情報保護學會論文誌
第 23 卷 第 1 號, 2013. 2

스마트폰 메신저 어플리케이션에서의 개인정보보호에 관한 연구*

강 성 훈,[1†] 김 승 주[2‡]
[1]고려대학교 정보보호대학원, [2]고려대학교 사이버국방학과/정보보호대학원

Study on the personal Information Retrieval of Smartphone Messenger Service*

Sunghoon Kang,[1†] Seungjoo Kim[2‡]
[1]Center for Information Security Technologies(CIST), Korea University
[2]Department of Cyber Defense/Center for Information Security Technologies(CIST), Korea University

요 약

세계적으로 스마트폰 이용자의 수가 증가하고, 다양한 종류의 스마트폰 어플리케이션들이 개발, 배포되고 있다. 특히, 소셜 네트워크 서비스(이하 SNS)가 가장 많이 개발, 배포되는 분야 중 하나이다. 다양한 형태의 SNS 중 커뮤니케이션 중심의 SNS의 경우 거의 모든 스마트폰 이용자들이 이용하고 있다. 스마트폰 메신저 어플리케이션은 커뮤니케이션 중심의 SNS를 이용하기 위한 어플리케이션이다. 이 어플리케이션은 서비스 탈퇴, 기기변경 등과 같은 회원관리 기능을 제공한다. 서비스 이용자가 회원 관리 기능을 사용할 경우 기존의 이용자 데이터는 완전히 삭제되어야 한다. 이러한 완전 삭제 기능이 정상적으로 동작하지 않을 경우 이용자의 정보가 유출될 수 있다. 이용자의 정보가 유출될 경우 피싱과 같은 피해를 당할 수 있어 문제가 된다. 특히, 스마트폰 메신저 어플리케이션의 경우 대화 내용과 같은 프라이버시를 침해당할 수 있는 정보까지 포함되어 있어 유출시 문제는 더 심각하다. 본 논문에서는 대표적인 스마트폰 메신저 어플리케이션이 제공하는 회원관리 기능의 개인정보보호법 부합여부를 분석하고, 이용자의 개인정보 및 프라이버시를 보호하는 방법에 대해 법적, 기술적 조치에 대한 해결책을 제시한다.

ABSTRACT

The recent increase in smartphone usage has ignited the development of new applications which have changed the way of living in this internet era in the world. Almost all users which have smartphone have used many kinds of applications for lots of part. Especially, Social Network Service is the most popular part for smartphone users. The greater part of smartphone users take messenger service for smartphone. This kinds of applications provide to manage as deactivation of user or change of device. When users take to manage their information, their information would be deleted securely. If secure deletion didn't work correctly and released, their personal information can be easily abused to by others through various means such as internet phishing. In this paper, we analysis that the messenger application's management function keeps on the Personal Information Protection Act and suggest to prevent legally and technically for user's personal information and privacy.

Keywords: Privacy, Personal Information, Smartphone Messenger Service, Social Network Service

접수일(2012년 9월 4일), 수정일(1차: 2012년 11월 16일, 2차: 2012년 12월 12일), 게재확정일(2013년 1월 9일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT연구센터육성 지원사업의 연구결과로 수행되었음 (NIPA-2012-H0301-12-3007)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT연구센터육성 지원사업의 연구결과로 수행되었음 (NIPA-2012-H0301-12-4008)
† 주저자, korhoon@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr

I. 서 론

2012년 8월 중순을 기점으로 국내 스마트폰 이용자가 3000만 명을 넘어섰고, 전 세계적으로도 계속 증가하고 있다. 스마트폰 이용자의 증가와 함께 이용자의 편의를 위한 어플리케이션들 역시 다양하게 개발 및 배포되고 있다. 스마트폰의 보급과 함께 소셜 네트워크 서비스 (SNS)가 가장 많이 활용되고 있다. 특히, Short Message Service (SMS)와 Multimedia Message Service (MMS)를 대체하는 커뮤니케이션 중심의 SNS를 제공하는 어플리케이션들이 많이 등장하였다. K사의 K 어플리케이션 과 N사의 L 어플리케이션은 국내뿐만 아니라 전 세계에 걸쳐 6000만 명이 넘는 이용자를 확보하였다. 이렇게 널리 사용되는 스마트폰 메신저 어플리케이션들 중에는 이용자의 편의를 위해 이용자가 소유하고 있는 연락처나 E-mail 주소와 같은 개인정보들을 기반으로 자동으로 대화 상대를 찾아주는 기능을 가진 것들이 많이 있다. 이런 종류의 어플리케이션들은 이용자에게 2가지 경우에 대해 삭제 기능을 제공한다. 첫 번째 경우는 이용자가 어플리케이션의 불필요하여 탈퇴 옵션을 사용할 때와 두 번째 경우는 기기변경 등으로 인해 새로운 기기에 이용자 인증을 받을 때이다. 이런 스마트폰 메신저 어플리케이션은 한 개의 휴대전화번호 당 한 개의 계정만을 가질 수 있다. 따라서 서비스 제공자는 서비스 이용자가 새로운 기기에서 이용자 인증을 했을 경우 기존 휴대기기에서는 더 이상 사용을 할 수 없게 하는 서비스를 제공하며 이용자는 이에 동의를 했을 경우에만 새로운 기기에서 서비스를 이용할 수 있다. 만약, 이와 같은 기능을 이용한 후 이용자의 데이터가 완전한 삭제가 이루어지지 않는다면 개인정보 유출 및 사생활 침해의 가능성이 매우 높다. 완전한 삭제가 이루어지지 않은 채 이러한 정보들이 빠져나간다면 피싱과 같은 범죄에도 악용될 수 있어 관리가 매우 중요하다. 최근에는 개인정보유출과 프라이버시 침해사고는 점차 대형화, 지능화, 다양화되고 있는 추세이며, 2011년 3월 개인정보보호법 제정과 함께 시행령과 시행규칙이 공표된 이후 국민들의 관심과 의식 수준도 점차 높아지고 있다[1][2]. 행정안전부는 서비스 이용자의 개인정보보호 및 기업의 이해를 돕기 위해 지침과 가이드라인을 제공한다[3]. 서비스 제공자들은 지침과 가이드라인을 활용하여 이용자의 데이터를 보호하기 위해 최선의 노력을 다하고 있다. 그럼에도 불구하고 2011년 8월 방송통신위원회가 애플을 상대로 위치정보 보호 및 이용에 관한 법률 위반으로 과태료가 부과된 것처럼, 법이나 정보통신서비스 제공자가 미처 준비하지 못하거나 간과하고 있는 부분들이 존재한다.

본 논문에서는 전 세계적으로 가장 널리 사용하고 있는 스마트폰 OS인 Google의 안드로이드를 기반으로 제작된 대한민국 대표 커뮤니케이션 중심의 소셜 네트워크 서비스 제공자인 K사의 K 어플리케이션(이하 K앱)과 D사의 M 어플리케이션(이하 M앱)의 회원관리 기능의 개인정보보호법 준수 여부와 함께 개선점을 찾아보고, 이용자의 개인정보 및 프라이버시를 보호하는 법적, 기술적 조치 방안을 제안한다.

II. 관련연구

2.1 개인정보의 관리

대부분의 스마트폰 어플리케이션들은 개인정보보호법, 통신비밀보호법, 전기통신사업법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 같이 정보통신서비스제공자가 준수하여야 할 관련 법령상의 개인정보보호규정을 준수하여야 하며, 관련 법령에 의거한 개인정보취급방침을 정하여 이용자의 권익 보호에 최선을 다해야한다. 개인정보취급방침을 세우고 이를 명시화하여 이용자에게 알리고 이용자가 원하면 언제든지 쉽게 열람할 수 있게 해야 한다[4][5][표 1]

또한, 대부분의 스마트폰 어플리케이션들은 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법), 제4장 개인정보의 보호, 제2절 개인정보

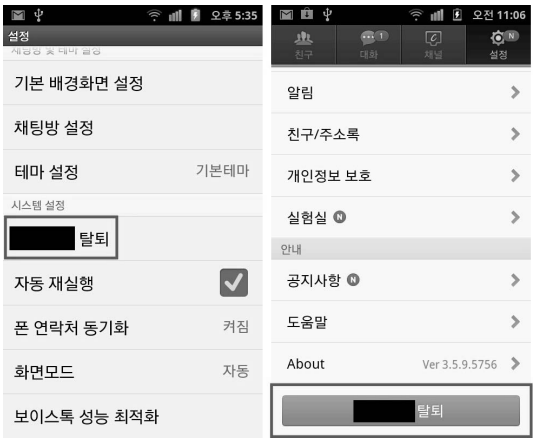
[표 1] 개인정보취급방침 목록

개인정보취급방침
1. 수집하는 개인정보 항목 및 수집방법
2. 개인정보의 수집 및 이용목적
3. 개인정보의 보유 및 이용기간
4. 개인정보의 파기절차 및 방법
5. 개인정보의 공유 및 제공
6. 수집한 개인정보의 위탁
7. 이용자 및 법정대리인의 권리와 그 행사방법
8. 개인정보 자동수집 장치의 설치, 운영 및 그 거부에 관한 사항
9. 개인정보의 기술적, 관리적 보호 대책
10. 개인정보에 관한 민원서비스
11. 부칙

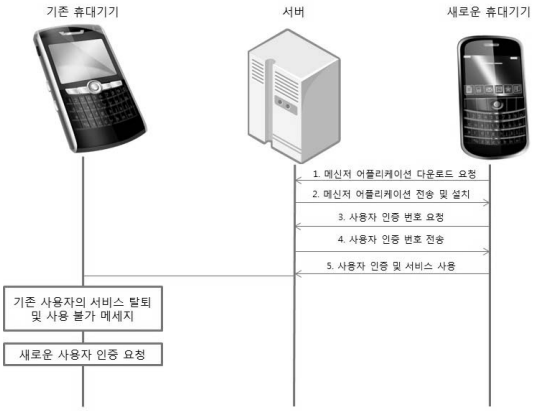
의 관리 및 파기 등에 의하여 이용자의 개인정보보호를 위해 수집된 정보들을 보호하고 그 목적이 달성되었을 때에는 폐기해야 한다. 즉, 서비스 제공자는 지침에 따라 서비스 제공자가 보유한 서버에 대해서는 법을 잘 준수하여 이용자의 정보를 보호하고 있다. 하지만, 법에는 이용자의 단말기에 대한 조치를 명확하게 명시하지 않고 있다.

2.2 테스트 환경

대부분의 스마트폰 어플리케이션은 이용자가 더 이상 사용을 원치 않을 경우에 탈퇴를 할 수 있는 항목을 가지고 있다. K앱과 M앱도 역시 이와 같은 기능을 가지고 있다. 〔그림 1〕



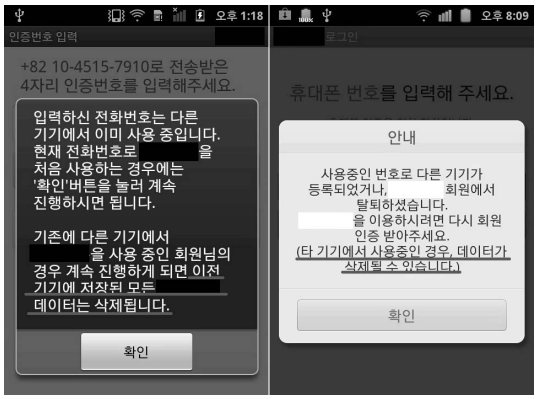
〔그림 1〕 어플리케이션에서 제공하는 탈퇴 기능



〔그림 2〕 새로운 기기에서 이용자 인증 시

본 논문은 안드로이드 O/S를 사용하는 S전자의 갤럭시 S모델에 K앱(버전 3.3.3)과 M앱(버전 3.5.9)을 설치하여 3가지 경우에 대해 연구한다. 첫 번째, 정상적으로 사용하였을 때, 획득 가능한 정보를 수집, 분석한다. 두 번째, 정상적으로 사용하다 이용자 본의의 의지로 탈퇴했을 경우, 획득 가능한 정보를 수집, 분석한다. 세 번째, 다양한 이유로 인하여 새로운 기기로 기기변경을 하여 새로운 기기에 이용자 인증을 한 후, 기존 기기에서 획득 가능한 정보를 수집, 분석한다.〔그림 2〕 또한, 〔그림 2〕의 1부터 5까지의 절차는 메신저 어플리케이션을 사용하기 위한 일반적인 이용자 인증 절차이다.

스마트폰 메신저 어플리케이션은 정책적으로 한 개의 휴대전화번호 당 한 개의 계정만을 가질 수 있다. 따라서 서비스 제공자는 서비스 이용자가 새로운 기기에서 이용자 인증을 했을 경우 기존 휴대기기에서는 더 이상 사용을 할 수 없게 하는 서비스를 제공하며 이용자는 이에 동의를 했을 경우에만 새로운 기기에서 서비스를 이용할 수 있다. 즉, 〔그림 3〕의 안내 메시지처럼 새로운 기기를 사용하게 된다면 다른 어떤 기기에도 이용자의 데이터는 남아있으면 안 되며, 이에 대해 이용자도 충분히 인지하고 있다.



〔그림 3〕 기존 기기에 저장된 데이터의 사용 불가에 대한 안내 메세지

III. 이용자 정보 획득 및 어플리케이션별 데이터 분석

3.1 데이터 획득 방법

스마트폰의 설치된 어플리케이션을 분석하기 위해서는 우선적으로 스마트폰에 저장되어 있는 데이터를

추출해야 한다. 데이터를 추출하기 위해서는 안드로이드 운영체제의 취약점을 공격하여 관리가 권한을 얻는 루팅을 해야 한다. 리눅스 기반으로 제작된 안드로이드 운영체제는 리눅스와 동일한 유저 권한 체계를 사용한다. 리눅스의 관리자 권한인 "root"는 안드로이드 운영체제에서도 동일하게 존재한다. 하지만 권한 상승을 할 수 있는 "su" 명령어가 존재하지 않아 취약점을 이용하여 일시적으로 권한을 상승시켜 관리자 권한을 얻는 것이다. 루틴의 방법으로는 크게 3가지 방법이 있다. 첫 번째 방법은 커널 취약점을 이용한 관리자 권한 획득이다. 취약점을 공격하는 exploit을 실행하여 일시적으로 관리자 권한을 얻은 뒤 "su"명령어를 삽입하여 필요시 마다 관리자 권한을 얻는 방법이다. 하지만 이 방법은 안드로이드의 버전에 따라 취약점이 보완되거나 스마트폰 기종에 따라 실패할 확률이 존재한다. 두 번째 방법은 펌웨어 업데이트를 통한 방식이다. 루팅된 혹은 루팅 가능한 ROM 이미지를 단말기에 업로드 하여 기존 ROM을 덮어 씌워 관리자 권한을 획득한다. 이러한 방식의 단점은 ROM의 버전이나 기종에 따라 ROM을 만들어야한다. 세 번째 방법은 부트로더 수정을 통한 업데이트 방식이다. 일반적으로 부트로더 업데이트에 사용되는 "update.zip"파일 안에 스크립트를 삽입하여 부트로더를 업데이트한다. 이 때 "su"명령어를 삽입한다. 이 방식의 단점은 루팅 전의 상태로 되돌릴 수 없다는 것이다.[6] 본 연구에서는 삼성전자에서 출시된 스마트폰 갤럭시 S에 루팅된 ROM을 기존의 ROM에 덮어씌우는 방식을 사용한다[7]. 또한, 현재 사용 중인 기기로부터 어플리케이션의 데이터를 추출하면 SQLite 형태의 데이터베이스 파일로 구성되어 있다. 또한, 해당 파일들은 아래 경로에 저장된다. [표 2]

[표 2] 데이터베이스 경로

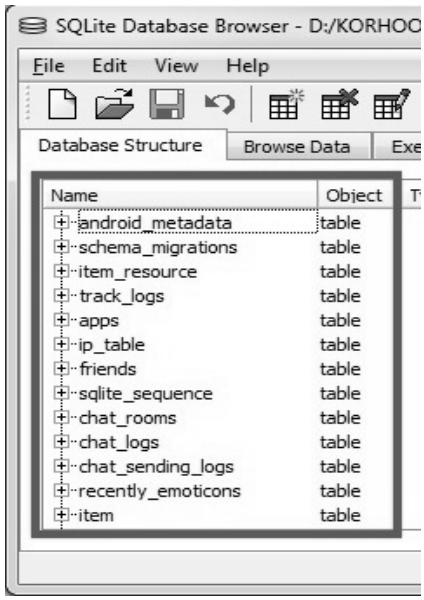
어플리케이션 명	경로
K앱	/data/data/com.△△△△△.talk/databases/
M앱	/data/data/net.△△△△.android.air/databases/

3.2 어플리케이션별 데이터 분석

3.2.1 K앱

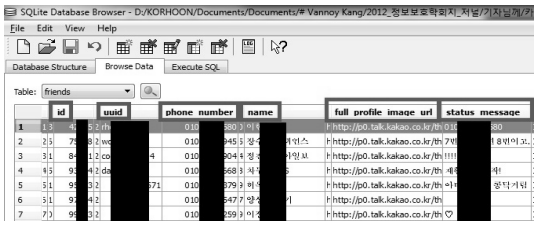
3.2.1.1 사용 중인 기기의 개인정보 존재 여부 분석

현재 사용 중인 기기로부터 어플리케이션의 데이터를 추출하면 SQLite 형태의 데이터베이스 파일로 구성되어 있다. K앱의 데이터베이스 파일은 /data/data/com.△△△△△.talk/databases/의 경로에 △△△△△.Talk.db라는 SQLite 형태의 파일로 존재한다. 이 파일은 11개(android_metadata, schem a_migrations, item_resource, track_logs, apps, ip_table, friends, sqlite_sequence, chat_rooms, chat_logs, chat_sending_logs)의 테이블로 구성되어있다. [그림 4]



[그림 4] △△△△△.Talk.db Table List

11개의 테이블 중에서 friends 테이블에는 [그림 5]와 같이 이용자가 가지고 있는 데이터베이스에서 주어지는 고유한 값(id), 대화 상대의 ID(uuid), 연락처(phone_number), 이용자가 등록한 사진 URL(profile) 및 개인 메시지(status_message)와 같은 개인 정보가 저장되어 있다[그림 5].



[그림 5] friends Table의 필드 값

또한, chat_rooms, chat_logs 테이블에는 이용자가 주고받았던 메시지(message)와 상대방에 대한 정보(user_id)가 저장되어 있다.

3.2.1.2 탈퇴 후의 개인정보 존재 여부 분석

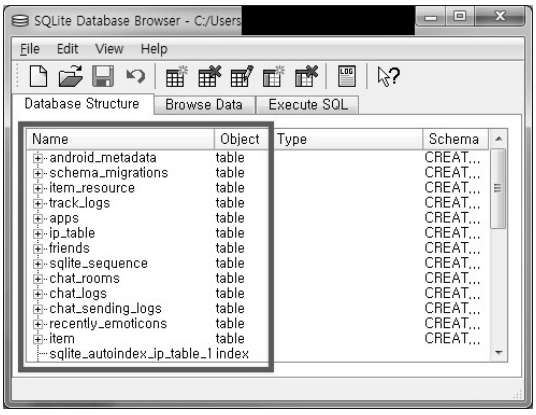
이용자가 기기 변경이나 혹은 서비스의 불편함으로 인해 탈퇴 기능을 이용하여 스스로 탈퇴를 할 경우에도 기기에는 탈퇴 전과 동일한 경로에 동일한 파일명으로 존재한다. 하지만, 데이터베이스 파일의 레코드들을 삭제하는 것을 확인할 수 있다. 또한, SQLite의 레코드 복구를 시도했을 때에도, 원래 값이 아닌 무의미한 값이나 null 값으로 복구됨을 확인했다.〔8〕〔그림 6〕

	A	B	C	D	E	F	G	H	I
1	Status	_id	contact_id	id	type	uuid	phone_nu	raw_phon	name
2	Deleted		35	NULL	NULL	NULL	NULL	NULL	NULL
3	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL
4	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL
5	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL
6	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL
7	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL
8	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL
9	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL
10	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL
11	Deleted		NULL	NULL	0	NULL	NULL	NULL	NULL

〔그림 6〕 SQLite 레코드 복구 툴을 사용하여 복구된 레코드

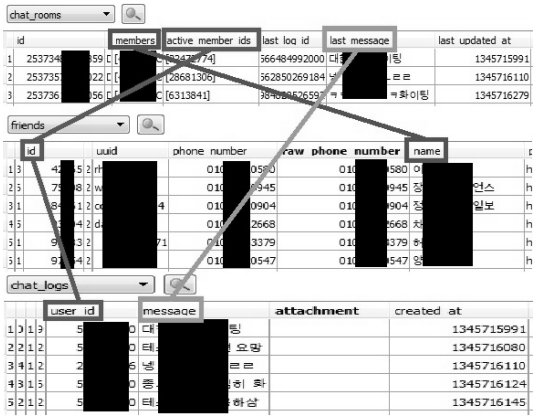
3.2.1.3 기기 변경 시 개인정보 존재 여부 분석

이용자가 기기의 분실이나 도난 혹은 기기 변경으로 인해 더 이상 기존 기기의 사용을 원치 않고, 새로운 기기에서 이용자 인증을 받았을 경우, 기존 기기의 데이터를 분석하였다. 새로운 기기에서 인증을 할 경우 기존 기기의 데이터는 사용할 수 없다는 메시지를 확인할 수 있다.〔그림 3〕 하지만, 이 경우에도 동일한 경로에 동일한 파일명으로 데이터베이스 파일이 존재한다. 즉, 기존 기기로부터 어플리케이션의 데이터를 추출하면, 탈퇴 전과 동일한 정보를 포함한 파일을 얻을 수 있다.〔그림 7〕



〔그림 7〕 △△△△△.Talk.db Table List (기기변경 후)

만약, 〔그림 8〕과 같이 friends, chat_rooms, chat_logs 테이블들에 저장된 필드 값들을 비교한다면 쉽게 타인의 개인정보 및 과거 대화내용을 획득할 수 있다.



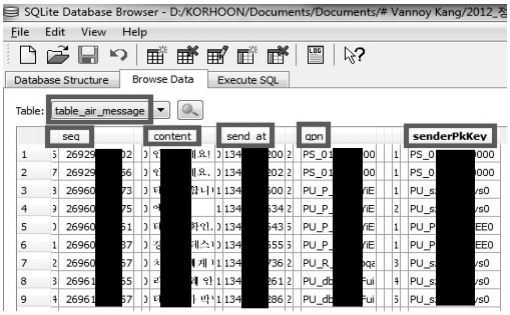
〔그림 8〕 friends, chat logs, chat rooms 테이블 비교 (기기변경 후)

3.2.2 M앱

3.2.2.1 사용 중인 기기의 개인정보 존재 여부 분석

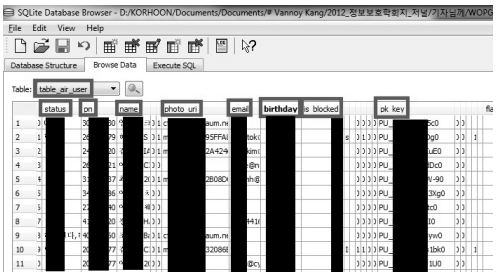
〔표 1〕 M앱의 데이터베이스 파일은/data/data/net.△△△△.android.air/databases/의 경로에 다음과 같은 air.db, MFKJHUDISW, SIFY- DHSCKE, WOPGYDUIXV 4개의 SQLite 형태의 파일로 존재한다. 4개의 파일 중에서 air.db, SIFYDHSCKE파일에는 데이터베이스의 메타정보와 메신저 어플리케이션에서 사용가능한 스티커 및 이모티콘의 정보가 들어있다. MFKJHUDISW파일 table_air_messege 테이블에는 이용자가 주고받았던 메시지 내용과 상대방 식별값 등이 저장되어 있다.〔그림 9〕

또한, WOPGYDUIXV파일은 android_metadata,table_air_user, sqlite_sequence 테이블로 구성되어 있다. 이 중 table_air_user 테이블에는 이용자가 가지고 있던 대화 상대식별 번호(pk_key), 상대의 연락처(pn), 이름(name), 이메일(email),



〔그림 9〕 table_air_message Table

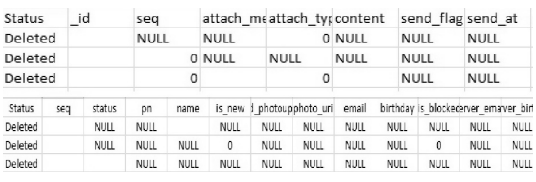
생일(birthday), 상태 메시지(status)와 같은 개인정보가 저장되어 있다.〔그림 10〕



〔그림 10〕 table_air_user Table

3.2.2.2 탈퇴 후의 개인정보 존재 여부 분석

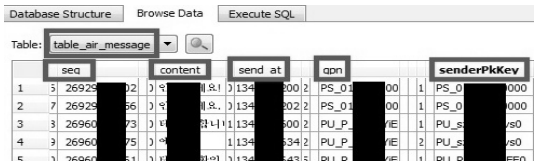
이용자가 기기 변경이나 혹은 서비스의 불편함으로 인해 스스로 탈퇴를 할 경우에도 기기에는 탈퇴 전과 동일한 경로에 동일한 파일명으로 존재한다. 하지만, 데이터베이스 파일의 레코드들을 삭제하는 것을 확인할 수 있다. 또한, SQLite의 레코드 복구를 시도했을 때에도, 원래 값이 아닌 null 값으로 복구됨을 확인했다.〔8〕〔그림 11〕



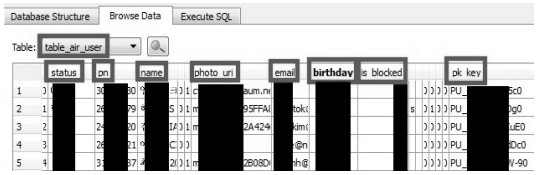
〔그림 11〕 SQLite 레코드 복구 툴을 사용하여 복구된 레코드

3.2.2.3 기기 변경 시 개인정보 존재 여부 분석

이용자가 기기의 분실이나 도난 혹은 기기 변경으로 인해 기존 기기를 더 이상 사용을 원치 않고, 새로운 기기에서 이용자 인증을 받았을 경우, 기존 기기의 데이터를 분석하였다. 이 경우에도 기존 기기의 데이터는 모두 삭제된다고 서비스 제공자의 안내 메시지를 확인할 수 있지만〔그림 3〕, 동일한 경로에 동일한 파일이 존재하는 것을 확인할 수 있다. 즉, 기존 기기로부터 어플리케이션의 데이터를 추출하면 2개의 SQLite파일MFKJHUDISW, WOPGYDUIXV)을 획득하여 분석하면, 탈퇴 전과 동일한 정보를 포함하고 있음을 확인할 수 있다.〔그림 12〕〔그림13〕

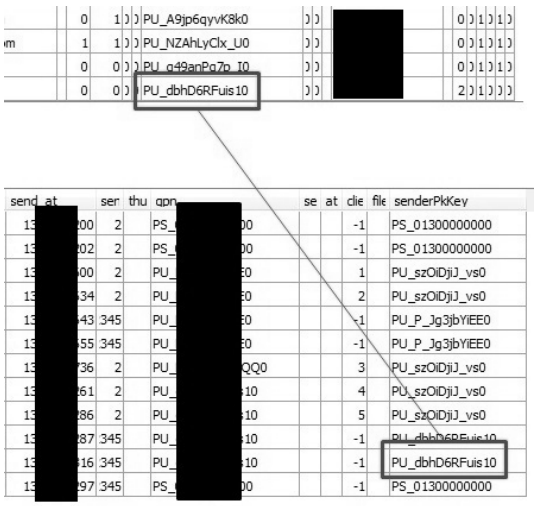


〔그림 12〕 table_air_user Table



〔그림 13〕 table_air_user Table

만약, 〔그림 14〕과 같이 두 테이블에 저장된 필드 값들을 비교한다면, 쉽게 타인의 정보와 함께 대화 내용도 확인이 가능하다.



〔그림 14〕 table_air_messege, table_air_user 테이블 비교 (기기변경 후)

IV. 이용자 정보보호 방안

법적 정보보호 방안

2011년 8월 방송통신위원회가 애플을 상대로 위치정보 보호 및 이용에 관한 법률 위반으로 과태료를 부과한 후, 법을 제정할 당시 예상하지 못한 부분에 대해 법 개정을 준비 중이라고 했듯이, 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률도 이용자 단말기 보호와 같이 입법 당시 예상하지 못한 부분에 대해 보완이 필요하다. 행정안전부는 개인정보보호법의 이해를 돕기 위해 가이드라인과 지침을 제공한다. 클라우드 서비스나 SNS와 같은 새로운 서비스를 뉴미디어 서비스라고 칭하고 서비스 제공자와 서비스 이용자가 준수하여야 할 뉴미디어 서비스 개인정보보호 가이드라인을 제공한다[3][표 3][표 4]. 이 가이드라인은 서비스 제공자와 서비스 이용자로 나누어 보호해야할 대상과 의무에 대해 기술했다. 서비스 제동자는 서비스 제공자의 서버와 어플리케이션 간의 통신 시에는 암호화 통신을 해야 하고, 서버에 저장되는 데이터는 암호화를 해야 한다고 명시되어 있고, 서비스 제공자가 보호해야할 대상을 서비스 제공자의 서버에 저장된 데이터로 한정시켰다. 그리고 스마트폰에 저장된 중요 정보는 서비스 이용자가 스스로 안전하게 관리하라고 명시되어 있다. 스마트폰 어플리케이션에 저장된 데이터들은 어플리케이션을 설치할 때 생성되고 어플리케이션이 관리하는 데이터베이스에 저장된다. 따라서 어플리케이션 내부에 저장된 데이터 역시 서비스 제공자가 처리해야 할 정보이며, 이를 보호해야 할 책임이 따른다. 하지만 행정안전부에서 제공하는 가이드라인에서 위와 같이 서비스 제공자에게도 보호의 책임이 있는 정보에 대해 서비스 이용자만의 책임으로 명시 되어 있으므로 개선되어야 한다. 즉, 가이드라인은 스마트폰에 저장된 데이터를 단순히 이용자가 보호해야할 대상으로 한정 짓는 것이 아니라, 개인정보처리자도 보호를 해야 할 대상으로 확대하고, 이를 보호하기 위한 기술적 조치가 필요하다고 수정되어야 한다.

〔표 3〕 개인정보보호 가이드라인 - 서비스 제공자

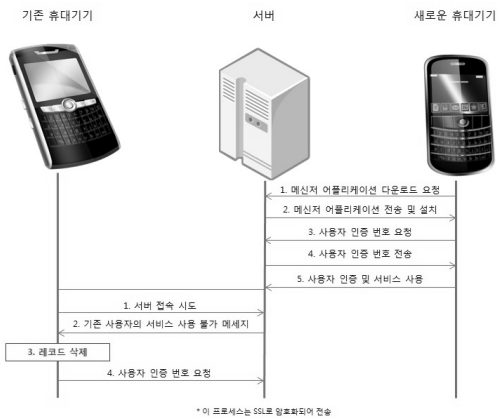
개인정보보호 가이드라인	서비스 제공자	
처리단계	구분	내용
개인정보 수집	1. 방침수립	서비스 제공자는 서비스 이용자가 쉽게 확인할 수 있도록 개인정보 처리(취급) 방침을 수립하고 공개하여 함
	2. 책임자 지정	서비스 제공자는 개인정보 보호(관리)책임자를 지정하여 이용자의 개인정보 보호와 피해구제를 위한 체계를 마련하여야 함
	3. 수집원칙	서비스 제공자는 서비스 제공에 필요한 최소한의 정보를 수집하여야하며, 수집 시 정보주체의 동의를 받아야 함
개인정보 이용	4.목적 내 이용 · 제공	서비스 제공자는 개인정보 수집 시 이용자로부터 동의 받은 범위 내에서 이용하거나 제3자에게 제공하여야 함
개인정보 제공	5.개인정보 위탁	서비스 제공자는 이용자의 개인정보를 위탁하는 경우 사전에 위탁 목적, 범위, 대상 등에 대해 반드시 고지하고 관련 법령에 따라 동의 받아야 함
개인정보 이용	6. 개인정보 공개설정	서비스 제공자는 회원가입 시 이용자의 개인정보 공개범위를 서비스 이용을 위해 필요한 최소한의 정보를 제외하고는 공개안함으로 하며, 이용자가 공개범위를 단계별로 설정할 수 있는 기능 제공을 권장함
개인정보 파기	7. 개인정보 파기	서비스 제공자는 개인정보의 처리목적을 달성하였거나 서비스 이용자가 개인정보 파기를 요청한 경우 관련 법령에 따라 지체 없이 개인정보를 파기하여야 함
개인정보 이용	8. 보호조치	서비스 제공자는 개인정보의 안전성 확보를 위하여 기술적 · 관리적 · 물리적 보호조치를 이행하여야 함
개인정보 제공	9.국외이전	서비스 제공자는 개인정보를 국외로 이전하는 경우 국내의 관련 법 의무사항을 준수하여야 함
	10. 양도 시 고지의무	서비스 제공자는 서비스의 전부 또는 일부의 양도 · 합병 등으로 개인정보를 다른 사람에게 이전하는 경우 정보주체에게 관련 내용을 고지하여야 함
정보주체 권리강화	11. 유출신고	서비스 제공자는 개인정보 유출사고 발생 시 이용자에게 고지하고 유출피해 최소화를 위해 노력하여야 함

〔표 4〕 개인정보보호 가이드라인 - 서비스 이용자

개인정보보호 가이드라인	서비스 이용자	
처리단계	구분	내용
개인정보 수집	1. 정보제공 최소화	서비스 이용자는 개인정보 제공 시 불특정 다수에게 열람될 수 있다는 점을 유의하여 서비스에 필요한 최소한의 개인정보를 제공하여야 함
	2. 보호조치 확인	서비스 이용자는 서비스에 가입할 때에는 개인정보 처리방침 등을 통해 개인정보 보호를 위한 적절한 조치가 이행되고 있는지 확인하여야 함
개인정보 이용	3. 공개범위 최소화	서비스 이용자는 불필요한 개인정보 노출을 최소화하기 위해 개인정보 공개범위를 설정하여야 함
	4. 정기적 업데이트	서비스 이용자는 모바일 앱 및 보안프로그램을 정기적으로 업데이트 하여야 함
	5. 중요정보의 안전한 관리	서비스 이용자는 클라우드 컴퓨팅서비스, 스마트폰 등에 중요 정보 저장 시 암호화하여 저장하거나 비밀번호를 부여하여 안전하게 관리하여야 함
	6. 기능 비활성화	서비스 이용자는 개인정보 전송 시 유 · 노출 위험이 있는 무선통신서비스나 위치정보서비스는 필요 시 기능을 활성화하여 사용하고, 사용 후에는 기능을 비활성화하여야 함
개인정보 제공	7. 신중한 정보공유	서비스 이용자는 타인의 게시글, 사진정보 등을 공유 시 신중히 검토하여 개인 또는 타인의 개인정보를 보호하여야 함
정보주체 권리강화	8. 아동의 개인정보보호 인식 제고	뉴미디어 서비스를 이용하는 아동의 경우 개인정보 유출방지와 건전한 서비스 사용을 위해 부모의 지속적인 관심이 필요함
	9. 권리보장	서비스 이용자는 뉴미디어 서비스 이용 시 제공한 개인정보에 대한 열람 · 정정 · 삭제 청구권이 보장됨을 인지하고 필요 시 적극적으로 권리를 행사하여야 함
	10. 침해신고	서비스 이용자는 서비스 이용 시 자신의 개인정보가 유출 또는 오 · 남용된 사실을 아는 즉시 신고하여 피해 확산을 방지하여야 함

4.2 기술적 정보보호 방안

〔그림 2〕에서와 같이 현재 기기변경 기능을 이용 시 기존 기기에서의 삭제 과정은 일어나지 않는다. 하지만, 3.2.1.2와 3.2.2.2에서 확인한 바와 같이 서비스 제공자가 제공하는 탈퇴 기능 이용 시 동작하는 데이터 삭제 기능을 기기변경 기능을 사용할 때 제공한다면 기존 기기에 있는 이용자 데이터를 보호할 수 있다. 만약, 기존 기기로 단 한번이라도 서버에 접속이 시도 될 경우 기존 기기의 사용 불가 메시지가 나타날 때, 어플리케이션에 설치된 삭제 기능을 실행시켜 데이터를 삭제시킨다〔그림 15〕. 이 방법은 이미 서비스 제공자가 제공하는 옵션이므로 새롭게 개발을 한다거나 연구가 필요한 기능이 아니므로, 어플리케이션에 쉽게 추가가 가능하다. 하지만, 이 기능은 데이터의 완전 삭제를 보장하지는 않는다. 따라서 데이터의 복구 가능성이 존재하기 때문에 완전한 보호 방안은 아니다. 일반적인 이용자들은 데이터가 삭제되면, 복구는 어렵다고 생각하지만, 데이터 복구 프로그램이나 데이터 포렌식 프로그램들을 사용한다면, 삭제된 데이터의 복구는 가능하다.



〔그림 15〕 새로운 레코드 삭제 프로세스

따라서 안전한 보호를 위해서는 완전 삭제 기능이 제공되어야 한다. 미국 국방부(Department of Defence)와 미국 국가안전보장국(NSA)은 하드 디스크와 플래시 메모리 삭제에 대한 가이드라인을 제공한다〔표 5〕〔표 6〕. 일반적으로 하드 디스크 방식의 저장 매체는 완전 삭제를 위해서 무의미한 데이터를 여러 번 덮어쓰기를 하여 완전 삭제를 구현한다. 따라서

완전 삭제를 비교적 쉽게 구현할 수 있다.

〔표 5〕 하드 디스크 삭제 방법[9]

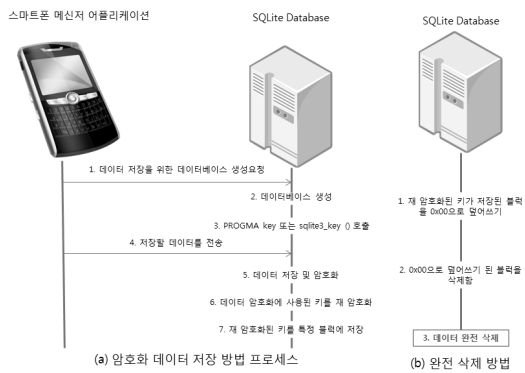
Deletion method	Description
Single pass	Overwrites once with either 0x00, 0xff or pseudo-random data
DoD 5220.22-M	Step 1 : Overwrites with random single value Step 2 : Overwrites with complement of that value Step 3 : Repeats Step 1-2 seven times
NATO standard	Step 1 : Overwrites with 0x00 Step 2 : Overwrites with 0xff Step 3 : Repeats Step 1-2 six times
NSA	Step 1 : Overwrites with 0x00 Step 2 : Overwrites with 0xff Step 3 : Repeats Step 1-2 seven times

하지만, 스마트폰은 NAND 플래시 메모리를 사용하기 때문에 메모리에 쓸 수 있는 횟수가 정해져있다. 하드 디스크의 완전 삭제 방법을 이용하여 USB 플래시 메모리를 완전 삭제한다면 메모리 수명에 치명적인 영향을 미친다.

〔표 6〕 플래시 메모리 데이터 삭제 방법

Deletion method	Description
DoD 5220.22-M (July 1997) [10]	Step 1 : Overwrites with a single character Step 2 : Erase overwritten area
NSA/CSS storage device declassification manual[11]	Step 1 : Overwrites with a known unclassified pattern Step 2 : verify that only the known pattern can be recovered by randomly re-reading

[12]는 DoD와 NSA의 가이드라인과 플래시 메모리의 수명 문제를 고려하여 만든 USB 플래시 메모리 완전 삭제 방법 중 하나이다. 데이터를 암호화하고 그 키들을 다시 암호화 하여 한 개의 블록에서 따로 관리를 하다가 데이터를 삭제할 때 암호화 된 키가 보관된 해당 블록만을 삭제하거나 해당 블록만 덮어쓰기를 하여 데이터의 복구를 어렵게 만드는 방법이다. 이 방법은 DoD와 NSA가 요구하는 모든 데이터의 삭제뿐만 아니라, 덮어쓰는 방법까지 만족시킴과 동시에 쓰기제한 문제도 해결했다. 스마트폰은 NAND 플래시 메모리를 사용하기 때문에 USB 플래시 메모리 완전 삭제 방법은 쉽게 적용이 가능하다. 스마트폰은 하드웨어적인 제약과 경량화로 인해 SQLite와 같은 비교적 가벼운 데이터베이스를 사용한다. [12]가 제안한 방법에 스마트폰에서 사용하는 SQLite의 암호화 기능을 사용하여 암호화를 하여 적용한다면 스마트폰에 적합한 데이터 보호 방법이 된다. 하지만, 최신 버전의 SQLite는 암호화 기능을 제공하지 않는다. 따라서 스마트폰 어플리케이션에 저장된 데이터들을 암호화하려면 써드파티 프로그램을 이용해야한다. 일반적으로 SQLite를 암호화하기 위해 사용되는 프로그램은 오픈소스로 제공되는 SQLCipher이다. SQLCipher는 데이터베이스를 생성하고 OpenSSL과 Xcode Project를 이용하여 데이터베이스를 암호화한다. 데이터베이스를 생성하고, 다른 커맨드나 함수를 호출하기 전에 'PROGMA key' 또는 sqlite3_key() 함수를 호출하면, 이후 생성되는 모든 데이터베이스 정보는 암호화되어 저장된다. 그리고 암호화된 데이터베이스 정보를 불러올 때는 다른 커맨드나 함수를 호출하기 전에 'PROGMA key' 또는 sqlite3_key() 함수를 호출해야 한다[13]. SQLite의 암호화와 USB 플래시 메모리의 완전 삭제 방법을 같이 사용한다면, 스마트폰에 저장된 데이터의 암호화 문제와 완전 삭제 문제를 해결할 수 있고, 이용자의 데이터를 안전하게 보호할 수 있다[그림 16].



〔그림 16〕 스마트폰에 적합한 완전 삭제 방법

V. 결론 및 향후 과제

스마트폰의 시장이 확대됨에 따라, 이용자의 스마트폰 교체 주기도 짧아지고 다양한 어플리케이션들이 개발, 배포 되고 있다. 이용자가 새로운 기기를 구입하는 경우부터 분실이나 도난과 같은 다양한 이유로 스마트폰의 교체 빈번히 발생하고, 기기의 성능향상으로 더 많은 어플리케이션들을 설치하고 사용한다. 우리나라의 법은 서비스 제공자들의 보호 대상을 서비스 제공자의 서버에 저장된 데이터에 대해서만 국한하여 적용하고 있다. 스마트폰이나 어플리케이션에 저장된 데이터 보호는 간과하고 있다. 특히, 이러한 데이터 유출에 대한 위험을 제대로 인식하지 못하고 있고, 이를 막기 위한 방안 역시 거의 없다. 본 논문에서는 스마트폰 메신저 어플리케이션이 제공하는 회원 관리 기능에 대해 법 준수 여부 및 획득 가능한 이용자 정보를 수집, 분석하는 방법에 대해 조사하고, 이용자의 정보를 보호하는 법적, 기술적 방안에 대해서 제시하였다. 향후에는 보다 다양한 어플리케이션에 대한 연구로 확대하고, 논문에서 제시한 이용자 정보보호 방안을 실제로 구현하여 실험까지 확장할 계획이다.

참고문헌

〔1〕 대한민국 국회, "개인정보 보호법," 법률 제 10465호, 2011. 3. 29. 제정

〔2〕 행정안전부, "개인정보 보호법 시행령·시행규칙," 행정안전부, 2011. 9. 공포

〔3〕 행정안전부, "뉴미디어 서비스 개인정보보호 가이드라인," http://www.privacy.go.kr/inf/gdl/selectBoardArticle.do

〔4〕 대한민국 국회, "정보통신망 이용촉진 및 정보보호 등에 관한 법률," 법률 제 11048호, 2011. 9. 15. 공포

〔5〕 대통령령, "정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령," 대통령령 제24102호, 2012. 9. 공포

〔6〕 오정훈, 이상진, "안드로이드 스마트폰 포렌식 분석 방법에 관한 연구," 디지털 포렌식 연구, 9, 2013. 2. 게재 예정

〔7〕 Blog about android phone rooting : Blog of Tegrak, http://pspmaster.tist- ory.com

〔8〕 Sangjun Jeon, Jewan Bang, Keunduck Byun and Sangjin Lee, "A recovery method of deleted record for SQLite database," Personal and Ubiquitous Computing, vol. 16, no. 6, pp. 707-715, August 2012.

〔9〕 J. R. Mallery, "Secure file deletion : Fact or fiction?," GSEC Practical Assignment Version 1.2e, 2006.

〔10〕 National Industrial Security Program Operating Manual, http://www.usaid.gov/policy/ads/500/d522022m.pdf, Jul. 1997.

〔11〕 NSA/CSS Storage Device Declassification Manual, http://nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf, Nov. 2000.

〔12〕 Byunghee Lee, Kyungho Son, Dongho Won, Seungjoo Kim, "Secure Data Deletion for USB Flash Memory," Journal of Information Science and Engineering, vol. 27, no. 3, pp. 993-952, May 2011.

〔13〕 SQLCipher, http://sqlcipher.net/sqlcipher-api/

〈著者紹介〉

강 성 훈 (Sunghoon Kang) 학생회원
2010년 2월: 서원대학교 컴퓨터공학 졸업
2010년 9월: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보증, 정보보호제품 보안성 평가, 디지털 포렌식, Usable Security

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: KISA(舊한국정보보호진흥원) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 정보보호대학원 정교수
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~현재: 대검찰청 디지털수사 자문위원
2007년~2009년: 전자정부 서비스 보안위원회 사이버 침해사고대응 실무위원회 위원
2010년~현재: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: SK커뮤니케이션즈 보안강화 특별자문위원
2012년: 중앙선거관리위원회와 서울시장후보 홈페이지 사이버테러 특별검사 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security