March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

"Secure Password Managers" and "Military-Grade Encryption" on Smartphones: Oh, Really?

Andrey Belenko and Dmitry Sklyarov

Elcomsoft Co. Ltd.

Agenda

- Securing Data-at-Rest: PC vs Smartphone
- Threat Model
- BlackBerry applications
- iOS applications
  - Level 0: Absolute Zero
  - Level 1: Too Cunning?
  - Level 2: Almost Good
- Apple's way
- Summary

Common Way for Securing Data

- Data protected with strong encryption
- Master Key is derived from RNG
- Master Key is stored in encrypted form, preferable – in Hardware Security Module
- Access to Master Key is managed by some access-control mechanism

Master Key Protection

Personal Computer

- Trusted Platform Module
- Biometrics
- SmartCard + PIN
- Password/Passphrase

Smartphone

- ~~Trusted Platform Module~~
- ~~Biometrics~~
- ~~SmartCard + PIN~~
- Password/Passphrase

No effective ways other than
Password/Passphrase
is available for smartphones

Password/Passphrase

Personal Computer

- Easy to use long and complex passwords (full-sized keyboard, motor memory)
- Able to calculate PBKDF2 with thousands of iterations (powerful CPU)

Smartphone

- Hard to enter good passwords (tiny touch keyboard)
- Big number of PBKDF iterations leads to awful usability (slow CPU)
- Attack could be performed on PC with GPU!

Handling passwords on Smatphones much more difficult rather than on PC

Other thoughts

Personal Computer

- Hard to steal or lose. You know where is your PC most of the time
- Password entered not too often (usually just after unlocking console)

Smartphone

- Lot of phones goes in wrong hands every year. Do you really know where is your phone exactly right now?
- Password entered every time you need access data (after switching applications or by short time-out)

Smatphone requires stronger password protection in comparison with PC but provides less capabilities for doing so!

Threat Model

Attacker has (any combination of):

- Physical access to Device
- Copy of a backup of the Device
- Access to password manager database

Attacker's goal (any combination of):

- Recover master password for password manager(s) installed on the mobile device
- Extract passwords stored in those managers

Obtaining Password Manager Database

For BlackBerry devices:

- From Device Backup
  - May be protected with password, testing requires calculation of PBKDF2-SHA1 with 20’000 iterations
  - Device PassCode is needed for creating backup
- By Physical Acquisition
  - Available only if Device PassCode is known

Obtaining Password Manager Database

For iOS-based devices:

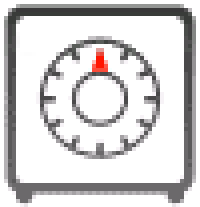
- From Device Backup
  - May be protected with password, testing requires calculation of PBKDF2-SHA1 with 10’000 iterations
  - Device should be paired with Desktop to perform backup
- From JailBroken Device via OpenSSH
- By Physical Acquisition (for models prior to iPhone 4S / iPad 2). Data could be protected with Device PassCode

BlackBerry Applications

Two of number of password manager apps, both developed by Research In Motion Ltd.

- BlackBerry Password Keeper
- BlackBerry Wallet

BlackBerry Password Keeper



by Research In Motion Ltd.

Note: Pre-installed on BlackBerry Devices

FREE

- Encryption key is calculated by PBKDF2-SHA1 with 3 (three) iterations
- SHA-1 hash value is encrypted along with data to check integrity, but more than 99,6% wrongful keys are rejected by PKCS7 padding checking
- Password validation is very fast and requires 3*PBKDF2-SHA1 + 1*AES-256

BlackBerry Wallet

FREE

by Research In Motion Ltd.

Claim: Designed for BlackBerry smartphones, BlackBerry Wallet helps make mobile, online purchasing faster and easier

- Ver 1.0 stores SHA-256(SHA-256(Pwd)) in database
- Password validation is very fast and requires 2*SHA-256
- Ver 1.2 works like BB Password Keeper, but password initially hashed with SHA-512, and 50…100 PBKDF iterations are used
- Password validation is fast and requires 1*SHA-512 + (50…100)*PBKDF2-SHA1 + 1*AES-256

iOS App, Level 0: Absolute Zero

Randomly-chosen Free programs from AppStore "Password Keeper" search results

- Safe – Password
- Awesome Password Lite
- Password Lock Lite
- iSecure Lite
- Secret Folder Lite
- Ultimate Password Manager Free

[un]Safe Triplets

Safe – Password

by The Best Free, Lite and Pro Edition

Awesome Password Lite

by Easy To Use Products

Password Lock Lite

by chen kaiqian

Claim: FINALLY! THE SAFEST APP TO PROTECT YOUR ALL PASSWORDS, BANK ACCOUNT, CREDIT CARD, WEB LOGINS AND ETC.

[un]Safe Triplets

- All three are identical (except names and background images)
- Stores data in SQLite database `Documents/Password_Keeper.sqlite`
- Master Password is always 4 digits
- No data encryption is involved at all
- Master Password is stored in plaintext

```
SELECT ZPASSWORD FROM ZDBCONFIG;
```

iSecure Lite - Password Manager

FREE

by Roland Yau

Claim: You data is extremely secure, even you have lost your device or stolen

- Stores data in SQLite database `Documents/app_creator.sqlite`
- Master Password of any length/chars
- No data encryption is involved at all
- Master Password is stored in plaintext

```
SELECT passcode FROM preference;
```

Secret Folder Lite

FREE

by chen kaiqian (the same as for Password Lock Lite)

Claim: The BEST AND MOST ADVANCED PHOTO & VIDEO PRIVACY APP in the App Store today

- Password-protect access to media files
- Stores data in SQLite database `Documents/privatephototwo.sqlite`
- No data encryption is involved at all
- All passwords are stored in plaintext

```
SELECT ZDISPLAYNAME,ZPASSWORD FROM ZDBFILE;
```

Ultimate Password Manager Free

FREE

by Jean-Francois Martin

Note from developer: The free version has the following limitations over the paid version:
- no data encryption

- Stores data in Binary Property List
  `Library/Preferences/com.tinysofty.upmfree.plist`
- Master Password is stored in plaintext

Are you interested in Password Manager which intentionally designed to be insecure, even if its FREE?

iOS App, Level 1: Too Cunning?

One FREE and one paid application that seems to be designed with …hmm... unintelligible approach

- My Eyes Only™ - Secure Password Manager
- SplashID Safe for iPhone ($9.99)

My Eyes Only™ - Secure Password Manager

FREE

by Software Ops LLC

Claim: allows personal information to be stored on iPhones, iPods and iPads without the threat of unauthorized access if lost or stolen

- RSA asymmetric encryption is used to protect secrets
- Data is stored as NSKeyedArchiver encoded objects
- Plain-text Master Password, Public and Private RSA keys are stored in KeyChain with attribute kSecAttrAccessibleWhenUnlocked

RSA sounds impressive, isn't it?

My Eyes Only™ - Secure Password Manager

- RSA modulus length is only 512 bits: could be factored in several days on modern super-computer
- File `Documents/MEO.archive` holds RSA-encrypted Master Password
- Both Public and Private RSA keys are stored in the same `MEO.archive` file

- Master Password and all user secrets could be instantly decrypted

Why storing RSA Private key in plaintext?

SplashID Safe for iPhone

$9.99

by SplashData

Claim: the award-winning password manager with over 500’000 users worldwide, is now available for iPhone! The all new iPhone version 5 makes SplashID better than ever

- Supported on Win, Mac, iOS, Android, BB, WM, Palm…
- On iOS stores data in SQLite database
  `Documents/SplashIDDataBase.db`
- All sensitive data is encrypted with Blowfish

Seems to be a good choice?

SplashID Safe for iPhone

- Encryption key is just a Master Password
  - no salting
  - no iterative hashing
- All data encrypted in ECB mode
- Password is encrypted on hard-coded key
  `g.;59?^/0n1X*{OQlRwy`
  and stored in database

- Instant Master Password recovery is possible

Poor 500’000 users…

iOS App, Level 2a: Almost Good

Three FREE Password Keepers that provides some level of security

- Keeper® Password & Data Vault
- Password Safe - iPassSafe free version
- Strip Lite - Password Manager

Keeper® Password & Data Vault

FREE

by Callpod Inc

Claim: With Keeper's military-grade encryption, you can trust that no one else will have access to your most important information

- Stores data in SQLite database `Documents/keeper.sql`
- MD5 of Master Password is stored in database
- SHA1 of Master Password is used as AES-128
- Very fast password testing: just 1*MD5
- No salting – MD5 Rainbow Tables could be used

Password Safe - iPassSafe free version

by Netanel Software

Claim: iPassSafe - To Be True Protected.
AES-256 Double Encryption Layers.

FREE

- Stores data in SQLite database
  `Documents/iPassSafeDB.sqlite`
- Prevents usage of “weak” passwords:
  `0000 1234 2580 1111 5555 0852 2222 1212 1998 5683`
- Master Password is not hashed/salted but just padded with zeros and used as AES-256 key to decrypt 256-bit AES Master Key
- Very fast password testing: just 1*AES-256

Strip Lite - Password Manager

FREE

by Zetetic LLC

Claim: highly rated Password Manager and Data Vault. Strip has been protecting sensitive information on mobile devices for over 12 yrs.

- Stores data in SQLite database `Documents/strip.db`
- Whole database file is encrypted using open-source component sqlcipher developed by Zetetic
- Database Encryption Key is derived from Master Password with PBKDF2
- Password validation requires 4000*PBKDF2-SHA1 + 1*AES-256

iOS App, Level 2b: Almost Good

Five paid Password Keepers that provides some level of security

- SafeWallet - Password Manager ($3.99)
- DataVault Password Manager ($9.99)
- 1Password Pro ($14.99)
- mSecure - Password Manager ($9.99)
- LastPass for Premium Customers ($1/month)

SafeWallet - Password Manager

$3.99

by SBSH Mobile Software

Claim: Password Manager is the most secure and easy to use way to store your passwords and sensitive information

- Supported on Win, Mac, iOS, Android, BB, Symbian…
- Uses proprietary database format common for all platforms
- Master Password is used to decrypt Master Key
- All payload is encrypted with AES-256 CBC PKCS7
- Password validation is fast and requires 10*PBKDF2-SHA1 + 1*AES-256

DataVault Password Manager

by Ascendo Inc

Claim: Leading Password Manager for iPhone, iPad & iPod Touch ☆ AES Encryption

$9.99

- All secrets are stored in Device KeyChain
- Master Password trimmed/padded to 16 bytes is used as encryption key without hashing/salting
- SHA-256 of Master Password is stored in Comments (not in Data) attribute of KeyChain item
  - Attributes other than Data not encrypted in iOS 4
  - SHA-1 hash of encrypted attribute value is stored in iOS 5
- Password validation is very fast and requires 1*SHA-256 + [in iOS 5] 1*SHA-1

mSecure - Password Manager

$9.99

by mSeven Software, LLC

Claim: used by almost a million users worldwide, providing secure solution for storing your important information

- Data is stored as NSKeyedArchiver encoded objects
- Secrets encrypted with Blowfish
- SHA-256 of Master Password is used as Master Key
- Master Key encrypted on Master Key is stored for password verification
- Password validation is fast and requires 1*SHA-256 + 1*Blowfish

LastPass for Premium Customers

$12/yr

by LastPass

Claim: password data on your PC and your iPhone seamlessly synced. Encrypted by AES-256 which is used by the US Government for Top Secret documents

- Subscription-based service, local storage created after first sync
- Master Key = SHA-256 (Username + Password)
- SHA-256 hash of Master Key encrypted by AES-256 is stored for verification
- Off-line password validation is very fast and requires 2*SHA-256 + 1*AES-256

1Password Pro

$14.99

by Agilebits Inc

Claim: 1Password Pro is a special edition of the award-winning 1Password application with more than 1 million users worldwide

- Supported on Mac, Win, iOS, Android
- Allows set simple PIN and compex Master Password
- Two types of secrets: PIN- and Password-protected
- AES-128 encrypted Validator is present, but Master Key is encrypted in CBC PKCS7 mode. Thus, correct padding confirms password correctness
- Password/PIN validation is very fast and requires 1*MD5 + 1*AES-128

Apple's way

- Starting from iOS 4 PassCode is involved in encryption of sensitive data (including some KeyChain records and files)
- PassCode Key derivation is slowed down by iteration function (7 pwd/sec on iPhone 4G)
- Requires physical access to Device (can't be performed off-line and scaled)

- Even 6-digits PassCodes could not be exhaustively tested in 24 hours!

Summary

Name	Complexity	CPU p/s	GPU p/s	Len/24h
Keeper® Password & Data Vault	1x MD5	60 M	6000 M	14.7
Password Safe - iPassSafe Free	1x AES-256	20 M	N/A	12.2
Strip Lite - Password Manager	4000x PBKDF2-SHA1 + 1x AES-256	5000	160 K	10.1
SafeWallet - Password Manager	10x PBKDF2-SHA1 + 1x AES-256	1500 K	20 M	12.2
DataVault Password Manager	1x SHA-256 + 1x SHA-1	7 M	500 M	13.6
mSecure - Password Manager	1x SHA-256 + 1x Blowfish	300 K	N/A	10.4
LastPass for Premium Customers	2x SHA-256 + 1x AES-256	5 M	20 M	12.2
1Password Pro	1x MD5 + 1x AES-128	15 M	20 M	12.2
BlackBerry Password Keeper	3x PBKDF2-SHA1 + 1x AES-256	5 M	20 M	12.2
BlackBerry Wallet 1.0	2x SHA-256	6 M	300 M	13.4
BlackBerry Wallet 1.2	1x SHA-512 + 100x PBKDF2-SHA1 + 1x AES-256	200K	3200 K	11.4
iOS PassCode	50000 iterations with HW AES	**7**	**0**	**5.8**

Conclusion

- Strip Lite (btw – it's FREE) is better than others due to 4000*PBKDF2
- mSecure seems not bad. Possible reason: we don't have GPU-optimized Blowfish code [yet?]
- Many developers avoids usage of PBKDFs, RNG-keys, salting and even hashing
- Extremely popular paid apps as well insecure as free ones

- iOS PassCode protection mechanism much stronger than self-invented solutions

March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

THANK YOU!

QUESTIONS?

black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

PLEASE DO NOT FORGET TO COMPLETE YOUR FEEDBACK SURVEY FORMS!