스마트폰 백업 데이터 획득 연구 동향

박영서, 김종성. 정보보호학회지, 28(5), 2018.

IT융합공학부 윤세영

유투브 주소: https://youtu.be/hMV6muTCKhw

서론

스마트폰 백업 데이터의 암/복호화 방식

스마트폰 제조사별 백업 데이터 획득에 대한 기존 연구

향후 연구 제시와 결론

서론

백업 데이터는 단순 평문 상태로 저장 되지 않음
제조사 별로 상이한 인코딩 또는 암호화 방식을 제공 함

스마트폰 백업 데이터의 암/복호화 방식

- **스마트폰 백업 시 암호화 방식**

〔그림 1〕 백업 데이터 암호화 과정

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 비[illegible] 된 출력을 방지하기 위한 SALT를 사용[illegible] PBKDF는 키 스트레칭의 목적으로 반복횟[illegible] 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.

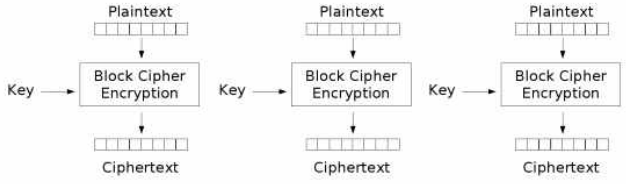
PBKDF

CBC, CTR

ECB, CBC, CTR

- **ECB (Electronic CodeBook, 전자 코드북)**

- 블록 암호 운용 방식 중 가장 간단한 구조를 가지며, 암호화하려는 메시지를 여러 블록으로 나누어 각각 암호화하는 방식이다.



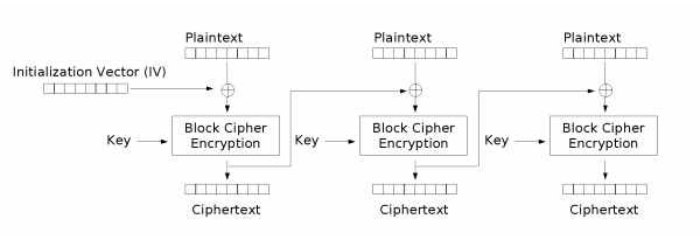
Electronic Codebook (ECB) mode encryption

ECB, CBC, CTR

- CBC (Cipher-Block Chaining, 암호 블록체인 방식)

- 각 블록은 이전 블록의 암호화 값과 XOR 된다.

- 첫 블록의 경우에는 초기화 벡터를 사용한다. (초기화 벡터의 경우 출력 결과가 항상 같기 때문에 매 암호화 마다 다른 초기화 벡터를 사용해야 한다.)



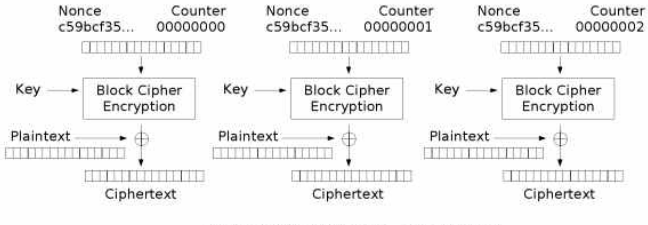
Cipher Block Chaining (CBC) mode encryption

ECB, CBC, CTR

- CTR (Counter, 카운터)

- 블록 암호를 스트림 암호로 바꾸는 구조를 가진다.

- 각 블록마다 현재 블록이 몇 번째인지 값을 얻어, 그 숫자와 난수를 결합하여 블록 암호의 입력으로 사용한다. 이후 각 블록 암호에서 연속적인 난수를 얻은 다음, 암호화하려는 문자열과 XOR한다.



Counter (CTR) mode encryption

PBKDF

- PBKDF(Password-Based Key Derivation Function)이란?

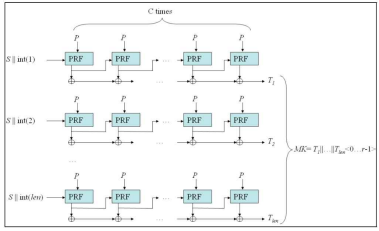
- 패스워드를 사용해 키를 유도하기 위해 사용하는 함수
- 사용자 패스워드에 해시함수, Salt, 반복 횟수 등을 지정하여 패스워드에 대한 Digest를 생성하는 방식

DIGEST = (PRF, Password, Salt, 반복 횟수, dkLen)

PRF = 의사 난수 함수

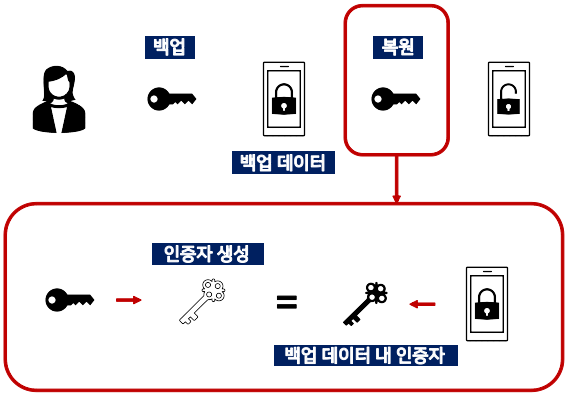
Salt = 난수

dkLen = 추출(유도)하고 싶은 키의 길이 값



스마트폰 백업 데이터의 암/복호화 방식

- 스마트폰 복원 시 복호화 방식



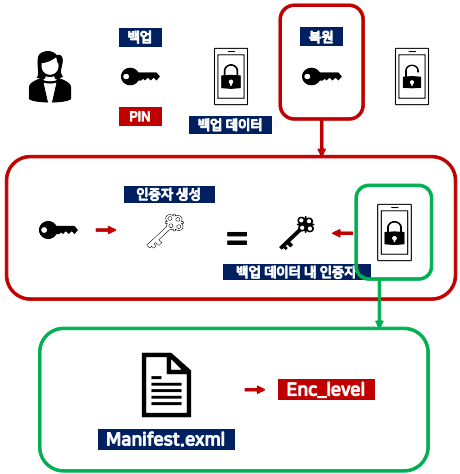
스마트폰 제조사별 백업 데이터 획득에 대한 기존 연구

- 삼성 스마트폰: Smart Switch

Smart Switch

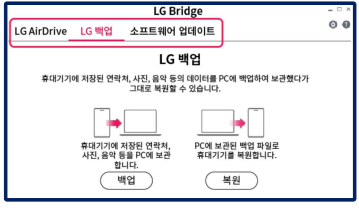
스마트 스위치로
빠르고 쉽게
데이터 이동하기

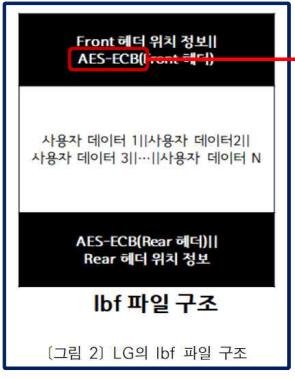
SHA256
PBE - SHA256
AES-ECB
AES-CBC



스마트폰 제조사별 백업 데이터 획득에 대한 기존 연구

- **LG 스마트폰: LG Bridge**





〔그림 2〕 LG의 lbf 파일 구조

Data Carving

• Data Carving이란?

- 파일 시스템의 정보 없이 비할당 영역에서 파일을 추출하는 기법

• 고려할 요소

- 카빙 소요 시간: 복구 시 사용하는 검색 알고리즘 및 처리 부분 최적화
- 데이터 정확성: 파일의 특성들을 조합한 정확성 향상

항목	연속적 데이터 카빙	비연속적 데이터 카빙
개념	데이터가 저장 매체의 연속된 공간에 저장된 경우 수행하는 기법	데이터 단편화가 발생하여 저장매체 여러 부분에 조각나 저장된 경우 수행하는 기법
주요 기법	헤더/푸터, 램 슬랙 카빙, 파일 크기 카빙, 파일 검증 카빙	파일 조각화 비율, 시그니처 기반 기법, 엔트로피 이용 기법

https://itpenote.tistory.com/460

스마트폰 제조사별 백업 데이터 획득에 대한 기존 연구

- **Apple 스마트폰: iTunes** → 2019년 서비스 종료

hashcat
advanced password recovery

BackupKeyBag
- ver
- WPKY
- ITER

- FINALMobile Forensics
- Elcomsoft Phone Breaker

향후 연구 제시와 결론

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.

Q & A