MDM과 위치정보를 활용한 모바일 오피스 보안 시스템 설계

박민규*, 박석천**
*가천대학교 일반대학원 모바일소프트웨어학과
**가천대학교 컴퓨터공학과 정교수(교신저자)
e-mail : sodemingu@naver.com

Design of Mobile Office Security System using MDM System and Location Based Information

Min-Gyu Park*, Seok-Cheon Park**
*Dept of Mobile Software, Gachon University
**Dept of Computer Engineering, Gachon University

요 약

현대 사회는 모바일 장치와 통신기술의 발달로 장소와 상관없이 자유롭게 네트워크에 접속할 수 있게 되었다. 모바일 디바이스 사용자의 폭발적인 증가는 이동성이 보장된 모바일 오피스 환경 구현을 가속화시키고 있으며 개인의 모바일 기기를 업무에 사용하는 경향도 두드러지고 있다. 개인소유 디바이스를 통해 기업 네트워크에 접속하는 횟수가 늘어나면서 기기를 통해 중요한 데이터의 분실이나 유출과 같은 보안 문제를 해결하려는 연구들이 발표되었다. 이와 같은 보안 문제 해결 방안으로 통합적으로 이동 단말을 관리하는 MDM(Mobile Device Management) 시스템 도입이 전망되고 있다. 하지만 아직 MDM 시스템에 대한 위협, 보안에 대한 연구가 미흡하다. 이에 본 논문에서는 보안강화와 효율적인 MDM 시스템 사용을 위해 MDM 시스템을 기반으로 위치정보를 활용하여 모바일 오피스 보안 시스템을 설계하였다.

Ⅰ. 서 론

현대 사회는 모바일 장치와 통신기술의 발달로 언제 어디서나 사용자가 컴퓨터나 네트워크를 의식하지 않고 장소와 상관없이 자유롭게 네트워크에 접속할 수 있게 되었다. 우리나라 4,500만 명중 휴대폰 가입자의 수가 4000만 명에 육박하는 것은 모바일 환경으로의 전환을 보여주고 있다. 이처럼 모바일 디바이스 사용자가 폭발적으로 증가하면서 기업에서도 이동성이 보장된 모바일 오피스 환경 구현이 가속화되고 있는 가운데 다양한 개인의 모바일 기기를 업무에 사용하는 경향도 두드러지고 있다.

이른바 BYOD(Bring Your Device)현상이다. 이에 따라 기업들이 이동 단말 관리시스템을 개발하고 도입하는 사례 역시 증가하고 있다. 이것은 직원들이 단말을 분실 또는 도난당하거나 잘못 사용하더라도 기업의 기밀정보가 유출되지 않도록 하기 위해서 기업이 이동 단말 관리시스템을 이용하여 직원의 이동 단말의 상태를 감시하고 기능을 제어하고자하기 때문이다.

MDM 시스템은 모바일 기기 정책을 실행하는 방법 중 하나이다. MDM은 무선 데이터 통신 기술을 이용하여 원격으로 이동 단말의 상태를 조사하고 이동 단말을 제어하며, 필요한 업무 자원을 지원하는 등 통합적으로 이동 단말을 관리하는 시스템이다. 비록 MDM 시스템 시장이 빠르게 확대되고 있지만, 아직 MDM 시스템의 보안에 관한 연구는 심도 있게 이루어지지 않았다. 이것은 MDM 시스템이 새로운 기술로서 MDM 시스템에 대한 위협, 보안 요구사항 등에 대한 연구가 부족하기 때문이다[1][2]. 따라서, 본 논문에서는 MDM과 위치정보를 활용하여 강화된 모바일 오피스 보안 시스템을 설계한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 설계하는 시스템에 대한 이해를 돕기 위한 관련 연구를 소개하고, 3장에서는 모바일 오피스 환경에서 필요로 하게 되는 보안요구사항에 대해 설명한다. 4장에서는 MDM과 위치정보를 활용한 모바일 오피스 보안 시스템을 설계하며, 마지막으로 5장에서는 결론 및 향후 연구방향을 제시한다.

Ⅱ. 관 련 연 구

2.1 모바일 디바이스 관리 (MDM)

MDM은 휴대폰 무선전송기술(OTA)을 이용하여 언제 어디서나 모바일 디바이스가 네트워크에 연결되어 있으면 원격에서 모바일 기기를 관리할 수 있는 시스템을 지칭한다. MDM은 2007년말 국내 모 이동 통신사에서 '원격 휴대폰 관리 서비스'라는 이름으로 일반인 대상의 서비스를 제공하기 시작했으며, 해외의 경우에는 그 이전부터 다양한 형태의 모바일 디바이스에 대한 관리시스템이 주목 받아오고 있다. MDM의 원래 사용 목적은 원격에서 휴대폰

등 모바일 기기의 어플리케이션 배포, 데이터 및 환경설정 변경, 모바일 분실 및 장치 관리들을 통합적으로 관리해 주는 시스템으로 짧은 서비스 다운타임과 최소의 비용으로 모바일 보안과 기능을 최적화 시켜주는 시스템이었으나 최근 보안 위협에 대한 강화 대책으로 관리의 필요성이 대두되면서 모바일 보안의 핵심요소가 되고 있다[1].

MDM의 주요 기능은 대략 다섯 가지로 분류할 수 있다. 첫째, 업무 프로세스 수행 시 또는 특정 위치 출입 시 카메라, 무선랜, 블루투스 등의 I/O 포트 및 외장 메모리를 원격 제어하여 기업 내 중요정보 또는 데이터의 유출을 방지할 수 있다. 둘째, 모바일 디바이스에 일정 시간 동안 사용자의 입력이 없을 경우, 화면 잠금 기능이 작동하여 디바이스의 무단 사용을 방지할 수 있다. 셋째, 모바일 디바이스 도난 도는 분실 시 관리자에 의해 원격으로 해당 디바이스를 초기화 상태로 제어할 수 있으며, 외장 메모리 카드에 저장된 데이터에 대해서도 원격 삭제가 가능하여 기업 내 중요 정보 또는 개인정보의 유출을 방지할 수 있다. 넷째, 디바이스의 프로세스를 모니터링 하여 업무 프로세스를 실행 중인 경우 다른 프로세스를 제한할 수 있다. 마지막으로 업무용 S/W 또는 애플리케이션을 OTA를 통해 해당 디바이스에 일괄 자동 배포가능하며 원격으로 최신 버전으로 업데이트를 시키는 기능을 제공한다[3].

MDM의 각 구성 요소는 MDM은 게이트웨이 서버, 모바일 관리서버, MDM 등록서버, MDM 에이전트 등 4개로 구성되며 MDM에 대한 설명은 표 1과 같다.

<표 1> MDM 구성 요소

구성요소	설명
게이트웨이 서버	사내 네트워크의 모바일 관리서버와 모바일 기기 간의 통신 연결 및 인증 암호화/모바일 VPN 인증서 기반의 사용자 인증 및 통신 암호화
모바일 관리 서버	모바일 디바이스 관리 운영, 보안 정책 및 소프트웨어 배포 기능
MDM 등록 서버	모바일 디바이스 등록/승인/변경/회수 처리 및 보안 소프트웨어 배포 및 설치, 분실/도난시 원격 정보 삭제기기 모니터링, 사용자 모바일 VPN 지원
MDM 에이전트	모바일 기기 내부에 에이전트가 설치되어 MDM 서버와 통신

2.2 위치기반 서비스

위치기반 서비스는 무선 인터넷 사용자에게 사용자의 변경되는 위치에 따르는 특정 정보를 제공하는 무선 콘텐츠 서비스들을 지칭한다. 위치기반 서비스는 이동성과 휴대성을 특징으로 하는 휴대폰의 특성 때문에 이동통신의 시작과 더불어 항상 킬러앱의 하나로 전망되어 왔다. 스마트폰 이전의 피처폰에서는 플랫폼 상에서의 기술 지원 부족, 애플리케이션 개발을 위한 기술의 개방성 부족, 위치기반 서비스를 위한 제반 인프라 지원 부족 등의 여러 이유로 서비스의 활성화를 가져오지는 못했으며 언제나 성공 가능한 서비스의 하나로 인식되어 왔다. 그러나 스마트폰의 폭발적인 성장은 위치기반 서비스를 시장의 전면에 등장하게 했다. 아이폰과 안드로이드에서는 GPS, WLAN, 디지털 컴퍼스 등의 하드웨어적인 지원, 위치 기반서비스를 위한 다양한 기술 및 API, Database 제공 등을 통해 위치기반 서비스 활성화를 위한 토대를 마련했다[4].

위치정보는 기본적으로 무선 단말에 내장된 GPS칩을 통해 측정할 수 있다. 이 경우 무선 단말은 복수 GPS 위성으로부터의 신호를 수신하고 신호로부터 위치 좌표를 계산하는 측위 기능 전체를 직접 담당하며 이동통신망을 통해 그 좌표를 입력값으로 각종 정보를 조회할 수 있다. 그러나 모바일 디바이스는 저전력 및 낮은 계산 성능 문제로 위성신호 수신과 좌표 계산 기능을 직접 수행하는 데에 어려움이 있다. 이에 따라 GPS 신호를 보조적으로 이용하고 인접 이동통신 기지국의 거리 관계 및 전파 상태 측정값을 추가하여 복합적으로 위치좌표를 계산하는 혼합 측위 방식이 다양하게 고안되어 왔으며 이를 일반적으로 A-GPS(Assisted GPS)라고 지칭한다.

위치 측정값의 정확도는 GPS 및 그에 준하는 위성 기반 위치 측정 방법이 가장 높으며 기지국 기반 방식은 위경도 좌표가 아닌 지역 구분만을 측정할 수 있으므로 정확도가 가장 낮다. 현재의 이동 통신망에는 위치 측위 성능이 서로 다른 다양한 단말이 보급되어 있기 때문에 GPS, A-GPS 방식이나 기지국 기반 방식을 혼용하여 위치 기반 서비스를 제공한다[5].

III. 모바일 오피스 보안 시스템 설계

3.1 위치정보와 MDM을 활용한 보안 시스템

MDM 시스템을 기반으로 위치 기반 서비스와 연동하여 기업의 모바일 보안성을 확보할 수 있다. 모바일 디바이스의 원격 잠금을 통해 사용을 제한할 수 있으며, 데이터 및 애플리케이션 삭제 등 초기화를 통해 디바이스 분실에 대한 대응이 가능하다. 디바이스 I/O 통제를 통해서는 스마트폰의 카메라 잠금 및 USB 포트 연결, 블루투스, 테더링 등 네트워크 사용을 제어할 수 있다. 또한 모바일 오피스를 통한 사내 메일 보기, 메일 첨부파일 보기, 메일 보관 기간 등의 기능 제어를 통해 기업의 중요 콘텐츠를 보호할 수 있으며 회사 외부에서는 위치 정보를 이용해서 중요문서에 대한 열람 기록과 함께 위치 정보를 로그로 남김으로써 회사의 기밀문서에 대한 관리를 효율적으로

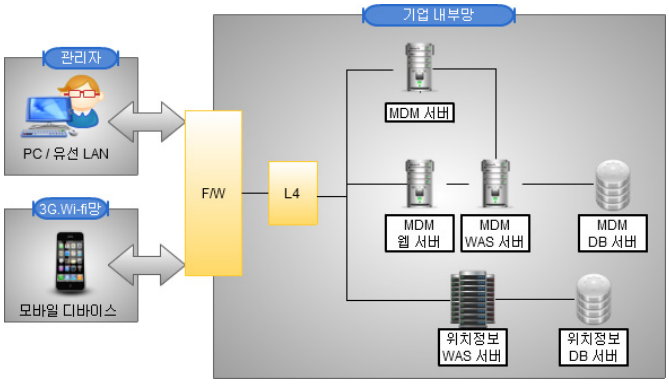
할 수 있으며, 위치 정보를 이용해서 MDM 시스템의 문서 열람 보안 등급을 유연하게 조정할 수 있다.

3.2 모바일 오피스 보안 시스템 전체 구성

본 논문에서 제안하는 보안 시스템의 전체 구성은 그림 1과 같이 모바일 보안 서버를 통해서 회사에 들어오게 되면 카메라, 블루투스, 이동식 저장장치 기능을 차단하며 회사 밖으로 나오게 되면 중요 문서 열람 시 위치정보를 모바일 보안 서버로 전송하여 문서 열람기록과 함께 저장함으로써 중요문서 열람에 관한 데이터 관리를 용이하게 한다. 또한, 회사 밖에서 자주 중요 문서 열람을 해야 하는 다른 위치를 사전에 서버에 등록하여 인증 절차를 유연하게 변경할 수 있다.

(그림 1) 시스템 전체 개요도

구축하는 보안 시스템의 H/W는 그림 2와 같이 MDM 서버, MDM 웹/WAS 서버, MDM 서버, 위치정보 WAS 서버, 위치정보 DB 서버로 구성된다.



(그림 2) 보안 시스템 구성도

보안 시스템의 각 서비스 별 구성 및 서버의 기능과 역할은 아래 표 2와 같다.

<표 2> MDM 구성 요소

서버	기능	설명
MDM 서버	디바이스 인증 및 통제 원격 관리	- 단말에 대한 정책을 그룹별로 관리 가능 - 필요시 OTC를 통하여 단말을 원격 통제 - 단말의 정책 적용 결과를 DB에 반영
MDM 웹 서버	단말에서 MDM 서버로 접속을 위한 연계 서버	- 단말에서 MDM 서버로 접속하기 위한 웹 서버 - 외부 인터넷에서 접속을 위해 DMZ존에 위치
MDM DB 서버	MDM 데이터 관리	- MDM 서버에서 사용하는 데이터를 관리
위치정보 WAS 서버	디바이스의 위치정보를 받는 서버	- 중요 문서 열람 시 디바이스의 위치정보를 받아옴
위치정보 DB 서버	위치정보 데이터 관리	- 열람 인증 절차를 위한 위치정보와 중요문서 열람 시 위치정보 데이터 관리

3.3 보안 시스템 흐름 구성

사용자가 회사에 사원증을 태깅하고 게이트를 통과해 사업장 내부로 입문하게 될 경우 입문 정보가 MDM 서버로 전송되고 기록 된다. MDM 서버에서는 사전에 설정된 사내 모바일 보안 통제 정책에 따라 사용자의 모바일 디바이스의 카메라, 블루투스 이동식 저장장치 기능을 차단한다. 사용자가 출구 게이트를 통과해 회사 밖으로 나오게 될 경우 출문 정보를 MDM 서버로 전송하며 디바이스에 차단되어 있던 기능을 해제한다.

회사 밖에서 회사 네트워크에 접속하여 문서열람 시 사용자의 위치정보를 위치정보 서버로 받아온다. 위치정보 DB 서버에 저장되어 있는 위치정보 데이터와 비교하여 문서열람 승인 절차를 조정한다. 중요문서 열람 시 인증절차를 걸쳐 문서를 열람하게 되며 이때 열람한 문서의 정보와 위치정보가 데이터베이스에 저장된다.

사용자의 회사업무를 위해 사용되었던 모바일 디바이스를 분실하였을 경우 MDM 서버에서 분실된 모바일 디바이스를 잠금 상태로 만들며 I/O 기능을 차단하여 사용자가 패스워드를 입력해도 잠금이 해제되지 않도록 제어한다. 분실된 상태가 일정 시간 이상 지속되면 디바이스를

초기화 하여 기업 내 중요정보 또는 개인정보의 유출되지 않도록 한다.

Ⅳ. 결 론

오늘날 모바일 디바이스 사용자의 증가는 모바일 오피스 환경 구현을 가속화시키고 있으며 개인의 모바일 기기를 업무에 사용하는 경향도 두드러지고 있다. 개인 소유 디바이스를 통해 기업 네트워크에 접속하는 횟수가 늘어나면서 중요한 데이터의 분실이나 유출 문제와 같은 보안 문제를 해결하기 위해 MDM이 도입되고 있다. 하지만 MDM 시스템에 대한 위협, 보안에 대한 연구가 부족하며 디바이스 관리적인 측면에서의 보안만을 가진다는 단점이 있다.

따라서 본 논문에서는 위치정보를 활용하여 디바이스 관리적인 측면과 회사 밖에서 효율적인 보안 관리를 위한 모바일 오피스 보안 시스템을 설계하였다. 중요문서의 경우 열람 시 위치정보를 함께 기록함으로써 중요문서 관리를 좀 더 체계적으로 할 수 있는 환경을 제공 한다 또한, 중요문서를 자주 열람하게 되는 회사 밖에 위치한 공간에 대한 정보를 미리 서버에 등록시킴으로써 문서 열람 인증 절차의 효율적 관리를 할 수 있도록 하였다.

향후 연구로는 중요 문서 열람 시 위치 정보를 활용한 인증 시스템을 구현함으로써 하나의 보안 시스템으로 사내와 사외 보안을 함께 제어할 수 있도록 연구를 진행 할 계획이다.

Ⅴ. 시사의 글

본 연구는 2013년도 지식경제부의 SW전문인력양성사업의 재원으로 정보통신산업진흥원의 고용계약형 SW석사과정 지원사업(HB301-13-1003)으로부터 지원받아 수행되었습니다.

참고문헌

[1] 한송훈, “MDM과 출입 시스템을 연계한 모바일 보안 시스템 구축 사례 연구”, 2012
[2] 홍종욱 “모바일 오피스 환경에서 위치와 시간정보를 이용한 강화된 인증 방법”, 2012
[3] 윤상인 “스마트워크 시대 필수 솔루션 MDM”, 2011
[4] 정구민, 최완식 “스마트폰 위치기반 서비스(LBS) 기술 동향”, 2012
[5] http://en.wikipedia.org/wiki/Location-based_service
[6] NIPA, “2013년 주요 IT 트렌드 전망”, 2013
[7] 윤상인, “스마트워크 시대 필수 솔루션 ‘MDM’” 2012