제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

스마트폰 환경에서 개인정보 보안 기법

정민경, 최옥경, 예홍진
아주대학교 대학원 지식정보보안학과
e-mail: jeongmk0106@ajou.ac.kr, okchoi@ajou.ac.kr, hjyeh@ajou.ac.kr

Personalized Private Information Security Method on Smartphone.

MinKyoung Jeong, Okkyung Choi, HongJin Yeh
Dept. of Knowledge Information Security, Graduate School of Ajou University

요 약

최근 개인이 작성한 글과 사진, 동영상 등의 자료를 시간과 장소에 따라 저장 할 수 있는 라이프로그 서비스들이 증가하고 있다. 이러한 정보들은 개인의 일상생활을 기록하는 것으로 민감한 프라이버시임에도 불구하고 관리에 취약하다. 스마트폰 환경에서 데이터를 저장하기 위해 SQLite를 이용하고, 이를 암호화하기 위한 방안으로 SEE와 SQLCipher가 있지만 전체 데이터를 암호화하는 방식으로 중요하지 않은 데이터까지 암호화하여 저장한다. 본 논문은 개인 정보 보호를 위한 방안으로 SQLite에서 SEED 암호를 이용하여 주요한 개인 정보를 컬럼 단위로 암호화한다. 즉 라이프로그 데이터를 개인 프라이버시 중요도에 따라 분류하고, 분류된 데이터 중에서 중요한 데이터만 선택적으로 암복호화 함으로써 기존 데이터 암호화 방식에 비해 암복호화에 소모되는 연산 시간을 감소시키고 라이프로그 데이터의 개인 정보 보안을 강화시키고자 한다.

1. 서론

최근 모바일 기기가 급격히 발전함에 따라 주로 PC환경에서 서비스되던 라이프로그가 스마트폰에서도 서비스되고 있다. 라이프로그란 디지털 기기를 이용하여 글, 사진, 동영상 등의 일상생활에서 경험하는 모든 정보를 기록할 수 있는 기술이다[1]. 이러한 라이프로그는 언제 어디서나 원하는 내용을 기록하고 쉽게 꺼내볼 수 있으며, 타인과 공유할 수 있다.

그러나 이러한 정보들은 개인의 일상생활을 기록하는 것으로 사생활 보호라는 측면에서 민감할 수 있지만 관리에는 취약하다.

개인의 생활 정보를 수집하기 위한 플랫폼 기술[2]은 다양하지만, 본 논문에서는 스마트폰으로 제한하기로 한다.

스마트폰 환경에서 데이터를 저장하기 위해 SQLite를 이용하는 방법이 있지만 SQLite에 기본적으로 암호화를 지원하지 않는다[3]. 지난해 스마트폰에 저장된 이메일 비밀번호가 평문 상태로 저장되어 SQLite viewer를 통해 볼 수 있어 논란이 있었다[4]. 최근 애플이 사용자의 위치 정보를 무단으로 수집해서 논란이 있었고, SQLite로 작성된 해당 파일은 암호화되어 있지 않았다[5]. 또한 SQLite 비할당 영역에 삭제된 레코드가 잔존하는 경우 레코드가 복원되는 것이 연구를 통해 확인되었다[6].

본 논문의 구성은 다음과 같다. 먼저 2장 관련연구에서 SQLite와 현재 SQLite를 암호화하기 위한 방법들에 대해 기술하고, SEED 암호알고리즘에 대해 알아본다. 3장에서 스마트폰 환경에서 SEED 암호를 이용한 개인정보 관리 시스템을 설계한다. 마지막으로 결론과 향후 연구 방향을 제시한다.

2. 관련연구

2.1 SQLite

스마트폰 환경에서 데이터를 저장하기 위한 방법 중 하나는 SQLite를 이용하는 것이다. SQLite의 특징은 다음과 같다[3].

- 별도의 설정이나 관리가 필요 없다.
- public domain으로 어떤 목적으로든 사용이 가능하다.
- 크로스 플랫폼을 지원한다.
- 빠르고 가벼우며, 높은 신뢰성을 보여준다.
- 일반적인 디스크 파일에 데이터를 저장한다.

그러나 앞서 말하였듯이 SQLite는 기본적으로 암호화 기능을 지원하지 않아 그대로 사용하게 되면 개인 정보의 보안이 취약해진다.

이를 보완하기 위해 SQLite를 암호화하기 위한 방안으로 SEE[7]와 SQLCipher[8]가 있다.

2.2 SEE

SEE는 SQLite Encryption Extension의 약자로 저작권에 상관없이 누구나 사용할 수 있는 SQLite에 데이터베이스 파일을 읽고 쓰기 위해 추가한 상용 프로그램이다. SEE는 암호알고리즘으로 RC4, AES-128 [OFB, CCM], AES-256[OFB]가 제공된다. 각 데이터베이스 파일은 자체 암호키를 가질 수 있으며, 데이터베이스 파일 자체를 암호화한다.

2.3 SQLCipher

SQLCipher는 Zetetic에서 만들어진 오픈소스이며, 어느 플랫폼에서나 동작한다[8]. 암호 알고리즘으로 AES-256 CBC를 제공하며, 전체 데이터베이스를 암·복호화한다.

지금까지의 특징을 간략히 정리하면 [표1]과 같다.

<표 1> SEE와 SQLCipher의 비교

	암호화 기능		비용
SQLite	없음	-	-
SEE	RC4, AES-128[OFB, CCM] , AES-256[OFB]	Full Database Encryption	상용 US $2000
SQLCipher	AES-256[CBC]	Full Database Encryption	오픈 소스

2.4 SEED

블록 암호 알고리즘은 데이터의 기밀성 기능을 제공하기 위한 핵심기술로, 안전성과 효율성을 고려하여 개발된 국내 암호 알고리즘으로 SEED가 있다[9][10].

SEED는 크게 다음과 같은 특성을 가진다[11].

· 16라운드의 Feistel 구조
· 128비트 입출력 데이터 블록 크기
· 4개의 8×8 S박스
· XOR 연산과 모듈러 2^{32} 연산

[표2]와 같이 SEED의 암복호화 속도는 대략 DES와 비슷하지만 키 스케쥴링은 4배 가까이 빠른 편이다.

<표 2> 블록 암호알고리즘들의 성능 비교

알고리즘명	라운드 키 생성	암복호화
DES	1606 cycles = 8.03 μsec	432 cycles/ 8 bytes = 28.97 Mbps
3DES	4704 cycles = 23.52 μsec	1133 cycles/ 8 bytes = 9.38 Mbps
RC5	1594 cycles = 7.97 μsec	140 cycles/ 8 bytes = 89.40 Mbps
SAFER	8150 cycles = 40.75 μsec	571 cycles/ 8 bytes = 21.90 Mbps
Blowfish	142770 cycles = 713.85 μsec	262 cycles/ 8 bytes = 47.66 Mbps
CAST	1124 cycles = 5.62 μsec	349 cycles/ 8 bytes = 35.82 Mbps
IDEA	13266 cycles = 66.33 μsec	516 cycles/ 8 bytes = 24.25 Mbps
SEED	411 cycles = 2.06 μsec	870 cycles/16 bytes = 28.00 Mbps

3. 제안하는 개인정보관리 시스템 설계

3.1 설계 방안

스마트폰을 통해 라이프로그 데이터를 수집하고 저장한다. 본 논문에서는 일정 관리를 위한 라이프로그 데이터로 가정한다.

이때 수집되는 데이터 중요도를 다음과 같이 정의한다.

· Major Privacy : 외부에 공개되면 안 되는 개인의 민감하고 중요한 데이터.
· Minor Privacy : 개인 정보가 포함이 안 된 사소한 데이터.

데이터를 분류하는 이유는 Minor Privacy는 암호화 하지 않고 Major Privacy만 암호화하여, 중요한 데이터에 대해서 안전성을 보장하면서 전체적인 성능은 높이기 위해서이다.

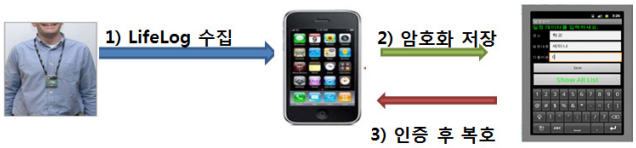
전체적인 구조는 [그림1]과 같이 수집한 라이프로그 데이터를 저장하고, Major Privacy를 128-SEED(CBC)로 암호화 한 후 데이터베이스에 저장한다.

데이터 암호화를 위한 알고리즘으로 SEED를 선정한 이유는 다음과 같다.

SEED의 키 생성 알고리즘은 암복호화시 암호키로부터 필요한 라운드키를 간단히 계산할 수 있도록 설계되어 기본적으로 모든 라운드 키를 저장할 수 없는 제한된 자원을 갖는 장치에서도 효율적으로 이용할 수 있다[9].

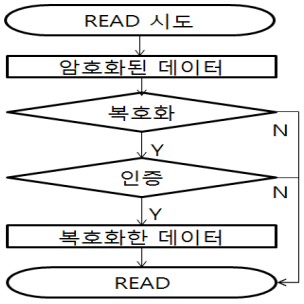
AES는 SPN 구조로 복호화시 별도의 복호화 모듈이 필요한 반면, SEED는 Feistel 구조로 별도의 복호화 모듈이 필요치 않다는 장점이 있다.

SEED는 AES 등과 함께 ISO/IEC 표준으로 제정되었으며, mVoIP, 전자우편, TLS, IPSec 표준으로 채택된 바 있다. SEED를 개발한 KISA에서는 9개 분야에서 22건의 국제 표준화를 추진하고 있으며, IPTV, 클라우드 등 최근 등장한 서비스에 SEED를 적용하기 위한 표준화 활동을 하고 있다[13].



(그림1) 개인정보관리 시스템

저장된 데이터를 읽기 위한 단계는 [그림2]와 같다. 기본적으로 중요 컬럼은 암호화된 상태로 데이터를 읽을 수 있다. 평문 상태의 전체 데이터를 읽고자 한다면 인증 단계를 통과하여야 한다. 전체 평문 데이터가 필요할 때 복호화하게 되는데 이 경우에만 인증을 함으로써 수행시간을 단축한다. 인증을 거쳐 복호화시 본인이 아닌 경우에는 암호화된 상태의 데이터만 읽도록 한다.



(그림2) 데이터 읽기 단계

3.2 데이터베이스 설계

[표2]는 사용자가 일정을 추가하면 schedule_info 테이블에 일정 정보가 입력된다. 날짜, 시간, 장소, 참석자, 일정내용, 지출비용, 메모 필드 중에서 Major Privacy만 선택적으로 암·복호화 할 수 있다.

중요한 데이터를 Major Privacy로 분류하고 암호화하는 기준은 개인이 느끼는 데이터의 민감도가 각각 다르기 때문에 데이터 저장시 개인이 직접 암호화 유무를 결정하도록 한다.

<표 2> 일정 정보 테이블 (schedule_info)

필드명	타입	내용
Num	Integer(pk)	번호
Date	Timestamp	날짜
Time	Timestamp	시간
Location	Text	장소
Attendee	Text	참석자
Content	Text	일정내용
Cost	Integer	지출비용
Memo	Text	메모

[표3]은 Major Privacy와 Minor Privacy를 분류하기 위한 Privacy_info 테이블이다. Privacy 필드는 Major Privacy와 Minor Privacy에 따라 1과 0으로 설정한다. FieldName과 [표2]에서의 필드명을 매칭하여 Privacy에 따라 암호화 여부를 결정한다.

<표 3> 프라이버시 테이블 (Privacy_info)

필드명	타입	내용
Num	Integer(pk)	번호
FieldName	Text	암호화 할 필드명
Privacy	Boolean	암호화 유무

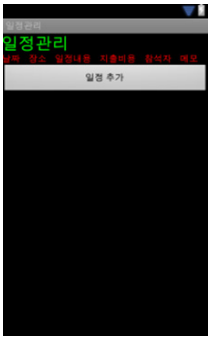
3.3 결과 화면

사용자는 처음 App 실행시 인증용 비밀번호를 등록한다. 개인의 선호도에 따라 암호화하고자 하는 각 필드명의 체크박스를 선택한다.

사용자는 [그림3]과 같이 데이터 수집을 위해 일정 데이터를 입력하고 저장한다. 암호화 유무를 식별하기 위한 체크박스는 비활성화 된다.

저장된 데이터는 [그림4] 데이터베이스 Viewer로 확인할 수 있으며, 일정 데이터 추가가 가능하다.

(그림3) 데이터 수집



(그림4) Viewer

4. 결론

모바일 컴퓨팅 기기가 발전함에 따라 기존에 PC에서 서비스되던 라이프로그가 스마트폰 환경에서도 서비스가 가능해졌다.

스마트폰에 수집되고 저장된 많은 데이터를 관리하기위해 SQLite 데이터베이스가 필요하고, SQLite에서 암호화가 필요한 이유와 방법들을 알아보았다.

본 논문에서는 전체 데이터베이스를 암호화하는 기존 방식에 비해 데이터의 중요도에 따른 선택적 암호화를 하는 방식을 제안하였다. 따라서 본 논문의 제안방식은 기존 DB 암호화 방식에 비해 암복호화 연산에 드는 시간을 줄이고, 저장되는 데이터 공간의 낭비를 줄여 효율적으로 라이프로그 데이터를 관리할 수 있을 것으로 기대된다.

향후 연구방향은 제안한 개인정보관리 시스템 설계를 토대로 안드로이드 환경에서 구현을 하고, 기존의 SEE, SQLCipher와의 성능비교를 통한 효율성 분석을 하고자 한다.

참고문헌

[1] AR Doherty, AF Smeaton, “Automatically augmenting lifelog events using pervasively generated content from millions of people”, Sensors, pp.1423-1446, 2010.

[2] 배창석, 이원혜, “퍼스널 라이프로그 및 기억력 강화 기술”, 한국정보기술학회, 한국정보기술학회지, 제7권 제1호 2009.12, page(s): 15-24

[3] Features of SQLite, [online] http://www.hwaci.com/sw/sqlite/features.html.

[4] 안드로이드, 혹시 내 이메일 비밀번호 유출됐니?, [online] http://www.bloter.net/archives/69229, 2011.07.

[5] 애플이 수집한 정보는 무엇?, [online], http://www.ddaily.co.kr/news/news_view.php?uid=77127, 2011.04.

[6] 전상준, 변근덕, 방제완, 이근기, 이상진, “SQLite 데이터베이스의 비 할당 영역에 잔존하는 삭제된 레코드 복구 기법”, 한국정보보호학회, 정보보호학회논문지, 제21권 제3호 2011.6, page(s): 143-154

[7] Features of SEE, [online], http://www.hwaci.com/sw/sqlite/see.html

[8] Features of SQLcipher, [online], http://sqlcipher.net/design.

[9] 한국정보보호진흥원, 128비트 블록암호 알고리즘 (SEED) 개발 및 분석 보고서, 2009.

[10] 박정희, “SEED 암호 알고리즘을 이용한 데이터베이스 칼럼 단위 암호화에 관한 연구”, 성균관대학교, 2006.

[11] 이종일, “암호 알고리즘 SEED와 ARIA의 비교”, 서강대학교, 2010.

[12] RFC4009(The SEED Encryption Algorithm), [online], http://tools.ietf.org/html/rfc4009

[13] 국산 암호기술 SEED, VoIP 보안 국제표준 채택, [online], http://www.datanet.co.kr/news/articleView.html? idxno=51206, 2010.09.