Apple iCloud inside out

iCloud backups, FindMyPhone, document storage, iCloud keychain

DeepSec 2013, Vienna, Austria
Vladimir Katalov, ElcomSoft Co. Ltd.
Global smartphone market

- About 1.2 billion smartphones worldwide
- “Smart devices” – carry a lot of sensitive data
- Corporate deployments are increasing
- ... hard need for forensics!

(Source: IDC Worldwide Quarterly Mobile Phone Tracker)
# Smartphone forensics methods

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>iOS</th>
<th>Windows Phone</th>
<th>BlackBerry OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical acquisition</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>?</td>
</tr>
<tr>
<td>Physical acquisition</td>
<td>Yes/No</td>
<td>Yes/No</td>
<td>No</td>
<td>Yes*</td>
</tr>
<tr>
<td>Chip-off</td>
<td>Yes/No</td>
<td>No</td>
<td>?</td>
<td>Yes</td>
</tr>
<tr>
<td>Local backup</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cloud backup</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Documents in cloud</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Location service</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
iOS forensics

- Physical acquisition
  - Boot-time exploit to run unsigned code or jailbreak
  - Device lock state isn’t relevant, can bruteforce passcode
  - Can get all information from the device (incl. deleted data)
- Logical acquisition
  - “Ask” device to produce backup
  - Device must be unlocked*
  - Device may produce encrypted backup
  - Limited amount of information (but more than you think)
- Advanced logical acquisition
  - By direct access to some services running on the iPhone
  - Device must be unlocked*
  - Limited amount of information (some as in local backup, but plus something extra)
  - Backup password isn’t relevant
  - Can be performed over Wi-Fi
- iCloud
  - Need Apple ID and password
  - Can be performed without the device itself
  - Almost the same information as in local backup
  - Can get the documents and location data, too

* But there is a workaround :)
iOS passcode

- Device passcode
  - Protect unauthorized access to the device
  - Bypassing is not enough (used in encryption)
- Disk encryption
- Keychain
  - System-wide storage for sensitive data (keys, passwords etc)
  - Data is encrypted
Backups - what & when

- Contacts and Contact Favorites
- Messages (including iMessages)
- Call history
- Application data
- Device settings
- Camera roll (photos and videos)
- Purchases (music, movies, TV, apps, books)
- Mail accounts
- Network settings (saved Wi-Fi hotspots, VPN settings etc)
- Paired Bluetooth devices
- Safari bookmarks, cookies, history, offline data
- ... and much more

★ Local backups
- iTunes create backups when:
  - Sync with iTunes
  - [File] | [Devices backup]

★ iCloud backups
- Backup runs daily when device is:
  - Connected to the Internet over Wi-Fi
  - Connected to a power source
  - Locked
- Can force backup
  - [Settings] | [iCloud] | [Storage & Backup] | [Back Up Now]
## iPhone 5 Global

![iPhone 5](image.png)

- **Vladimir's iPhone 5**
- **iOS 7.0.2** (build 11A501)
- **Phone Number:** +7 (985) 998-68-20
- **Serial Number:** C39JT46F39D
- **Unique Identifier:** b026b06988940617008c9f81dd9e6ab13e07bbcc
- **IMEI:** 0113420001267660

## What's In Backup

(Note: Before making any changes please select Duplicate from the File menu to make a copy of the backup)

<table>
<thead>
<tr>
<th>Backup Date</th>
<th>Tue Oct 22 09:59:11 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Location</td>
<td>/Users/vkatalov/Downloads/b026b06988940617008c9f81dd9e6ab13e07bbcc</td>
</tr>
<tr>
<td>Total</td>
<td>8677 Files, 13.4 GB</td>
</tr>
</tbody>
</table>

**System Files:** 4698 Files, 12.8 GB

**User Information:**
- Contacts
- Messages
- Call History
- Calendars
- Notes
- Recent Email Address
- Safari Bookmarks
- Safari History

**Multimedia Files:**
- Camera Roll
- Voice Mails
- Voice Memos
- Other Multimedia Files

**User App:** 134 Apps, 3979 Data Files, 578.5 MB
But wait, there is more...

Google Apps data: Search, Maps, YouTube, Gmail, Drive, Translate, Orkut etc.)

AppDomain-com.google.*

**Social networking & communications**

AppDomain-net.whatsapp.WhatsApp\*
AppDomain-com.burbn.instagram\*
AppDomain-com.facebook.Facebook\*
AppDomain-com.facebook.Messenger\*
AppDomain-com.skype.skype\*
AppDomain-com.atebits.Tweetie2\*
AppDomain-com.linkedin.LinkedIn\*
AppDomain-com.naveenium.foursquare\*
AppDomain-com.viber\*

**Other**

HomeDomain\Library\Keyboard\*
HomeDomain\Library\Passes\*
HomeDomain\Library\Voicemail\*
HomeDomain\Library\Maps\*
RootDomain\Library\Caches\locationd\*

• Message attachments (even from deleted conversations!)
• Pictures from twitter posts
• Last backup date & time
• Info on Wi-Fi access points you ever connected to (SSID, security, signal etc)
• ... a lot of other interesting stuff :(
<table>
<thead>
<tr>
<th>Type</th>
<th>Remote party</th>
<th>Description</th>
<th>Time stamp (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td></td>
<td>We've missed you on Twitter, Patrick...</td>
<td>9/8/2012 4:36:31 PM</td>
</tr>
<tr>
<td>SMS</td>
<td></td>
<td>We won the tender!!!</td>
<td>9/4/2012 1:27:42 PM</td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td>We think that the price is too high! L...</td>
<td>4/26/2011 7:22:06 AM</td>
</tr>
<tr>
<td>Kik Message</td>
<td>John Crow</td>
<td>We have a cat now!</td>
<td>9/8/2012 10:12:11 AM</td>
</tr>
<tr>
<td>Kik Message</td>
<td>Nina Lanie</td>
<td>Water flowers - ask Clara</td>
<td>10/12/2011 11:20:00 AM</td>
</tr>
<tr>
<td>MMS</td>
<td>+79688865326</td>
<td>Watch out! We have guests!</td>
<td>9/8/2012 3:39:49 PM</td>
</tr>
<tr>
<td>WhatsApp message</td>
<td>Mr John Peter Crow</td>
<td>Watch &quot;Hall Yeah! Covers...</td>
<td>12/18/2012 1:35:01 PM</td>
</tr>
<tr>
<td>Texte messages</td>
<td></td>
<td>Wanted to send a photo</td>
<td>12/4/2011 10:31:30 AM</td>
</tr>
<tr>
<td>Kakao Talk messages</td>
<td>Mr John Peter Crow</td>
<td>Wanna see this photo?</td>
<td>10/12/2011 2:01:56 PM</td>
</tr>
<tr>
<td>Kakao Talk messages</td>
<td>Patrick</td>
<td>voice note</td>
<td>11/8/2012 2:01:56 PM</td>
</tr>
<tr>
<td>Kakao Talk messages</td>
<td>Lena Soloveva</td>
<td></td>
<td>11/8/2012 2:01:56 PM</td>
</tr>
<tr>
<td>Kakao Talk messages</td>
<td>Patrick</td>
<td></td>
<td>11/8/2012 2:01:56 PM</td>
</tr>
<tr>
<td>Opera Mini history</td>
<td></td>
<td></td>
<td>11/8/2012 2:01:56 PM</td>
</tr>
<tr>
<td>Opera Mini history</td>
<td></td>
<td></td>
<td>11/8/2012 2:01:56 PM</td>
</tr>
<tr>
<td>Line messages</td>
<td>John Crow</td>
<td>Visit private club with Mark Allen</td>
<td>2/23/2013 6:56:00 AM</td>
</tr>
</tbody>
</table>

**Evidence note**

Mr Crow John Peter
Nickname: Good Guy
Birthday: 5 July 1970
Company: SPS LTD
Job title: CEO
Mobile: +79688865326
Work: vpetrov123@gmail.com
Other: john@yahoo.com
Home Page: www.bestservices.com
Home: www.johncrow.com
Work: www.sps.org
Note: Do not call him on weekends
Father: Bob
Mother: Sara
Country: United States
Country: United Kingdom

**Attachments**

- **IMG_2714.jpg**
  - Description: Item cata
  - MIME Type: image/jpeg

- **text_0002.txt**
  - Description: Item cata
  - MIME Type: text/plain
Frequent locations (iOS 7)

Frequent Locations
Allow your iPhone to learn places you frequently visit in order to provide useful location-related information.

Improve Maps
Allow Apple to use your frequent location information to improve Maps. Learn More...

HISTORY
Moscow, Moscow
9 locations recorded 11.09.13 - 21.10.13
Bang Phli, Samut Prakan
1 location first recorded on 19.10.13
Elsewhere
15 locations recorded 24.09.13 - 19.10.13
Kuala Lumpur, Kuala Lumpur
4 locations recorded 16.10.13 - 19.10.13
Prague, Prague

Home
26 visits recorded since 11 сентября 2013 г.
Звездный бульвар 21
9 visits recorded since 11 сентября 2013 г.
улица Генерала Антонова 2
2 visits recorded since 14 сентября 2013 г.
улица Введенского 16
1 visit recorded since 21 октября 2013 г.
улица Кржижановского 18к3
1 visit recorded since 13 октября 2013 г.

Madeira
4 visits recorded since 24 сентября 2013 г.
Muelle Pantalán
2 visits recorded since 29 сентября 2013 г.
Avenida Arriaga 4
2 visits recorded since 24 сентября 2013 г.
Kuala Lumpur Airport
1 visit recorded since 19 октября 2013 г.
Kuala Lumpur Airport
1 visit recorded since 19 октября 2013 г.
Home, sweet home...

If you choose to enable Improve Maps, Apple will collect the GPS coordinates obtained through the Frequent Locations feature on your device and correlate them with the street address associated with your Apple ID. This will enable Apple to better approximate the geographic location of that and other addresses. Apple will only retain the resulting coordinates in an anonymous form to improve Maps and other Apple location-based products and services. You can turn off Improve Maps or Frequent Locations at any time under Settings > Privacy > Location Services > System Services > Frequent Locations.
Touch ID

“All fingerprint information is encrypted and stored securely in the Secure Enclave inside the A7 chip on the iPhone 5s; it’s never stored on Apple servers or backed up to iCloud.”

(From “Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World” at apple.com)
Backups when charging??
Pair-locking

- iOS device: /var/root/Library/Lockdown
- Mac: /var/db/lockdown

`lockdownd` service

- backup service
  - software installation service
  - get device name & UDID
  - sync data
  - retrieve a screenshot
  - request iOS diagnostic information
  - put device into recovery mode
  - manage provisioning profiles

More information:

- How to Pair-Lock Your iOS Device
  http://www.zdziarski.com/blog/?p=2307

- How Juice Jacking Works
  http://www.zdziarski.com/blog/?p=2345

- libmobiledevice
  http://www.libmobiledevice.org

Thanks to Jonathan Zdziarski (@JZdziarski)
Advanced logical acquisition

- for jailbroken devices - the entire file system
- device information: name, model, IMEI, UUID, serial number etc
- all the media (photos, videos, iTunes library, iBooks)
- application data (including temporary files and *caches* folder)
- various device settings
- log files and diagnostic information
- cached web data (e.g. pictures from social networks)
- keyboard typing caches
- SMS and iMessages (including attachments, even to deleted messages)
- address book
- calendar
- voice mail
- .WAL (Write-Ahead Logging) files for most SQLite databases
- for jailbroken devices - the entire file system
- ...and more

Works even if device is passcode-locked and backup encryption is set
Can be done over Wi-Fi
Only need the pairing record
iCloud Control Panel
iCloud backups reverse-engineering

- no backup to iCloud from iTunes :(  
  so...
- jailbreak iPhone
- Install Open SSH, get keychain (keychain-2.db)
- [Settings] | [iCloud] | [Delete Account] | [Delete from My iPhone]
- [Settings] | [General] | [Reset] | [Reset All Settings]
- reboot
- set up Wi-Fi connection (proxy)
- replace keychain with our own trusted root certificate (need key 0x835 & keychain)
- ... read all the traffic :(
iCloud backup protocol flow

- Dynamic: endpoints depend on Apple ID
- Built on Google Protocol Buffers (mostly)
- Files are split into chunks
- Apple provides file-to-chunks mapping, chunk encryption keys, and full request info to 3rd-party storage provider (Amazon/Microsoft)
- Encryption key depends on chunk data
Files in iCloud
iCloud backup: authentication

query:
https://setup.icloud.com/setup/authenticate/$APPLE_ID$,

Authorization: Basic <authentication data>
authentication data = mime64 (AppleID:password)

returns: mmeAuthToken, dsPrsID

example:

GET /setup/authenticate/$APPLE_ID$ HTTP/1.1
Host: setup.icloud.com
Accept: */*
User-Agent: iCloud.exe (unknown version) CFNetwork/520.2.6
X-Mme-Client-Info: <PC> <Windows; 6.1.7601/SP1.0; W> <com.apple.AOSKit/88>
Accept-Language: en-US
Authorization: Basic cXR0LnRId3RAaWNtb3VkLmNvbTqRd2VydHkxMjM0NQ==
iCloud backup:
get auth. token, backup IDs, keys

query:
https://setup.icloud.com/setup/get_account_settings
Authorization:Basic <authentication data>
authentication data = mime64 (dsPrsID:mmeAuthToken)
returns: mmeAuthToken (new/other one!!)

query:
https://p11-mobilebackup.icloud.com/mbs/(dsPrsID)
Authorization: <authentication data>
authentication data = mime64 (dsPrsID:mmeAuthToken)
returns: list of backup IDs (backupudid)

query:
https://p11-mobilebackup.icloud.com/mbs/2005111682/(backupudid)/getKeys
Enumerate snapshots

HTTPS GET
https://p11-mobilebackup.icloud.com/mbs/(dsPrsID)/(backupudid)/(snapshotid)/listFiles?offset=(offset)&limit=(limit)

Get file authentication tokens

HTTPS POST
https://p11-mobilebackup.icloud.com/mbs/(dsPrsID)/(backupudid)/(snapshotid)/getFiles

Get URLs for file chunks

HTTPS POST
https://p11-content.icloud.com/(dsPrsID)/authorizeGet
iCloud backup: download files (2)

Download chunks

Windows Azure:
http://msbnx000004.blob.core.windows.net:80/cnt/g6YMJKQBPxQruxQAr30C?sp=r&sr=b&byte-range=154-31457433&se=2013-06-07T10:14Z&st=2013-06-07T09:19Z&sig=0EdHy75gGHCe%2BjKePZBqz8xbWxpTxaYyASwFXVx2%2Fg%3D

'se' contains iCloud authorization time (expires in one hour)

Amazon AWS:
http://us-std-00001.s3-external-1.amazonaws.com/I9rh20QBPX4jizMAr3vY?x-client-request-id=739A222D-0FF5-44DD-A8FF-2A0EB6F49816&Expires=1371208272&byte-range=25556011-25556262&AWSAccessKeyId=AKIAIWWR33ECHKPC2LUA&Signature=PxAdegw0PLyBn7GWZCnu0bhi3Xo%3D
iCloud backups: data encryption

- get keyData from iCloud
- wrappedOffset = keyDataSize - (ECP_LEN + WRAPPED_KEY_LEN)
- get wrappedKey (at wrappedOffset)
- get CLASS_KEY
  - iOS 5/6: ((UINT32*)(keyData + wrappedOffset))[-1]
  - iOS 7: ((UINT32*)(keyData + wrappedOffset))[-3]
- decrypt wrappedKey using CLASS_KEY
- get AES_KEY from wrappedKey
- file decryption: by 0x1000 blocks (unique IV for every block)

```c
#define HFS_IV_GENERATOR 0x80000061
#define IV_GEN(x) (((x) >> 1) ^ (((x) & 1) ? HFS_IV_GENERATOR : 0))

static UInt8 *genIV (UInt32 seed, void *pIV) {
    UInt32 *pdw = (UInt32*)pIV;
    pdw[0] = seed = IV_GEN(seed);
    pdw[1] = seed = IV_GEN(seed);
    pdw[2] = seed = IV_GEN(seed);
    pdw[3] = seed = IV_GEN(seed);
    return (UInt8*)pIV;
}

// to get aesIV: sha1(AES_KEY)
AES_KEY aesIV;
makeIVkey (&aesIV, abKey, SYSTEM_KEY_LEN);
(abKey is AES_KEY we have got from wrappedKey)

static AES_KEY *makeIVkey (AES_KEY *pAES, UInt8 *pb, size_t cb) {
    SHA_CTX sha;
    UInt8 abHash[SHA_DIGEST_LENGTH];
    SHA1_Init (&sha);
    SHA1_Update (&sha, pb, cb);
    SHA1_Final (abHash, &sha);
    AES_set_encrypt_key (abHash, 128, pAES);
    return pAES;
}
```
iCloud encryption

- Data stored at 3rd-party storage providers is encrypted
- Apple has encryption keys to that data
- Few files are further encrypted using keys from OTA backup keybag
- Keychain items are encrypted using keys from OTA backup keybag
- Need key 0x835 (securityd) to decrypt most keys from OTA backup keybag

iCloud backups - summary

- There is no user-configurable encryption for iCloud backups
- iCloud backups are stored in Microsoft and Amazon clouds in encrypted form
- Apple holds encryption keys and thus have access to data in iCloud backups
  - **If Apple stores 0x835 keys then it can also have access to Keychain data (i.e. passwords)**
- Apple may have legal obligations to do this (e.g. LE)
- No notification after backup downloading (as with device restore)
Find My Phone
FindMyPhone protocol

How: just sniffing HTTP traffic (www.icloud.com, Find My Phone)

Authentication:

validate:
https://setup.icloud.com/setup/ws/1/validate

ClientBuildNumber=1M.63768 (constant)
ClientId (random GUID)
<- instance

login:
https://setup.icloud.com/setup/ws/1/login

AppleID
extended_login
id=sha1(apple_id+instance)
password
<- dsid

Get devices with location:

initClient:
https://p11-fmipweb.icloud.com/fmipservice/client/web/initClient

refreshClient:
https://p11-fmipweb.icloud.com/fmipservice/client/web/refreshClient

id
dsid
<- content (location)
FindMyPhone - demo output

Device #1
- deviceModel: SixthGen-white
- modelDisplayName: iPhone
- id: QV8TDmTwM1zIMD4y5OOG5ndaAMTCwMdhjQMy4MWRkOuU2ywITyM2UwM2JlY2M-
- deviceDisplayName: iPhone 5
- name: Vladimir's iPhone 5
- batteryLevel: 0.700216
- locationEnabled: 1
- longitude: 37.6243
- latitude: 55.8114
- positionType: wifi
- isOld: 0
- Device found: 00:00:27.786000 ago

Device #3
- deviceModel: MacBookAir3_2
- modelDisplayName: MacBook Air
- id: QV8TDgMzQFN1Q5L7dGRfkhNTztZC1CMzJjU2ZCMkRfnjA2NjIcRA~
- deviceDisplayName: MacBook Air 13
- name: Vladimir Katalov's MacBook Air
- batteryLevel: 0
- locationEnabled: 1
- longitude: 0
- latitude: 0
- positionType: isOld: 0
- Device not found

Device #6
- deviceModel: ThirdGen-4G
- modelDisplayName: iPad
- id: QV8TDjAzYj2UyzhM1yZWfZmE3NwU2Tk5YzQwYzQwNDJiYyIjNkRkZig~
- deviceDisplayName: iPad
- name: Vladimir Katalov's iPad
- batteryLevel: 0.74746
- locationEnabled: 1
- longitude: 37.6245
- latitude: 55.8113
- positionType: Wifi
- isOld: 0
- Device found: 00:00:36.485000 ago
iCloud documents
Get files from iCloud

To get list of files

- Authentication request (with given AppleID & password). Client gets mmeAuthToken in return; which, in order, is used to create authentication token (together with dsid). dsid (Destination Signaling IDentifier) is an unique ID assigned to the user when registering at iCloud.com.

- Request to get AccountSettings. Client gets an URL (ubiquityUrl) with an address to get UUID (unique user identifier), file list, info on file tokens and for authorization.

- Request to get file list (POST). Output (for every file):
  - file name
  - file id
  - parent folder id
  - last change time
  - checksum
  - access rights

To download given file

- Request to get file token (using file id, checksum and aliasMap).

- Authorization request. Returns information on file chunks and containers. Output: container list (with URLs) and chunk information.
iCloud backup: packages

- KeyNote: PDF, Microsoft PowerPoint, KeyNote ’09
- Pages: PDF, Microsoft Word, Pages ’09
- Numbers: PDF, Microsoft Excel, Numbers ’09
- Some other programs (1Password etc)

Storage: plist + content (text, media files)

Requests:

- Validate
  https://setup.icloud.com/setup/ws/1/validate
- Login
  https://setup.icloud.com/setup/ws/1/login
- Export
- Check export status
- Download converted file
<table>
<thead>
<tr>
<th>File name</th>
<th>File path</th>
<th>File id</th>
<th>File size</th>
</tr>
</thead>
<tbody>
<tr>
<td>buildVersionHistory.plist</td>
<td>/com-apple-Pages/Documents/EIFT FAQ.pages.tef/buildVersionHistory.plist</td>
<td>4222124650662430</td>
<td>221 bytes</td>
</tr>
<tr>
<td>index.db</td>
<td>/com-apple-Pages/Documents/EIFT FAQ.pages.tef/index.db</td>
<td>4222124650662429</td>
<td>376832 bytes</td>
</tr>
<tr>
<td>index.viewstate</td>
<td>/com-apple-Pages/Documents/EIFT FAQ.pages.tef/index.viewstate</td>
<td>4222124650662435</td>
<td>713 bytes</td>
</tr>
<tr>
<td>metadata.plist</td>
<td>/com-apple-Pages/Documents/EIFT FAQ.pages.tef/metadata.plist</td>
<td>4222124650662431</td>
<td>416 bytes</td>
</tr>
<tr>
<td>preview-micro.jpg</td>
<td>/com-apple-Pages/Documents/EIFT FAQ.pages.tef/preview-micro.jpg</td>
<td>4222124650662442</td>
<td>1489 bytes</td>
</tr>
<tr>
<td>preview-web.jpg</td>
<td>/com-apple-Pages/Documents/EIFT FAQ.pages.tef/preview-web.jpg</td>
<td>4222124650662443</td>
<td>11782 bytes</td>
</tr>
<tr>
<td>preview.jpg</td>
<td>/com-apple-Pages/Documents/EIFT FAQ.pages.tef/Previews/preview.jpg</td>
<td>4222124650662444</td>
<td>45229 bytes</td>
</tr>
<tr>
<td>EIFT FAQ.jpg</td>
<td>/com-apple-Pages/iWorkPreviews/EIFT FAQ.jpg</td>
<td>4222124650662514</td>
<td>45229 bytes</td>
</tr>
</tbody>
</table>
Apple 2FA
(two-step verification)
Apple 2FA
(cont-d)

Requires to verify your identity using one of your devices before you can:

- Sign in to My Apple ID to manage your account.
- Make an iTunes, App Store, or iBookstore purchase from a new device.
- Get Apple ID-related support from Apple.

Does **NOT** protect:

- iCloud backups
- Find My Phone data
- Documents stored in the cloud
Apple iOS 7
iCloud keychain
iCloud keychain

Keychain Access

Click to lock the iCloud keychain.

Keychains
- login
- iCloud
- System
- System Roots

Category
- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates

Name | Kind | Date Modified | Keychain
--- | --- | --- | ---
appleid.apple.com (apple@elcomsoft.com) | Web form password | 11 Jun 2013 07:31:55 | iCloud
Apple iOS 7

iCloud keychain - cont-d

- iCloud Security Code

Enter your iCloud Security Code.

- Verification Code

VERIFICATION CODE SENT TO 7 (985) 998-6820

Enter Verification Code

To verify your identity, a message was sent to the phone number Apple has on file.

- Allow “Mac Mini” to use iCloud Keychain

Enter the Apple ID password for “vkatalov@mail.ru” to allow Mac Mini to use your passwords.
iCloud keychain setup
iCloud keychain components

- com.apple.preferences.icloud.remoteservice
  process that interacts with iCloud control

- com.apple.sbd
  (daemon) caching and restoring keychain, get notifications
  ~/Library/Keychain/keychain-2.db

- com.apple.lakitu
  (daemon) talks to iCloud (get requests from com.apple.sbd, make queries to iCloud, get and decrypt responses, passes them back to com.apple.sbd)

- secd
  (daemon) caching and restoring keychain, get notifications

- AppleKeyStore.kext
  driver to interact with KVS (key-value storage)

- Security.framework
  functions to restore keychain, save it to SQLite database, send notifications (e.g. to Keychain access)

- libcorecrypto.dylib
  encryption/decryption
Setup iCloud keychain

Diagram showing the process of setup iCloud keychain with various steps including:
- Setting up iCloud Keychain
- Entering pass code
- Recovering records
- On keychain downloaded (NSUbiquitousKeyValueStore)
- Decrypting backup password
- Restoring keychain with backup password
- Secure keychain in restore syncable (KeyBag, KeyBagKey, keychain)
- Restoring keychain with backup password
- Keychain actions
- Security framework
Query:
POST https://p18-keyvalueservice.icloud.com/sync HTTP/1.1
Host: p18-keyvalueservice.icloud.com
Authorization: X-MobileMe-AuthToken MTc3Mzg ... meWRINDg9
[
<dict>
    <key>apns-token</key>
    <data>
    D7wxUExz2av7JaSgJD6j2yQKENzH0e4DGJzfOeLBbYA=
    </data>
    <key>apps</key>
    <array>
        <dict>
            <key>bundle-id</key>
            <string>com.apple.security.cloudkeychainproxy3</string>
            <key>kvstore-id</key>
            <string>com.apple.security.cloudkeychainproxy3</string>
            <key>registry-version</key>
            <string>FT=-@RU=40c72786-6f77-4190-85d8-3ae1f4df91ca@S=1296</string>
        </dict>
        <dict>
            <key>bundle-id</key>
            <string>com.apple.sbd</string>
            <key>kvstore-id</key>
            <string>com.apple.sbd3</string>
            <key>registry-version</key>
            <string>FT=-@RU=40c72786-6f77-4190-85d8-3ae1f4df91ca@S=1259</string>
        </dict>
    </array>
    <key>service-id</key>
    <string>iOS</string>
</dict>
Response:
<dict>
    <key>apps</key>
    <array>
        <dict>
            <key>kvstore-id</key>
            <string>com.apple.security.cloudkeychainproxy3</string>
            <key>keys</key>
            <array>
                <dict>
                    <key>data</key>
                    <data>
                    AYYkF93rOBg ... AABVag==
                    </data>
                    <key>name</key>
                    <string>com.apple.securebackup.record</string>
                </dict>
            </array>
            <key>bundle-id</key>
            <string>com.apple.sbd</string>
        </dict>
    </array>
    <key>timestamp</key>
    <integer>1384690786479</integer>
</dict>

Sync (get KeyChain and KeyBag)
srp_init

POST https://p18-escrowproxy.icloud.com:443/escrowproxy/api/srp_init HTTP/1.1
Host: p18-escrowproxy.icloud.com:443

[...]
<dict>  
  <key>blob</key>
  <string>dSyhi0M/...CQ==</string>
  <key>command</key>
  <string>SRP_INIT</string>
  <key>label</key>
  <string>com.apple.securebackup.record</string>
  <key>phoneNumberToken</key>
  <string>AQAAAABSidUhUkYydkSNDx8dc4r/QMudn0Q1ctg==</string>
  <key>version</key>
  <integer>1</integer>
</dict>
</plist>

HTTP/1.1 200 OK

recover

POST https://p18-escrowproxy.icloud.com:443/escrowproxy/api/recover HTTP/1.1
Host: p18-escrowproxy.icloud.com:443

[...]
<dict>  
  <key>blob</key>
  <string>AAAAYAAA...+m8</string>
  <key>command</key>
  <string>RECOVER</string>
  <key>version</key>
  <integer>1</integer>
</dict>
</plist>

Ответ:
HTTP/1.1 200 OK

[...]
Apple iCloud: Conclusion

- Balance between security, privacy and convenience
- iCloud security risks
- Use additional encryption
- Better 2FA implementation
- Need further work
  - My Photo Stream
  - Photo Sharing
  - 3rd party apps data
  - Back To My Mac
  - Frequent locations
  - Touch ID (iPhone 5S)
  - iCloud keychain

After all, does Apple (read: NSA) have access to your data? ;)
Thank you!

Vladimir Katalov, ElcomSoft Co. Ltd.
(twitter: @vkatalov)

http://www.elcomsoft.com
http://blog.crackpassword.com
Facebook: ElcomSoft
Twitter: @elcomsoft