Apple Health

Vladimir Katalov, ElcomSoft

Heartrate  Sleeping habits  Workouts  Steps and walking routines

© ElcomSoft Ltd. www.elcomsoft.com
Apple Health

What Is Apple Health?

- Introduced in Sep 2014 with iOS 8
- Health app pre-installed on all iPhones
- Makes use of low-energy sensors
- Always active, always collecting information
- Supported by Apple Watch, additional data collected
Apple Health

Main Data Categories

- **Activity** – how much you move
- **Nutrition** – breakdown of your diet
- **Sleep** – your sleep habits
- **Mindfulness** – native support limited to Mindful Minutes, Activity and Sleep; third-party apps help build out your mindfulness data. Pretty meaningless in its current state, may improve in iOS 12
Apple Health

Additional Data Categories

- **Body Measurements** – height and weight
- **Health Records** - CDA + Health Records
- **Heart** – blood pressure, heart rate
- **Reproductive Health** – sexual activity and menstruation cycles
- **Results** – various medical test results (e.g. sugar level)
- **Vitals** – blood pressure, body temperature, heart rate, breathing rate
- **Medical ID** – essential medical data:
Apple Health

Clinical Document Architecture (CDA)

- Standard architecture for transferring health information across medical facilities
- Widespread in USA, UK, Australia
- XML format
- CDA documents are stored in Health Records
- Prior to iOS 11 Health Records only contained CDA documents
Apple Health

Clinical Document Architecture (CDA)

- Registering a CDA document in Apple Health
  - Must receive complete file (e.g. from the hospital)
  - Open with Apple Health app
  - Data will be synced with other devices via iCloud
- Contains highly sensitive medical information
Apple Health

Health Records

- March 2018: **Apple Health Records**
- 39 US hospitals joined at the time of introduction
- The number of participating facilities quickly growing
- FHIR (Fast Healthcare Interoperability Resources) interoperability via HealthKit
Apple Health

Apple Health Records

- What’s inside:
  - Information about allergies, chronic diseases, immunizations
  - Lab tests, prescriptions, studies
  - Basic health data
Apple Health

Third Party Access

- Third-party apps have access to Health data
- User permission required
  - Do you trust all of them?
- Other types of data leaked before (Celebgate, location leaks etc.)
- Can Health data leak?
- Leaked Health data may be used for targeted advertising
Apple Health

Where Apple Health Gets Data From

- Manual entry in the Health app
- Data received from HealthKit devices (iPhone, Apple Watch, compatible fitness trackers etc.)
- Third-party apps (Nike+, MyFitnessPal, Pillow)
Apple Health

Where Apple Health Gets Data From

- Manual entry in the Health app
  - CDA documents
  - Electronic medical card data
- No Health Records
Apple Health

Where Apple Health Gets Data From

- Data received from HealthKit devices (iPhone, Apple Watch, compatible fitness trackers etc.)
  - Automatic data submission
  - Pulse, blood pressure
  - Data for Mindfulness, Heart and Activity
  - Apple Watch collects Sleep data; **no automatic mode** (third-party apps can be used)
Apple Health

Apple Watch

- Apple Watch contributes greatly to Health data
- Compatible with third-party apps (e.g. Pedometer++, Runkeeper)
- Steps (Health app calculates distance travelled)
- Heart rate
- Basic activity info: how long you stand, how much you exercise, calories burned
- New: Apple Watch 4 supports ECG (Electrocardiogram) (US only)
Apple Health

Apple Watch

- New: Fall detection
- Three fall patterns
- Automatic call to emergency number
- Logs and syncs fall events
- Essential bit of evidence: exact timestamp (down to the second) of the crime
  - Synced with the cloud, data may be available even if phone and watch are taken from the victim
Apple Health

Where Apple Health Gets Data From

- Third-party apps (Nike+, MyFitnessPal, Pillow)
  - All data categories supported…
  - Except Health Records and Medical ID
  - Each data category has a list of “Recommended” third-party apps for collecting that type of data
  - Third-party apps must be activated in categories tracked in Health > Sources
Apple Health

Apple Watch and Health security
Apple Health

How Apple Health Data Is Stored

- Main data stored at /private/var/mobile/Library/Health/
- Two linked SQLite databases: healthdb.sqlite and healthdb_secure.sqlite
- Training geodata: healthdb_secure.hfd
- Encrypted database: healthdb_secure.hfd
Apple Health

Database Structures

- `healthdb.sqlite` mainly contains information about data sources
- `healthdb_secure.sqlite` stores basic health information with frequent links to the first DB
Someone’s iPhone
But it also can be an app:
Nike+ Run Club
MyFitnessPal

Apple Watch
Watch 1,2
4.3.1
...
Apple Health

**healthdb_secure**

- **objects**: information on “samples” including ID and source
- Samples contain information including timestamp, type, numerical data (e.g. “10 steps”) or category data (“test result positive”), and ID
- Samples are linked with “samples” table via ID
- Data values may be stored in various tables, e.g. `quantity_samples` or `cda_documents`
Apple Health

Category Samples

- Category samples contain non-numerical data
- Corresponds to list view selection in the app
- category_samples table stores these values
- Restoring category_samples values to meaningful data is essential for understanding Apple Health data
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>objects</td>
<td>Sample’s uuid and source</td>
</tr>
<tr>
<td>samples</td>
<td>id, event type and time</td>
</tr>
<tr>
<td>quantity_samples</td>
<td>Source of numeric values</td>
</tr>
<tr>
<td>category_samples</td>
<td>Non-numerical category samples (e.g. “positive” or “negative” test result)</td>
</tr>
<tr>
<td>correlations</td>
<td>Keeps references to data instances, allowing to corellate quantitative data with activities</td>
</tr>
<tr>
<td>key_value_secure</td>
<td>Information about the user</td>
</tr>
<tr>
<td>metadata_values, metadata_keys</td>
<td>Sample metadata. Could be a note, time zone etc.</td>
</tr>
<tr>
<td>workouts, workout_events</td>
<td>Cumulative information about the workout: length, calories burned, distance walked, workout type etc.</td>
</tr>
<tr>
<td>fitness_friend_activity_snapshots</td>
<td>Data received via &quot;share with friends &amp; family&quot;. The contact is linked via an extra file ActivitySharing/contacts.dat. This file contains information about the contact (name, phone number and e-mail)</td>
</tr>
<tr>
<td>cda_documents</td>
<td>Binary data of a corresponding CDA document</td>
</tr>
<tr>
<td>data_provenance</td>
<td>Allows linking data sample with data source (device, app etc.)</td>
</tr>
<tr>
<td>unit_strings</td>
<td>Metric type (lb/kg etc.) from quantity_samples</td>
</tr>
</tbody>
</table>
## Known healthdb tables

<table>
<thead>
<tr>
<th>Таблица</th>
<th>Описание</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorization</td>
<td>Authentication and sync data</td>
</tr>
<tr>
<td>cloud_sync_stores</td>
<td>Last sync data</td>
</tr>
<tr>
<td>key_value</td>
<td>App-specific values (e.g. if emergency sos mode is active)</td>
</tr>
<tr>
<td>source_devices</td>
<td>Information about devices the data was synced from</td>
</tr>
<tr>
<td>sources</td>
<td>Information on received data (source, modification date)</td>
</tr>
<tr>
<td>subscription_data_anchors</td>
<td>Data about synchronization</td>
</tr>
<tr>
<td>sync_stores</td>
<td>List of synchronization sources</td>
</tr>
</tbody>
</table>
Apple Health

Accessing Apple Health Data

- Export from Apple Health app
- Local backup
- GDPR request
- Physical acquisition
- Cloud extraction
Apple Health

Exporting Data

- Apple Health has export option
- Data can be exported to a ZIP file
- Analysis?
Apple Health

Extracting Apple Health Data: The Easy Way

- Apple Health is available via logical acquisition
- No Apple Health data in unencrypted backups!
  - Unlike keychain, which is still present in unencrypted backups, protected with a hardware key
- Set a known password before making a backup
- Make local backup (iOS Forensic Toolkit or iTunes)
- Decrypt backup, access Apple Health data
- View with Elcomsoft Phone Viewer
Apple Health

Extracting Apple Health Data: The Complex Way

- Apple Health is available via file system acquisition
- Jailbreak required
  - At this time, jailbreak is available for all versions of iOS 8.0-10, iOS 11.0-11.3.1
- Jailbreak, use Elcomsoft iOS Forensic Toolkit
- Obtain TAR image
- Open TAR with Elcomsoft Phone Viewer
Apple Health

Extracting Apple Health Data: GDPR

- EU users can access their Health data by pulling a GDPR request
- Registering GDPR request: privacy.apple.com
- Apple ID, password, 2FA required
- Takes up to 7 days to receive the data
- Multiple binary formats
Apple Health

Apple Health and Cloud

- Native Apple Health data is synced with iCloud to all registered devices
- Third-party apps operate through HealthKit
- Some third-party app data is not shared with Apple Health
- Certain apps use proprietary cloud sync (Strava, Endomondo)
- **Medical ID** data is unique per device and **does not sync**
Apple Health

Apple Health and iCloud

- Apple Health data can be obtained from iCloud
- May contain significantly more information compared to what is available on device
- Technically, Apple Health belongs to “synced data” as opposed to “cloud backups”
  - This results in significantly more reliable extraction
  - Loose expiration rules of iCloud tokens compared to backups
Apple Health

How Apple Health Data Is Synced

- Regular syncing: scheduled, after device reboot, on account change
- Data is stored in iCloud Drive (in chunks)
- Unlike iCloud Keychain or Messages, iCloud Health data has no additional protection
  - No need to enter device passcode, no additional encryption
Apple Health

Accessing Health Data

- Receive encrypted file chunks
- Request zone list
- Request zone sync
- Request file links
- Download files
Apple Health

Request Zone List

- All zones start with PrimarySyncCircle
- Followed by zone UUID, e.g. 1AA8B4D0-9B73-4D88-A740-BFE04DD8A5AC
- New zones created with logging in or on subsequent logins
- Zones are periodically merged

containerId: "com.apple.health.sync"
bundleId: "com.apple.healthd"
Request / Result:

```json
propertyName {
  name: "ChangeSet"
}
propertyValue {
  valueType: 6
  authInfo {
    owner1Dsid: "8888888888"
    fileChecksum: "\001\233\254\2671GQ\316\324mM\243\031\254\322|\017\364\233N"
    structSize: 13465
    token: "B3B9SvMwRNXBK6fGaX6vOuVLwfbWA1H5QwEAAAMR7kM"
    url: "https://p29-content.icloud.com:443"
    owner2Dsid: "8888888888"
    wrapped_key {
      name: "\003\242\000\335\266\255\312\0304\226e\344\333\235\227\226a\266\323H\364\021DM3\341\020~B\3370\346\016\017\357\375C[\346\301\311\356\261"
    }
    fileSignature: "\001\310\273\331\332\326a\337\202Xd\035e`p\277\321\226\211\222\312"
    downloadTokenExpiration: 1529588220
  }
}
```
Apple Health

Request File Links

1 {  
1: "\001\233\254\2671\GQ\316\324\243\031\254\322\017\364\233\254\f"
2: "B3B95vMwRNX\6fGaX6vOuVLwfbWA1H5QwEAAAMP7kM"
4: "\001\310\273\331\332\326\202\312"
}
Apple Health

Download Files

- Files from the list are downloaded by chunks
- Downloaded chunks must be decrypted
- record/sync request returns encrypted key (wrapped_key)
- Key is decrypted
- We’ve got a key for unwrapping encryption keys that accompany each chunk
- These keys are unwrapped with wrapped_key and are used to decrypt the chunks
- Decrypted chunks are merged into files
- Files can be saved into a ZIP archive
Apple Health

Sounds too simple?

- Synced data is received in protobuf structures
- Received structures are serialized objects described in HealthDaemon header files
- There are several types of Protobuf structures (see next slide)
Apple Health

Accessing Health Data in iCloud

We can download **synced data**, which includes Apple Health

What can go wrong:

- Two-factor authentication may be an issue
- Access to secondary authentication factor is required (unless using authentication token)
Apple Health

Accessing Health Data in iCloud

- If iCloud for Windows is installed, binary authentication token may exist
- Use Elcomsoft Phone Breaker to locate and extract the token
- Use Elcomsoft Phone Breaker to download synced data, which includes Apple Health, using the authentication token
Apple Health

iCloud Data Sync

- Health data
- If Settings | iCloud | Safari is enabled, it syncs:
  - Bookmarks
  - Open tabs
  - Reading list
  - Browsing history
  - Call logs (not in the Settings; syncs if iCloud Drive is enabled)
- Contacts, Notes, Calendars, Wallet (including boarding passes), Maps (searches and bookmarks)
- Keychain
  - With luck, password to Google Account (device passcode required)
- Messages (iMessages, SMS): since iOS 11.4 (device passcode required)
Apple Health

Authenticate into iCloud

- Using Apple ID and password:
  - Sign in
  - Respond to 2FA request
- Using iCloud token:
  - Sign in (synced data only)
  - Note: iCloud tokens do not appear to expire for synced data
Using a login and password is pretty straightforward

Two-Factor Authentication can complicate things

If the device is locked, you can pull a SIM card out and receive 2FA code
Apple Health

Vladimir Katalov, ElcomSoft

Questions?

© ElcomSoft Ltd. www.elcomsoft.com