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

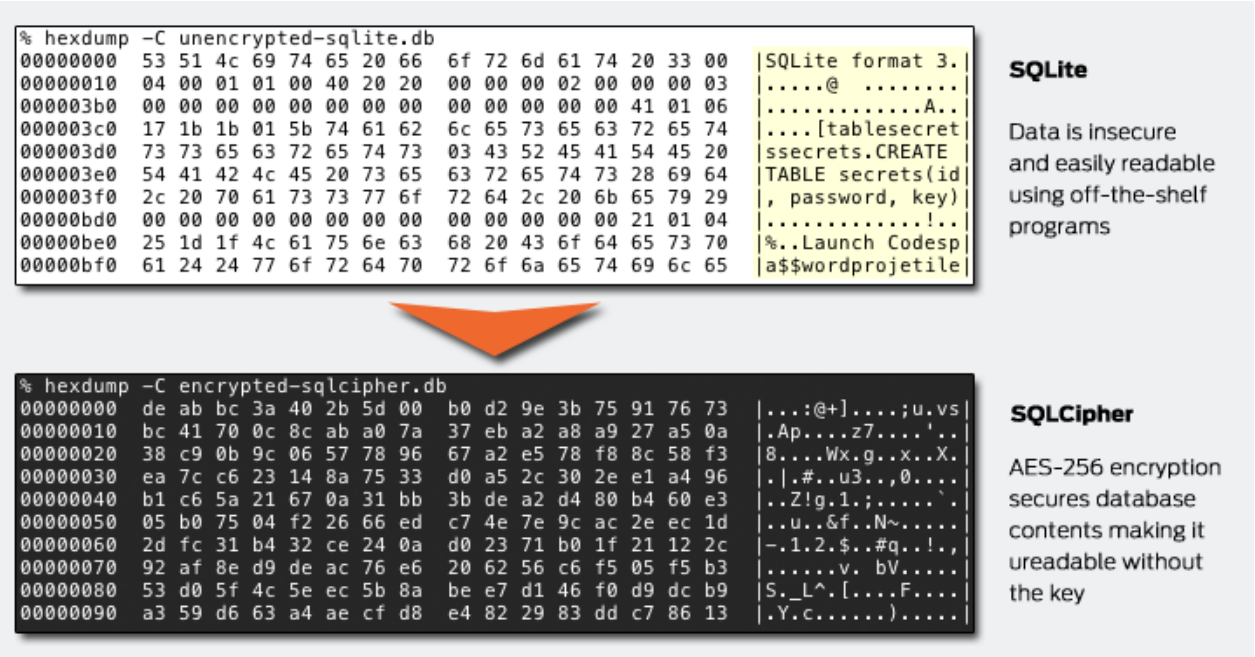
Why protect data?

- 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



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">7HIpactkIAq2Y49orFOOQKurWxmmSFZhBCoQYcRhJ3Y=</pin>
            <!-- backup pin -->
            <pin digest="SHA-256">fwza0LRMXouZHRC8Ei+4PyuldPDcf3UKgO/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