iOS 8

Security and Privacy Changes

Alban Diquet
December 5th, 2014

Agenda

- Data Protection in iOS 8
- HealthKit
- Custom Keyboards
- Local Authentication
- Privacy Changes

Introduction

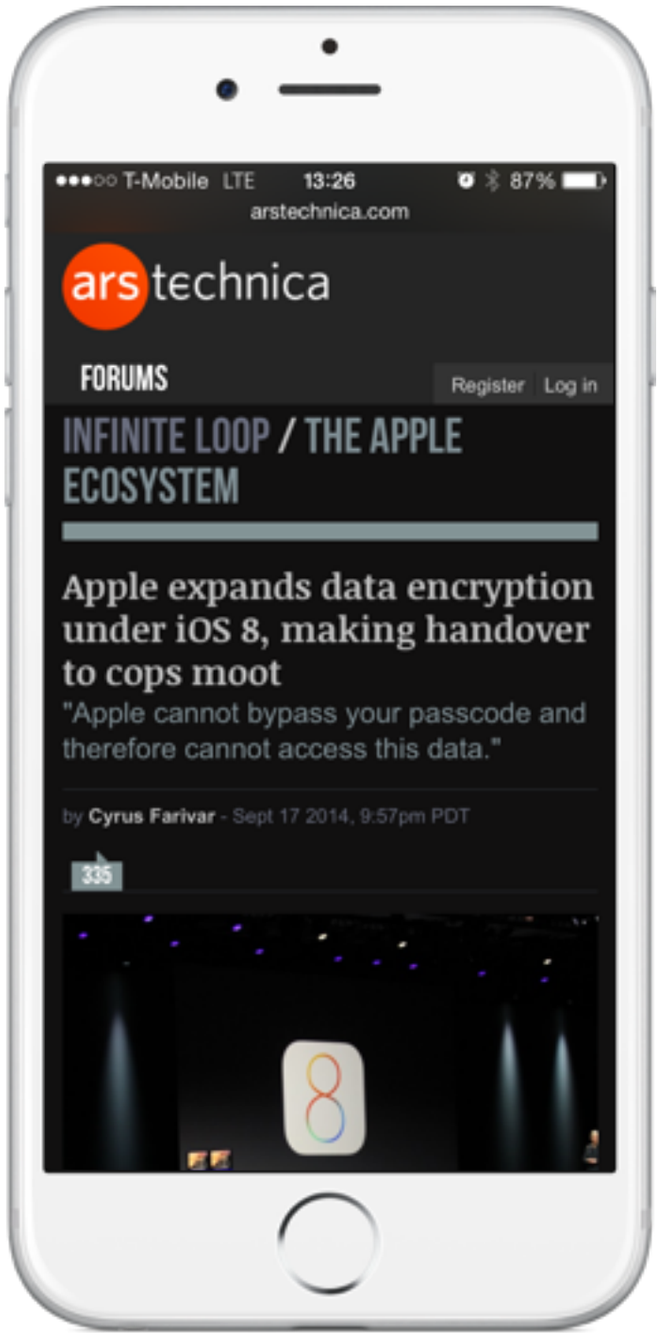
- iOS 8.0 was released on September 17, 2014
- "The biggest iOS release ever”
  - Many new APIs available to App developers
  - Significant limitations in what the OS allows Apps to do have been lifted
    - App Extensions, Metal, Nitro

Data Protection in iOS 8

- Since iOS 4, files can be encrypted using the device's passcode
  - Initially used for email messages only
  - The API was then opened to developers and Apps in iOS 5
- On iOS 8 SMSes, calendar, contacts, and photos are now protected with Data Protection

Data Protection in iOS 8

- Apple claims that files protected this way are inaccessible even to them
  - DOJ officials said that it was "marketing to criminals" and that "a child will die" because of the expanded encryption
- Pre iOS 5, Apple used to rely on a custom, Apple-signed PIN brute force tool to unlock phones for law enforcement purposes



HealthKit

- The HealthKit API was created as a centralized data store for all health information

- Apps and devices can store and retrieve health data from the phone's HealthKit store

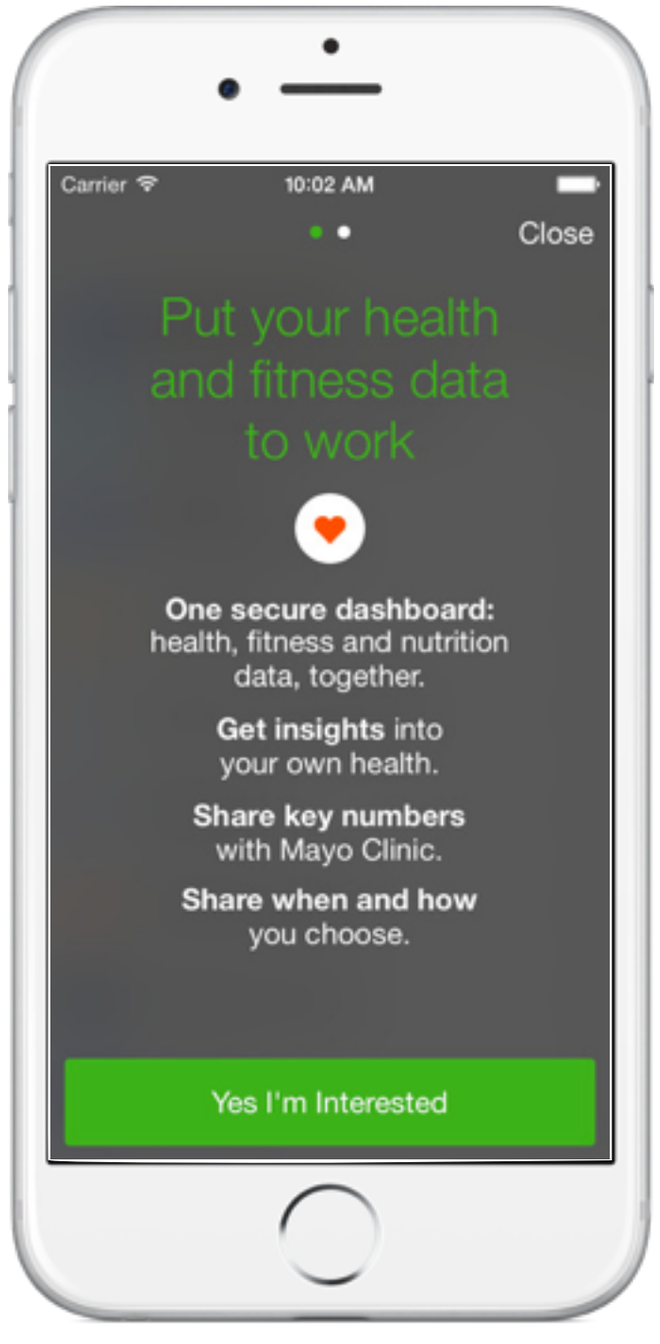
- All Apps have access to the same, device-wide store/data

HealthKit

- Apple has also partnered with major healthcare players (Mayo Clinic, software vendor Epic Systems)

- Goal is to integrate HealthKit into healthcare/hospital software

- Patient data sharing, health monitoring and alerts, etc.



HealthKit

Steps

Calories

Nike Fuel

Vitamin C

Heart Rate

Oxygen Saturation

Body Temperature

Distance

Body Mass

BMI

Blood Pressure

Potassium

Vitamin B6

RR Interval

Vitamin B12

Body Fat Percentage

BAC

Height

Respiratory Rate

Perfusion Index

Vitamin A

Blood Glucose

Vitamin D

HealthKit

- Any access to the Health store requires the user's consent
    - Permission is based on:
        - The type of access: read or write
        - The type of health data: heart rate, steps count, glucose levels, etc.
- Permission model is finer-grained than other iOS permissions (location, contacts, etc.)

Demo

HealthKit

- The Health store is encrypted when the device is locked

- HealthKit data is not saved to iCloud or synced across multiple devices*

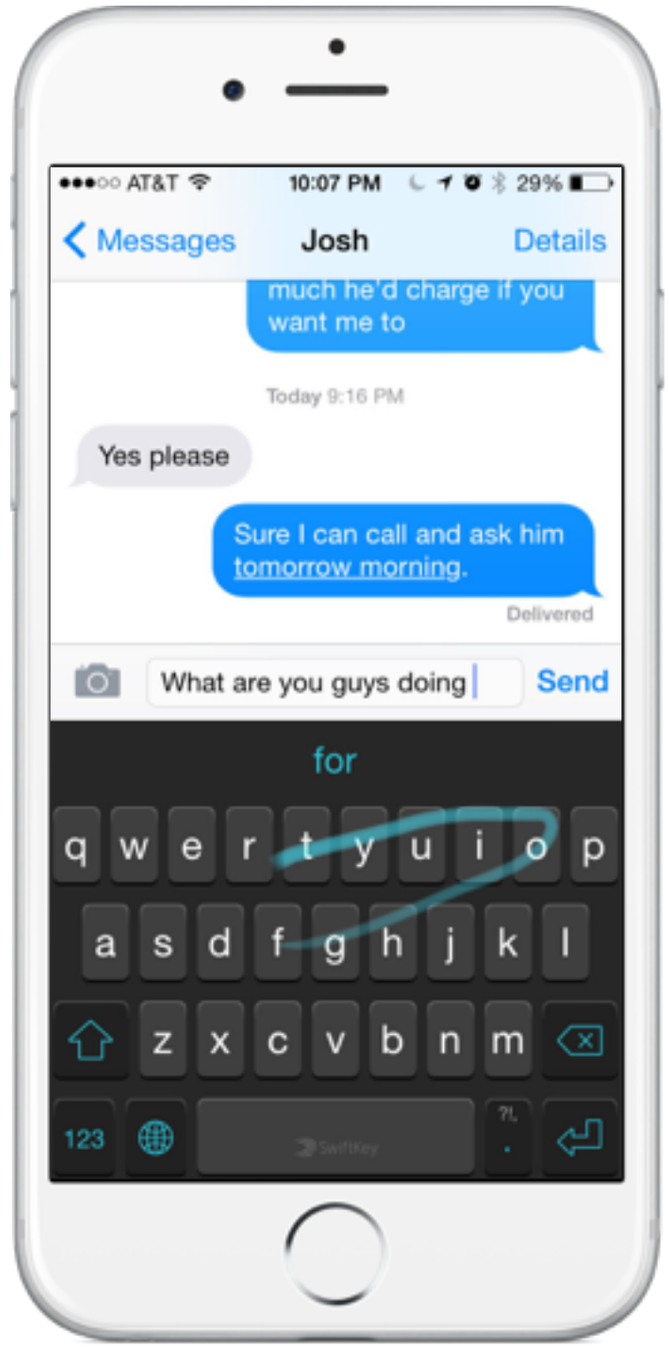
- However, nothing prevents an App that was granted access to HealthKit from misbehaving

  - Leaking data to third-parties (Apps, servers, etc.)

  - Injecting invalid data in the Health store

Custom Keyboards

- Part of the new “App Extension” APIs
- Allows the user to install 3rd party keyboards that can be used in any Apps



Custom Keyboards

- Custom keyboards are never loaded by iOS when typing in “Secure" fields
- By default, a custom keyboard has very little permissions
  - No Internet, no shared files with containing App, etc.
  - The user’s keystrokes cannot be exfiltrated

Custom Keyboards

- The developer can request for additional permissions by enabling “open access”
  - Provides access to the Internet, location, contacts and files shared with the containing App
- It seems difficult to write a full-fledged keyboard without requesting “full access”
  - No In-App purchases for monetizing extra features.
  - No network for extra processing or storing the user’s preferences

Custom Keyboards

- Research project on security and privacy-related changes in iOS 8 with CMU students
- The students looked at the custom keyboard APIs
- They wrote a key-logging custom keyboard as a proof of concept

Demo

Custom Keyboards

- Apple made an unexpected security trade-off
  - For good or bad reasons, keystrokes will definitely be logged and sent to servers
- Apps can decide to opt-out and disable custom keyboards
  - We have added a check for this to our iOS scanner

Local Authentication

- Apps can now prompt the user for either their fingerprint or their device passcode
  - Fingerprint check (TouchID) requires an iPhone 5s, 6 or 6+
  - Keychain items can also be “locked" this way
- Allows Apps to verify the user’s identity before doing something sensitive

Local Authentication

- Usual use case: prompting the user on App launch
- Prevents someone in possession of the unlocked device from accessing the App
    - Cloud storage Apps with the user's files
    - Medical Apps with the user's health data
- Harder to implement than it seems
    - Requires encrypting all of the App's files
        - Otherwise files can be accessed directly via USB

Demo

Local Authentication

- Consider using the local authentication framework to “lock" sensitive Apps
  - Relatively painless user experience, especially with TouchID
  - Developers don’t have to implement a PIN mechanism from scratch
- But don’t do what I just demo-ed…

Misc Privacy Changes

- WiFi MAC address randomization
  - Only used if cellular data is off!
- New "people picker" API for contacts access
  - Doesn’t require the contacts permission
  - Allows the user to only share one specific contact
- Apps need to provide a reason for accessing the user’s location

iOS 8 Conclusion

- iOS 8 brings useful security and privacy tools to developers
- However, some of the new APIs open the door to significant abuses by misbehaving or malicious Apps
  - HealthKit, Custom Keyboard
- This puts even more pressure on Apple's App Store vetting process
  - Not all Apps go through the App Store
  - The review process has been circumvented in the past

Questions?

Alban Diquet
December 5th, 2014

DataTheorem