http://dx.doi.org/10.5392/JKCA.2013.13.12.560

스마트폰에서 가상 디스크 플랫폼을 사용한 프라이버시 데이터 보호 방안

Privacy Data Protection Methods on Smartphone Using A Virtual Disk Platform

신숙조*, 김선주**, 조인준*
배재대학교 컴퓨터공학과*, 한국정보통신기술협회**

Suk-Jo Shin(sukssj@pcu.ac.kr)*, Seon-Joo Kim(uneedme@paran.com)**,
In-June Jo(injune@pcu.ac.kr)*

요약

2009년 애플사에서 아이폰을 출시하면서 스마트폰이 개인의 생활패턴을 크게 바꿔 놓았다. 즉, 스마트폰이 등장하면서 음성통화위주에서 음성/화상통화, 카메라, 전자메일 송수신, 웹 브라우징 등 다양한 서비스가 이루어지고 있다. 그러나, 스마트폰의 사용범위가 넓어지는 만큼 기업은 주요 문서 보호를 위해 MDM솔루션을 도입할 필요성이 커지고 있다. 하지만, 이러한 MDM 솔루션은 스마트폰내에 저장된 연락처, 사진, 메모 등의 모든 데이터를 제한 없이 접근 가능한 문제점이 발생한다. 이로 인해 스마트폰 사용자는 원하지 않는 사생활 침해가 발생할 우려가 있다. 본 논문에서는 스마트폰 사용자가 공개를 허락한 파일만 기업의 보안담당자 또는 MDM 관리자에게 접근이 가능케 하고 비공개 파일은 가상 디스크에 별도로 저장하여 스마트폰 사용자 이외에는 접근이 불가능하게 하는 스마트폰 사용자의 개인 프라이버시 파일 보호방안을 제안하였다.

■ 중심어 : | 프라이버시 보호 | 개인정보보호 | Moble Device Management |

Abstract

The release of iPhone by Apple in 2009 has changed the life pattern of an individual tremendously. That is, with the emergence of a smart phone, various services including voice/video call, camera, receiving and sending of e-mail, and web browsing have been realized. However, the broader the scope of the use of a smart phone has become, the greater the need for companies to introduce an MDM solution for protecting important documents has become. However the MDM solution may have a problem in that all data such as contacts, pictures, and memos saved in the smart phone can be accessed unlimitedly. For this reason, there is a risk that unwanted violation of privacy may happen to smart phone users. This paper proposed a plan to protect a personal privacy file of smart phone users, which disables access by others except for related smart phone users by enabling a person in charge of security or an MDM manager in a company to have access only to the file which was allowed by smart phone users to be disclosed and by saving non-disclosed files in a virtual disk.

■ keyword : | Privacy Prevention | Personal Information Protection | Moble Device Management |

접수일자 : 2013년 10월 25일
수정일자 : 2013년 11월 14일
심사완료일 : 2013년 11월 14일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

스마트폰이 일상생활에서 중요한 부분을 차지하면서 스마트폰내의 개인 프라이버시 정보 보호 및 회사중요 업무 보호 등의 쟁점이 대두되고 있다. 즉, 개인 소유의 스마트폰이 기업 업무수행에 활용될 뿐만 아니라 인터넷 활용, 금융거래에 활용 등 다양한 영역으로 점차 확대됨에 따라 이에 부응한 보안문제가 부각되고 있다.

이와 같이 스마트폰이 다양한 영역으로 확대면서 보안을 중요시 하는 기업에서는 MDM(Mobile Device Management)솔루션을 사용하여 기업의 보안정책을 내부 임직원 스마트폰에 강제적으로 적용하는 방향으로 전환 중에 있다.

하지만, 보안담당자 또는 MDM 관리자의 권한이 막강하여 스마트폰에 탑재된 기업업무 영역뿐만 아니라 스마트폰 소지자의 사생활 영역의 정보까지 자유롭게 침해 할 수 있는 문제가 발생하고 있다.

본 논문에서는 이러한 스마트폰에서 사적인 개인정보 침해문제 해결을 위해서 가상 디스크 기술 및 키 체인기술을 이용하여 스마트폰 사용자의 프라이버시 보호방안을 새롭게 제시하였다.

II. 연구 동기 및 관련기술

1. MDM 개요 및 문제점

현재 스마트폰은 MDM을 통해서 원격으로 관리되고 있다. 이는 스마트폰 사용자의 의지와는 관계없이 MDM관리자에게 자신의 스마트폰 자원을 자유롭게 노출시키는 문제가 발생한다.

기업에서 사용하는 스마트폰 MDM은 기업 내부의 임직원 스마트폰을 대상으로 자사의 보안정책에 부합되도록 스마트폰을 제어하는 스마트폰 관리 솔루션이다[1]. 즉, 스마트폰에 기업의 보안정책을 적용하고, 스마트폰에서 발생하는 문제해결을 목적으로 개발이 되었다. MDM의 기능은 업체마다 차이는 있지만 일반적으로 사용자정보 조회(이름, 부서, 이메일, 전화번호등), 단말정보 조회(OS버전, 제조사, CPU, 메모리등), 소프트웨어 배포 관리(앱 배포, 삭제, 설치 현황 조사), 디바이스 제어(카메라, WiFi, GPS, 블루투스, E-mail. 화면캡처 등), 앱 제어(실행 중인 앱조회, 앱 실행, 프로세스 실행통제 등), 백업 및 복원, 무선 및 VPN설정, 기타 앱스토어, 브라우저 사용제한, AD 및 LDAP 연동 기능 등이 제공 된다[13].

국내 기업에서 이러한 상용 MDM 도입이 일반화되는 추세이다. 2011년 말~2012년 상반기 코오롱그룹, 이랜드그룹, 금호아시아나 등이 상용 MDM 솔루션을 검토, 도입했고 이어 신한금융그룹, 롯데카드, LIG손해보험 등이 연달아 모바일 기기 보안 관리 및 모바일 오피스 보안을 위해 MDM 솔루션을 도입하였다.

따라서, 이러한 MDM의 도입은 MDM의 제어 하에 있는 스마트폰의 개인 프라이버시 정보가 MDM관리자에게 노출되는 문제점을 지니고 있다.

2. 개인 프라이버시 정의

본 논문은 스마트폰에서 개인 프라이버시 침해문제 해결방안을 제시했다. 따라서 개인 프라이버시 정보에 대한 정의를 다음과 같이 하여 보호대상 범위를 정하였다.

개인 프라이버시의 사전적 의미는 개인의 사생활이나 집안의 사적인 일. 또는 그것을 남에게 간섭 받지 않을 권리를 의미한다[14]. 보안업체 시만텍은 스마트폰 분실 시 습득자가 어떤 행동을 하는지 관찰하는 실험이 있었다[15].

즉, 스마트폰 50대를 택시, 음식점, 화장실, 길가 등에 일부러 분실하고 습득자가 어떤 행동을 하는지 관찰하는 실험 결과가 [표 1]과 같다. 표에서 보듯이 스마트폰 분실은 곧 개인 프라이버시 유출이란 보안사고로 이어짐을 보여주고 있다.

표 1. 스마트폰 분실 시 정보별 접속 시도

구 분	비율(%)
사진	72
소셜미디어	60
암호	57
회사월급파일	53
기업 전자메일	45
모바일 뱅킹	43
회사관련사례파일	40

이는 분실 시에 발생한 개인프라이버시 침해유형이지만 스마트폰을 자유롭게 제어할 수 있는 MDM 관리자에게도 동일한 유형의 침해사고가 발생할 수 있다[4]. 본 논문에서는 개인 프라이버시에 대한 정의를 다음에 제시한 개인정보와 프라이버시 정의를 준용하여 보호범위를 반영하도록 하였다.

개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다[16].

프라이버시: 사생활 정보이며, 심리적 주관적인 것으로 사람에 따라 민감한 것일 수도 있으며 그렇지 않은 것 일수도 있다. 개인의 취미, 습관 등 개인의 사생활적 이익을 통칭하는 개념을 말한다[3].

3. 가상 디스크 기술

본 논문에서 가상 디스크 기술을 스마트폰에 새롭게 도입하여 개인 프라이버시 문제를 해결하는 방안을 제시하고 있다. 따라서 가상 디스크 기술을 간략하게 요약하면 다음과 같다.

가상 디스크는 디스크 이미지 파일을 실제 물리 디스크처럼 사용하는 것을 의미한다[17]. 실제로는 존재하지 않는 디스크를 디스크 이미지파일을 통해 논리적으로 구현하여 마치 실제 물리 디스크를 사용하는 것과 같은 효과를 나타낸다.

디스크 이미지는 저장 장치를 하나의 파일로 복제한 것이다. 디스크에 포함한 데이터뿐만 아니라 해당 저장장치의 구조까지 그대로 복제한 것으로 해당 디스크를 완벽하게 복제한 하나의 파일이다. 일반적으로 섹터 대 섹터 방식으로 복사가 진행되며 복사의 주체는 디스크의 섹터이다. 디스크와 디스크 단위에서의 복사에 적용되는 개념으로 원본 디스크와 대상 디스크의 섹터를 1:1로 대응시켜 각 섹터의 데이터를 그대로 원본 섹터에서 대상 섹터로 일일이 복사하는 방식이다[5]. 이런 방식으로 원본 디스크의 데이터를 옮겨 담은 복제 디스크가 만들어진다. 디스크 이미지는 원본 디스크의 내용을 그대로 복제한 것이기 때문에 원본과 동일한 크기를 가진다. 이렇게 생성된 이미지 파일을 마운트하여 가상 디스크를 생성한다.

4. 키체인 기술

본 논문에서 키체인 기술을 도입하여 개인 프라이버시 파일의 암복호 키를 용이하게 관리하는 방안을 제안하고 있다. 따라서 키체인 기술을 간략하게 요약하면 다음과 같다.

키체인(Keychain)이란 애플사의 MacOS에서 사용하는 비밀번호 관리 시스템을 뜻하는 용어로써, MacOS 8.6때 처음 소개되었다[18]. 해당용어는 애플사의 iOS에서 처음 나왔다. 키체인은 웹사이트, FTP 서버, SSH 계정, 무선 네트워크 정보 등 다양한 형식의 데이터를 포함할 수 있다.

키체인 파일은 일반적으로 사용자의 로그인 암호, 로그인 해제 키체인이다. 유휴시간이나 응용프로그램에서 수동으로 잠글 수 있으며 모든 프로그램에 대한 인증 시 키값을 저장하고 차후 프로그램 재사용 시 별도의 인증 절차 없이 키체인에서 인증키를 찾아 인증을 시도한다. 응용프로그램에서는 키체인에 저장되어 있는 인증키가 확인되어 동작이 수행된다.

아이폰에서 암호를 저장하는 장소로 키체인이 있으며, 키체인은 iOS에서 관리를 하고 이곳에 들어가는 데이터는 모두 암호화되어 저장이 된다. 따라서 아이디와 암호를 안전하게 저장할 수 있다

아이폰 키체인은 MacOS X의 키체인과 유사하며 password, 인증서들을 저장하기 위해서 사용된다. iOS에서도 민감한 데이터를 저장하기 위해서 사용된다.

아이폰에서 보안성 강화를 위해 모든 프로그램에 대한 인증을 제공한다. 프로그램을 사용하기 위해서 인증을 받아야 하며 매번 인증을 받아야 하는 불편함을 별도의 키체인을 사용함으로써 그 유용성을 개선 시켰다.

Ⅲ. 제안 방안

본 논문의 기본 아이디어는 첫째, 스마트폰 내의 모

든 파일을 개인 프라이버시 파일과 일반 공개 파일 2가지로 분류한다. 둘째, 스마트폰에 장착된 하나의 물리적인 디스크에 논리적인 디스크인 가상 디스크를 새롭게 생성한다. 셋째, 2가지로 분류된 파일 중 일반 공개파일은 기존처럼 물리적 디스크에 저장하여 관리하고, 개인 프라이버시 파일은 논리적인 디스크인 가상 디스크에 저장하여 보안을 강화하는 방안이다.

즉, MDM관리자는 스마트폰에서 일반 공개 파일에 대해서는 해독이 자유롭지만 보안이 강화된 가상 디스크에 저장된 개인프라이버시 파일은 접근 및 해독이 불가능하도록 하였다.

본 장에서는 가상 디스크 드라이브 기술과 비밀번호 관리 기술인 키체인 기술을 적용하여 스마트폰 사용자의 프라이버시 데이터 보호방안을 기술하였다.

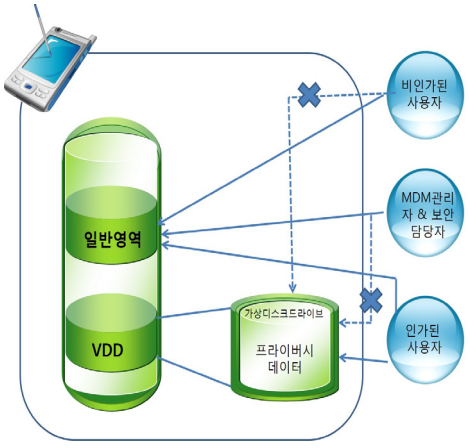

그림 1. 제안시스템 개념도

제안시스템의 전체적인 개념도는 [그림 1]과 같다. 그림에 보듯이 기존의 물리적 저장영역을 일반영역과 논리적인 암호화 가상 디스크 영역으로 구분한다. 그런 다음 사용자의 프라이버시 파일은 암호화 영역에만 저장하도록 하였다. 이때, 일반영역에 들어갈 데이터와 암호화 영역에 저장될 데이터는 스마트폰 사용자가 설정할 수 있도록 했다.

이렇게 설정하여 접근권한이 없는 사용자와 MDM관리자 및 보안담당자는 일반영역에만 접근이 가능하고, 접근권한이 있는 사용자만 암호화된 데이터 영역에 접근이 가능하다. 이때, 사용자의 접근권한 유무는 사용자가 설정한 비밀번호를 입력 받아 확인한다.

1. 가상 디스크 생성절차

스마트폰에서 다음과 같은 절차로 가상 디스크를 생성한다.

가상 디스크 드라이브를 만들기 위하여 스마트폰에서 저장될 위치 및 파일명을 설정한다.

스마트폰의 내장 디스크의 여유 공간을 고려하여 사용자로부터 가상 디스크의 크기를 입력받아 설정한다.

가상 디스크 드라이브에 접근권한을 인증하기 위한 비밀번호를 설정한다.

위의 ① ~ ③의 과정에서 입력 받은 파일명 및 저장위치와 가상 디스크 크기에 따라 가상 디스크를 생성 후 ③에서 입력 받은 비밀번호를 이용하여 가상 디스크를 암호화하여 가상 디스크 파일을 생성한다.

④의 과정에서 생성된 가상 디스크 파일을 가상 디스크 드라이브로 마운트 한다.

가상 디스크 드라이브에 저장될 프라이버시 보호 대상 데이터를 설정한다.

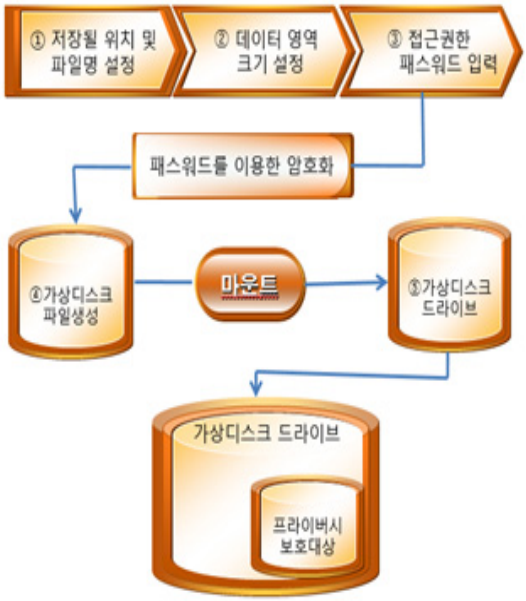

그림 2. 가상 디스크 드라이브 생성

가상 디스크 드라이브에 저장되는 파일의 크기가 최대 가상 디스크 드라이브보다 크게 될 수 없다. 파일관리에 있어서 파일의 데이터영역을 제외하고 파일 헤더 부분을 따로 관리할 수 있도록 하며 각 파일별로 암/복호화 하여 디스크 관리한다.

가상 디스크 드라이브 내부구조를 살펴보면 다음 [그림 3]과 같다.

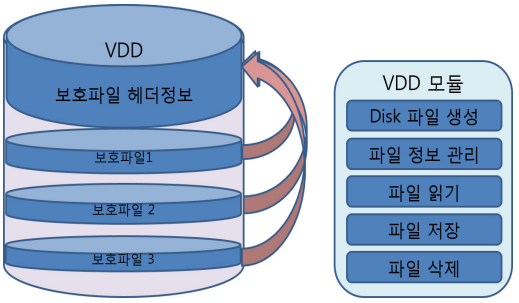

그림 3. 가상 디스크 드라이브 구조

2. 제안시스템 구조

스마트폰에서 사용자가 가상 디스크 드라이브에 데이터 파일을 저장관리 하며, 해당 데이터 파일의 암호화를 위한 Key 생성 및 관리, User 접근제어를 간략하게 [그림 4]와 같이 볼 수 있다.

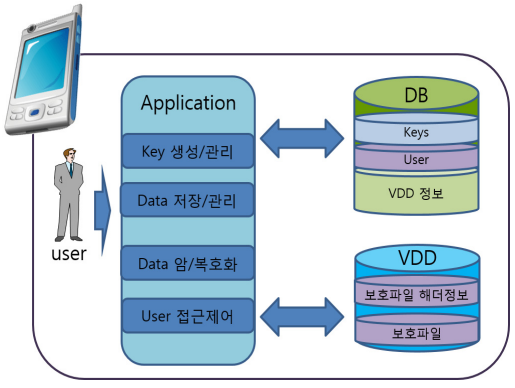

그림 4. 제안시스템 구성

인가된 사용자가 사생활 보호를 위해 가상 디스크 드라이브를 이용하여 파일을 저장하기 위해 연동되는 상세 모듈을 다음과 같이 설명할 수 있다.

제안 시스템이 동작하기 위해서 Application 모듈을 통하여 가상 디스크 드라이브에 보호파일에 저장된다. DB에는 Key정보, User정보, 가상 디스크 드라이브의 헤더정보가 보관되며, 가상 디스크 드라이브에는 인가된 사용자가 보호하려고 하는 보호파일과 보호파일의 헤더 정보가 보관된다. Application의 Key 생성/관리 모듈, Data 저장/관리 모듈, Data 암/복호화 모듈, User 접근제어 모듈을 통하여 가상 디스크 드라이브와 DB에 저장하고 조회할 수 있으며, 각 모듈에 대한 상세 구성은 다음 [그림 5]와 같다.

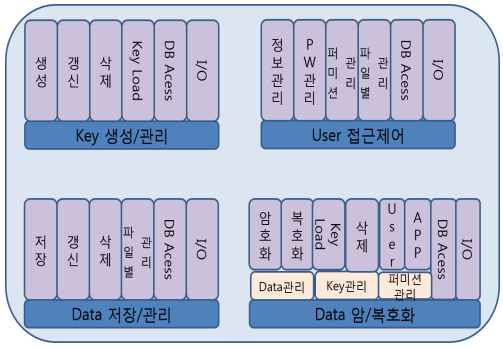

그림 5. 제안시스템 모듈구성

Key 생성/관리 모듈은 사용자로부터 입력받은 ID/Password와 사용자에 대한 정보를 관리하며, DB의 Key Table로부터 ID/Password의 유효성 검사를 하고 전달받은 KeyID를 관리한다. 키생성은 아래 [그림 6]과 같다.

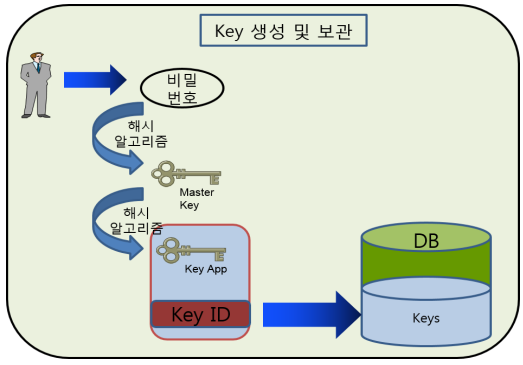

그림 6. Key 생성 및 보관

마스터키를 이용하여 Application별 key를 생성하는데 마스터키는 사용자가 입력하는 비밀번호를 해시알고리즘을 이용하여 마스터키를 생성한다. 여기서 생성되는 마스터키는 저장되지 않는다. 생성된 마스터키와 Application명칭을 조합하여 해쉬알고리즘으로 Key app값과 Application명칭을 해쉬알고리즘으로 Key ID 값을 생성한다. 생성된 Key ID와 Key(app)을 DB의 Key Table에 저장한다.

Data 암복호화 모듈은 Data관리 모듈로 보호파일별 암/복호화 하며 Key관리 모듈을 통하여 Key load, 삭제한다. 파일의 암호화는 Key(app)로 암호화 하며 복호화 할 경우 DB에서 KeyID를 확인하여 Key(app)를 획득 후 파일을 복호화 한다. 다음 [그림 7]은 암호화 과정을 나타낸다.

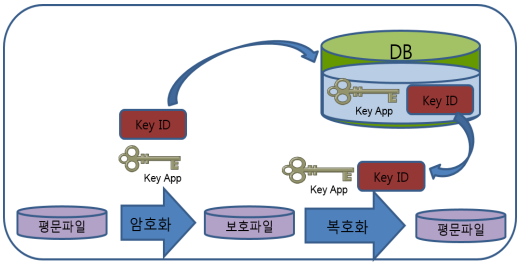

그림 7. 파일 암복호화

User 접근제어 모듈은 사용자 추가, 수정, 삭제기능과 비밀번호 관리 기능이 있다. ID/Password로 다음 [그림 8]과 같이 인가된 사용자를 확인한다.

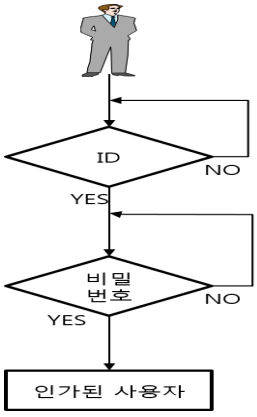

그림 8. 사용자 접근제어

2. 동작 절차

가상 디스크 드라이브에 저장될 프라이버시 보호 대상 데이터를 설정 후 스마트폰에 설치된 여러 개의 앱에서 프라이버시 보호 대상 데이터에 접근할 때마다 다음과 같은 절차로 수행된다.

사용자가 스마트폰 초기 접속이 아니며 개인 사진 파일을 보호하기 위해 가상 디스크 드라이브에 보호파일로 등록하는 전체 동작을 다음과 같이 기술한다.

접근을 허가받기 위해 사용자로부터 ID/비밀번호를 입력한다.

처음 접속 하였을 때 생성한 마스터키로 Key(App), KeyID가 DB에 저장되어 있다. DB의 저장되어 있는 정보로 사용자의 유효성을 검사한다.

사용자 유효성 확인과 KeyID를 받는다.

사용자는 사진 등록 요청을 한다.

VDD에 사진파일 저장하기 전 파일을 암호화하기 위해 Key(App)가 필요하다. DB로부터 KeyID를 전송하여 Key(App)를 요청한다.

사진파일 암호화를 위해 DB로부터 Key(App)를 전송받는다.

사진파일을 Key(App)로 국내 표준 128비트 블록 암호화 알고리즘 SEED를 사용하여 암호화 한다.

VDD에 암호화 된 보호파일로 저장된다.

암호화 된 보호파일의 헤더 정보만 VDD의 보호파일 헤더정보테이블에 저장한다.

사진파일 정상적으로 저장완료

사진파일2 등록 요청

⑤ ~ ⑩ 과정을 반복적으로 진행

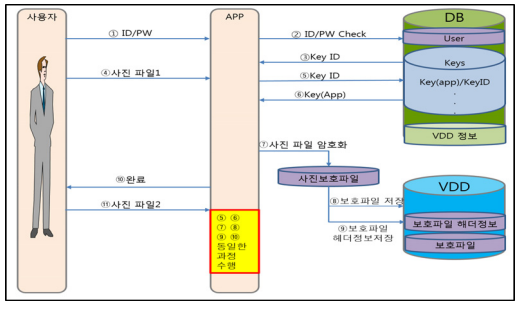

그림 9. 제안시스템 동작절차

여러 가지 앱의 사용이 종료되거나 사용자에 의해 가상 디스크 드라이브를 더 이상 사용할 이유가 없는 경우 마운트를 해지한다.

Ⅳ. 검 증

본 논문에서 제안한 프라이버시 데이터에 대한 보호 방안으로 가상 디스크 드라이브를 사용하는 방안을 제안하였다.

제안한 방안의 유효성을 검증하기 위해 다음 표와 같이 조사하였다.

표 2. 프라이버시 데이터 접근 여부

	일반사용자		MDM 관리자 보안관리자		스마트폰 사용자	
	일반 데이터	프라이버시 데이터	일반 데이터	프라이버시 데이터	일반 데이터	프라이버시 데이터
MDM 솔루션 미적용	O	O	O	O	O	O
MDM 솔루션 적용	X	X	O	O	O	O
제안 방안	X	X	O	X	O	O

위의 표에서 보는 바와 같이, MDM솔루션이 미 적용된 상태에서는 모든 사용자가 제한 없이 접근이 가능하며, MDM 솔루션이 적용된 경우 외부의 일반사용자가 일반데이터 및 프라이버시 데이터에 접근이 제한된다. 하지만, 제안방안은 일반사용자 및 MDM 관리자/보안관리자가 스마트폰 사용자가 설정한 프라이버시 데이터에 접근이 제한되고, 스마트폰 사용자만 프라이버시 데이터에 접근이 허용된다.

Ⅴ. 결 론

스마트폰이 등장하면서 음성통화뿐만 아니라, 사진, 전자메일, 주소록, 메모 등 다양한 서비스에 활용된다. 그러나, 스마트폰의 활용범위가 넓어지면서 개인의 프라이버시 데이터의 중요성이 더욱 증가하고 있다. 이에 일부 기업에서는 기업의 주요 데이터를 보호하기 위해 MDM 솔루션을 설치하여 운영한다. 하지만, MDM 솔루션이 설치된 경우 스마트폰 사용자가 공개를 원하지 않는 사생활 데이터에 대해서도 MDM 관리자/보안관리자가 제한 없이 접근이 가능하다.

따라서, 본 논문에서는 스마트폰 프라이버시 보호를 위해 가상 디스크 드라이브에 저장되어있는 자료를 보호하고, 프라이버시 데이터에 접근 시 매번 입력하지 않고 인증할 수 있는 방안을 제시하였다. 또한, 스마트폰 분실에 따른 프라이버시 데이터 유출을 방지하는데 활용 될 수 있을 것이다.

마지막으로 MDM 솔루션에서 회사관련 자료가 프라이버시로 인식되어 보안영역에 저장되었을 경우 관리자가 프라이버시 데이터 접근 없이 회사관련 데이터를 확인할 수 있는 방법이 모색되어야 하며, 스마트폰에서 가상 디스크의 효율적인 성능에 대한 연구가 필요하다.

참 고 문 헌

[1] 조인준, *모바일 단말 관리 솔루션 및 스마트폰 APP개발 플랫폼 BMT평가모델 개발*, 연구보고서, 2011.

[2] 이선호, 이임영, “모바일 플랫폼에서 MTM을 이용한 보안영역 제공 및 인증에 관한 연구”, 정보처리학회지, 2011.

[3] 김형중, “스마트폰 프라이버시 논쟁”, 통신연합, 제1권, 제54호, pp55-56, 2010.

[4] 박현아, 최재탁, 임종인, 이동훈, “모바일환경에서의 개인정보 위협 분석 연구”, 정보보호학회, 제17권, 제4호, pp.56-73, 2007.

[5] 장태섭, “디스크 스토리지 가상화 기술의 이해”, 한국정보기술학회, 제7권, 제1호, pp.67-74, 2009.

[6] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”, 정보보호학회, 제19권, 제5호, pp.21-28, 2009.

[7] 강훈식, 김승주, “스마트폰 메신저 어플리케이션에서의 개인정보보호에 관한 연구”, 정보보호학회논문지, 제23권, 제1호, pp.97-107, 2013.
[8] 전두현, 천지영, 정익래, “소셜 네트워크에 적합한 효율적인 프라이버시 보호 데이터 공유 기법”, 정보보호학회논문지, 제22권, 제3호, pp.447-461, 2012.
[9] 강영복, 황현욱, 김기범, 이경호, 김민수, 노봉남, “디스크 암호화 키의 효율적인 탐색을 위한 커널 메모리 수집 방법”, 정보보호학회논문지, 제23권, 제5호, pp.931-938, 2013.
[10] 이종만, 박종학, “스마트폰 사용이 성과에 미치는 영향”, 한국콘텐츠학회논문지, 제2권, 제1호, pp.296-300, 2004.
[11] 이원구, 이재광, “모바일 인터넷 상의 보안 기법 연구”, 한국콘텐츠학회논문지, 제2권, 제1호, pp.296-300, 2004.
[12] 최승권, 김송영, 신동화, 이병록, 조용환, “전달 계층의 보안 암호화 알고리즘 개선”, 한국콘텐츠학회논문지, 제3권, 제1호, pp.107-111, 2005.
[13] J. M. Kang, H. T. Ju, M. J. Choi, James W. K. Hong, and J. G. Kim, “OMA DM-based remote software fault management for mobile devices,” International Journal of Network Management (IJNM), Vol.19, No.6, pp.491-511, 2009.
[14] *표준국어대사전*, 국립국어원
[15] http://money.joins.com/news/article/article.asp?total_id=7744376&ctg=16
[16] “개인정보 보호법” 1장, 2조1항.
[17] http://en.wikipedia.org/wiki/Disk_image
[18] http://en.wikipedia.org/wiki/Keychain_(Apple)

저 자 소 개

신 숙 조(Suk-Jo Shin) 정회원

- 2008년 2월 : 배재대학교 컴퓨터공학과(공학사)
- 2010년 2월 : 배재대학교 컴퓨터공학과(공학석사)
- 2013년 3월 ~ 현재 : 배재대학교 컴퓨터공학과(박사과정)

<관심분야> : 모바일 보안, 컴퓨터 네트워크

김 선 주(Sun-Joo Kim) 정회원

- 1999년 2월 : 배재대학교 컴퓨터공학과(공학사)
- 2001년 2월 : 배재대학교 컴퓨터공학과(공학석사)
- 2013년 2월 : 배재대학교 컴퓨터공학과(공학박사)

<관심분야> : 모바일 보안, 컴퓨터 네트워크

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과(공학사)
- 1985년 2월 : 전남대학교 전자계산학과(공학석사)
- 1999년 2월 : 아주대학교 컴퓨터공학과(공학박사)
- 1983년 ~ 1994년 : 한국전자통신연구원 선임연구원
- 1994년 ~ 현재 : 배재대학교 컴퓨터공학과 교수

<관심분야> : 정보보호, 컴퓨터 네트워크, 전산조직응용