SecureSuite Security

December 5, 2018

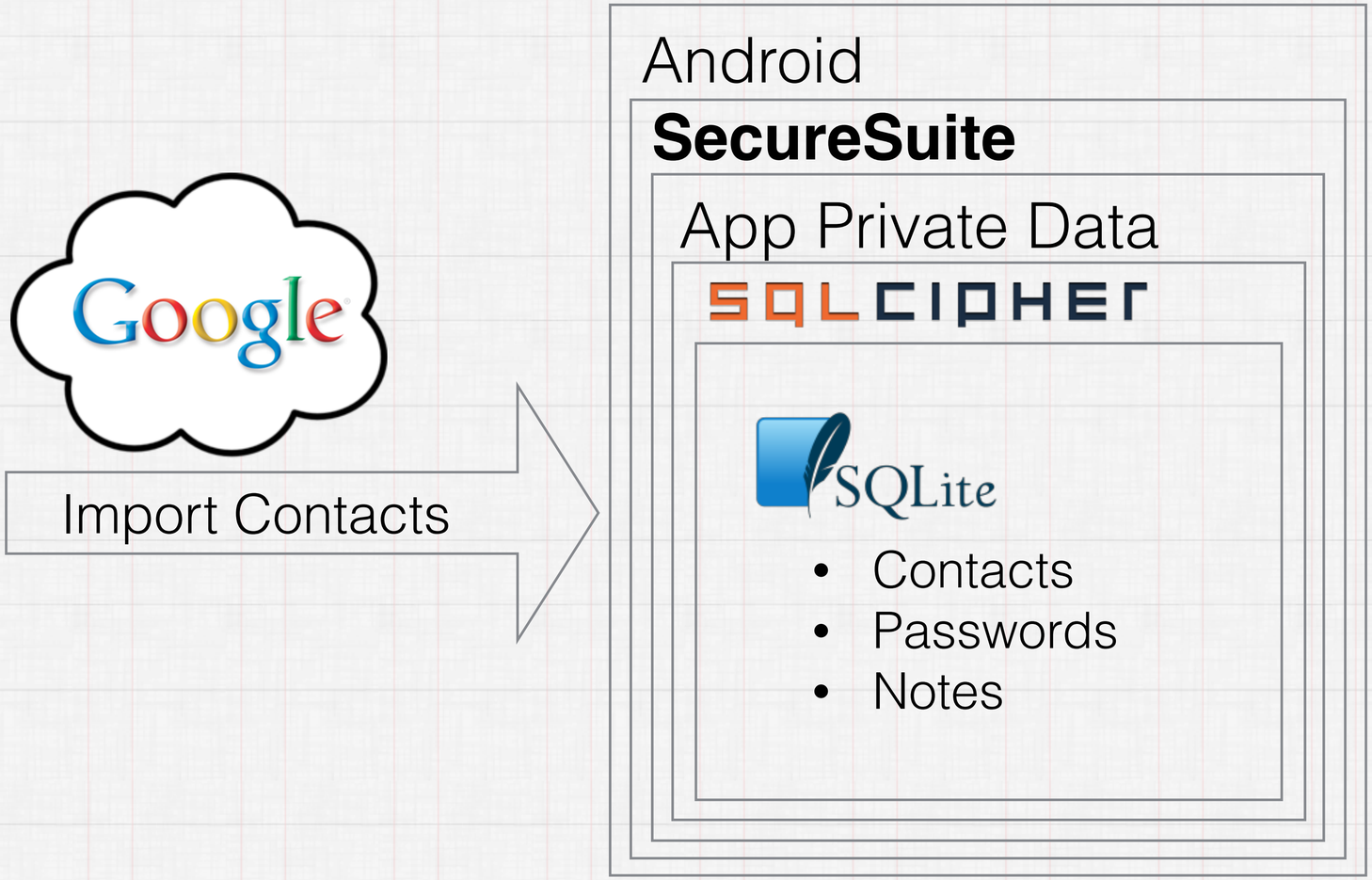
https://nuvolect.com/securesuite/

SecureSuite Security Summary

- AES 256 bit encrypted SQLite database SQLCIPHER
- TLS 2.1 HTTPS over LAN 
- YubiKey NEO authentication 

- No Internet access, only LAN (other than help page)

Security Layers



https://guardianproject.info/code/sqlcipher/

SqlCipher Database

- Database files are accessible
  - Menu: Contacts-Backup/restore-Backup to email
  - Menu: Contacts-Backup/restore-Backup to storage
- Database passphrase is accessible and changeable
  - Menu: Settings-Manage database passphrase
  - User may assign own passphrase
  - The database passphrase is encrypted with the Android Keystore System.
- When encrypted, the entire database file appears to contain random data

```
~ sjlombardo$ hexdump -C sqlite.db
00000000  53 51 4c 69 74 65 20 66  6f 72 6d 61 74 20 33 00  |SQLite format 3.|
...
000003c0  65 74 32 74 32 03 43 52  45 41 54 45 20 54 41 42  |et2t2.CREATE TAB|
000003d0  4c 45 20 74 32 28 61 2c  62 29 24 01 06 17 11 11  |LE t2(a,b)$.....|
...
000007e0  20 74 68 65 20 73 68 6f  77 15 01 03 01 2f 01 6f  | the show..../.o|
000007f0  6e 65 20 66 6f 72 20 74  68 65 20 6d 6f 6e 65 79  |ne for the money|

~ $ sqlite3 sqlcipher.db
sqlite> PRAGMA KEY='test123';
sqlite> CREATE TABLE t1(a,b);
sqlite> INSERT INTO t1(a,b) VALUES ('one for the money', 'two for the show');
sqlite> .quit

~ $ hexdump -C sqlcipher.db
00000000  84 d1 36 18 eb b5 82 90  c4 70 0d ee 43 cb 61 87  |.?6.?..?p.?C?a.|
00000010  91 42 3c cd 55 24 ab c6  c4 1d c6 67 b4 e3 96 bb  |.B?..?|
00000bf0  8e 99 ee 28 23 43 ab a4  97 cd 63 42 8a 8e 7c c6  |..?(#C??.?cB..|?|

~ $ sqlite3 sqlcipher.db
sqlite> SELECT * FROM t1;
Error: file is encrypted or is not a database
```

Example courtesy of sqlcipher.net/design

Web App Security

- The app generates a self-signed certificate secured with the Android Keystore System. No static certificates or passphrase are stored in the app.
- Unavoidable warning 
  - The identity of this website has not been verified.
  - Server's certificate does not match the URL.
  - Server's certificate is not trusted.
- Self-signed certificate 
  - LAN assigned IP address
  - Not associated with domain URL or static IP address
  - I.E., cannot be verified by browser
- SecureSuite uses TLS 1.2 encryption and is safe to use
- Communications are AES encrypted

https://github.com/NanoHttpd/nanohttpd

https://en.wikipedia.org/wiki/Self-signed_certificate

YubiKey NEO Authentication

- Near Field Communications (NFC) used for Android authentication
  - App can be configured with a primary and secondary key
  - Same key can be use with multiple devices: Android phone and Android tablet
- Key configuration can be deleted and replaced if key is lost or stolen

https://www.yubico.com/products/yubikey-hardware/yubikey-neo/

Questions and Comments

- We encourage your feedback
- team@nuvolect.com