情 報 保 護 學 會 誌
第21卷 第7號, 2011. 10

방송통신융합서비스 보안위협 및 대응방안 연구

강 석 철*, 박 해 룡**

요 약

최근 디지털 기술의 발달로 방송과 통신의 경계가 허물어지면서 지금까지 없었던 새로운 융합서비스들이 지속적으로 출현하고 있다. 그동안의 방송과 통신은 독자적인 영역을 고집하며 서로 독립적으로 발전해왔다. 하지만, 방송통신융합기술의 발전, 네트워크 성능 향상 그리고 스마트 기기의 폭발적인 증가 등 여러 가지 요인으로 인해 다양한 융합서비스들이 출현 하게 되었으며 빠른 속도로 발전, 확산되고 있다. 논문은 융합서비스의 대표주자인 IPTV 서비스 보안 이슈는 물론 스마트TV, N-Screen, OPEN IPTV 등 IPTV가 발전함에 따라 새롭게 등장하는 융합서비스에 대한 보안위협을 분석하고 그에 대한 대응방안을 제시한다.

Ⅰ. 서 론

최근 방송통신융합기술의 급속한 발전으로 인해 다양한 서비스가 출현하고 있으며, 각종 스마트 기기와 연동하여 빠른 속도로 확산되고 있다. 그동안의 방송과 통신은 독자적인 영역을 고집하며 서로 독립적으로 발전해왔다. 하지만, 디지털 기술의 발전, 네트워크 성능 향상 그리고 각종 스마트 기기의 폭발적인 증가 등 여러 가지 요인으로 인해 다양한 융합서비스들이 출현하게 되었으며 빠른 속도로 발전, 확산되고 있다. 스마트폰 열풍으로 인한 방송과 통신의 융합이 개별적인 수준의 1단계를 지나, 현재까지 구축된 융합 환경과 인터넷/모바일 서비스의 확산에 기초하여 융합 생태계를 형성해 나가는 2단계로 진화하고 있다.

이러한 융합은 경제적인 측면에서 새로운 시장기회를 제공하며, 기업·서비스·기술간 경쟁을 통해 소비자의 선택권을 증가시키는 등 방송과 통신이 융합되면서 사용자나 사업자 모두에게 다양한 장점과 편리함을 가져왔다. 하지만 기존 전파를 매개로 이용되던 방송이 통신과 융합하면서 인터넷망을 이용함에 따라 기존 인터넷이 가지고 있던 보안 위협들 또한 그대로 가지고 왔다. [1]

본 논문을 통해 IPTV의 보안 이슈는 물론 스마트TV, N-Screen, OPEN IPTV등 방송통신융합기술이 발전함에 따라 새롭게 등장하는 융합서비스에 대한 보안위협을 분석하고 그에 대한 대응방안을 제시한다.

Ⅱ. 방송통신융합서비스 종류

방송통신융합서비스는 방송과 통신의 각 요소들이 상호 결합되어 방송통신 서비스 자체를 상승시키는 동시에 이를 타 서비스 분야에 적용하여 보다 더 큰 시장가치를 창출하는 서비스이다. [2] 본 논문에서 말하고자 하는 융합서비스의 종류는 [표 1]과 같다.

〔표 1〕 방송통신융합서비스 정의

IPTV	스마트TV
· 초고속 인터넷망을 이용하여 제공되는 양방향 TV 서비스	· 디지털 TV에 운영체제 및 인터넷 접속 기능을 탑재하여 PC 기능을 포함하는 서비스
N-Screen	**OPEN IPTV**
· 하나의 멀티미디어 콘텐츠를 N개의 기기에서 연속적으로 끊임없이 즐길 수 있는 서비스	· IPTV 서비스 사업자가 자신의 콘텐츠, STB 등을 제 3 사업자에게 공개하여 누구나 콘텐츠를 사고 팔 수 있는 환경을 제공하는 서비스

* 한국인터넷진흥원 (ksc9817p@kisa.or.kr)
** 한국인터넷진흥원 (hrpark@kisa.or.kr)

2.1. IPTV 서비스

IPTV(Internet Protocol Television)는 광대역 네트워크상에서 인터넷프로토콜을 사용하여 소비자에게 디지털 TV 서비스를 제공하는 시스템을 말한다. 양방향 통신이 가능한 인터넷 프로토콜의 특성을 이용하기 때문에 사용자와의 활발한 커뮤니케이션이 가능하다는 장점이 있다. 이런 장점을 이용하여 주문형 비디오(VoD : Video On Demand)는 물론 기존 웹에서 이루어지던 정보검색, 쇼핑, 뱅킹 서비스나 VoIP와 같은 인터넷 서비스를 부가적으로 제공할 수 있게 되었다. 하지만 스마트TV와 각종 융합서비스의 등장으로 서비스 확산에 어려움을 겪을 것으로 예상된다.

2.2. 스마트TV 서비스

스마트TV는 최근 방송·통신 분야의 큰 화두 중 하나이다. 하지만 스마트 TV에 대한 명확한 정의는 없으며 세계 여러 기관에서는 스마트TV를 아래 [표 2]와 같이 정의하고 있다.

현재의 스마트TV 동향은 스마트폰 사업모델이 TV 시장에 그대로 전이되고 있으며 스마트 기기의 다양화와 무선 네트워크의 급속한 발전을 통해 언제 어디서나 사용가능한 TV로 발전하고 있다.

〔표 2〕 스마트TV 서비스 정의

방통위 스마트TV 보고서	LG 스마트TV 포럼 발표자료
· 디지털 TV에 운영체제 및 인터넷 접속 기능 탑재 · 실시간 방송, VoD, 게임, 검색 제공 · 편리한 이용자 환경에서 이용 가능한 TV	· 방송 서비스와 인터넷이 결합하여 실시간 방송뿐만 아니라 앱스토어, 검색, 게임, SNS 등 다양한 콘텐츠를 편리한 UI를 통해 사용할 수 있는 TV
지경부 스마트TV 산업 발전전략	위키피디아
· 방송 시청은 물론 인터넷에 연결되어 컴퓨터의 기능이 가능한 TV · 인터넷 연결을 통한 PC 기능 제공 · 향후 인터폰, 에너지 제어와 같은 스마트홈 서비스 수행이 가능한 TV	· Connected TV 혹은 Hybrid TV라고도 함 · 인터넷, 웹 2.0 그리고 컴퓨터와 TV/STB 간 기술적 융합을 TV혹은 STB에 포함 · 온라인 인터랙티브 미디어, OTT 콘텐츠, VoD에 중점

2.3. N-Screen 서비스

사용자가 구입한 콘텐츠를 단말기가 아닌 클라우드 기반의 서버에 저장함으로써, 사용자가 언제 어디서나 원하는 단말기를 통해 콘텐츠를 이용할 수 있도록 해주는 서비스이다. 현재의 N-Screen 서비스는 콘텐츠를 단순히 모바일 또는 인터넷으로 동시에 시청하거나 공유하는 정도의 수준이다. 미래 N-Screen 서비스는 사용자, 서비스 업체, 콘텐츠 개발 업체 모두에 다양한 이점을 가져올 것이다. 사용자에게는 언제 어디서나 원하는 콘텐츠를 소비하는 것을 가능케 한다. 서비스 업체의 경우에는 동일한 인프라에서 화면을 송출함에 따라 비용절감이 가능하며 콘텐츠 개발 업체 역시 1회 콘텐츠 개발을 통해 다양한 디바이스에 제공이 가능해짐에 따라 콘텐츠 제작비용 절감효과를 가져올 수 있다.

2.4. OPEN IPTV 서비스

기존 유선 초고속망을 기반으로 IPTV 서비스를 제공하는 사업자가 자신의 콘텐츠, STB 등을 개방하여 제3사업자(콘텐츠 사업자 혹은 어플리케이션 개발자 등)에 방송자원을 개방하는 형태의 신규 서비스이다.

기존 IPTV는 폐쇄형으로 사업자가 제공하는 서비스만 제공받을 수 있는 형태였다면 OPEN IPTV는 누구나 콘텐츠 및 어플리케이션을 만들어 사고 팔 수 있는 환경이다. 이러한 환경을 통해 시청자 입장에서는 무수한 콘텐츠 이용이 가능하며 사업자의 경우에는 24시간 제공해야 하는 콘텐츠 확보에 대한 부담을 덜 수 있다.

〔표 3〕 방송통신융합서비스별 특성

	IPTV	스마트TV	N-Screen	OPEN IPTV
서비스망	프리미엄망	일반망	일반망	일반망
서비스방식	양방향	양방향	단방향	양방향
OS탑재여부	X	O	-	-
단말기	STB	STB, TV, 게임콘솔	스마트 기기 및 PC 등	-
사업자 또는 대표조직	KT, SKB, LGU+, AT&T	삼성, LG, 애플, 구글	KT, SK플래닛, APPLE, CJ헬로비전 등	WAC, Korea Apps
서비스명	올레TV, AT&T U-Verse	삼성 스마트TV, 애플TV, 구글TV	올레TV나우, Playy, Tving	K앱스, WAC Service

위와 같은 방송통신융합서비스들은 [표 3]에서 보는 바와 같이 다양한 특성을 가지고 있으며 각 서비스별로 발생할 수 있는 취약점 및 보안위협의 범위도 다양할 것으로 생각된다.

Ⅲ. 방송통신융합서비스 보안 위협

방송통신융합서비스는 기존의 인터넷 프로토콜을 기반으로 동작하기 때문에 IP 네트워크에서의 보안 취약성들이 IPTV의 보안취약성으로서 그대로 포함하게 된다. 또한 스마트 TV나 N-Screen 단말의 경우 운영체제가 포함되면서 기존의 PC가 가지는 취약점 또한 존재한다.

방송통신융합서비스에서 발생 가능한 공격 유형은 데이터 가로채기 및 위·변조, 신분 위장, 서비스 거부(Dos, DDoS) 공격 등 IP 네트워크 취약성으로 인한 공격들과 SQL 인젝션, 버퍼오버플로우, XSS(Cross Site Scripting), CSRF(Cross-Site Request Forgery) 등 기존의 웹과 OS가 가지고 있는 취약점 역시 가능성 있는 공격의 유형이 된다. 본 논문에서는 위에서 언급한 각 서비스 유형별 보안위협을 분류하여 설명한다.

3.1. IPTV 서비스 보안위협

IPTV 서비스는 IP 망에서 이루어지는 서비스이므로 기존의 인터넷 망에서 발생 가능한 보안 위협들에 그대로 노출될 수 있다. 또한 IPTV는 크게 헤드엔드, 기간사업자망(인터넷), 홈 네트워크(STB, 터미널) 등의 구성요소들을 기반으로 이루어지는데 각 영역마다의 취약점을 악용한 공격들이 발생할 수 있다. 이러한 관점에서 IPTV 서비스는 서비스 거부공격, 콘텐츠(VoD) 불법 복제 및 유통 등 다양한 보안 위협들에 노출될 수 있다.

3.2. 스마트TV 서비스 보안위협

스마트TV 서비스는 기존의 TV 형태와는 달리 TV자체 혹은 STB에 운영체제가 탑재되는 특성을 가지고 있다. OS 탑재로 인해 TV의 기능이 스마트폰, PC와 비슷해지며 이들이 가지고 있던 취약점을 가질 가능성이 있다.

가능성 있는 공격 형태로는 스마트TV 웹브라우저를 악용한 MITM(Man-In-The-Middle) 공격을 통한 개인정보와 같은 중요 인증정보 노출 등이 가능하다. 또한 OS 취약점을 악용한 시스템 해킹(오버플로우, OS 보안패치 Zero-Day 공격 등)이나 DoS, DDoS 등과 같은 서비스거부 공격의 가능성도 배제할 수 없을 것이다.

3.3. N-Screen 서비스 보안위협

N-Screen 서비스는 여러 종류의 단말(스마트TV, PC, 스마트 폰이나 패드 등)에서 사용자가 원하는 콘텐츠를 언제 어디서나 볼 수 있는 서비스다. N-Screen 서비스에서는 콘텐츠 보안이 가장 큰 이슈라고 볼 수 있다. 대부분의 콘텐츠에는 콘텐츠보호기술(DRM, CAS, Finger Printing 등)이 적용되어 있다. 하지만 탈옥이나 루팅이 된 스마트 단말기를 통해서 N-Screen 어플리케이션을 디컴파일하여 DRM 체크 루틴을 제거하거나 서비스 중 스트리밍 되고 있는 동영상 다운로드 패킷을 분석하여 다운로드 링크를 알 수 있을 것이다.

3.4. OPEN IPTV 서비스 보안위협

통신사업자가 자사의 고객들에게만 부가적인 요금을 받으며 각종 다양한 콘텐츠와 서비스들을 제공하던 기존 일반 IPTV(Closed)의 성격과는 달리 OPEN IPTV는 서비스 사업자들이 그들의 플랫폼을 개방하여 누구나 콘텐츠나 서비스를 업로드/다운로드 하거나 사고 팔 수 있는 성격을 가지고 있다. 이러한 성격으로 인해 다양한 보안 위협들이 발생할 수 있다. 예를 들어 유료콘텐츠 과금 조작/전가, 불법 어플리케이션 및 콘텐츠 배포, 앱스토어를 통한 악성 어플리케이션 감염 등 다양한 보안 위협들이 존재한다.

Ⅳ. 서비스별 보안위협에 대한 대응방안

3장에서 구분한 융합서비스별 보안 위협과 위협별 대응방안을 정리하면 [표 4]와 같다. 앞서 언급한 융합서비스의 보안위협 및 대응방안을 살펴보면 기존 PC의 취약점(시스템, 웹, 네트워크 취약점 등)과 유사함을 알 수 있다.

Ⅴ. 결 론

지금까지 IPTV와 스마트 TV, N-Screen, OPEN IPTV 등의 융합서비스의 종류, 보안위협과 그에 대한

〔표 4〕 방송통신융합서비스별 보안 위협 및 대응방안

구분	세부 위협 내용	대응방안
IPTV 보안위협	콘텐츠 불법 시청	콘텐츠 보호기술 적용(DRM, CAS, Finger Printing 등)
	데이터 스니핑을 통한 주요 정보 도청	서버 단말 간 인증 기법(SSL) 사이트 전체 적용
	다량의 VoD 요청 메시지 전송을 통한 서비스 거부 공격	인증 프로토콜, 방화벽, 주기적인 보안 업데이트
스마트TV 보안위협	OS취약점을 악용한 시스템 해킹	스마트기기에 내장되는 OS의 불법사용(탈옥, 루팅 등) 방지 기술 개발 및 지속적인 OS 업데이트
	악성코드 감염	
	탈옥을 통한 위험노출	
	서비스거부공격	DDoS 전용백신 설치 및 주기적인 OS 보안 업데이트
	인증정보 노출	서버/브라우저 간 인증 기법(SSL) 사이트 전체 적용
	웹취약점(XSS, SQL 인젝션 등)	신뢰할 수 없는 사이트 접근 금지 및 주기적인 백신 업데이트
N-Screen 보안위협	해킹된 단말 내부 접근을 통한 정보 유출	스마트기기에 내장되는 OS의 불법사용(탈옥, 루팅 등) 방지 기술 개발 및 지속적인 OS 업데이트
	콘텐츠 불법 복제 및 배포	콘텐츠 보호기술 적용(DRM, CAS, Finger Printing 등)
	DRM 해킹을 통한 콘텐츠 불법 복제	N-Screen 어플리케이션에 코드레벨 난독화적용 또는 디버깅 방지 기능추가
OPEN IPTV 보안위협	MITM 공격을 통한 유료 콘텐츠 과금 조작	서버/브라우저 간 인증 기법(SSL) 사이트 전체 적용
	위장 앱스토어 구축을 통한 결제 정보 추출	서버 단말 간 네트워크 세그먼트 분리, 사용자 단말에서 접근하는 쇼핑몰에 대한 유효성을 검증할 수 있는 루틴 필요
	저작권에 위배되는 콘텐츠 불법 송출	사용자 콘텐츠 검증 프로세스를 통해 불법 콘텐츠 업로드 방지
	콘텐츠 결제정보 조작	인증 프로토콜, 암호화 메시지 서명 등을 통한 결제 정보의 무결성 보장

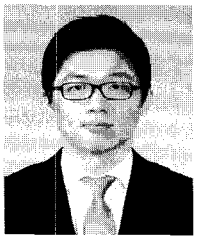
대응방안 등에 대해 살펴보았다. 방송통신융합 기술의 개발로 인해 다양한 서비스의 출현과 대중화는 향후 경제적으로 큰 파급효과를 기대해도 좋을 만큼 발전하고 있다. 하지만 융합기술을 위한 보안 기술의 개발은 매우 미흡한 상황으로 판단할 수 있다. 이러한 융합기술들에 대한 보안 문제가 해결되지 않은 상태에서 스마트TV, N-Screen, OPEN IPTV 등의 서비스가 대중화된 후, 보안 문제의 심각성이 제기된다면 그 상황에서의 보안문제는 더욱 어려운 문제로 남게 될 가능성을 배제할 수 없다. 따라서 현재의 시점에서의 융합서비스들의 보안상 취약점을 발견하고 그 해결책으로서 보안요구사항들을 도출하여, 서비스가 개발, 적용되는 시점에서 포함시킬 수 있어야 한다. 본 논문에서는 방송통신융합서비스 현황과 각 서비스별 보안취약점 및 대응방안에 관하여 기술하였다. 안전한 융합서비스의 사용을 위해서는 본 논문에서 기술한 융합서비스별 취약점과 대응방안을 점차적으로 해결하고 관련 보안 기술을 개발해 나가야 할 것이다. 또한, 앞으로의 융합은 다른 다양한 분야와도 연동되어 그 범위가 커질 것으로 예상되므로 발생 가능한 서비스를 미리 예상하여 그에 대한 보안 이슈 사항을 도출해야 할 것이다.

참 고 문 헌

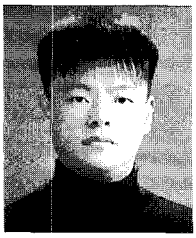
[1] 전파연구소, "방송통신 융합 연구 보고서", 방송통신위원회, pp. 35, 2010

[2] 강도현, "방송통신 융합서비스 활성화 방안", Kodima Digital Medians, pp. 4, Aug 2010 Volume 11

〈著者紹介〉



강 석 철 (SokChul Kang)
비회원
2010년 2월 : 대구가톨릭대학교 정보통신공학과 학사
2011년 3월~현재 : 성균관대학교 정보보호학과 석사과정
2010년 7월~현재 : 한국인터넷진흥원 서비스인프라보호팀 주임연구원
관심분야 : 정보보호, IPTV 등



박 해 룡 (Haeryong Park)
종신회원
1999년 2월 : 전남대학교 수학과 학사
2001년 2월 : 서울대학교 대학원 수학과 석사
2006년 8월 : 전남대학교 정보보호협동과정 박사
2000년 12월~현재 : 한국인터넷진흥원 서비스인프라보호팀 팀장
관심분야 : 암호알고리즘 설계 및 분석, 신규 IT서비스 정보보호, 주요 정보통신 기반보호