Journal of the Korea Academia-Industrial cooperation Society
Vol. 14, No. 6 pp. 3032-3042, 2013

http://dx.doi.org/10.5762/KAIS.2013.14.6.3032

멀티미디어 방송통신 융합서비스에 대한 보안위협 검증 및 대응방안 연구

정찬석[1*], 신용태[1]
[1]숭실대학교 컴퓨터공학

A Study on Verification of Security Threat and Method of Response for Multimedia Broadcasting and Communication Convergence Services

Chan-Suk Jung[1*] and Yong-Tae Shin[1]
[1]**Department of Computer Science, Soongsil University**

요 약 멀티미디어 방송통신 융합서비스는 TV 디바이스에 다양한 인터넷 및 미디어 관련 응용 서비스들을 구동하기 위한 플랫폼 기술을 접목한 새로운 형태의 방송통신 융합서비스이다. 기존의 TV 기술에 임베디드 OS를 탑재하고, 다양한 스마트 응용 서비스를 지원할 수 있도록 하기 위해 OS 위에서 다양한 플랫폼 등을 탑재한 형태의 진화된 TV 기술이라고 할 수 있다. 이렇게 융합된 서비스는 Open IPTV, Smart TV, 모바일 IPTV, N-스크린 등의 멀티미디어 방송통신 융합 신규 서비스가 국내 서비스 3사를 주축으로 활발히 서비스 되고 있다. 하지만 서비스 제공을 위해 인터넷에 접속하고 소프트웨어를 사용하기 때문에 인터넷과 소프트웨어의 취약성을 내제하고 있다. 이러한 취약성은 심각한 보안 사고로 이어질 수 있다. 따라서 본 논문에서는 기존의 보안 위협들과 취약성들을 바탕으로 멀티미디어 방송 서비스 환경에서 발생 가능한 보안 위협들을 도출하였고, 실제로 위협이 보안 사고 등으로 이어질 수 있는지 보안 위협에 대한 검증을 모의 해킹을 통해 실시하였다. 이러한 결과를 이용하여 멀티미디어 방송 융합통신 융합서비스 환경에서의 대응 방안을 제시하였다.

Abstract Multimedia Broadcast communication convergence services are broadcast communication convergence services new form that combines a platform technology for driving the application services of various media-related Internet and TV devices. It is possible to mounted the embedded OS of TV existing technology and to support a variety of smart application services to a TV technology evolved form equipped with various platforms on the OS. The services that are fused in this way, multi-media broadcasting communication convergence new services Open IPTV, Smart TV, mobile IPTV, and N-screen, are services actively focusing on three companies domestic services. However, in order to use the software to connect to the Internet for the provision of services, is inherent software vulnerabilities or the Internet. These vulnerabilities can lead to serious security incidents. Therefore, in this paper, or be able to derive the potential security threats that occur in multimedia broadcasting service environment based on security threats and vulnerabilities of existing threats lead to such security incidents in fact, the security it was carried out through a mock hacking validation for threats. It was also suggested necessary technical security measures that can be protect against security threats revealed by using the verification result through the penetration testing. Has been presented countermeasures in fusion communication service environment of multimedia broadcasting by using these results.

Key Words : Convergence Services, IPTV, N-Screen, T-commerce

[*]Corresponding Author : Chan-Suk Jung(Soongsil Univ.)
Tel: +82-10-9913-6410 email: izmit70@gmail.com
Received March 29, 2013 Revised May 10, 2013 Accepted June 7, 2013

1. 서론

멀티미디어 방송통신 융합서비스는 TV 디바이스에 다양한 인터넷 및 미디어 관련 응용 서비스들을 구동하기 위한 플랫폼 기술을 접목한 새로운 형태의 방송통신 융합서비스로서 완전히 새로운 기술이아니라 기존의 TV 기술에 임베디드 OS를 탑재하여 다양한 스마트 응용 서비스를 지원하는 서비스이다. 그러므로 빠른 기술 진화와 함께 디지털 컨버전스를 통하여 국내· 외에서 유·무선의 통합, 방송과 통신의 융합, 온·오프라인의 결합 등으로 다양하게 확대되고 있다. 방송통신 융합서비스 도입이 확산됨에 따라 Open IPTV, Smart TV, 모바일 IPTV, N-스크린 등의 멀티미디어 방송통신 서비스가 국내 서비스 3사를 주축으로 활발히 서비스되고 있다. 멀티미디어 방송통신 서비스 활성화를 위해서 기존 Walled-Garden 형태의 서비스 제공 방식을 플랫폼 및 네트워크 자원을 개방하여, 누구든지 자유롭게 콘텐츠와 서비스를 제작, 이용할 수 있게 제공하는 개방화 서비스를 제공하고 있다. 개방화 서비스는 사업자가 자사 환경에 맞는 콘텐츠 저작도구(SDK)을 공개하여 자유로운 콘텐츠 및 서비스 개발을 촉진시켰다. 하지만 멀티미디어 방송통신 서비스는 인터넷에 연결되기 때문에 다양한 인터넷 위협에 노출되고, OS 상에서 다양한 시스템 소프트웨어와 응용 소프트웨어가 동작하므로 소프트웨어 취약성으로 인해 야기될 수 있는 보안 위협들이 존재 한다. 충분한 보안 요구사항 분석과 이를 바탕으로 한 보안 아키텍처 설계와 보안 솔루션 적용이 이루어지지 않는다면 매우 큰 보안 사고로 이어질 수 있다. 융합서비스 사업자 측면에서도 플랫폼 개방(SDK 등)에 따라 콘텐츠 제작도구 및 라이브러리 등에 내재된 보안 위협의 상속 가능성이 존재하고, 융합서비스 콘텐츠에 다양한 경로의 보안 위협 가능성이 존재한다. 하지만 멀티미디어 방송통신 서비스의 대표적 신규 서비스인 Open IPTV, 모바일 IPTV, N-스크린 등은 서비스에 적용할 보안대책이 구체화되지 않고, 단지 CAS(수신제한 시스템)나 DRM 중심의 방송 콘텐츠 보호 솔루션을 적용하고 있다. 따라서 망 연동구간(인터넷과 연동 구간, PP 사와의 연동구간, 사업자간 연동구간) 및 주요 시스템에 대한 침해사고 대응책, 정보보호 관리체계에 대한 현황 파악이 되어 있지 않아 신규 보안 위협에 노출되어 있다.

이에 본 논문에서는 대표적인 멀티미디어 방송통신 서비스 환경에서 발생 가능한 보안 위협들을 정의하고, 발생 가능한 보안 위협에 대하여 침해 위험성 테스트(모의해킹)를 통하여 검증하고, 보안 위협별 대응 방안을 제시한다.

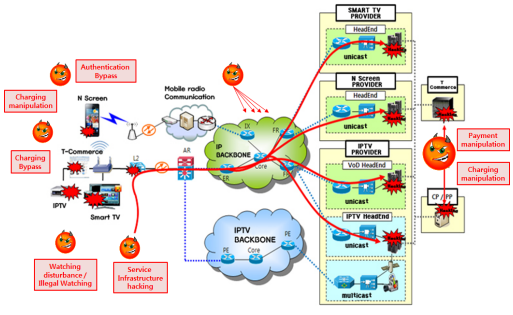
2. 멀티미디어 방송통신 융합 서비스 현황

2.1 서비스 개요

멀티미디어 방송통신 융합서비스는 All-IP망을 기반으로 A/V(Audio/Video)의 방송 또는 멀티캐스트와 데이터(Vod/Data), 음성(Voice, SMS, 영상통화)이 유선통신망, 무선/이동통신망, 방송망이 결합하고, PC와 노트북, 디지털TV, PDA, 스마트폰과 같은 다양한 단말매체를 통해 제공하는 서비스라고 할 수 있다[3].

멀티미디어 방송통신 융합서비스는 방송통신 기술과 서비스를 전통 산업에 접목하여 이종 콘텐츠, 이종 네트워크, 이종 단말기과의 교류를 통해 새로운 조합을 만들어 내는 융합 서비스의 형태를 보이고 있다[4]. 멀티미디어 방송통신 융합서비스의 대표적인 서비스는 IPTV (Internet Protocol Television) 서비스이다. IPTV는 IP 망을 통해 사용자가 원하는 멀티미디어 서비스를 양방향으로 제공하고 있다[5]. IPTV 서비스는 기존 TV (Television)와 PC가 가지고 있는 고유한 서비스 특성을 그대로 가지고 있으며, 최근 유무선 통합망 및 모바일 통신망의 확산으로 다양한 멀티미디어 방송통신 융합서비스로 확대되고 있다[6]. IPTV 기반위에서 OpenIPTV, SmartTV, N-screen, T-commerce 등의 다양한 양방향 서비스가 제공되고 있다. Fig. 1은 IPTV 기반위에서 제공하고 있는 다양한 멀티미디어 방송서비스 개념도 있다[11].

방송통신 융합서비스의 기본이 되는 IPTV의 구성요소는 크게 콘텐츠 서버, 서비스 서버, 셋톱박스(Set-top Box, STB)&스마트카드로 나눌 수 있으며, 그 역할은 다음과 같다.



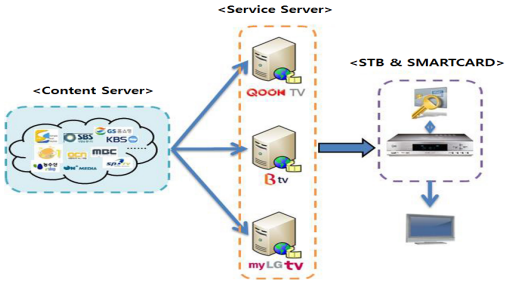
[Fig. 1] Multimedia Broadcasting and Communications Convergence Services Concepts

o STB&스마트카드: STB는 서비스 서버로부터 전송 스트림(Transport Stream, TS)을 수신하여 파싱(parsing)

과정을 거친 후 제어단어(Control Word, CW)로 콘텐츠를 디스크램블링 하는 역할을 수행한다. 이 과정에서 스마트 카드는 가입자를 인증하는 역할을 하며, 합법적인 가입을 통하여 발급받은 스마트카드일 경우에만 CW를 획득하여 콘텐츠를 디스크램블링 할 수 있다.

o 서비스 서버: 가입자를 유치 및 관리 하며, 가입자에게 플랫폼을 제공한다. 또한, 콘텐츠 서버로부터 구입한 콘텐츠를 판매하여 수익을 얻는다. 경우에 따라서 네트워크 제공자의 역할을 동시에 수행하기도 한다. 서비스 서버는 정당한 가입자만 콘텐츠를 시청할 수 있도록 하기 위해 접근제한시스템(Conditional Access System, CAS)을 사용한다. 또한, 서비스 서버는 미들웨어를 제공하는데 미들웨어는 어플리케이션과 디바이스 드라이버 사이에 위치하며 사용자에게 편의를 제공하는 것으로 사업자별로 다양하게 정의 될 수 있다.

o 콘텐츠 서버: 스트림 또는 VoD(Video on Demand) 형태의 콘텐츠를 제공한다. 콘텐츠 서버는 서비스 서버와의 계약을 통해 콘텐츠를 판매하고 그에 따른 수익을 얻게 된다. 콘텐츠 서버는 자신의 콘텐츠에 대한 권익 보호를 위하여 DRM(Digital Right Management) 기법을 사용한다.



[Fig. 2] broadcasting and communication Convergence Services Concepts

IPTV 서비스는 컨텐츠 보호 및 컨텐츠 지적재산권 보호을 위한 보안 기술은 방송분야에서 다루고 있는 CAS(Conditional Access System)기술과 통신 분야(PC)에서 다루고 있는 DRM(Digital Right Management) 기술을 적용하고 있고 최근에는 방통융합 서비스가 핵심 쟁점으로 대두됨에 따라 이 두 기술을 융합한 CAS-DRM 연동 보안 기술이 부각되고 있다[1,7]. Table 1에서는 분야별 컨텐츠 보호기술에 대한 정의를 나타내고 있다[9,10].

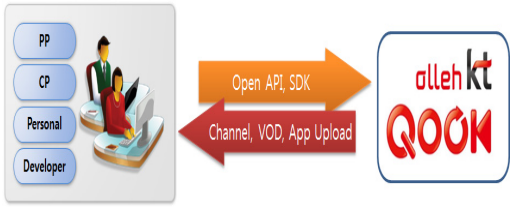
[Table 1] Content protection Techniques

Security Technology field	Description	Remark
DRM (Digital Right Management)	Digital Content and Target the entire distribution process Digital Content Copyrigjt of Protection and Distribution Management A variety of permission / Format Support a variety of content model support	-Standard technology of absence - Interoperability almost impossible
CAS (Conditional Access System)	Broadcasting services / Content Protection / Control target Authorization of program reception for qualified viewer Paid digital broadcasting services / Plenty of code case Defines concrete standards	Broadcasting Service/ Content Restrictions
Copy Protection	Digital content of Illegal Copy Protection function that is transmitted between devices Digital content of Illegal Copy Protection is stored as a recording Device	Limited range Independent functions / Product

2.2 Open IPTV 및 Mobile IPTV 서비스

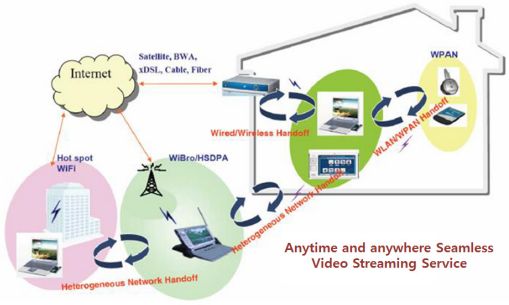
Open IPTV란 인터넷 사업자가 자사 보유한 플랫폼 및 네트워크를 통제하고, 콘텐츠 및 어플리케이션을 선별적으로 수급하여 제공하는 형태(Walled-Garden 서비스)의 서비스 제공 방식에서, 플랫폼 및 네트워크 자원을 개방하여, 누구든지 자유롭게 콘텐츠와 서비스를 제작, 이용할 수 있도록 하는 IPTV 서비스로, 자유로운 콘텐츠 및 서비스 개발, 이용 활성화를 위해 IPTV 사업자는 API 공개 및 SDK 등을 제공한다.

유선인터넷 상에서 이루어진 Open IPTV 서비스가 유·무선 네트워크를 통해 이동성을 지원하여 언제 어디서나 자유롭게 IPTV 서비스를 이용하도록 하는 Mobile IPTV 서비스로 확대되고 있다[2].



[Fig. 3] Open IPTV Outline

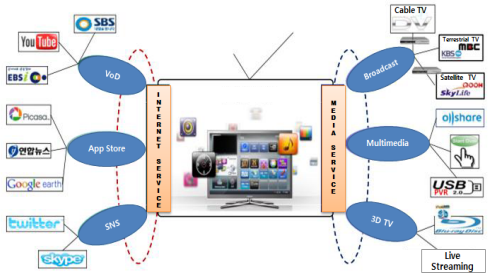
Mobile IPTV는 멀티미디어 서비스를 QoS/QoE, 보안, 이동성 및 양방향 기능이 부여된 유무선 네트워크를 통해 사용자가 송수신 할 수 있도록 서비스를 지원한다. 이러한 서비스를 위해, 콘텐츠 확장성(Scalability), 단말기 및 네트워크 상황에 따른 서비스 제공, 이동성지원, 보안 관리 등이 요구된다. 국내의 경우 와이브로망을 이용한 모바일 IPTV 기술을 개발하고, IPTV 셋톱박스를 통해 디바이스 독립성을 향상시키고, 무선인터넷과 결합하여 다양한 콘텐츠 제공을 하고 있다.



[Fig. 4] Mobile IPTV Concept (ITU-T Standard)

2.3 Smart TV

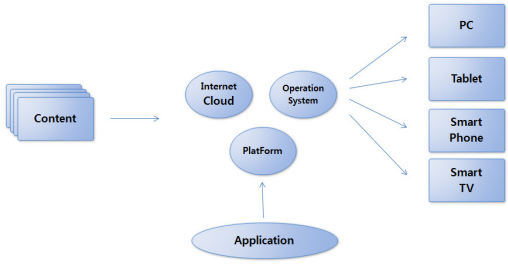
스마트 TV는 인터넷으로 연결되어 있는 TV를 통해 양방향 방송서비스 시청뿐만 아니라, 각종 어플리케이션을 사용할 수는 TV를 말한다. 주요기능은 다양한 서비스를 구동하기 위한 별도의 운영체계와 응용 프로그램 작동을 위한 리소스(CPU, 메모리 등)가 요구되고, TV를 켜면 운영체계 OS와 브라우저 등이 작동되어 서비스 어플리케이션 동작이 가능하도록 제공한다. 사례로 구글 TV의 경우, 안드로이드 OS와 구글 크롬 브라우저 작동하는 방식이다. Smart TV는 TV 앱스토어를 통하여 다양한 형태의 앱 활용이 가능하고, 방송 프로그램 검색, 인터넷 검색, 영상전화, 게임 등의 서비스 제공 및 스마트폰 등과의 연동으로 다중 스크린 서비스를 제공한다[8].



[Fig. 5] Smart TV Composition

2.4 N-Screen

N스크린은 인터넷을 통해 연결된 여러 플랫폼과 단말기에서 사진, 음악, 데이터 및 동영상까지 끊김없이(seamless) 접근할 수 있으며, 콘텐츠를 이동시켜 소비하거나 여러 이용자가 협동적으로 공유 또는 소비할 수 있는 이용환경을 의미한다[12]. N-Screen 환경이 구축되기 위해서는 첫째, 풀 브라우징의 인터넷 연결, 둘째 플랫폼과 단말기 간의 운영체계(OS) 통합, 셋째 클라우드 컴퓨팅(cloud computing)이라는 세 가지 조건이 핵심이다.



[Fig. 6] N-screen Services Concept

2.5 T-Commerce

T-Commerce란, TV의 쌍방향 정보교류를 통한 재화나 서비스의 거래를 의미하여 재화나 서비스의 예약, 주문, 구매 등을 포함하지만, 이에는 거래를 목적으로 하거나 단순 정보추구의 정보검색 행위도 포함 된다[4]. 또한 T-commerce는 양방향 서비스가 가능한 디지털화된 TV를 통해 발생하는 상거래 서비스를 제공하고 TV홈쇼핑 강점과 인터넷쇼핑의 강점이 결합되어 있는 서비스 이다.

3. 국내서비스 현황 및 특성

Open IPTV는 애플 앱스토어의 폭발적인 성공으로 인해, KT, SKBB, LGT 등 IPTV 사업자 및 삼성전자 등 스마트폰 사업자 등이 플랫폼 개방을 추진하고 있다. Open IPTV 주요 서비스는 채널 Open, VoD Open, IPTV 앱 스토어, 개방형 CUG(동호회), SNS(블로그) 등을 제공하고 있다. 유·무선 통합화로 Open IPTV는 Mobile IPTV 서비스로 영역을 확대하고 있다. 국내 사업자인 KT는 Mobile IPTV 서비스 확대를 위해 와이브로망을 이용한 모바일 IPTV 기술을 개발하고, “쿡 TV 모바일 서비스” 도입을 추진하고 있고 SKBB는 “i-스크린 전략”을 발표하여, IPTV 셋톱박스를 통해 디바이스 독립성을 향상시키고, 모바일 TV(티유미디어)는 무선인터넷(네이트)과 결합하

여 다양한 콘텐츠 제공을 추진하고 있다. Smart TV는 삼성전자, LG전자 등의 제조사에서 TV 제조 기술을 바탕으로 스마트 TV 제품을 출시하고 있으며, 구글에서는 안드로이드 플랫폼과 크롬 브라우저 엔진 기술을 앞세워서 구글 TV를 출시했으며, 애플도 자사의 안정적인 에코시스템을 기반으로 애플 TV를 출시하였다.

N-Screen 서비스 경우는 PC, 휴대폰, IPTV 등을 통해 일부 서비스가 제공되고 있으나, 대부분, N-Screen 이용자들은 제공되는 멀티미디어 서비스를 영화, VoD 등으로 인식하고 있으며, AT&T, 애플, 구글, MS, 소니 등 외국 기업뿐만 아니라, KT, 삼성전자 등 국내 통신사 및 전자 업체에서도 N-Screen 서비스를 추진하고 있다. 향후 N-Screen 서비스는 클라우드 컴퓨팅(가상화) 기술과 개방형 미디어 마켓을 활용, 언제 어디서나 IPTV, PC, 모바일 단말로 게임, SW, 콘텐츠 등을 끊김없이 이용할 수 있는 SMART(Semantic, Mobile, Awareness, Reactive, Trinity) Screen로 발전할 것으로 예상된다.

4. 멀티미디어 방송통신 융합서비스 보안위협 및 대응방안

4.1 멀티미디어 방송통신서비스 보안 위협 항목 도출

멀티미디어 방송통신 융합서비스 기술은 IP 프로토콜을 기반으로 하기 때문에 기존의 보안 취약성들을 그대로 포함하고 있다. 따라서 네트워크에서 일어날 수 있는 데이터 가로채기, 데이터의 위·변조, 신분 위장, 서비스 거부, 과금 우회, 인증 우회 등의 공격들이 서비스에 대한 잠재적 보안 위협으로 존재한다. 기존의 방송통신 서비스에 대한 보안 대응책은 주로 DRM 솔루션, CAS 솔루션, Copy Protection을 적용하여 보안 위협에 대응하고 있다. 하지만 신규 방송통신 융합 서비스는 유·무선 통합, 응용 어플리케이션 통합, 다양한 디바이스 호환성 등을 제공하는 서비스로 CAS, DRM의 적용 범위를 넘어선 다양한 신규 보안 위협이 발생 가능하다.

Open IPTV 서비스의 경우, 개방화에 따라 콘텐츠 제작을 위해 지원하는 저작도구(SDK 등) 및 라이브러리 자체에 내재된 보안 위협의 상속 가능성 존재하고, 저작도구(SDK 등) 및 라이브러리를 이용한 IPTV용 콘텐츠에 악성코드 삽입 등으로 인한 정보유출, 셋톱박스에 유해 프로그램 감염으로 좀비화 등의 위협이 발생 가능하며, IPTV 앱스토어를 통한 악성코드 유포, 앱스토어 싸이트 해킹을 통한 콘텐츠 및 사용자 정보 유출 가능성, 셋톱박스 좀비화로 셋톱박스를 이용한 DDoS 공격 등의 보안 위협이 존재한다.

스마트TV는 셋톱박스를 활용하지 않고, TV내에 별도 운영 체계를 구현하고, 앱스토어를 이용한 다양한 서비스를 제공하기 때문에 스마트 TV 디바이스 및 앱 스토어에 대한 신규 위협 발생이 가능하고, 콘텐츠 비인가 획득, 정보유출 및 위장, 패킷 도청, 재전송 공격 등의 보안 위협이 존재한다.

N-Screen 서비스는 콘텐츠 크기/용량 변경, 실시간 정보공유 등 서비스 특성에 따른 보안위협 가능성이 존재한다. N-Screen 단말기의 스크린 크기, 네트워크망의 전송 속도/용량 변경, 콘텐츠의 크기가 변경될 때, 전송구간에서 암호 프로토콜이 해지된 평문 형태의 콘텐츠가 존재하여 불법 복제 등의 보안 위협이 존재한다. 또한 단말기 분실 혹은 가입자 정보 노출시, 공격자의 서비스 제공 서버로 접속을 유도하여 개인 및 그룹의 스케줄/이메일 노출 등의 피해 발생 보안 위협이 존재한다. 기존 유·무선 통합망에서 발생 가능한, 악성코드 삽입, 무선구간 정보 노출, 대량의 패킷 접속 등으로 무선구간 서비스 거부공격, 셋톱박스 등의 보안 위협이 존재한다.

[Table 2] Open IPTV Security Threat Case

Division	Threat / Vulnearability
SDK, API Related Threats	Development environment of SDK vulnerability
	Found hidden code memory using the SDK
	Accessing to unauthorized territory through utilizing SDK function.
	Access to specific memory and acquire an information through SDK debugging tool
	Abusing the vulnerable point of Security module be used in SDK.
앱스토어 운영에 관한 위협	Distribution of malicious code
	App Store Web site attacks
Set-top Box	Set-top box operating system Vulnerability
	DoS Attack by the set-top box

이러한 보안 위협은 크게 서비스에서 공통적으로 발생할 수 있는 공통 보안 위협과 각 서비스의 특성을 고려한 서비스별 보안위협으로 구분할 수 있다.

이에 본 논문에서는 신규 방송통신 융합서비스에서 발생할 수 있는 보안 위협을 공통 보안위협과 각 서비스에서 발생할 수 있는 위협으로 분류하여 35개의 보안 위협 항목을 정의하였다. 정의된 보안위협 항목은 보안 위협 테스트가 가능한 항목으로 정의하였다.

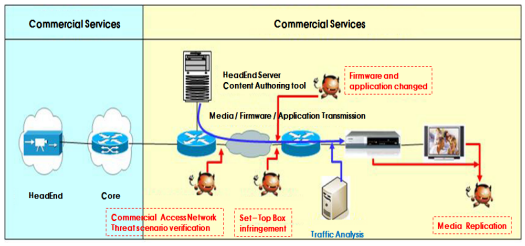
[Table 3] Multimedia Broadcasting and Services Security Threat

Division		Threat
Common Elements	Infrastructure	Infrastructure DDos attacks
		Equipment and web site hacking
Open IPTV	STB	replicated Smard Card
		STB HDD Illegal Access (Mount)
		STB Debug Mode access
		STB Inside the console unauthorized access
		STB identification / Authentication Bypass
		STB malicious code infection
	IGMP	IGMP Join flooding
		IGMP Multi Leave Attack
		IGMP Multicast Packet Replay
		Pay Channels force to IGMP Join
	Content	Content illegal Replication/ circulation
		Real Time/VOD Content Replication
		Paid content charging manipulation
	Authentication Bypass	OPEN market of paid content charging manipulation
		disguised Shopping mall Exploit attacks
		User Open Illegal content transmitted through channels
Smart TV	Operation system	Smart TV Debug Mode Approach
		Smart TV inside console illegal access
		Smart TV identification / Authentication Bypass
		Smart TV malicious code infection
	App Store	App Store Authentication manipulation
	Content	VOD Content illegal Replication
		Paid content charging manipulation
N Screen	Service Deivce	Device inside Approach
	Content	Content illegal Replication / circulation
		Content illegal Replication
		Content illegal Download
		Paid content charging manipulation
		N-Screen Authentication information manipulation
T - Commerce	Authentication	Authentication information disclosure
		Authentication information manipulation
	Payment	Payment information disclosure
		Payment information manipulation

4.2 보안위협 테스트 및 보안위협 검증

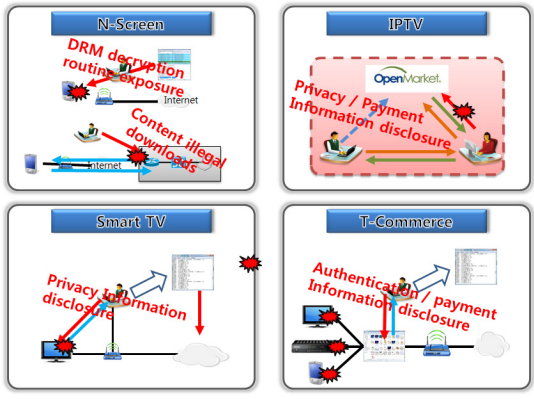
4.2.1 보안위협 테스트 검증

보안위협 침해 위험성 테스트는 도출된 35개의 보안위협 항목 중에서 시험 환경에서 테스트가 가능한 19개 항목에 대하여 침해 위험성 테스트를 수행하였다. 35개의 보안위협 항목 중에서 DDoS 보안 위협 항목과 같은 실 서비스에 영향을 줄 수 있는 항목과 스마트 카드 복제 위협과 같은 고가의 복제 장비가 필요한 항목, STB 악성코드 제작이 필요한 STB 악성코드 감염 위협 등에 대한 항목은 침해 위험성 테스트에서 제외하였다. 침해 위험성 테스트 환경은 Open IPTV 서비스 2개 사업자, N-Screen 서비스 1개 사업자, Smart TV 3개 사업자, T-커머스 모듈 1개 사업자에 대하여 테스트 환경에서 외부에 오픈된 웹 및 서비스 포트로 접근하여 서버 침투 가능성을 테스트 하였으며, 각 서비스에서 제공하는 인증 및 결제 어플리케이션을 분석하여 인증 도용 및 과금 조작 가능성 등을 테스트 하였다.



[Fig. 7] Security Threats Test Environment

보안 위협 침해위험성 테스트 결과 주요 보안 위협으로 개인정보, 결제 정보 노출 및 콘텐츠 불법 다운로드, DRM 복호화 루틴 추출 등 신규 서비스에서 중대한 보안 위협이 취약점으로 도출되었다.



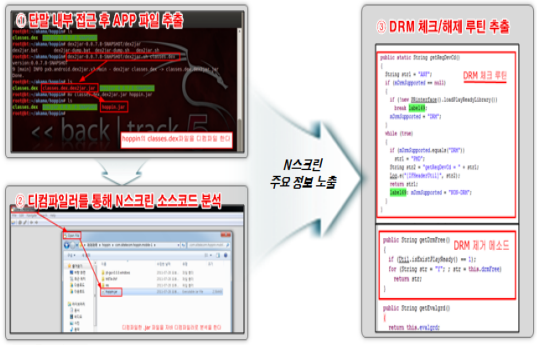
[Fig. 8] Security Threats Test Main Result

19개 보안 위협 테스트 항목 중 N-Screen 2개 항목, 스마트 TV 1개 항목, Open IPTV 1개 항목, T-커머스 1개 항목에 대하여 보안 위협이 존재하는 것으로 확인되었다.

[Table 4] Security Threats Test Result

Division		Threats code	Test results	Security vulnerabilities
Common Elements	Service Infrastructure		NA	Test Except
			P	
Open IPTV	STB		NA	Test Except
			O	
			NA	Test Except
			O	
			P	Identity value disclosure
			NA	Test Except
	IGMP		NA	Test Except
			NA	Test Except
			NA	Test Except
			NA	Test Except
		NA	Test Except	
		Content		
			NA	Test Except
		P	Charging Information Disclosure	
		Authentication		P
			O	
	NA	Test Except		
		Smart TV	Operation system	
			O	
			P	Authentication value disclosure
		NA	Test Except	
	App Store		P	Authentication value disclosure
		Content		NA
	P	Content Information disclosure		
	N Screen	Device		O
		Content		NA
			NA	Test Except
			P	Packet analysis enable
			P	Content Information Disclosure
	P	Authentication information disclosure		
		T-Commerce	Authentication	
		X	Authentication bypass	
		Payment		O

N-Screen 서비스의 경우 스마트폰 설치형 APP 구조인 N 스크린의 경우 단말 루팅, Jailbreak 등을 통해 내부 접근 후 N스크린 APP를 추출하여 디버깅, 디컴파일을 통해 DRM 복호화 루틴 등 N스크린 서비스의 중요 정보가 노출될 가능성이 존재하였고, 콘텐츠 불법 다운로드는 VOD 서비스 콘텐츠에 대해 다운로드 패킷 분석을 통해 PC에서 직접 다운로드가 가능하였으며, 콘텐츠 자체에 DRM이 적용되어 있지 않아 불법 시청이 가능한 보안 취약점이 존재하였다.



[Fig. 9] N-Screen Main App Disclosure of Information

N스크린 APP를 추출 후 디컴파일을 통해 DRM 복호화 루틴의 분석 및 추출이 가능하며, 이를 악용하여 콘텐츠의 DRM을 불법적으로 복호화 가능한 보안 위협 존재한다. 또한 N스크린 VOD 서비스의 콘텐츠에 대해 다운로드 패킷 분석을 통해 PC에서 직접 다운로드가 가능하였으며, 콘텐츠 자체에 DRM이 적용되어 불법 시청 및 유포가 가능한 보안위협 존재한다.

스마트 TV 보안 테스트 점검 결과는 스마트 TV에 내장된 웹브라우저는 SSL Strip 및 Phishing 방지 기능이 없어, SSL 복호화 및 MITM 공격에 취약하였고, 이를 악용하여 정상 사용자가 웹 서핑 시 SSL 복호화 및 MITM 공격을 통해 인증 및 개인정보가 유출되는 보안 취약점이 존재한다. 스마트TV에 대한 ARP 스푸핑 진행 후 HTTPS 요청에 대해 강제로 복호화 하여 HTTP 패킷으로 전송하도록 MITM 공격을 진행하고 스마트 TV의 웹 브라우저를 통해 HTTPS 인증을 사용 중인 Gmail 사이트로 접근하여 로그인 실시하여 공격자의 PC에서 스마트TV의 접

속 로그를 확인한 결과, HTTPS를 사용중인 Gmail의 아이디, 패스워드가 평문으로 유출 가능성이 존재 하였다. 스마트TV에 대한 중간자 공격(MITM)을 통해 웹 인증(아이디/패스워드) 정보 등 개인정보의 유출이 가능한 보안위협 존재한다.

[Fig. 10] N-Screen Content Illegal Dowonload

[Fig. 11] Smart TV Web Browser Authentication and Privacy Exposed Screen

Open IPTV의 경우 쇼핑몰이 DNS/WEB 기반으로 구성되어 있어 MITM 공격에 취약하다. 이를 악용하여 정상 쇼핑몰을 대상으로 위조 웹페이지를 만들어 사용자의 접속을 유도한하여 결재/개인 정보가 유출이 가능하다. Open IPTV공격은 STB에 대한 ARP스푸핑을 통하여 모든 패킷을 수집을 통해 정상 쇼핑몰의 도메인명 및 요청 페이지 확인한 뒤 수집된 데이터를 토대로 위장 쇼핑몰 서버 및 홈페이지를 구축하고, ARP 및 DNS 스푸핑을 통하여 정상 쇼핑몰 사용자를 위장 쇼핑몰로 유도한 후 중간자 공격(MITM)을 통하여 가짜 인증서 발급 후 수집된 모든 SSL 암호화 패킷을 복호화 후 결제/개인 정보를 추출할 수 있다. IPTV STB에 대한 중간자 공격(MITM)을 통해 위조 쇼핑몰로 사용자의 접속을 유도하여 결제/개인 정보의 유출이 가능한 보안위협도 존재한다.

[Fig. 12] Open IPTV Shopping Mall Spoofing Attacks

T-커머스 서비스 보안위협 검증 결과는 T-커머스를 통한 인증 및 결제 시도 시 SSL 인증서에 대한 유효성 검증 루틴이 없을 경우 중간자 공격(MITM)으로 SSL패킷을 복호화하여 인증 및 결제 정보의 유출이 가능한 보안 취약점이 있다. T-커머스 공격은 서비스 단말에 대한 ARP 스푸핑으로 인증 및 결제 패킷을 수집 및 분석하여 T-커머스 인증 및 결제 진행 후 중간자 공격(MITM)을 통하여 가짜 인증서 발급 후 수집된 모든 SSL 암호화 패킷을 복호화를 통해 인증 및 결제 정보를 추출 할 수 있다. T-커머스 인증 및 결제 시 SSL 인증서에 대한 유효성 검증 루틴이 없어 중간자 공격(MITM)을 통해 인증 및 결제 정보가 노출되는 보안 위협이 존재한다.

[Fig. 13] T-Commerce Authentication And Payment Information Exposure

4.2.2 보안위협별 대응 방안

보안 위협 테스트 결과에서 멀티미디어 방송통신 융합서비스에 보안 위협이 존재하고 있다. 제어단어 획득, 프라이버시 침해, 서비스 거부 공격, 콘텐츠 유출, 저작권 침해, 시청 방해, 결제정보 조작 등의 보안 위협이 존재한

다. 각각의 보안위협에 대한 대응하기 위해서는 표 6과 같은 보안 기술을 적용하여 융합 서비스에 대한 보안을 강화해야 한다.

4.2.3 Open IPTV 보안 위협 대응방안

앞에서 확인된 플랫폼(SDK 등)에 내재된 취약점, SDK 구조에 따라 발생 가능한 보안취약점을 사전분석, 콘텐츠 개발 환경(자바 등)에 알려진 보안 취약점을 제거해야 하며, 콘텐츠 업로드 시 악성코드 사전분석 및 콘텐츠 심의절차 마련, TV 앱 스토어 보호를 위해 홈페이지 해킹방지를 위한 대책 마련이 필요하다. 또한 셋톱박스 운영체계 취약점에 대한 주기적인 점검 및 패치를 수행해야 한다.

[Table 6] Security Threats Countermeasures and Applied Technology

Types of Attack	Countermeasure	Applied Technology
Acquired control word	Secure channel formation	cryptographic, key establishment protocol
privacy invasion	Checking the rules of privacy is applied or not., Penalty strengthened	Cryptographic
Denial Service Attacks	Only receive messages from legitimate users	Authentication Protocol, firewall, Security update
Content Disclosure	Application of Contents Copy Prevention Technology, Penalty strengthened	DRM(water marking, finger printing)
Copyright invation	Provision of Contents Protection Technology, Penalty strengthened	DRM, media fittering
Watching disturbance	Mutual authentication between user devices and servers	Authentication protocol, Cryptographic
Charging Information manipulation	Buyer and seller authentication, Ensure the integrity of your payment information	Authentication protocol, Cryptographic, Message signature

제어단어 획득 공격은 CAS에서 제어단어가 전송 및 임시 저장되는 과정에서 쉽게 획득 가능하다는 구조적인 문제에서 비롯된 것이다. 그러므로 제어단어 획득 공격을 막기 위해서는 셋톱박스와 스마트카드 사이에 안전한 채널을 형성하여야 한다. 또한, 임시 저장된 제어단어의 획득을 막기 위하여 소스코드의 난독화와 주기적인 업데이트를 통하여 제어단어 획득을 막는 것이 중요하다. 제어단어 획득에 대한 대응방안을 위해서 적용 가능한 기술들은 암호화와 키 확립 프로토콜이 있다. 제어단어가 평문 형태로 전송되는 부분에서 키 확립 프로토콜을 통해 제어단어를 암호화할 키를 확립한 후, 제어단어를 암호화하여 전송함으로써 제어단어 획득 공격을 방어할 수 있다.

프라이버시 침해는 개인정보와 같은 민감한 데이터를 암호화하지 않는다는 문제에서 비롯된 것이다. 공격자가 악성코드나 패킷 도청을 통하여 데이터를 획득하더라도 암호화 되어 있을 경우, 데이터로부터 사용자의 개인정보를 획득하기는 쉽지 않다. 따라서 민감한 데이터의 암호화를 통하여 사용자의 프라이버시를 보호하는 것이 필요하다. 또한, 프라이버시 관련 규정을 사업자가 잘 적용하고 있는지 여부를 주기적으로 검사하여 미흡할 경우 제재를 가하는 것이 필요하다. 사용자의 개인정보가 유출되었을 경우에도 관련 법규를 적용하여 강력한 처벌을 통해 개인정보의 재사용을 방지하는 것이 필요하다.

서비스 거부 공격 데이터 패킷의 송신자를 인증하지 않는다는 문제에서 비롯된 것이다. 송신자를 인증하지 않음으로 인해서 악성코드에 쉽게 감염될 수 있으며, 이는 DDoS나 PDoS로 연결될 수 있다. 방송통신 서비스 환경은 일반적인 컴퓨터 환경에 비해 폐쇄적인 특성을 지니지만, 이 역시 모바일 IPTV, 개방형 IPTV와 같은 새로운 형태의 서비스가 등장하면서 폐쇄성이 약화된다. 따라서 패킷의 송신자를 인증하여 적합한 데이터만 수신하여 악성코드 감염을 예방하는 것이 중요하다. 또한, 사업자는 가입자의 기기에 방화벽, 백신 프로그램 등을 설치하여야 하며, 새로운 악성코드가 발견되는 즉시 보안 업데이트를 통하여 이를 방어할 수 있도록 발 빠른 조치가 필요하다.

콘텐츠 유출은 콘텐츠를 전송/관리 하는 과정에서 취약점이 발생한다는 문제에서 비롯된 것이다. HDD에 콘텐츠를 저장하거나, 미디어 기기로 전송할 때, 콘텐츠를 암호화하지 않고 평문 형태로 저장한다는 점이 대표적인 예이다. 콘텐츠 유출을 막기 위해서는 콘텐츠 복제방지기법을 적용하는 것이 필요하다. 적용기술로는 워터마킹, 핑거프린팅과 같은 DRM이 있다. 또한, 콘텐츠 유출에 대해 관련 법규를 적용하고 처벌을 강화하여 공격자가 콘텐츠를 획득하였을 경우에도 유출을 사전에 방지하는 것이 필요하다.

저작권 침해 콘텐츠에 저작권 정보를 삽입하지 않거나, 삽입된 저작권 정보를 삭제할 수 있다는 취약점에서 비롯된 것이다. 주로 UCC와 같이 가입자가 콘텐츠를 제작하는 경우에 많이 발생하게 되며, 사업자는 콘텐츠 보호기법을 제공하여 저작권을 보호하여야 한다. 적용기술로는 동영상 필터링 프로그램을 제공하여 UCC를 보호할

수 있으며, 콘텐츠 유출과 동일하게 DRM을 콘텐츠에 삽입하여 저작권을 보호하여야 한다. 또한, 저작권 침해에 대해 관련 법규를 적용하고 처벌을 강화하여 저작권 유출에 적극 대응하는 것이 필요하다.

시청 방해는 방송통신시스템에서 사용자 그룹관리를 위해 사용되는 IGMP 프로토콜과 미디어 스트리밍을 제어하기 위한 RTSP 프로토콜에서 메시지를 인증하지 않는 취약점에서 비롯된 것이다. 이러한 문제를 해결하기 위하여 사용자 기기와 서버 사이의 상호인증을 통해 메시지 검증 과정을 거치는 것이 필요하다. 적용기술로는 상호인증 프로토콜을 통해 합법적인 메시지만 수신하고 처리하는 과정이 필요하며, 전송되는 데이터의 암호화를 통해 메시지 위조를 방지하고 무결성을 제공하는 것이 필요하다.

결재정보 조작 공격은 가입자가 결재 시스템을 이용하는 과정에서 인증이나 암호화가 제대로 설계되어 있지 않은 경우 발생할 수 있는 취약점이다. 이러한 문제를 해결하기 위하여 결제 시스템을 이용하기 전 구매자 및 판매자 상호인증 과정이 필요하다. 또한, 결제를 진행하는 과정에서 결제 정보의 무결성을 보장하는 것이 필요하다. 적용기술로는 인증 프로토콜을 통하여 합법적인 판매자와 구매자를 검증하여야 하며, 전송되는 데이터의 암호화를 통하여 무결성을 보장하는 것이 필요하다. 결제정보의 서명을 통하여 추후 부인방지 기능을 제공하여야 하며, 타임스탬프나 난수를 추가하여 재전송 공격을 방어하는 것이 필요하다.

5. 결론

IPTV는 IP 네트워크를 통해 콘텐츠를 전송한다. 따라서, IPTV 환경에서 발생할 수 있는 보안 취약점은 기존 IP 네트워크에서 발생할 수 있는 보안 위협과 기존 TV 환경에서 발생할 수 있는 보안 위협을 모두 포함하게 된다. 이러한 IPTV 서비스의 특성 상 안전한 IPTV 서비스를 위해 적절한 대응방안을 마련하는 것은 어려운 실정이며, 국내외 IPTV 서비스에 대한 다수의 잠재적인 위협이 존재한다. 또한, 사용자의 편의와 서비스에 대한 욕구를 만족시키기 위하여 IPTV 서비스에 다양한 응용 서비스가 포함되었으며, 무선 네트워크 기술의 발달과 다양한 콘텐츠 확보를 위한 자유 경쟁체제의 구축을 기반으로 모바일 IPTV와 개방형 IPTV와 같은 새로운 형태의 IPTV 서비스가 등장하게 되었다. 다양한 형태의 IPTV 환경은 사용자에게 다양한 서비스를 제공할 수 있다는 장점을 가져다주지만, 새로운 환경의 등장으로 인해 다양한 보안위협을 야기시킬 수 있는 잠재성을 지니게 된다. 따라서, 안전한 IPTV 서비스 제공을 통하여 신뢰성 있는 방송 서비스를 제공하기 위해 잠재적인 보안위협을 분석하고 이에 대한 대응방안을 도출하여 위협을 사전에 방지하는 것이 중요하다.

앞서 설명한 잠재적인 보안위협에 대한 대응방안을 수립하기 위하여 본 연구를 진행하였다. IPTV의 여러 요소기술들의 동향 및 구조에 대해 분석하고 이를 바탕으로 다양한 보안위협을 도출하였다. 기존 TV 환경과 IP 네트워크 환경 및, 두 환경이 결합된 IPTV 환경에 대한 보안 요구사항 모두 고려하여 적절한 대응방안을 제시하였으며, 미래 IPTV 환경에 대해서도 서비스 동향과 발전방향을 충분히 고려하여 보안위협을 도출하고 대응방안을 제시하였다. 본 연구에서는 보안위협 도출의 효율성을 위하여 IPTV를 크게 구성요소, 프로토콜, 응용서비스, 미래 IPTV의 네 범주로 분류하였다. 네 범주를 다시 IPTV 환경에 따라 9개의 카테고리로 분류하였으며, 공격 유형에 따라 7개의 카테고리로 분류하였다. 대분류는 셋톱박스와 스마트카드, 서비스 서버, 콘텐츠 서버, IGMP, RTSP/RTP, VoD, 양방향 서비스, 모바일 IPTV, 개방형 IPTV의 9개 대분류로 나누어 각 카테고리별 특성을 분석하여 발생 가능한 보안위협을 도출하였다. 도출한 보안위협은 공격 유형에 따라 제어단어 획득, 프라이버시 침해, 서비스 거부, 콘텐츠 유출, 저작권 침해, 시청방해, 결제정보 조작 7개로 분류하여 9개의 대분류에서 7개의 공격유형에 대해 발생 가능성을 분석하였으며, 이 외에도 잠재적인 보안 위협의 발생 가능성을 분석하였다.

본 연구를 통해 분석한 보안위협 및 대응방안을 종합하여 IPTV의 잠재적인 보안위협의 발생을 방지하기 위하여 수행하여야 할 대응방안을 제시하였다. 제어단어 획득공격의 대응방안으로는 안전한 채널 형성이 있으며 이와 관련된 기법으로는 암호화, 키확립 프로토콜이 있다. 프라이버시 침해 공격의 대응방안으로는 프라이버시 관련 규정 적용여부를 검사하고 처벌을 강화하는 방안이 있으며, 관련기법으로는 데이터 암호화가 있다. 서비스 거부 공격에 대한 대응방안으로는 합법적인 사용자의 메시지만 수신하는 방안이 있으며 관련 기법으로는 인증 프로토콜, 방화벽, 보안 업데이트가 있다. 콘텐츠 유출의 대응방안으로는 콘텐츠 복제방지기법 적용, 처벌 강화가 있으며, 관련기법으로는 DRM(워터마킹, 핑거프린팅)이 있다. 저작권 침해에 대한 대응방안은 콘텐츠 보호기법 제공, 처벌강화가 있으며, 관련기법으로는 DRM, 동영상 필터링이 있다. 시청 방해에 대한 대응방안은 사용자 기기와 서버 사이의 상호인증이 있으며, 관련기법으로는 인증 프로토콜, 암호화가 있다. 결제정보 조작의 대응방안

으로는 구매자 및 판매자 인증, 결제 정보의 무결성 보장이 있으며, 관련기법으로는 인증 프로토콜, 암호화, 서명이 있다. 이와 같이 공격 유형에 따라 적절한 대응방안을 마련하였으며, 대응방안을 적용하기 위해 필요한 기법들에 대해 분석하였다. 또한, 올바르게 보안 대책을 수립하고 있는지 검증하기 위한 도구로써 대응방안 점검 체크리스트를 작성하였다.

본 연구의 결과를 통해 IPTV 주체들이 IPTV 서비스를 위해 필요한 정보보호 대응방안 들을 충분히 이해하며, 이를 바탕으로 올바른 대책을 마련하는데 기여할 것이다. 각 주체별로 올바른 대책을 마련하여, 알려진 보안위협 및 잠재적인 보안위협에 대해 안전한 시스템을 마련할 수 있으며, 이러한 결과는 곧 IPTV 서비스의 안정적인 제공으로 이어지게 될 것이다. 더 나아가 IPTV 서비스의 신뢰도 향상을 바탕으로 IPTV 시장과 기술의 발전을 가져올 것이며, 세계 IPTV 서비스의 모범이 되어 시장을 이끌어 가기 위한 초석이 될 것이다.

References

[1] Jongyoul Park, Jin-young Moon, Eui-Hyun Paik “ Module based Security system for a Convergence IPTV Service” Korean Institute of Information Technology Spring Conference, 2010

[2] SooHong Park, Mobile IPTV And Standard issue, OSIA Standard & Technology Review, 2007 27 (65)

[3] ChiDeuk Ahn, Broadcasting and Communications Convergence Technology Outlook In the IP Convergence, Mobile Frontier Conference 2008 Presentations, 2008.11]

[4] [A Study on Value Grid for the Convergence of Broadcasting and Telecommunications in U-city].

[5] [O.Gerard, "Next Generation IPTV services and Technologies," Wiley Inter-Science, 2007.]

[6] [S.Park, and S.Jeong, "Mobile IPTV:Approaches, Challenges, Standards, and QoS Support," IEEE Internet Computing, Vol. 13, Issue 3, pp.23-31, 2009. DOI: http://dx.doi.org/10.1109/MIC.2009.65

[7] heekuk Oh, JiHwang Lim, Countermeasures research and analysis of security threat for IPTV component technology, KISA-WP-2010-0070

[8] MoonGu Kim, JongHyung Park, “Smart TV Global Trends and Development”, TTA Journal, No.131,

[9] Young-Hun Jung, Chang-Bo Lee, Kwang-Hyoung Lee, Moon-Seog Jun, "A Study on Secure Contents Transer Based on Home Network", Journal of Korea Academia-Industrial Cooperation Society, Vol 8, No 5, pp. 1114-1121, 2007

[10] So-Yeon Min, Jung-Jae Kim, "A Study on Encrypted Matrix Puzzle for Digital Contents Protection", Journal of Korea Academia-Industrial Cooperation Society, Vol 9, No 4, pp 936-944, 2008 DOI: http://dx.doi.org/10.5762/KAIS.2008.9.4.936

[11] Bo-Seoung Kim, Jeong-Jai Kim, Ki-Young Lee, Yong-Tae Shin, "A Study of Secure Group Key Management Based on Key-Chain for Multicast Data Transmission", Vol 11, No 9, pp. 3495-3501, 2010 DOI: http://dx.doi.org/10.5762/KAIS.2010.11.9.3495

[12] Se-Kyoung, Choi, KOCCA Focus, No 11,(통권 39호), Korea Creative Contents Agency, 2011

정 찬 석(Chan-Suk Jung) **[정회원]**

- 2002년 2월 : 숭실대학교 정보과학대학원 정보통신과 (정보통신석사)
- 2009년 2월 : 숭실대학교 숭실대학원 컴퓨터학과 (박사수료)
- 2011년 4월 ~ 현재 : ㈜엔오비즈 대표이사

<관심분야>
모바일 인터넷, html 5 플랫폼, 정보보호

신 용 태(Yong-Tae Shin) **[정회원]**

- 1985년 2월 : 한양대학교 산업공학과 (공학사)
- 1990년 12월 : Univ. of Iowa, Computer Science (공학석사)
- 1994년 5월 : Univ. of Iowa, Computer Science (공학박사)
- 1995년 3월 ~ 현재 : 숭실대학교 컴퓨터학부 교수

<관심분야>
멀티캐스트, 센서네트워크, 컨텐츠 보안, 모바일인터넷, 차세대인터넷 기술, 정보보호