모바일 단말기 분실 시 사용자 정보 보호방안

정우철, 황재연, 이동민, 이경석, 전문석
숭실대학교 대학원 컴퓨터공학과
e-mail : {jeong0116, eyestorys, ldm1021, 2008kslee, mjun}@ssu.ac.kr

A Method on Protecting User Information in Lost Mobile

Woo-Cheol Jeong, Jae-Yeon Hwang, Dong-Min Lee,
Kyung-Seok Lee, Moon-Seog Jeon
Dept of Computer Science, Graduate School of Soongsil University

요 약

최근 모바일 단말기의 급격한 발전으로 인해 단말기에 유입되는 정보의 중요성이 더욱 부각되고 있다. 분실 혹은 도난 시 발생하는 사고는 서비스 과다 사용으로 인한 금전적인 피해뿐만 아니라 사용자 정보 유출 등으로 인한 정신적인 피해, 개인정보를 악용한 협박 등의 범죄로 점차 발전하여 그 심각성은 나날이 더해가고 있는 실정이다. 본 논문에서는 모바일 단말기와 이동통신사간의 상호인증을 통하여 원격제어 권한을 얻어 사용자 정보를 판독 불가능 상태 혹은 삭제할 수 있게 하여 외부 노출 시 안전하게 보호할 수 있게 하고, 이동통신사를 통해 사용자 정보를 안전하게 수집하여 향후 원래 상태로 완벽하게 복구할 수 있는 시스템을 제안한다.

1. 서 론

최초의 모바일 단말기는 이동 시 상대방과의 통화가 주된 목적으로 사용되었다. 그렇게 만들어진 모바일 단말기는 사용자의 요구사항 증가와 기술의 발전으로 인하여 현재 PC(Personal Computer)의 성능과 대동소이하게 기능이 발전하고 있다.

최근 동향은 이동 중 풀브라우징(Full-Browsing)을 통하여 인터넷 통신이나 팩스 전송 등 기존 PC에서나 가능했던 막강한 기능을 제공하는 차세대 휴대전화로 스마트폰 시장이 점차적으로 발전하고 있다. 스마트폰의 등장은 미려한 디자인을 바탕으로 편의성에 중점을 둔 UI(User Interface)와 제품이 더욱 경량화되고 있고 풀터치스크린(Full- Touchscreen)을 제공하는 등 휴대성과 편의성 측면에서 매우 뛰어난 성능을 보여주고 있다. 그러나 다양한 기능들을 지원하는 만큼 그에 따른 보안의 문제는 더욱 심각해졌다.

이처럼 최근의 모바일 단말기는 풀브라우징 지원, Bluetooth 기능, E-mail전송, 동화상 촬영, MP3 재생 등의 다양한 기능 수행이 가능하고, 모바일 단말기에 다양한 방법으로 정보의 유입이 가능해짐으로써, 단말기 상에 사용자 정보가 점차 증가하고 그 정보의 종류도 다양해지고 있다. 이로 인해 최근의 모바일 단말기가 분실 또는 도난을 당했을 시 초래할 수 있는 문제는 단말기에 저장된 개인정보를 이용하여 각종 범죄로 악용하는 경우와 사용자 개인정보가 외부로 노출 되어 개인 사생활에 심각한 위협요소로 대두될 수 있다.

2008년 12월말 방송통신위원회의 조사결과에 의하면 모바일 단말기 가입자는 지난해 210만 명이 증가하여 국내 총가입자 수는 4560만 명을 넘어섰다[1]. 가구 수와 비교하면 가구 당 2.73명으로 집계된다.

<표1> 모바일 단말기 분실신고 및 회수량 연도별 현황

(단위 : 대)

구분	2002	2003	2004	2005	2006	2007
신고	67,852	57,785	66,347	118,704	104,945	108,595
회수	66,119	56,923	61,356	105,623	82,758	47,272

한국정보통신산업협회에서 조사한 휴대폰 분실신고와 회수현황은 <표1>과 같이 모바일 단말기의 보급률이 점차적으로 높아짐으로써 그에 따른 분실량도 점점 늘어나고 있으며, 그에 반해 모바일 단말기의 회수량은 줄어들고 있는 추세이다.

본 논문에서는 사용자가 모바일 단말기를 분실 혹은 도난 시 대비할 수 있는 기존 서비스의 문제점을 분석하고, 더욱 안전하게 사용자 정보를 보호할 수 있는 정보 보호 방안과 시스템 설계를 제안한다.

2. A사의 기존 서비스 분석

본 장에서는 현재 이동통신사에서 실시하고 있는 기존 서비스들이 어떤 형식으로 서비스되고 있는지 살펴보고, 그에 따른 서비스의 문제점들을 분석해 본다.

1) A사 서비스 구조

단말기에 저장된 사용자 정보를 이동통신사 서버에 저장함으로써 단말기 소유자에 의한 직접적인 백업 서비스로 웹-하드(Web-Hard) 개념과 유사하며, 현재 상용화 서비스가 이루어지고 있다.

A사 서비스는 사용자가 모바일 단말기를 분실이나 도난 혹은 기기를 변경했을 시 미리 이동통신사의 서버에 수집해둔 사용자 정보를 다운로드하여 사용할 수 있다.

2) A사 서비스의 문제점

주로 개인정보의 중요성을 인식하고 어느 정도의 보안의식을 갖춘 상태의 사용자가 사전에 중요정보를 백업해 둠으로써 정보 유출 사고를 방지하는 목적을 달성할 수 있다. 그러나 이 서비스는 급변하는 현재의 모바일 환경에서 다음과 같은 문제점들을 내포하고 있다.

- 사용자가 능동적으로 정보를 이동통신사의 서버에 비정기적으로 저장하는 개념이기 때문에 가장 최근 백업한 시점부터 분실한 시점까지의 정보는 복구할 수 없다.
- 분실된 모바일 단말기의 사용자 정보를 삭제할 수 있는 방법이 없으므로 사용자 정보가 외부로 유출될 위험이 있다.
- 분실된 모바일 단말기의 사용자 정보 자체를 판독 불가능 상태로 할 수 없으므로 사용자 정보가 노출될 위험이 있다.
- 습득자가 단말기 훼손 등 물리적인 손상을 가했을 시 사용자 정보를 복구시킬 방법이 없다.

이처럼 다수의 문제점들이 발견되었으며 현재 다른 이동통신사들은 SMS(Short Message Service)메시지만을 사용자가 백업해두는 정도의 서비스 외에 사용자 정보를 안전하게 보호할 수 있는 서비스가 없거나 시행을 앞두고 있는 실정으로 사용자 정보 보호에 무방비한 상태라 할 수 있다.

본 논문에서는 사용자가 모바일 단말기를 분실 혹은 도난이 발생하였을 때, 사용자 정보를 안전하게 수집하여 단말기 습득자가 함부로 도용하거나 정보 유출을 불가능하게 하고, 차후 단말기를 회수하거나 타단말기를 구입할 경우 이전 상태로 완벽히 복구할 수 있는 안전한 사용자 정보 보호 시스템을 제안한다.

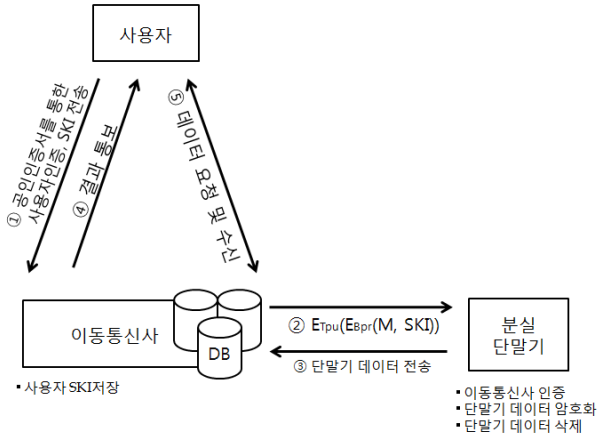
3. 제안 프로세스

본 장에서는 모바일 단말기의 특성을 이용하여 이동통신사를 통한 분실된 단말기의 사용자 정보를 암호화하고 암호화된 사용자 정보를 이동통신사 DB로 전송 후 삭제하는 과정을 통해 사용자 정보를 안전하게 보호하고, 복구할 수 있는 시스템을 제안한다.

이동통신사는 제안 프로세스를 요청한 사용자에게 분실된 단말기의 사용자 정보를 대칭키 암호화 알고리즘으로 암호화할 비밀키(SKI)를 입력받아 공개키 암호화 알고리즘으로 전달받은 비밀키를 안전하게 분실된 단말기에 전달한다. 분실된 단말기는 이동통신사로부터 전달받은 비밀키로 사용자 정보를 암호화하고, 암호화된 사용자 정보는 이동통신사의 DB에 전송한다.

암호화 프로세스를 통해 분실된 단말기의 사용자 정보를 이동통신사의 DB에 보관한 사용자는 분실된 단말기를 회수하거나 다른 단말기로 교체하는 경우 사용자 인증을 통하여 기존에 사용하던 정보를 안전하게 이동통신사로부터 받아 사용할 수 있다.

본 논문에서 제안하는 프로세스를 수행하기 위해서는 수행 전 이동통신사의 공개키와 단말기만의 고유한 개인키를 소유하고 있어야 하며, 세부 내용은 다음과 같다.

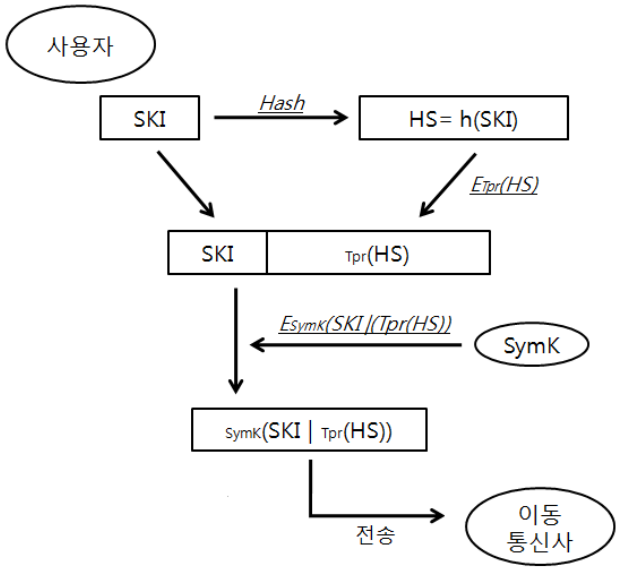


SKI	: 비밀키(secret key) 정보	M	: 단말기 고유번호
Bpr	: 이동통신사 개인키	h	: Hash
Tpu	: 단말기 공개키	E	: Encryption
TS	: Time Stamp		

(그림1) 제안 프로세스 구조

제안하는 (그림1)의 프로세스를 위하여 단말기는 분실되기 전 이동통신사의 제안 프로세스 서비스 신청 등을 통해 이동통신사의 공개키와 단말기만의 고유한 개인키를 부여받아야 한다.

① 사용자는 단말기 분실 후 이동통신사의 홈페이지에 분실된 단말기의 정보 암호화를 요청함으로써 프로세스가 시작하며, 사용자 인증을 위하여 이동통신사에 공인인증서와 함께 비밀키(Secret Key Information; SKI)를 발송한다.



SKI : 비밀키(secret key) 정보 SymK : Symmetric Key

Bpu : 이동통신사 공개키 Tpr : 사용자 개인키

(그림2) SKI 인증 프로토콜 구조

비밀키(SKI)에 대한 무결성과 기밀성을 보장하고 제안 프로세스를 요청하였던 사실에 대하여 부인봉쇄(Non-repudiation)를 위한 메커니즘을 포함한다. SKI 인증 프로토콜은 (그림2)와 같으며 세부사항은 다음과 같다.

- 사용자가 입력한 SKI의 해쉬값 HS=h(SKI)를 사용자의 개인키로 디지털 서명하여 SKI에 병합한다.
- SKI와 사용자의 개인키로 디지털 서명된 결과값을 병합한 데이터를 사용자와 이동통신사의 비밀키(Symk)로 대칭키 암호화 알고리즘을 사용하여 암호화한다.
- 비밀키(SymK)는 사전에 사용자와 이동통신사만이 알고 있는 키 값으로서, 이동통신사는 사전에 사용자와 통신을 통해 해당 키 값을 저장하고 있어야 한다.

이동통신사는 사용자의 개인키로 디지털 서명된 SKI의 해쉬값(Tpr(HS))을 사용자 공개키로 검증하여 사용자의 SKI 발송 부인을 봉쇄할 수 있고, 전달받은 SKI를 사용자와 동일한 해쉬 알고리즘으로 해쉬하여 전달받은 해쉬값 HS와 비교를 통하여 SKI에 대한 무결성을 보장할 수 있다. 또한 비밀키(SymK)로 SKI를 대칭키 암호화 알고리즘으로 암호화하여 SKI에 대한 기밀성을 보장한다.

(그림1)의 ① 과정을 종료하면 이동통신사는 사용자에게 전달받은 SKI를 외부 혹은 내부에서의 해킹을 통해 이동통신사의 DB에 저장된 SKI가 유출될 수 있으므로 SKI를 해쉬한 값을 DB에 저장한다.

② 이동통신사는 분실된 단말기의 사용자 정보를 암호화하기 위하여 암호화 요청 프로토콜을 분실된 단말기에 전송하며, 암호화 요청 시 다음과 같은 두 가지 조건이 만족되어야 한다.

우선 정당한 사용자를 접근하지 못하게 하려는 목적을 지닌 제 3자가 이동통신사임을 가장하여 단말기의 정보를 암호화하려는 공격(Masquerade Attack)으로부터 저항성을 지녀야 한다. 따라서 이동통신사는 단말기의 사용자 정보를 암호화하기 위해서 암호화 요청 프로토콜에 정당한 이동통신사의 요청임을 포함할 필요가 있다. 그리고 단말기의 사용자 정보를 암호화할 비밀키(SKI)의 기밀성의 보장이다.

두 가지 요소를 고려한 암호화 요청 프로토콜의 구성은 다음과 같다.

- 제 3자가 이동통신사로 가장하는 공격에 대하여 저항하기 위해 이동통신사의 개인키로 단말기가 인지할 수 있는 단말기 고유 정보와 SKI를 병합하여 이동통신사의 개인키로 서명한다.
- 이동통신사의 개인키로 서명된 정보의 기밀성을 보장하기 위해 단말기의 공개키로 암호화한다.

③ 단말기 내에서 사용자 정보의 암호화 과정이 종료되면 단말기는 암호화된 정보를 이동통신사의 DB로 전송한다. 암호화된 정보의 전송이 완료되면 단말기 내의 사용자 정보를 모두 삭제한다.

④ 분실된 단말기로부터 암호화된 사용자 정보를 모두 수집한 이동통신사는 사용자에게 수행결과를 알림으로써 암호화 과정을 종료하게 된다.

⑤ 암호화 과정이 모두 종료되어 이동통신사의 DB에 사용자 정보가 수집되면 사용자는 원하는 시기에 인증서를 이용하여 사용자 인증 후에 이동통신사에 요청하여, 사용자 정보를 전송 받아 사용할 수 있다.

4. 분석 및 비교

본 장에서는 제안한 모바일 단말기에서의 안전한 사용자 정보 보호 시스템과 이동통신사의 상용화 중인 서비스의 시스템을 분석 및 비교하며, 그 결과는 <표2>와 같다.

<표2> 제안 프로세스와 A사 서비스 간의 비교 분석

비교분석 항목	A사	제안
단말기 내 사용자 정보 수집	○	○
단말기 변경 시 사용자 정보 이동	○	○
물리적 파손 시 사용자 정보 복구	△	○
단말기 회수 시 사용자 정보 복구	△	○
사용자 정보 외부 유출 방지	X	○
단말기 상에서 사용자 정보 노출 방지	X	○

두 프로세스 모두 단말기 내의 사용자 정보를 수집할 방법과 단말기 변경 시 사용자 정보를 이동할 방법은 갖추어져 있다. 그러나 A사의 경우 가장 최근 백업한 시점부터 분실 혹은 도난 되었을 때까지의 사용자 정보는 수집할 수 없는 단점을 가지고 있다.

그리고 A사 서비스의 가장 큰 문제점은 사용자 정보를 미리 수집은 해두었지만 단말기를 분실 혹은 도난 되었을 경우 그 단말기에 사용자 정보는 여전히 남아있다는 점이다. 따라서 단순히 사용자 정보를 수집해 두는 것 뿐만 아니라 그 단말기의 모든 사용자 정보 자체를 최소 판독 불가능 상태로 만들거나 모든 사용자 정보를 삭제 해두는 것이 가장 안전한 방법이라 할 수 있겠다.

제안하는 프로세스는 타 서비스와 비교하여 모든 점에서 개선된 것을 볼 수 있고, 분실된 시점에서부터 모든 사용자 정보를 완벽히 복구할 수 있으며, 물리적인 레벨에서도 제안 시스템은 사용자 정보를 안전하게 수집 한 뒤 단말기에 저장된 정보를 삭제함으로써 파손되어도 복구할 수 있는 대비책이 마련되어 있는 장점이 있다.

5. 결론

모바일 단말기 분실 시 사용자 정보를 보호하는 서비스들은 지금까지 유용하게 사용되어 왔지만 현 세대의 모바일에서는 그에 맞는 보안 대책이 필요하다.

본 논문에서 제안한 방식은 분실된 단말기내의 사용자 정보를 이동통신사를 통하여 원격 제어하게 되며, 암호화, 전송, 삭제의 과정을 통하여 사용자의 정보를 보호하기 위해 설계되었다. 과제로는 이동통신사와 분실 혹은 도난 된 모바일 단말기 간의 상호인증 부분에서의 더욱 안전하고 효율적인 모듈과 이동통신사를 통해 내부 유출이나 기타 해킹 등을 고려하여 모바일 단말기에서 전달되어 저장되어진 사용자 정보를 더욱 안전하게 키를 관리할 수 있는 모듈의 추가 적용이 이루어져야 한다.

참고문헌

[1] 문은자, '유,무선 가입자 통계 현황', 방송통신위원회, 2008년 12월

[2] FIPS PUB 186-2, 'Digital Signature Standard(DSS)', 2000년 1월

[3] 박현아 외, '모바일 환경에서의 개인정보 위협 분석 연구', 정보보호학회지, 제17권 제4호, 2007년 8월

[4] T. Aura, 'Strategies against replay attacks.' In Proceedings of the 10th IEEE Computer Society Foundations Workshop, pages 59 - 68, Rockport, MA, June 1997. IEEE Computer Society Press