N-Screen 방송융합서비스의 모바일 환경에서 보안 위협 연구

지성인*, 서희석*

요약

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 내게 되었다. 또, 여러 단말기에서 같은 플랫폼과 클라우딩 시스템을 기반으로 하여 다른 단말기에서도 같은 콘텐츠를 이용하도록 하는 N-Screen 서비스가 대두되고 있다. 최근, Smart Phone, Tablet PC에 이어 Smart TV까지도 등장하면서 N-Screen 서비스의 상용화가 멀지 않았음을 말해주고 있다. IPTV 등의 IT융합서비스는 IP기반 네트워크 기술과 방송기술의 결합을 기반으로 하기 때문에 기존 인터넷에서의 위협들이 그대로 나타날 수 있다. 이러한 IT융합서비스의 보안 메커니즘을 올바르게 적용하기 위한 N-Screen에서의 보안 위협과 취약점을 도출하고자 한다.

A Study on Security Threat of Broadcasting Convergence Service and Mobile Environment for N-Screen

Seong-In Ji*, Hee-Suk Seo*

ABSTRACT

Today, new television service is activated called IPTV. Content delivery method called VOD(Video On Demand) can watch the program which viewers want to watch. And be on the rise N-Screen Service which use same platform and clouding system in multiple terminal. Recently, Smart Phone, Tablet PC and Smart TV is appear, so it is said N-Screen Service is becoming. IT convergence service like IPTV as appear threaten on the original internet, because it is stand on the basis IP network and broadcasting technology. Therefore, security threaten and weak point should be identified for Security mechanism of IT convergence service is correctly applied.

Key Words : IPTV, N-Screen, Security Threat, Smart Platform, IT Covergence Service, IPTV Security

* 한국기술교육대학교 컴퓨터공학부(✉seongin26@kut.ac.kr)
· 제1저자(First Author) : 지성인 · 교신저자(Correspondent Author) : 서희석
· 접수일(2012년 1월 5일), 수정일(1차 : 2012년 2월 6일), 게재확정일(2012년 2월 8일)

Ⅰ. 서 론

최근 IPTV, Mobile TV등의 방송과 통신이 융합된 새로운 방송서비스가 전 세계적으로 큰 인기를 끌고 있다. 인터넷 망을 이용한 인터넷 텔레비전 서비스로, VOD서비스 등 자신이 원하는 프로그램만 원하는 시간에 골라 볼 수 있는 IPTV와 장소에 구애받지 않고 가벼운 휴대폰 등의 단말기를 이용하여 방송을 시청할 수 있는 Mobile TV는 매력적인 방송서비스가 아닐 수 없다. 이러한 방송통신 융합은 통신과 방송이 상호 결합하여 방송의 풍부한 콘텐츠를 통신의 양방향성과 결합하여 이용자에게 보다 편리하고 다양한 서비스를 제공하는 것을 의미한다.[1] 국내에서는 2008년부터 주요 통신 3사에서 IPTV 서비스를 시작한 이후, 가입자 수가 꾸준히 증가하고 있다. 국내 사업자들은IPTV 활성화에 따라 방송, 교육은 물론 금융 서비스 , 게임 등 다양한 부가서비스를 제공함으로써 새로운 수익모델을 창출하였다. 하지만 많은 서비스를 제공하고 개인정보, 금융정보 등 많은 정보를 담고 있지만, 해당 정보가 충분히 보안되고 있는지에 대해서는 의문점이 든다. 다양한 부가서비스를 제공하며 정보를 수집하여 보안 위협에 노출될 경우 엄청난 피해를 입을 수 있으므로 보안의 강화에 신경써야 한다.

이 외에도 최근에는 N-Screen이라 불리는 서비스가 대두되고 있다. 이는 여러 단말기에서 같은 플랫폼과 클라우딩 시스템을 기반으로 하여 서로 다른 단말기에서도 같은 콘텐츠를 이용하는 서비스를 말한다. Smart Phone, Tablet PC는 이미 일반인들에게서 흔히 볼 수 있는 상품이 되었고, 최근 상용화되기 시작한 Smart TV까지 가세하여 본격적인 N-Screen 서비스를 준비하고 있다. 이는 플랫폼 단일화를 통해 휴대폰, PC, TV 등 다른 단말기에서 같은 콘텐츠, 서비스를 이용할 수 있도록 하는 N-Screen 서비스의 상용화가 멀지 않았음을 말해주고 있다. 이렇듯, 여러 단말기에서 같은 콘텐츠를 이용하게 된다면, 하나의 단말기에서의 악성코드 감염이 전체 단말기의 악성코드 감염으로 번질 우려가 있다. 이를 방지하기 위해서는 N-Screen 서비스의 기반이 되는 스마트 플랫폼에서의 보안이 크게 강화되어야 한다고 생각된다.

IPTV 등의 IT융합서비스는 IP기반 네트워크 기술과 방송기술의 결합을 기반으로 하기 때문에 기존 인터넷에서의 위협들이 그대로 IPTV 서비스의 위협이 될 수 있다.[2] 많은 가입자가 이용하고 있는 IT융합서비스에서 위협들을 사전에 방지하고 이용자의 정보나 콘텐츠들이 유출되지 않기 위해서는 올바른 보안 메커니즘을 적용한 보안의 강화가 필수적이다. 하지만 그 전에 어떠한 보안위협과 취약점이 존재하는 지를 명확히 분석해야 올바른 보안 메커니즘을 적용할 수 있을 것이다. 이에 따라 본 연구에서는 IT융합서비스들의 보안 위협과 취약점을 분석해 보았다. 2장에서는, IPTV와 N-Screen 서비스를 포함한 전체적인 방송서비스에서의 보안 위협 및 취약점에 대해 알아본다. 3장에서는, N-Screen 서비스에서 나타날 수 있는 스마트 플랫폼에서의 보안 위협 및 취약점에 대해서 알아본다.

Ⅱ. 방송서비스 보안 위협 및 취약점

이 장에서는 IPTV와 N-Screen 서비스를 포함한 방송통신융합서비스에서 발생할 수 있는 취약점에 대해서 말한다. 전체적인 방송서비스에서의 취약점을 이 장에서 말하고, 다음장에서는 N-Screen 서비스에만 해당되는 취약점에 대해 말할 것이다. IPTV 서비스는 크게 콘텐츠 공급, 서비스 공급, 가입자의 3단계로 이루어져 있다고 생각해 볼 수 있다.[3] 콘텐츠 제작자가 콘텐츠를 만들고, 이를 다른 사업자가 서비스하여 가입자에게 제공되는 식이다. 이 과정에서 사소한 피해를 입는 취약점부터 서비스 전체, 사업자, 가입자의 개인 정보 등이 피해를 입을 수 있는 중대한 취약점까지

다양한 취약점이 존재한다. 또한 서버실, 사업자의 통신망, 개인 단말기 등에서의 각 구성요소들도 취약점을 가지고 있을 수 있다. 이 장에서는 각각의 단계에서 존재할 수 있는 취약점에 대해 알아보도록 한다.

2.1 콘텐츠 공급 단계에서의 보안 위협 및 취약점 존재

콘텐츠 공급 단계에서의 위협에서는 저작권 문제를 빼놓을 수 없다. 아직 서비스가 시작되지 않은 단계인 만큼 이 단계에서 콘텐츠가 유출된다면 저작권 문제가 커질 수밖에 없다. 헤드엔드 내부의 관리자의 패스워드 노출 등으로 인한 위협이 존재하고, 저작권 등록 이전에 단순히 내부 직원에 의해 외부에 유출 될 수도 있다. 또, 서비스 제공을 위해 연결된 네트워크로 인한 악의적인 접근으로 통신이 도청당해 콘텐츠가 유출될 수도 있다. 새로운 콘텐츠가 저작권 보호 메커니즘이 적용되기 전에는 사후 추적의 문제점이 존재하기 때문에 더욱 주의해야 한다.

2.2 서비스 공급 단계에서의 보안 위협 및 취약점 존재

서비스 공급 단계에서도 역시 올바른 저작권 메커니즘이 적용되지 않은 콘텐츠의 유출 가능성이 가장 크게 대두된다. 또, 인터넷과 직접적인 연결이 되어 있기 때문에, 도청 위협과 함께, 악성코드에 감염되는 경우도 빼놓을 수 없다. 특히 서비스 공급 단계는 콘텐츠 공급자와 가입자 모두와 연결되어 있기 때문에 악성코드에 감염되는 경우 이 양방향에도 악성코드를 확산시킬 수 있는 위협이 존재한다.

2.3 가입자 단계에서의 보안 위협 및 취약점 존재

가입자 단계에서는 가정에 설치된 단말기 즉, 셋톱박스의 문제점이 취약점으로 연결될 수 있다. 이미 가입자들에게 공급된 기기는 사업자가 각 기기들의 상태를 확인할 수가 없다. 때문에 사용자가 고의적으로 셋톱박스의 기술을 노출시키거나 개조하는 등의 방법을 사용하여 취약점을 드러낼 수 있다. 또, 이렇게 개조된 셋톱박스를 통해, 악성코드가 감염되어 셋톱박스에 저장되어 있는 사용자의 결제 정보, 개인 정보 등이 유출될 위협이 존재한다.

그림 1. 악성코드 침투에 의한 콘텐츠 유출
Fig. 1 Contents outflow of malignant code invasion

2.4 악의적 목적의 서버, 네트워크 접근 위협

앞에서 나눈 3가지 보안 위협 외에 악의적 목적으로 서버와 네트워크에 접근하는 위협도 생각해 볼 수 있다. 먼저, 서버 장비와 기술에 대해 이미 알려진 취약점을 이용한 공격이 실행될 수 있다. 또, 외부에서 서버로 연결할 수 있는 통로가 있다면 그 자체가 위협적이 될 수 있다. 불필요한 서비스나 포트를 사용하여, 신뢰되지 않는 프로그램이 실행되는 경우 등 외부 기기 연결을 통해 클라이언트에서 악의적인 접근을 할 위험성이 생기기 때문이다. 이 외에도, 해킹, TCP 세션 하이재킹, 서비스 거부 공격(DoS), 위장 접근, IP 스푸핑, TCP SYN, UDP Flooding 등 여러 네트워크 공격이 감행될 수 있다. 이렇듯, 공개된 네트워크 프로토콜, 오픈된 포트 등 외부와 연결된 모든 곳에 위협이 존재한다고 말할 수 있다.

III. 스마트 플랫폼 보안 위협 및 취약점

최근 모바일 시장의 패러다임이 개방형으로 변화함에 따라, 모바일 단말에서도 사용자에게 다양한 애플리케이션과 콘텐츠 제공이 가능하도록 하는 모바일 소프트웨어 플랫폼에 대한 관심이 증가되고 있다.[4] 이와 함께 대두되고 있는 N-Screen 서비스는 PC, Smart Phone, Tablet PC, Smart TV의 플랫폼을 단일화시켜 다른 단말기에서도 같은 어플리케이션과 콘텐츠를 이용할 수 있는 서비스를 말한다. N-Screen 서비스에서는 동일한 플랫폼, 클라우딩 서비스가 기본이 되기 때문에 한 단말기에서만 악성코드에 감염되더라도 모든 단말기가 위험해질 수 있다. 때문에 사용하는 플랫폼의 보안이 무엇보다도 중요하다고 할 수 있다. 본 연구에서는 스마트 플랫폼에서의 공격방법은 크게 2가지로 분류하는데 웹을 통한 공격과 앱을 통한 공격으로 생각할 수 있다. 현재, N-Screen 서비스를 적극 추진하고 있는 플랫폼은 현재 Apple사의 iOS와 Google사의 Android, Microsoft사의 Windows를 꼽을 수 있다. 하지만, 아직 Windows Mobile이 탑재된 휴대폰은 점유율이 미미하고 성장단계에 있기 때문에 아직 충분히 성장하지 못했다고 판단하여 이 취약점 분석에서 제외하였다. 이 장에서는 iOS와 Android, 두 플랫폼에서 나타났던 취약점과 앞으로 나타날 가능성이 있는 위협에 대해 알아보도록 한다.

그림 2. 높은 점유율을 보이는 두 스마트 플랫폼
iOS(왼쪽), Android오른쪽)
Fig. 2 Two smart platform which have high share
iOS(left), Android(right)

3.1 모바일 플랫폼 보안 취약점

1) Apple사의 iOS

현재 전 세계에서 높은 점유율을 가진 Smart Phone과 Tablet PC를 얘기하면 Apple사의 iOS를 탑재한 아이폰과 아이패드를 빼놓을 수 없다. 최근에는 iOS5 업데이트를 통해 iCloud라는 본격적인 클라우딩 시스템을 도입했고, Smart TV 출시로 N-Screen 서비스 도입이 사실상 멀지 않았다고 볼 수 있다. Apple사는 앱스토어에 등록되는 앱들에 대한 검사를 엄격히 하고 있어 앱을 통한 취약점은 현재로서는 발견되지 않고 있다.

과거 iOS 4.3.3 이하버전에서 iOS에 기본적으로 탑재된 웹브라우저 Safari가 링크가 걸린 PDF파일을 자동으로 읽어오는 기능에서대두된 취약점이 있으나 iOS 4.3.4 버전이 배포된 이후로 이렇다 할 문제점이 드러나지 않고 있다. Apple사는 공식 앱스토어에 등록되는 앱들을 철저히 관리하기 때문에 웹을 통한 공격이 아니라면 취약점이 쉽게 발견되지 않을 것으로 보인다.

표 1. iOS 4.3.3 이하 버전에서 드러난 문제점[5]
Table 1. Problem in below iOS 4.3.3

대상 단말기	iPod Touch, iPhone iPad
홈페이지 방문에 의한 공격	1. PDF를 Base64로 인코딩
	2. 웹페이지에 PDF 직접 삽입
	3. 웹페이지 접속 시 어플리케이션 설치 여부 확인
	4. 설치 버튼을 누를 경우 PDF가 읽혀지면서 공격
악의적 PDF 실행에 의한 공격	1. 웹페이지에 접속
	2. PDF가 실행되며 취약점으로 다른 파일 다운로드
	3. 해당 파일로 다른 파일 다운로드
	4. 연속적인 악의적 파일 다운로드

2) Google사의 Android

Google사의 Android 역시 세계 모바일 시장에서 높은 점유율을 가진 플랫폼으로 iOS와 함께 거론된다. 최근 4.0 버전 아이스크림 샌드위치(ICS)를 통해 Smart Phone과 Tablet PC의 플랫폼 단일화를 이루었다. 하지만 운영체제 자체가 오픈소스인 만큼 취약점이 쉽게 발견되고 있고, 공식 마켓에 등록되는 어플리케이션에 대한 관리를 Apple사 만큼 철저히 하지 않아 악의적 앱들이 많이 배포되고 있다. 또, 공식 안드로이드 마켓과 통신사에서 운영하는 마켓이 아닌 제 3자가 운영하는 써드-파티(Third-Party) 마켓이라고 불리는 제 3의 마켓도 존재해 검열되지 않은 악의적 앱들이 많이 퍼져 있다.

최근에는 모든 Android OS가 탑재된 휴대폰에 큰 영향을 미칠 수 있는 '허가 단계 취약점'이 발견 되었다.[6] 공격자에게 임의로 허가를 내줘 앱을 설치하는데 동의 여부를 묻지 않는 것으로, 악의적으로 이용될 경우 큰 피해를 입을 수도 있다. Android OS는 오픈소스이고 마켓에 등록되는 앱들에 대한 관리가 Apple사에 비해 철저하지 않은 만큼 앱과 웹을 통한 양방향에서 모두 지속적으로 취약점이 발견될 것으로 보인다.

표 2. Android 허가 단계 취약점
Table 2. Android permission level weakness

대상 단말기	Adnroid OS가 탑재된 모든 단말기
공격 방법	1. 일반 애플리케이션 실행
	2. 해당 앱에서 특정 버튼을 통해 사용자의 동의를 묻지 않고 악의적 어플리케이션 설치
	3. 악의적인 앱을 통해 개인 정보 추출

3.2 잠재 보안 위협

앞에서도 언급했듯이 현재 Apple사는 앱스토어에 등록되는 어플리케이션들을 철저히 감시하고 있다. 때문에 일명 탈옥이라고 불리는 행위를 하지 않은 단말기에서는 현재까지 어플리케이션을 통해 문제가 된 적은 없었다. 하지만 최근 HTML5의 발전과 함께, 앞으로는 모바일 단말기에서 웹이 큰 힘을 가질 것이라는 분석이 나오기 때문에, 웹을 통한 공격에 대해 감시를 소홀히 해선 안된다. Google사의 Android는 이미 어플리케이션을 통한 악성코드의 사례가 몇 차례 발견된 바 있다. Android는 웹을 통한 공격에 대해서도 철저히 관리를 하는 한편 마켓에 등록되는 어플리케이션의 관리도 어느 정도 강화할 필요성이 있다. 일반인이 어플리케이션 이름만 보고 악성코드인지 아닌지 파악할 확률은 매우 낮다.

1) 추가 파일 다운로드를 이용한 공격

먼저, 어플리케이션 내에서의 추가 파일 다운로드로 인한 문제에 대해 생각해 볼 수 있다. 현재 iOS와 Android 두 플랫폼 모두에서 특정 어플은 어플리케이션을 실행하면 공식 앱스토어나 마켓을 거치지 않고 자체적으로 인터넷에 연결하여 추가 파일을 다운로드 하게 되는 부분이 존재한다. 이 때, 추가 파일에 악의적 코드가 포함되어 다운로드 될 수 있다. 추가 다운로드 이전에 어플리케이션에는 악성코드가 포함되어 있지 않기 때문에 어플리케이션 감시를 통과하고, 이 추가 다운로드를 통해서 의도적으로 악성코드를 배포할 수 있는 위협이 생길 수 있다. 이 문제를 해결하기 위해서는 Apple사와 Google사에서 먼저 추가 다운로드를 받아 확인해보거나, 공식 앱스토어와 마켓을 통한 업데이트가 아닌 자체적 추가 파일 다운로드를 불가하도록 해야 한다.

표 3. 추가 파일 다운로드를 이용한 공격 가상 시나리오
Table 3. Virtual scenario of attack for download additional file

대상 단말기	모든 스마트폰
공격 방법	1. 악의적 코드가 포함되지 않은 어플리케이션 제작
	2. 해당 어플리케이션으로 어플리케이션 심사 통과
	3. 어플리케이션 내에서의 추가 파일 다운로드를 통해 악의적 코드 삽입
	4. 삽입된 악의적 코드를 통해 피해 유발

2) 좀비 스마트폰의 활동

최근 분산 서비스 거부 공격(DDoS)에 활용되어 널리 알려진 좀비PC라는 것이 있다. 좀비PC란 컴퓨터가 악성코드에 감염되어 실제 컴퓨터 이용자가 아닌 제 3자에 의해서 원격 제어되거나 악성코드 확산, 다른 시스템을 공격하는 데 사용되는 PC를 말한다. 주로, DDoS 공격을 감행하는데 필요한 수많은 PC를 얻기 위해 해커들이 사용한 방법이다.

안철수연구소에서는 2012년 한해 예상되는 주요 스마트폰 보안 이슈 중 하나로 좀비폰 및 봇넷 본격적 활성화를 꼽았다.[7] 손바닥 안의 컴퓨터라고 불리는 Smart Phone도 좀비의 위험에서 벗어날 수 없는 것이다. 만약 Smart Phone이 해커들에게 조종당하는 '좀비폰'이 되는 경우에 생길 피해는 엄청날 것이다. 대부분의 개인이 각 1대씩 소지하고 있고, 거의 하루종일 부팅되어 있는 휴대폰이 DDoS 공격을 같이 감행한다면, 서버의 가벼운 마비는 물론, 일반인들의 데이터 폭탄 요금이 부과될 수 있다. 아직까지는 좀비폰에 대한 눈에 띄는 활동이 보고되지는 않았지만 앞으로도 계속 없을 것이라는 보장은 없다.

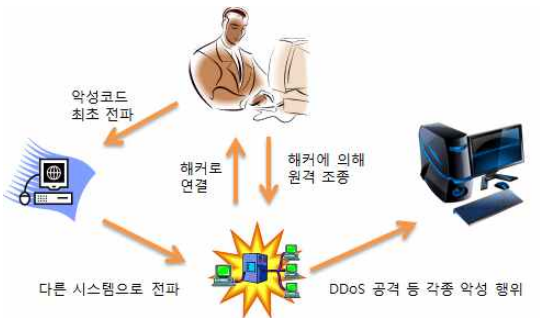

그림 3. 좀비 PC의 활동
Fig. 3 Activity of Zombie PC

Ⅳ. 결론

본 연구에서는 방송서비스와 스마트 플랫폼에서의 보안 위협과 취약점에 대해 알아보았다. 앞에서 살펴보았듯이 콘텐츠 유출에 의한 저작권 문제는 방송서비스에서 빼놓을 수 없는 문제이며 끊임없이 야기되고 있다. 콘텐츠는 올바른 저작권 메커니즘이 적용된 이후에 배포될 수 있어야 한다. 그리고 셋톱박스의 개

조 등 사용자 고의로 위협에 노출시키는 경우도 주의해야 한다. 원칙적으로는 사업자가 각 가정에 설치된 셋톱박스를 확인할 수 없지만, 더 큰 피해를 막기 위해 주기적으로 방문검사하는 등의 방법을 통해 막아야 할 것이다. 또, 서버와 네트워크에 악의적인 접근이 시도되지 않도록 항상 주의하고 감시해야 할 것이다.

상용화되지 얼마 되지 않은 Smart Phone이나 Tablet PC는 최근 가입자 수가 급속도로 증가했고 앞으로도 꾸준히 증가하여 아마 거의 모든 사람들이 사용하게 될 것으로 보인다. 또 단말기들의 플랫폼이 단일화되는 만큼, 특정 플랫폼에 대한 사람들의 의존도는 높아지고 있다. 이러한 상태에서 플랫폼의 취약점이 발견되고, 공격당한다면 엄청난 피해를 입게 될 수 있다. 본문에서 예로 들었듯 iOS와 Android 모두에서 이미 위협적인 문제들이 발견된 바 있다. 모바일 단말기는 앞으로 꾸준히 발전될 것이고, 해커들의 기술도 발전될 것이다. 기존에 발생했던 취약점들을 지표로 삼아, 앞으로 발생할 수 있는 취약점들에 대해 생각해보고, 미리 방지할 수 있어야 할 것이다. 또, 스마트 플랫폼 개발사에서는 플랫폼의 꾸준한 업데이트 뿐만 아니라 공식 앱스토어와 마켓 등에 등록되는 어플리케이션의 감시 또한 소홀하지 않아야 한다.

IPTV등의 방송통신융합서비스 기술은 다양한 기술이 융합되어 있는 다차원적 기술로써 안전하고 신뢰성 있는 서비스를 제공하기 위해서는 정보보호 기술의 적용이 필수적이다. 하지만 IPTV 서비스를 위한 보안 기술은 인터넷이 가지고 있는 양방향성과 방송이 가지고 있는 대중성을 기반으로 하고 있고,[8] 다차원적 기술인만큼 정보보호 솔루션을 사용하는 것 자체에 어려움도 있다. 서비스 사업자들이 안전하고 신뢰성 있는 서비스를 제공하기 위해 필요한 기술들에 대한 이해와 정보보호 정책 수립을 용이하게 해야 할 것이고 그 이전에 보안 위협과 취약점에 관해 알아둘 필요가 있다.

추후 연구에서는 보안 위협을 통해 시나리오를 작성하고 요소 위협 별 대응 방법에 대해 연구하고자 한다.

본문에서 살펴보았듯, IT융합서비스와 모바일 환경에서는 쉽게 드러나 있는 취약점도 있고, 잘 알려지지 않은 취약점도 있을 것이다. 하지만 드러난 취약점이든 아니든 악용당한다면 피해를 입을 것임은 분명하다. 취약점을 분명히 파악하고 정보보호 솔루션을 올바르게 적용하여 안전한 방송통신융합서비스와 모바일 단말기의 이용이 이루어지도록 해야 할 것이다.

참고문헌

[1] 정보통신연구진흥원, "*국내 IPTV 서비스 이용 특성 및 확산 방향*", 2009.06

[2] KISA(한국정보보호진흥원), "*IPTV 사업자 정보보호 가이드 개발 연구*", 2009.06

[3] 금융보안연구원, "*금융부문IPTV 보안가이드*", 2010.12

[4] D. H. Kim, C. Ryu, J. H. LEE S. .J. Kim,"*Mobile Software Platform Trends for Smartphone,*" 2010.06

[5] 데일리시큐, "*[iOS] 취약점 상세한 공격방법과 대응책은 이렇다*", 2011.07

[6] ZDNet, "*안드로이드 OS, 또 보안 취약점 발견*", 2011.09

[7] etnews, "*안랩 '2012 년 좀비 스마트폰 등장 가능성 경고*", 2012.01

[8] 박종열, 문진영, 백의현, "*IPTV 융합 서비스를 위한 보안 기술 동향*", 2008.10

감사의 글

본 논문은 2010년도 정보(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2010-0021951).

저자소개

지성인(Seong-In Ji)

2010~현재 한국기술교육대학교 컴퓨터공학부 공학사 과정

※ 관심분야 : IPTV, N-Screen, Mobile Platform

서희석 (Hee-Suk Seo)

2000년 성균관대학교 산업공학과 학사

2002년 성균관대학교대학원 전기전자 및 컴퓨터공학과 석사

2005년 성균관대학교대학원 전기전자 및 컴퓨터공학과 박사

2005년~현재 한국기술교육대학교 컴퓨터공학부 부교수

※ 관심분야 : 모델링&시뮬레이션, 네트워크보안, 보안 시뮬레이션, USN