

uc3m

Universidad **Carlos III** de Madrid

Grupo de investigación:
Computer Security Lab

Mobile Devices Security

Degree in Computer Engineering

2019

Why protect data?

- ▶ Users who use your app trust you
 - ▶ Would they have to think that your data is safe?
 - ▶ Who must protect?
- ▶ The developer can not rely on the user using application
 - ▶ It assumes that you can lose your device
 - ▶ Assumes that installed malicious applications
 - ▶ Assumes no security expertise

Why protect data?

- ▶ Any device can be put in debug mode. Anyone can extract any database with different tools.
- ▶ Threats related to mobile computing devices

SQLCipher

- ▶ simple solution to encrypt databases SQLite
- ▶ It is an open source library that provides encryption AES 256-bit files database
- ▶ Negligible performance loss (5-15%) to SQLite
- ▶ No configuration is required and encryption is done at the application level

```
% hexdump -C unencrypted-sqlite.db
00000000 53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 |SQLite format 3.
00000010 04 00 01 01 00 40 20 20 00 00 00 02 00 00 00 03 |.....@.....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 41 01 06 |.....A..
00000030 17 1b 1b 01 5b 74 61 62 6c 65 73 65 63 72 65 74 |....[tablesecret
00000040 73 73 65 63 72 65 74 73 03 43 52 45 41 54 45 20 |sscrets.CREATE
00000050 54 41 42 4c 45 20 73 65 63 72 65 74 73 28 69 64 |TABLE secrets(id
00000060 2c 20 70 61 73 73 77 6f 72 64 2c 20 6b 65 79 29 |, password, key)
00000070 00 00 00 00 00 00 00 00 00 00 00 00 21 01 04 |.....!..
00000080 25 1d 1f 4c 61 75 6e 63 68 20 43 6f 64 65 73 70 |%...Launch Codesp
00000090 61 24 24 77 6f 72 64 70 72 6f 6a 65 74 69 6c 65 |a$$wordprojetele
```

SQLite

Data is insecure
and easily readable
using off-the-shelf
programs

```
% hexdump -C encrypted-sqlcipher.db
00000000 de ab bc 3a 40 2b 5d 00 b0 d2 9e 3b 75 91 76 73 |...: @]...;u.vs
00000010 bc 41 70 0c 8c ab a0 7a 37 eb a2 a8 a9 27 a5 0a |.Ap....z7....'..
00000020 38 c9 0b 9c 06 57 78 96 67 a2 e5 78 f8 8c 58 f3 |8....Wx.g..X.
00000030 ea 7c c6 23 14 8a 75 33 d0 a5 2c 30 2e e1 a4 96 |.|.#..u3...0...
00000040 b1 c6 5a 21 67 0a 31 bb 3b de a2 d4 80 b4 60 e3 |..Z!g.1.;.....
00000050 05 b0 75 04 f2 26 66 ed c7 4e 7e 9c ac 2e ec 1d |..u..&f..N~....
00000060 2d fc 31 b4 32 ce 24 0a d0 23 71 b0 1f 21 12 2c |-.1.2.$..#q..!.,
00000070 92 af 8e d9 de ac 76 e6 20 62 56 c6 f5 05 f5 b3 |.....v. bV....
00000080 53 d0 5f 4c 5e ec 5b 8a be e7 d1 46 f0 d9 dc b9 |S..L^.[....F....
00000090 a3 59 d6 63 a4 ae cf d8 e4 82 29 83 dd c7 86 13 |.Y.c.....).....
```

SQLCipher

AES-256 encryption
secures database
contents making it
unreadable without
the key

Module III: What to do?

- ▶ Use Android KeyStore to obtain an encrypted secret key
- ▶ Use the secret key along with SQLCipher and encrypt the database
- ▶ Run and test the app to verify that its features remain and has also encrypted the database properly
- ▶ Leverage *Certificate Pinning* in the app, in order to ensure that secured connections can only be established with trusted sites

Password encryption

- ▶ Using the KeyStore Provider
 - ▶ A pin code to unlock the mobile device
 - ▶ Create the Android Key Store
 - ▶ Create the key pair
 - ▶ Create a random passphrase and encrypt it using the public key.
 - ▶ Encrypt/decrypt - by the private key



Certificate Pinning

- ▶ Certificate filtering on HTTPS connections
- ▶ Accepted certificates defined with *SHA-256* hash
- ▶ Transparent implementation by leveraging Android's `android:networkSecurityConfig`

`res/xml/network_security_config.xml`:

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
  <domain-config>
    <domain includeSubdomains="true">example.com</domain>
    <pin-set expiration="2018-01-01">
      <pin digest="SHA-256">7HIpactkIAq2Y49orF00QKurWxmmSFZhBCoQYcRhJ3Y=</pin>
      <!-- backup pin -->
      <pin digest="SHA-256">fwza0LRMXouZHRC8Ei+4PyulDPDcf3UKg0/04cDM1oE=</pin>
    </pin-set>
  </domain-config>
</network-security-config>
```

uc3m

Universidad **Carlos III** de Madrid

Grupo de investigación:
Computer Security Lab

Mobile Devices Security

Degree in Computer Engineering

2019