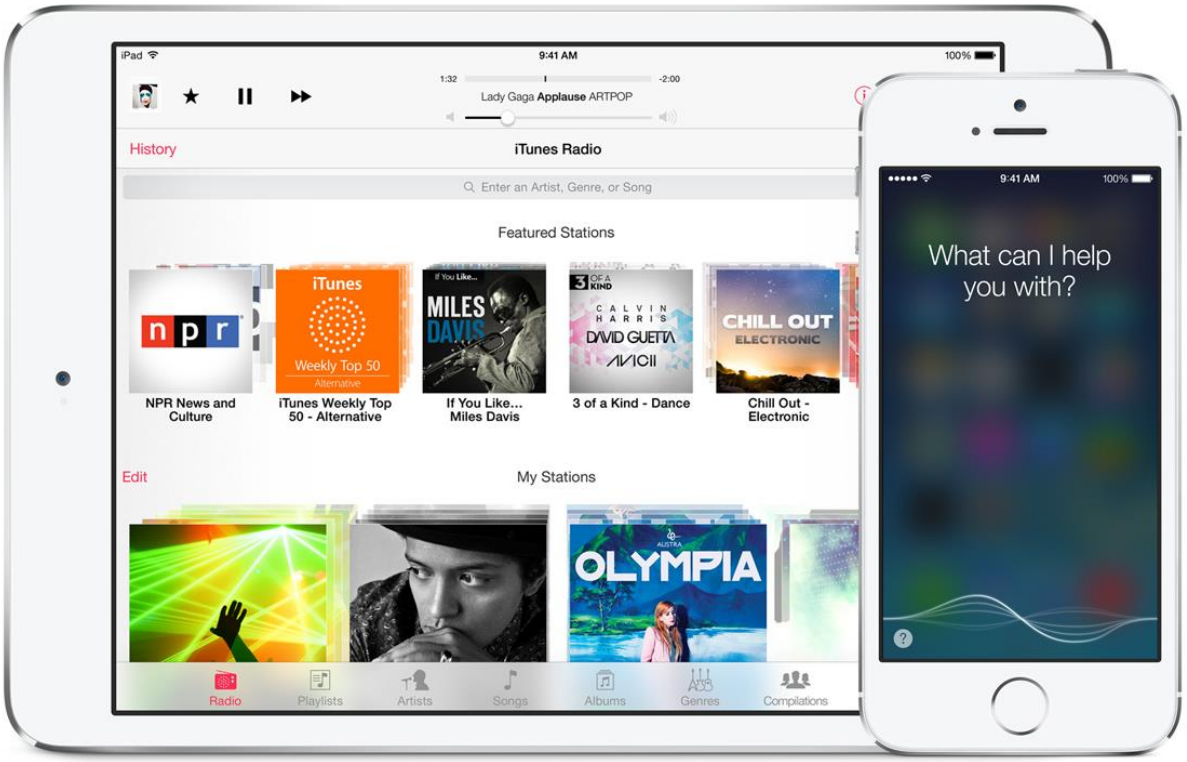
UNENCRYPTED iTunes STORE PASSWORD ON iOS 7.1.x



July 24th, 2014

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

[Indonesian Version]

DAFTAR ISI

DAFTAR GAMBAR

I. ABSTRAK

Perkembangan teknologi yang begitu pesat pada saat ini tentu semakin dapat memudahkan orang untuk menyelesaikan pekerjaannya dan tentu tidak sedikit pula yang menggantungkan aktivitasnya pada gadget yang dimiliki. Kecepatan mengakses ataupun memperoleh informasi sering kali menjadi santapan sehari-hari dalam mendukung aktivitas setiap individu. Bahkan, tidak sedikit orang yang menyimpan data ataupun informasi sensitif di dalam gadget nya sehingga mudah untuk diakses setiap saat ketika diperlukan. Dengan melihat sedikit kejadian ini, tentu kita pun dapat menyadari bahwa kehilangan gadget merupakan suatu hal yang sangat berisiko. Terlebih lagi, ketika seseorang kehilangan gadget, maka orang ini pun akan kehilangan data yang disimpannya.

Mungkin, atas dasar inilah banyak pelaku industri teknologi yang menawarkan kemudahan untuk mem-backup data melalui layanan cloud yang dimilikinya. Mengingat bahwa pembahasan di sini akan lebih spesifik pada produk Apple, maka, sebut saja Apple dengan fitur iCloud nya yang dapat memudahkan penggunanya untuk mengambil kembali data dari layanan yang ada.

Selain untuk mem-backup data milik penggunanya, layanan iCloud ini pun telah diintegrasikan dengan beberapa fitur yang dapat digunakan oleh para penggunanya untuk melacak lokasi iDevice miliknya, me-restore data, menghapus data, atau bahkan mematikan fungsi iDevice itu sendiri bila jatuh ke tangan yang salah (Activation Lock / Kill Switch feature).

Berdasarkan statistik yang diberitakan oleh media seperti NYDailyNews (http://www.nydailynews.com/new-york/apple-iphone-kill-switches-deter-thieves-report-article-1.1836930), disampaikan bahwa fitur ini telah membuat kasus pencurian terhadap iDevice di sejumlah negara telah menjadi menurun.

"*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.*"

Tentu saja hal ini dapat membuat para penggunanya sedikit lega mengingat bahwa selama fitur ini tetap aktif, maka para Attacker pun tidak akan dapat memanfaatkan kembali iDevice miliknya secara utuh (Kami mengatakan demikian dikarenakan iDevice dapat digunakan secara tidak utuh dengan metode bypass yang dikeluarkan oleh salah satu hacker pada beberapa bulan yang lalu walaupun celah ini dinilai telah ditutup oleh Apple ketika mereka mengeluarkan update terhadap iDevice dengan iOS 7.1.2).

Pada topik ini, Kami akan membahas mengenai kelemahan akan metode penyimpanan password yang dilakukan oleh Apple pada iDevice di iOS 7.1.x yang dapat menyebabkan seorang Attacker untuk mematikan fitur iCloud milik seorang pengguna.

II. PENDAHULUAN

2.1. iCloud dan Activation Lock

Perlu diketahui bahwa walaupun layanan iCloud telah tersedia sejak lama, namun fitur "Activation Lock" pada "Find My iPhone" ini baru di-release saat iOS 7 keluar. Berikut ini merupakan penjelasan sederhana dari Apple terkait fitur "Activation Lock" (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.*"

Secara umum, fitur iCloud dapat diaktifkan dengan masuk ke menu "Settings" > "iCloud". Dengan menjalankan beberapa tahap, maka fitur ini pun langsung terintegrasi dengan iDevice milik pengguna. Perlu diketahui bahwa untuk mengaktifkan fitur Activation Lock, pengguna diharuskan menghidupkan fitur "Find My iPhone" yang tersedia pada menu iCloud.

Dengan melihat begitu mudahnya fitur ini diaktifkan, apakah fitur ini memerlukan password untuk kembali dinonaktifkan? Jawabannya tentu saja iya. Dan password yang diperlukan untuk menonaktifkan fitur ini pun memiliki password yang sama dengan Apple ID milik penggunanya.

2.2. Keychain

Mungkin sebagian besar pembaca sudah mengetahui dengan jelas arah tujuan dari paper ini. Dan Kami pun yakin bahwa sebagian lagi telah mengetahui secara jelas akan definisi dan konsep yang terdapat di dalam Keychain. Secara ringkasnya, keychain merupakan suatu aplikasi / fitur yang dibuat oleh Apple yang digunakan untuk menyimpan segala macam identitas maupun password dari berbagai aplikasi. Di dalam iOS, akses ke dalam fitur ini dibatasi sehingga hanya pengguna yang telah men-jailbreak iDevice nya saja yang dapat mengaksesnya.

Dikarenakan keychain mengandung begitu banyak credentials, maka dapat dipastikan bahwa pengelolaannya sendiri pun menggunakan database. Keychain database ini telah dienkripsi oleh Apple dengan kunci spesifik pada hardware yang artinya enkripsi ini bersifat unik untuk setiap iDevice.

Lalu, apa tujuan dari keychain dalam menyimpan identitas dan password ini? Sederhananya adalah, dengan menyimpan credentials dari pengguna, maka pengguna tidak perlu lagi bersusah payah dalam mengetikan kembali credentials miliknya saat ingin login ke dalam aplikasi yang terbilang sering digunakan.

2.3. Hubungan antara Keychain dengan iTunes Store Password

Sesuai dengan pembahasan di bagian abstrak, pada paper sederhana ini, Kami ingin membahas mengenai kelemahan akan metode penyimpanan password yang telah dilakukan oleh Apple pada iDevice dengan iOS 7.1.x. Celah ini sendiri baru dapat Kami temukan ketika Kami telah men-jailbreak device Kami.

Pada salah satu diskusi menarik yang pernah Kami lakukan dengan salah satu security engineer dari Facebook (saat Kami memaparkan temuan dari aplikasi yang bukan dibuat oleh Facebook - akan Kami paparkan nanti di paper lain), terdapat statement menarik mengenai 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."

Setujukah Anda dengan quote yang menarik ini? Bagi Kami, Kami setuju. Dan sulit untuk tidak setuju dengan quote terkait. Namun, Kami mencoba berpikir, bukankah tujuan dari security itu sendiri yaitu untuk meminimalisasi adanya risiko bahkan di level database administrator sekalipun? Sebaiknya, kita tahan sebentar argumentasi ini sementara waktu sampai menuju ke titik utama pembahasan Kami.

Celah ini pada dasarnya Kami temukan setelah Kami melakukan dump pada keychain dari iPhone 4s dan 5 dengan iOS 7.1.1. Dari hasil dump, Kami mendapati bahwa password dari Apple ID milik pengguna telah tersimpan pada keychain dan terletak pada "com.apple.account.iTunesStore.password" (untuk iPhone 4s dan iPhone 5) dan "com.apple.account.AppleAccount.password" (untuk iPhone 5).

Mengapa kami akhirnya menyatakan hal ini sebagai celah keamanan? Karena:

1. Pada iOS 6, Kami tidak mendapati komponen terkait ataupun komponen lainnya yang menyimpan identitas dan password dari Apple ID.
2. Dengan situasi bahwa saat ini iOS 7.1.2 dari suatu iDevice dapat di-jailbreak dan belum terdapat perbaikan lagi dari Apple untuk hal ini, maka seorang Attacker yang memiliki akses fisik ke iDevice yang tidak di-passcode akan dapat men-jailbreak dan menghapus proteksi iCloud pada iDevice terkait dengan menggunakan value dari kedua komponen yang telah Kami sampaikan.

III. AFFECTED VERSION AND CONDITION

Kami melakukan pengujian terhadap iOS 7.1.1 untuk iPhone 4s dan iPhone 5. Kami sendiri belum mencoba pada versi iOS 7.0.x sehingga Kami menuliskan iOS 7.1.x pada paper Kami.

IV. PROOF OF CONCEPT

1. Hubungkan iDevice dengan PC.
2. Jailbreak lah iDevice yang telah terhubung.
3. Lakukan dump pada keychain yang terletak pada /private/var/Keychains/keychain-2.db.
4. Temukan "com.apple.account.iTunesStore.password" dan "com.apple.account.AppleAccount.password". Maka kita akan dapat melihat identitas dan password dari Apple ID yang tersimpan:

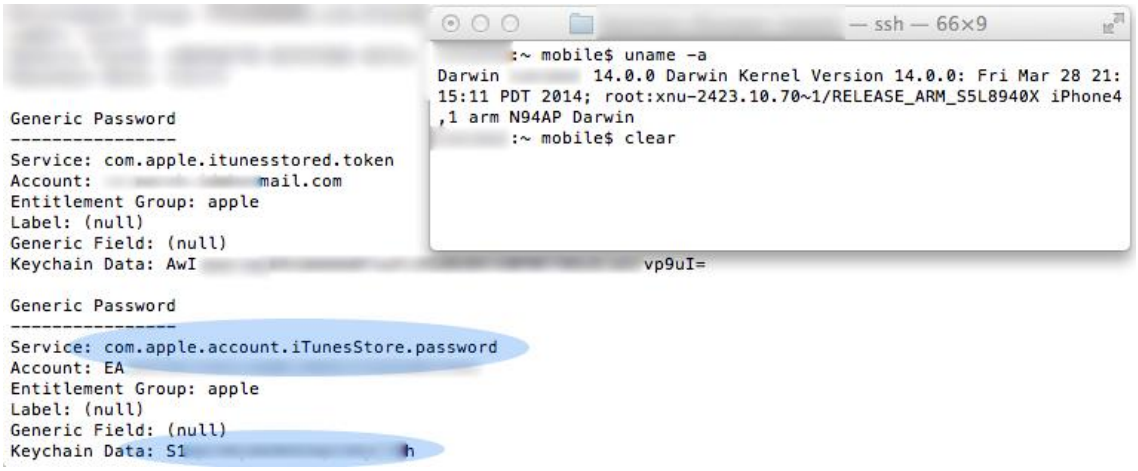


Figure 1 com.apple.account.iTunesStore.password

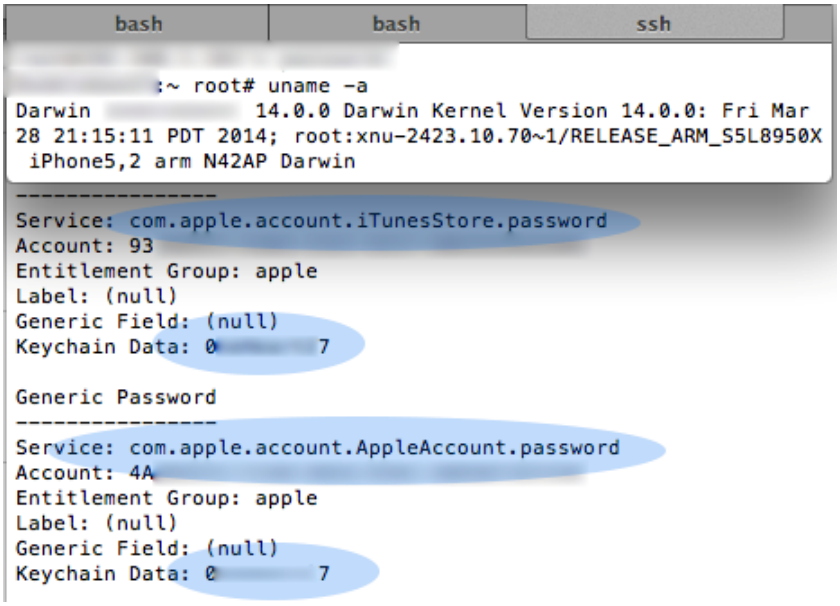


Figure 2 com.apple.account.AppleAccount.password

V. RESPONSE FROM APPLE

Belum terdapat respon oleh pihak Apple dari July 2nd, 2014 lalu sejak Kami melaporkan hal terkait. Kami pun belum mengetahui secara pasti akan keperluan Apple dalam menyimpan password dari Apple ID pada keychain di iOS 7 (yang sebelumnya pada iOS 6, Apple tidak melakukan hal ini).

Figure 3 Bug Report July 2nd, 2014

VI. SUMMARY AND RECOMMENDATION

Secara umum, dengan memanfaatkan kerentanan ini, tentunya Attacker akan dapat meraih akses secara penuh terhadap suatu iDevice dengan mematikan fitur "Find My iPhone" tanpa harus bersusah-payah mencari bug seperti yang sebelumnya pernah ada pada iOS 7.0.x.

Dengan melihat status yang ada terkait hal ini, maka rekomendasi yang dapat diterapkan oleh para pengguna untuk menghindari hal ini adalah:

1. Selalu menggunakan passcode pada iDevice milik pengguna dan jangan pernah meninggalkan iDevice tanpa terkunci dengan passcode.
2. Aktifkan fitur 2FA (Two-Factor Authentication) / Two-Step Verification (http://support.apple.com/kb/HT5570) pada Apple ID milik pengguna. Tujuannya yaitu tidak lain untuk pencegahan penyalahgunaan data yang telah disinkronisasikan oleh pengguna dengan layanan iCloud milik Apple. Dengan mengaktifkan fitur ini, maka Apple telah meminimalisasi risiko terkait pencurian data dari sisi pengguna walaupun Attacker telah mengetahui identitas dan password dari Apple ID seseorang.

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