

Hacking Storage in iOS

Long was the time when Mobile phones were used only for making calls or sending SMS. With Smart phone and applications running on it, definition of mobile phones has been changed in last 5 years. Provide different services, companies have started writing mobile applications. This mobile application came with ease of use for the user. Easier the application is to use, chances of having popular is more. Today, There is a mobile application for virtually everything - for banking, for shopping, to find a restaurant, to plan your travel trip, to review your business documents or last but not least social media. Only iOS platform has more than 750000 applications. To serve clients with minimal information or click, applications have started storing information on the device. As a result, One of the key checks is to look for information in the iOS device while performing iOS application security review as the biggest threat is data stored in temporary files or default locations. In 9 out of 10 applications, we find some sensitive information stored in the local device. What happens if you leave your device to someone or you are connected to open Wifi at the airport or you lose your device. All your information is in the attacker's hand which can be stored password of your bank account or a PDF statement which you downloaded from your bank account or a credit card information which you used last night to do some shopping or your home address as you came back from your friend's home last night and you were lost. We have created a list of locations where different sensitive information is usually stored. The list is divided in different categories -

System Information

Detail	Location
Applications	/var/stash/Applications
Etc	/private/etc
Var	/private/var
User	/var/mobile
Provisioning Profile	/var/mobileDevice/ProvisioningProfiles
Logs	/var/log, /var/logs /var/mobile/Library/Logs
Network Settings	/var/preferences/SystemConfiguration/com.apple.network.identification.plist
Wifi Settings	/var/preferences/SystemConfiguration/com.apple.wifi.plist
	/var/preferences/SystemConfiguration/preferences.plist
Apple ID, Owner information and Firmware	/root/Library/Lockdown/data_ark.plist

Information	
Keychain	/var/Keychains
KeyBoard Cache	/User/Library/Keyboard/dynamic-text.dat
Tmp	/private/var/tmp

Default Application Information

Detail	Location
Address Book	/var/mobile/Library/AddressBook/AddressBook.sqlitedb /var/mobile/Library/AddressBook/ AddressBookImages.sqlitedb
Last searched Google maps	/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb
Google Map History Information	/var/mobile/Library/Maps/History.plist /var/mobile/Library/Maps/Directions.plist
Calendar	/var/mobile/Library/Calendar/Calendar.sqlitedb
Data under notes application	/var/mobile/Library/Notes/notes.sqlite
Configuration file for Applications	/var/mobile/Library/Preferences
Photos	/var/mobile/Media/DCIM/
Application Pictures when HOME button is pressed (Each application has its own directory - Default applications)	/User/Library/Caches/Snapshots

Default services Information

Detail	Location
Call History (Odd number is for Outgoing calls, Even number is for Incoming calls)	/var/mobile/Library/Callhistory/call_history.db

SMS (Odd number is for Outgoing calls, Even number is for Incoming calls)	/var/mobile/Library/SMS/sms.db
Voicemail	/var/mobile/Library/Voicemail/voicemail.db
Voice mail recording	/var/mobile/Library/Voicemail/
System provided applications, ringtones and wallpapers	/var/stash
Call History	/var/wireless/Library/CallHistory
Call Log	/var/wireless/Library/logs
Call Preferences	/var/wireless/Library/Preferences

User Installed Application information

Detail	Location
Installed Applications	/User/Applications
Application Directory (Binary, supporting files)	/User/Applications/<app GUID>/<appname.app>
Applications documents i.e. images, PDF, text files	/User/Applications/<app GUID>/Documents
Application cookies	/User/Applications/<app GUID>/Library/Cookies/Cookies.binarycookies
Application Preferences (plist files)	/User/Applications/<app GUID>/Library/Preferences
Application temporary storage	/User/Applications/<app GUID>/tmp
Application crash report	/User/Library/Logs/CrashReporter
Application Screens when pressed HOME button	/User/Applications/<app GUID>/Library/Caches/Snapshots



Browser Information

Detail	Location
Browser Cookie	/var/mobile/Library/Cookies/Cookies.binarycookies
Browser favorites (Book marks)	/var/mobile/Library/Safari/Bookmarks.db
Browser History	/var/mobile/Library/Safari/History.plist
Browser Settings	/var/mobile/Library/Preferences/com.apple.mobilesafari.plist
Browser Cache	/User/Library/Caches/com.apple.WebAppCache/ApplicationCache.db