모바일 단말에서의 정보 유출 방지를 위한 클라우드 플랫폼 구축

송왕은, 정승욱, 정수환
숭실대학교 정보통신공학과

An Established Cloud Platform for Data Loss Prevention on Mobile Device

Wangeun Song, Seungwook Jung, and Souhwan Jung
School of Electronic Engeneering, Soongsil University.

요 약

BYOD(Bring your own device) 환경에서는 개인의 스마트 기기를 이용하여 회사 시스템을 이용하는 것으로, 개인의 단말을 업무에 이용하는 만큼 사원의 개인정보, 고객의 개인정보, 신규 사업 아이템, 상품의 거래내역, 계좌번호 등 유출시 막대한 손해를 발생시키는 사내 정보 유출에 대한 문제가 발생 가능하다. 화사 시스템을 관리하기 위해 개개인이 사용하는 다양한 종류의 단말에 맞는 설정이 필요함으로 즉각적인 대응이 어렵다. 때문에 위 같은 문제를 해결하고자 삼성이 개발한 듀얼 OS 구조의 KNOX가 제안되었으나, 특정 단말과 OS에 의존적이어서 다양한 종류의 단말에 적용하기 위해서는 지속적 개발이 필요한 단점이 있다. 다른 방법으로 MDM(Mobile Device Management) 시스템을 제안하였지만 새로운 모바일 단말에 대한 즉각적인 대응이 힘들며, 유지보수에 많은 시간과 투자가 필요한 단점이 있다. 따라서 본 논문에서는 단말에 의존적이지 않으면서, 기업의 정보를 보호하기 위하여 클라우드 기반 정보 유출 방지 플랫폼을 설계하고 제안한다.

I. 서론

최근 IT 기술의 발전으로 스마트기기의 보급 증가 하고 있다. 이에 따라서 BYOD(Bring your own device)대한 관심도 증가하고 있다. BYOD란 개인이 보유하고 있는 모바일 단말을 직장에서 사용함으로써, 언제 어디서나 쉽고 빠르게 업무를 처리 할 수 있는 장점이 있다. 하지만 직장의 네트워크를 사용하는 모든 종류의 모바일 단말을 MDM(Mobile Device Management) 기술을 활용하는 데는 한계가 존재한다. 이러한 한계점은 모바일 단말을 통한 정보 유출의 위험성을 가지고 있다.

본 논문에서는 클라우드 컴퓨팅을 기반으로 A Clientless Remote Desktop Gateway based html, Android VM(Virtual Machine)을 활용해 서로 다른 종류의 모바일 단말을 간편하게 관리하므로써 모바일 단말을 통한 정보 유출을 방지 할 수 있는 클라우드 플랫폼을 제안한다.

논문의 구성은 다음과 같다. 2장에서는 관련 연구를 설명하고 3장에서는 본 논문에서 제안한 플랫폼에 대해 설명하고 마지막으로 4장에서 결론을 제시한다.

II. 관련 연구

2.1 BYOD(Bring your own device)

스마트기기의 발달과 무선 네크워크의 발전으로 인해 스마트기기를 비즈니스에 적극적으로 활용하기 위해 BYOD의 도입이 확산되는 추세이다. BYOD 환경에서는 개인 소유의 노트북, 스마트폰, 테블릿 등을 각자의 업무환경에 맞추어 사용한다. 개인 소유의 스마트기기를 업무에 이용하는 것은 기업 입장에서도 효율적으로 업무를 진행 할 수 있으며, 디바이스 활용에 대한 유성이 증가하기 때문에 새로운 업무 프로세스

로 자리를 잡아 가고 있다. 하지만 이러한 BYOD 환경은 확실한 보안 관리 정책이나 보안 시스템이 구축되어 있지 않다면 오히려 문제를 야기 한다. 따라서 BYOD 환경 도입을 위해서는 보안과 관리에 대한 보다 강력한 조치와 통제 정책이 필요한 시점이다. BYOD 디바이스를 서버에 등록하고 강력한 인증체계와 네트워크 암호화를 통하여 사용자를 확인하는 과정, 모바일 디바이스의 분실우려를 위한 MDM 기능 구현이 동시에 이루어져야 한다. 또한, 유무선 인프라에 지속적인 점검이 수반된 안전한 네트워크를 구축 및 유지해야 한다[1][2].

2.2 KNOX

KNOX는 삼성이 안드로이드를 기반으로 제작한 모바일 보안 플랫폼이다[3]. SE Android 기반에서 작동하며, 하드웨어에 따라 수정 가능한 Secure Boot와 TrustZone-based Integrity Measurement Architecture(TIMA)가 존재한다. TrustZone은 ARM CPU에서 제공되는 기술로, KNOX의 실행 유무에 따라 보안모드와 일반모드를 분리되며 각 모드는 독립적으로 작동한다[4]. 하지만 KNOX 단말 의존 적인 모바일 보안 플랫폼이라는 한계를 가지고 있다. 삼성을 제외한 LG, 베가, iphone등에서 재조된 모바일 단말에서 KNOX를 사용하기 위해서는 단말 OS 통합, 기술 공유 등 많은 어려움이 존재한다.

2.3 MDM

MDM(Mobile Device Management)은 회사 내의 부서별, 개인별로 IT 정책을 정의하여 차별적으로 적용이 가능한 기업형 모바일 단말 관리 서비스이다. 모바일 단만을 기업의 자산으로 관리하기 위해 소프트웨어 배포나 실시간 진단 및 컨트롤, 원격 백업 및 복구, 삭제, 관리 등의 다양한 기능을 제공한다. 데이터 원격 삭제를 통한 분실관리, 화면 잠금, 암호 길이 및 변경 주기 설정, 디버깅 및 루팅 허용 정책을 통한 보안 설정 제어, I/O 제어 및 저장 매체 제어를 통한 모바일 단말 잠금 설정을 할 수 있다. 또한, 어플리케이션 및 프로세스 모니터링을 통하여 관리하고 S/W는 OTA(Over The Air) 배포가 가능한 방식이다[5]. 하지만 MDM은 모바일 단말 OS의 의존도가 높은 관리방식이며 모바일 단말 OS에 따라 제어 할 수 있는 범위가 달라진다. 현재 Android OS는 원하는 대부분의 기능을 제어 할 수 있다. 하지만 이와 달리 IOS는 제어 할 수 있는 범위가 Android OS와 비교하여 차이가 크다. 다음 [표 1]은 공통적으로 제어 할 수 있는 범위를 나타내며, [표 2]는 Android OS는 제어 할 수 있지만 IOS는 제어 할 수 없는 범위를 나타낸다. 위와 같이 모바일 단말 OS에 따라 제어 할 수 있는 범위가 다르며 MDM 서비스를 이용 시 특정 모바일 단말 OS만을 사용하도록 제어 할 수 없는 상황에서 모바일 단말에 비 의존적인 MDM 시스템 환경이 요구된다[6].

[표 1] 공통 지원 통제 범위

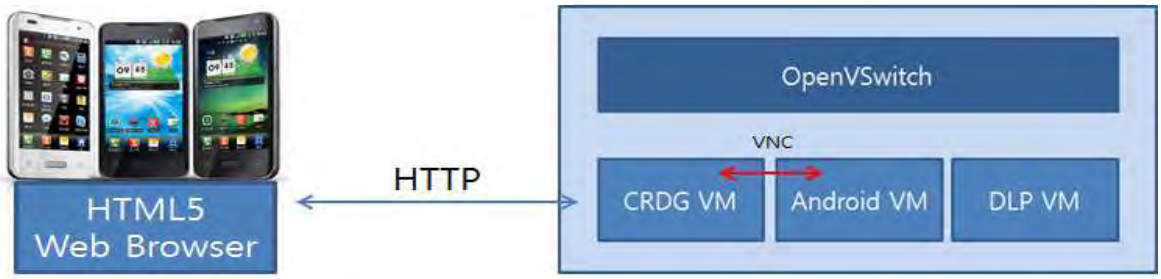
원격제어	원격 데이터 삭제 및 공장초기화(Remote Wipe)
	원격화면 잠금(Remote Lock)
	단말기 위치 확인(MAP상 표시 지원)
	회수 요청 및 긴급통화 설정
비밀번호 제어	비밀번호 강제 변경
	간단한 패스워드 사용 제어
	최소 패스워드 길이
	숫자 ,알파벳, 특수문자 조합 설정
	자동 잠금 시간 설정
	비밀번호 오류 횟수 제한
	비밀번호 사용 유효 기간
디바이스 제어	카메라 사용 차단
	IMEI/MEID 제어
	Current carrier network 정보
	스크린캡쳐 방지

[표 2] 차별되는 통제 범위

기능	Android OS	IOS
녹음기 사용 차단	O	X
사용가능한 Wi-Fi	O	X
블루투스 제어	O	X
SSID of wireless network 정보	O	X
테더링제어	O	X
USB 데이터 전송 차단	O	X
USIM 상태 체크 및 정보	O	X

III. 제안플랫폼

본 논문에서 MDLP VM(Mobile Data Loss Prevention Virtual machine), CRDG VM(A Clientless Remote Desktop Gateway VM), Andorid VM을 구축, 표준 프로토콜 VNC를 사용하여 사용자 단말에 비 의존적인 클라우드 기반의 정보 유출 방지 플랫폼을 제안한다.



[그림 1] 모바일 단말에서의 정보 유출 방지를 위한 클라우드 플랫폼 구성도

3.1 제안플랫폼 구성

[그림 1]은 제안플폼의 전체 구성을 보여준다. CRDG VM, Android VM, MDLP VM을 구축하고 OpenVSwitch를 설정하여 VM들 간에 Flowrules를 만들어 Flowtable에 저장한다. 저장된 Flowrules에는 각 VM의 패킷이 전송 될 VirtualPort들이 지정되어 있고, 각 패킷들은 지정된 VirtualPort를 통해 전송된다. 모바일 단말과 CRDG VM은 HTTP 프로토콜을 이용하여 통신하며, CRDG VM와 Android VM은 VNC 프로토콜을 이용하여 통신한다. 표준 프로토콜인 HTTP, VNC를 사용하여 모바일 단말의 종류에 상관없이 제어하기 쉬운 Android VM을 사용하여 개인 정보 유출 방지 플랫폼을 구성했다.

3.2. 제안플랫폼 시나리오

모바일 단말에서의 정보 유출 방지를 위한 클라우드 플랫폼의 테스트 시나리오는 [표 3]과 같이 총 9단계로 구성된다. 단말의 종류에 비의존적인 플랫폼으로써 사용자의 모바일 단말에 개별적인 인증 절차 없이 간단한 회원가입, 승인 과정으로 서비스 사용이 가능하다. 관리자가 사용자 권한을 승인 후, 사용자 별 Android VM 생성된다. 사용자는 사용자 페이지에서 VM 생성을 확인 한 후 모바일 단말에서 웹 브라우저를 이용, CRDG 서버로 접속한다. 서버에 접속 후 VNC 프로토콜을 이용하여 Android VM에 연결한다. 마지막으로 웹 페이지에 접속하여 게시판에 개인 정보를 입력한다. MDLP VM이 개인 정보 입력을 감지하고 웹 페이지 차단을 확인한다.

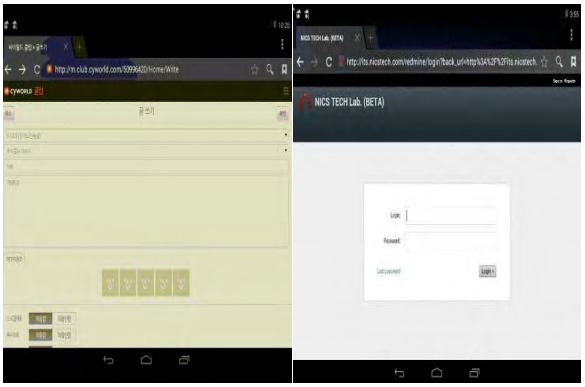
[표 3] 플랫폼 시나리오

1. 사용자 서비스 가입
2. 관리자 승인
3. Android VM 생성
4. 사용자 페이지에서 VM 생성 확인
5. 모바일 단말에서 웹 브라우저로 CRDG VM 접속
6. 모바일 단말에서 Android VM 접속
7. 웹 브라우징하여 싸이클럽 접속
8. 싸이클럽 게시판에 개인정보 입력

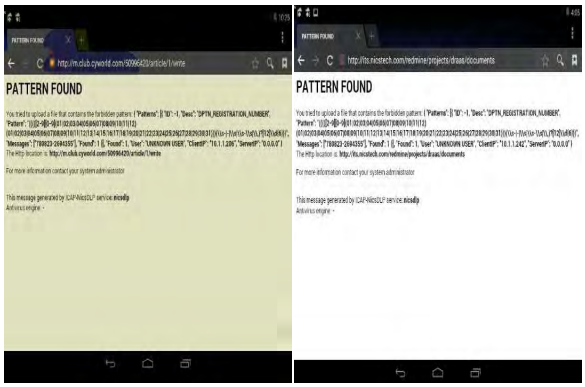
3.3. 제안플랫폼 테스트 결과

제안하는 테스트의 구성은 다른 종류의 모바일 단말 2대를 사용하여 개인 정보 유출 방지 기능을 확인 한다. 사용된 단말 기종은 갤럭시S4와 아이패드을 사용했다. 테스트 웹 페이지는 일반적으로 많이 쓰이는 싸이클럽 게시판을 사용했다. [그림 2]와 같이, 2가지 종류의 단말 모두 CRDG 서버에 접속 가능했다. 다음으로 [그림 3]과 같이 2가지 종류의 단말 모두 Android VM과 VNC 프로토콜을 이용하여 통신이 가능했다. 마지막으로 [그림 4]와 같이 2가지 종류의 단말 모두 웹 게시판에 자신의 개인정보 등 중요 정보를 입력 할 경우, 페이지가 차단되는 것을 확인했다.

[그림 2] CRDG 서버 접속



[그림 3] Android VM 접속



[그림 4] 개인 정보 유출 차단 페이지

IV. 결론

본 논문에서는 BYOD환경에서 모바일 단말에서의 정보 유출 방지를 위한 클라우드 기반의 플랫폼을 제안한다. 제안 플랫폼의 구성은 CRDG VM, Android VM, MDLP VM 등을 구축하고, OpenVSwitch를 설정하여 VM들 간에 Flowrules를 설정하여, Flowtable 저장한다. 저장된 Flowrules은 패킷이 전송될 VirtucalPort를 지정한다. 이를 통해 Servcie Function Chaining을 구성한다. 모바일 단말에 비 의존적인 플랫폼을 구현하기 위해 표준 프로토콜을 사용한다. 모바일 단말과 CRDG 서버는 HTTP 프로토콜을 사용하고, CRDG 서버와 Android VM는 VNC 프로토콜을 사용함으로써 모바일 단말의 종류에 따른 특별한 설정이 필용 없으며, Android VM에서 외부로 전송하는 모든 패킷을 MDLP VM으로 전송되고, Android VM에서 전송된 패킷은 MDLP VM에 설정된 특정 패턴(주민등록번호, 전화번호, 계좌번호 등)과 비교하여 패턴 발견 시 개인정보 등 중요 정보 유출을 경고하는 메시지를 사용자에게 전송하고. 패킷 전송을 차단한다. 위 같은 방식을 이용하여 개인 단말에 비의존적인 정보 유출 방지 플랫폼의 구축이 가능하다.

본 제안 플랫폼을 통해 BYOD 환경에서 정보 유출 방지 솔루션을 구축하기 힘든 소규모의 기업체에서 BYOD 환경의 모바일 단말에서의 정보 유출의 취약점을 해소 할 수 있을 것으로 판단된다.

ACKNOWLEDGMENT

본 연구는 산업통상자원부 및 한국산업기술평가관리원의 우수기술연구센터(ATC)사업의 일환으로 수행하였음. [10045904, 클라우드 컴퓨팅 환경하에서 정보보안 서비스를 제공하기 위한 SecaaS 프레임워크 원천기술 개발과 이를 이용한 1Gbps급 모바일 정보유출방지 서비스 구축]

[참고문헌]

[1] A. Scarfò, “New security perspectives around BYOD,” in Proc. 7th Int. Conf. Broadband, Wireless Computing, Commun., Applicat. (BWCCA), pp. 446-451, Victoria, Canada, Nov. 2012.

[2] 박정수 박민호 정수환, “S모바일 단말을 이용한 whitelist 기반 비인가 AP 탐지 및 접속 차단 기법 ”, 한국통신학회논문지 제38권 제8호 Aug 2013

[3] Samsung, “KNOX,” https://www.sam-sungknox.com/en/

[4] 박상호 김현진 권태경, “안드로이드 스마트폰 암호 사용 앱 보안 분석 및 대응” 정보보호학회지 제23권 제6호, 2013.12, 1049-1055 (7 pages)

[5] L. Liu, R. Moulic, and D. Shea, “Cloud service portal for mobile device management,” in Proc. IEEE 7th Int. Conf. e-Business Eng. (ICEBE), pp. 474-478, Shanghai, China, Nov. 2010.

[6] 이강현 윤두식, “모바일보안을 위한 MDM의 효과적인 접근 방법” 정보보호학회지 제23권 제2호, 2013.4, 29-34 (6 pages)