모바일 단말을 통한 내부 정보 유출 방지 방안 연구

김진형, 김지연, 장은영, 김형종
서울여자대학교 컴퓨터학과
e-mail:{jinny, jykim07, yadury, hkim}@swu.ac.kr*

A Study of Prevention Measures about the Internal Information Leakage through Mobile Devices

Jinhyung Kim, Hyung-jong Kim
Dept. of Computer Science & Engineering, Seoul Women's University

요 약

최근 다양한 기능을 수행할 수 있는 모바일 단말 개발이 확산됨과 함께 모바일 단말기를 이용해 회사 업무를 처리 할 수 있는 모바일 오피스를 구축하는 기업이 빠르게 증가 하고 있다. 모바일 오피스에 사용되는 단말기에는 회사 업무 처리가 가능한 업무 시스템 및 업무 기능을 포함하는 앱스(Apps)가 설치 되어있으며, 이를 통해 외부에서 네트워크를 통해 업무를 수행하게 된다. 다양한 단말을 통한 내부 시스템의 접속 및 외부에서부터 기업 내부 망으로 접속하는 것을 허용하게 됨에 따라 내부정보 유출 시스템의 적용 범위를 모바일 단말 사용자에게 확대할 필요가 생겼다. 효율적인 업무 운영이 가능하면서, 안전하게 수행 가능한 모바일 오피스 운영을 위해 직원의 프라이버시 보호가 가능하면서 내부 정보 유출을 방지할 수 있는 방안에 대해 연구 해 보고자 한다.

1. 서론

최근 단말기 개발 기술의 발달과 함께 모바일 단말기를 이용해 회사 업무를 처리 할 수 있는 모바일 오피스를 구축하는 기업이 증가 하고 있다. 모바일 오피스(Mobile Office)란, 언제 어디서나 모바일 단말기를 통해 외부에서도 회사 업무를 처리할 수 있는 업무 시스템이라고 정의할 수 있다.[1] 업무 처리에 있어 시간 및 공간적 제약 문제를 해결 할 수 있도록 해 준다는 장점으로 인해 모바일 오피스를 구축하는 관공서 및 기업은 급속도로 증가하고 있다.

그러나, 다양한 단말을 통한 내부 시스템의 접속 및 외부에서부터 기업 내부 망으로 접속하는 것을 허용하게 됨에 따라 발생 가능한 보안 위협이 증가 하게 되었다. 이에 기업은 모바일 오피스에 접속하는 단말을 이용한 내부 정보의 유출로 인한 자산의 위협에 대한 대비가 필요하게 되었고, 강력한 내부정보유출 방지 시스템을 운영한다. 그러나 이러한 과정에서 개인 소유의 단말에 존재하는 프라이버시 정보에 임의로 접근 하게 되는 등, 직원의 프라이버시를 보호할 수 없게 되어, 이를 반영한 시스템 설계의 필요성이 생겼다. 본 논문에서는 모바일 오피스에서 사용하는 모바일 단말을 통한 내부 정보 유출 방지 시스템에 대한 연구를 수행한다. 다만, 모바일 단말을 이용한 내부 정보유출을 방지하기 위한 시스템에서의 사용자의 프라이버시 정보를 보호할 수 있는 방안을 고려하는 것이 매우 중요하며, 본 논문에서 제안하는 시스템은 이를 반영하였다.

2장에서는 모바일 오피스를 정의하고 모바일 오피스에서의 내부 정보 유출에 대해 알아보고, 프라이버시 보호와 내부 정보 유출 방지와의 관계에 대해 정리한다. 3장에서는 모바일 오피스에서의 내부 정보 유출 방지 및 프라이버시 보호를 반영한 내부 정보 유출 방지 시스템을 설계해 본다. 4장에서는 결론 및 향후 연구 방향에 대해 정리한다.

* 이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (2009-0068361)

2. 모바일 오피스에서의 내부 정보 유출

본 장에서는 모바일 오피스에서의 내부 정보 유출이 발생할 수 있는 가능성을 확인 해 보고자하며, 이와 관련된 모바일 오피스의 정의 및 내부 정보 유출의 위협에 대해 정리 해 본다.

2.1 모바일 오피스

모바일 오피스란, 시간과 공간의 제약 없이 모바일 단말기를 통해 외부에서도 회사 업무를 처리할 수 있는 시스템이라고 정의할 수 있다. 현대 사회는 출장, 외근 및 재택근무 등의 외부에서 업무를 수행하는 경우가 많아지면서, 외부에서도 업무를 처리가 가능하도록 하는 시스템의 필요성이 생겼다. 단말 기술의 발달로, 스마트폰, 태블릿

PC와 같은 이동통신 기기를 통해 사내 컴퓨터 네트워크에 접속함으로써 외부에서 회사 업무를 처리 할 수 있게 되었다. 모바일 오피스를 도입하면서 이동 중에도 실시간으로 업무를 파악하고, 처리 할 수 있도록 하여 직원들의 업무 효율성을 높일 수 있고, 재택근무 등의 다양한 근무 형태가 원활하게 운영 될 수 있다. 또한, 이동시간과 출퇴근 시간 및 공간 등에 필요한 경비를 절약하는 경제적인 효과도 기대할 수 있게 되어 최근 정부 및 대기업에서부터 중소기업 까지 모바일 오피스를 도입하고 구축하여 운영하고 있다. 모바일 오피스는 스마트폰과 같은 모바일 단말기와 업무관련 기능을 수행할 수 있는 솔루션을 포함하고 있는 앱스(Apps) 및 이동통신망과 모바일 플랫폼으로 구성한다. 이러한 구성요소를 통해 모바일 오피스에서는 일반적으로 그룹웨어 형식의 결재, 회계처리와 같은 기업의 일반 업무 서비스를 제공하며, 원격으로의 관리 및 음성통화 서비스를 제공한다.

2.2 모바일 오피스에서의 내부 정보 유출 위협[2]

모바일 단말을 통한 모바일 오피스를 구축하여 운영하고자 할 경우, 단말의 위협 및 무선 구간의 위협으로 인한 내부 정보 유출 위협을 고려하여야 한다. 기존의 내부 업무 처리 시스템에서는 내부 정보 유출을 막기 위해 인트라넷에서 외부로 나가는 패킷 등의 내용을 차단하거나 삭제 하는 방안으로 외부로의 유출을 막는 방법을 적용할 수 있었으나, 모바일 오피스의 경우, 접속 자체가 외부에서 내부로 이루어지는 것으로, 권한 자에 한해 내부 정보에 접근 하고, 인증된 단말에 한해 내부 정보를 저장할 수 있도록 권한 관리를 수행하게 된다. 그러나 이러한 관리가 제대로 되지 않는다거나, 단말 분실 등의 이유로 타인에 의해 단말을 통한 접속이 이루어질 경우, 내부 정보의 유출에 대한 위험은 높아지게 되며, 이러한 위협은 기업의 자산 보호를 위협하게 된다.

2.3 내부 정보 유출 방지와 프라이버시

기업은 자산의 보호를 위해 정보 유출 방지 솔루션을 구입하여 기업 내 네트워크 시스템을 통해 운영한다. 이는 네트워크 패킷 등을 통해 기업 내 행위의 주체, 행위 내용 등의 정보를 확인 하여, 이상 행동이 있는 경우 자산 보호를 위해 외부로의 패킷이 전달되는 것을 차단하거나, 관련 데이터를 삭제 하는 등의 조치를 수행 하는 시스템이다. 그러나 이러한 과정에서 직원의 개인정보를 무분별하게 확인 하게 되어 직원의 프라이버시 침해가 발생하게 된다. 또한 모바일 오피스가 확산 되면서 기업 내부에 접속하는 사용자는 개인 소유의 모바일 단말을 사용하여 내부 뿐 아니라 외부에서 접속이 가능하게 되었다. 이에 모바일 단말을 통한 내부 정보 유출 방지 방안이 구현 되어야 하며, 이때 직원의 프라이버시 보호 방안은 반드시 반영 되어야 한다.

3. 프라이버시를 고려한 내부 정보유출 방지를 단말에 적용하기 위한 방안 연구

3.1 모바일 오피스에서의 보안 이슈

모바일 오피스를 구축하여 운영할 경우 모바일 단말에 대한 보안 이슈를 고려하지 않을 수 없다. 이러한 환경에서 모바일 오피스에 대한 보안 이슈는 표 1과 같이 단말 보안, 응용 프로그램 및 플랫폼 보안, 네트워크 및 서버 보안 이슈는 다음과 같이 정리 할 수 있다.

첫 번째 보안 이슈는 단말 보안이다. 단말기의 도난· 분실로 인해 개인정보 또는 업무 정보의 유출이 발생하거나 단말을 사용하여 기업 내부에 접속하여 내부 정보를 유출할 수 있게 된다. 두 번째는 단말과 서버에서 사용하는 응용 프로그램 및 플랫폼의 보안 이슈를 생각할 수 있다. 악성코드 감염 등으로 응용프로그램이 오작동 하게 되고, 이를 통한 내부 정보의 유출, 서버 사용 제한 등의 위협이 발생 가능하다. 또한 플랫폼의 보안을 약화시켜 시스템의 보안 수준을 변화 시킬 위협도 있다. 마지막으로 네트워크 및 서버 보안에 대한 생각을 해 보아야 한다. 서버와 단말간의 무선 네트워크와 같은 통신 구간에서 발생 하는 패킷 스니핑 또는 해킹 등의 방법으로 내부 시스템에 접속하여 발생 가능한 보안 위협이 존재 하게 되므로, 이에 대한 고려도 필요 하다.

<표 1> 모바일 오피스에서의 보안 이슈

보안 이슈	상세 내용
단말 보안	o 단말기의 도난 분실로 인한 단말기 내 데이터 소실 o 분실된 단말기를 사용한 내부 서버로의 불법 접속 및 내부 정보의 유출
응용프로그램 및 플랫폼 보안	o 단말기의 악성코드 감염 등의 허용되지 않은 데이터 삽입을 통해 내부 정보의 유출, 장치 이용 제한, 부정 과금 유발등의 위협 o 단말기 플랫폼 또는 펌웨어 변조에 따른 보안 기능 약화 위협
네트워크 및 서버 보안	o 무선 네트워크를 사용하는 단말과 서버간의 통신 과정에서 패킷 스니핑 또는 해킹 o 단말기의 내부 접속 권한을 획득하여 내부 정보유출

3.2 모바일 오피스에서의 보안 위협

본 장에서는 앞의 3.1장에서 알아본 모바일 오피스에서의 보안 이슈를 요인으로 하여 발생 가능한 모바일 보안 위협을 정리 해 보고자 한다. 모바일 오피스의 주요 특징인 언제 어디에서나 접속이 가능하며 누구나 콘텐츠 및 어플리케이션을 제작할 수 있다는 개방적인 특성에 따라 보안 위협이 발생 하게 된다. 모바일 오피스의 보안 위협을 정리 해 보면 다음 표 2와 같다.

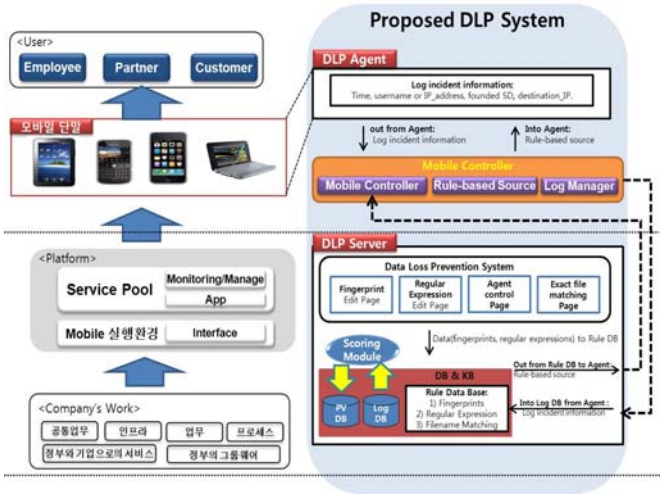
<표 2>모바일 오피스에서의 보안 위협

보안 위협	세부 사항
단말기 도난·분실	o이동형 단말로 도난 및 분실
단말기 악성코드 감염	o개방성 휴대성으로 인한 악성코드 감염
무선 구간 해킹	o단말과 서버간의 통신 과정에 사용되는 무선 구간의 해킹
단말기 플랫폼 변조	o플랫폼을 변조로 인한 단말 오작동
단말 경유 인트라넷 접속	o분실 등의 단말을 불법으로 획득한 권한이 없는 사용자가 사내 인트라넷에 접속
단말의 이동 저장매체화	o내부 정보에 접속하여 정보를 열람하는 것 뿐 아니라 단말에 저장하여 외부로 유출

위의 표 2에서 확인 가능한 보안 위협에 대한 대응책이 마련되지 않는다면, 모바일 오피스를 관공서에 적용 하였을 때, 국가보안에도 큰 위협이 발생 하게 되므로, 이에 대한 고려가 반드시 필요 하다.

3.3 프라이버시를 고려한 내부 정보유출 방지를 단말에 적용하기 위한 방안

본 장에서는 기존의 모바일 오피스의 구조에 적용 가능한 프라이버시 보호를 고려한 내부 정보유출 시스템 구조를 제안 해 본다.



(그림 1)모바일 단말에 적용 가능한 내부정보유출방지 시스템 구조

그림 1은 모바일 단말에 적용 가능한 내부 정보 유출 방지 시스템 구조이다. 기존의 [3]에서 제안한 프라이버시를 고려한 내부 정보 유출 방지 시스템 모델을 적용하였다. 모바일 오피스는 기업의 업무와, 이러한 업무가 기술적으로 가능하도록 하는 플랫폼, 사용자의 모바일 단말기기, 그리고 실제 사용하는 사용자로 구성된다. 이러한 구성요소 중 모바일 오피스에서 보안이 필요한 부분은 단말과 내부 업무를 연결 해 주는 플랫폼 부분에서 내부 정보 유출 방지 시스템을 운영할 수 있다. 기본적으로 내부 정보 유출 방지 시스템은 서버와 클라이언트 형태로 구성이 가능하며, 서버와 클라이언트 통신 과정에서 발생하는 패킷을 이용해 모니터링을 수행한다. 서버의 경우 플랫폼에 설치하여 운영하며, 클라이언트는 모바일 단말에 설치하여 운영하여야 한다.

위의 그림 1에서 하단의 DLP 서버는 플랫폼에 설치하여 운영하는 내부 정보 유출 방지 시스템의 서버 부분에 해당한다. 플랫폼으로 접속하는 단말이 요청하거나, 단말을 통해 유입되는 패킷의 모니터링을 수행하는 기능을 가지고 있으며, 프라이버시 보호를 위한 로그 분석 및 지식 베이스 기능을 보유하고 있다.

또한 상단의 DLP Agent는 클라이언트인 모바일 단말에 설치하여 운영한다. 기업 내부의 클라이언트에 설치하여 운영 가능한 모델과 달리, 모바일 단말의 경우 경량화 된 솔루션을 설치하여 운영하여야 하므로, Agent와 Server를 연결해주는 Mobile Controller를 설계 하여 추가 하였다. 본 모델에서 사용하는 Agent는 기존의 Agent에 포함 되어 있는 Rule-based Source부분을 제외 하고 모바일 단말에 설치하도록 하여, 경량화 된 Agent를 사용한다. 그리고 중요한 기능인 Rule-based Source 모듈을 Mobile Controller에 포함 시켜, 동일한 기능을 수행할 수 있도록 하였다.

설계한 Mobile Controller의 구성요소는 표 3과 같다.

<표 3> Mobile Controller 구성요소

	Module name	Description
1	Mobile Controller	모바일 단말의 접속을 관리 모듈 -보안 접속, 단말 인증 등
2	Rule-based Source	Reg, File matching 등의 기법을 적용할 수 있도록 관리 하는 모듈 -DB, XML, text File etc.
3	Log Manager	단말과 서버 사이에서 발생하는 Log 관리 모듈

첫 번째 구성 요소인 Mobile Controller는 DLP서버와 Agent간의 접속을 관리 해주는 역할을 담당하며, 보안 접속, 단말 인증 과정에서의 모니터링을 수행하게 된다. Rule-based Source는 Regular Expression, File Matching 등의 기법을 적용할 수 있도록 관리 하는 모듈이며, 경량화를 위해 기존 Agent에서 제외 한 모듈이다. Log Manager는 단말과 서버서 사이에서 발생하는 Log Data를 관리하는 모듈이며, 모바일 단말에서 발생하거나 요청한 패킷 로그 데이터를 수집하여 서버에 전달하는 기능을 가지고 있다.

4. 결론 및 향후 연구

기업의 효율적 운영을 위해 모바일 오피스 운영은 더 이상 선택이 아닌 필수가 되어가고 있다. 그러나 이러한 환경에서 사용되는 모바일 단말로 인해 내부 정보가 유출된다면 기업의 효율적 운영을 통해 자산의 손실이 발생하게 된다. 모바일 오피스를 운영하게 되면 단말을 통해 기업의 중요 문서, 전자 메일, 결재 시스템 등의 고유 시스템에 접속이 가능하게 되어 위협에 노출 될 가능성이 존재 하게 된다. 이러한 자산을 보호하기 위해 모바일 오피스에서의 보안은 필수 사항이다. 동시에 모바일 단말은 개인의 많은 정보를 포함하고 있으며, 이러한 프라이버시 보호 또한 중요한 문제이다. 본 논문에서는 모바일 오피스를 사용하는 사용자(직원)과 기업의 자산 보호를 위해 적용 가능한 내부 정보 유출 방지 시스템에 관한 연구를 진행 하였다.

본 논문에서 제시한 프라이버시를 고려한 내부 정보유출 방지 시스템을 모바일 오피스에서 사용하는 단말 영역으로 확장 하여 적용한다면, 편리하고 안전한 서비스를 제공하는 데 기여할 수 있다.

참고문헌

[1] 한국정보화진흥원, “스마트폰과 모바일 오피스의 보안 이슈 및 대응 전략”, 2010.10.25

[2] 백서: 보안 및 컴플라이언스, “ 내부자 위협 차단을 통한 IT리스크 감소”, 2011.01

[3] Jinhyung Kim, Hyung-jong Kim, “Design of Internal Information Leakage Detection System Considering the Privacy Violation”, ICTC2010, 2010.11