장소 한정을 통한 모바일 기기 데이터 보호 기법

정지정, 박지민, 이종협
*한국교통대학교 소프트웨어학과
{asdfzxcvzxcv@nate.com, wlalsqqq@naver.com, jhlee@ut.ac.kr}

Data protection for mobile devices via location restriction

Ji Jung Jung*, Ji-Min Park**,JongHyup Lee*
*Dept of Software, Korea National University of Transportation

요 약

모바일 환경이 발달함에 따라서 사용자의 개인 모바일 기기에 저장되었던 민감한 개인정보 및 기업의 비밀과 같이 기밀성을 필요로 하는 데이터의 누출 사고가 빈번히 발생하고 있다. 본 논문에서는 모바일 기기의 데이터를 지정된 장소에서만 안전히 사용할 수 있도록 하는 기법을 제안한다. 제안된 기법은 공개키 암호화 시스템을 바탕으로 지정된 장소에서만 발행되는 키를 통해서만 모바일 기기의 접근이 가능하게 함으로써 데이터 사용 위치를 강제하고, 의도하지 않은 데이터 누출을 방지한다.

1. 서론

최근 스마트폰의 발달에 따라 개인의 모바일 단말을 통하여 회사업무를 처리하는 BYOD(Bring You Own Device)의 개념이 도입되어 다양한 분야에서 사용되고 있다. 비즈니스 환경 뿐만이 아니라 모바일 단말들이 다양한 서비스의 창구로 사용되면서 은행, 의료 등의 민감한 개인정보들 또한 사용자의 스마트폰에 저장되어 사용되고 있다.

모바일 환경의 특성상 고정된 장소가 아닌 다양한 장소에서 모바일 기기가 사용되면서 더 많은 위험에 노출되게 되었다. 사용자의 기기의 의도하지 않은 분실로 인한 정보누출과 Rogue AP와 같이 공격자가 정상적인 통신망을 가정하여 도청을 시도하는 피해 사례가 급증하고 있다. 저장되어 있는 정보의 가치가 높아질수록 이러한 모바일 단말에 의한 정보누출의 피해액도 급격하게 증가하고 있으며, 모단 스마트폰 무단 사용으로 인한 요금 부과, 소액결제 피해등의 2차 피해도 심각한 수준이다.

컴퓨팅 환경이 모바일 환경으로 이미 변화되어버린 현재의 상황에서 모바일 OS를 개발하고 있는 Apple이나 Google를 위시한 다양한 소프트웨어 업체에서 기업 및 개인의 데이터 보호를 위하여 MDM(Mobile Device Management) 서비스를 제공하고 있지만, 많은 경우에 분실 단말이 네트워크에 연결된 경우에만 효용성을 가진다는 측면에서 한계를 가지고 본다.

이러한 모바일 환경에서의 문제점을 해결하고자 본 논문에서는 모바일 기기에 저장된 데이터에 장소 종속성을 부여하여 지정된 장소에서만 데이터를 열람 또는 수정할 수 있는 기법을 제안하고자 한다. 지정된 장소에서만 데이터를 열람할 수 있게 제한함으로써 단말기 분실에 따른 정보 누출을 최소화하고 데이터 사용을 위치와 연결하여 강제함으로써 안전한 데이터 관리를 가능하게 하고자 한다. 제안하는 기법에서는 공개키 암호화 알고리즘을 이용하여 사용자 모바일 기기 내에 저장되어 있는 데이터를 암호화하고 특정 지역에서만 복호화 키를 제공하여 열람 및 수정을 가능하게 한다. 데이터는 사용 직후 새로 제공 받은 공개키를 이용하여 바로 암호화하여 복호화 키를 제공하는 지역을 벗어나는 경우에는 해당 데이터가 드러나지 않도록 보호한다.

2. 관련 기술 및 연구

MDM(Mobile Device Management)은 Over The Air (OTA)를 이용하여 언제 어디서나 원격에서 모바일 기기를 관리할 수 있는 통합시스템으로 모바일 환경에서의 원격 또는 중앙 관리를 통해 단말기의 분실, 도난을 방지하고, 카메라 및 USB 등의 디바이스 제어를 통해 정보유출을 방지할 수 있는 통합 모바일 보안 기능을 제공한다. 국내의 MDM의 주요 기능을 나누면 다음과 같다.

- 모바일 보안기능 : 디바이스 제어와 네트워크 보안으로 모바일을 통한 자료 유출을 방지하며, 원격 데이터보호, 분실 도난 대비 등을 통해 단말기 분실 시 타인에 의한 기업데이터 접근을 차단함으로써 안전하게 데이터를 보호 할 수 있다.
- 모바일 관리기능 : 관리자만을 위한 기능으로 중앙관리를 통해 새로운 사용자를 추가하거나, 사용자별, 그룹별로 정책을 관리하고 사내 앱을 배포한다. 또 단말기 사용현황, 사용자, 앱, 에이전트 등에 대한 통합적인 관리 및 모니터링을 할 수 있다.

또한 이러한 맥락에서 최근 Apple사와 Google사에서도

iOS와 Android에서 원격에서 도난이나 데이터 누출이 의심되는 모바일 기기의 데이터를 삭제하는 이른바 kill switch라 불리는 기능들이 도입되었다. 하지만 일반적으로 모바일 보안 기능, 모바일 관리 기능 대부분을 기업의 관리자가 관리하며 사용자가 직접 관리할 수 있는 부분은 극히 제한적인 상황이다.

모바일 기기의 데이터 보안을 위하여 다양한 연구가 수행되었다. [1]에서는 관리자의 데이터 유출 가능성이 있어 이 문제점을 보안하기 위해 사용자 스스로가 직접 스마트폰을 관리 할 수 있게 함으로써 사용자의 개인정보를 보다 더 안전하게 보호 할 수 있도록 하는 관리 기법을 제안하였다. 또한 스마트폰 내의 모든 파일을 개인 프라이버시 파일과 일반 공개 파일 2가지로 분류하여 스마트폰에 장착된 하나의 물리적인 디스크에 논리적인 디스크인 가상 디스크를 새롭게 생성하고 2가지로 분류된 파일 중 일반 공개파일은 기존처럼 물리적 디스크에 저장하여 관리하고, 개인프라이버시 파일은 논리적인 디스크인 가상 디스크에 저장하여 보안을 강화하는 기법[2]도 연구되었다. 하지만 두 방안은 모두 모바일 기기가 통신망을 통해서 항상 연결되어 있어야 하고 MDM 솔루션에서 회사관련 자료가 프라이버시로 인식되어 보안영역에 저장되었을 경우 관리자가 프라이버시 데이터 접근 없이 회사관련 데이터를 확인할 수 있는 방법을 필요로 한다는 문제점을 가지고 있다. MDM 형태의 지원 시스템을 이용하지 않는 경우에는 모바일 기기에 저장되어 있는 데이터를 샘플링하여 시그니처로 만들어 누출을 확인하는 기법[3]과 PC가 아닌 다른 디바이스에 여러 백업데이터를 생성시키는 백업관리 기법[4]들 또한 제안되었지만, 이러한 연구 또한 기존 컴퓨팅 환경과 달리 통신망과 저장 장치에 대한 직접 접근 등의 위험한 환경을 가정해야 하는 모바일 기기의 데이터 보안에는 한계점을 가지고 있다.

3. 제안 방안

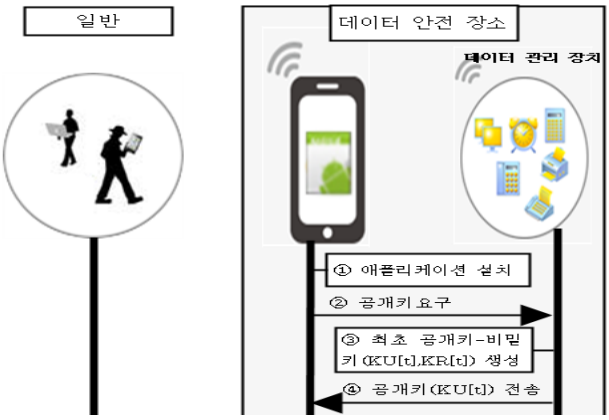
본 논문에서는 모바일기기가 지정된 데이터 안전장소에서만 데이터 열람/수정 할 수 있는 데이터 보호 기법을 제안한다. 제안하는 기법에서는 모바일 기기에 보호 대상 데이터를 지정된 데이터 안전 장소에서만 복호화가 가능하도록 암호화하여 저장한다. 따라서 암호화된 데이터는 모바일기기 분실 시에도 데이터 누출을 방지한다. 이러한 특성을 제공하기 위하여 우리는 공개키 암호 시스템을 이용한다.

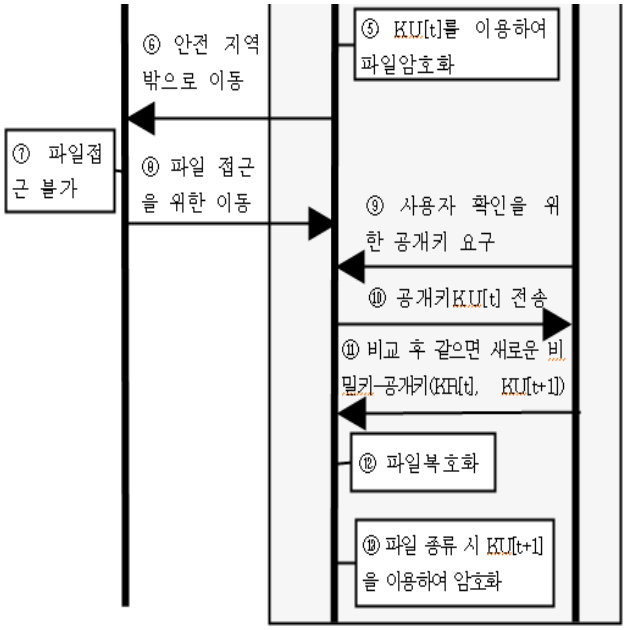
안전성이 중요한 '보호대상 데이터'는 지정된 '데이터 보호 지역'에서만 생성 또는 초기화 될 수 있다. 데이터 보호 지역의 핵심은 무선 AP와 서버로 구성된 '데이터 관리 장치'이다. 데이터 관리 장치는 공개키-비밀키를 생성하고 저장하였다가 요청에 의하여 무선 통신을 통해 키를 제공할 수 있지만, 통신 범위는 데이터 관리 장치가 설치되어 있는 데이터 보호 지역으로 한정된다.

데이터 관리 장치에서는 보호 대상 데이터를 초기화하기 위하여 우선 초기 공개키-비밀키 쌍(KU[t],KR[t])을 생성한다. 사용자의 보호대상 데이터는 이 중 공개키에 해당하는 KU[t]를 데이터 관리 장치로부터 받아 암호화한다. 공개키로 암호화된 데이터는 대응되는 비밀키로만 복호화될 수 있으므로, 이후 보호대상 데이터를 열람/수정 할 경우에는 데이터 관리 장치에서 KR[t]에 대응되는 비밀키인 KR[t]를 제공받아야 한다. 하지만 데이터 관리 장치의 통신 범위가 데이터 안전 장소로 한정되어 있기 때문에 사용자는 데이터를 열람/수정하기 위하여 필수적으로 데이터 보호 지역 내에 위치해야 한다. 또한 데이터에 접근 시마다 데이터 관리 장치에서는 새로운 공개키-비밀키를 생성하고, 복호화를 위한 비밀키를 제공할 때마다 데이터 재암호화를 위한 새로운 공개키를 함께 전달하여 데이터가 사용 직후 새로운 공개키로 암호화될 수 있도록 한다. 따라서 데이터의 사용을 데이터 보호 지역내로 강제하면서 재암호화를 통하여 데이터의 안전성을 보장한다.

이러한 과정을 자동으로 수행하고 데이터의 안전성을 보장하기 위하여 사용자는 지정된 '데이터 보호 어플리케이션'을 통해서만 모바일 기기에서 보호대상 데이터를 열람/수정할 수 있다. 데이터 보호 어플리케이션에서는 사용자가 데이터 접근을 필요로 하는 경우, 데이터 관리 장치와 통신이 가능한 경우(데이터 안전 장소에 있는 경우)에 비밀키를 요청한다. 인가되지 않은 데이터 재사용을 방지하고자 데이터 관리 장치에서 현재의 비밀키(KR[t])와 함께 새로 생성한 공개키(KU[t+1])를 제공하면, KR[t]를 이용하여 데이터를 복호화하여 사용자에게 열람/수정할 수 있도록 하고 작업이 끝나는 대로 바로 제공 받은 KU[t+1]을 이용하여 데이터를 암호화 한다. 이렇게 암호화된 데이터의 접근을 위해서는 다시한번 데이터 관리 장치에서 비밀키(KR[t+1])을 요청하고 새로운 공개키 KU[t+2]로 암호화하는 과정을 반복하게 된다.

데이터 보호 지역을 벗어난 모바일 기기는 항상 공개키에 의하여 암호화 되어 있는 상태로 존재하기 때문에, 스마트폰의 도난 등에 의한 정보 누출을 방지 할 수 있다. 심지어 데이터의 사용자 또한 자신의 데이터를 데이터 안전 장소에서만 복호화 할 수 있으므로 데이터 악의적인 사용 또한 방지할 수 있다. 자세한 기법의 진행과정은 (그림 1)과 같다.





(그림 1) 제안한 기법의 진행과정

① 데이터 보호 어플리케이션 설치 및 데이터 관리 장치 설치
② 데이터 보호 어플리케이션을 실행하여 보호할 파일을 지정 후 데이터 관리 장치에 공개키 요구
③ 데이터 관리 장치에서 최초 공개키-비밀키(KU[t], KR[t])를 생성
④ 데이터 관리 장치에서 모바일 기기로 KU[t]를 전송
⑤ KU[t]를 이용하여 지정된 파일 암호화
⑥ 안전 지역 밖으로 이동
⑦ 암호화로 인하여 지정된 데이터 안전 장소 이외의 장소에서는 KR[t]를 받아 복호화 할 수 없으므로 파일 접근 불가
⑧ 파일 접근을 위해 데이터 안전 장소로 이동
⑨ 사용자 확인을 위하여 공개키를 요구
⑩ 모바일 기기에서 KU[t]를 데이터 관리 장치로 전송
⑪ 데이터 관리 장치에서는 모바일 기기의 공개키와 저장되어 있는 공개키를 비교하여 똑같은 공개키일 때에 새로운 비밀키-공개키(KR[t], KU[t+1])를 생성 후 모바일 기기에 전송, 데이터 관리 장치에서는 KU[t+1]을 저장
⑫ 데이터 관리 장치로부터 KR[t]를 받은 모바일기기는 암호화가 되어있는 파일을 복호화
⑬ 사용자가 업무가 끝나 파일을 종류 시에 KU[t+1]을 이용하여 파일 암호화

4. 보안성 및 성능 검토

제안하는 기법에서는 모바일 기기에 저장된 데이터가 데이터 안전 장소에서만 평문(plain text)로 복호화될 수 있고 데이터 안전 장소를 벗어나는 경우에는 항상 데이터 관리 장치에 의하여 암호화 되어있는 상태로 존재하기 때문에 안전성을 보장받을 수 있다. 특히 데이터는 사용시마다 새로운 공개키로 암호화되고 대응되는 비밀키는 사용직전에만 노출(disclose)됨으로써 키를 재사용하는 replay 공격 또한 불가능하다.

본 기법에서는 데이터 사용시마다 공개키 암호 시스템을 이용한 암호화와 복호화의 과정이 한번씩 수행되면서 성능 및 반응 속도의 저하의 문제를 감수하여야 하지만, 보안성이 중요시 되는 데이터의 경우에는 사용 위치를 한정하고 도난등의 문제에서 데이터 안전성을 지킬 수 있다는 장점을 가지고 있다 .

5. 결론

본 논문에서는 모바일 기기의 데이터 보호를 위하여 보호 대상 데이터가 지정된 데이터 안전 장소에서만 사용될 수 있도록 강제하며, 안정 장소 외에서는 의도하지 않은 데이터 누출을 방지할 수 있는 기법을 제안한다. 사용 시마다 업데이트되는 공개키 시스템을 바탕으로 지정된 데이터 안전 장소에서만 데이터가 열람/수정 될 수 있으므로, 모바일 기기에 저장되어 있는 데이터의 보호뿐만이 아니라 데이터의 회사 외 유출 문제가 심각한 기업내에 보안 기법으로도 활용 가능하다.

참고문헌

[1] 강성태, 조인준, “개인사용자 기반 스마트폰 원격관리 시스템 설계 및 구현”, 한국정보통신학회논문지, 제16권 제12호, 2012.12.
[2] 신숙조, 김선주, 조인준, “스마트폰에서 가상 디스크 플랫폼을 사용한 프라이버시 데이터 보호 방안”, 한국콘텐츠학회논문지, 제13권 제12호, 2013.12.
[3] 정보흥, 김정녀, “모바일 단말에서 외부 저장 매체로의 불법 데이터 유출 방지 기법”, 정보보호학회논문지, 제21권 제1호, 2011.2.
[4] 맹호규, 오태원, “스마트폰 동기화의 개인정보 유출방지 모델”, 한국정보과학회 2011한국컴퓨터종합학술대회 논문집 제38권 제1호(D), 2011.6.