HACKITO ERGO SUM

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

Andrey Belenko and Dmitry Sklyarov

Elcomsoft Co. Ltd.

{a.belenko,d.sklyarov} @ elcomsoft.com

Agenda

- Authentication: PC vs. Smartphone
- Threat Model
- BlackBerry Password Managers
- iOS Password Managers
  - Free
  - Paid
- Summary & Conclusions

Authentication: PC

- Trusted Platform Module

- Biometrics

- SmartCard + PIN

- Password/Passphrase

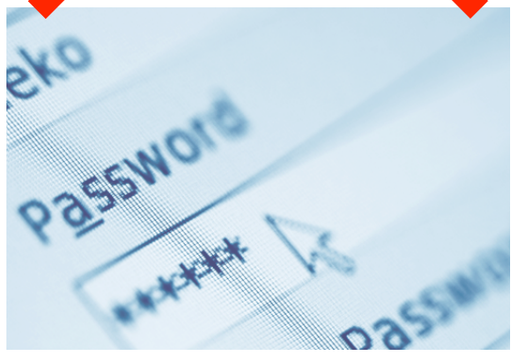
Authentication: Smartphone

- ~~Trusted Platform Module~~

- ~~Biometrics~~

- ~~SmartCard + PIN~~

- Password/Passphrase



Authentication: Smartphone

Password is the only option on the smartphones

“Lock patterns” are essentially numeric passcodes

(1-4-2-5-6-9-8)

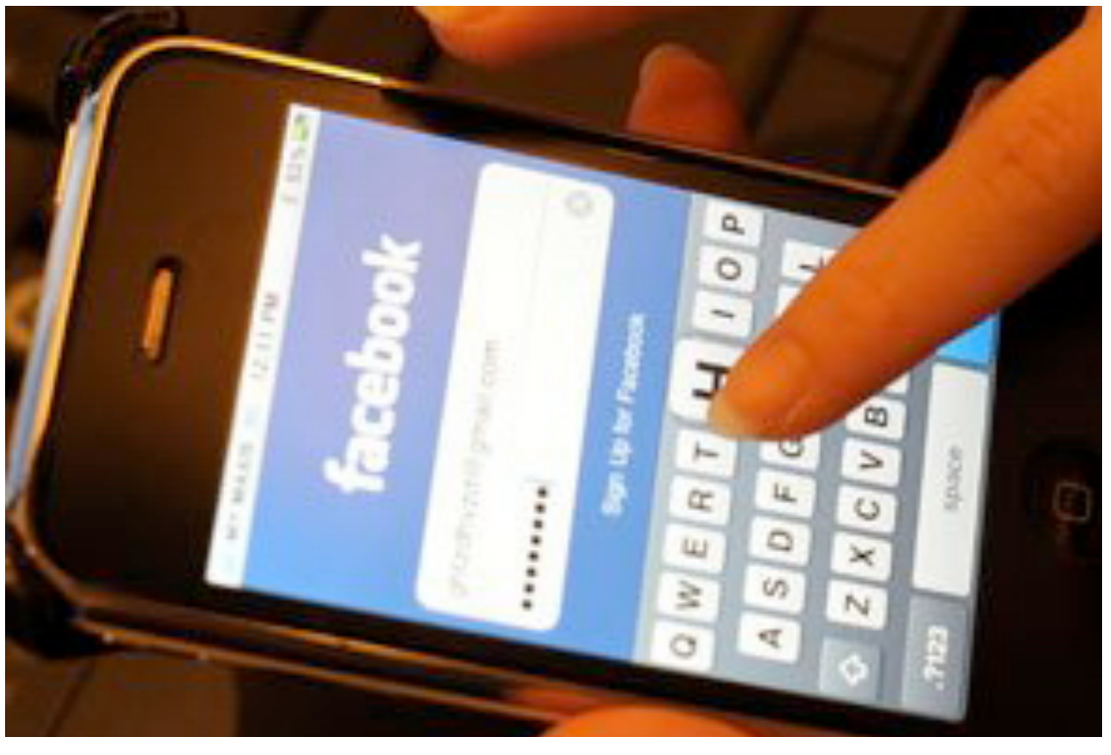
Password Typing

PC:

- Full-sized keyboard, motor memory
- Long and complex passwords are easy

Smartphone:

- Touch keyboard
- Long and complex passwords are hard



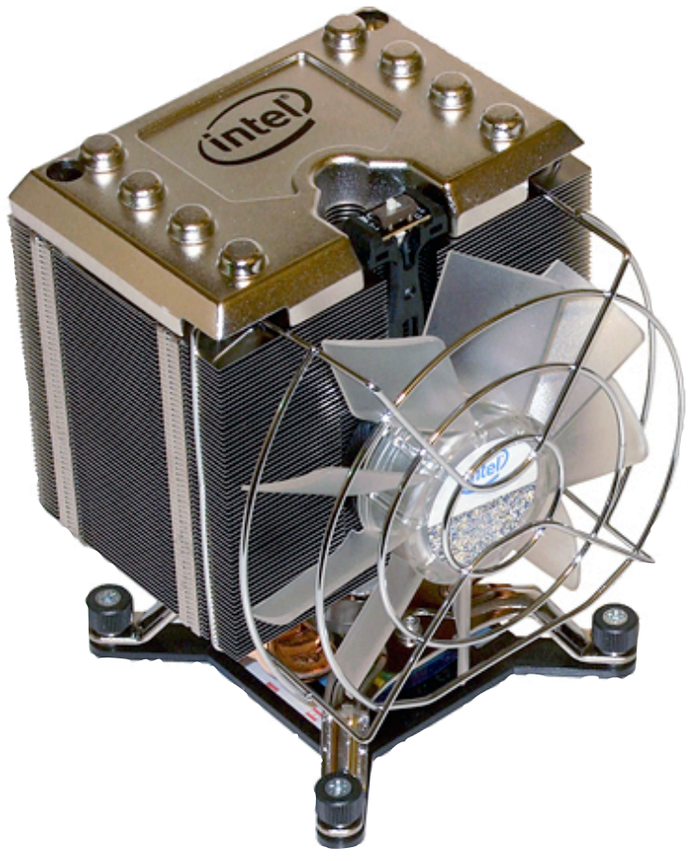
Password Typing

It is fair to assume that passwords on the smartphones are shorter than their PC counterparts

Password Cracking

Smartphone:

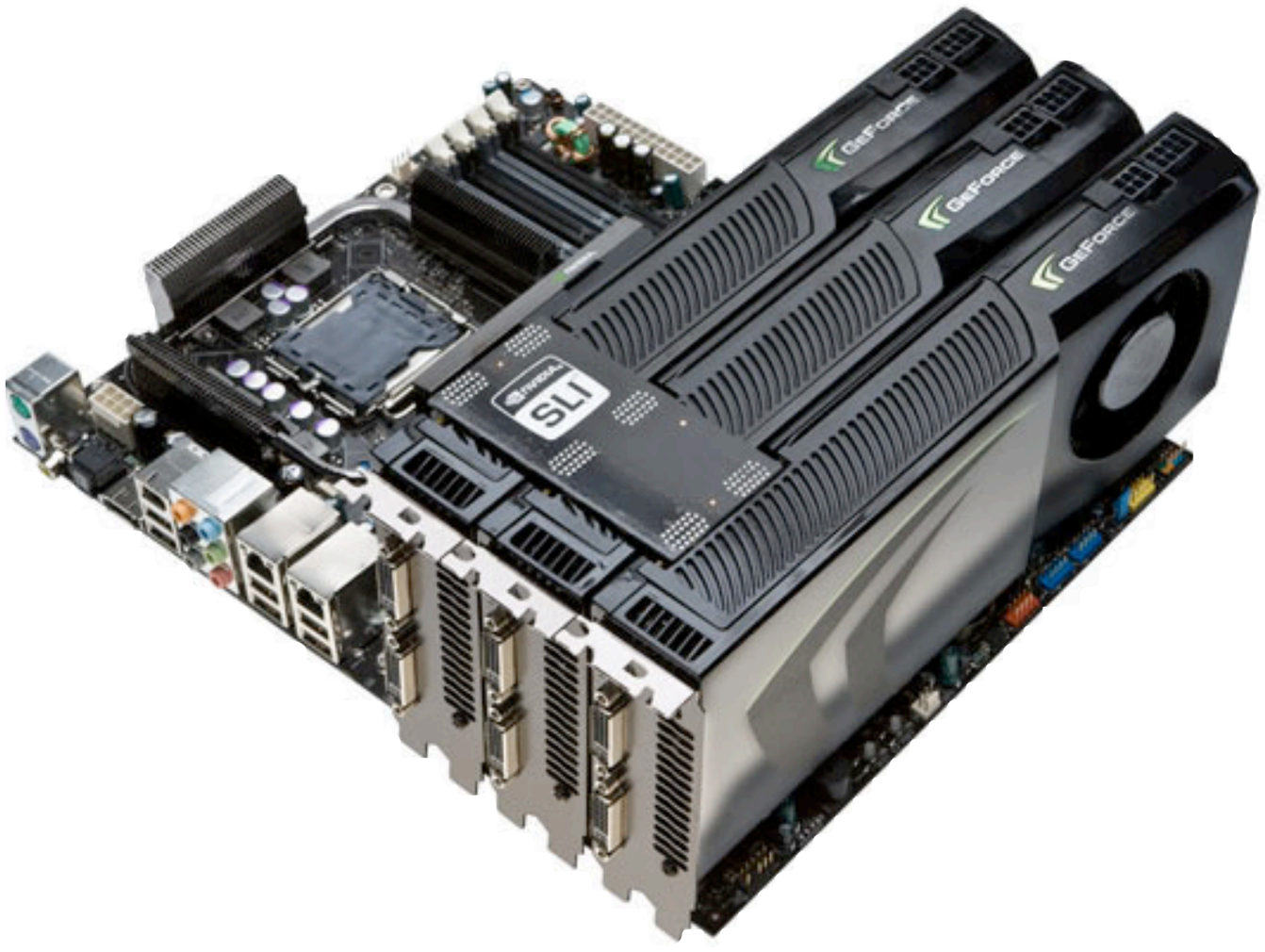
- Relatively slow CPU
- Complex password-to-key transforms will impact usability



PC:

- Fast CPU
- Can do complex password-to-key transforms

Password Cracking



Offline attacks can utilize GPUs for attackers' advantage

Authentication Wrap Up

PC	Smartphone
Password entered not too often (usually just after unlocking console)	Password entered every time you need access data (after switching applications or after short time-out)

- Handling passwords on smartphone is more difficult than on PC
- Smartphone requires stronger password protection than PC but provides less capabilities for doing so!

Agenda

- Authentication: PC vs. Smartphone
- Threat Model
- BlackBerry Password Managers
- iOS Password Managers
  - Free
  - Paid
- Summary & Conclusions

Threat Model

Assumptions:

1. Attacker has:
   - Physical access to the device, or
   - Backup of the device, or
   - Access to password manager database file
2. Attacker wants to:
   - Recover master password for password manager(s) on the mobile device
   - Extract passwords stored by those managers

Are those assumptions fair at all?

Physical Access

Computers are relatively big. Thus, hard to steal or lose.

You know where it is (well, most of the time).

Lots of phones go in wrong hands every year. Many are left in the bars.

Do you really know where exactly your phone is right now?

Someone’s just got physical access to the device

Device Backup

Apple iOS:

- Need device passcode or iTunes pairing
- Optional encryption (enforced by device)
  - PBKDF2-SHA1 with 10’000 iterations

BlackBerry:

- Need device password
- Optional encryption (not enforced)
  - PBKDF2-SHA1 with 20’000 iterations

Database Files

Apple iOS:

- Via afc (need passcode or iTunes pairing)
- Via SSH (jailbroken devices)
- Via physical imaging (up to iPhone 4)

BlackBerry:

- Need device password

Agenda

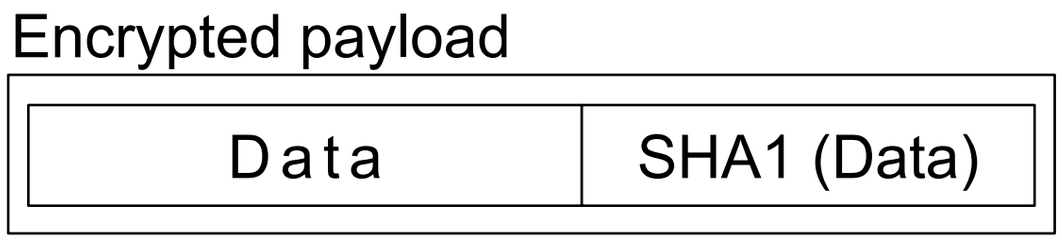
- Authentication: PC vs. Smartphone
- Threat Model
- BlackBerry Password Managers
- iOS Password Managers
  - Free
  - Paid
- Summary & Conclusions

BlackBerry Applications

- BlackBerry Password Keeper
  - Included with OS 5
- BlackBerry Wallet
  - Version 1.0 (for OS <= 5)
  - Version 1.2 (for OS > 5)

BlackBerry Password Keeper

- Key is calculated by PBKDF2-SHA1 with 3 iterations
- Encrypted payload is PKCS7-padded
  - Allows to quickly reject wrong keys ($p \approx 2^{-8}$)
  - Survived keys are checked by verifying SHA-1

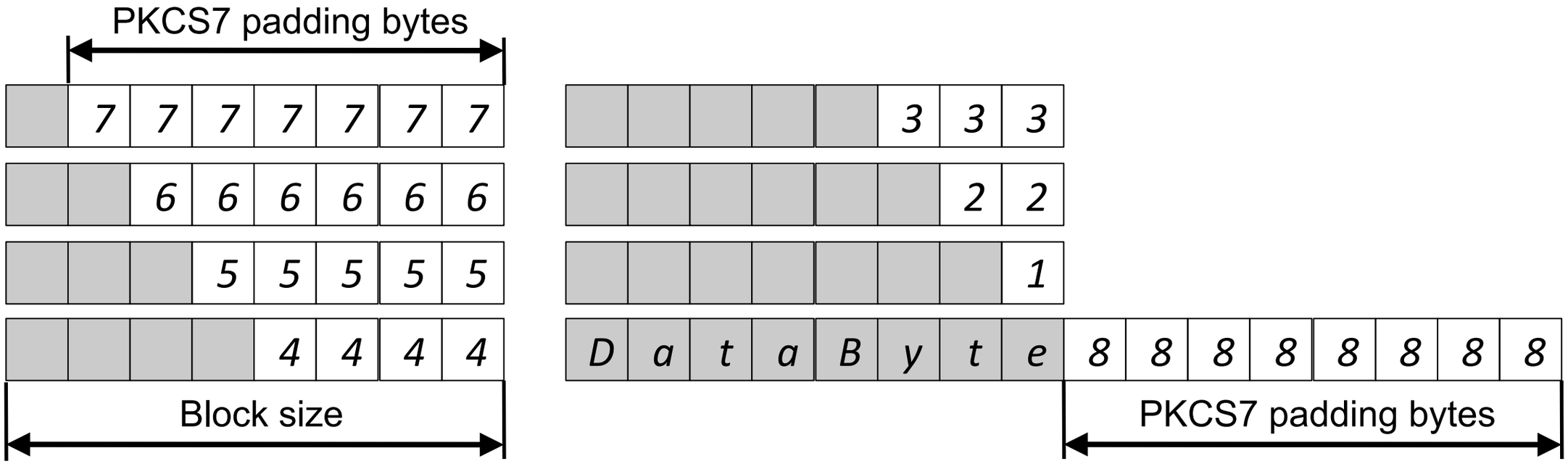


- Password verification is fast
  - 3 x PBKDF2-SHA1 + 1 x AES-256
  - ~5M passwords/sec on a CPU, ~20M with GPU

PKCS7 Padding

Plaintext padded to completely fill last block

- Done even if block size divides plaintext length
- Padding value == number of bytes appended



- After decryption padding verified and removed
- Decryption with random key produces valid padding with $p \approx 2^{-8}$ (0.4%)

BlackBerry Wallet

“*Designed for BlackBerry smartphones, BlackBerry Wallet helps make mobile, online purchasing faster and easier*”

Version 1.0

- Stores SHA-256 (SHA-256 (Password))
- Password verification requires 2 x SHA-256
- Very fast: ~6M on CPU, ~300M on GPU
- No salt: Rainbow Tables may be built

BlackBerry Wallet

"*Designed for BlackBerry smartphones, BlackBerry Wallet helps make mobile, online purchasing faster and easier*"

Version 1.2

- Similar to BB Password Keeper, but...
- Password initially hashed with SHA-512
- PBKDF2-SHA1 uses random number (50..100) of iterations
- Password verification requires 1xSHA-512 + 100xPBKDF2-SHA1 + 1xAES-256
- Est. 200K p/s on CPU, 3200K on GPU

Agenda

- Authentication: PC vs. Smartphone
- Threat Model
- BlackBerry Password Managers
- iOS Password Managers
  - Free
  - Paid
- Summary & Conclusions

iOS Free Apps

Search App Store for “Password Keeper” and pick a few from top 20 free apps

- Safe – Password (x3)
- iSecure Lite
- Secret Folder Lite
- Ultimate Password Manager Free
- My Eyes Only™ - Secure Password Manager
- Keeper® Password & Data Vault
- Password Safe – iPassSafe free version
- Strip Lite - Password Manager

[un]Safe Triplets

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

Safe – Password

by The Best Free, Lite and Pro Edition

Awesome Password Lite

by Easy To Use Products

Password Lock Lite

by chen kaiqian

[un]Safe Triplets

- All three are identical (except for names and background images)
- Store data in SQLite database at **`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

by Roland Yau

"*You data is extremely secure, even you have lost your device or stolen*"

- Stores data in SQLite database at **`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

by chen kaiqian

"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 at **`Documents/privatephototwo.sqlite`**
- No data encryption is involved at all
- All passwords are stored in plaintext

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

iOS Ultimate Password Manager Free

by Jean-Francois Martin

"*The free version has the following limitations over the paid version:*
- no data encryption"

- Stores data in binary Property List at **`Library/Preferences/com.tinysofty.upmfree.plist`**
- Master password is stored in plaintext

Are you interested in password manager intentionally designed to be insecure, even if it's free?

My Eyes Only™ - Secure Password Manager

by Software Ops LLC

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

- Stores data in NSKeyArchiver files at **`Documents/*.archive`**, encrypted with RSA
- Master password, public and private RSA keys are stored in keychain with attribute kSecAttrAccessibleWhenUnlocked

Wow, RSA looks impressive for a password keeper, isn't it?

My Eyes Only™ - Secure Password Manager

- 512-bit RSA modulus: factorization is easy
- **`Documents/MEO.archive`** holds RSA-encrypted master password
- RSA private key is stored in the same file
- Yes, RSA *private* key is stored along with encrypted data
- Master password and everything else can be instantly decrypted

Keeper® Password & Data Vault

by Callpod Inc

"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 at **`Documents/keeper.sql`**
- MD5 of master password is stored in database
- SHA1 of master password is used as AES key
- Very fast password verification: 1 x MD5
  - ~60M p/s on CPU, 6'000M p/s on GPU
- No salt: MD5 Rainbow Tables can be used

Password Safe - iPassSafe free version

by Netanel Software

"*iPassSafe - To Be True Protected. AES-256 Double Encryption Layers*"

- Stores data in SQLite database at **`Documents/iPassSafeDB.sqlite`**
- Prevents usage of "weak" passwords:

```
0000 1234 2580 1111 5555
0852 2222 1212 1998 5683
```

Password Safe - iPassSafe free version

by Netanel Software

"*iPassSafe - To Be True Protected. AES-256 Double Encryption Layers*"

- Random master key (M_k)is used for encryption
- M_k is encrypted with master password as a key
  - Password not hashed, only null-padded
  - PKCS7 padding allows to reject wrong keys
- Very fast password verification: 1 x AES-256
  - ~20M on CPU, haven't done AES on GPU yet :)
  - Rainbow Tables may be built

Strip Lite - Password Manager

by Zetetic LLC

"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 at **`Documents/strip.db`**
- Whole database file is encrypted using open-source component **`sqlcipher`** developed by Zetetic

Strip Lite - Password Manager

- Database encryption key is derived from master password using PBKDF2-SHA1 with 4’000 iterations
  - ~~By far the most resilient app to password cracking~~
- Password validation requires 4000 x PBKDF2-SHA1 + 1 x AES-256
- Est. 5K p/s on CPU, 160K on GPU

Agenda

- Authentication: PC vs. Smartphone
- Threat Model
- BlackBerry Password Managers
- iOS Password Managers
  - Free
  - Paid
- Summary & Conclusions

iOS Paid Apps

Google “Top Password Keepers for iOS” and pick a few from various reviews

- SafeWallet - Password Manager
- DataVault Password Manager
- mSecure - Password Manager
- LastPass for Premium Customers
- 1Password Pro for iPhone
- SplashID Safe for iPhone

SafeWallet - Password Manager

$3.99

by SBSH Mobile Software

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

- Versions for Win, Mac, iOS, Android, BB…
- Database format common for all platforms
- Master key encrypted with master password
- Data encrypted with AES-256, PKCS7
- Password verification is fast
  - 10 x PBKDF2-SHA1 + 1 x AES-256
  - Est. 1500K p/s on CPU, 20M on GPU

$9.99

by Ascendo Inc

DataVault Password Manager

"*Leading Password Manager for iPhone, iPad & iPod Touch ☆ AES Encryption*"

- Data encrypted by the master password and stored in device keychain
  - Master password not hashed, only padded
- SHA-256 of master password is stored in the keychain

Keychain is used, so it should be hard to get hash to brute force master password, right?

DataVault Password Manager

- In iOS 4 keychain is a SQLite database
  - Data column is supposed to store passwords and is always encrypted
  - Other item attributes are not encrypted
- Password hash stored as a ‘Comment’ attribute
- Still, this is better than storing hash in a file

Wait, I’ve heard iOS 5 encrypts all attributes in the keychain. Does that help?

DataVault Password Manager

- iOS 5 encrypts all keychain items' attributes
  - But it stores SHA-1 hash of original attribute to facilitate search/lookup
- So we have SHA-1 (SHA-256 (*password*))
- Very fast password verification:
  - 1 x SHA-256 [+ 1 x SHA-1 in iOS 5]
  - 7M p/s on CPU, 500M on GPU
  - No salt: Rainbow Tables can be built

$9.99

by mSeven Software LLC

mSecure - Password Manager

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

- Stores data in NSKeyArchiver files at **`Documents/msecure.db.plist`**
- Data encrypted with Blowfish
- Master key is SHA-256 of master password
- Fixed string encrypted on master key is stored for password verification

$9.99

by mSeven Software LLC

mSecure - Password Manager

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

- Password verification:
  - 1 x SHA-256 + 1 x Blowfish
  - 300K p/s on CPU, no Blowfish on GPU yet

LastPass for Premium Customers

$12/yr.

by LastPass

"...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"

- 'Cloud' service, local storage created after first login
- Master key computed by 500* x PBKDF2-SHA256
- Hash of master key is encrypted with AES-256 using master key and stored for verification
- Off-line password validation is very fast:
  - 500* x PBKDF2-SHA256 + 1 x AES-256
  - 12K p/s on CPU, 600K on GPU

1Password Pro for iPhone

$14.99

by Agilebits Inc.

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

- Versions for Mac, Win, iOS, Android
- Two protection levels: master PIN and master password
- Data encrypted with AES-128, key derived from master PIN or master password

1Password Pro for iPhone

```
Read EncDatabaseKey and EncValidator from Database
KEK := MD5 (Password + Salt)
IV := MD5 (KEK + Password + Salt)
DatabaseKey := AES-128-CBC (KEK, IV, EncDatabaseKey)
Validator := AES-128-CBC (DatabaseKey, NULL, EncValidator)
If Validator = DatabaseKey Then password is correct
```

- Database key encrypted on itself is stored for PIN or password verification
  - PKCS7 padding allows to reject wrong keys
- Password/PIN verification is very fast
  - 1 x MD5 + 1 x AES-128
  - 15M p/s on CPU, 20M p/s on GPU

1Password Pro for iPhone

Version 3.6.5 released on 09 April 2012 has new protection:

- 10’000 x PBKDF2-SHA1 + 1 x AES
- 2’000 p/s on CPU, 65K p/s on GPU
- Only applies to master password (not PIN!)

SplashID Safe for iPhone

$9.99

by SplashData

"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"

- Versions for Win, Mac, iOS, Android, BB…
- On iOS stores data in SQLite database at **`Documents/SplashIDDataBase.db`**
- All sensitive data is encrypted with Blowfish
- Master password is used as a Blowfish key
- Master password is encrypted with...

SplashID Safe for iPhone

- ...a random key (as per XKCD definition)

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

- 'Random' key is **`g.;59?^/0n1X*{OQlRwy`**
- Master password can be decrypted instantly

Agenda

- Authentication: PC vs. Smartphone
- Threat Model
- BlackBerry Password Managers
- iOS Password Managers
  - Free
  - Paid
- Summary & Conclusions

iOS Passcode

- Starting with iOS 4 passcode is involved in encryption of sensitive data
- Passcode key derivation is slowed down by doing 50’000 iterations
  - Each iteration requires talking to hardware AES
    - 6 p/s on iPhone 4
- Can’t be performed off-line and scaled

Checking all 6-digit passcodes will take more than 40 hours

Cracking Passwords

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~~
LastPass for Premium Customers	500*x PBKDF2-SHA256 + 1x AES-256	12K	600K	10.7
~~1Password Pro~~	~~1x MD5 + 1x AES-128~~	~~15 M~~	~~20 M~~	~~12.2~~
1Password Pro	10’000x PBKDF2-SHA1 + 1x AES-256	2000	65K	9.7
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**	**6**	**0**	**5.7**

Conclusions

- None of the tested password keepers offer reliable protection on top of OS security
- Using them on improperly configured device may expose sensitive data
- Paid apps are not necessarily more secure than free ones

Our Wishlist

Users:

- Use passcode
- Set backup password (complex one!)
- Do not connect your phone to untrusted devices

Developers:

- Use built-in OS security services
- Don’t reinvent or misuse crypto
- Really, don’t reinvent or misuse crypto

THANK YOU

Andrey Belenko and Dmitry Sklyarov

Elcomsoft Co. Ltd.

{a.belenko,d.sklyarov} @ elcomsoft.com