융합서비스 환경에서의 보안 취약점 분석

윤성열*, 박석천**
경원대학교 전자계산학과
e-mail:existmaster@naver.com scpark@kyungwon.ac.kr

Analysis of Security Vulnerability in Convergence Environments

Sung-Yeol Yun*, Seok-Cheon Park**
Department of Computer Science, Kyungwon University

요 약

시스템 또는 네트워크 자원을 공격 대상으로 하는 서비스 거부 공격 및 분산 서비스 거부 공격의 문제가 심화됨에 따라 이런 DDoS 공격이 일반 인터넷상에서의 공격보다 VoIP 서비스, IPTV 서비스, 스마트폰 등 융합서비스를 대상으로 시도 될 수 있다. 본 논문에서는 DDoS 공격이 융합서비스를 대상으로 하는 경우를 고려하여 각각의 플랫폼의 보안 취약점을 분석하였다.

1. 서론

통신망에 발달에 따라 다양한 분야에서의 인터넷기반 서비스들이 등장하게 되었다. 특히, 인터넷이 진화한 형태인 융합서비스망은 다양한 플랫폼과 서비스, 네트워크가 결합한 형태로써 대표적인 서비스로는 IPTV, 스마트폰, VoIP 등이 있다.

이런 융합서비스는 기존 인터넷이 가지고 있는 특징을 그대로 가져오게 되는데, 보안의 취약점도 함께 가지고 온다. 게다가 각각의 서비스에 특화된 취약점도 추가적으로 고려하게 되어 결국은 많은 보안 인프라가 필요하게 된다.

특히, 다양한 위협 중에 일반인들에게 잘 알려져 있으면서 빈번한 해킹사고를 일으키는 것 중의 하나로 분산서비스거부공격(DDoS:Distributed Denial-of-service)을 꼽을 수 있다[1].

본 논문에서는 이런 DDoS 공격을 대비하기 위해 융합서비스에서의 플랫폼 별 보안 취약점을 분석한다. 각각의 서비스별로 도출되는 보안 취약점은 스마트폰의 경우 OS를 중심으로 도출하고, VoIP는 프로토콜을 중심으로, IPTV는 장비를 중심으로 도출한다.

2. 스마트폰의 보안 취약점

스마트폰에서의 보안 취약점은 주로 모바일 바이러스에 의한 위협을 들 수 있다. 모바일 바이러스란 개인정보를 유출하고 DDoS 공격 등 악의적인 용도의 소프트웨어로 사용자의 허가 없이 자가 복제를 하고 다른 기기(스마트폰 등)를 감염시킬 수 있는 프로그램을 말한다.

이런 모바일 바이러스의 공격 대상은 Content, Mobile Device, Network(Infra 포함) 등으로 스마트폰 기반 이동통신 서비스 전 구간에 걸쳐 영향을 줄 수 있다. 스마트폰 환경이 되면서 다양한 네트워크 인터페이스를 통해 다양한 인프라와 연동함으로써 모바일 바이러스의 감염 경로가 다양해지고 감염 확률이 높아진다.

스마트폰은 운영체제에 따라 그 취약점이 상이한데, 최근까지 출시된 스마트폰의 운영체제는 크게 3가지가 있다. Window Mobile, Google Android, Apple MAC OS X 로 구분되는데, 이런 OS에 따라 상이한 취약점은 멀티태스킹, 스마트폰 OS 및 API의 OPEN, 안전한 콘텐츠 공급 프로세스, 네트워크 보호 기술 항목의 해당사항에 따라 결정된다[2].

2.1 Microsoft Windows Mobile

Windows Mobile을 사용하는 스마트폰의 경우 일반 PC의 Windows와 유사한 동작환경을 제공한다. 따라서 PC에서의 위협 요소가 모바일 환경에 그대로 적용 가능한데, 먼저 멀티태스킹을 지원하기 때문에 백그라운드 서비스에 바이러스 및 해킹 툴이 동작할 수 있는 환경이 제공된다. 그리고 OS는 공개되지 않았으나 API는 공개 되어 누구나 쉽게 스마트폰의 어플을 제작할 수 있다.

컨텐츠 공급 프로세스를 분석해보면 다른 OS와는 다르게 별도로 실행가능한 프로그램을 검증할 수 있는 프로세스가 없고, OS 자체 코드서명은 존재하지만 서명이 안 된 프로그램에 대해 사용자가 설치를 허락할 경우에는 정상적으로 설치가 된다는 점이 보안상 큰 허점이다.

네트워크 보호 기술로는 WPA/WPA2 Personal / Enterprise를 제공하고 TSL/SSL, VPN 기술을 제공한다.

---

* 경원대학교 일반대학원 전자계산학과 박사과정
** 경원대학교 IT대학 정교수(교신저자)

표 1은 Microsoft Windows Mobile의 취약점을 요약한 것이다.

<표 1> Microsoft Windows Mobile의 취약점 분석

항목	분석 결과	설명
멀티태스킹	지원	• 백그라운드 실행 가능
OPEN OS	X	
OPENS API	O	• MSDN에서 제공
안전한 콘텐츠 공급 프로세스	△	• MS 별도 검증 프로세스 부재 • OS 코드서명은 존재 • 서명되지 않은 프로그램 설치 가능
네트워크 보호 기술	제공	• WPA/WPA2 Personal / Enterprise 제공 • TSL/SSL, VPN 기술 제공

2.2 Google Android

Google Android는 Java를 기반으로 하여 최근에 출시되는 스마트폰에 탑재되고 있다. 특히 스마트폰뿐만 아니라 다양한 Embedded 기기에도 탑재되어 향후 가장 주목받는 운영체제이다. Android 운영체제는 멀티태스킹을 기본적으로 지원하여 백그라운드 서비스의 실행이 가능하다. 또한 OS와 API가 모두 공개되어있기 때문에 스마트폰 내에서의 데이터 구조 및 동작 방식이 누구든지 파악할 수 있다는 것을 의미한다.

Android의 특징 중 하나는 안전한 콘텐츠 공급 프로세스에 있다. 코드 서명이 의무화 되어 있어 비교적 안전하게 프로그램을 이용할 수 있다. 그러나 Google의 자체적인 강력한 컨텐츠 검증 절차가 없기 때문에 악성 프로그램을 조기에 발견하여 차단할 수 있는 제도가 불가능 하다.

네트워크 보호 기술은 Microsoft Windows Mobile과 동일하고 기타 보안 기술로 Permission 기반 Secure Sandbox 기반 시스템을 들 수 있다. 이는 타 어플리케이션이 Permission 없는 요청을 거부할 수 있기에 어플리케이션 간 간섭이 발생하지 않는 특징을 가지고 있다. 표 2는 Google Android의 취약점을 분석한 것이다.

<표 2> Google Android의 취약점 분석

항목	분석 결과	설명
멀티태스킹	지원	• 백그라운드 실행 가능
OPEN OS	O	
OPENS API	O	
안전한 콘텐츠 공급 프로세스	△	• Google 별도 검증 프로세스 부재 • 코드 서명이 의무화
네트워크 보호 기술	제공	• WPA/WPA2 Personal / Enterprise 제공 • TSL/SSL, VPN 기술 제공

2.3 Apple MAC OS X

Apple MAC OS X는 아이폰에 탑재되는 운영체제로써 다른 운영체제에 비해 강력한 보안상의 이점을 가지고 있다. 먼저 멀티태스킹의 경우 원래는 불가능 하였으나, 최근 버전(4.0)의 경우 부분적으로 멀티태스킹을 허용한다. 그러나 여기에서의 멀티태스킹은 프로그램의 마지막 지점을 저장하고 다른 프로그램을 실행 시키는 방식을 취함으로써 백그라운드에 불법 프로그램이 동작하지 않게 설계되었다.

Apple MAC OS X는 OS는 공개되어있지 않지만 API는 공개되어 있다. 그리고 콘텐츠 공급 프로세스는 모든 스마트폰 중에서 가장 안전하다. 코드 서명이 의무화 되어 있음은 물론 Apple 자체적으로 강력한 검증 프로세스를 보유하고 있기 때문이다. 또한 Android와 동일하게 Sandbox 기반의 시스템을 도입하여 각 어플리케이션이 아이폰 내 안전한 공간에 설치되며, 다른 어플리케이션에서 접근을 할 수 없도록 OS가 설계되어 있다.

그러나 아이폰의 경우 탈옥(Jailbreak)을 하게 되면, 애플의 앱스토어에 의해 인가되지 않은 어플리케이션의 설치 및 실행이 가능하게 되기 때문에 보안에 상당히 취약한 상태가 된다. 표 3은 Apple MAC OS X의 취약점을 분석한 것이다.

<표 3> Microsoft Windows Mobile의 취약점 분석

항목	분석 결과	설명
멀티태스킹	부분 지원	• 프로그램의 중지점을 임시 저장
OPEN OS	X	
OPENS API	O	
안전한 콘텐츠 공급 프로세스	O	• Apple의 강력한 검증 프로세스 보유 • 코드 서명이 의무화
네트워크 보호 기술	제공	• WPA/WPA2 Personal / Enterprise 제공 • TSL/SSL, VPN 기술 제공

3. VoIP의 보안 취약점

VoIP는 기존 TCP/IP 기반의 공격위협을 상속받고, 신규프로토콜 취약성을 이용한 공격 기법들이 많다. 이로 인해 프라이버시 침해, 서비스 품질 저하 야기, 불법 서비스 사용 등 피해 발생 VoIP 서비스 확산에 장애물로 작용한다.

특히 교환 장비나 단말의 경우 DDoS 공격에 취약점이 존재한다. 우선 VoIP에서의 DDoS 공격은 다양한 계층(L2~L7)의 DDoS 공격이 발생 가능하다.

기존에 DDoS 공격 툴은 TCP/IP 계층을 대상으로 공격하고, SIP-Specific 툴은 응용계층(SIP/RTP) 대상으로 공격한다. 응용계층의 공격으로는 SIP floods(INVITE flooding, Request Looping, Malformed 메시지 등), RTP floods(RTP Insertion, RTP play-out 등)가 있다[3].

4. IPTV의 보안 취약점

IPTV는 아직까지는 폐쇄망의 구조로 DDoS 공격의 위협이 다른 서비스에 비해 적지만, 향후 개방형 구조를 취할 때 다음과 같은 취약점이 발생 할 수 있다[4].

4.1 PMS, BBS/OSS, IP 미디어 플랫폼 시스템

PMS, BBS/OSS, IP 미디어 플랫폼은 IPTV 서비스에서 서비스 가입자에 대한 핵심 정보를 처리하고 관리하므로 해커들에 주공격 대상이 될 확률이 높다. IPTV 서비스와 같은 폐쇄형 네트워크라고 해도 중요 서버나 시스템은 악성코드에 언제나 노출될 우려가 있으며 이로 인한 정보 유출, 시스템 마비 등이 있을 수 있다.

4.2 셋톱박스

데이터통신 중 사용자가 STB를 통해 웹 사이트를 접속하게 될 경우 악성코드 공격이 가능하다. 마찬가지로 웹 환경에서의 세션 하이재킹 등의 공격도 시도될 수 있다.

5. 결론

인터넷 기반 서비스의 등장으로 융합 서비스 환경에서의 DDoS 문제가 심각하게 다루어지고 있다. 이러한 DDoS 공격은 스마트폰이나 VoIP, IPTV 등에서 시도될 수 있으며, 각각의 서비스에서 특수하게 발생되는 DDoS 공격 방법이 존재한다.

본 논문에서는 시스템 또는 네트워크 자원을 공격 대상으로 하는 서비스 거부 공격 및 분산 서비스 거부 공격의 문제가 심화됨에 따라 이런 DDoS 공격이 일반 인터넷상이 아닌 VoIP 서비스, IPTV 서비스, 스마트폰 등 융합서비스를 대상으로 하는 경우를 고려하여 각각의 플랫폼의 보안 취약점을 분석하였다.

향후 본 논문에서 분석한 자료는 융합서비스 환경에서 발생할 수 있는 DDoS 공격에 대한 기초자료로 활용될 수 있다.

참고문헌

[1] 정현철, “안전한 인터넷전화 서비스제공을 위한 보안대책”, KISA, 2009.6

[2] 김기영, 강동호, ″개방형 모바일 환경에서 스마트폰 보안기술″, 한국정보보호학회, 정보보호학회지, 제 19권 제5호 2009. 10, pp. 21~28

[3] 박진범, 백형구, 원용근, 임채태, 황병우, “VoIP 보안 취약점 공격에 대한 기존 보안 장비의 대응 분석 연구”, 정보보호학회지 제17권 제5호, pp. 57 ~ 65, 2007. 10

[4] 박종열, 문진영, 김정태, 백의현, ″IPTV 서비스를 위한 보안 기술″, 한국통신학회, 한국통신학회지(정보와통신), 제25권 제8호 2008.7, pp. 32~38