한국컴퓨터정보학회 동계학술대회 논문집 제22권 제1호 (2014. 1)

스마트폰 중요정보 보호를 위한 관리 메커니즘

장은겸°, 정진영*, 안우영*
°대전대학교 컴퓨터공학과
*대전보건대학교 바이오정보과
e-mail:jangegu@nate.com°,{jyjung, wyahn}@hit.ac.kr*

Management Mechanism for Protection of Important Information in Smart Phone

Eun-Gyeom Jang°, Jin-Young Jung*, Woo-Young Ahn*
°Dept. of Computer Engineering, Daejeon University
*Dept. of Bio Information, Daejeon Health Sciences College

● 요 약 ●

스마트폰을 활용한 다양한 서비스는 다양한 문화 및 편의성을 제공하고 있다. 그러나 무분별한 컨텐츠의 접근으로 인해 발생하는 개인의 사적인 정보 유출과 시스템에 악영향을 미치는 코드의 접근으로 사회적인 문제를 발생시키고 있다. 이에 본 논문에서는 스마트폰의 중요 정보를 보호하기 위한 매체접근 관리 정책을 기반으로 단계별 접근 관리 기술을 적용하여 안정한 컨텐츠 및 중요 정보를 보호하기 위한 기술을 제안한다.

키워드: 스마트폰(smart phone), 중요정보(important information), 정보보호(information Protection)

I. 서 론

스마트폰이 가진 편리함으로 인하여 스마트폰이 급속도로 확산되자 이와 함께 스마트폰의 보안 취약점을 이용한 보안사고 또한 꾸준히 증가하였다. 스마트폰은 개인연락처 및 사진 등 중요정보를 포함하고 있고, 폰 자체의 보안 취약점을 가지고 있기 때문에 악의적인 목적을 가진 사람들의 좋은 표본이 되고 있다. 또한, 스마트 폰은 무선네트워크를 이용하기 때문에 실시간으로 인터넷으로 연결할 수 있으나 무선구간에서 패킷스니핑 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 존재하고 있다. 이에 스마트폰 기반의 중요데이터를 보호하기 위한 보안 메커니즘을 연구하였다.

II. 관련 연구

1. 중요데이터 유출 위협

1.1 안드로이드 보안 취약점

공격목표에 의한 분류는 크게 표 1과 같이 정보유출, 오작동, 과금회피로 나눌 수 있다.

표 1. 공격 대상
Table 1. Target of an attack

분류	공격내용
정보유출	정보의 유출(개인/업무/위치 /금융거래 등)
오작동	단말기사용불능, 단말기전력소모, DDOS 공격, SMS 과금유도
과금회피	컨텐트 무단복제

공격대상의 의한 분류는 표 2와 같이 플랫폼 공격, 어플리케이션 공격, 네트워크 공격 및 단말기 분실 등으로 인한 공격이 존재한다.

표 2. 공격대상
Table 2. Object of an attack

분류	공격내용
플랫폼 공격	바이러스/웜
	시스템Unlock
	키보드해킹
어플리케이션 공격	Malicious 앱, Fishing 앱
네트워크 공격	Wi-Fi/무선 네트워크 도청/변조
	DDOS공격
단말기 공격	단말기 도난/분실
	Malicious 앱

1.2 악성코드에 의한 피해 사례

악성코드의 경우 감염되면 개인정보 및 단말기 고유정보를 유출하거나 단말기 이용의 방해 및 SMS 무단 전송 등을 통한 과금유발 등의 피해를 이용자에게 입힌다. 해외에서에는 심비안 및 안드로이드 OS 탑재 스마트폰을 대상으로 이러한 피해 사례가 보도되고 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 감염된 경우가 있었다.

표 3. 악성코드
Table 3. Malignant code

No	악성코드명	주요 악성행위
1	Jackeey wallpaper	정보유출
2	Christmas wallpaper	정보유출
3	Trojan-SMS.AndroidOS.FakePlayer.a	SMS 무단전송
4	Tapsnake	정보유출
5	Trojan-SMS.AndroidOS.FakePlayer.b	SMS 무단전송
6	Trojan-SMS.AndroidOS.FakePlayer.c	SMS 무단전송
7	FLEXISPY	정보유출
8	Secret SMS Replicator	SMS 유출
9	Geinimi	정보유출, SMS 무단전송

악성코드에 의한 피해 종류로는 표 4와 같이 5가지 형태로 나눌 수 있다.

표 4. 악성코드 분석
Table 4. Malware analysis

악성코드종류	설명
단말 장애 유발형	단말의 사용을 불가능하게 만들거나 장애를 유발하는 공격 유형
배터리 소모형	배터리를 고갈시키는 공격 유형
과금 유발형	메시징 서비스나 전화 시도를 지속적으로 시도하여 과금을 발생시키는 공격 유형
정보유출형	단말의 정보나 사용자 정보를 외부로 유출시키는 공격 유형
크로스 플랫폼형	모바일 단말을 통해 PC를 감염시키는 공격 유형

2. 안드로이드 보안 기술

2.1 MTM 기술

사용자의 부주의로 인한 시스템 (노트북, 휴대 단말 등) 분실 혹은 외부 제 3자에 의한 시스템 도난 등을 통해 단말 복제, 도청 및 악용, 단말의 프라이버시 데이터 보호 위협, 악성 코드 삽입 등의 보안 위협은 여전히 해결되지 않은 숙제로 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.

2.2 앱스토어 보안 기술

앱스토어에 어플리케이션을 등록하고 배포 시, 어플리케이션의 안전성을 확보하는 기술이다. 모바일 어플리케이션의 유통 인증 기술과 앱스토어에 등록된 어플리케이션에 대한 보안 검증 기술로 모바일 어플리케이션의 유통 인증 기술은 어플리케이션이 앱스토어에 등록되어 구매자에게 전달되기까지 유통자 증명을 제공하는 기술로써 이를 위해 코드 사이닝(Code Signing)기술을 적용하고 있다. 개발자는 개발한 모바일 어플리케이션의 신원증명을 위해 인증서로 코드사이닝하여 앱스토어에 등록하고 앱스토어에서는 해당 어플리케이션에 대한 신원증명을 확인하여 개발자 확인 절차를 수행한다.

2.3 중요정보 유출방지 기술

기업 구성원, 프로세스, 기술의 결합을 통해 고객 또는 직원 기록 등의 개인 신원확인 정보, 재무제표, 마케팅 계획과 같은 기업 정보, 제품 계획, 소스 코드와 같은 지적 재산을 포함하는 기밀정보 등의 중요정보가 기업 밖으로 유출되는 것을 방지하는 기술이다. 정보유출은 외부로부터의 악의적인 공격이라기보다 일반 직원들의 부주의와 기업 프로세스 위반으로 인해 주로 발생하였으나, 최근 스마트폰에서의 정보유출은 스마트폰의 취약점 및 도난, 분실에 의한 유출이 많다. 이에 스마트폰에서도 데이터의 유출을 방지하는 기술이 필요하다.

III. 중요데이터 보호 메커니즘

악성 코드와 악성 앱, 도난, 분실 등으로 인하여 중요데이터가 유출될 수 있으며, 안드로이드의 경우 SD카드와 같은 공용 영역의 보안은 제공하지 않음으로 이에 대한 방안으로 중요데이터의 경우 유출 방지를 위하여 그림 1과 같이 항시 자동 암호화된 상태로 보관되어야 하며, 필요시 원격에서 삭제할 수 있는 기술이 필요하다.

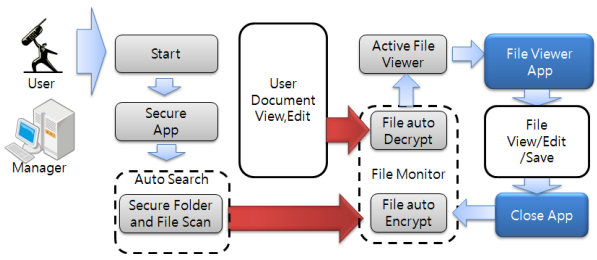

그림1. 앱 보안 모듈
Fig. 1. App security module

1. 안드로이드 스마트폰 데이터 관리

안드로이드 어플리케이션의 경우 가장 크게 어플리케이션 데이터가 저장되는 내부 저장소 영역과 사진, 비디오, 데이터 등을 저장하는 외부 저장소 영역으로 나뉠 수 있으며, 각 영역별로 다시 캐시 데이터가 저장되는 영역, 데이터베이스가 저장되는 영역 등으로 나뉜다.

① 데이터관리 구조

내부 저장소는 각 어플리케이션에서만 데이터를 읽고 쓸 수 있으며, 크게 캐시(Cache), 데이터베이스, 일반파일이 있다. 외부저장소는 일반적으로 이는 단말기의 외장SD카드를 지칭하는데, 특정 어플리케이션에서만 사용하는 어플리케이션 고유 영역과 공용 영역이 각각 존재한다. 어플리케이션 고유 영역에 각 데이터 유형별로 데이터를 저장하는 영역으로 데이터의 유형에 따라 별도의 디렉터리를 사용한다. 안드로이드에서는 총 7개 데이터 유형에 대한 표준 저장 경로와 위치를 지정하지 않았을 경우에 대한 경로가 있다. 공용 영역은 여러 어플리케이션에서 공용으로 사용할 수 있는 데이터들을 저장하는 부분으로, 고유영역과 동일하게 총 7개 데이터 유형에 대한 표준 저장 경로를 제공한다.

② 중요데이터 분류

안드로이드 스마트폰의 경우 앞서 설명한 데이터 구조에서와 같이 데이터 유형에 따라서 각각 저장되는 위치는 다르나, 사진이나, 동영상 및 업무용 문서 파일, 다운로드한 파일 등은 외부저장소인 SD카드에 저장되게 된다. 하지만, 안드로이드는 SD카드에 대해서는 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 중요데이터로 분류하여 설정한다.

③ Intent의 동작구조

Activity에서 다른 Activity를 호출하는 주된 이유는 파일을 선택하거나 그림을 보여주라거나 하는 등의 뭔가 작업을 시키기 위해서로, Main Activity에서 혼자 다하려면 반복이 심해지고 형식성에도 떨어지므로, 다른 Activity를 호출하여 일을 분담시키게 된다. 이때 Activity끼리 서로 호출하려면 통신을 위한 장치가 필요한데 이 장치가 바로Intent이다.

2. 중요데이터 유출방지 메커니즘 설계

2.1 중요데이터 설정 기능

사용자가 중요데이터를 설정할 경우 그림 2와 같이 탐색기 창을 통하여 중요데이터를 설정하도록 한다.

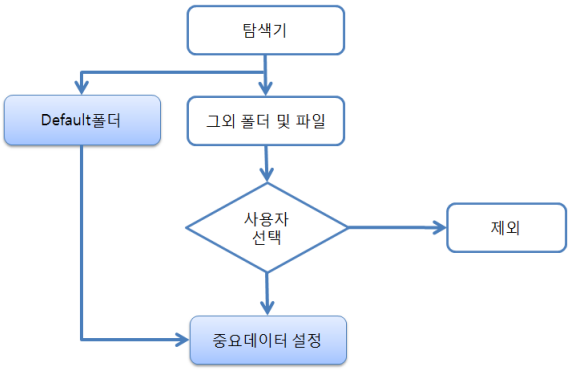

그림 2. 중요데이터 설정
Fig. 2. Important information set

2.2 중요데이터 관련 앱 보안 연동 기능

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

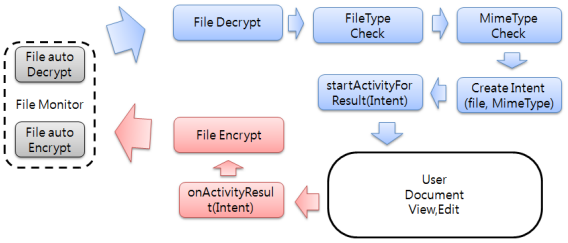

그림 3. File management 모듈 구조
File management module structure

그림 3은 사용자가 선택한 파일을 복호화하여 File View에게 해당 Content를 제공하고 이후 파일 사용이 끝났을 때 다시 암호화하는 기능을 수행한다. 이 후 복호화 된 파일타입을 체크한다. 그 다음, 파일 MimeType을 체크하고, Intent를 생성하여, startActivityforResult()함수를 통하여 해당 값을 전달한다. 이후 onActivityResult() 함수를 통하여 결과 값을 전달받아 해당 파일을 다시 암호화하게 된다.

IV. 중요데이터 유출방지 기능 구현 및 실험

1. 중요데이터 암호화 기능 실험

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

표 5. 암호화 실험
Table 5. Encryption test

타입	종류	횟수	직접	개발앱
hwp	한글	100	0	100
doc	office	100	0	100
pdf	office	100	0	100
ppt	office	100	0	100
xlsx	office	100	0	100
jpg	Image	100	0	100

실험 진행결과 개발한 앱으로 연동시 모두 정상적으로 연동되어 열람이 가능하였고, 직접 연동시에는 모두 실패하였다.

2. 자동 암호화 여부 실험

개발된 앱을 통한 파일 File Viewer를 실행 뒤, 일부 수정 후 종료하여 해당 파일이 암호화된 상태로 보관되는지 확인하는 실험을 진행하였다. 총 실험횟수는 100번으로 진행하였고, polaris office, 한글 뷰어, Image Viewer의 3종류에서 실험하였다.

표 6. 자동 암호화 실험
Table 6. Auto Encryption Test

앱	횟수	성공	실패
office	100	100	0
한글	100	100	0
Image	100	100	0

실험 결과 앱 연동 종료 후 모두 암호화된 상태로 보관되었다.

3. 분실시 중요데이터 삭제 실험

도난, 분실시에 대비하여, 설정된 SMS문자 메시지를 전송하였을 때 중요데이터가 정상적으로 삭제되는지 확인하는 삭제 테스트를 진행하였다.

표 7. 삭제 테스트 결과
Table 7. Delete Test result

전송횟수	성공	실패
100	98회	2회

테스트 결과 삭제가 실패하는 경우가 2회 발생하였으며, 원인 확인 결과 google C2DM 모듈에서 SMS 메시지를 받지 못하는 경우가 발생하였을 때 실패하였다.

V. 결론

본 논문에서는 안드로이드 스마트폰 기반의 중요데이터가 악성코드 및 악성 앱, 도난, 분실에 의하여 외부로 유출되는 것을 대비하여 항시 단계별 접근 권한 기술을 적용하였다. 중요정보 및 컨텐츠를 로컬 및 원격에서 관리할 수 있도록 시스템을 설계하여 외부의 위험성으로부터 스마트폰을 보호하였다.

향후 사용자의 편의성과 다양한 컨텐츠의 특성을 고려한 접근 관리기술을 단계별로 적용하여 외부의 도난 및 분실 등의 위험성으로부터 보호할 수 있도록 추가적인 연구를 통해 활성성 높은 안전한 기술을 연구할 것이다.

참고문헌

[1] IDC, "IDC Worldwide Quarterly Mobile Phone Tracker", http://www.idc.com/getdoc.jsp?containerId=prUS22689111, 2011.

[2] Google Android Site, "What is Android?", http:// developer.android.com/guide/basics/what-is-android.html, 2012.

[3] UOS R&DB Foundation, "Analys is of Android Mobile Platform Security Model", KISA, Research Report, 2010.

[4] D.J. Kang, J,H.Han, Y.K.Lee, Y.S.Cho, S.W.Han, J.N.Kim, H.S.Cho, "Smartphone Threats and Security Technology", ETRI, Vol. 25, No. 3, 2010.

[5] Trusted Computing Group, "TCG Specification Architecture Overview", Specification Revision, 1.4. 2007.