情 報 保 護 學 會 誌
第23卷 第2號, 2013. 4

모바일보안을 위한 MDM의 효과적인 접근 방법

이 강 현*, 윤 두 식**

요 약

최근 들어 비즈니스 환경이 모바일과 클라우드 화 되고 있으며, 그에 따른 보안기술은 핵심적인 이슈로 손꼽히고 있다. 모바일 디바이스의 개인과 기업 활용도가 높아지면서 이로 인한 정보 유출 위험성이 심각한 문제로 제기되고 있다. 이를 해결하기 위한 다양한 보안정책이나 가이드가 제시되고 있지만, 모바일 보안에 대하여 명확한 규정이나 솔루션이 없었기 때문에, 보안담당자와 IT기획담당자들은 그 필요성과 적용 방법에 대하여 의문을 가지고 있는 것이 현실이다. 2011년부터 국내 개발사들이 MDM제품을 출시하면서 국내 모바일 업무 환경에 대한 본격적인 보안 해법들이 제시되고 있다. 본 고에서는 모바일 업무 환경에서의 보안에 대한 올바른 이해와 실제적인 적용 방법을 제시하고자 한다.

Ⅰ. 서 론

미국 올랜도에서 개최된 Gartner Symposium에서 2013년 10대 전략기술이 발표되었고, 최근 몇 년 동안 그래 왔듯이 모바일과 보안기술은 핵심적인 이슈로 손꼽히고 있다. 한국에서도 스마트폰, TabletPC에 대한 개인과 기업의 활용도가 높아지면서 이를 통한 정보 유출 위험성이 심각한 문제로 제기되어 왔으며, 이를 해결하기 위한 다양한 보안정책이나 가이드가 제시되고 있다.

그러나 모바일 보안에 대하여 명확한 규정이나 솔루션이 없었기 때문에, 보안담당자나 IT기획담당자들은 그 필요성과 적용 방법에 대하여 잘 모르고 있는 경우가 대부분이었다.

2011년 하반기 애플 社의 iOS에 대한 MDM API가 공개되고 기존의 Android와 더불어 iOS까지 지원할 수 있는 국내 MDM 제품이 출시되면서 모바일 보안의 본격적인 해법들이 제시되고 있다.

이제 보안담당자, IT기획담당자들에게 모바일 보안에 대한 올바른 이해를 돕고 실질적인 적용이 가능한 방법을 논해 보고자 한다.

Ⅱ. MDM이란 무엇인가

MDM의 개념은 OTA(휴대폰무선전송기술, Over The Air)을 이용하여 언제 어디서나 모바일 기기가 Power On 상태로 있으면 원격에서 모바일 기기를 관리할 수 있는 시스템을 말한다.

MDM의 원래 사용 목적은 원격에서 휴대폰 등 모바일 기기의 어플리케이션 배포, 데이터 및 환경설정 변경, 모바일기기 분실 및 장치 관리들을 통합적으로 관리해 주는 시스템으로 짧은 서비스 다운 타임과 최소의 비용으로 모바일 보안과 기능을 최적화시켜 주는 시스템이었으나, 최근 보안 위협에 대한 강화대책으로 관리의 필요성이 대두되면서 모바일 보안의 핵심요소가 되고 있다.

MDM은 보안된 통신을 제공함으로써 기업의 업무환경에서 데이터가 유출될 수 있는 메일, 웹, 그룹웨어, USB 저장매체 등 다양한 통신 채널에 대해 포괄적 보호기능을 제공함과 동시에 중앙 관리 콘솔을 통해 전사적 모니터링 및 사용자 환경에 대한 통제를 수행하고 있다.

본 연구는 (주)지란지교소프트 연구소 관리로 수행되었습니다.
* (주)지란지교소프트 모바일보안사업부 (leon@jiran.com)
** (주)지란지교소프트 보안사업본부 (dsyoon@jiran.com)

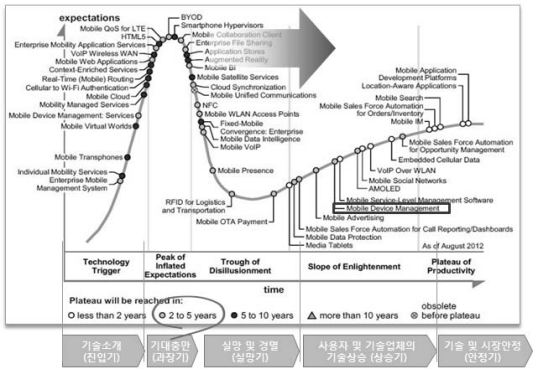
2.1. MDM의 성장

모바일 비즈니스 디바이스의 중심이 기존 Blackberry에서 Android, iOS로 이동하면서 기업용 모바일 SW중 MDM이 가장 빠른 성장세를 보이고 있다. 스마트폰, 태블릿 등의 디바이스에 대한 관리 니즈가 증가함에 따라 성장세가 더 가팔아지고 있는 것이 현실이다.

MDM 라이선스 판매 현황을 보았을 때 북미와 서유럽 중심으로 2011년 35억불 매출에서 2012년 50억불(한화 5조4천여만원) 이상으로 시장이 형성되고 있다.

[그림 1]의 2012년 Gartner Hype Cycle (기술의 성숙도와 라이프사이클을 보여주는 그래프)을 보면, MDM은 2011년 실질보급기로 접어드는 바로 이전단계에서 실사용자 및 기술업체의 기술상승기 단계에 이르러 대중화 이전에 위치하고 있다.

한국도 이와 동일한 사이클 내에 있으며, 많은 기업이 모바일 업무 환경에서 MDM을 실제 적용하고자 고민을 하고 있다.



〔그림 1〕 Hype Cycle for Wireless Devices, Software and Service, 2012

Ⅲ. 모바일 보안, 과연 해야 할까?

최근 3~4년 동안 모바일과 스마트워크에 대한 위협요소와 모바일 보안의 필요성에 대하여 수많은 기고문이나 발표에서 언급되어 왔지만, 너무나 전문적이고 생소한 분야라 이해하기 쉽지 않았다. 과연 모바일보안을 꼭 해야 하는 것인지, 왜 해야 하는지에 대한 의구심들이 많았다.

〔그림 2〕 모바일 보안의 위협요소

모바일보안의 위협 요소는 크게

1) 모바일 단말 자체에 대한 위협,
2) 모바일 운영체제(플랫폼),
3) Application,
4) 무선네트워크

등의 영역으로 나누어 볼 수 있는데, 각각 살펴보면 다음과 같다.

첫째, 모바일 기기는 특성상 손에 쥐고 이동할 수 있는 '움직이는 또 다른 PC'이기 때문에, 사용자의 부주의에 의한 분실/도난 등에 의하여 개인이나 기업 정보가 노출되거나 유출 될 수 있다. 또한 모바일 기기가 담고 있는 카메라, 녹음기 등 다양한 종류의 '스마트 장치'(Smart Device)를 통하여 내부정보는 쉽게 외부로 유출될 가능성이 있다.

둘째, 모바일 운영체제는 사용자에 의하여 쉽게 루팅되거나 탈옥되어 OS 보안 취약점을 이용한 비정상적인 정보의 접근이나 유출 위험이 존재한다.

셋째, 모바일 기기에서 사용되는 수많은 Application에는 PC에서와 마찬가지로 악성코드가 담겨 있을 수 있고, 모바일오피스 App은 해커에 의하여 위변조 되어 손쉽게 정보가 유출 될 수도 있다.

마지막으로, 모바일 기기의 특성상 모든 네트워크는 무선을 사용하게 되면서 해커에 의한 Fake Wi-Fi AP를 통해 데이터가 스니핑 될 수 있고, 사내에서는 허용되지 않은 개인 무선네트워크(테더링 등)를 통하여 정보가 유출 될 수 있다.

결국 개인의 정보나 기업의 정보를 보호하기 위해서는 PC기반의 기간계 인프라에서 다양한 보안을 적용하듯이, 움직이는 PC인 모바일 디바이스에서도 보안을 적용해야 한다는 것은 자명하다.

Ⅳ. MDM은 보안의 모든 것인가

국내에서 MDM에 대한 인식은 매우 다양하다. 누군가는 '모바일 보안은 곧 MDM이고 MDM만 적용하면 모두 해결된다'고 생각하고, 또 누군가는 'MDM은 보안을 위한 솔루션이 아니라 관리를 위한 것'이라고 생각한다.

MDM에 필드 경험이 다양한 필자는 MDM을 이렇게 정의 하고자 한다.

"전통적인 MDM은 단말기관리를 위한 것이지만, MDM 응용기술은 한국에서 요구되는 모바일 보안의 핵심적인 해법을 제공할 수 있다." 단, MDM만으로 모든 모바일 보안 이슈를 해결할 수 있다는 뜻은 아니다. PC기반의 기간계에서와 마찬가지로 각각의 보안대상에 맞는 적합한 솔루션이 적용되어야 하는 것이다.

MDM이 모바일 보안에서 필요로 하는 대부분의 보안요건에 대응 할 수 있다는 것은 사실이다. 이를 위해 아래 표를 참고해 보자. [표 1]은 모바일 보안의 위협 영역에서 국내의 대표적인 보안 Compliance 기관인 국정원과 금융감독원의 모바일 보안 정책의 주요 요건에 대하여 이를 해결 할 수 있는 적정한 모바일 보안 솔루션을 분류해 본 것이다.

이외에도 보안의 요구 수준이나 목적에 따라, 모바일 VPN, 모바일 가상화, 키패드보안 등의 모바일 보안 솔루션들도 이용될 수 있다. 하지만, 이상의 내용에서 살펴본 바와 같이 매우 핵심적이고 다양한 모바일 보안의 정책요건에 대하여 MDM에 보안기술을 적용한 보안 MDM (이른바 '한국 업무 환경에 맞는 MDM'이라고 할 수 있다.)에서 그 기술과 해법을 대부분 제공해 줄 수 있다. 물론 모든 MDM제품이 다 그렇지는 않기 때문에 기술적인 검증은 반드시 필요하다.

〔표 1〕 보안 영역에 따른 주요 보안정책

보안 레이어	주요 보안정책	적정 솔루션
단말	비밀번호 사용 의무	MDM
	단말 및 사용자 인증	MDM
	단말기 통제	MDM
	분실대응 및 데이터 원격삭제	MDM
APP	위변조 체크 및 접속통제	MDM/위변조방지솔루션
	신뢰있는 앱배포 및 설치	MDM/MAM
	업무 APP사용시 특정디바이스 기능 차단 (화면캡쳐,WiFi등)	MDM
	악성코드 탐지/치료	백신
	악성프로그램 탐지 및 사용차단	백신/MDM
	사용자 인증 보안강화	공인인증
플랫폼	루팅/탈옥 검증 및 접속차단	MDM
	운영체제 업데이트 무결성 검증	MDM
네트워크	통신 데이터 암호화	암호
	Wifi통한 업무서버 접속통제	MDM
	특정 무선 네트워크만 사용통제	WIPS/NAC

4.1. MDM의 보안 요구 사항

최근 "International Journal of Security and Its Applications"에 발표된 MDM agent에 대한 보안 테스트 방법론을 보면 MDM으로서 갖추어야 할 보안 테스트를 위한 요구사항들을 다음과 같이 기술하고 있다.

MDM의 보안테스트 요구사항이 중요한 이유는 모바일 업무 환경에서 MDM의 적용이 필수가 되고, MDM의 보안 위협이 곧 기업의 보안위협의 가장 큰 요인이 될 수 있기 때문이다.

〔표 2〕 MDM의 보안 요구사항

R1. MDM agent는 Server와의 사이에 안전한 통신 채널을 제공해야 한다.
R2. MDM agent는 인증된 MDM server와 통신을 해야 한다.
R3. MDM agent는 채널의 끊어짐에 대비해야 한다.
R4. MDM agent는 모바일 기기가 동작하기 전 사용자 인증을 수행해야 한다.
R5. MDM agent는 설정과 로그 데이터의 수정 및 삭제를 방어할 수 있어야 한다.
R6. MDM agent는 모바일 디바이스의 하드웨어 모듈을 제어할 수 있어야 한다.
R7. MDM agent는 민감한 데이터를 보호할 수 있어야 한다.
R8. MDM agent는 최소 암호 메커니즘을 강제해야 한다
R9. MDM agent는 애플리케이션을 설치, 삭제, 실행, 정지 할 수 있어야 한다.
R10. MDM agent는 운영체제의 변조를 감지할 수 있어야 하고, 변조를 방지할 수 있어야 한다.

이상에서 보다시피 MDM의 보안 요구 사항은 단말, 애플리케이션, 플랫폼, 네트워크에 대한 통합적인 보안을 요구하고 있으며 이를 만족해야만 안전한 모바일 업무 환경을 지킬 수 있다고 정의한다.

4.2. 보안성 테스트 아이템과 프로세스

[표 2]의 보안 요구사항에 맞추어 MDM agent가 갖

추어야 할 보안 기능들에 대해서 테스트 아이템과 방법들을 간략히 살펴보면 다음과 같다.

제안된 방법은 15가지의 테스트 아이템이 기술되어 있다.

〔표 3〕 테스트 아이템과 프로세스

측정 항목	SR
Item 1. MDM agent와 서버간 암호화 채널 형성 Step1. MDM agent와 서버 간의 전송되는 패킷을 수집 Step2. 수집된 패킷의 분석	R1
Item 2. 서버 접근 프로파일 관리 Step1. 모바일 기기 내의 서버 접근 프로파일을 수집 Step2. 프로파일의 수정 가능여부 체크 및 수정된 프로파일 감지 Step3. Step2실패시 Agent가 Fake서버로 접근하는지 체크	R2
Item 3. 연결에 대한 정기적인 점검 Step1. Airplane 모드, WiFi Off 등의 기능을 통해 통신채널 연결을 끊기 Step2. 연결이 끊긴 시간 동안 수행하는 보호조치를 점검	R3
Item 4. 유저 인증 Step1. 유저 인증 정책을 세팅 (예: password/PIN /locking pattern, length, combination, history, expiration period 등) Step2. 유저가 인증 정책에 맞게 수행하도록 Agent가 제재하는지 체크	R4 R8
Item 5. 유저 인증 상태 전 디바이스 잠금 Step1. 유저 인증이 성공하기 전 MDM Agent가 touch screen, USB port, 외장 메모리, 블루투스 등과 같은 스토리지 또는 모바일 기기 기능에 접근하는 인터페이스를 감금	R4
Item 6. 설정파일과 로그파일의 무결성 Step1. 디바이스 내에서 설정파일과 이벤트 로그 찾기 Step2. 찾은 파일이 수정 또는 삭제가 되지 않는지 체크 혹은 수정과 삭제 감지 체크 Step3. 실패 시 수정 혹은 삭제된 설정을 탐지하고 수정된 로그가 서버로 전송되었는지 체크	R5
Item 7. 하드웨어 컨트롤 Step1. 하드웨어 모듈 활성 혹은 비활성 Step2. 비활성 하드웨어 모듈을 유저가 사용하지 못하는지 체크	R6
Item 8. 경로 우회 Step 1. 디버깅 툴을 이용해 비활성화된 하드웨어 모듈을 사용하지 못하는지, 제조사가 만든 숨겨진 메소드를 사용할 수 없는지, 설정파일을 수정하지 못하는지 체크	R6
Item 9. 데이터 보호 Step1. 보호해야 할 데이터 찾기 Step2. 찾은 데이터가 암호화가 적용이 되어있는지 체크	R7
Item 10. 원격 감금 혹은 와이핑 Step1. 서버가 보내는 잠금 혹은 와이핑 메시지를 받은 후 agent가 즉각 처리하는지 체크 Step2. 와이핑의 경우 모든 데이터가 삭제된 후 스스로 리셋 체크 Step3. 포렌직 툴로 복구가 불가능한지 체크	R7
Item 11. 암호키와 암호화된 데이터 관리 Step1. 암/복호화 키, 암호화된 데이터 찾기 Step2. 찾은 데이터가 평문인지 체크 Step3. MDM Agent App을 디컴파일 Step4. 암/복호화 키가 평문으로 보이는지 체크	R7
Item 12. 인증 실패 대책 Step1. 인증시도의 횟수에 따라 어떤 처리 방식을 가지고 있는지 체크	R8
Item 13. Agent 삭제 및 정지 제약 Step1. Agent 삭제 및 정지 시도 Step2. 삭제 및 정지가 되지 않는지 체크 Step3. 삭제 및 정지가 되었을 때엔 재설치 혹은 재시작 하는지 체크	R9
Item 14. App 설치, 삭제, 실행, 정지 제약 Step1. App 설치, 삭제, 실행, 정지 시도 Step2. Server의 설정에 따라서 agent가 설치, 삭제, 실행, 정지가 제어되나 체크	R9
Item 15. OS 변조 탐지 Step1. OS 변조 시도 (탈옥) Step2. Agent가 탐지하는지 체크 Step3. 탐지 후 OS 수정에 대해서 어떤 대책이 있는지 체크	R10

여기서 주의해야 할 점은 MDM의 특성상 Agent가 삭제되거나 중지될 수 있기 때문에 이 경우 모바일 기기는 통제에서 벗어날 수 있게 된다. 또한 운영체제가 변조된다면 MDM agent의 기능들은 제대로 수행되지 않거나 아예 기능을 수행할 수 없게 된다.

이와 관련된 보안 적합성 평가 규격과 CC인증 규격이 제작되고 있는데, 앞에서 정의된 보안 요구사항과 테스트 항목들이 기반이 될 것으로 보인다.

4.3. MDM의 OS별 통제 범위

MDM은 모바일 기기의 통제를 위해 정의되지만, 모바일 OS마다 그 범위의 한계가 다르다. Android 운영체제는 원하는 대부분의 기능을 지원할 수 있으나, iOS는 통제할 수 있는 범위가 매우 제한적이다.

[표 4]는 Android와 iOS가 공통적으로 지원 가능한 통제 범위를 나타낸다.

[표 5]는 Android와 iOS가 통제할 수 있는 기능 중 차이가 있는 통제 범위를 나타낸다.

기업 업무에서 BYOD(Bring Your Own Device)를 실현하기 위해서는 기업이 특정 OS (또는 특정 제조사

〔표 4〕 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
비밀번호제어	비밀번호 강제 설정
	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
디바이스제어	카메라 사용 차단
	IMEI/MEID 제어
	Current carrier network 정보
	스크린캡쳐 방지

〔표 5〕 차별되는 통제 범위

기능	Android	iOS
녹음기 사용 차단	O	X
사용가능한 Wi-Fi 체크 및 제어	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

의 단말)만을 한정할 수 없고, 범용적인 기기를 대부분 지원할 수 있어야 한다. 따라서 위의 사례에서 보는바와 같이 기업은 모바일 업무 환경에서 OS의 특성을 고려한 통제 범위를 스스로 결정하고 운영할 수 있는 최소한의 능력을 갖추고 있어야 한다.

4.4. 보안으로서 MDM의 미래

MDM이 발전하고 모바일 업무 환경의 요구사항이 증가함에 따라 Mobility, Interface 등에 초점을 맞춰 보안, PC관리, 원격 지원 등을 추가 지원함으로써 디바이스 관리로부터 확장된 기능을 제공하는 추세이다.

2011년도에 MDM은 소비자의 Mobile Device에 대한 기본적인 보안을 지원하는 기업정책 강화 기능에 초점을 맞췄다면, 2012년도 이후에는 3rd Party, 기업 자체 어플, 콘텐츠 등을 지원하고, Tablet Device를 지원하는 것이 관건이 되고 있다.

최근 부상하고 있는 Dropbox, Box.com 등 온라인 클라우드 파일 동기화 서비스는 보안상의 위험으로 기업용 데이터 저장과 활용에 적합하지 않아 MDM 벤더들이 MAM(Mobile Application Management)분야로 시선을 돌리고 있다.

2013년에 들어서는 다수의 MAM 기업들이 보안, 공유 기능이 가미된 '기업용 문서관리 시스템'을 선보일 것으로 예상된다. 시만텍의 누코나 인수 및 앱센터 구축을 그 사례로 들 수 있다.

향후 2년간 MDM 플랫폼 영역이 확대되고 디바이스 관리 넘어 기업 모바일 관리 시스템 플랫폼을 제공하게 될 것으로 예상된다.

Ⅴ. 효과적인 모바일보안 적용 사례와 사용자 불만 해소방법

모바일 보안은 PC기반의 보안과는 다르게 사용자 불만에 대한 우려가 매우 높은 편이다. 모바일 오피스에 있어서도 BYOD가 전반적인 Trend이고, 법인 지급 단말기라고 하더라도 그 단말기를 이용하는 사람은 결국 '개인'이다. 이는 곧, 그 모바일 기기의 소유주가 누구이든, 개인이 사용하는 단말기에 어떠한 보안을 적용하면 그 사용자는 불편함과 불안감을 느낄 수 밖에 없다는 것이다. 이 때문에 보안담당자나 IT기획 담당자들은 모바일 보안에 대한 필요성이 있어도, 개인 사용자의 불만에 대한 걱정이 앞서 적극적인 업무추진이 어려운 경우가 많다.

이에, 사용자 불만을 최소화 하고 효율적이고 효과적인 모바일 보안을 적용하기 위하여 국내 업무환경에 맞는 MDM에서는 다음과 같은 해법을 제시하는데, 실제 사례를 중심으로 살펴 보겠다.

5.1. 모바일 오피스 사용 시 보안 적용

신한금융그룹(신한은행, 신한생명 外)과 수자원공사 등의 금융 및 공공기관이 대표적인 사례이다. 모바일오피스(업무 App)를 BYOD에 적용하면서 사용자 단말기內 회사의 정보를 보호하기 위하여, 해당 업무 App을 사용 하는 동안에만 보안 통제(무결성체크, 화면캡쳐차단, 루팅/탈옥체크, Wi-Fi 접속차단, 악성코드검사 등)를 적용하고 평상시에는 화면잠금 비밀번호 사용 정도의 기본적인 보안 이외의 모든 사용이 자유롭다. 심지어 모바일보안 프로그램(MDM 등)의 삭제도 사용자에게 권한을 주어 언제든지 삭제가 가능하다.

물론, 보안프로그램을 삭제하면 해당 업무 App은 접속이 불가능하여 업무수행이 어렵게 된다. 따라서, 사용자는 효율적인 모바일업무 수행을 위해서는 회사에서 제공하는 최소한의 안전 장치를 꼭 따라야 하는 것이므로 큰 거부감 없이 사용할 수 있게 되었다.

5.2. 사내에서만 모바일 기기 통제

코오롱그룹(중앙기술연구소)와 LG화학기술연구원 등이 대표적인 사례이다.

연구소, 지식기반산업체(반도체 등), 군 관련 기관 등은 모두 회사 내부의 핵심정보에 대해 카메라, 녹음기, USB등을 통하여 외부에 유출되는 것을 방지하고자 한다. 따라서, 모바일기기의 사내 출입에 대한 엄격한 통제가 필요한데, 기존의 스티커 부착 방식만으로는 출퇴근시간도 지연되고 모바일기기 內 다양한 디바이스(녹음기 등)을 통제하기에는 역부족이었다. 이에, MDM을 통하여 해당 디바이스를 차단하는데, 여기서 중요한 것은 해당 단말기가 사내(보안구역)에 들어왔을 때에만 자동 차단하고 회사 외부로 나갔을 때는 자동 해지한다는 것이다.

단말기 사용자는 외부에서는 자유롭게 모든 디바이스를 사용할 수 있지만, 사내 보안 구역에서는 정보유출의 수단이 될 수 있는 각종 디바이스를 사용할 수 없다는 것이다. 이는 결국, 회사에서는 회사의 자산을 지키고 개인의 공간에서는 개인의 권리를 지켜준다는 것이므로 사용자 불만이 크지 않다는 것이다.

여기서 참고로, 단말기 입출에 대한 제어 방식은 기지국이나 AP기반, 또는 출입통제시스템(Speed Gate등) 연계기반 등이 있으며 각각의 회사 환경에 따라 다양한 방법으로 적용될 수 있다.

Ⅵ. 결 론

이상 살펴본 바와 같이 MDM의 실제 적용단계에서 사용자 불만을 최소화하여 모바일 보안을 효과적으로 적용하고 있다. 그리고 이러한 기술적인 방법 이외에도, 성공적인 모바일 보안 서비스 제공을 위해서 꼭 필요한 것은 충분한 사내 홍보 활동이다. 지금까지 모바일 보안을 적용한 기업 중에 사내 홍보나 교육 등을 충분히 제공한 기업들은 사용자 불만이 거의 없었다.

끝으로, 모바일 보안은 스마트폰 사용 인구가 3천만 명을 넘고 각종 모바일 위협이 존재하는 현 시점에서 개인과 기업의 정보를 지키기 위해 꼭 필요한 사항이며, 각 기업에 맞는 MDM의 적절한 도입 운영이야말로 이 문제에 근본적으로 대처할 수 있는 필수 과정이 될 것이다.

참고문헌

[1] Keunwoo Rhee, Hawon Kim and Hac Yun Na, Security Test Methodology for an Agent of a Mobile Device Management System, International Journal of Security and Its Applications Vol.6, No.2, April 2012

[2] 금융감독원 IT감독국, 금융권 스마트워크 정보보호 가이드라인, June 2011

[3] Gartner, Hype Cycle for Wireless Devices, Software and Services, 2012, August 2012

[4] Gartner, Magic Quadrant for Mobile Device Management Software, May 2012

[5] Apple, Mobile Device Management Protocol Reference, August 2011

[6] Google, API Guides, http://developer.android.com/guide/components/index.html

〈著者紹介〉

이 강 현 (Lee, Kang Hyun)
1999년 2월 : 충남대학교 컴퓨터과학과 졸업
1996년 8월 ~ 현재 : (주)지란지교소프트 모바일보안사업부 사업부장
<관심분야> 정보보호, 모바일보안, MDM

윤 두 식 (Yoon, Doo Shik)
1997년 8월 : 충남대학교 컴퓨터과학과 졸업
2000년 2월 : 충남대학교 컴퓨터과학과 석사
1999년 11월 ~ 현재 : (주)지란지교소프트 연구소장 겸 본부장
<관심분야> 정보보호, 메일보안, 모바일보안, MDM, 클라우드 보안