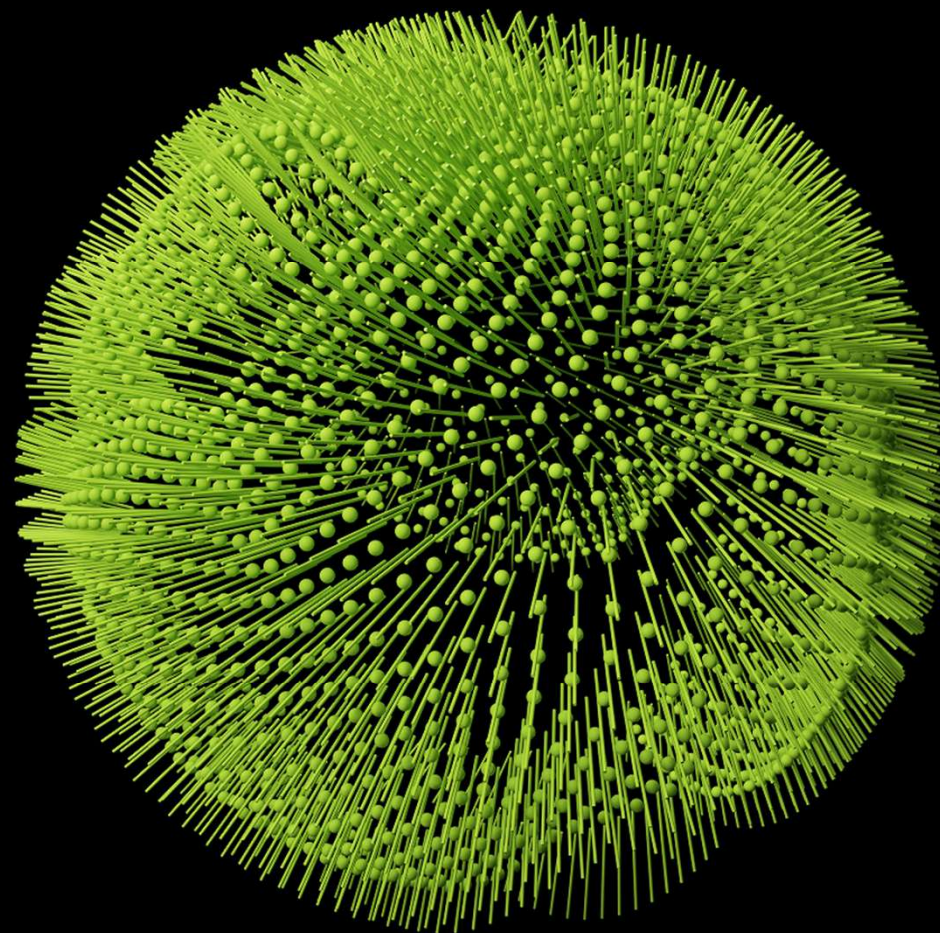


Deloitte.

NOVEMBER 16, 2018

Mobile Forensics

Forensic Challenges due to Encryption Mechanisms

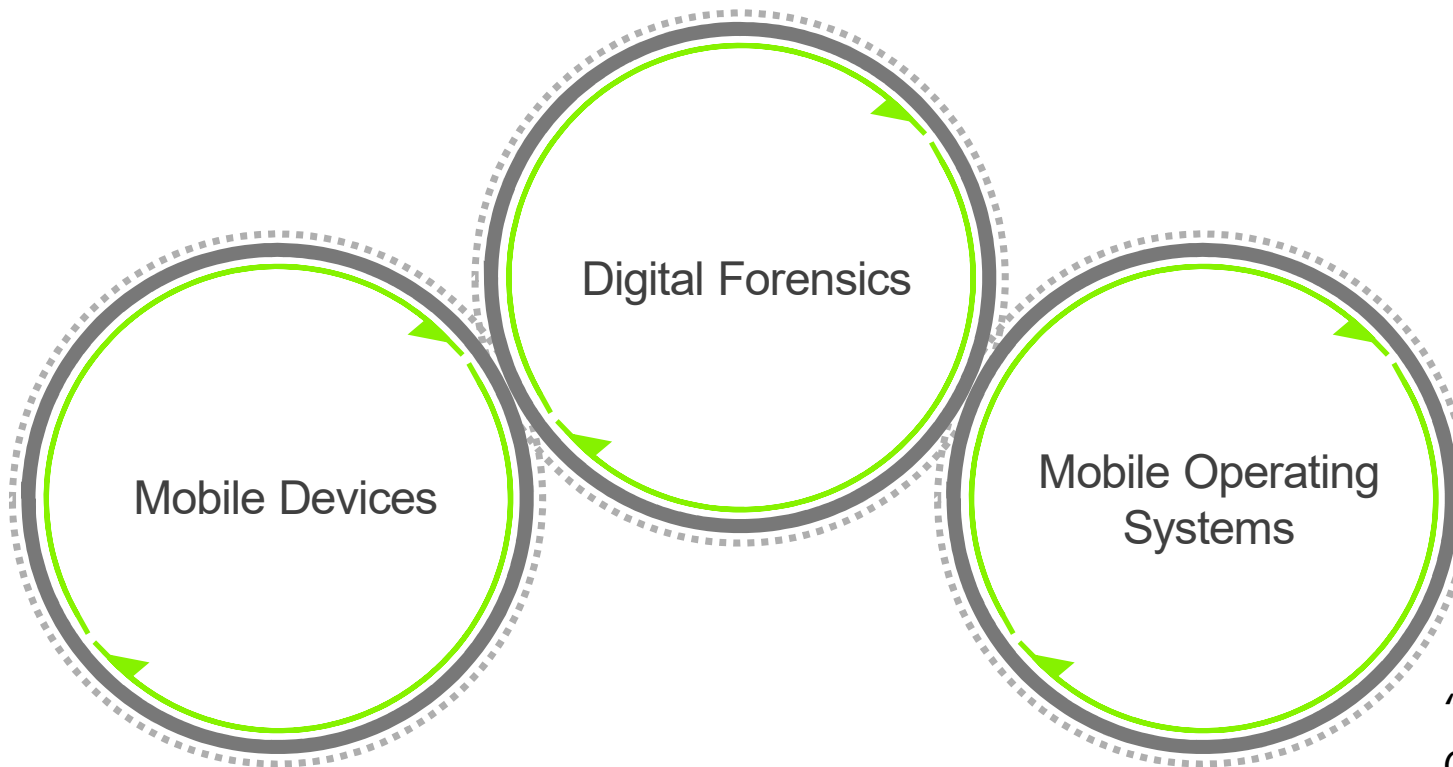


Section Overview

3	Mobile Forensics Definition	16	Demo iTunes Backup
6	Data Acquisition Methods, Tools	17	Password Manager Browsers
10	Android Encryption	22	Demo Firefox PM, Oxygen
12	iOS Encryption, iTunes Backup		

DEFINITION

Mobile Forensics, a combination of...

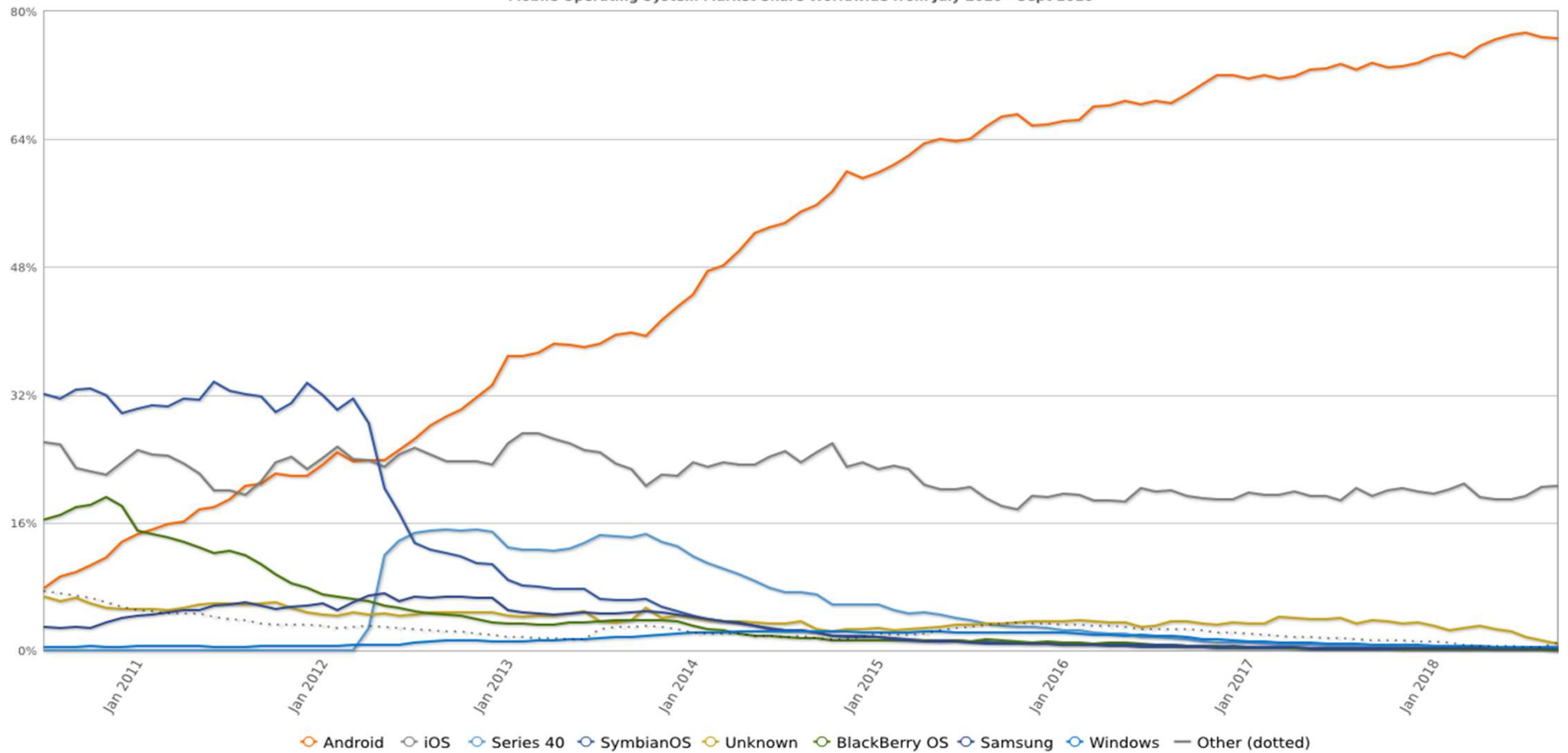


“Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods [...]”

MARKET SHARE WORLDWIDE

Mobile Operating Systems, 2010 – 2018

StatCounter Global Stats
Mobile Operating System Market Share Worldwide from July 2010 - Sept 2018



COMPARISON

Mobile Forensics vs. Computer Forensics

Mobile Forensics

Computer Forensics

No write blocker	Use of write blocker
Live acquisition	Dead and live acquisition
Typically more connectivity options (LTE, UMTS, Bluetooth, NFC, ...)	Typically less connectivity options
Mainly Android and iOS	Mostly Windows
SoC (Combined CPU, GPU, Modem, WiFi, Bluetooth, GPS, Audio, ...)	Separated CPU, RAM, WiFi, ...
PIN/Passcode required	Decryption key of HDD/SSD required Password/Username not required
Different cables: Micro-USB, USB-C, Lightning	Mostly SATA/SAS/NVME
Typically more private data on phones	Typically more work related data
„Conservation“ necessary due to live acquisition (Faraday Bag, flight mode)	Usage of seal bags



Data Acquisition

Methods and Tools

Data Acquisition Methods

Comparison of different acquisition methods

Logical

- Limited amount of data, not a full image
- Unlocked phone is required (Passcode)
- Example: iTunes Backup, ADB Backup/Pull

Cloud

- Limited amount of data
- Credentials needed
- Example: iCloud Extraction

Physical

- May alternate data
- Jailbreak/root required
- Data may be encrypted
- Example: dd-image via SSH on jailbroken iPhone

JTAG/chip-off

- May break the device and destroy evidence
- Encryption makes offline attacks useless
- Many devices do not have test-access ports

Renowned Mobile Forensic Tools



Cellebrite UFED

- Allegedly cracked the San Bernardino iPhone
- Offer an all in one hardware box solution
- Data extraction and reports can be viewed in the kit itself
- Promises for physical extraction while bypassing lock from over 3,000 devices



Oxygen Forensic Suite

- Offers a software based suite
- Support for more than 11,000 devices and more than 300+ apps
- Cheaper than other solutions



XRY

- Also offers a hardware solution
- Extraction of data from a wide variety of mobile devices (smartphones, satellite navigation units, modems, music players and tablets)





iOS and Android

Encryption, Backups, ...

Android Encryption

**Android 4.4
KitKat**

**Android 5
Lollipop**

**Android 6
Marshmallow**

**Android 7
Nougat**

**Android 8
Oreo**

**Android 9
Pie**

Full disk encryption since Android 4.4
(weak because of key in data partition)

Important new encryption features with Android 5.0

Mandatory since Android 6.0 (with exceptions for weak hardware)

File-based encryption since Android 7.0

Metadata encryption with Android 9.0

Full-Disk vs. File-Based Encryption (Android)

Full-Disk

File-Based

Encryption at block level

Encryption at file system level (only data partition)

Needed to provide credentials before any data can be accessed

Native ext4 file system encryption

Just basic operations before entering boot time password

Enables direct boot (boots straight to the lock screen)

After encryption password is entered, disk is unencrypted

New API – makes applications aware of encryption

One key: DEK – Device Encryption Key

More than one user to be protected (multi user system)

Two keys per user: CE – credential encrypted key and DE – device encrypted key

iOS Encryption

AES 256 crypto engine between flash storage and memory

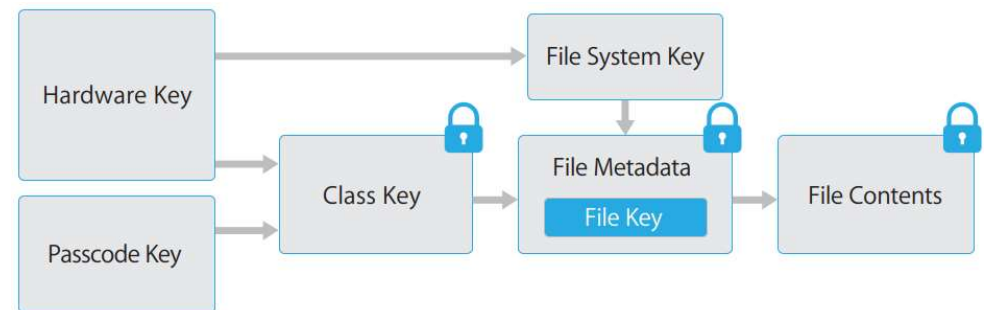
Encryption since iPhone 3GS

Two hardware keys (no software or firmware can read them directly)

- Unique ID (UID): unique per device
- Group ID (GID): unique per processor generation

Secure enclave since iPhone 5S (A7 chip and later)

- Security coprocessor (SEP)
- Handles sensitive Information
- Runs its own operating system



Effaceable storage

- A dedicated area of NAND storage, used to store cryptographic keys, that can be addressed directly and wiped securely

iTunes Backup

iTunes backup creates a copy of the information from your Apple device

Does not include

Content from the iTunes and App Stores, or PDFs downloaded directly to Apple Books

Content synced from iTunes, such as imported MP3s or CDs, videos, books, and photos

My Photo Stream

Face ID or Touch ID settings

Apple Pay information and settings

Activity, health, and keychain data (only in encrypted iTunes backup)

Location of iTunes backups

Windows computer:

%AppData%\Apple Computer\MobileSync\Backup\

On a Mac:

~/Library/Application Support/MobileSync/Backup/

Encrypted iTunes Backup

iTunes backup can be encrypted with a separate backup password which locks and encodes your data

Does also include

Your saved passwords

Wi-Fi settings

Website history

Health data

If you cannot remember your backup password:

- Pre-iOS 11: it is not possible to disable backup encryption for a device without knowing the backup password
- iOS 11: backup password can be removed in settings app (access to device required)

Encrypted iTunes Backup Security

Different versions of operating systems have different security implementations

manifest.plist – contains all the information needed to crack the backup

Hashes are salted - no rainbow tables!

iOS 3
pbkdf2_sha1(2,000)

iOS 10.0
Same as above works
Single sha256 hash is also stored (very weak)

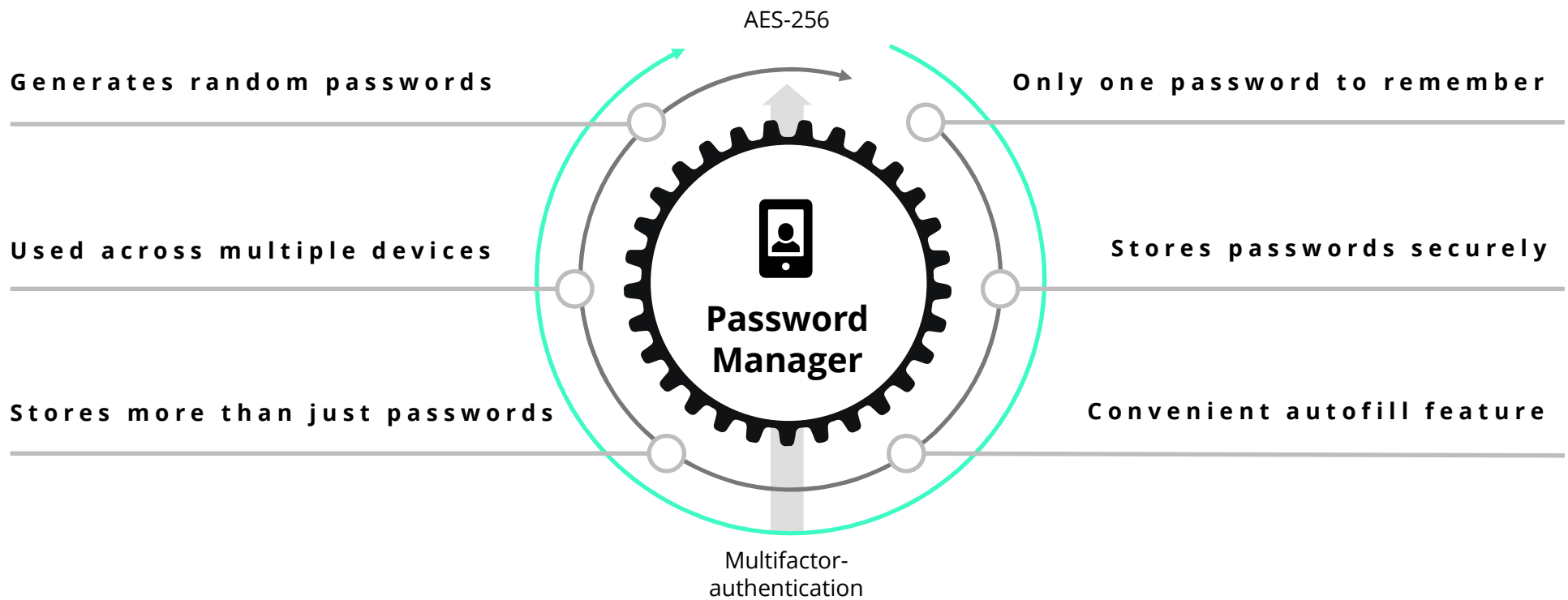
iOS 4 to 10.1 (but 10.0)
Same as iOS 3, but 10,000 iterations

iOS 10.2+
pbkdf2_sha256 (10,000,000)
pbkdf2_sha1 (10,000)

DEMO: iTunes Backup

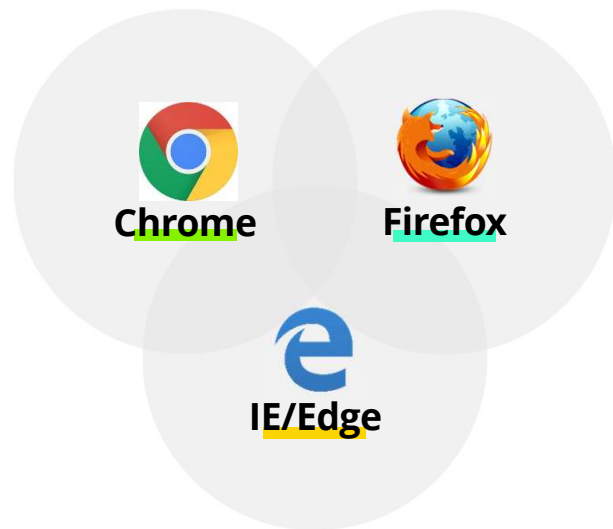


Password Manager



Browser Password Manager

Different variants of browser password managers with strikingly different levels of security



Chrome

- Chrome without account (default)
- Chrome Sync (Google Acc.)
- Chrome Sync with passphrase

Firefox

- Firefox without account (default)
- Firefox Sync (Firefox Acc.)
- Firefox PW with master password
- Lockbox (beta)

IE/Edge

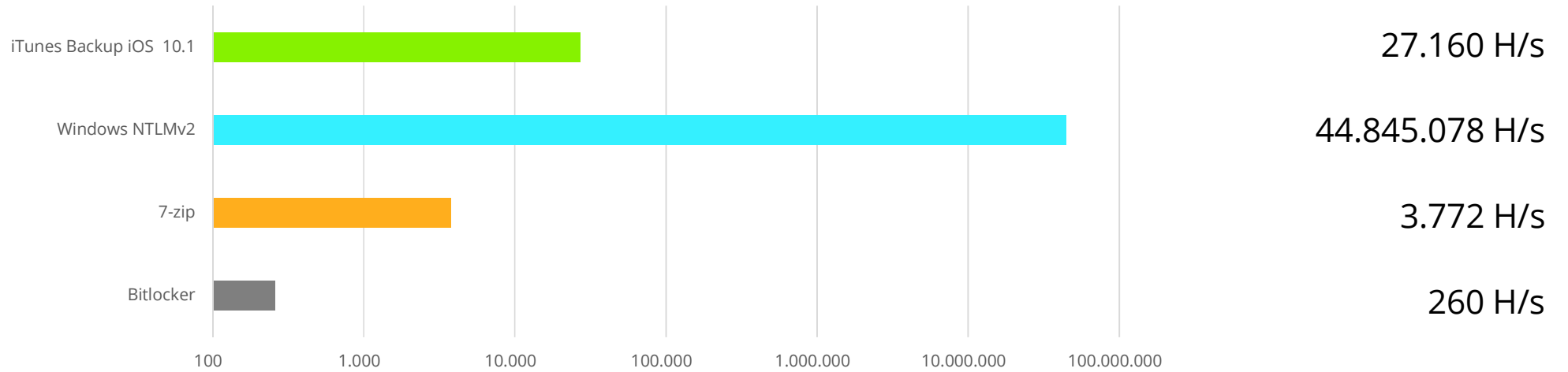
- Edge without account (default)
- Edge Sync (Microsoft Acc.)

Be careful with default implementation of BPMs!

PASSWORDS

Passware Speed Comparison

Benchmark based on Passware 2017 and NVIDIA Tesla K20m Graphics Card



Justin Schuh, Chrome browser security tech lead

**The only strong
permission boundary for
your password storage is
the OS user account**

Firefox Bug 524403 - https://bugzilla.mozilla.org/show_bug.cgi?id=524403

Bug 524403
softtoken's master password KDF process should be stronger (currently easily brute forced due to low iteration count) [Get help with this page](#)

NEW Unassigned (NeedInfo from [rrelyea](#))

Status

Product: NSS Reported: 9 years ago
Component: Libraries Modified: 6 days ago
Importance: P5 normal
Status: NEW

People (Reporter: Dolske, Unassigned, NeedInfo)


Tracking

Version: trunk Blocks: 973759
Target: --- Duplicates: [584528](#)
Keywords: sec-want

Firefox Tracking Flags (Not tracked)

Details (Whiteboard: [sg:want P2])

Bottom ↓ Tags View ▾


 **Justin Dolske [:Dolske]** (Reporter)
Description • 9 years ago

I recently ran across "Firemaster", a master password cracking tool (<http://www.securityxploded.com/firemaster.php>). The keys-per-second claimed seemed higher than I was expecting, so I went looking at exactly how the master password was handled by softtoken.

Skimming over a few details, sftkdb_passwordToKey() first computes an intermediate key with just SHA1(salt, passphrase). This is then used in sftkdb_DecryptAttribute() as input to a PKCS#5 PBKDF1 routine. **The default iteration count is just 1** though [set by sftkdb_EncryptAttribute() passing 1 to nsspkcs5_NewParam()].

A higher iteration count would make this more resistant to brute forcing (by increasing the cost of testing password), the PKCS#5 spec suggests a "modest value" of 1000 iterations. And that was 10 years ago. :)

As an implementation detail, it might be better to change sftkdb_passwordToKey() to actually use PKCS#5 with a high iteration count (instead of just a single simple hash). and leave sftkdb_EncryptAttribute() as-is. The intermediate key is only computed once, so attribute crypting would remain existing DBs.]

 **Mark Straver**
Comment 31 • 7 months ago

A few weeks of silence have passed. Robert, what do you think? I clearly like the simple short-term solution to secure the pw store without a complicated migration path for a different crypto approach, with further improvements down the line.

Flags: needinfo?(rrelyea)

DEMO: Firefox PM
DEMO: Oxygen





Thank you

Mikhail Arshinskiy

Contact: marshinskiy@deloitte.at

SOURCES:

- https://www.researchgate.net/publication/267986937_Mobile_Forensics_overview_of_digital_forensic_computer_forensics_vs_mobile_forensics_and_tools
- <http://gs.statcounter.com/os-market-share/mobile/worldwide/#>
- <http://www.militarysystems-tech.com/articles/mobile-forensics-solutions-pc-based-ufed-software-turnkey-hardware>
- <https://www.youtube.com/watch?v=aw57j3usRRw>
- https://lcdiblog.champlain.edu/wp-content/uploads/sites/11/2014/10/1027291_orig.png

This publication contains general information only, and none of the member firms of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collective, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte USA LLP, Deloitte LLP and their respective subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

**Copyright © 2018 Deloitte Development LLC.
All rights reserved. Member of Deloitte Touche Tohmatsu Limited**