Android Forensics: Lock Protection

Posquit0

pbj92220@postech.ac.kr

http://posquit0.com

I Can Do It!!

개요

- 안드로이드의 **내부적인 Lock**에 대해 알아보고 안전성을 확인한다.

- 어플리케이션에서 사용하는 자체적인 Lock에 대해 알아본다.

INDEX

Android Lock

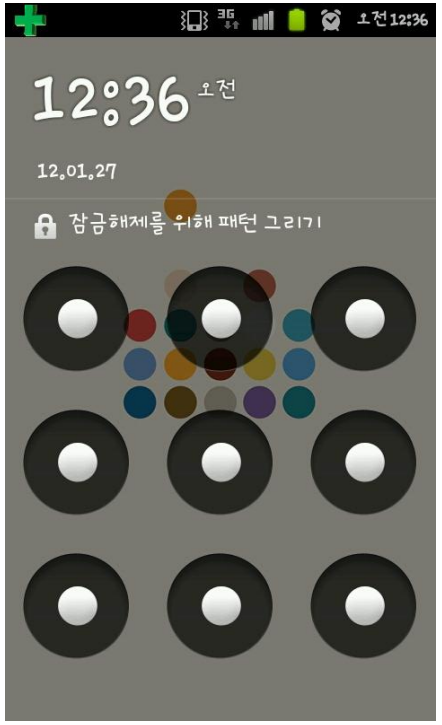
Lock 이란?

- **잠금(Lock)**
  - 제 3자가 특정 컨텐츠에 접근하지 못하도록 특수한 장치를 해두는 것
    - ✓ 자물쇠
    - ✓ 도어락
    - ✓ **안드로이드의 패턴 잠금**
    - ✓ **안드로이드의 PIN / Password 잠금**
    - ✓ **어플리케이션에서 제공하는 잠금**
      - **KAKAO TALK's Lock**
    - ✓ … …

Pattern Lock

패턴 잠금이란?

- Android 기반 스마트 폰의 화면 잠금을 풀기 위해 사용하는 새로운 방법
- 9개의 점 중에서 **최소 4개 이상의 점을 연결**하여 특정 패턴을 사용
  - 각 점에 숫자를 대입하면 이해하기 쉽다.
- **경우의 수가 한정**
  - 같은 점을 두 번 이상 지나지 못한다.
  - 총 ***895,824의 경우의 수***가 존재한다.



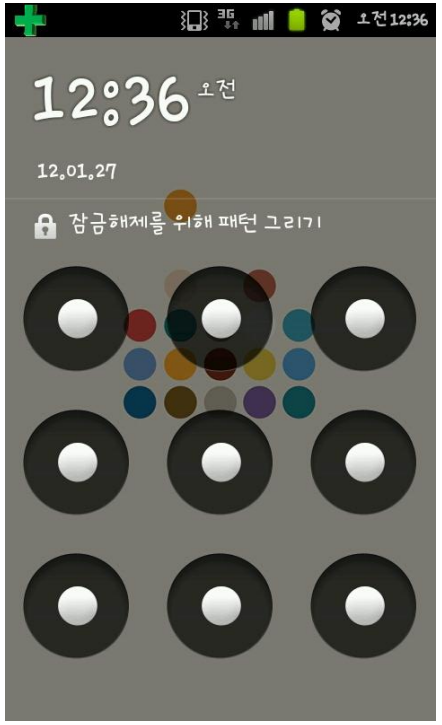
gesture.key

```
0000h: FF EC 1E 70 D1 13 B0 B9 6C 7E 6C B2 B3 34 60 E2  ÿì.pÑ.°¹l~l²³4`â
0010h: 44 07 A9 6E                                      D.©n
```

- Android 상의 Pattern Lock에 관한 데이터 파일
- **/data/system/ 폴더**에 존재
- Lock Sequence가 **SHA-1 Hash 알고리즘**으로 암호화되어 저장
  - Original Sequence로 되돌릴 수 있는 역함수가 존재하지 않는다.
    - ✓ *복호화가 불가능할까?*
- 895,824 라는 적은 경우의 수를 가짐
  - ***레인보우 테이블을 작성하여 복호화가 가능!***

Rainbow table

- 895,824개의 경우의 수에 대한 해시 테이블 작성
- Original Sequence는 ***0x00~0x08 의 헥스 값***으로 구성



Oxygen-forensic's Rainbow Table

```
1234;00 01 02 03;A02A05B025B928C039CF1AE7E8EE04E7C190C0DB
1235;00 01 02 04;6E36A9BFACF6C4637D64042B11CB78BFDDAF8BF3
1236;00 01 02 05;101B2A675E9FB9546336D5B9EF70418B594184F4
1237;00 01 02 06;30F26B9825EA6F2EF6DBF6A88959774314D83F65
```

- 레인보우 테이블의 구성
  - 사람들에게 친숙한 1~9 로 이루어진 Sequence
  - SHA-1 Hash 복호화된 Original Sequence
  - SHA-1 Hash Value

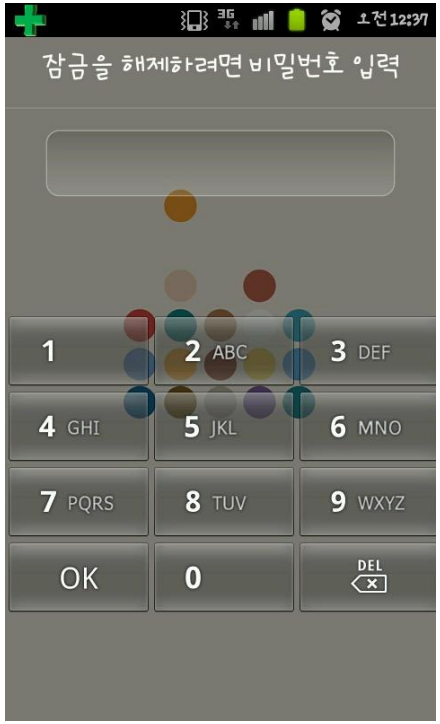
Demo

- 패턴 잠금 설정
- 레인보우 테이블을 이용하여 패턴 추출

PIN / Password Lock

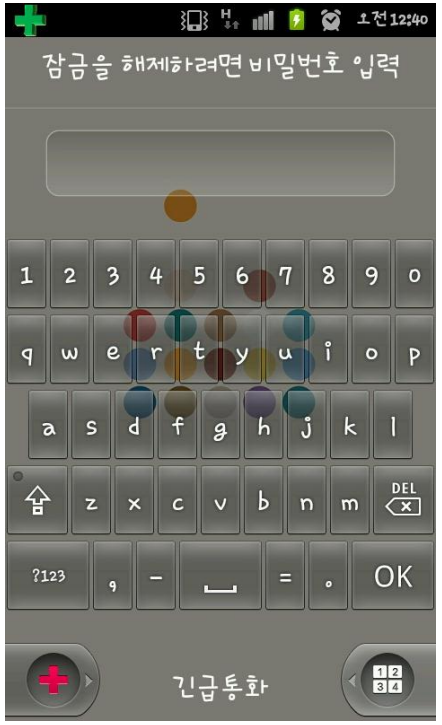
PIN Lock이란?

- Android 기반 스마트 폰의 화면 잠금을 풀기 위해 사용하는 고전적인 방법
- 10개의 숫자를 이용하여 **길이가 4인 Number Sequence**를 사용
- **경우의 수가 한정**
  - 같은 숫자를 여러 번 사용할 수 있다.
  - 총 *10,000의 경우의 수*가 존재한다.



Password Lock이란?

- Android 기반 스마트 폰의 화면 잠금을 풀기 위해 사용하는 방법 중에 하나
- 숫자와 문자 모두 사용 가능
- **경우의 수가 무한정**
  - 같은 문자를 여러 번 사용할 수 있다.
  - 길이에 제한이 없다.



password.key

```
667A90B331338288A2F115DF9D1EF73BEC05F48A4FF1FFFC0646ACFACE60B6E3D9249261
```

- 안드로이드 상의 PIN / Password에 관한 데이터 파일
  - 두 가지 잠금에 대한 데이터 파일의 이름이 동일

- */data/system/ 폴더*에 존재

- Lock Sequence가 **SHA-1 Hash 알고리즘**으로 암호화되어 저장
  - **패턴 잠금과 동일**

password.key

- PIN의 경우: 10,000 라는 적은 경우의 수
  - ***Make a rainbow table !***
- Password의 경우: 무한정한 경우의 수
  - ***It is impossible !***

Application Lock

어플리케이션 잠금

- 어플리케이션 자체에서 잠금 기능을 지원
- Example:
  - 카카오 톡
  - 틱톡
  - 마이피플
  - …

어플리케이션 잠금

- 보통 **PIN / Password 방식**의 잠금 기능을 사용
- 암호에 대한 **저장 공간**과 **암호화 방법**이 필요

암호 저장 공간

- "/data/data/package_name/shared_prefs/*.xml"
  - 어플리케이션에서 사용하는 기본 환경 설정 파일
  - 환경 변수에 대한 값들이 저장되어 있음
  - 잠금 암호의 저장소로 많이 사용
  - 자동 로그인에 대한 정보도 있을 수 있음
  - 폴더 명은 바뀔 가능성 있음
  - 파일 명은 사용하는 환경변수 함수에 따라 달라짐

암호 저장 공간

- "/data/data/package_name/databases/*.db
  - 어플리케이션이 사용하는 SQLite 데이터 베이스 파일
  - 사용하는 일련의 데이터를 저장하는 공간
  - 잠금 패스워드를 저장하는 공간으로도 사용 가능

암호 방식

- **대부분의 어플리케이션이 잠금에 대한 암호화를 하지 않음**
  - 평문으로 저장된 어플리케이션이 많이 존재

- 암호화를 할 경우, **MD5** 또는 **SHA-1 알고리즘**을 많이 사용
  - 하지만, 대부분 **PIN 방식**을 사용
  - **적은 경우의 수**를 가짐
    - ✓ 레인보우 테이블을 작성하여 복호화 가능

Problems

- 모든 잠금에 대한 데이터 파일이 **로컬에 저장**
  - 복호화를 하지 않아도 접근이 가능
    - ✓ 잠금에 대한 **데이터 파일을 삭제**시키면 잠금이 풀리기 때문
- 패턴 잠금의 경우, **화면에 남은 지문의 움직임**을 통해 풀릴 가능성

질문 및 답변

1. **Forensic focus**

Android forensics study of password and pattern lock protection

- **Android Forensics: From Decompilation To Reversing**
  - 다루는 내용
    - ✓ APK 파일 디컴파일
      - DEX 포맷 구조
      - DEX to Jar 디컴파일
      - Jar to Java 디컴파일
      - DEX to Smali 디컴파일
    - ✓ Re-packaging
    - ✓ Reversing
    - ✓ …