정 보 보 호 학 회 지
제28권 제5호, 2018. 10

스마트폰 백업 데이터 획득 연구 동향

박 명 서*, 김 종 성**

요 약

현대인에게 필수적인 스마트폰에는 통화기록, 문자 메시지, 이메일과 같은 사용자 개인 정보뿐 아니라 사진, 동영상, 문서 등과 같은 미디어 파일이 저장된다. 이러한 스마트폰 데이터는 포렌식 수사 입장에서 중요한 증거로써 사용될 수 있기 때문에 필수적으로 획득해야 하는 데이터이다. 하지만, 스마트폰의 꾸준한 업데이트와 FDE (Full Disk Encryption), FBE(File Based Encryption)과 같은 암호 기능의 적용으로 인해 스마트폰에서 사용자 데이터를 추출하는데 어려움이 있다. 이에 따라 스마트폰에서 사용자 데이터를 추출하는 연구가 지속적으로 수행되고 있으며, 본 논문에서는 그 중 하나인 백업 데이터에서 스마트폰의 데이터를 획득하는 연구 동향에 대해 설명한다.

Ⅰ. 서 론

스마트폰의 사용은 급격히 증가하고 있으며, 스마트폰은 더 이상 통화의 목적으로만 사용되지 않는다. 최신 스마트폰은 데스크탑 이상으로 성능이 향상되어 인터넷 뱅킹, SNS 등 다양한 용도로 사용되고 있으며, 저장장치의 크기도 증가하여 메시지, 연락처, 통화기록뿐 아니라 사진, 동영상, 문서 등의 대용량 데이터를 저장할 수 있다. 스마트폰에는 로그인 정보, 미디어 데이터, 개인정보 등 중요한 정보가 저장되기 때문에 스마트폰의 유실, 고장 등의 예기치 못한 상황에도 문제를 해결할 수 있는 방안이 필요하며, 이에 대한 해결책으로 데이터 백업을 수행할 수 있다. 스마트폰의 백업을 위해 스마트폰 제조사들은 스마트폰 자체의 내부 저장소에 데이터를 백업하거나, Smart Switch(삼성)[1], iTunes(애플)[2], LG Bridge(LG)[3] 등의 백업 프로그램을 이용하여 PC에 데이터를 백업하는 방식을 제공한다. 일반적으로 백업 데이터는 단순 평문 상태로 저장되지 않으며, 제조사별로 상이한 인코딩 또는 암호화 방식을 사용한다. 이는 사용자 데이터를 공격자로부터 보호하는 기능을 제공하지만, 디지털 포렌식에서는 안티 포렌식으로 작용하게 된다. 디지털 포렌식 수사 관점에서 암호화된 백업 데이터는 복호화 없이 디지털 증거로써 활용할 수 없다. 따라서 암호화된 백업 데이터를 디지털 포렌식 수사에 활용 가능한 평문 상태로 획득하기 위해서는 제조사 별 암/복호화 방식에 대한 분석이 선행되어야 하며, 관련 연구가 활발하게 진행되고 있다.

본 논문에서는 기존의 암호화된 스마트폰 백업 데이터 복구 연구에 대해 살펴본다. 본 논문은 총 4장으로 구성되며, 1장은 서론이고, 2장은 일반적인 스마트폰 백업에 사용되는 암/복호화 방식에 대해 설명한다. 3장에서는 삼성, LG, 애플 스마트폰 제조사 별 백업 과정 및 암호화 방식 및 백업 데이터 복구 연구에 대한 기존 결과에 대해 설명하고, 마지막으로 4장에서 향후 연구 제시와 결론을 맺는다.

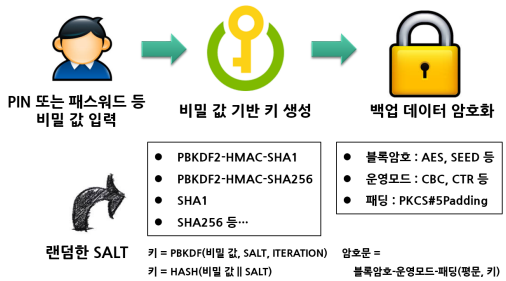
Ⅱ. 스마트폰 백업 데이터의 암/복호화 방식

본 장에서는 스마트폰 데이터의 백업 및 복원 과정에서 사용하는 암/복호화 방식에 대해 설명하고, 키 생성 및 암호 알고리즘을 식별한다.

2.1. 스마트폰 백업 시 암호화 방식

일반적으로 스마트폰 데이터 백업 시 사용자는 선택적으로 PIN (Personal Information Number) 또는 패스

본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 작성되었습니다. (No.2017-0-00344, 최신 모바일 기기에 대한 암호해독 및 포렌식 분석)
* 국민대학교 금융정보보안학과 DF&C Lab. (pms91@kookmin.ac.kr)
** 국민대학교 정보보안암호수학과, 금융정보보안학과 DF&C Lab. (jskim.kookmin.ac.kr)



〔그림 1〕 백업 데이터 암호화 과정

워드와 같은 비밀 값을 입력할 수 있으며, 이를 기반으로 백업 데이터는 암호화 된다(그림 1). 사용자의 비밀 값이 입력되지 않은 경우에는 백업 데이터가 암호화되지 않거나, 백업 프로그램 내에 고정된 값을 비밀 값으로 사용하여 백업 데이터를 암호화 한다.

비밀 값은 백업 데이터를 암호화하기 위한 암호 키를 생성하기 위해 사용된다. 키 생성 알고리즘은 일방향 함수를 사용하며, PBKDF(Password Based Key Derivation Function)와 같은 패스워드 기반의 키 유도 함수나 SHA1, SHA256과 같은 해쉬 함수를 사용한다. 키 생성 알고리즘의 인자는 기본적으로 비밀 값과 고정된 출력을 방지하기 위한 SALT를 사용한다. 특히, PBKDF는 키 스트레칭의 목적으로 반복횟수를 인자로 사용하며, 전수조사로 비밀 값을 복구하는 공격으로부터 내성을 갖도록 해준다. 백업 데이터 암호화에 사용되는 암호 알고리즘은 AES와 같은 블록암호를 사용한다. 또한 블록암호의 블록 길이 이상의 데이터를 암호화하기 위해 사용되는 운영모드로써, CBC나 CTR을 사용하고, 패딩은 PKCS#5Padding 또는 NoPadding을 사용한다.

2.2. 스마트폰 복원 시 복호화 방식

스마트폰 백업 데이터 복원 시 사용자가 암호화를 위해 패스워드를 입력하여 백업했을 경우 복원을 위해서도 동일한 패스워드를 입력해야 한다. 올바른 패스워드를 입력했는지에 대한 검증은 대부분 백업 데이터 내에 인증자를 통해서 수행하게 된다. 따라서 스마트폰 복원 수행 이전에 사용자가 입력한 패스워드를 기반으로 인증자를 생성하고, 이를 백업 데이터 내에 있는 인증자와 비교하여 값이 같으면 올바른 패스워드로 간주하고 복원 과정을 수행하게 된다. 백업 데이터는 블록암호를 사용하여 암호화를 수행했기 때문에 백업 시 사용했던, 암호 키를 복원 시에는 복호 키로 사용하여 백업 데이터를 복호화하면 된다.

Ⅲ. 스마트폰 백업 데이터 획득에 대한 기존 연구

본 장에서는 실제 스마트폰 제조사인 삼성, LG에 대해 2장에서 설명한 백업 데이터 암/복호화가 어떤 방식으로 적용되었는지 기존 연구 결과를 통해 설명한다[4, 5]. 추가적으로 기존의 오픈 소스와 상용도구를 사용한 애플 스마트폰의 암호화된 백업 데이터 추출 방법에 대해 설명한다.

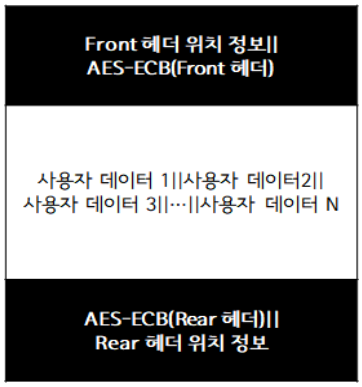
3.1. 삼성 스마트폰-Smart Switch

삼성에서는 삼성 스마트폰 백업 전용 프로그램으로써 Smart Switch를 제공한다. 백업 데이터 암호화 설정은 Smart Switch의 환경 설정에서 선택할 수 있다. 암호화 설정 시에는 스마트폰 상에서 PIN을 입력하게 되며, 이를 기반으로 백업 데이터가 암호화된다. 암호화 미설정 시에는 프로그램 내에 고정된 값을 이용하여 백업 데이터를 암호화 한다. 키 생성 알고리즘은 SHA256, PBE (Password Based Encryption)-SHA256, PBKDF2-HMAC -SHA1을 사용하며, 암호 알고리즘 및 운영모드는 AES-ECB과 AES-CBC를 사용한다. 키 생성 알고리즘과 암호화은 암호화 대상 백업 파일의 확장자에 따라 달리 적용된다.

백업 데이터 복원 시 암호화에 사용된 PIN을 검증하기 위해 백업 데이터 내 인증자를 사용하며, 인증자는 입력한 PIN에 대한 검증 역할을 수행한다. 백업 데이터 내 암호화된 “Manifest.exml” 파일을 입력한 PIN 기반으로 생성된 키를 통해 복호화한 후 내부에 “Enc_level”이라는 문자열이 존재하는지를 확인함으로써 입력한 PIN이 올바른 PIN인지 검증할 수 있다. 여기서 사용된 인증자는 “Enc_level”이 된다.

3.2. LG 스마트폰-LG Bridge

LG 스마트폰 백업을 위해 LG Bridge를 사용한다. LG 스마트폰 백업은 .lbf의 단일 파일 형태로 저장되며, 추가적인 사용자의 비밀 값 입력을 요구하지 않는다.



〔그림 2〕 LG의 lbf 파일 구조

lbf 파일의 구조는 (그림 2)와 같으며, 파일의 앞, 뒤로 헤더가 암호화되어 붙어있고, 중간에 사용자 데이터가 평문 상태로 연접되어 있는 형태이다.

헤더 정보가 없어도 단순 카빙을 통해 사용자 데이터를 추출할 수 있지만, 파일의 이름과 같은 구체적인 정보를 획득할 수 없고, 알려지지 않은 LG 고유의 파일 포맷에 대해서는 카빙을 적용할 수 없다. 따라서, 사용자 데이터 추출은 암호화된 헤더를 복호화하여 이용하는 방법이 가장 효율적이다. 헤더 암호화에 사용된 암호 알고리즘 및 운영모드는 AES-ECB를 사용하며, 암호키는 프로그램 내 고정된 값을 사용한다. 복호화된 헤더는 xml 파일 형태로써, 사용자 데이터의 백업 파일의 이름, 오프셋, 크기 정보를 포함한다. 이를 이용한 사용자 데이터 복구 방법은 기존 카빙 기술과 동일하며, 먼저 헤더를 참조하여 lbf 파일 내의 추출 대상 파일의 오프셋에서 파일 크기만큼 잘라 파일 형태로 추출하고, 파일의 이름을 붙이면 된다.

3.3. Apple 스마트폰-iTunes

Apple 스마트폰은 백업을 수행하기 위해 iTunes를 사용한다. 백업 데이터 암호화 설정은 iTunes의 설정을 통해서 수행할 수 있으며, 암호화 미설정과 달리 계정 암호, 건강 및 HomeKit 데이터가 추가적으로 백업이 된다. 암호화 미설정은 수행하면, 백업 데이터는 평문 상태로 저장된다. 반면에 암호화 설정을 하면 모든 백업 데이터는 암호화되어 저장된다. 백업 데이터 암호화에 사용된 비밀번호는 hashcat[6]이라는 전용 비밀번호 크랙 도구에 Manifest.plist의 BackupKeyBag 노드에 포함된 ver, WPKY, ITER 등의 인자를 파싱하여 대입하여 복구할 수 있다. 비밀번호를 복구를 통해서나 이미 알고 있는 경우에는 해당 비밀번호와 FINALMobile Forensics[7], Elcomsoft Phone Breaker[8]과 같은 상용도구를 이용하여 암호화된 백업 데이터를 복구할 수 있다.

Ⅳ. 결 론

본 논문에서는 스마트폰의 데이터를 획득하기 위한 방법으로 백업 데이터를 활용했던, 기존의 연구 동향에 대해 조사하여 설명하였다. 백업된 데이터 중 특정 중요한 파일들은 인코딩 또는 암호화 되어 저장되기 때문에 이를 디코딩 또는 복호화하여 획득하기 위한 연구가 필요하다. 현재까지 삼성, LG, 애플과 같은 제조사에 대한 백업 데이터 복구 연구는 진행되었으나, Huawei, Xiaomi, Sony와 같은 스마트폰 제조사에 대한 백업 데이터 복구 연구는 진행되지 않았다. 세 제조사도 HiSuite[9], Mi PC Suite[10], Xperia Companion[11]과 같은 백업 프로그램을 제공하며, 백업 데이터를 확인해본 결과 모두 암호화 기능을 제공했다. 따라서, 이를 복구하는 연구가 필요하며, 향후 연구로써 진행할 예정이다.

참 고 문 헌

[1] Smart Switch, http://www.samsung.com/ sec/support/smartswitch

[2] iTunes-Apple, https://www.apple.com/kr/itunes

[3] LG Bridge-LG, http://www.lge.co.kr/lgekor/download-center/downloadCenterList.do.

[4] Myungseo Park, H. Kim. J. Kim, “How to decrypt PIN-Based encrypted backup data of Samsung smartphones”, Digital Investigation, Vol 26, pp. 63-71, 2018

[5] 박명서, 김한기, 김종성, “향상된 LG 스마트폰 백업 데이터 복구 방법 연구”, 디지털 포렌식 연구, 12(1), pp.1-7, 2018

[6] hashcat, advanced password recovery, https://hashcat.net/hashcat/

[7] FINALMobile Forensics, http://www.finaldata.co.kr/mobile/
[8] Elcomsoft Phone Breaker, https://www.elcomsoft.com/eppb.html
[9] HiSuite, https://consumer.huawei.com/minisite/HiSuite_en/
[10] Mi PC Suite, http://pcsuite.mi.com/
[11] Sony-Xperia Companion, https://support.sonymobile.com/kr/xperia- companion/#gref

〈저 자 소 개〉

박 명 서 (Park, Myungseo)

2015년 2월 : 국민대학교 금융정보보안학과 석사
2014년 12월~2017년 2월 : 국가보안기술연구소 연구원
2017년 3월~현재 : 국민대학교 박사과정
관심분야 : 정보보호, 암호 알고리즘, 디지털 포렌식

김 종 성 (Kim, Jongsung)

2006년 11월 : K. U. Leuven, ESAT/SCD-COSIC 정보보호 공학박사
2007년 2월 : 고려대학교 정보보호대학원 공학박사
2007년 3월~2009 8월 : 고려대학교 정보보호기술연구센터 연구교수
2009년 9월~2013년 2월 : 경남대학교 e-비즈니스학과 조교수
2013년 3월~현재 : 국민대학교 정보보안암호수학과 부교수
2013년 3월~현재 : 국민대학교 금융정보보안학과 부교수
관심분야 : 정보보호, 암호 알고리즘, 디지털 포렌식