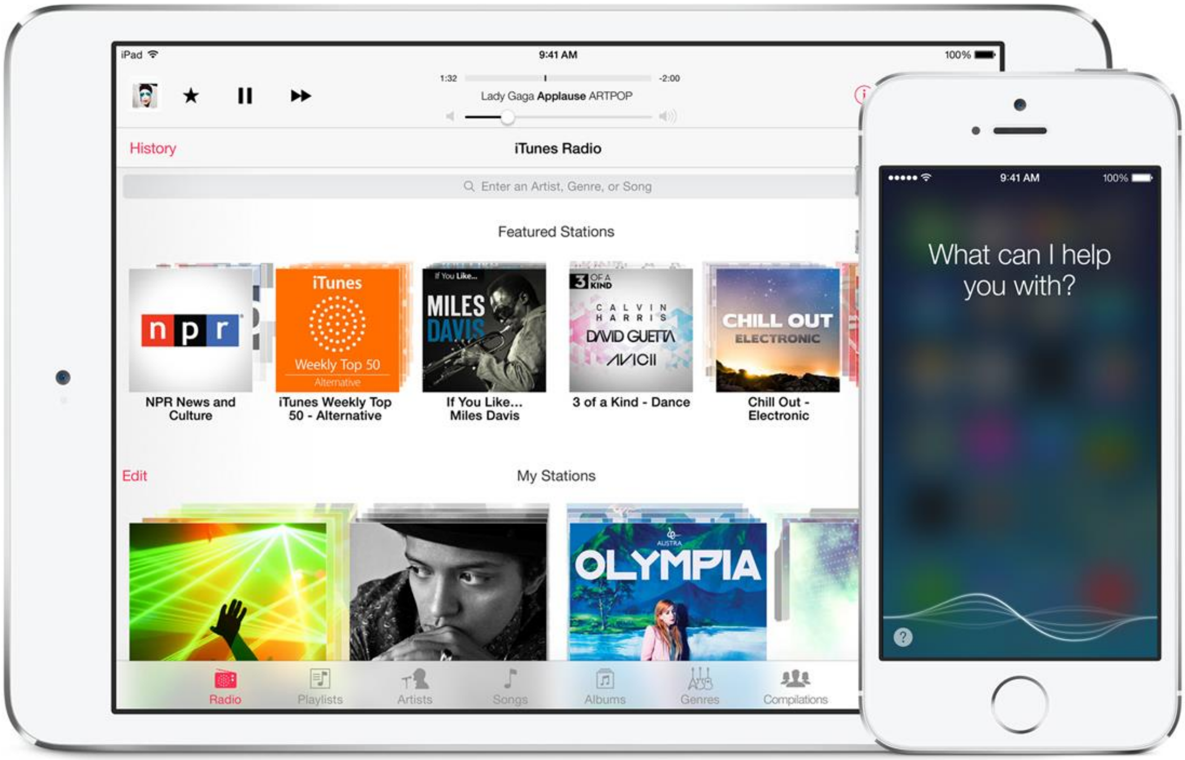
UNENCRYPTED iTunes STORE PASSWORD ON iOS 7.1.x



July 24th, 2014

@YoKoAcc (yk@firstsight.me) & @tocped

[English Version]

TABLE OF CONTENTS

TABLE OF FIGURES

I. ABSTRACT

Technology is developing so fast nowadays, and it can't be denied that it's helping people to finish their works & most of them are depending it to their gadget. The speed to access and get information is being the 'weapon' in daily life to support individual's activities. And even, not a little of them are saving their data or sensitive information in their gadget, so it'll be easier to be opened in critical times. After seeing those facts, it can be concluded that losing our gadget is a very-risky thing. Moreover, if someone loses his/her gadget, it'll also make them lose their saved data.

It's possible that many technology industries are offering an easy way to back-up data through the 'cloud' service, because of those factors. Seeing that our discussion will be more specified about Apple, so let's say Apple with its iCloud feature is helping its users for saving back their data.

Besides for backing its user's data, this iCloud feature is being integrated with many side features that can be used by its users, such as: locating their iDevice's location, restoring data, erasing data, and even turning off the iDevice's function if it's used by irresponsible person (Activation Lock/ Kill Switch feature).

According to the statistic which has been reported by some media like NYDailyNews (http://www.nydailynews.com/new-york/apple-iphone-kill-switches-deter-thieves-report-article-1.1836930), this feature was the reason that made theft cases in some countries being decreased.

"*Robberies and grand larcenies involving Apple products in New York City, which currently have the 'kill switch,' have dropped 19% and 29% respectively in the first five months of 2014 compared to the same period in 2013, Schniederman said in a Thursday statement.*"

Of course this thing is easing the users, considering that as long as this feature is activated, all Attackers won't be able to fully use the iDevice (We said so because iDevice can be not fully used with bypass method which has been published by a hacker few months ago, although this gap has been 'closed' by Apple when they were releasing update to the iDevice with iOS 7.1.2)

In this topic, we will discuss about the weaknesses of the password-saving method that is used by Apple in iDevice with iOS 7.1.x that can make an Attacker be able to turn off the user's iCloud feature.

II. INTRODUCTION

2.1. iCloud and Activation Lock

It's important to know that although iCloud was available since long ago, but "Activation Lock" feature in "Find My iPhone" was just released when iOS 7 was released as well. Here is a simple explanation from Apple related to the "Activation Lock" feature. (http://support.apple.com/kb/PH13695).

"*With iOS 7 or later, Find My iPhone includes a new feature called Activation Lock, which is turned on automatically when you set up Find My iPhone. Activation Lock makes it harder for anyone to use or sell your iPhone, iPad, or iPod touch if it's ever lost or stolen.*"

Generally, iCloud feature can be activated by going to the (menu) "Settings" > "iCloud". After completing some phases, then this feature will be directly integrated to the user's iDevice. And it's a need to know that, for activating the Activation Lock feature, the user has to activate "Find My iPhone" feature that is available in iCloud's menu.

With seeing the easiness to activate this feature, is this feature require password to be disabled? Absolutely yes. And the required password to disable this feature is sharing the same one with the User's Apple ID.

2.2. Keychain

There is a possibility that most of the readers have known surely what the paper's objectives are. And we're sure that most of the readers have known the exact definition and concept of Keychain. Concisely, Keychain is an application or a feature that is made by Apple and used for saving any kind of identities or passwords from any applications. In iOS, access to this feature is limited, so only the users who have 'jailbreak' their iDevice can access it completely.

Because Keychain is consisting of many credentials, so it can be confirmed that the developer itself is using database. This Keychain database has been encrypted by Apple with a specific key in the hardware, which means this encryption is unique for every iDevice.

Then, what is the purpose of Keychain in saving these identities and passwords? Concisely, with saving credentials from the users, so the users won't need to take times to retype their own credentials when logging in to the application which is often used.

2.3. Relation between Keychain with iTunes Store Password

According to the discussion in Abstract part, in this simple paper, we will discuss about the weaknesses of password-saving method which has done by Apple in iDevice with iOS 7.1.x. This gap itself could only be found after we have 'jailbreak' our devices.

In a very interesting discussion that we have done with one of Security Engineers from Facebook (when we explained a detection from an application that is made by Facebook- we will describe it in another paper), there is an interesting statement about jailbreak:

"Jailbreaking the device violates most of the fundamental security assumptions underlying the OS. It's a bit like saying "I can steal your car if you leave the doors unlocked, the keys in the ignition, and walk away for an hour or two."

Do you agree with this interesting quote? For us, we agree. And it's hard to disagree with the related quote. However, we asked ourselves: isn't the purpose of the Security itself is for minimalizing the chances of risk, even in database-administrator level? It's better to hold this argumentation for a second until we reach the main point of our discussion.

This gap essentially is found after we did 'dump' to the Keychain from iPhone 4s and 5 with iOS 7.1.1. From the dump result, we found that the passwords from the user's Apple ID have been saved to the Keychain and located in:

1. "com.apple.account.iTunesStore.password" (for iPhone 4s and iPhone 5), and
2. "com.apple.account.AppleAccount.password" (for iPhone 5)

Why are we stating those things as vulnerability? Here are the reasons:

1. In iOS 6, we don't find related component or other components that save identity and passwords from Apple ID.
2. With the current situation that iOS 7.1.2 from an iDevice is able to be jailbreak and there isn't any corrections from Apple about this one until now, so an Attacker who has physical access to an unlock (isn't protected by passcode) iDevice will be able to jailbreak and delete iCloud protection in the related iDevice with using the value from the 2 components which we have said.

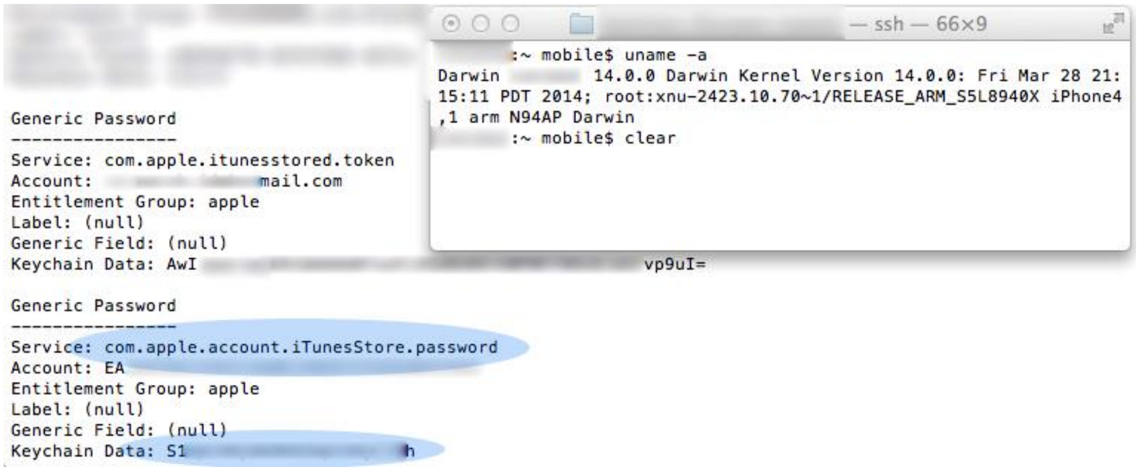
III. AFFECTED VERSION AND CONDITION

We have performed a test to iOS 7.1.1 for iPhone 4s and iPhone 5. We haven't performed the test to the iOS 7.0.x yet, so we only write iOS 7.1.x on our paper.

IV. PROOF OF CONCEPT

1. Connect the iDevice to the PC.
2. Do 'jailbreak' to the connected iDevice.

3. Do dump to the Keychain that is located in /private/var/Keychains/keychain-2.db.
4. Find "com.apple.account.iTunesStore.password" and "com.apple.account.AppleAccount.password". Then, we can see the identity and password from the saved Apple ID:



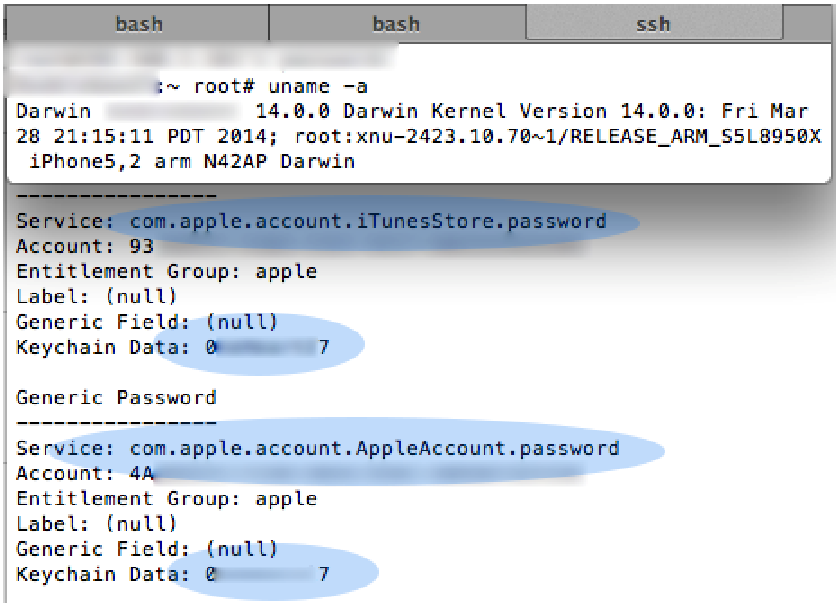
```
[redacted]:~ mobile$ uname -a
Darwin [redacted] 14.0.0 Darwin Kernel Version 14.0.0: Fri Mar 28 21:
15:11 PDT 2014; root:xnu-2423.10.70~1/RELEASE_ARM_S5L8940X iPhone4
,1 arm N94AP Darwin
[redacted]:~ mobile$ clear
```

```
[redacted]

Generic Password
----------------
Service: com.apple.itunesstored.token
Account: [redacted]mail.com
Entitlement Group: apple
Label: (null)
Generic Field: (null)
Keychain Data: AwI[redacted]vp9uI=

Generic Password
----------------
Service: com.apple.account.iTunesStore.password
Account: EA[redacted]
Entitlement Group: apple
Label: (null)
Generic Field: (null)
Keychain Data: S1[redacted]h
```

Figure 1 com.apple.account.iTunesStore.password



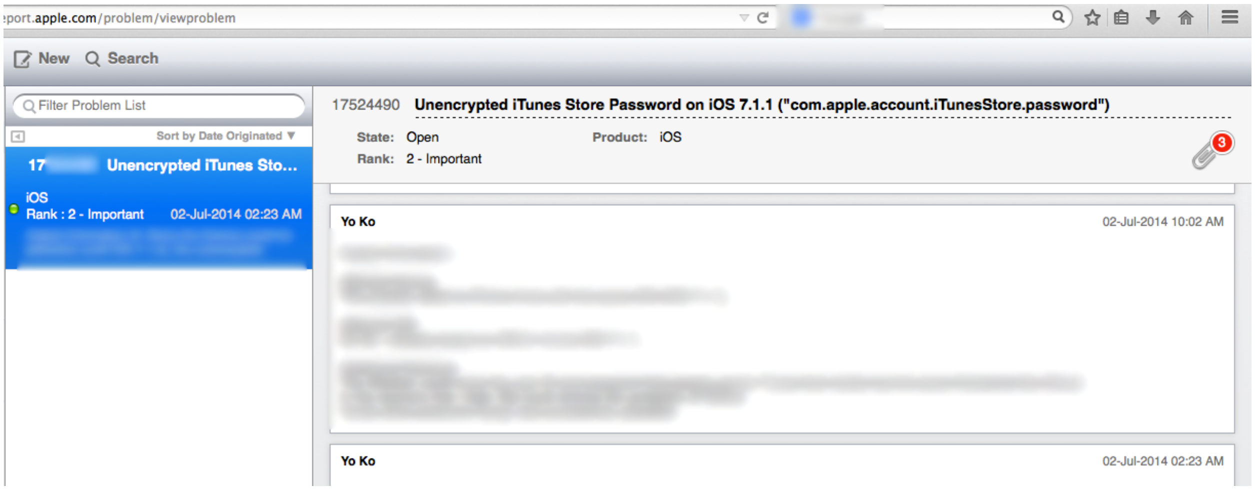
```
[redacted]
[redacted]:~ root# uname -a
Darwin [redacted] 14.0.0 Darwin Kernel Version 14.0.0: Fri Mar
28 21:15:11 PDT 2014; root:xnu-2423.10.70~1/RELEASE_ARM_S5L8950X
 iPhone5,2 arm N42AP Darwin
----------------
Service: com.apple.account.iTunesStore.password
Account: 93[redacted]
Entitlement Group: apple
Label: (null)
Generic Field: (null)
Keychain Data: 0[redacted]7

Generic Password
----------------
Service: com.apple.account.AppleAccount.password
Account: 4A[redacted]
Entitlement Group: apple
Label: (null)
Generic Field: (null)
Keychain Data: 0[redacted]7
```

Figure 2 com.apple.account.AppleAccount.password

V. RESPONSE FROM APPLE

There isn't any responses from Apple side from July 2nd, 2014 when we reported the related things. We haven't known surely about the Apple's need in saving passwords from Apple ID in Keychain in iOS 7 (which was in iOS 6, Apple didn't do things like this).



17[redacted] Unencrypted iTunes Sto...
iOS
Rank : 2 - Important 02-Jul-2014 02:23 AM
[redacted]

17524490 Unencrypted iTunes Store Password on iOS 7.1.1 ("com.apple.account.iTunesStore.password")

State: Open Product: iOS
Rank: 2 - Important

Yo Ko 02-Jul-2014 10:02 AM

[redacted]

Yo Ko 02-Jul-2014 02:23 AM

Figure 3 Report - July 2nd, 2014

VI. SUMMARY AND RECOMMENDATION

Generally, with using those vulnerabilities, an Attacker will gain full access to an iDevice with turning off "Find My iPhone" feature without bothering to find a bug like the one which have ever existed in iOS 7.0.x.

After seeing the status related to this, so the recommendations that can be implemented by the users to avoid this trouble, are:

1. Always use passcode in the user's iDevice and never leave the iDevice without locked with passcode.
2. Activating the 2FA (Two-Factor Authentication) / Two-Step Verification (http://support.apple.com/kb/HT5570) feature in your Apple ID. The purpose is none other than preventing the misusing of data that have been synchronized by user with Apple's iCloud feature. With activating this feature, Apple has minimalized the risks related to data theft from the user's side, although the Attacker has known the identity and password of someone's Apple ID.

VII. REFERENCES

1. Penetration Testing of iPhone Application - Part 3 - http://www.securitylearn.net/tag/penetration-testing-mobile-applications/
2. Keychain Services Concepts – https://developer.apple.com/library/mac/documentation/security/conceptual/keychainServConcepts/02concepts/concepts.html
3. iOS Application Security Part 20 - http://resources.infosecinstitute.com/ios-application-security-part-20-local-data-storage-nsuserdefaults-coredata-sqlite-plist-files/
4. iCloud: Find My iPhone Activation Lock in iOS 7 - http://support.apple.com/kb/HT5818
5. Frequently Asked Questions about Two-Step Verification for Apple ID - http://support.apple.com/kb/HT5570