Journal of The Korea Society of Computer and Information
(ISSN 1598-849X) Vol. 20 No. 6, pp. 43-50, June 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2015.20.6.043

Management for the Protection of Information in Smart Phone

Eun-Gyeom Jang*

Abstract

In order to protect important information of smart phone from these security threats, this paper has studied a mechanism for protecting information from the leakage of various information and personal information stored in the smart phone.

This paper has configured the basic protection scope for the information protection and applied real time encodement when new contents were created. Also, this paper has applied a security function so that the content of the protected scope can be managed and erased remotely in preparation for loss and burglary.

▸ Keyword : Smart phone, Important information, Information protection, Protection model

• First Author: Eun-Gyeom Jang
*Eun-Gyeom Jang(jangeg@jangan.ac.kr), Dept. of Internet Communication, Jangan University
• Received: 2014. 12, 15 Revised: 2015. 01. 12, Accepted: 2015. 06. 05.

Journal of The Korea Society of Computer and Information
(ISSN 1598-849X) Vol. 20 No. 6, pp. 43-50, June 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2015.20.6.043

I. Introduction

시스템에 부하가 적은 PC의 응용 서비스와 휴대성, 이동성의 특성이 부각된 다양한 서비스를 제공하고 있다. 이러한 특성은 가정 및 기업의 업무, 인터넷 쇼핑, 전화, 멀티미디어 영역 등 다양한 영역에서 다양한 문화를 접할 수 있는 서비스 환경을 제공하여 현대인의 필수 매체가 되었다. 스마트폰의 간편성과 휴대성의 특성으로 개인정보나 자료의 접근과 공유를 손쉽게 다룰 수 있는 환경을 제공한다. 이러한 서비스 환경은 서로 간에 더욱 긴밀한 네트워크를 형성함으로서 새로운 가치를 창출한다는 의미에서 스마트폰의 보급 및 확대는 한층 더 높은 정보화 시대를 부각 시키는 아이템으로 각광 받고 있다. 그러나 스마트폰을 활용한 다양한 개인정보 활용 및 매체접근으로 발생하는 개인 정보보안의 문제를 가지고 있다. 즉 안드로이드 폰의 경우에는 오픈된 개발 환경으로 다양한 개발자가 있으며 다양한 앱을 제공한다. 이러한 환경에서 구동되는 앱 서비스는 기능 중심의 서비스가 대표적으로 보안에 지식을 갖추지 않은 일반 IT 개발자가 앱을 만들어 보급하는 사례가 많다.

스마트폰의 오픈된 개발 및 앱 접근 환경은 스마트폰의 보안 취약점을 보이고 있으며, 앱을 사용하는 사용자는 보안에 미흡한 일반인으로 인증서를 포함한 다양한 개인정보를 스마트폰에 저장하여 관리하고 있다. 이러한 스마트폰의 예민한 정보의 공격 및 활용은 날로 지능적으로 보안을 위협하고 있다. 스마트폰은 패킷스니핑을 이용한 해킹 우려가 있으며, 간편한 휴대성으로 인한 도난, 분실 등으로 개인정보 또는 업무상의 중요정보가 유출될 수 있다. 이외에도 스마트폰 플랫폼 또는 펌웨어의 취약점을 이용하는 방법과 악성코드, 악성 앱을 이용하는 등 많은 유형의 보안 위협들이 존재한다[1,2].

이러한 인증서를 포함한 개인 정보, 지적재산권 디지털콘텐츠의 유출 및 접근을 방지하기 위해 본 논문에서는 매체접근 관리 정책을 적용한 단계별 접근제어 메커니즘을 제안한다. 2장에서는 관련연구로서 안드로이드 폰의 보안 기술과 보안 취약점 및 공격유형을 분석하고 3장에서는 본 연구에서 제안한 중요정보 유출 방지 메커니즘을 제시한다. 4장에서는 실험 및 테스트를 통한 성능을 분석하고 5장에서 연구 결과로 논문을 구성하였다.

II. Related Research

1. Smartphone Security

모바일 환경의 스마트폰은 악성코드를 통한 개인정보 유출, 해킹을 통한 정보 유출, 위·변조된 어플리케이션을 통한 정보 유출, 피싱에 의한 정보 유출 등을 볼 수 있다. 각각의 유형을 살펴보면 스마트폰용 앱을 통해 각 스마트폰에 부여된 국제단말기 인증번호(IMEI)와 범용 가입자식별 모듈(USIM)번호를 사용자 동의 없이 유출하여 복제품에 활용할 수 있고, 아이폰 OS인 '아이폰 iOS4.1' 탈옥도구를 가장해 비밀번호를 일정 서버로 전송, 이메일 피싱 수법으로 타인의 결제정보를 빼내는 방법 등이 있다[3,4,5].

스마트폰에 공통으로 적용되고 있는 보안 기능은 프로세스와 파일을 격리 시키는 방법으로 어플리케이션을 다른 어플리케이션으로부터 보호하기 위한 프로세스 및 파일시스템 격리화 기능을 제공한다. 이 기능은 모든 어플리케이션이 자신의 콘텍스트 내에서만 실행되도록 한다. 데이터의 읽기, 쓰기 또한 콘텍스트 내에서만 가능하다. 코드서명 방법으로 어플리케이션의 개발자나 스마트폰 플랫폼 업체에서 어플리케이션에 전자서명을 첨부하고, 사용자는 다운로드 후 실행 이전에 전자서명을 검증함으로써 어플리케이션이 훼손되지 않았음을 확인할 수 있다. 또한 스마트폰 플랫폼 업체에서는 운영체제 업데이트나 스마트폰 복구를 위해서 ROM에 설치된 운영체제, 즉 펌웨어를 초기화하는 기능을 제공한다[4,5].

2. Analysis of Smartphone Security Threats

가장 많은 시장 점유율을 차지하는 안드로이드 폰의 보안 취약점은 폰 자체의 플랫폼을 이용한 공격 또는 네크워크 취약점을 이용한 공격, 단말기 자체를 공격하는 방법이 있다. 표 1과 같이 공격목표에 의하여 분류 방법과 공격대상에 의한 분류 방법으로 구분 할 수 있다. 공격목표에 의한 분류는 크게 정보유출, 오작동, 불법 콘텐츠 접근으로 나눌 수 있다.

- 정보유출 : 정보의 유출(개인/업무/위치/금융 등)
- 오작동 : 단말기 사용불능, 단말기 전력소모, DDOS
- 불법 콘텐츠 접근 : 콘텐츠 무단 복제 등

공격대상에 의한 분류는 플랫폼 공격, 어플리케이션 공격, 네트워크 공격 및 단말기 분실 등으로 인한 공격이 있다[4,5,6,7].

- 플랫폼 공격 : Wi-Fi/블루투스/Web 등 여러채널을 이용한 전파 및 PC동기화(Active Sync)전파, 단말기UI변경, 단말기 파손(오류발생), 배터리소모, 자동프로그램 삭제 및 설치, Rootin, SecurityOff(WM)플랫폼 취약점 이용(API 취약점 이용), Rootkit 같은 프로그램 악용
- 어플리케이션 공격 : Web 다운로드, PC 동기화를 통한 설치, 개인정보(파일, 일정, 주소록, SMS, 통화내역, 메모, 위치정보 등) 유출, 인터넷뱅킹, 소액결제 등의 금융거래 정보, 업무용 파일 등 기밀정보 유출, SMS의 부정사용 및 스팸문자 발송 오과금 발생, 단말기사용불능발생, 좀비단말기발생, 휴대전화 소액결제 악용, 무선인터넷이용 유료 전화 서비스 악용
- 네트워크 공격 : Wi-Fi/블루투스 네트워크 공격으로 인한 단말기 통신 도청/변조, 특정사이트, 특정단말기, AP 등에 트

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2015.20.6.043

유발 DOS공격, 스마트폰 채널을 통한 직접적인 이동통신망에 대한 DDOS 공격

- 단말기 공격 : 도난 및 분실, 이동 저장매체 감염

악성코드에 감염되면 개인정보 및 단말기 고유정보를 유출하거나 단말기 이용의 방해 및 SMS 무단 전송 등을 통한 과금 유발 등의 피해를 준다. 해외에서에는 심비안 및 안드로이드 OS 탑재 스마트폰을 대상으로 Jackeey wallpaper(정보유출), Christmas wallpaper(정보유출), Trojan-SMS.AndroidOS.-FakePlayer.a(SMS 무단전송), Tapsnake(정보유출), Trojan-SMS. AndroidOS. Fake Player.b(SMS 무단전송) 등이 있다.

국내의 경우 2010년 4월 윈도우모바일 탑재 폰을 대상으로 첫 스마트폰 악성코드(WinCE/TerDial)가 보도된 바 있으며, 이외에도 국내 스마트폰 가입자 약 160여만 명 중 약 150여명(0.01%)의 스마트폰이 WinCE/TerDial 악성코드에 감염되었다[8,9,10].

최근 스마트폰의 악성코드 증대로 스마트폰 이용자는 블루투스 송·수신 또는 사설 블랙마켓 및 웹 사이트 접속을 통해 다운로드된 어플리케이션을 실행 후, 오작동 또는 작동불능 상태가 되거나 저장된 개인정보가 임의로 삭제되었다면 악성코드 감염을 의심해야 하며, 다운로드 한 어플리케이션에 대해서는 설치 전에 반드시 백신 어플리케이션으로 악성코드 유무를 검사하여야 한다. 하지만, 다발적으로 신종 악성코드가 생겨나고 있으며, 사용자의 부주의 등으로 인한 백신 최신 업데이트 관리 소홀 등으로 피해 사례가 생겨나고 있다. 이로 인하여 사용자가 저장한 중요데이터가 악성코드, 악성 앱에 의해 유출될 수 있는 위협이 존재하며, 이에 따른 대응 방안이 필요하다.

3. Android Security Technique

안드로이드는 모바일 환경에 적합하게 수정된 고유의 보안 메커니즘을 가진 리눅스 기반의 플랫폼이다. 어플리케이션과 시스템간의 대부분의 보안은 어플리케이션에 할당된 유저 ID나 그룹 ID와 같은 표준 리눅스 기능을 통해 상속받고 프로세스 레벨에서 강제된다. 안드로이드 보안 모델은 표 1과 같다[6,7].

사용자의 부주의로 인한 시스템 (노트북, 휴대 단말 등) 분실 혹은 외부 제 3자에 의한 시스템 도난 등을 통해 단말 복제, 도청, 단말의 프라이버시 데이터 보호 위협, 악성 코드 삽입 등의 보안 위협은 여전히 해결되지 않은 과제로 남아있다. 일반적으로 소프트웨어는 하드웨어에 비해 쉽게 조작될 수 있기 때문에 물리적 보안성을 제공해주는 MTM(Mobile Trusted Module) 기술을 이용하여 외부 공격으로부터 데이터, 키, 인증서 등을 안전하게 보호하고, 스마트 단말 플랫폼의 무결성 검증을 통해 악성 코드 실행을 사전에 탐지하여 차단함으로써 보다 향상된 보안 기능을 제공할 수 있다.

Table 1. Android security model

구분	보안 기능	설명	보안이슈
리눅스	UID/GID	각 응용은 고유의 사용자 ID, 그룹ID 가짐	특정 응용이 다른 응용에 영향을 끼치지 않음
	파일 접근	각 응용의 디렉토리는 해당 응용프로그램만이 사용가능	특정 응용이 다른 응용 소유의 파일에 접근하는 것을 방지
안드로이드	컴포넌트 캡슐화	각 응용 컴포넌트는 다른 응용으로부터 접근에 관한 visibility level을 가짐	응용이 다른 응용으로부터 영향을 미치는 것을 방지
	응용 프로그램 권한	각 응용은 설치시에 요구되는 권한 선언	응용의 비정상적인 동작을 예방
	응용 프로그램 서명	응용은 개발자 서명을 가져야 함	응용이 같은 제작자로부터 제작된 것인지 여부를 대조· 검증
자바언어	Dalvik 가상기계	각 응용은 고유의 가상기계 안에서 실행	버퍼 오버플로우, 원격코드실행, 스택 스매싱 방지

3.1 Application permissions

안드로이드 보안 구조의 핵심은 기본적으로 어떠한 어플리케이션들도 다른 어플리케이션과 운영체제, 또는 사용자에게 나쁜 영향을 미칠 수 있는 임의의 오퍼레이션을 수행할 수 있는 퍼미션을 가지지 않는 것에 있다. 이는 그림 1의 형태와 같다[5].

이것은 사용자의 개인적인 데이터에 대한 읽고 쓰기 및 다른 어플리케이션의 파일에 대한 읽고 쓰기, 네트워크 접근, 디바이스에 대한 활성 상태 유지 등을 포함한다. 어플리케이션의 프로세스는 각각 보안 샌드박스(Secure Sandbox) 형태로 생성된다. 이것은 추가적인 기능들을 위해 필요한 퍼미션을 명시적으로 선언하지 않고서는 다른 어플리케이션의 동작을 방해할 수 없음을 의미하며, 이러한 퍼미션들은 다양한 방법을 통해 운영체제에 의해 제어될 수 있다. 전형적인 방법으로는 인증서를 기반으로 자동으로 허용하거나, 사용자에게 확인을 요청하는 방법에 의해 제어된다.

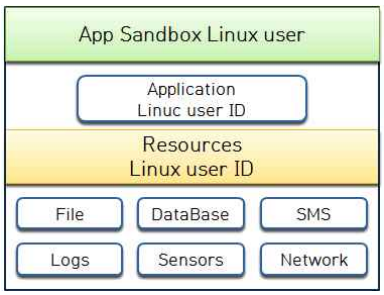

Fig. 1. Android application process model

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2015.20.6.043

설치시 요청된 퍼미션은 그 어플리케이션 내에 정적으로 선언되고, 또한 권한이 부여되는지 알 수 있으나, 설치 후에는 변경할 수 없다. Android Market에서 새로운 어플리케이션을 다운로드 받아 설치할 때 해당 어플리케이션이 가지는 퍼미션에 대한 정보를 나타내는 것이다. 만약 같은 퍼미션을 가진 어플리케이션이 설치시 부여하지 않았던, 권한을 가지지 않는 것에 대한 작업을 수행하려 할 때 Security Exception이 발생하며 해당 어플리케이션은 멈추게 된다.

3.2 Component Encapsulation

컴포넌트들은 다른 어플리케이션에 액세스하고자 할 때 각각 독립된 API로 이루어져 있기 때문에, 제한적인 권한만 가진다. 이는 개인 정보나 다른 API에 접근하는 것을 방지하는 수단이 된다. 하지만 위에서 설명한 바와 같이 명시적인 방법을 통해서는 데이터 공유가 가능하다.

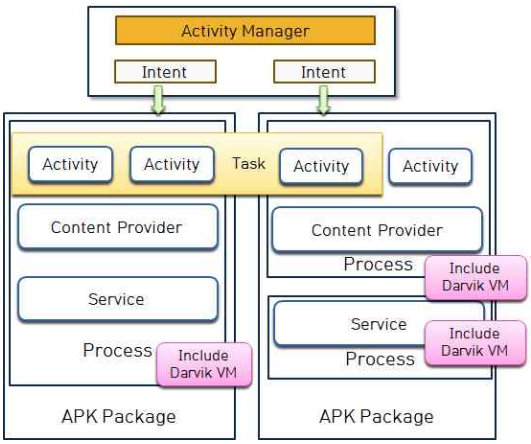

Fig. 2. Access to the components belonging to other applications

명시적인 방법이란 다른 응용 프로그램에서 데이터를 가져오려면 그림 2와 같이 해당 응용프로그램의 컴포넌트를 거쳐 데이터를 가져오게 된다[5].

3.3 Signing applications

모든 안드로이드 어플리케이션 설치파일(APK)은 개발자가 보유한 개인키 인증서로 서명되어야 한다. 이 인증서는 어플리케이션의 작성자를 식별하며, 공식적인 인증기관에 의해 서명될 필요는 없다. 어플리케이션들 간의 신뢰 관계를 확립하기 위해서 사용될 뿐이며, 서명이 보안에 미치는 가장 중요한 사항들은 서명 기반의 퍼미션에 누가 접근 가능하며 누가 사용자 ID를 공유할 수 있는지를 결정하는 것으로, 인증서는 설치파일(APK)에 서명된 개발자를 확인하여, source code로 검증된 어플리케이션임을 확인하는 수단이 된다.

또한, 기본으로 디바이스의 보호된 기능을 사용하기 위해서는 AndroidManifest.xml내에 어플리케이션이 필요로 하는 퍼미션을 선언하는 하나 또는 그 이상의 <uses-permission> 엘리먼트를 포함해야 한다. 이렇게 어플리케이션 설치 시점에 요청된 퍼미션은 어플리케이션 서명확인을 기반으로 사용자와의 상호작용에 기반하여 패키지 인스톨러에 의해 그 어플리케이션에 부여된다. 하지만, 어플리케이션이 실행되는 동안에는 사용자와의 어떤 확인 절차도 이루어지지 않는다. 다만, 퍼미션 실패가 있는 경우 일반적으로 시스템 로그에 기록한다[8].

안드로이드 시스템에 의해 제공되는 퍼미션은 Manifest permission에서 볼 수 있다. 모든 어플리케이션은 자기 자신의 퍼미션을 정의하고 강제할 수 있다.

3.4 Dalvik virtual machine

어플리케이션은 달빅(Dalvik) 가상머신(VM)에 설치된다. 달빅(Dalvik) 가상머신(VM)은 안드로이드 폰에 탑재된 가상머신으로서 버퍼 오버플로, 원격 코드 실행, 스택 스매싱 등과 같은 보안 문제를 방지하는 하는 기능을 가진다.

안드로이드는 응용 프로그램 간에 접근 할 수 있는 권한을 통하여, 악성코드 및 악성 앱에 의한 피해를 방지하고 있다. 하지만 모든 앱에서 접근 할 수 있는 사진, SNS, 연락처, SD카드 등 공용 영역에 대한 보안 메커니즘을 제공하고 있지는 않다. 단순히 앱에서 사진, SNS, 연락처, SD카드의 활용은 Android -Manifest.xml에 명시만 해두면 접근이 가능하다. 즉, SD카드에 보관되는 중요정보가 악성코드, 악성 앱에 의해 손쉽게 유출될 수 있는 위험이 존재한다.

III. Security Mechanism for Important Information Efflux Prevention

악성 코드와 악성 앱, 도난, 분실 등으로 인하여 개인정보가 유출될 수 있으며, 안드로이드의 경우 SD카드와 같은 공용 영역의 보안은 제공하지 않음으로 이에 대한 방안으로 중요정보의 경우 유출 방지를 위하여 그림 3과 같이 시스템을 구성하였으며 항시 자동 암호화된 상태로 보관되고 필요시 원격에서 관리 할 수 있도록 하였다.

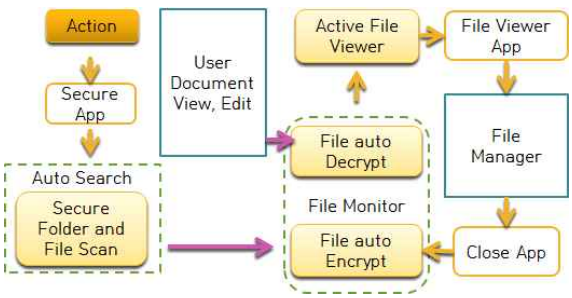

Fig. 3. Important information security module

1. Data Management of Smartphone

안드로이드 어플리케이션의 콘텐츠 저장 영역은 어플리케이션 데이터가 저장되는 내부 저장소 영역과 사진, 비디오, 데이

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2015.20.6.043

등을 저장하는 외부 저장소 영역으로 나뉠 수 있으며, 각 영역별로 다시 캐시 데이터가 저장되는 영역, 데이터베이스가 저장되는 영역 등으로 나뉜다.

내부 저장소는 각 어플리케이션에서만 데이터를 읽고 쓸 수 있으며, 캐시(Cache), 데이터베이스, 일반파일이 있다. 외부저장소는 일반적으로 이는 단말기의 외장SD카드를 지칭하는데, 특정 어플리케이션에서만 사용하는 어플리케이션 고유 영역과 공용 영역이 각각 존재한다.

어플리케이션 고유 영역은 각 데이터 유형별로 데이터를 저장하는 영역으로 데이터의 유형에 따라 별도의 디렉터리를 사용한다. 안드로이드에서는 총 7개 데이터 유형에 대한 표준 저장 경로가 있다. 공용 영역은 여러 어플리케이션에서 공용으로 사용할 수 있는 데이터들을 저장하는 부분으로, 고유영역과 동일하게 총 7개 데이터 유형에 대한 표준 저장 경로를 제공한다.

안드로이드 스마트폰의 경우 데이터 유형에 따라서 각각 저장되는 위치는 다르나, 사진이나, 동영상 및 업무용 문서 파일, 다운로드한 파일 등은 외부저장소인 SD카드에 저장되게 된다. 하지만, 안드로이드는 SD카드에 대한 보안을 적용하지 않는다. SD카드의 경우 운영체제와는 분리된 기억장치로, 보안에 취약한 FAT32 포맷으로 이루어져 있다.

안드로이드 스마트폰의 데이터관리 정책상 SD카드에 저장되는 파일은 악성코드 및 악성 앱, 도난, 분실 등에 의하여 언제든지 외부로 유출될 수 있는 취약점이 존재한다. 이에 다운로드한 파일이 저장되는 경로를 default로 설정하고, 그 외 사용자가 지정한 경로 및 파일들을 본 논문에서 구현하는 중요정보로 분류하여 설정한다.

2. Technology Design for Efflux Prevention of Important Information

2.1 중요정보 설정 기능

사용자가 중요정보를 설정할 경우 그림 4와 같이 탐색기 창을 통하여 중요정보를 설정하도록 한다.

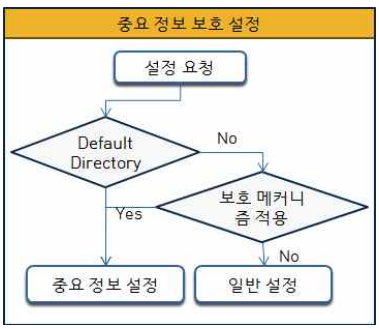

Fig. 4. Configuration of important information

Default 폴더는 SD카드의 다운로드하는 파일이 저장되는 장소로서 사용자의 선택 없이 자동으로 설정되고 그외는 사용자의 설정에 따라 적용한다.

2.2 File Monitor 모듈

중요정보 앱 보안 모듈은 중요정보를 자동으로 Search하는 모듈과 파일View가 파일을 요청하거나, 수정 또는 끝냈는지 확인 후 자동으로 암/복호 모듈로 이루어져 있다.

그림 5는 File Monitor 모듈로서 사용자가 선택한 파일을 복호하여 File View에게 해당 Content를 제공하고 이후 파일 사용이 끝났을 때 다시 암호화하는 기능을 수행한다.

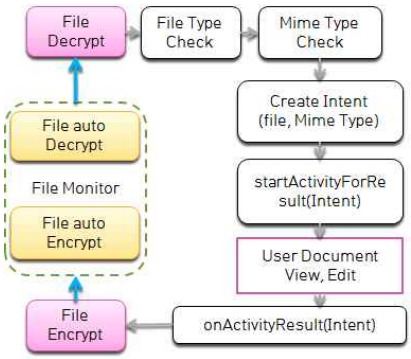

Fig. 5. File Monitor's module structure

사용자가 파일을 선택하면 해당 파일을 복호하고, 복호화된 파일타입을 체크한다. 그 다음, 파일 Mime Type을 체크하고, Intent를 생성하여, startActivityforResult()를 통하여 해당 값을 전달한다. 이후 onActivityResult() 함수를 통하여 결과값을 전달받아 해당 파일을 다시 암호화하게 된다.

2.3 Auto Search 모듈

구글에서 제공하는 FileObserver API를 이용하여 설계하였다. FileObserver API로 보호 정보 폴더의 Event를 감지하여 Event가 발생할 경우 FileType 및 MimeType을 체크하여, 암호화되어 있지 않는 파일일 경우 해당 파일을 암호화한다.

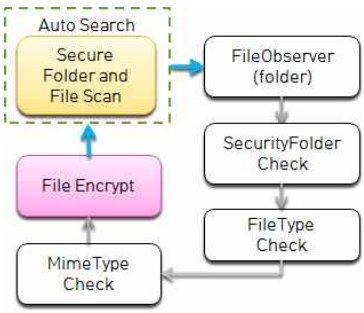

Fig. 6. Auto Search module

파일의 상태를 자동으로 체크하는 Auto Search 모듈(그림 6)을 통해 중요정보로 설정된 파일을 항시 암호화된 상태로 보존할 수 있다.

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2015.20.6.043

2.4 분실대비 중요데이터 삭제 기능

, 분실에 대비하여, 중요정보를 삭제하는 기능은 Google의 C2DM push 모듈을 활용하여 설계하였으며, 사용자가 보안 앱을 통하여, 설정한 중요데이터는 도난, 분실시에 대비하여 SMS에 특정 메시지를 설정한다. 이후 분실 또는 도난시 해당 메시지를 보냄으로써, SD 카드에 저장된 중요데이터를 원격으로 삭제한다.

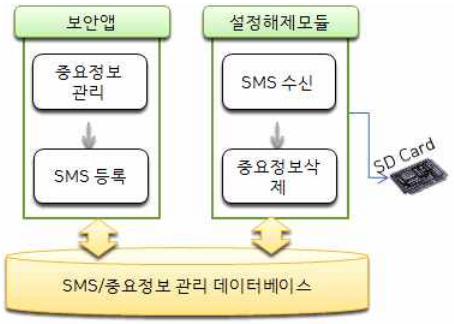

Fig. 7. Important information erasure function

IV. Test the Proposed System

1. Function Test for Efflux Prevention

1.1 보호 모드 설정

SD카드의 다운로드하는 파일이 저장되는 장소인 /sdcard/download로 사용자의 선택 없이 자동으로 중요정보로 설정하고, 사용자가 직접 선택하여 중요정보를 선택 할 수 있는 기능을 구현하였다. 그림 8에서는 /sdcard/data와 /sdcard/ DCIM 폴더를 중요데이터로 설정하였다. 보호 폴더가 설정되면 이후, 구글 FileObserver API에 의해서 파일이 추가될 경우에 자동으로 암호화한다.

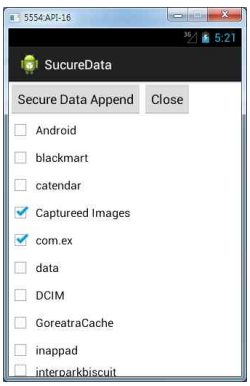

Fig. 8. Configuration of important information

1.2 문서 앱 보안 연동 기능

중요정보의 경우 해당 앱 프로그램을 통하여 다른 앱으로 연동되게 구현하였다. 암호화 된 중요 파일을 클릭하면, 연결된 File Viewer 앱에서 정상적으로 열람되는 것을 확인 할 수 있다(그림 9).

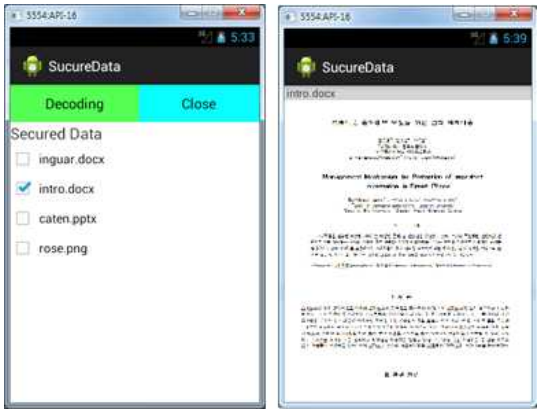

Fig. 9. Security connection of important file apps

1.3 분실시 중요정보 삭제 기능

중요정보 삭제 기능은 도난, 분실시에 대비하여 구현한 기능으로, Google의 C2DM push 모듈을 활용하여 구현하였다. 그림 10과 같이 사용자가 환경설정을 통하여, 분실시 이용할 SMS 메시지를 설정하고, 이후, “DeleteFlag”라는 SMS 메시지를 해당 스마트폰으로 전송하게 될 경우, 데이터 관리 프로세스에 의해 중요데이터로 설정되어 있던 /sdcard/download폴더의 내용이 모두 지워지는 것을 알 수 있다.

Fig. 10. Erasure of important information

2. Efflux Prevention Function Analysis

2.1 중요정보 암호화 기능 실험

중요정보 암호화 기능 실험을 위하여, 암호화한 정보 파일들을 직접 File Viewer를 통해서 열어보고, 개발된 앱을 통하여 해당 문서 File Viewer를 선택하여 열어보았다. 각각 동일하게 100회 반복 실험하였다.

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2015.20.6.043

Table 2. Experiment of Encodement function

파일 타입	종류	횟수	직접	개발앱	처리속도 (mil)
hwp	한글	100	0	100	501.51
doc	office	100	0	100	478.20
pdf	office	100	0	100	708.24
ppt	office	100	0	100	765.45
xlsx	office	100	0	100	479.41
jpg	Image	100	0	100	824.11

2와 같이 실험 진행결과를 얻었다. 제안 모듈을 탑재한 앱 연동시 모두 정상적으로 연동되어 열람이 가능하였고, 복호 모듈을 탑재하지 않은 콘텐츠 접근에 의해서는 보호되어 연결 실패가 발생하였다. 콘텐츠 암호화 처리속도는 각 파일의 용량과 스마트폰 프로세서 성능에 차이에 있다.

2.2 자동 암호화 및 삭제 실험

제안 앱을 통한 파일 File Viewer를 실행 뒤, 일부 수정 후 종료하여 해당 파일이 암호화된 상태로 보관되는지 확인하는 실험을 진행하였다. 총 실험횟수는 100회 진행하였고, polaris office, 한글 뷰어, Image Viewer의 3종류에서 실험하였다. 실험 결과, 앱 연동 종료 후 모두 암호화된 상태로 보관되었다. 도난/분실시에 대응으로 설정된 SMS문자 메시지를 전송하여 중요데이터 제거 기능이다. 삭제 테스트는 중요정보 삭제를 실패하는 경우가 3회 발생하였으며, 원인 확인 결과 네트워크와 서버의 부하에 의한 일시적인 google C2DM 모듈에서 SMS 메시지를 받지 못하는 경우가 발생하였을 때 실패하였다. 이러한 실패의 경우 패킷 재전송에 의한 프로세스 추가로 문제를 해결한다.

V. Conclusions

본 논문에서는 안드로이드 스마트폰 기반의 중요정보가 악성코드 및 악성 앱, 도난, 분실에 의하여 외부로 유출되는 것을 대비하여 항시 암호화된 상태로 보관 및 관리되는 메커니즘을 구현하였다. 또한, 도난, 분실에 대비하여 원격에서 삭제할 수 있는 기능도 구현하였다.

중요데이터 유출방지 메커니즘은 암호화된 상태로 자동 저장되기 때문에, 다운로드한 파일이 저장되는 영역을 항시 확인해야 하는 번거로움 없고, 원격삭제가 가능하여 도난, 분실시에도 외부로 유출될 가능성이 적다. 그런데 배터리 소모량이 기존에 비하여 많아져 재충전해야 하는 시간이 짧아지는 단점이 존재하지만 사용시 크게 불편하지는 않았다.

향후, 안드로이드 SDK의 SDcard 접근 제어 기법과 연관한 연구와 배터리 소모량을 줄이는 방안, 접근 매체별 접근 권한을 단계별로 적용하여 유연성 있는 접근 방법과 효율적 서비스 활용을 위한 연구를 진행 할 것이다.

References

[1] Garner Newsroom: PressRelease, "Gartner Says Indian Mobile Handset Sales To Reach 231 Million Units in 2012", Nov. 2011.

[2] Garner Newsroom: PressRelease, "Gartner Says Android to Command Nearly Half of Worldwide Smartphone Operating System Market by Year-End 2012", Apr. 2011.

[3] Google Android Developers OfficialSite: DevGuide, "What is Android?", 2012. http://developer.android.com/guide/basics/what-is-android.html.

[4] Ongtang, M., McLaughlin, S., Enck, W., and McDaniel., P. "Semantically Rich Application-Centric Security in Android", In Proceedings of the 25th Annual

[5] Sang-ho Park, Hyeonjin Kim, Taekyoung Kwon, "On Security of Android Smartphone Apps Employing Cryptography", Journal of The Korea Institute of Information Security & Cryptology, Vol. 23, No. 6, Dec. 2013.

[6] Woongryul Jeon and Jeeyeon Kim, Youngsook Lee, Dongho Won, “Analysis of Threats and Countermeasures on Mobile Smartphone” Journal of the Korea society of computer and information, Vol.16 No.2, pp.153-163, 2011.

[7] Educational industrial group of university of Seoul, "Analysis of Android Mobile Platform Security Model", Korea Internet and Security Agency, 2010.

[8] Moon-Goo Lee, "Implementation of Remote Physical Security Systems Using Smart Phone", Journal of the Korea society of computer and information, Vol. 16 No.2, pp.217-224, 2011.

[9] Eun-Gyeom Jang, Seok-Woo Nam, "Study on the Camera Image Frame's Comparison for Authenticating Smart Phone Users" Journal of the Korea society of computer and information, Vol. 16, No. 6, pp.155-164, 2011.

[10] Moon Gun-Hwan, "Security Mechanism based on Android smart phone for Preventing Important Data", Master´s thesis of Daejeon University, August 2012.

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2015.20.6.043

Authors

Eun-Gyeom Jang received a PhD in Daejeon University in 2007.
He is currently a Professor in the Department of Internet Communication, Jangan University.
It has an interest in mobile communications, system security and Computer Forensics.