포렌식을 고려한 휴대폰 개인정보 보호 기법

노한영*, 김장성*, 김광조*

* 한국정보통신대학교, 공학부

Private Information Protection Method Supporting Forensic in Cell Phone

Hanyoung Noh*, Jangseong Kim*, Kwangjo Kim*

* Engineering, Information and Communications Univ.

요 약

Gartner에서 언급되었듯이 휴대폰 성능이 향상과 다양한 서비스의 제공으로 휴대폰 보안 사고는 계속해서 늘어날 것으로 예측된다 [1]. 특히, 휴대폰은 컴퓨터에 비해 상대적으로 크기가 작아 쉽게 도난 혹은 분실 될 수 있으며, 다양한 개인정보가 저장되어 더욱 철저한 보안이 요구되지만 휴대폰 보안은 대부분 네트워크 보안 연구만 이루어지고 있다. 게다가 모바일 포렌식 툴을 활용하면 누구나 손쉽게 휴대폰에 저장되어 있는 개인 정보를 추출할 수 있어 문제는 더욱 심각하다. 본 논문에서는 휴대폰에 저장된 개인정보를 보호하기 위하여 컴퓨터 환경에서의 데이터 보안 기법을 살펴보고, 이를 응용하여 휴대폰 환경의 특징을 이용한 개인정보 보호 기법을 제안한다. 제안한 기법은 적법한 포렌식 기관에만 키를 제공하며, 휴대폰에 저장된 개인정보를 보호한다. 또한, 휴대폰 분실 시에도 효과적으로 대처할 수 있는 기법이다.

I. 서론

휴대폰의 성능이 점점 좋아지고 있으며, 지금까지 제공했던 통화 그리고 문자메시지 등의 서비스를 넘어 모바일 뱅킹, 인터넷 등의 다양한 서비스를 제공하고 있다. 하지만, 다양한 서비스를 제공하면서 휴대폰 관련 보안사건, 사고가 늘어나고 있으며, 다른 IT 기기에 비해 더 많은 개인정보들을 담고 있고 작은 크기를 지니고 있어 도난, 분실의 위험이 크다.

지난 2008년 3월 휴대폰 사용자들의 보안 인식에 대해 조사한 결과, 10명중 9명은 개인정보를 휴대폰에 저장을 하고 있다고 응답을 하였으며, 중고 휴대폰 거래를 할 때에 휴대폰에 담긴 개인정보를 삭제하지 않는 경우가 많았다 [4].

최근 Gartner에서는 휴대폰 환경에서의 보안 사건, 사고는 계속 늘어날 것이며 이를 막기 위해 휴대폰에 저장되는 데이터도 암호화를 해야 하며, 침입탐지 기법등과 같은 보안 기법을 적용해야한다고 하였다 [1].

본 논문에서는 컴퓨터 환경에서 이루어지고 있는 데이터 보호 기법을 휴대폰 환경에 적용하며, 기존 컴퓨터 환경의 데이터 보호 기법의 취약점인 키 관리 기법을 휴대폰 환경의 특징을 활용하여 해결하였다. 또한, 최근 이슈가 되고 있는 포렌식 수사를 고려한 보안 기법을 제안한다. 제안 기법은 사용자의 편의성을 해치지 않으면서도 기기 분실 시에도 사용자 개인정보를 보호할 수 있는 장점을 가지고 있으며, 적법한 기관만이 포렌식 툴을 활용할 수 있다는 장점도 있다.

본 논문은 다음과 같이 구성되어있다. Ⅱ장에서는 휴대폰에서 보호할 개인정보란 무엇인지에 대한 정의를 내리고, 제안기법을 설명하기 위한 모바일 포렌식 툴과 컴퓨터 환경에서의 데이터 보호

기법을 설명한다. Ⅲ장에서는 본 논문에서 제안하는 휴대폰 개인정보를 보호하기 위한 기법을 설명하며, 보안성을 분석한다. Ⅳ장에서는 제안한 기법에 대한 보안성 비교를 하고, 마지막으로 Ⅴ장에서는 내용을 정리하고 마무리한다.

II. 관련연구

1. 휴대폰의 개인정보

휴대폰의 개인정보 보안 기법에 관한 설명에 앞서서 '개인정보'의 정의를 살펴본다. '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에서는 "개인정보라 함은 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성 및 영상 등의 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)"라고 정의하고 있다 [5].

따라서, 휴대폰 환경에서의 개인정보는 '전화번호, 전화번호부, 문자메시지, 일정, 사진, 동영상, 통화기록, 인터넷 접속 기록 등' 휴대폰에 저장된 대부분의 정보가 휴대폰 환경에서의 개인정보라고 정의할 수 있다.

2. 모바일 포렌식 툴

휴대폰에 저장된 데이터를 추출하는 대표적인 방법은 통신사에서 제공하는 프로그램을 이용하는 방법과 모바일 포렌식 툴을 사용하는 방법이 있다. 그림 1과 같이 제조사 프로그램을 통해 데이터를 추출할 수 있으며, 일반적으로 기본적인 PIN 4자리를 이용하여 사용자 인증을 하고 있으며, 인증 과정 후 휴대폰에 저장된 데이터를 추출 또는 복사, 그리고 수정 할 수 있다.

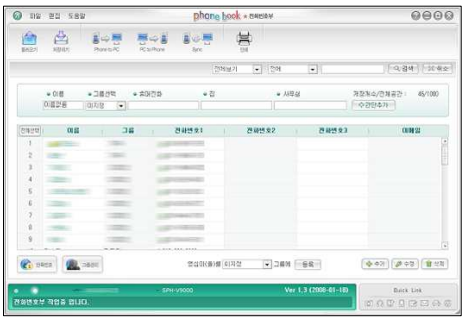

그림 1 : S휴대폰 제조사 프로그램을 이용한 데이터 추출

하지만, 모바일 포렌식 툴은 일반적으로 PIN 번호와 같은 인증 절차를 건너뛰고 휴대폰의 데이터를 추출 또는 복사할 수 있다. NIST에서는 15종류의 모바일 포렌식 툴에 대한 설명과 19가지에 대한 휴대폰과 스마트폰에 대한 포렌식 툴 테스트를 진행하고 그 결과를 정리해놓았다 [2]. 그림 2는 포렌식 툴을 이용하여 전화번호부를 추출한 결과를 보여주고 있다..

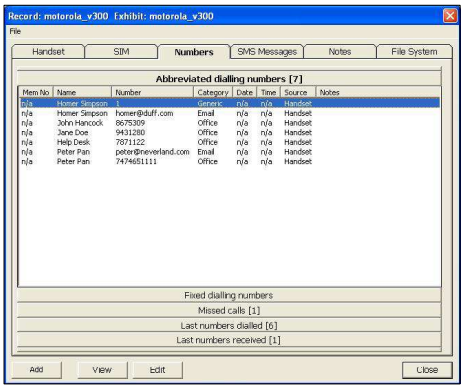

그림 2. PhoneBase2를 이용한 전화번호부 추출[2]

하지만, 포렌식 툴은 법무기관과 같은 적법한 사용자뿐만 아니라 누구나 사용할 수 있다는 단점이 있다. 따라서, 휴대폰을 입수할 수 있다면 누구라도 간단히 휴대폰에 저장된 개인정보를 추출할 수 있다.

실제로 Bitpim과 같은 포렌식 툴은 공개 프로그램으로 누구나 쉽게 인터넷에서 다운로드를 받을 수 있으며 USB 케이블을 통해 쉽게 휴대폰에 저장된 개인정보를 추출하고 수정, 복사할 수 있다. 그렇기 때문에 포렌식 툴에 대한 휴대폰 개인정보를 보호하는 것은 중요한 일이다.

III. 휴대폰 개인정보 보호 기법

휴대폰에서 개인정보가 노출되는 경우는 두 가지 경우가 있다. 첫 번째는 아날로그 형태로 휴대폰의 정보를 확인하는 것이고, 두 번째는 디지털 형태로 정보를 추출하거나 복사하는 방법이 있다. 일반적으로 전자의 경우를 막기 위해서는 정책적, 물리적으로 보호를 하여야 한다. 두 번째의 방법을 막기 위해서는 일반적으로 기술적인 방법으로 보호를 한다. 본 논문에서는 이 두 가지 유출 모두를 최소화하기 위한 보안 기법을 제안한다.

앞에서 설명한 휴대폰 환경에서의 개인정보는 휴대폰에 저장된 대부분의 데이터이다. 이를 효과적으로 보호하기 위한 기법은 저장된 데이터를 모

두 암호화해서 저장하는 방법이 있다.

컴퓨터 환경에서는 저장된 데이터 보호를 위해 디스크 암호화 기법을 주로 사용을 한다 [3]. 디스크 암호화 기법은 디스크 전체를 암호화하는 '전체 디스크 암호화 기법', 파일 시스템을 암호화하는 '파일 시스템 암호화 기법', 그리고 특정 디렉토리나 파일만을 암호화 하는 '파일 암호화 기법'이 있다.

디스크 암호화 기법은 모두 장단점이 있지만, 공통적으로 '암호화 키' 관리의 문제점을 가지고 있다. 일반적으로 디스크 암호화에 사용되는 키는 특정 문자열의 패스워드이거나 외부저장장치를 사용하여 저장하여 사용된다. 특정 문자열의 패스워드의 경우에는 문자열에 따라서 무차별 대입 공격에 취약점을 가지고 있으며, 외부저장장치를 활용하는 경우에는 자리비움이나 도난 등에 취약할 수 있다는 단점이 있다.

1. 외부저장장치를 이용하는 휴대폰 보안

먼저, 휴대폰 데이터 보안도 컴퓨터 환경에서처럼 외부저장장치(SIM카드, MicroSD카드 등)를 사용하는 방법을 제안한다. 그림 3은 제안 기법 1을 간단히 표현하고 있다.

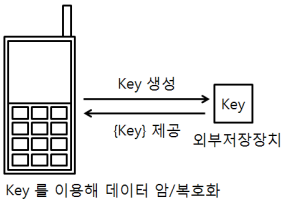

그림 3 : 외부저장장치를 사용한 휴대폰 보안

이는 휴대폰에서 키를 생성하여 외부저장장치에 저장을 하고 필요할 때마다 외부저장장치에서 키를 읽어와 데이터를 암/복호화하는 기법이다.

제안기법은 통신망 구조에 변화를 가하지 않고, 휴대폰 단말기만을 수정하여 암호화를 사용자 개인정보를 보호 할 수 있다. 기존의 포렌식 툴을 이용해서는 복호화 된 데이터를 받을 수 없으며 외부저장장치에 저장된 키가 있어야만 복호화가 가능하다. 또한, 휴대폰을 더 이상 사용하지 않게 될 때에 외부저장장치의 키 값만 삭제해주면 데이터를 간단히 보호할 수 있다는 장점이 있다.

하지만, 휴대폰의 도난, 분실 시에 외부저장장치가 함께 분실된다면 데이터의 보안에 필요한 키가 노출되므로 보안이 취약할 수 있다는 단점이 있다. 이는 기존 컴퓨터 환경에서 외부저장장치를 사용하여 키를 저장할 때와 같은 문제가 발생한다. 문제는 외부저장장치를 컴퓨터 환경에서처럼 사용할 때만 연결해놓지 않는 경우가 많을 것이기 때문에 더 효과적인 키 관리가 필요하다. 다음의 제안기법에서는 통신망의 특징을 이용하여 효과적으로 키를 관리하는 기법을 제안한다.

2. 통신사를 이용하는 휴대폰 보안

첫 번째로 제안한 기법은 외부저장장치에 저장된 키를 보호하고 있어야 사용자 개인정보를 보호할 수 있다. 이번에 제안하는 기법은 일정 시간 단위로 통신사와 휴대폰이 통신을 하는 특징을 이용하여 키를 관리하고, 이 키를 이용하여 휴대폰에 저장된 데이터를 보호하는 기법이다. 단, 기존 휴대폰 통신망은 암호화 통신을 하고 있으므로 안전한 채널이라고 가정한다. 그림 4는 휴대폰의 키 설정을 초기화 작업으로 통신사에 암/복호화에 사용하는 키 생성을 요청하는 것이며 통신사는 키를 생성후 키를 저장 한다.

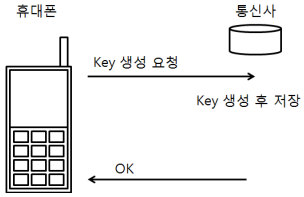

그림 4 : 초기화 작업 : 키 생성 요청

그림 5는 실제 데이터 암/복호화를 위한 과정을 간단히 도식화한 그림이다. 실제적인 프로토콜은 아래와 같이 간단하지는 않겠지만, 전반적인 절차는 그림과 같다. 휴대폰은 통신사에 Key를 요청하고 통신사는 저장하고 있던 Key를 시간값 t와 함께 전송 한다. 휴대폰은 Key를 이용하여 유효시간 t 동안 데이터를 암/복호화할 수 있다. 유효시간 t가 지난 후에는 메모리에 저장하고 있던 Key를 삭제하고 통신사에 Key를 재요청하게 된다.

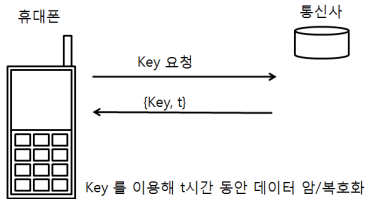

그림 5 : 데이터 암/복호화를 위한 키 요청

제안기법은 다음과 같은 장점을 가지고 있다. 휴대폰의 데이터를 암호화하고 있기 때문에, 기존

의 포렌식 툴로는 복호화에 필요한 키가 없으면 개인정보를 추출할 수 없게 되며, 휴대폰의 분실과 같은 사고 시에 통신사가 저장하고 있는 키를 휴대폰에 전송하는 것을 중단한다면, 유효시간 t가 지난 후에는 휴대폰의 데이터를 복호화 할 수 없게되고, 추가적인 개인정보 유출을 막을 수 있게 된다.

또한, 포렌식 수사를 위해서는 통신사에 복호화 키를 요청해야 데이터를 복호화 할 수 있는 키를 얻을 수 있으므로 적법한 포렌식 기관이 아니라면 포렌식 수사를 할 수 없다.

IV. 제안기법 비교 분석

표 1은 기존의 휴대폰 환경과 제안기법 1, 2를 각각 비교해본 표이다. 기존 휴대폰에서는 데이터 보안을 주로 단순한 4자리 비밀번호에 의존하고 있어서 보안의 강도가 매우 약하며, 포렌식 툴을 사용했을 때는 비밀번호 인증절차를 건너뛸 수 있다. 하지만, 제안한 기법의 경우에는 하드 디스크 암호화 기법을 사용하여 데이터를 보호 할 수 있으며, 디스크가 아닌 휴대폰의 논리 기억장치인 메모리를 덤프(Dump)하는 수준으로 키 값을 추출하지 않는 이상 안전하다고 할 수 있다.

표 1 :. 제안기법 비교 분석

	기존 휴대폰	제안기법 1	제안기법 2
데이터 보안	불가능	가능	가능
분실 시 데이터 보안	불가능	알 수 없음	가능
포렌식 수사	누구나 가능	불가능	적법한 기관만 가능
통신망 구조 변경	-	불필요	필요

휴대폰을 분실 했을 때는 기존 휴대폰 환경에서는 데이터 유출을 막을 수 없지만, 제안기법 1에서는 외부저장장치에 저장된 Key를 안전하게 관리하면 데이터 보호가 가능하지만, 외부 저장장치를 분리하는 경우는 거의 없기 때문에 데이터 보안은 불충분하다. 하지만, 제안기법 2는 주기적으로 통신사에서 키를 얻어오는 작업을 하기 때문에 사용자가 분실신고를 하여 키 전송을 막으면 분실했을 때도 데이터를 보호 할 수 있다.

포렌식 수사는 기존에는 누구나 가능했지만, 제안기법 1에서는 개인이 가지고 있는 키 값을 공개하지 않는다면 불가능고, 제안기법 2는 키 값을 통신사에 요청해야 받을 수 있으므로 적법한 기관만 포렌식 수사가 가능하다는 장점이 있다.

그리고 제안기법 1은 기존 통신망 구조를 변경하지 않고, 단말기 제조할 때의 구조만 변경하면 되므로 간단하게 적용이 가능하다는 장점이 있지만, 제안기법 2는 기존 통신망 구조를 변경해야 한다는 단점이 있다.

마지막으로 본 논문에서 제안한 기법들은 모두 사용자의 편의성을 해치지 않는 기법들로 암/복호화시에 필요한 키 생성 및 키 관리, 그리고 키를 사용한 암/복호화 할 때의 시간이 더 걸린다는 측면 외에는 사용자에게 추가적인 입력이나 절차를 필요로 하지 않는다는 장점이 있다.

V. 결론 및 향후 과제

본 논문에서는 휴대폰 개인정보 유출을 막기 위한 보안 기법을 크게 두 가지를 제안하였다. 첫 번째 기법은 기존 컴퓨터 환경에서처럼 키 값을 외부 저장장치에 저장하여 사용을 하는 기법이며, 두 번째 기법은 휴대폰 환경을 고려하여 통신사에서 키 값을 관리하는 방법으로 휴대폰 분실 등으로부터 데이터를 보호 할 수 있으며 부적합한 포렌식 등으로부터 데이터를 보호할 수 도 있다.

향후 연구과제로는 실제 제안 기법을 적용하기 위한 적합한 알고리즘과 프로토콜을 연구하여야 하며, 휴대폰의 논리 메모리상의 데이터 추출이 가능한지에 대한 여부를 조사할 예정이다.

참고문헌

[1] Gartner, “Security risks rise as smart phones get smarter”, Computerworld, 29th, Sep. 2008.

[2] NIST, “Cell Phone Forensic Tools : An overview and Analysis Update”, March, 2007.

[3] WinMagic. “White paper : Disk Encryption Products”, July, 2005. http://www.winmagic.com/downloads/diskencryption_whitepaper.pdf

[4] 이혜경, “휴대폰 사용자의 개인정보 보호 의식 연구”, 한국통신학회논문지, Vol. 33, No. 5, March, 2008.

[5] 최정열, “인터넷과 개인정보의 보호, 제6차 학술심포지엄 자료집”, 한국정보법학회, 2002.