기업 정보유출 방지를 위한 가상화·클라우드 기반 BYOD 연구

배효빈*, 민재원*, 최영현*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신대학
e-mail:{hbbae, jwmin, yhchoi}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Study of BYOD Based on Virtualization·Cloud for Prevention of Enterprise Information Leakage

Hyo-Bin Bae*, Jae-Won Min*, Young-Hyun Choi*, Tae-Myoung Chung**
*Dept of Electrical and Computer Engineering, SungKyunKwan University
**College of Information and Communication Engineering, SungKyunKwan University

요 약

최근 개인소유의 모바일 디바이스를 이용해 기업의 정보에 접근할 수 있도록 하는 Bring Your Own Device(BYOD)가 기업의 생산성과 효율성을 높이는 IT혁신 전략으로 각광받고 있다. 하지만, 개인의 모바일 단말을 기업 업무에 이용하게 되면서 엄격한 통제가 불가능해졌다. 이로 인해 기업의 정보가 더욱 쉽게 유출될 수 있는 보안상의 문제점이 있다. 본 논문에서는 BYOD 상에서 보안문제를 해결하기 위해 단말 가상화와 클라우드 서비스를 혼합한 방식을 기반으로 한 접근제어, 인증, DRM 등에 대한 설명을 하고 활용방안을 제안한다.

1. 서론

최근 Bring Your Own Device(BYOD)가 기업의 생산성과 효율성을 높이는 IT혁신 전략으로 각광받고 있다. BYOD는 직원들이 개인 소유의 모바일 디바이스를 이용해 기업의 정보에 접근할 수 있도록 허용하는 정책을 의미한다[1]. 이런 BYOD는 모바일 시장의 폭발적인 성장과 무선 인프라의 확산, BYOD 정책 도입에 대한 직원들의 기대와 요구 그리고 실시간 커뮤니케이션과 업무 연속성이 중시되는 기업 환경으로 인해 빠르게 확산되어가고 있다[2].

BYOD를 도입하게 되면 기업들은 기기 구매 및 관리와 관련한 업무를 직원들에게 위임할 수 있게 된다. 업무에 쓰이는 기기를 기업이 아닌 직원들의 선택으로 구매하고, 기기에 대한 관리도 직원들이 맡아서 하게 된다. 또한 업무의 효율을 높일 수 있다. 우선, 개인용 모바일기기를 업무에 이용함으로서, 업무에 대한 사용자의 반응을 하루 종일 가속화 시킬 수 있다. 또한 익숙한 기기와 애플리케이션을 이용해 업무를 수행함으로서 업무시간단축을 가능하게 한다. 일례로 BYOD 개념을 처음 언급한 인텔의 경우 지난 해 임직원 9만 여 명에 대해 500만 시간을 절약하는 생산 효율을 거두었다[3].

하지만 업무에 쓰이는 모바일 디바이스가 직원 소유이기 때문에 기업의 디바이스와 비교해 엄격한 제재를 가할 수 없어 보안상 큰 결점을 갖게 된다. 대표적인 위협으로는 기업의 정보 통제권 상실, 단말의 도난 또는 분실로 인한 데이터 유출, 악성코드에 감염된 단말로 인한 데이터 유출 및 기업 네트워크 위협 등이 존재한다. 이런 보안 문제를 해결하기 위해 여러 가지 솔루션들이 제안되고, 활발하게 출시 중에 있다. 본 논문에서는 현재 BYOD 솔루션의 여러 접근방법에 대해 살펴보고, 더욱 안전하고 편리한 BYOD를 위한 여러 가지 기술들과 활용방안에 대해 제안한다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 BYOD 솔루션의 접근방식들에 대한 소개를 한다. 3장에서는 BYOD 시행 시의 여러 보안 위협으로부터 기업의 정보를 지키기 위한 기술들과 그 기술들을 적용하는 방법에 대해 제안한다. 이후 4장에서 제안한 방식에 대한 평가를 한 후 5장에서 결론을 맺는다.

2. 관련 연구

앞에서 살펴봤듯이 아무런 제재가 없는 BYOD 정책은 기업의 데이터 손실이나 악의적 위협을 야기한다. 이런 위협을 방지하기 위해 기업은 BYOD에 대해 어떤 정책을 사용할 것인가를 결정해야 한다. BYOD 솔루션은 크게 가상화를 이용하는 방식과 클라우드 서비스를 이용하는 방식으로 나뉜다. 2장에서는 이 두 가지 방식에 대해 살펴본다.

2.1 가상화를 통한 BYOD 환경 구축

가상화를 통해 구현한 BYOD는 가상화 툴을 이용해 두 개의 운영체제 인스턴스를 생성하여, 하나는 개인용으로, 다른 하나는 기업 업무용으로 구분하여 별개의 운영체제처럼 사용한다.

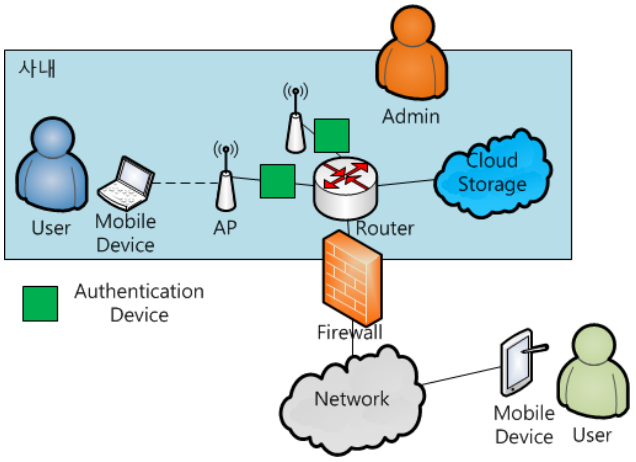
가상화를 이용하는 BYOD 솔루션은 VMware의 호라이즌 스위트[4], 삼성의 KNOX[5], 블랙베리 모바일 퓨전[6]등이 존재한다. 호라이즌 스위트는 데스크톱 가상화 솔루션, PC를 논리계층으로 분리하는 솔루션, 실무자나 그룹을 위한 가상공간 솔루션의 세 가지 파트로 구성된다. KNOX는 안드로이드 기기만을 지원하는 솔루션으로, 스마트 기기 내에 암호화된 '컨테이너'라는 별도의 공간을 만들어 업무용 데이터와 개인용 데이터를 분리해 관리한다. '컨테이너'는 샌드박스 같은 개념으로, 해킹, 바이러스, 정보 유출 등의 위협을 차단하는 기능을 가진다. 또한 Single Sign On(SSO)기능을 탑재하여 컨테이너 계정에 접속 시 내부 애플리케이션에 대한 별도의 로그인이 필요 없도록 해 사용자의 편의성을 높인다.

2.2 클라우드 서비스를 통한 BYOD 환경 구축

클라우드를 통해 BYOD를 구현하는 경우는, 기업의 정보를 개인의 단말이 아닌 클라우드 스토리지에 저장해 놓고, 단말에 클라우드 스토리지로 접근을 할 수 있는 애플리케이션을 설치하여 이용한다. 클라우드 스토리지를 이용한 BYOD 솔루션으로는 F5 네트웍스의 모바일 앱 매니저가 있다[7].

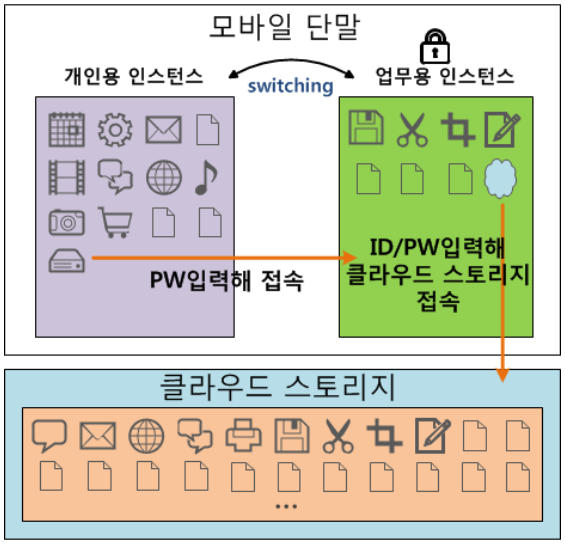
3. 본론

본 논문에서는 기업의 정보유출방지를 단말을 중심적 보호하는 방식이 아닌 정보를 중심적으로 보호하는 방식을 통해 구현하기 위해 가상화와 클라우드를 혼합하여 BYOD 환경을 구축하는 방법을 제안한다. 본 논문에서 제안하는 BYOD의 전체적인 네트워크는 그림1과 같다.



(그림 1) BYOD 네트워크

모바일 디바이스를 이용해 기업의 클라우드 스토리지에 접근하는 사용자는 크게 사내에서 접속한 사용자와 사외에서 접속한 사용자 두 부류로 나뉘게 된다. 사내에서 접속하는 경우에는 AP와 라우터 사이의 인증 장비(Authentication Device)에 의해 사내접속이라는 인증정보가 클라우드 스토리지로 전송된다. 또한 사용자의 단말정보나 클라우드 스토리지에 접근하는 사용자에 대한 정보를 모두 로그에 남겨 관리자가 모든 회사 정보에 대한 흐름을 쉽게 파악하고, 악의적 접근에 대해 신속한 조치를 취할 수 있도록 한다.



(그림 2) 시스템의 실행구조

그림 2는 본 논문에서 제안하는 시스템의 실행구조이다. 단말은 개인용과 업무용 가상 인스턴스로 나뉘어져 있으며, 업무용 인스턴스는 비밀번호 입력 이후 접근이 가능하다. 업무용 공간은 해킹, 바이러스 등으로부터 보호되는 공간이며, 여러 애플리케이션과 데이터를 저장할 수 있다. 업무용 가상 인스턴스에서는 클라우드 서비스 접속용 애플리케이션을 이용하여 기업 클라우드 스토리지에 접속할 수 있다.

3.1 분리된 개인/업무용 공간, 클라우드 서버

모바일 기기 내에서 가상화 애플리케이션에 의해 개인용 공간과 업무용 공간이 분리된다. 사용자는 단말의 업무용 공간에 자신의 손에 익은 애플리케이션들을 설치하여 업무효율을 높일 수 있다. 이런 애플리케이션은 네트워크 기능을 갖고 있지 않아야 하며, 네트워크 기능은 클라우드 서버 내에 설치된 애플리케이션이 담당한다. 그리고 업무용 공간에 존재하는 어떠한 정보도 개인용 공간으로 옮겨지거나 저장될 수 없다. 가상화된 업무용 공간에 접속 시에는 업무용 공간 접속용 비밀번호를 입력해야 하며, 업무용 공간 내의 정보들은 암호화되어 사용자 기기 내에 저장된다. 만일 잘못된 비밀번호를 통한 접속 시도가 일정 횟수 이상 진행되면, 사용자의 기타 개인 정보를 묻는 등 암호강도를 높인다. 그 이후에도 잘못된 접속 시도가 계속되면 기업 클라우드 서비스 접속용 애플리케이션, 기업 문서 등 해당 단말의 업무용 인스턴스 내에 저장된 모든 정보를 삭제해 기업 정보 유출을 막는다.

클라우드 스토리지에는 보안 등급에 따라 나뉜 여러 정보들과 애플리케이션이 저장되어 있다. 정당한 사용자 간의 커뮤니케이션을 돕는 애플리케이션, 클라우드 내에서 문서를 작성 또는 수정하기 위한 애플리케이션, 다른 사용자와 정보를 공유하기 위한 애플리케이션 등이 존재한다.

개인용 인스턴스가 가상화에 의해 업무용 인스턴스와

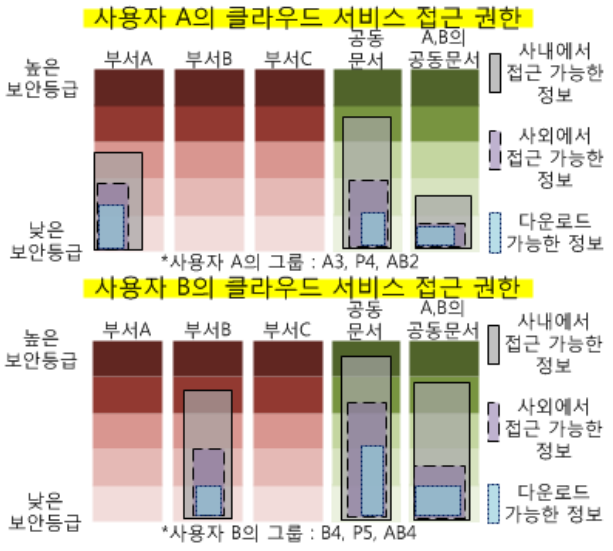
분리되어 있기 때문에 기업 정보 유출 방지를 위한 모든 정책들은 개인용 인스턴스에 적용되지 않는다. 이로 인해 사용자는 업무를 보지 않을 때는 기업의 디바이스 이용정책을 지키지 않아도 된다.

3.2 디바이스 관리

악의적 이용자가 정당한 사용자의 아이디와 비밀번호를 가로챌 수 있다면, 정당한 사용자의 단말을 훔치지 않더라도 자기 자신의 단말을 이용해 사내 클라우드 서비스에 접속하여 기업의 정보에 접근을 할 수 있다. 이런 경우를 방지하기 위해 사용자 단말의 정보를 서버에 등록한다. 사용자가 보내온 단말의 정보와 아이디의 정보를 비교하여 등록된 경우에만 접속을 허용한다. 또한, 일정 기간 사내 클라우드에 접속하지 않은 단말에 대해서는 권한을 없애는 방법으로 악의적인 접근을 막는다.

이를 위해서는 단말 고유의 식별자가 필요하다. 하지만 한정된 플랫폼이 아닌 다양한 플랫폼의 모바일 단말을 대상으로 서비스를 제공해야 하기 때문에, 기존에 존재하는 식별자가 아닌 새로운 고유 식별자(UUID; Universally Unique Identifier)를 만들어 이용한다. BYOD에 이용되는 단말은 스마트폰, 태블릿, 노트북이 존재하는데, 각각의 기기들도 서로 다른 OS를 이용해 각각의 식별자 포맷이 다르다. MAC은 네트워크를 이용하는 기기들이 모두 가지고 있으나, 쉽게 노출되고 변경할 수 있는 특성이 있어 적합하지 않다. 이런 이유로 기존의 식별자가 아닌 UUID를 만들어 이용한다. UUID는 애플리케이션이 설치되는 시점에 생성되며, 관리자에 의해 아이디와 한 쌍으로 묶여 클라우드 서버 내부의 인증 시스템에 저장된다.

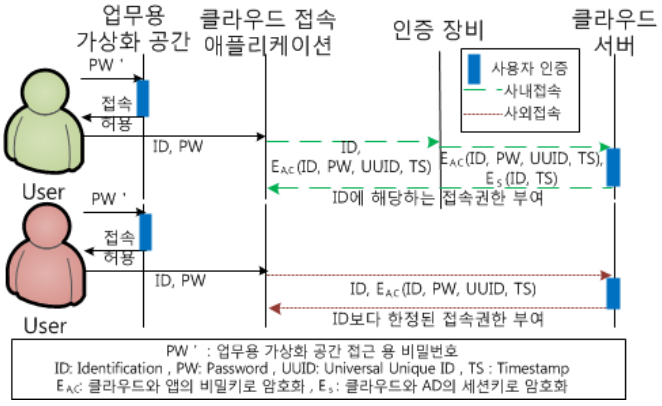
3.3 접근 제어



(그림 3) 직원이 가질 수 있는 정보의 권한 예시

정당한 사용자라고 해서 기업 내의 모든 정보에 접근할 수 있어서는 안 되고 자신의 직위, 업무에 해당하는 정보에만 접근 할 수 있어야 한다. 클라우드 스토리지에 저장된 정보는 부서별·보안등급 별로 구분되어 있으며, 각각의 사용자는 자신의 역할에 적합한 그룹에 속해 있다. 그룹은 특정 문서에 관한 최대 권한을 의미한다. 예를 들어 그림 3에서 사용자 A가 속한 그룹은 A3, P4, AB2이다. 부서A의 문서에는 레벨3, 공동문서에는 레벨4, A,B의 공동문서에는 레벨2가 A가 접근할 수 있는 최대 권한이라는 것을 의미한다. 하지만 그 레벨 내부의 모든 정보에 접근할 수 있는 것은 아니고 개인마다 설정된 권한이 있어 그에 속하는 정보에만 접근이 가능하다. 자신이 접근할 수 있는 정보 중에서도 일정 보안 등급이상의 정보는 단말에 다운로드 할 수 없어야 하며, 자신에게 권한이 없는 정보는 은닉되어 해당 정보가 존재한다는 사실조차 알 수 없어야 한다.

또한, 동일한 사용자라도 사내에서 회사 내부와 외부에서 사내 클라우드 스토리지에 접속하는 경우에 각각 다른 보안규정을 적용해야 한다. 정보유출을 막기 위해 여러 기술을 사용하더라도 사외에서는 사내에서에 비해 악의적인 정보유출을 손쉽게 할 수 있기 때문이다.



(그림 4) 접근제어 시퀀스 다이어그램

사용자가 사내와 사외, 어느 곳에서 접속했는지를 알아내기 위하여 사내 AP와 라우터 사이에 인증 장비를 설치해 이용한다. 인증 장비와 클라우드는 서로 신뢰관계에 있고, 동일한 관리자에 의해 관리 받기 때문에 해당 관리자에 의해 직접 공개키 암호 키 분배를 받는다. 실제 인증 과정에서는 이 공개키 암호를 이용해 분배한 세션 키를 이용한다. 세션 키는 기업에서 설정한 보안 강도에 따라 일정 시간마다 자동적으로 새로 생성된다.

그림 4와 같이 사내 사용자가 업무용 인스턴스에 대한 로그인을 한 후 클라우드 서버에 접속을 요구하면, 인증 장비는 사용자가 보내온 아이디와 자신이 인증한 시간(TS)을 클라우드와 공유하는 세션키로 암호화해 전송한다. 사외에서 클라우드 서버에 접근하는 경우에는 인증 장비를 거치지 않기 때문에, 모바일 단말에서 발신된 ID, $E_{A,C}$(ID, PW, UUID, TS)가 그대로 전송되게 된다.

접근제어는 단편일률 적으로 적용되어서는 안 되며 각 기업의 업무 환경, 보안이 필요한 정도, 기업문화 등 여러 요소 및 개별 사용자에 대한 정보들을 토대로 유연성 있는 정책을 만들어 시행해야 한다.

3.4 DRM(Digital Right Management)

중요한 기업의 정보가 모바일 단말이 아닌 클라우드

스토리지 내에 저장되어 있고, 권한을 가진 정당한 사용자만이 정보에 접근할 수 있다고 해서 모든 보안문제가 해결된 것은 아니다. 사실 기업의 기밀유출이 대부분 내부자의 소행이기 때문에[8], 권한을 가진 정당한 사용자의 정보 유출을 막기 위한 방법이 필요하다. DRM기술을 이용하여 이런 문제를 방지할 수 있다.

기업의 정보를 보호하기 위해 낮은 등급의 정보만을 모바일 단말에 저장하지만, 사실 낮은 등급으로 매겨진 정보라도 악의적 사용자에게는 좋은 정보가 될 수 있으며 높은 권한을 가진 사용자의 단말에는 높은 보안 등급의 정보가 저장되어 있을 수 있다. 이런 단말 내에 저장된 정보들이 유출된다면 기업은 큰 손해를 입을 수 있다. 또한 단말에 저장할 수 없는 등급의 정보도 복사나 캡쳐 기능을 통해 쉽게 유출 될 수 있다.

사용자 단말에서는 업무용 가상 인스턴스 내에서만 기업의 정보에 대한 접근이 가능하다. 그러므로 업무용 공간 내에서의 캡쳐 기능을 막아야 한다. 설령 캡쳐 기능을 막지 않는다고 해도 캡쳐된 결과물이 인스턴스 내부에 저장되도록 해야 한다. 그리고 업무용 인스턴스 내에서 복사한 내용을 해당 인스턴스 밖으로는 빼낼 수 없도록 만들어야 한다. 그리고 필요 시 일정시일이 지난 이후에 업무용 인스턴스에 저장된 정보가 자동적으로 삭제되는 기능을 추가한다.

3.5 로그 모니터링

관리자가 전체적인 정보에 대한 가시성을 갖기 위해 사용자들이 어떤 기기를 이용해 기업 내의 어떤 정보에 접근했고, 저장하거나 인쇄 했는지 또는 누구와 어떤 정보를 공유 했는지 등의 로그를 남겨야 한다. 또한 정보의 유출의 의심되는 경우에 로그분석을 통해 정보의 흐름을 추적할 수 있어야 한다.

4. 평가

4.1 정보의 보안

DRM은 복사 및 캡쳐 방지, 정보 저장의 유효기간을 두는 등 단말 내부에서 정보의 유출을 방지하는 기능을 제공한다. 그러나 DRM이 에러나 버그 없이 잘 동작하더라도, 사용자가 자신의 단말을 켜놓은 상태로 외부에서 사진을 찍거나 타이핑 하는 방식으로 데이터를 유출하는 것이 가능한 단점이 있다. 이런 단점을 접근제어를 통해 해결하였다. 단말 외부에서의 악의적 접근은 감시가 이루어지는 사내보다는 사외에서 일어날 가능성이 높다. 따라서 사외 환경에서 접근할 수 있는 데이터의 레벨을 낮춰 악의적 유출의 가능성을 낮추었다. 또한 사내인지 사외인지를 인증하는 과정에서도 무작위 공격에 대비하여 클라우드 서버와 인증장비 사이의 인증에 세션 키를 이용한다.

4.2 관리자의 가시성

사용자와 디바이스의 접속 및 행동에 대한 로그를 클라우드 서버에 남김으로서 관리자가 전체적인 데이터의 흐름을 손쉽게 파악할 수 있다.

4.3 사용자의 자유도

모바일 단말이 사용자의 소유물이기 때문에 기업 정보에 접근하지 않는 경우에는 사용자의 완전한 자유를 보장한다. 기업 정보에 접근하기 위해서는 가상화에 의한 업무용 인스턴스로 진입해야 하며, 이 공간 내에서만 기업의 규율을 따르면 된다. 또한 기업용 업무 소프트웨어에 대해서도 사용자의 편의를 위해 사용자가 원하는 애플리케이션을 업무용 인스턴스에 다운받아 사용할 수 있도록 했다.

5. 결론

업무 효율 증진과 기기에 대한 관리위임 등 여러 이점으로 인해 BYOD 정책이 주목받고 있다. 하지만 개인의 단말에 엄격한 규제를 가할 수 없어서 보안문제점이 생겨날 수 있다. 따라서 어떻게 보안 문제를 해결할지에 대한 많은 논의가 이루어지고 있다. 본 논문에서는 단말 가상화와 서버 클라우드를 혼합한 환경에서 기업의 정보를 안전하게 지키기 위한 기술들과 그 적용 방법에 대해 제안했고 그 유용성을 분석했다. 향후에도 연구가 지속적으로 이루어져 보다 더 안전한 BYOD가 업무에 적용되기를 기대한다.

ACKNOWLEDGEMENT

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)[10041244, 스마트TV 2.0 소프트웨어 플랫폼]의 일환으로 수행하였음.

참고문헌

[1] Bring Your Own Device(BYOD), http://en.wikipedia.org/wiki/Bring_your_own_device , 2013년 3월

[2] KT 경제경영연구소, “스마트 오피스의 새로운 트렌드 BYOD”, 2011년 11월

[3] Intel, "2012-13 Intel IT Annual Report"

[4] VMware Horizon Suite, http://www.vmware.com/products/desktop_virtualization/horizon-suite/overview.html , 2013년 3월

[5] Samsung KNOX, http://www.samsung.com/global/business/mobile/solution/security/samsung-knox , 2013년 3월

[6] Blackberry Enterprise Service 10, http://us.blackberry.com/business/software/bes-10.html , 2013년 3월

[7] f5 mobile app manager, http://www.f5.com/products/mobile-app-manager/overview/ , 2013년 3월

[8] 산업기밀보호센터 기술유출통계, http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00 , 2013년 3월