의 IP 네트워크에서의 보안 취약성들을 IPTV의 보안 취약성을 그대로 포함하게 된다.

따라서 네트워크에서 일어날 수 있는 데이터 가로채기, 데이터의 위변조, 신분 위장, 서비스 거부 등의 공격들이 IPTV 서비스에 대한 잠재적 보안 위협으로 존재한다. 따라서 콘텐츠 보안을 위한 대응 기술을 잘 적용하더라도 네트워크상의 보안 취약점들이 그대로 노출되는 한 IPTV 서비스의 보안 위협은 항상 존재하게 되고 이로 인해 국내 관련 ISP도 보안유지에 지속적인 노력을 아끼지 않고 있다.

현재 국내는 IPTV에 대한 보안가이드라인을 발간하거나 IPTV 정보보호정책서[6] 등 서비스 정보보안 정책서, 서버

보안 지침 등 10가지가 넘는 정보보호 지침서를 발간하고 있다. 또한 IPTV 운영 지침서, NW부분정보보호 실무지침서, 보안점검 지침서, IT보안 실무 가이드 등 다양한 영역에서의 보안지침서도 발간되었다. IPTV보안을 위해 담당자를 지정하고 정보보호 전담조직을 구성하는 등 실질적인 대응책도 준비되어 있다. 기업 자체적으로 모의 해킹을 통한 콘텐츠 유출 및 고객 정보유출에 대한 대비도 철저히 진행 중이다.

표 2 IP 방송 서비스 보안 모델
Table 2. Security Model of IP Broadcasting Service

Content Security	Service Security	Transport Security
o 콘텐츠 저작권 보호 o 콘텐츠 적법성 보호 o 텐츠 암호화 전송 o 콘텐츠 정보 및 이용기록 관리 o 악성프로그램으로부터의 콘텐츠 보호 o 콘트롤러 입력 신호 보호	o 서비스 침입 예방 o 서비스 접근제어 o 서비스 가용성 가입자 인증 o 가입자 개인정보 보호 o 애플리케이션 가용성과 안전성 o 사용자 결제정보 보호 o 가용성 보호	o 접근 제어와 인증 o 네트워크 엔티티 인증 o 무결성과 가용성 보호 o 보안위협 데이터 패킷 모니터링 o 멀티캐스트 보안 o 암호 기반의 통신 o 키 관리 기술

기존에 보안가이드는 광범위한 부분에 대해서 제시하고 있어 IPTV 서비스에 바로 적용하기 어려운 점이 있다. 본 논문에서 제시하는 한국형 IP 방송 서비스 보안 모델은 각 레벨에서 발생할 수 있는 보안위협을 분류하고 각 보안위협에 대한 대응책을 제시함으로써 기본의 가이드보다 IP 방송 서비스의 보안을 향상시키기 용이하다.

IPTV 서비스는 다양한 플랫폼들과 기술들이 집약되어 제공된다. IPTV 서비스 제공의 프로세스는 콘텐츠를 제작하고, 다양한 콘텐츠들을 제어, 가공하여 서비스로서 제공을 하고, 네트워크를 통해서 콘텐츠를 전송하여, 최종적으로 이용자 단말에서 콘텐츠를 이용하는 과정으로 이루어진다.

따라서 IPTV의 보안도 콘텐츠, 서비스, 네트워크를 통한 전송의 세 가지 클래스로 고려할 수 있다.

표 3 콘텐츠 보안을 위한 정보보호 모델
Table 3. Content Security of IP Broadcasting Service

관련 위협	필요 보안 수준
- 콘텐츠 저작권 위협 - 내부에서의 콘텐츠 유출 위협	보안 시스템으로부터 CAS/DRM 정보를 받아서 콘텐츠에 적용함으로써 콘텐츠의 정보보호 적용
	헤드엔드 내부에 관리자 출입 시 저장 매체나 카메라 등의 반입·유출 통제
- 콘텐츠 저작권 위협 - 서비스 제공 중 콘텐츠 유출 위협	헤드엔드 내부 관리 서버들을 공중망(인터넷)으로부터 철저히 분리
	저작권 보호 메커니즘 적용을 위한 DRM/CAS 서버를 운영하고, 사후 추적 기술 적용
- 콘텐츠 저작권 위협 - 단말장치에서의 콘텐츠 불법 복제 위협	매크로비전과 같은 복제 방지 기술을 적용
	워터마킹 등의 핑거프린팅 기술들을 적용
	단말장치에 설치되는 어플리케이션의 무결성 검사
- 콘텐츠 위법 위협	담당자들의 홍보 및 교육의 주기적인 실시 및 관리자 시스템 사용에 대한 로그 기록 관리
	관리자 권한, 인증과 권한 관리를 안전하고 적절하게 수행
- 통신 도청 위협	민감한 정보(인증, 개인 정보, 거래정보, 승인정보 등)을 통신을 경우 암호화 통신사용
	데이터의 보호 메커니즘과 안전한 파일전송을 위한 메커니즘 사용
- 콘텐츠 정보 악용 위협 - 이용기록 조작 위협	VoD 파일의 경로 정보를 추측하지 못하도록 함
	다운로드 서비스 지원 기능에 대한 로그 기록을 관리하고 불법 이용에 대한 사후추적 관리 대책 마련
- 악성프로그램 감염 위협	사용자가 콘텐츠 파일의 상세 정보를 확인할 수 없도록 조치
	단말장치 전용OS를 사용하고 불필요한 서비스가 구동되지 않도록 조치
	복제 방지 기술 적용 및 적절한 사후 대응 조치
	악성코드 감염·유입에 대한 충분한 사전 대응 수행
- 리모콘 신호 도청 위협	보안 기능을 탑재한 RF 리모콘 사용

1. 콘텐츠 레벨의 정보보호 모델

콘텐츠 저작권을 보호하기 위해 새로 만든 콘텐츠를 보안 시스템으로부터 CAS/DRM 정보를 받아서 해당 콘텐츠에 적용함으로써 콘텐츠의 정보보호를 적용한다. 또한 헤드엔드 내부로부터의 서비스나 고객 관련 데이터 갈취를 예방하기 위해 관리자 출입 시 저장 매체나 카메라 등의 반입 및 유출을 통제한다.

네트워크 트래픽 도청 문제는 원천적으로 해결하기 어렵기 때문에 도청이 되더라도 공격자가 원하는 정보를 어디 못하도록 하는 대응책으로 콘텐츠 다운로드 서버와 단말장치 사이에 민감한 정보(인증, 개인 정보, 거래정보, 승인정보 등)가 존재할 경우 암호화 통신을 권고한다.[7]

콘텐츠 보안을 위해서는 콘텐츠 정보 및 이용기록 관리해야 한다. VoD 파일 경로명을 악용하는 공격에 대응하기 위해 VoD 파일의 경로 정보를 추측하지 못하도록 한다. 예를 들어, 단말장치에서 파일 정보에 대한 접근을 못하도록 하거나, 파일명 무작위화 메커니즘을 사용하여 VoD 경로명 추측 공격이 무력화되도록 할 수 있다. FTP 등과 같은 다운로드 서

비스 지원 기능에 대한 로그 기록을 관리하여 콘텐츠의 불법 이용에 대한 사후추적 관리 대책을 마련한다.

콘텐츠 복제 위협, 악의적 저작권 침해 및 서비스 불법 접근 위협을 해결하기 위해 콘텐츠 파일의 상세 정보를 사용자가 확인할 수 없도록 조치한다. 외부 기기 연결을 통한 콘텐츠 복제를 막기 위해서 복제방지 기술을 적용하고 콘텐츠 복제방지 메커니즘을 우회하여 콘텐츠가 불법 유출된 경우에 적절한 사후 대응을 위한 조치를 해야 한다.

2. 서비스 레벨의 정보보호 모델

서버 장비 취약성으로 인한 악성코드(웜/바이러스)의 유입 감염에 대한 대응 체계를 구축하고 서버 장비 및 기반 기술 취약성 악용 공격에 대비하여 알려진 취약성에 대한 적절한 대응 체계를 마련해야 한다.

콘텐츠 제공 서버와 같이 외부 망에 접속된 서버들의 경우 관련 서버 장비는 웹 서비스(HTTP)와 같은 불필요한 서비스를 제공하지 않도록 조치해야 한다.

악성코드 감염을 통한 개인정보 유출 피해를 막기 위해 콘텐츠 다운로드 서버로의 악성 코드 유입을 원천적으로 차단한다. 이를 위해 콘텐츠 다운로드 서버는 주기적인 콘텐츠를 검사하고 평소 IPTV 서비스를 위해 반드시 필요한 기능을 제외한 나머지 불필요한 서비스나 포트 등은 모두 비활성화 시켜 유입될 경로를 봉쇄한다.

부득이하게 FTP 등과 같이 서비스 데몬이 동작하는 경우 관련 취약점을 분석하고 이에 대한 보안 패치를 수시로 점검 및 설치하여 관련 공격을 사전에 예방해야 한다.

서비스 침입 예방을 위해 악의적으로 저작권을 침해하거나 제공되는 서비스의 불법 접근으로부터 콘텐츠 파일들을 보호하기 위한 대응 조치 방안을 마련해야 한다. 또한 서버로의 불법 접근이나 이상 행위에 대한 사후 추적을 위한 로그를 저장 및 관리한다. 관리 서버 내의 데이터들에 대한 기밀성, 무결성 등을 제공하고 이 데이터들을 언제나 가용한 수준으로 유지할 수 있도록 하기 위해선 관리자가 관리 서버에 접속할 때마다 항상 사용자 인증과 접근제어를 수행하도록 한다.

표 5 전송 보안을 위한 정보보호 모델
Table 5. Transport Security of IP Broadcasting Service

관련 위협	필요 보안 수준
- 실시간 콘텐츠 비인가 시청 - 네트워크 장비 취약성 및 설정 오류 악용 위협	실시간 채널 서비스의 정당한 사용을 보장하기 위한 보안 정책 시행 체계를 구축
- 네트워크 프로토콜 취약성 악용 위협	가입자망 장비에 허가된 단말의 접속만을 허용하도록 적절한 접근제어 조치
- 네트워크 자원에 대한 서비스 거부 위협 - 네트워크 프로토콜 취약성 악용 위협	IGMP 리브 메시지 악용 방지 대책을 마련하고, 조치
- 네트워크 자원에 대한 서비스 거부 위협	대량 트래픽에 의한 서비스 거부 위협에 대응하기 위한 제어 메커니즘 적용 또는 설정
- 네트워크 자원에 대한 서비스 거부 위협 - 네트워크 장비 취약성 및 설정 오류 악용 위협	네트워크 관리자는 장비의 비밀번호를 주기적으로 변경
- 네트워크 장비 취약성 및 설정 오류 악용 위협	시스템 관리자는 장비의 안정적 운영을 위해 적절한 패치 적용을 수행
	시스템 관리자는 장비에 불필요한 서비스를 운영 지양
	적절한 neighbor IP 주소에 해당하는 PIM 메시지만 허용하도록 설정
- 네트워크 도청 위협	거짓 DHCP 서버가 로컬 네트워크 상에 운영되지 않도록 로컬 네트워크 운영 설정에 대한 충분한 검증
- 네트워크 자원에 대한 서비스 거부 위협	RP 병목현상 발생을 막기 위해 트래픽 모니터링을 통하여 과도한 트래픽을 발생에 대응
- 네트워크 장비 취약성 및 설정 오류 악용 위협	PIM 레지스터 메시지에 암호화 또는 적절한 오류탐지 등을 통해 불법적 레지스터 메시지 처리
	라우터 콘솔 접속에 대한 불법적 접근을 통제할 수 있도록 설정
	Neighbor IP 주소만 PIM 메시지를 허용하도록 접근제어 설정

전송 영역의 서비스 거부, DDoS, 비인가 방송, 멀티캐스트 취약성, IGMP 취약성, Noise Insertion, 네트워크 장비 취약성 등의 보안위협을 방지하는 대책도 필요하다. VOD 서비스와 실시간 서비스 인프라 분리와 24시간 보안 관제를 기업 자체적으로 실시, 이상 트래픽을 감시하거나 처리 시스템을 운용하고 인터넷망과 IPTV 망을 분리하여 운용하기도 한다. 나아가 Access 장비에 대한 Rate-Limit 실시, 비인가 시청 제한을 위한 IP확인 및 제한, Packet Signature를 도입하여 Packet 관리, 주기적인 전송망 취약성 점검이 필요하다.

서비스 가용성과 안전성을 위해 서비스 거부 위협이나 위장 접근, 정보 갈취의 위협으로 안전해야 하며, 이를 위해 IP 악용 공격에 대한 대응 조치 등이 필요하며 서버들에 대한 공격 발생 시 안정적인 서비스 운영을 지속할 수 있도록 시스템 백업을 주기적으로 수행해야 한다.

3. 전송 레벨의 정보보호 모델

3.1 접근망 장비

IGMP 불법 조인에 대응하기 위한 보안 정책을 수립하고, 가입자 종단 집선 장치들과 L3 스위치 등에서 정책에 따라 IGMP 관련 설정을 적용한다. 서비스 가입자에게 허가된 채널만 이용 가능하도록 가입자 종단 집선 장치에 MAC 필터링 설정을 하거나, L3 스위치에서 IP 및 IGMP 필터링을 수행할 수 있어야 한다. 또한 멀티캐스트 위협에 대응하기 위해서 L2 스위치에서 허가된 경로 이외의 포트에서 유입되는 멀티캐스트 프레임을 통제하도록 설정한다. L2 스위치의 필터링 데이터베이스 갱신에 따른 위조된 패킷을 사용하는 공격에 대응하기 위해서 L2 스위치의 허가된 경로 이외의 포트에서 들어오는 멀티캐스트 프레임을 차단하는 기능을 가져야 한다.

IGMP 리브 메시지 악용으로 네트워크 자원고갈 피해를 막기 위해 적절한 IGMP 리브 메시지 제어를 수행해야 한다.

3.2 백본망 라우터

Best Effort 기반 인터넷 망에서 QoS 기반의 실시간 IPTV 네트워크로 불필요한 패킷이 유입되지 않도록 통제해야 한다.

헤드엔드 망으로 접근할 경우 외부에서 헤드엔드 내부 구조에 대한 정보를 획득하지 못하도록 헤드엔드 망으로의 연결 부분에 L4 스위치를 통하여 접근하도록 구성해야 하며, 전체 네트워크 구성을 고려하여 방화벽, IDS, IPS 등의 효율적 운용을 통해 불법 접근을 방지하여 네트워크의 신뢰성과 안정성을 증진해야 한다.

망 장비 관리자의 원격 접속에 대한 인증을 강화한다. 예를 들어, ssh 접속만을 허용하게 한다거나 텔넷 접속을 가능하게 할 경우 신뢰할 수 있는 사용자만을 내부 접속을 허용한 후 비밀번호를 변경하여 사용하도록 할 수 있다.

운영체제 및 어플리케이션 취약점을 분석하여 해킹을 시도하는 위협에 대응하기 위해서, 운영체제 및 응용 소프트웨어들의 알려진 취약성에 대해 지속적으로 패치를 하고, 운영체제 상에서는 불필요한 서비스를 제거한다.

IPTV에서 방송 데이터는 멀티캐스트 방식을 이용해서 전송한다. 멀티캐스트 방식은 동일 네트워크에 다른 사용자가 있는 경우 하나의 전송으로 여러 사용자가 받아서 볼 수 있는 특징을 제공한다. 따라서 가입자 정보를 기반으로 채널인증을 하는 경우에는 동일 네트워크의 다른 사용자가 접근하는 것을 방지 할 수 있다. 하지만 이 방식은 사용자의 전송 중간에서 네트워크 가로채기(TCP-hijacking) 기술을 이용해서 연결되어 있는 세션에 대해서 연결을 가로채는 방식의 공격이 가능하다.

그렇기 때문에 결제 모듈을 위한 암호 기반의 통신이나 결제 모듈을 위한 키 관리 기술이 필요하다. 나아가 금융기관과 서비스 사업자간 전송되는 금융정보 등 중요 정보에 대한 비인가 복제, 변경 등의 위협이 있다. 전달 경로에 대한 보안채널 구성 필요하며, 복제 및 변경 등을 모니터링 할 수 있는 기술 적용이 필요하다.

Ⅴ. 결론

IPTV 기술은 다양한 IT 기술과 방송 기술이 융합되어 있는 다차원적 기술로서 안전하고 신뢰성 있는 IPTV 서비스를 제공하기 위해서는 정보보호 기술의 적용이 필수적이다. 사업자의 관점에서는 정보보호 솔루션의 도입이 가져오는 비용 발생이 매우 중요한 고려사항이 되며, 무수히 많은 정보보호 기술들에 대한 충분한 이해가 부족하기 때문에 반드시 필요한 보안 솔루션들을 무시하게 되는 문제를 야기할 수 있다. 따라서 IPTV 사업자들이 안전하고 신뢰성 있는 방송 서비스를 제공하는데 필요한 정보보호 기술들에 대한 이해와 정보보호 정책 수립을 용이하게 하기 위한 대책이 반드시 필요하다.

하지만 공식적으로 존재하는 국제 권고안 X.805와 X.1191은 매우 추상적이라 현장에 바로 적용시키기는 어려움이 많다.

따라서 권고안의 내용을 바탕으로 기본의 가이드를 분석하여 한국 IPTV 서비스 환경을 고려하여 IPTV 보안모델을 설계하였다. 한국형 IPTV 보안모델은 콘텐츠 레벨, 서비스 레벨, 전송 레벨로 나누어 각 레벨에서 발생 가능한 보안위협을 정리하여 보안모델을 설계되었다. 또한 각 레벨에서 발생 가능한 위협을 분석으로 끝나지 않고 위협으로부터 보호하기 위한 보안수준을 제시하였다. 이러한 필요보안 수준 제시를 통해서 중복되는 보안 대책을 제거하여 서비스 관리의 용이성을 향상시켰으며, 부족한 보안대책을 적용하기 용이하다.

이 연구를 통해 앞으로 IP 방송 서비스 보안 모델을 설계하였으며, 보안 모델을 근간으로 하여 IPTV 뿐만 아니라 IT 융합 방송서비스 전반에 걸친 보안성 향상을 가지고 올 수 있을 것이다.

참고문헌

[1] Lark Kwon Choi, “IPTV platform technology and services”, 2007 IPTV Standard Technologies and Services Workshop, 2007.

[2] S.J. Koh, Y.J. Park “Media Convergence, IPTV Policy and Mark”, Electronics and Telecommunications Trends, No.23 Vol.2 , 2008.

[3] C.H. Hyun, “IPTV Policy Proposals for activation”, TTA Journal No.119, pp 38-43, 2008.

[4] Zachary Zeltsanm, “ITU-T Recommendation X.805 and its application to NGN”, ITU/IETF Workshop on NGN, 2005.

[5] J.Y. Parkm, J.Y. Moon, E.H. Paik, “Technology Trends of IPTV Security Service”, Electronics and Telecommunications Trends, No.23 Vol.5, 2008.

[6] “Part II. Section 3, Service security and content protection,” in ITU-T FG Proceedings, Feb. 2008.

[7] Korea Internet Security Agency “IPTV Security Guide for the IPTV Service Provider”, 2009.

[8] Korea Internet Security Agency, “A Study on Analysis of Privacy Invasion and Protection in IPTV”, 2010.

저 자 소 개

서 희 석

2000: 성균관대학교 산업공학과 공학사

2002: 성균관대학교 전기전자및컴퓨터공학과 공학석사

2005: 성균관대학교 전기전자및컴퓨터공학과 공학박사

현 재: 한국기술교육대학교 컴퓨터공학부 부교수

관심분야: 네트워크보안, 보안시뮬레이션, USN

Email : histone@koreatech.ac.kr

김 성 준

2003: 동국대학교 법학학사

2006: 동국대학교 법학석사

2009: 동국대학교 법학박사

2011: 연세대학교 정보대학원 박사과정

현 재: 동국대학교 법학과 겸임교수

관심분야 : 개인정보보호, 산업보안, 네트워크 보안

Email : mvstar@hanmail.net

안 우 영

1988 : 중앙대학교 전자계산학과 이학석사

1999 : 홍익대학교 전자계산학과 이학박사

현 재 : 대전보건대학 바이오정보과 교수

관심분야 : 모바일컴퓨팅, 지식데이터베이스, 바이오인포메틱스

Email : wyahn@hit.ac.kr