# 사용자 중심의 스마트폰 보안 취약성 분석 어플리케이션 개발

조식완, 장원준, 이형우*
한신대학교 컴퓨터공학부

# Development of User Oriented Vulnerability Analysis Application on Smart Phone

Sik-Wan Cho, Won-Jun Jang, Hyung-Woo Lee*
School of Computer Engineering, HanShin University

**요 약** 최근 안드로이드 기반 상용 스마트워크 단말이 개발/보급되면서 다양한 형태의 앱이 개발되어 사용 중에 있으나 앱을 통해 사용자도 모르게 다양한 형태의 공격이 급증하고 있어 이에 대한 능동적 대응 방안이 제시되어야 한다. 본 연구에서는 안드로이드 기반 상용 스마트워크 단말의 사용자 환경을 중심으로 공격 등이 발생하였을 경우 이를 탐지하고 능동적으로 대응할 수 있는 기술에 대해 연구하였다. 본 연구에서 제시한 보안 취약성 분석 및 대응 기법인 경우 기존 방식보다 간편하고 최소화된 메모리 구조를 이용하여 단말내 이상현상을 모니터링 할 수 있으면서도 효율적으로 스마트워크 단말의 공격에 대한 능동적 대응 기능을 제공한다.

• **주제어** : 사용자중심, 취약점 분석, 스마트폰, 보안

**Abstract** An advanced and proactive response mechanism against diverse attacks should be proposed for enhance its security and reliability on android based commercial smart work device. In this study, we propose a user-oriented vulnerability analysis and response system on commercial smart work device based on android when diverse attacks are activated. Proposed mechanism uses simplified and optimized memory for monitoring and detecting the abnormal behavior on commercial smart work device, with which we can find and determine the attacker's attempts. Additionally, proposed mechanism provides advanced vulnerability analysis and monitoring/control module.

• **Key Words** : User Oriented, Vulnerability Analysis, Smart Phone, Security

## 1. 서론

최근 Flexispy 가 등장하면서 모든 스마트폰에 대한 개인 정보 유출 서비스를 제공하고 있다. 이 서비스는 일정 금액을 납부하면 특정 스마트폰 내 개인 통화정보, SMS, 내부 정보 등을 주기적으로 특정 서버로 전송하여 이를 불법적으로 확인할 수 있다. 이와 같은 모바일 악성코드를 검출하기 위해 여러 가지 제품 등이 개발되었다. BitDefender 사의 Mobile Security는 모바일 내 바이러스 탐지 도구로 설치 및 사용이 간편하며, 주요 기능으로 바이러스 스캔 및 방화벽 기능이 있다. BullGuard Mobile Security는 SMS, MMS, 전자메일, 블루투스 기능을 대상으로 바이러스 및 스파이웨어를 탐지하고 차단하는 기

본 논문의 일부 내용은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2012R1A1A2004573)
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2012년 5월 5일 수정일 2012년 5월 15일 게재확정일 2012년 5월 25일

능을 제공하고 있으며, 스마트단말을 분실하거나 도난당했을 경우 GPS 기능을 통해 탐지 및 원격 제어가 가능하다. Dr. Web Anti-Virus는 스마트단말 내 바이러스 및 스파이웨어, 루트킷에 대해 탐지하고 차단하는 기능을 제공한다. 또한 방화벽 기능을 통해 네트워크 공격으로부터 단말을 보호할 수 있으며, 내부 시스템을 스캔하여 시스템 정보 모니터링 기능을 제공한다. Norton Smartphone Security 제품은 스마트단말 내부 바이러스, 스파이웨어, 악성코드 등을 탐지하거나 차단할 수 있으며, 방화벽 기능을 제공하여 해킹이나 인가되지 않은 접근에 대해 차단할 수 있다. 또한 필터링 기능을 통해 원하지 않는 통화 및 문자메시지, 스팸 등을 차단할 수 있다.

하지만, 기존 악성 어플리케이션 진단 기술은 다음과 같은 문제점을 보이고 있다. 1) 활성 상태의 어플리케이션에 대한 모니터링 및 취약점 분석 기능이 미약하다. 2) 안드로이드 단말에서 백그라운드로 실행되는 각종 어플리케이션에 대한 사용자 중심의 진단 기능이 미약하다. 3) 악성 코드를 내포한 어플리케이션에 대한 진단만 하며 디바이스 자체 및 악성코드 배포 경로에 대한 진단 기능이 미약하다.

따라서 본 과제에서는 악성 어플리케이션 및 디바이스에 대해 이벤트 중심의 진단 방식을 설계하였으며, 사용자 중심의 모니터링 기능을 개발하였다.현재 스마트폰은 PC에서 제공하는 대부분의 기능을 수행하는 것은 물론 기존 전화망인 PSTN 망이 아닌 인터넷의 통한 폰 서비스를 제공함으로서 발생하는 편의성 및 비용절감 효과로 인해 상용화되어 있다. 하지만 이런 편의성으로 인해 사용자가 급증하는 만큼 이에 대한 보안 사고 또한 늘어나고 있다. 개인정보 유출, 악성코드 유포, 불특정 다수의 Call DoS 공격 등 스마트폰의 특징을 이용한 공격들이 생겨나고 있으며 그 정도가 점차 지능적이고 고도화 되어가고 있다.

특히 스마트폰 서비스의 경우 대부분 Wifi나 3G를 이용한 인터넷망을 기본으로 사용하고 있기 때문에 인터넷망이 지니고 있는 취약점을 그대로 지니고 있으며 일반적으로 사용하는 통신 서비스의 또한 공격자가 정산적인 통신 패킷을 수정 및 삭제하고 이를 변경하는데 있어서 문제가 없다. 즉, 쉽게 도청 및 위변조가 가능하다는 것이다.

결국 현재 이 같은 취약점에 대응하기 위한 다양한 형태의 백신이 나오고 있으며 사용자들 또한 쉽게 백신을 다운받아 사용하도 있다. 여기서 문제는 백신이 스마트폰 내의 시스템을 스캔하여 위험성이 있는 패킷을 감시하거나 차단하는 작업을 하며 이같은 작업이 자동화되어 있기 때문에 대부분의 사용자가 자신의 폰이 지니고 있는 주요 취약점에 대해 알지 못한다는 것이다. 백신 또한 주요 공격기법에 대응하기 위한 기법 및 감시, 차단 등의 작업 위주로 구성되어 있기 때문에 특정 위협에 대해 대응할 수는 있으나 그 외의 위협이나 사용자 부주의로 인한 취약점 노출 등에 있어서 즉각적인 대응을 바라기는 어렵다.

이에 본 논문에서는 스마트폰이 지닐 수 있는 주요 취약점에 대하여 시스템 내부 스캔하여 분석하는 것은 물론 외부의 다양한 접근 시도를 통해 내부와 외부에서 지닐 수 있는 주요 취약점에 대해 분석하였으며 이를 사용자에게 통보할 수 있는 시스템을 개발하였다.

## 2. 스마트폰 백신

### 2.1 스마트폰 전용 백신

대부분의 백신의 경우 공통적인 특징은 다음과 같다. 먼저 스파이웨어나 악성 코드를 탐지 및 차단하는 기능이 있으며 외부적 공격 위협을 차단하기 위한 방화벽 기능, 사용자 개인정보에 대해 변조 및 손상이 있을 시 이를 복구하기 위한 백업기능, 그리고 분실 시 이를 추적 및 데이터 보호를 위한 원격 제어 기능 등이 있다.

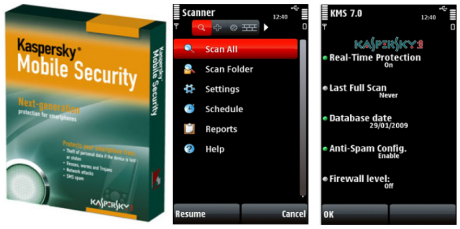
#### 2.1.1 BullGard Mobile Security

SMS와 MMS 전자메일, 블루투스 기능들을 대상으로 스파이웨어 탐지/차단하는 기능이 있으며 분실/도난시를 대비하여 GPS 기능을 이용한 원격제어가 가능하다. 또한 방화벽 및 필터링 기능을 통해 네트워크 공격으로부터의 보호 및 메시지 차단이 가능하고 연락처 및 캘린더 정보 등의 사용자 개인정보에 대해 백업 기능을 제공한다.


[Fig. 1] BullGard Mobile Security

### 2.1.2 Kaspersky Mobile Security

카스퍼스키에서 제공하는 도구는 백신으로 매우 유명하며 국내외에 걸쳐 모두 쓰이고 있는 도구 중 하나이다. 이 백신 또한 원격 제어를 통해 데이터 보고 및 완전 삭제가 가능하며 시스템에 잠금장치를 두어 스마트폰에서 제공하는 내부 기능을 차단할 수도 있다. 또한 악성 코드 및 바이러스를 차단하는 방화벽 기능과 필터링 기능을 제공하고 있다. 이 기능은 실시간 검사와 예약 검사가 가능하며 검사 결과는 수치화 하여 저장된다.




[Fig. 2] Kaspersky Mobile Security

### 2.1.3 Norton Smartphone Security

이 도구 또한 국내외에서 많이 쓰이고 있는 도구로 바이러스나 스파이웨어, 악성코드 등을 탐지 및 차단 기능 및 해킹이나 인가되지 않은 접근 차단하는 방화벽 기능을 제공한다. 또한 필터링 기능을 통해 원하지 않는 문자나 통화 연결, 스팸 등을 차단하는 기능을 제공한다.


[Fig. 3] Norton Smartphone Security

### 2.1.4 Lookout Mobile Security


[Fig. 4] Lookout Mobile Security

이 도구는 다른 도구들과 마찬가지로 유사한 기능을 제공하고 있다. 크게 3가지 기능을 제공하며 바이러스나 스파이웨어, 악성코드 등을 탐지 및 차단하는 기능 및 데이터 백업 기능, 스마트폰 도난/분실 시 구글 맵을 통해 위치정보 확인할 수 있는 기능을 제공하고 있다.

## 2.2 스마트폰 전용 백신 분석 결과

각 백신별 제공하고 있는 종합적인 기능은 다음과 같다. 대부분의 모바일 백신이 아래와 같은 기능을 따르고 있으며 업데이트를 통해 기능이 추가되거나 최적화 되어 사용된다.

[Table 1] Existing SmartPhone Oriented Vaccine

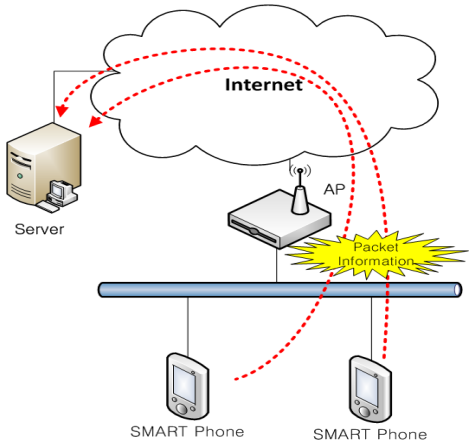
| 보안 SW 기능 | BullGard Mobile Security | Kaspersky Mobile Security | 노턴 스마트폰 보안 | Lookout Mobile Security |
|---|---|---|---|---|
| 악성코드 탐지 | | O | O | O |
| 악성코드 차단 | | O | O | |
| 실시간 감시 기능 | O | | O | O |
| 파일 감시 | | O | | |
| 트래픽 감시 | O | | | |
| e-mail/ SMS/ MMS 감시 | O | | O | |
| 필터링/방화벽 기능 | | O | O | |
| 업데이트 기능 | O | O | O | |
| 도난방지 및 추적 기능 | O | O | | O |
| 백업 및 복구 기능 | O | | | O |
| 원격 데이터 삭제 | O | O | | |
| 위치 추적 기능 | O | O | | |

# 3. 취약성 분석 시스템

## 3.1 분석 환경

스마트폰에 대한 보안 취약성을 분석하기 위해 다음

과 같은 실험 환경을 구축하였다. 스마트폰 보안 취약성에 대해 분석하고 이를 사용자에게 알릴 수 있는 취약성 분석 도구를 개발하였다.

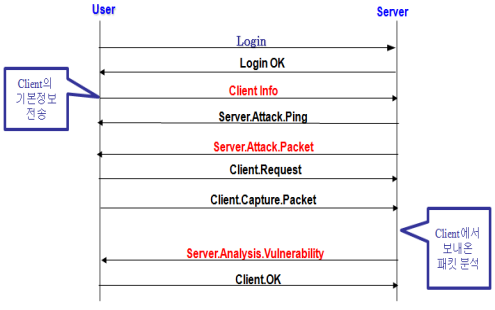



[Fig. 5] Vulnerability Testing System Architecture

외부적 접근으로서 통화서비스 분석 또한 해야 하기에 위 그림과 같이 스마트폰을 2대 연결하였으며 서버와 클라이언트는 인터넷을 통해 서로간의 통신을 할 수 있도록 구성되어 있다.

## 3.2 취약점 분석 시스템

시스템은 아래의 Call Flow와 같이 작동한다. 먼저 어플리케이션을 통해 Server로 로그인 과정을 거치게 되며 정상적으로 로그인이 되었을시 서버는 클라이언트로 Login OK 메시지를 보낸다.



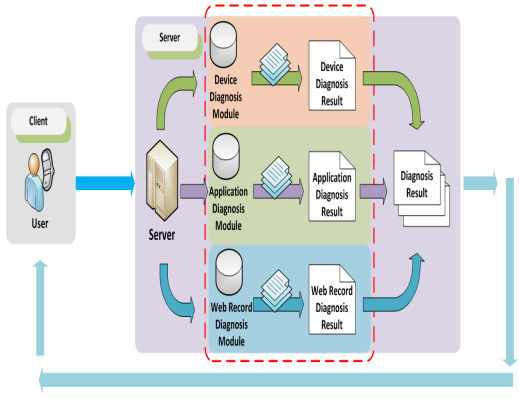

[Fig. 6] Call Flow for Vulnerability Testing

모든 로그인 과정을 정상적으로 마치게 되면 클라이언트는 서버로 클라이언트 시스템에 대한 정보를 전송한다. 이 때 정보를 전송하기 전 먼저 어플리케이션을 통해 스마트폰의 내부 시스템에 대해 스캔작업을 거치며 스캔을 통해 얻게 된 정보를 바탕으로 내부 취약점 분석 및 정보에 대한 서버 전송 작업을 거치게 된다.

서버는 클라이언트에서 보내온 정보를 바탕으로 스마트폰에 대해 보안 위협이 될 수 있는 접근을 시도하며 시도했을 시 클라이언트에서 보내온 정보를 통해 외부적 접근의 취약성을 분석한다.

이후 분석한 내용에 대해 클라이언트로 통보를 해줌으로서 사용자는 자신의 스마트폰이 지니고 있는 취약성에 대해 알 수 있으며 이를 통해 외부 위협에 대하여 사용자 중심의 빠른 대처를 기대할 수 있다.

다음 구조와 같이 서버는 클라이언트로부터 전달된 메시지를 분석하여 해당 스마트 단말에 대한 보안 위협과 취약성을 분석하게 된다.




[Fig. 7] Vulnerability Analysis Structure

## 3.3 개발 결과

개발한 어플리케이션의 모습은 다음과 같다. 먼저 어플리케이션을 실행하면 현재 네트워크 망이 3G인지 WiFi인지 분석하여 해당되는 연결을 통해 로그인을 한다. 물론 이 네트워크 정보는 로그인 후 나타나는 정보에 IP 및 Port 스캔 정보 등을 포함하여 사용자에게 나타난다.

이후 정상적인 로그인 과정을 거친 후에는 사용자의 폰 정보를 스캔하게 되는데 스마트폰이 지니고 있는 고유 ID 정보 및 스마트폰에 설정된 명칭, 스마트폰 버전, 모델명, 시스템 명칭 및 메모리 정보, 배터리 상태 및 충전 상태, 접촉에 따른 근접 여부, MMS, SMS 등의 사용자 개인정보 등 다양한 내부 정보를 스캔 작업을 통해 얻어낸 후 서버로 전송하게 된다.


[Fig. 8] Implemented SMART Check Application

서버에서는 전송된 정보를 바탕으로 공격 패킷을 생성하기 전 클라이언트로 Ping을 보내 연결이 유효한지 확인한 후 공격 패킷을 전송한다. 클라이언트는 서버에서 보내온 공격 패킷에 대한 결과 값을 전송하게 되며 서버는 이를 확인 한 후 처음에 보내온 정보 패킷과 비교하여 취약성 분석 작업을 진행한다. 그 후 분석 작업이 끝나면 이를 클라이언트로 전송하여 사용자가 확인할 수 있도록 하며 클라이언트가 정상적으로 전송 받았을 시 서버로 OK 패킷을 전송하여 분석 확인 작업을 마치게 된다. 아래 그림과 같이 스마트 단말에 분석 도구를 설치하여 획득된 이벤트 정보를 서버로 전송하여 그 결과를 분석하는 구조이다.


[Fig. 9] Implemented System Architecture

## 4. 결론

본 논문에서는 내부 및 외부의 접근 과정에 따른 시스템 변화를 통하여 스마트폰이 지니고 있는 보안 취약성에 대해 분석하였으며 이를 바탕으로 사용자 중심의 스마트폰 취약점 분석 어플리케이션을 개발하였다.

먼저 내부 정보에서는 시스템에 대한 대부분의 정보 및 사용자 개인의 정보에 해당하는 주소록이나 통화 기록에 대한 정보까지 별다른 인증과정 없이 내부 시스템 스캔 작업을 통해 가져올 수 있었으며 이를 통해 폰 정보를 저장하여 공격 대상으로 삼거나 개인 정보 유출 등의 피해를 입힐 수 있다는 것을 알 수 있었다. 또한 외부 정보를 통해 공격하였을 시 통화나 문자 등의 사용자 개인정보를 이용한 서비스일 경우 제공되는 대다수의 서비스가 암호화 되어있지 않아 그대로 노출되어 있으며 공격자가 이 정보를 획득하였을 시 도청 및 개인정보 유출로 이어질 수 있다는 것을 알 수 있었다.

그 결과 종합적으로 연구 분석한 내용을 토대로 사용자가 직접 시스템에 대한 내부 정보 및 주요 취약점을 파악하고 이를 분석할 수 있는 시스템을 개발할 수 있었다.

## Acknowledgement

본 논문은 학술대회 우수논문으로 선정된 것으로 일부 내용은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2012R1A1A2004573)

## REFERENCES

[1] ShinGaek Kang.「A State-of-Art of VoIP Technology」. VoIP Grand Conference 2005, 2005.
[2] JinBum Park, etc, “A Research on the Vulnerability and Response Mechanism against the VoIP Attack,” Journal of KIISC, Vol. 17, No. 5, 2007.
[3] Ji-Hun Kim, “VoIP Security Threats”, ASEC, 2008
[4] Mark Collier, "VoIP Vulnerabilities Registration Hijacking", SecureLogix Corporation, pp. 1-4, 2005.
[5] Su-Hwan Jung, Security Considerations on VoIP System, 2005.
[6] DISA, "IPTelephony & Voice over IP-Security Technical Implementation Guide ver2", 2004.
[7] S.Knuutinen, "Session Initiation Protocol security considerations", Seminar on Internetworking, Helsinky, 2003.

## 저자소개


**조 식 완(Cho-Sik Whan)** **[정회원]**

- 2010년 2월 : 한신대학교 소프트웨어학과 졸업
- 2010년 2월 ~ 현재 : 한신대학교 일반대학원 컴퓨터공학과 석사과정

<관심분야> : 정보보호, 포렌식, 네트워크 보안, 모바일 보안

**장 원 준(Won-Jun Jang)** **[정회원]**

- 2010년 2월 : 한신대학교 정보시스템공학과 졸업
- 2010년 2월 ~ 현재 : 한신대학교 일반대학원 컴퓨터공학과 석사과정

<관심분야> : 정보보호, 포렌식, 네트워크 보안, 스마트폰 보안

**이 형 우(Hyung-Woo Lee)** **[종신회원]**

- 1994년 2월 : 고려대학교 전산과학과 졸업
- 1996년 2월 : 고려대학교 일반대학원 전산과학과 석사
- 1999년 2월 : 고려대학교 일반대학원 전산과학과 박사
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 부교수

<관심분야> : 정보보호, 포렌식, 네트워크 보안, 바이오정보보호