Cross-service 공격 탐지를 위한 메커니즘 제안

오승희* · 한종욱*

*한국전자통신연구원 SW콘텐츠연구부문 정보보호연구본부 융합서비스보안연구팀

The proposal of detection mechanism against Cross-service attack

Seung-hee Oh* · Jongwook Han*

Convergence service security Research Team, Information Security Research Division,

S/W Content Research Laboratory, Electronics and Telecommunications Research Institute

E-mail : seunghee5@etri.re.kr

요 약

네트워크 환경이 컨버전스(convergence)되면서 하나의 단말에서 제공하는 서비스 역시 다양화되고 있다. 개인용 휴대 단말들도 기존에 개별 기능만을 주로 다루던 형태에서 다양한 융복합 서비스를 하나의 단말에서 제공하는 형태로 발전하고 있다. 따라서 본 논문에서는 컨버전스 네트워크 환경에서 제공되는 여러 서비스를 동시에 지원하는 단말을 "복합단말(All-in-one Mobile Device)"이라 정의한다. 복합단말은 기능, 성능, 네트워크 인터페이스 측면에서 다양한 컨버전스가 제공되고 있는데, 이 중에서 다양한 네트워크 인터페이스의 제공으로 인터페이스간 교차로 인해 기존에 존재하지 않았던 새로운 형태의 보안 위협인 Cross-service 공격이 등장하고 있다. 기존 모바일 디바이스와는 달리 복합단말에서의 Cross-service 공격은 사용자에게 과금이나 배터리 소모와 같은 치명적인 문제점을 발생시킨다. 본 논문에서는 Cross-service 공격으로부터 복합단말을 보호하기 위한 탐지 메커니즘 및 보안 요구사항을 제시한다.

키워드

네트워크 보안, 복합단말, Cross-service 공격

Ⅰ. 서 론

현재 유선 인터넷 위주의 네트워크는 통신과 방송, 유무선 및 이동 통신이 통합된 융복합 네트워크 형태로 발전하고 있으며, 이러한 융복합 네트워크 환경에서 제공되는 서비스는 지금보다 다양하고 통합된 형태로 진보하고 있다.

융복합 네트워크의 발전과 더불어 개인용 단말도 기존의 이동 통신 단말(Mobile Telecommunication Device)과 개인 휴대 단말(Personal Handheld Device)의 특징, 기능, 및 서비스가 통합된 형태로 진화하고 있으며 이러한 형태의 개인용 단말을 복합단말(All-in-one Mobile Device)이라 정의한다.

따라서, 향후에는 융복합 서비스를 지원하는 복합단말이 기존의 핸드폰, PC 및 노트북을 대신하여 생활 필수품이 될 것이며, 복합단말에는 다양한 서비스 제공을 위한 중요 개인정보(민감 데이터)가 포함되게 된다.

복합단말 사용자들은 갈수록 고도화, 지능화, 다양화되고 있는 침해 시도로부터 복합단말내의 중요 개인정보를 보호하기 위한 보안 기능들이 요구된다.

본 논문의 구성은 다음과 같다. 2장에서는 복합단말의 정의, 특징 및 복합단말 내에서 발생 가능한 보안 위협에 대해서 살펴보고, 3장에서는 여러 보안 위협 중에서 Cross-service 공격이란 무엇이며 이를 탐지하기 위한 매커니즘에 대해서 제시한다. 4장에서는 Cross-servcie 공격을 예방하기 위해 요구되는 보안 요구사항을 분석하고, 5장에서는 향후 연구 계획을 언급하고 결론을 맺는다.

Ⅱ. 복합단말의 보안 위협들

본 장에서는 개인휴대단말의 진화과정에서 새롭게 등장하고 있는 복합단말이란 무엇이며, 복합단말 환경 하에서 특수하게 발생 가능한 보안 위협들에는 무엇이 있

는지 살펴본다.

2.1 복합단말의 정의

복합단말(All-in-one mobile device)은 기존에 개별적으로 존재하던 이동 통신 단말, 휴대 단말, 업무용 단말의 기능 및 서비스가 둘 이상 포함되어 네트워크 컨버전스 환경의 여러 인터페이스와 이를 통해 복합적인 서비스를 제공하는 휴대 가능한 개인용 단말이다. 그 예로서 기존의 PDA에 이동 통신 기능이 포함된 단말, 기존의 휴대폰에 네비게이션 기능이 포함된 단말, 등을 들 수 있으며 그림1에 복합단말이 포함되는 영역을 나타내고 있다.

그림1. 복합단말의 포함 영역

그림 2에서 나타나는 바와 같이, 향후 네트워크 및 단말의 진화 방향을 살펴보면 이동통신인 3G 및 무선랜(Wireless LAN)과 Wibro는 기존의 유무선 통신망을 비롯한 방송망 등의 다양한 망과의 융합을 목표로 하여 2010년 이후 4G로 통합된다고 예측하고 있다. 또한 보다 빠른 이동 통신 서비스로 음성 및 데이터를 동시에 지원하기 위한 새로운 무선 전송 기술 및 단말이 제공될 것이다.

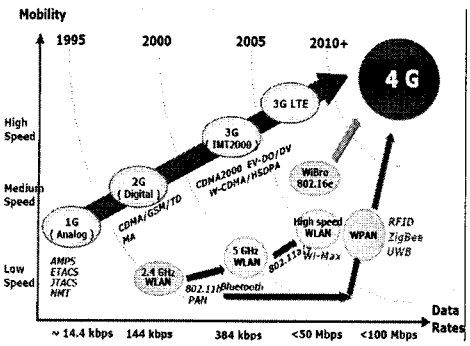

그림 2. 이동 통신 네트워크 진화 방향

따라서, 복합단말은 다양한 이동 네트워크 인프라와 고속 데이터 서비스를 수용하기 위해 다채널 통신 인터페이스(예: CDMA, WCDMA, 무선랜, Wibro, WiMax 등)을 지원하고, 고성능 컴퓨팅 환경과 이동성을 보장하는 이동 컴퓨팅 단말로서, 고성능, 빠른 이동성, 고속의 데이터 전송속도를 지원하면서 IPTV, Wibro, DMB, 네비게이션, MMS, MP3, 동영상 카메라, 전자사전, 네비게이션, 등과 같은 다양한 서비스를 제공하는 형태로 발전할 것이다.

현재 이동 통신과 Wibro 인터페이스를 동시에 제공하는 UMPC, Wibro 기능을 지원하는 휴대폰, Wibro와 무선랜 인터페이스를 함께 지원하는 노트북 등이 출시되고 있으며, 향후에는 4G 환경에 적합한 이동 통신, Wibro, 무선랜 인터페이스를 동시에 제공하는 복합단말이 일반화될 것이다.

올초에 있었던 CeBIT 2008이나 MWC 2008에서도 여러 인터페이스를 동시에 제공하면서 다양한 기능을 지원하는 형태의 단말에 대한 소개가 많았다.

즉, 복합단말은 다양한 이동 네트워크 인프라와 고속 데이터 서비스를 수용하기 위해 다채널 통신을 지원하고, 고성능 컴퓨팅 환경과 이동성을 보장하는 이동 컴퓨팅 단말로 정의할 수 있으며, 고성능, 빠른 이동성, 높은 data rate을 지원하면서 IPTV, Wibro, DMB, 네비게이션, MMS(Multimedia Messaging Service) 등과 같은 다양한 서비스를 제공하는 형태로 발전할 것이다.

2.2 예측되는 보안 위협들

복합단말은 다양한 서비스를 동시에 제공하므로 기존 이동통신, 무선랜, 데이터 통신에서 존재하던 보안 위협들이 그대로 존재하면서 또한 해당 서비스 영역을 넘어서 다른 서비스의 취약점을 공격하는 형태의 Cross-service 공격이 가능해진다[1].

복합단말내의 Cross-service 공격은 기존 무선랜 환경에서 존재하던 공격과는 달리 과금과 연계되어 있어 더 위협적이고 치명적이라 할 수 있다. 또한 복합단말에 악의적으로 불필요한 통신이나 프로세스를 작동하게 하여 배터리 소모를 빠르게 하는 형태의 공격도 예상되고 있다[2]. 이러한 공격은 시간과 공간에 대한 제약없이 단말을 사용하기 위한 목적인 복합단말의 편의성을 저해하는 요소로 사용자에게 많은 불편을 불러일으킨다.

표 1은 기존 이동통신, 무선랜, 데이터 통신에서 존재하던 보안 위협들이 그대로 네트워크 컨버전스 환경의 복합단말에도 존재하며 그 밖에 인터페이스 융합으로 인해 추가되는 보안 위협을 나타낸 표이다.

표 1. 보안 위협 비교표

복합단말	이동 통신 (3G 환경)	무선랜	데이터 통신
인증받지 않은 접근(데이터, 서비스)	인증받지 않은 접근(데이터, 서비스)	인증받지 않은 접근	

부인방지	부인방지		
DoS 공격	DoS 공격	DoS 공격	DoS 공격
도난/분실	도난/분실		개인정보 유출
단말/데이터 조작	단말/데이터 조작	데이터 가로채기/수정	
	UICC/USIM 취약점 공격		
		WEP 취약점 공격	
악성코드 유포			악성코드 유포
도청		도청	
Spoofing		Spoofing	
Cross-Service 공격			
배터리 소모 공격			
MMS 취약점 공격			

III. Cross-service 공격 탐지 메커니즘

본 장에서는 Cross-service 공격이 무엇인지 자세히 알아보고, 이를 탐지하기 위한 메커니즘에 대해 살펴본다.

3.1 Cross-service 공격

복합단말에서는 하나의 단말이 여러 네트워크 서비스에 동시 접근 가능하면서 복합단말내의 취약점을 이용하여 해당 서비스 영역을 넘어서 다른 서비스를 통한 다양한 형태의 Cross-service 공격이 가능해진다.

예를 들어 사용자가 인터넷 접속을 위해 연결한 무선랜 AP(Access Point)를 통해 침입한 공격자는 사용자 모르게 이동통신 인터페이스를 사용하여 다량의 SMS/MMS/전화 통화를 시도하는 공격이 있을 수 있다. 여기서 무선랜 인터페이스로 들어온 공격자가 이동통신 인터페이스를 이용하는 방식을 Cross-service라 한다. 이러한 공격은 기존 존재하던 보안 취약점(예: 버퍼 오버플로우 등)을 이용하지만 특정 네트워크 서비스로 들어온 프로세스가 다른 서비스와 관련된 자원을 접근함으로써 발생한다는 측면에서 기존 공격 위협과는 그 양상이 다르다. 또한, Cross-service 공격은 기존 무선랜 환경에서 존재하던 공격과는 달리 과금에 영향을 미치거나 휴대성을 지닌 복합단말의 배터리 소모를 빠르게 하여 사용에 지장을 주기 때문에 더 위협적이다.

그림 3은 Cross-service 공격을 설명하기 위한 예제 시나리오로서, 피해자는 복합단말의 무선랜 인터페이스를 이용하여 인터넷 서비스를 받고 있다. 무선랜 AP를 감시하고 있었던 공격자는 피해자의 복합단말에서 실행 중인 ftpserver의 버퍼 오버플로우 취약성을 확인하고 ftpserver에 접속하여 버퍼 오버플로우를 발생시킨다. 공격자는 악의적인 공격 코드로서 전화호출 서비스 코드를 실행시켜 침입 경로인 무선랜 인터페이스가 아닌 CDMA 인터페이스를 공격하는 Cross-service 방식을 악용했다. 이 공격으로 공격자는 자신이 운영하고 있는 정보 이용료가 부과되는 유료 정보 서비스로 불법적으로 통화를 시도하여 불법적인 이득을 취하고 피해자는 과금으로 인한 금전적인 손실을 입게 된다.

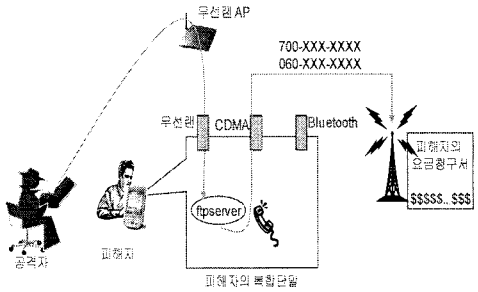

그림 3. Cross-Service 공격의 예

Cross-service 공격의 다른 형태로 특정 사용자나 익명의 다수 사용자에게 SMS/MMS를 전송시키는 공격이 있을 수 있다[3]. 이러한 메시지 전송은 네트워크나 다른 단말들에게 부당 과금은 물론 바이러스나 웜과 같은 악성코드를 전파시켜 오동작을 유발시킬 수 있다. 또한 복합단말에 불필요한 통신이나 프로세스를 작동하게 하여 배터리 소모를 빠르게 하여 정상적인 서비스 이용을 방해하거나, 불필요한 데이터 통신 및 유료 사이트/전화번호를 유발시켜 과금을 부가시키거나, 악성코드를 설치 및 유포하는 등의 방식으로 다양한 사용자 피해를 불러일으킨다. 또한, 복합단말내의 중요 정보에 접근 및 악의적으로 수정/삭제하거나 불법적으로 외부로 유출해 가는 경우도 있다.

3.2 Cross-service 공격 탐지 메커니즘

Cross-service 공격의 대표적인 특징은 무료 또는 정액 서비스인 무선랜 인터페이스로 침입하여 유료 서비스인 CDMA 인터페이스를 사용하는 서비스를 악용하는 방식이다. 본 논문에서 제안하는 Cross-service 공격을 탐지하는 메커니즘은 기존 리눅스 커널의 LSM(Linux Security Module)에서 제공하는 후킹(Hooking)을 사용하여 역할 기반 접근제어를 확장하는 방식이다. 제안하는 메커니즘을 통해 Cross-service 공격에 대해 탐지 및 대응할 수 있다.

각 인터페이스별로 접근 가능한 서비스 및 자원을 미리 프로파일로 정의하고, 모든 인터페이스로 들어

온 요청에 대해서 정의된 프로파일을 미리 확인한 후에 허용 여부를 알려준다. 따라서 특정 인터페이스가 미리 정의되지 않은 서비스나 자원에 접근하거나 또는 접근해서는 안 되는 서비스나 자원에 대한 요청이 들어오면 이를 차단하는 방식이다.

```
인터페이스: if1, if2, if3, if4
서비스(Service): S1, S2, S3
자원(Resource): R1, R2, R3

예: Deny if1, R1 and S1, S2
    Access if2, R1 and S1
    Access if3, R2 and S2, S3
    Deny if4, R3 and S2
```

그림 4. Cross-service 공격 탐지를 위한 역할기반 접근제어 프로파일 예시

IV. Cross-service 공격 방지를 위한 요구사항

Cross-service 공격으로부터 복합단말을 보호하기 위해서는 크게 인증/인가 측면, 개인정보 보호 측면, 악성코드 탐지 및 제거 측면의 보안 요구사항이 필요하다.

4.1 인증 및 인가 측면

인증 및 인가는 사용자, 복합단말, 플랫폼 측면에서 다양하게 지원되어야 하는 기능으로 크게 2가지의 요구사항이 필요하다.

- 정상적인 권한이 있는 사용자도 다른 네트워크 서비스와 관련한 자원의 접근을 제한하는 인증 및 인가 방식이 제공되어야 한다.
- Cross-service를 방지하기 위한 사용자 인증 및 인가 방식이 제공되어야 한다.

4.2 개인 정보의 보호 측면

복합단말은 개인의 중요 정보가 유출될 경우를 대비한 중요 정보의 암호화 기능 및 중요 정보 유출을 탐지하고 차단할 수 있는 기능들이 요구된다. 여기서 중요 정보에는 개인적인 정보 외에 단말의 정보도 포함한다.

- 정상적인 인증을 거친 사용자가 다른 네트워크 서비스와 관련된 중요 정보에 접근하지 못하도록 중요 정보에 대한 암호화 기능이 제공되어야 한다.
- Cross-service를 악용해 침입한 공격자가 최상위 사용자 인증 획득을 방지하기 위해서 인증에 사용되는 키의 안전한 관리 방안이 요구된다.
- Cross-service를 통해 침입한 공격자가 암호화된 중요 정보를 복호화하지 못하도록 암호화에 사용되는 키의 안전한 관리 방안이 요구된다.

4.3 악성코드 탐지 및 제거 측면

사용자가 알지 못하는 사이에 설치된 악성코드는 사용하고 있는 복합단말뿐 아니라 다른 복합단말에게도 위협적이다. 따라서 악성코드를 탐지하고 이를 제거할 수 있는 기능이 필요하다.

- Cross-service를 악용한 공격으로 복합단말 내 악성코드가 설치되는 것을 탐지하기 위한 보안 프로그램을 사용해야 한다.
- Cross-service를 악용한 공격을 수행한 후 불법적인 악성코드 다운로드 설치를 방지하기 위해서 파일 다운로드 시에는 보안 프로그램을 사용하여 실행 전 실시간 검사를 수행해야 한다.

V. 결 론

본 논문에서는 다채널 인터페이스와 여러 서비스 및 기능을 제공하는 휴대단말인 복합단말에 대해 정의하고, 이러한 복합단말 상에서 발생 가능한 Cross-service 공격에 대해서 살펴보았다. 본 논문에서는 Cross-service 공격을 탐지하기 위한 역할 기반 접근제어 메커니즘을 제안하였으며, 이를 통해서 다른 인터페이스를 통해 침입하여 자원, 서비스를 악용하는 공격에 대해 탐지 및 대응할 수 있다. 또한 Cross-service 공격 방지를 위한 요구사항을 정리하였다.

모든 응용에 대해 제안하는 접근제어 방식을 수행하는 것은 복합단말의 성능에 영향을 미칠 수 있으므로 이를 최적화하는 프로파일에 대한 구성 및 배터리 소모를 적게 하는 방안에 대한 추후 연구가 지속적으로 요구된다.

참고문헌

[1] Collin Mulliner, et. al, "Using Labeling to Prevent Cross-Service Attacks Against Smart Phones," DIMVA 2006, LNCS 4064, pp 91-108, 2006.

[2] Radmilo Racic, Denys Ma, and Hao Chen, "Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery," CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm), pp 1-10, 2006.8.

[3] Collin Mulliner, et.al, "Vulnerability Analysis of MMS User Agents," pp77-88,2006.12.

[4] 오승희, et. al, "Cross-service 공격방지를 위한 복합단말 보안 요구사항", TTAS.KO-12.0062, TTA 표준문서