OKsystem

Jak může iOS chránit vaše data, když mu v tom nezabráníte?

Ivo Rosol
ředitel vývojové divize

Agenda prezentace

- Bezpečnostní mechanismy iOS – přehled
- HW bezpečnostní mechanismy
- Proces bezpečného startu systému
- Zabezpečení dat uložených v systému
- Ochrana kryptografických klíčů
- Služba Apple Push Notification
- Zabezpečeni dat při komunikaci iMessage
- MDM

Bezpečnostní mechanismy iOS

iOS má bezpečnost navrženou systematicky (s podporou HW, OS i ekosystému), nikoli ale bez chyb. Ve spolupráci s hackery se bezpečnost nových verzi iOS i zařízení významně zlepšuje.

- Secure boot chain
- Podpis kódu aplikací
- Runtime proces security
- HW bezpečnostní mechanismy (AES crypto procesorRNG, bezpečné mazání flash paměti, UID a GID (AES 256 klíče) v procesoru
- Bezpečnost jádra iOS - XNU
- Zabezpečení dat v souborovém systému
- Ochrana klíčů
- Síťová bezpečnost
- Zabezpečení fyzického přístupu zařízení
- MDM
- Vzdálené vymazání

Bezpečnostní HW

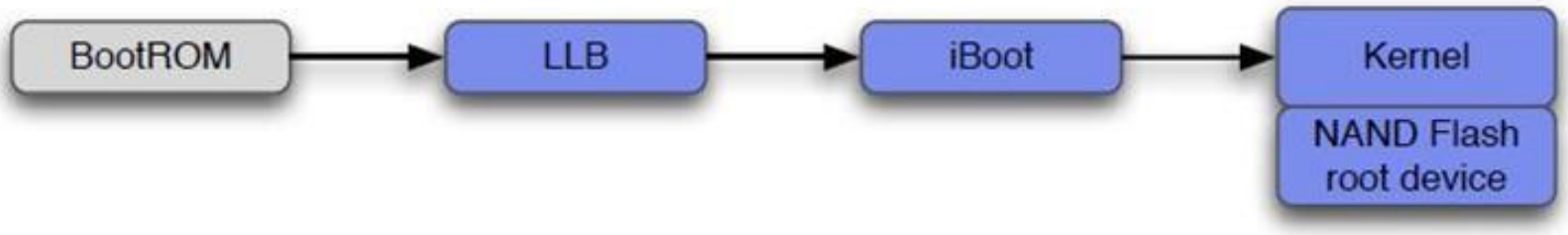
- AES crypto engine + HW výpočet SHA1
- Secure Enclave – kryptografický koprocesor a bezpečná paměť na procesoru A7, TRNG, UID
- Touch ID – systém pro snímání otisků prstů, spojený přes šifrovanou paměť se Secure Enclave
- Effaceable storage (blok 1 flash paměti)

Režim zařízení

iPhone pracuje v jednom z 3 režimů:

- Normal Mode
- Recovery Mode (uvedení do továrního nastavení s nejnovější verzí iOS)
- DFU Mode (obnova „čistého“ stavu z libovolného stavu zařízení)

Boot proces



Bylo by to neprůstřelné, kdyby nebyla žádná chyba v řetězci ověřování. Bylo objeveno několik zneužitelných slabin přímo v kódu bootRom, viz http://resources.infosecinstitute.com/iphone-forensics/

Boot do Normal Mode

Start iDevice zařízení tvoří posloupnost celků SW kódu, který začíná neměnným kódem v boot-rom čipu A7, který vzniká při výrobě čipu v rámci fotomasky a je tudíž považován za implicitně důvěryhodný.

Boot-rom kód obsahuje hodnotu veřejného klíče kořenové autority Apple Root CA, který se používá k ověření podpisu další části kódu zavaděče – LLB – Low-Level Bootloader (uložen ve Flash paměti, blok 0).

- LLB spustí několik rutin a zkontroluje podpis iBoot a pokud je v pořádku skočí na něj.
- Kód LLB je již vyměnitelný, jeho disassembly je uvedena na http://theiphonewiki.com/wiki/LLB

iBoot

- iBoot je bootloader fáze 2, společný pro všechny iDevice. iBoot nedovolí nahrát na zařízení starší verzi OS, nebo upravenou verzi OS, u které nesouhlasí elektronický podpis.
- je uložen ve Flash paměti, bloky 8 - 15
- iBoot umožňuje upgradovat iOS, nebo obnovit do továrního nastavení.
- iBoot zkontroluje podpis jádra iOS (XNU).
- Jádro zkontroluje podpis aplikací.

Řešení problémů

Pořadí při odstraňování problémů:

- restart
- reset (reboot)

pokud nepomůže, musí se obnovit systém:

- restore (factory reset)
- recovery
- DFU restore

a obnovit aplikace a data ze zálohy

Restart iOS

Restart (2 kroky – vypnutí, ruční zapnutí) se vyvolá přidržením tlačítka Power (Sleep/Wake), dokud se neobjeví posuvník s výzvou „Slide to power off/vypněte přejetím“. Po přejetí se ukončí všechny aplikace a zařízení se vypne (nemá žádný odběr z baterie).

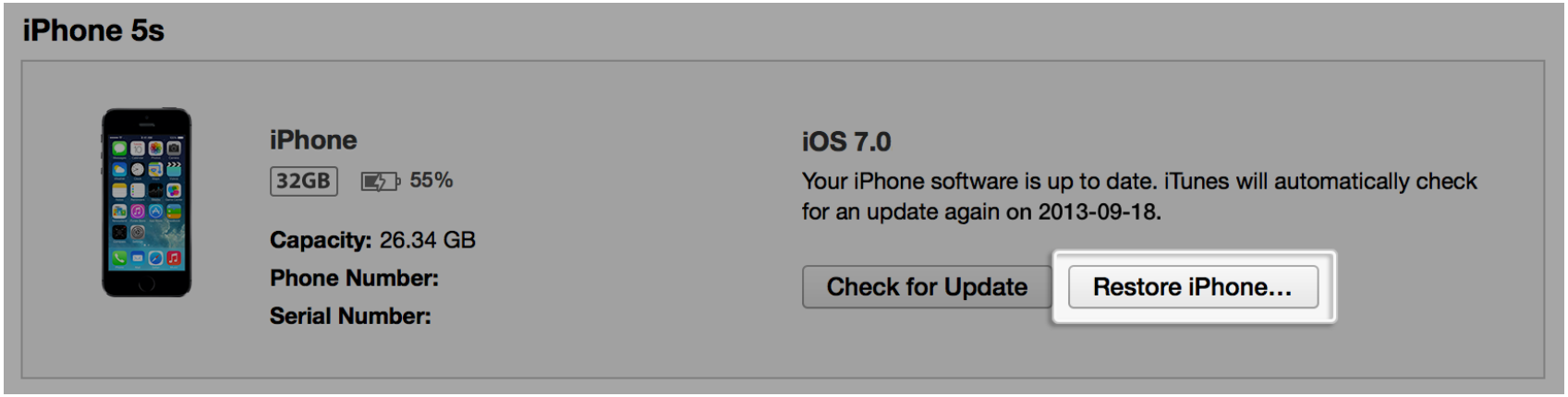
Pro zapnutí se podrží tlačítko Power, dokud se neobjeví logo Apple a po 30 sekundách se objeví domovská obrazovka, musí se zadat heslo zařízení a PIN pro SIM kartu. Po zapnutí běží všechny aplikace, které běžely před vypnutím – vypnutí je zřejmě hybernace, lze ale přijít o neuloženou práci, například rozepsaný e-mail..

Reset iOS

- Pokud je zařízení natolik zaseklé, že nepomůže ani restart, lze jako poslední východisko použít reset. Pro vyvolání reset se podrží současně Power a Home alespoň 10 sekund, dokud se neobjeví logo Apple. Během resetu zůstává zařízení pod napájením a není vypnuto.
- Na rozdíl od restartu jsou ukončeny všechny aplikace, zavřeny všechny soubory a probíhá kompletní boot proces, který trvá několik minut.
- Na rozdíl od restartu, reset nastaví některé parametry zařízení na výchozí hodnoty.

Restore

Restore (někdy též Factory reset nebo Master reset) lze standardně vyvolat z iTunes. Výsledkem je zařízení ve stavu, jako po vybalení z krabice, ale s nejnovějším iOS. Restore vymaže všechny aplikace, operační systém a nainstaluje ho znova, v nejnovější verzi, s továrním nastavením. Uživatelská data se poté obnoví pomocí ze zálohy v iTunes nebo iCloud.



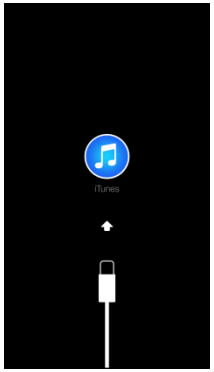
Recovery

Pokud nejde provést Restore (zařízení se neobjeví v iTunes, nebo např. opakovaně rebootuje, nebo se proces zastaví), je nutné aktivovat recovery režim

Recovery Mode

- Recovery režim používá iBoot pro každou aktualizaci zařízení, případně pro obnovu systému. Při Recovery režimu svítí na obrazovce ikona iTunes s kabelem. Obnova v Recovery režimu vymaže všechny aplikace, operační systém a nainstaluje ho znova, v nejnovější verzi, s továrním nastavením. Uživatelská data se obnoví pomocí restore ze zálohy v iTunes nebo iCloud.

Aktivace Recovery režimu



- zařízení s odpojeným kabelem se vypne Stiskne se tlačítko Home a podrží
- Při stisknutém tlačítku Home se připojí zařízení k počítači s iTunes
- Tlačítko Home se drží, dokud se neobjeví na zařízení obrazovka Connect to iTunes
- Uvolní se tlačítko Home
- iTunes se spustí a ohlásí, že zařízení je v Recovery Mode („*iTunes has detected an iPhone in recovery mode. You must restore this iPhone before it can be used with iTunes*“).
- Pomocí iTunes lze obnovit systém

DFU mode

DFU nepoužívá iBoot, zařízení pouze komunikuje s iTunes, bez toho, že by pomocí iBoot zavedlo iOS. Obrazovka je ale černá a není vidět, že se něco děje (pokud se cokoli zobrazí, nejste v DFU mode)

Vstup do DFU - Interaktivní postup

- zařízení se připojí USB kabelem k počítači, spustí se iTunes, zařízení se vybere v seznamu zařízení a zařízení se poté vypne přidržením tlačítka Power
- Na 3 vteřiny se podrží tlačítko Power, neuvolňuje se
- Poté se navíc stiskne tlačítko Home na 10 vteřin (přesně), Power se stále drží
- Uvolní se Power, Home se stále drží cca 10 vteřin, dokud iTunes neohlásí, že zařízení je v Recovery Mode („*iTunes has detected an iPhone in recovery mode. You must restore this iPhone before it can be used with iTunes*“). Je matoucí, že se píše, že zařízení je v Recovery mode

DFU restore

Postup Restore v DFU režimu

- V iTunes se vybere zařízení
- V záložce Summary se klikne na Restore
- Po Restore zařízení nabootuje a objeví se průvodce počátečním nastavením (jako u nového iphone)
- Obnoví se uživatelská data z poslední zálohy

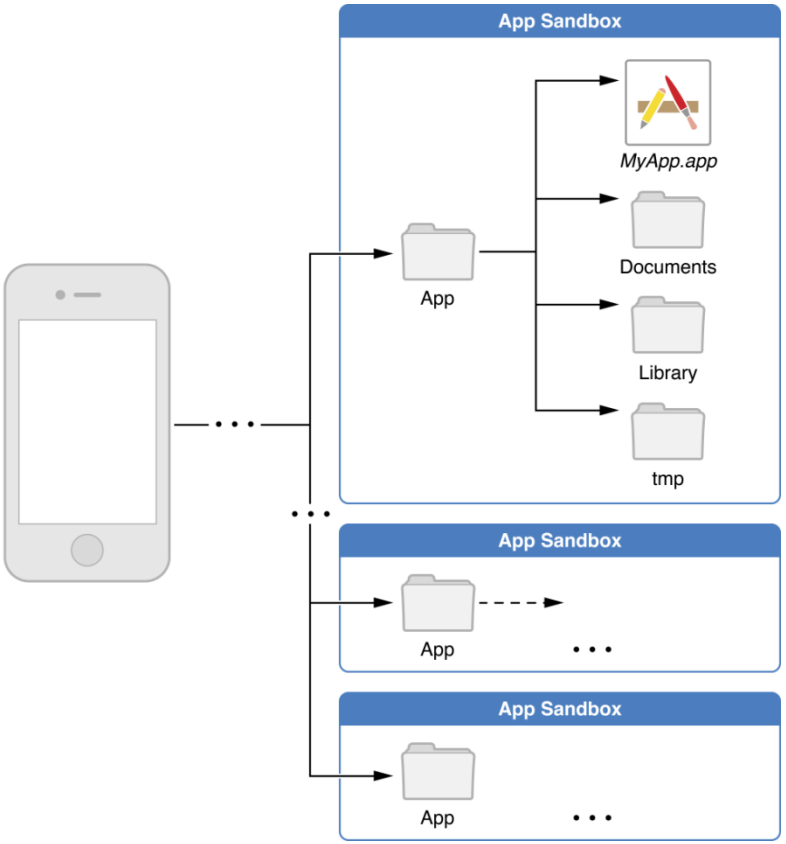
Ukončení DFU

- Současně se stiskne Home a Power tlačítko, dokud se neobjeví logo Apple (jablíčko uprostřed obrazovky).

Zabezpečení dat uložených v iOS

- Ačkoli je to před uživateli skryto (uživatelé iOS nemají přímý přístup k systému souborů), iOS má souborový systém, podobně jako platformy dospělých počítačů. Na rozdíl od nich, iOS zaručuje, že jednotlivé aplikace mají oddělená úložiště (tzv. **aplikační sandbox** – svůj „píseček“), tj. každá aplikace má vlastní složku (home directory obsahující vlastní aplikaci AppName.app). Tato bundle direktory je podepsána při instalaci, zápis do adresáře zneplatní podpis a znemožní spustit aplikaci.
- Aplikační adresář obsahuje podsložky tmp, Documents a Library. V těchto složkách každá aplikace vytváří své adresáře a soubory a nemůže je běžně vytvářet nikde jinde. Jedinou výjimkou je, když aplikace využívá public interface k přístupu k uživatelským kontaktům, obrázkům apod. V tomto případě iOS zpracovává všechny souborové operace pro čtení a modifikaci těchto úložišť. Takový přístup vyžaduje to povolení uživatele.
- Pro srovnání si lze představit, že PC aplikace MS Word by neumožnila uložit *.DOC soubory jinde, než ve svém sandboxu – takové uspořádání není na PC běžné.

Aplikační sandbox



- <App_Home>/Documents/ – obsahuje aplikační a uživatelská data přímo, nebo v podsložkách. Obsah složky může být k dispozici uživateli pomocí mechanismu File sharing. iTunes zálohuje tuto složku.
- <App_Home>/Documents/Inbox/ – aplikace v této složce nemůže vytvářet soubory, může je ale číst a mazat. Složka slouží k uložení souborů cizích entit. iTunes zálohuje tuto složku.
- <App_Home>/Library/ obsahuje podsložky a aplikační soubory, které nejsou uživatelské, ale aplikační. iTunes zálohuje tuto složku.
- <App_Home>/tmp/ obsahuje dočasné soubory, které aplikace může kdykoli smazat. iTunes nezálohují tuto složku.

Systém souborů

- Systém souborů iOS je založen na Unixu, jména souborů jsou citlivá na velikost písmen, komponenty cesty jsou odděleny dopřednými lomítky (/). Při vytvoření souboru se definuje vlastník a skupina vlastníků a řadu dalších atributů.
- Systém souborů kombinuje standardní BSD Unix práva (rwx-rxx-rwx) a práva založená na ACL. iOS systém automaticky přidělí ACL a práva souborům vytvořeným aplikací.
- Po startu aplikace je běžný adresář nastaven na kořenový adresář / aplikačního sandboxu.

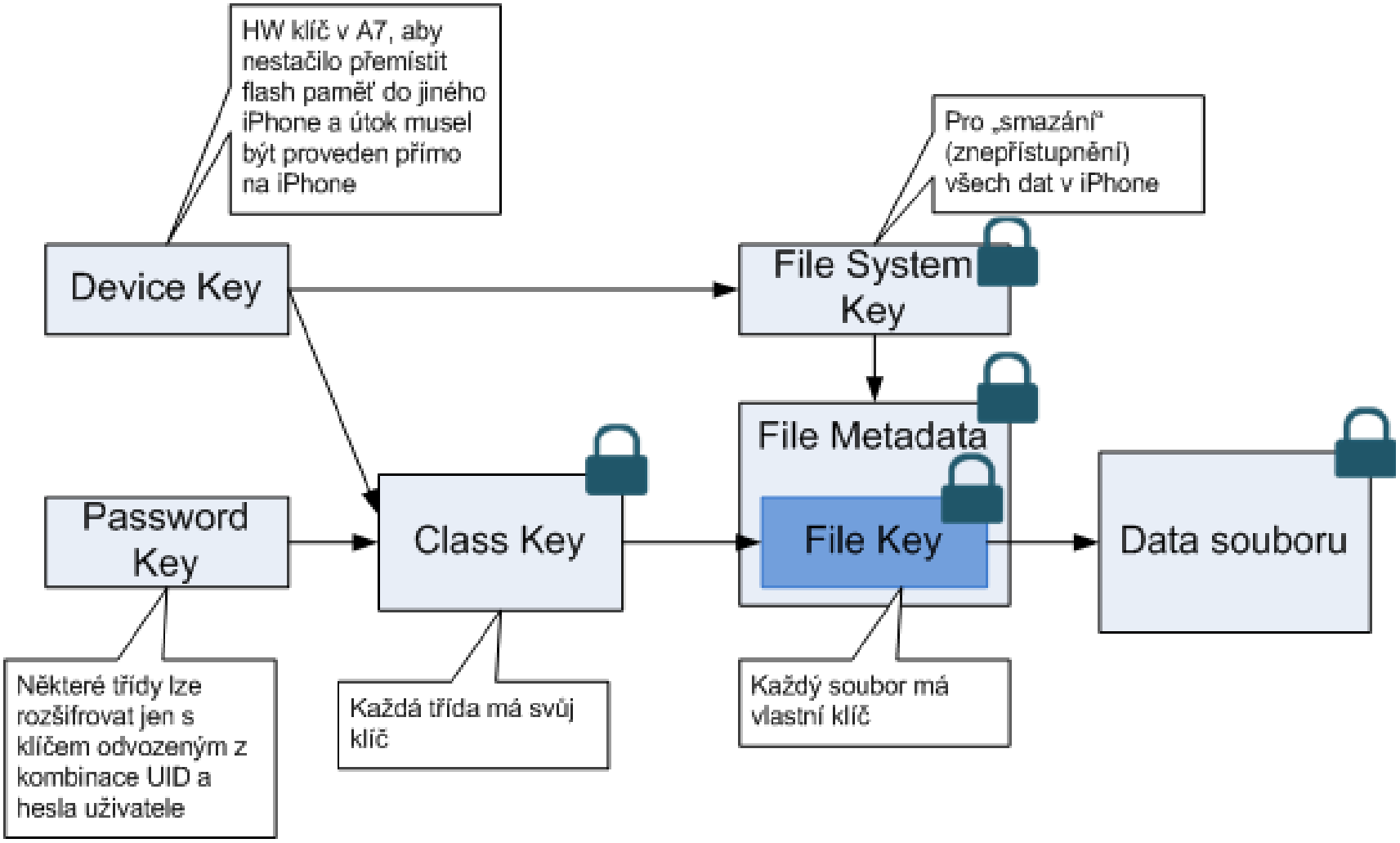
Ochrana souborů pomocí šifrování

Všechna data na iOS jsou zašifrována. Ochrana je pouze tak dobrá, jak silné je heslo.

iOS Data Protection umožňuje kryptograficky chránit data uložené ve flash paměti.

- **Podmínkou pro ochranu systému souborů šifrováním je nastavení hesla pro zařízení !!!**
  Setting>General>Passcode/Nastavení > Obecné > Touch ID a kódový zámek
  Pozor, implicitní nastavení je jednoduché heslo, které znamená 4 místný číselný PIN. To je zcela nedostačující, měl by být použito 8 místné komplexní heslo.
- iOS uměle zpomaluje snahy o pokus uhádnutí hesla hrubou silou (cca na 80 ms na jeden pokus), takže
  - 4 místný numerický PIN na cca 13 minut
  - 9 místný 2,5 roku
  - 6 místný znakový 5,5 roku
- Útok hrubou silou se musí dělat přímo na zařízení, neboť heslo je kombinováno s UID v procesoru. iOS navíc eskaluje zpoždění po určitém počtu neplatných pokusů.
- Dobrý kompromis mezi nepohodlím komplexního hesla a bezpečností lze dosáhnout s iPhone 5s, který umožňuje místo komplexního hesla použít biometriku otisku prstů. Rrelativně nízké FAR (nejsou údaje) je kompenzováno pomocí nutnosti zadat heslo po 5 neúspěšných pokusech s otiskem prstu.
- Na stejném místě je možné zapnout smazání dat v iPhone po 10 neúspěšných pokusech o zadání hesla.

Kryptografické schéma



Popis schématu

Obsah souboru je šifrován pomocí náhodného „per-file-key“, který je šifrován klíčem třídy Class key a uložen do metadat souboru. Metadata jsou zašifrována pomocí File system key (společný pro všechny soubory, uložený přímo v effaceable storage).

Class key je, v závislosti na třídě, šifrován klíčem UID, který je pro některé třídy diverzifikován uživatelským heslem (kterým se odemyká zařízení).

Flexibilita schématu

- Smazání všech dat zařízení (včetně remote wipe) – stačí smazat File system Key v effaceable storage, což efektivně znepřístupní všechna metadata a v nich obsažené per-fole-key
- Změna třídy – stačí přešifrovat per-file-key jiným class key
- po změně hesla stačí přešifrovat class key
- device UID znemožňuje přemístit flash do jiného zařízení, nebo útočit hrubou silou mimo zařízení

Flash paměť

Bezpečné smazání klíčů je stejně důležité jako bezpečné vytvoření a uložení.

Běžné systémy souborů (FAT, NTFS, UFS…) jsou navrženy pro magnetické disky a nelze je přímo přenést na flash paměť. Mezi iOS a flash je LBA (Logical Block Addressing), který každý zápis alokuje do nového bloku. Tato technologie (wear leveling) překonává omezení počtu přepisů bloků flash paměti pomocí rozprostření přes celé médium.

To ale znamená, že klíče by zůstávaly na více místech na disku.

Effaceable storage

iOS zařízení obsahují speciální HW, tzv. effaceable storage, což je blok 1 flash paměti (1KB), která slouží k rychlému a bezpečnému smazání klíčů.

Obsahuje 3 klíče:

- BAGI - klíč, který šifruje systém keybag
- Dkey (ProtectionNone Class key)* -
- EMF! (filesystem Encryption key – klíč, který šifruje metadata všech souborů)*

* *Tyto klíče nemohou být uložen v systému souborů, protože všechny soubory jsou šifrované*

Vytvoření šifrovaného souboru

NSFileManager Class

Třída umožňuje řadu generických operací se souborovým systémem a izoluje aplikaci od podkladového souborového systému, umožňuje pracovat i se soubory uloženými v iCloudu.
Vytvoření souboru pomocí metody:

(BOOL)createFileAtPath:(NSString *)*path* contents:(NSData *)*contents* attributes:(NSDictionary *)*attributes*

Parametr attributes:(NSDictionary *)*attributes* umožňuje nastavit atributy souboru, jedním z atributů je NSFileProtectionKey, který nastavuje úroveň ochrany souboru na následující hodnoty:

- NSFileProtectionNone
- NSFileProtectionComplete
- NSFileProtectionCompleteUnlessOpen
- NSFileProtectionCompleteUntilFirstUserAuthentication

Třídy kryptografické ochrany souboru

NSFileProtectionNone

- klíč třídy je zašifrován pouze pomocí device key odvozeného z UID a uložen v přímo effaceable storage.
- Je to implicitní třída pro všechny soubory, které nejsou přiřazeny do jiné třídy
- klíč třídy a soubory jsou k dispozici, když je zařízení nabootované
- lze použít pro soubory, s kterými je nutno libovolně pracovat, i když je zařízení zamčeno
- Bezpečnostní význam spočívá pouze v možnosti remote wipe (všechny klíče jsou na zařízení)

Třídy kryptografické ochrany souboru

NSFileProtectionCompleteUnlessOpen

- Soubor je uložen v šifrované formě, je chráněn, pokud není otevřen. Na rozdíl od ostatních případů, je zde ochrana různých souborů této třídy individuální a řídí se stavem otevření tohoto souboru. Soubor lze vytvořit, nebo do něj zapsat i při zamčeném zařízení, jakmile je ale soubor zavřen, nelze jej otevřít, dokud zařízení není odemčeno. Pokud je soubor otevřen při odemknutém zařízení, lze v přístupu pokračovat i po zamčení zařízení.
- Příklad použití nahrávání zvuku, které pokračuje i po zamčení zařízení
- Je toho dosaženo pomocí kombinace AES a ECDH kryptografie. Jakmile je vytvořen soubor, je k němu vytvořen AES „per file key“ a současně je vygenerován EC klíčový pár tohoto souboru. Pomocí privátního klíče souboru a veřejného klíče třídy Protected Unles Open se spočítá sdílené tajemství a jeho hash, tím vznikne sdílený klíč (mezi souborem a Data Protection). Per File Key se zašifruje tímto sdíleným klíčem a výsledek se uloží společně s veřejným klíčem souboru do metadat souboru. Poté se smaže privátní klíč souboru, který již nebude nikdy zapotřebí.

Třídy kryptografické ochrany souboru

NSFileProtectionCompleteUntilFirstUserAuthentication

- Soubory jsou uloženy v šifrované formě a soubory jsou nepřístupné, dokud zařízení nenabootuje a uživatel odemkne poprvé zařízení. Aplikace může přistupovat k souboru a pokračovat v přístupu, i když uživatel následně zařízení zamkne, neboť class key není smazán až do rebootu zařízení.
- Hlavní význam je ochrana proti útokům, které zahrnují reboot zařízení. Je to obdoba transparentního šifrování celého disku na desktopu.

Třídy kryptografické ochrany souboru

NSFileProtectionComplete

- Soubory této třídy jsou chráněny, pokud není zařízení odemčeno.
- Soubory jsou nepřístupné, pokud je zařízení zamčeno, nebo bootuje.
- Class key je šifrován klíčem odvozeným z UID a hesla uživatele.
- Jakmile uživatel uzamkne zařízení, rozšifrovaný klíč třídy je (po 10 vteřinách) smazán.

Uložení klíčů, hesel…

Řada služeb systému (wifi, BT, VPN, iCloud,..), systémových aplikací (iMessage, e-mail, Safari…) a uživatelských aplikací potřebuje bezpečně uložit hesla, klíče a autentizační tokeny.

Pro tyto účely je určen **iOS keychain**, v němž jsou tyto citlivé položky uloženy v zašifrované formě.

Poznámka:

- Klíče, které šifrují master klíče Data Protection a Keychain Data Protection jsou uložené System keybag a v Effaceable Storage

Keychain v iOS

- Keychain je „secure storage container“ realizovaný jako SQLite databázový soubor uložený s třídou ochrany No Protection.
- Bezpečnost keychain je zajištěna podobně jako Data Protection pro soubory, ale s jinou klíčovou hierarchií. Pokud iOS nemá aplikován jailbreak, jedná se o nejbezpečnější způsob uložení důvěrných dat v systému.
- SQLite databáze obsahující Keychain je jediná v systému, takže položky z aplikací uložené v keychain nejsou samozřejmě v aplikačním sandboxu.
- Každá aplikace má vždy přístup ke svým tajemstvím uloženým v keychain, nebo lze sdílet položky mezi aplikacemi stejného vývojáře, to zajišťuje keychain démon na základě prefixů alokovaných prostřednictvím Developer Programu.
- Keychain lze prohledávat podle hodnot SHA1 atributů v metadatech (server name, account…) bez nutnosti rozšifrovat položky

Třídy přístupu k položkám v keychain

kSecAttrAccessibleWhenUnlocked

- Data jsou přístupná pouze když je zařízení odemknuto uživatelem. Používá se pro aplikace, které přistupují k prvku v keychain pouze, když jsou v popředí. Položky s tímto atributem migrují, pokud je záloha šifrovaná.

kSecAttrAccessibleWhenUnlockedThisDeviceOnly

- Data jsou přístupná pouze když je zařízení odemknuto uživatelem. Používá se pro aplikace, které přistupují k prvku v keychain pouze, když jsou v popředí. Položky s tímto atributem se nepřenášejí na nové zařízení.

Třídy přístupu k položkám v keychain

kSecAttrAccessibleAfterFirstUnlock

- Data jsou přístupná po prvním odemčení, zůstávají přístupná až do dalšího restartu. Položky s tímto atributem migrují, pokud je záloha šifrovaná.

kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly

- Data jsou přístupná po prvním odemčení, zůstávají přístupná až do dalšího restartu. Položky s tímto atributem se nepřenášejí na nové zařízení

Třídy přístupu k položkám v keychain

kSecAttrAccessibleAlways

- Data jsou přístupná vždy, nezávisle na stavu odemčení zařízení. Položky s tímto atributem migrují, pokud je záloha šifrovaná.

kSecAttrAccessibleAlwaysThisDeviceOnly

- Data jsou přístupná vždy, nezávisle na stavu odemčení zařízení. Položky s tímto atributem se nepřenášejí na nové zařízení

Bezpečnost zálohování

Zálohování na iTunes

- Zálohování na iTunes se provádí na počítač (standardně přes USB, lze však dovolit i wifi, pokud jsou ve stejné síti), v případě Windows PC do adresáře:
  \Users\%username%\AppData\Roaming\Apple Computer\MobileSync\Backup\
- Každá záloha má svojí složku a v ní několik tisíc souborů, jejich jména jsou sha-1 hashe *domainName-filepath* souborů. Formát databáze je proprietární, obsahuje 4 metasoubory – Info.plist, Manifest.plist, Status.plist a Manifest.mbdb.
- Reverzní analýza struktury záloh je uvedena např. v http://esec-lab.sogeti.com/dotclear/public/publications/11-hitbamsterdam-iphonedataprotection.pdf .
- Pokud záloha není šifrovaná, lze využít různé nástroje pro její zpřístupnění, například https://code.google.com/p/iphonebackupbrowser/ pro Windows.

Postup zálohování

- Připojit zařízení k počítači s iTunes
- Vybrat File>Devices>Back Up, nebo pravé tlačítko na zařízení a vybrat Backup Now, nebo v Devices vybrat zařízení a v Summary v sekci Backup lze manuálně provést Backup a Restore
- Kontrola záloh Edit>Preferences>Devices – zobrazí se seznam záloh, zálohy lze pouze mazat

Poznámky

- Zálohování je rovněž prvním krokem synchronizace zařízení s iOS s počítačem (pokud je zaškrtnuto).
- Samotný počítač s iTunes by měl být samozřejmě zálohován. Starší zálohy tvoří vlastně archiv a je možné se k nim vrátit, vždy se ale obnovuje celek, nelze obnovit jeden smazaný údaj.

Šifrování záloh

- Je možné zaškrtnout Encrypt iPhone Backup v iTunes a zadat komplexní heslo pro odvození šifrovacího klíče. Toto heslo může být zapamatováno v Keychain na mobilu.
- Pokud je záloha šifrovaná, zálohuje se i Keychain, jsou tudíž zálohována i všechna hesla (kromě těch, které jsou „This device only“) v Keychain uložená (wifi, weby, e-maily, aplikace…) a lze je obnovit na nové zařízení.
- Záloha je šifrovaná AES-256, je ale nutné zvolit kvalitní heslo, protože na zálohu lze útočit hrubou silou.

Zálohování na iCloud

- Zálohování na iCloud se provádí bez připojení k počítači, zpravidla pomocí wifi a automaticky v okamžiku, kdy je zařízení připojeno k napájení a zamčeno (lze samozřejmě i spustit ručně v *Settings>iCloud>Storage & Backup>Back Up Now*.
- iCloud backup není kompletní, zálohuje album fotoaparátu, SMS, iMessage, dokumenty a nastavení; nezálohuje uživatelský obsah, který nebyl zakoupen na iTunes Store, ani to, co bylo synchronizováno z počítače (např. fotky, které nevznikly na zařízení).
- Při zálohování na iCloud se přestane automaticky zálohovat na iTunes do vašeho počítače!
- Po provedení zálohy na iCloud uživatel dostane e-mail notifikaci. Nedostane ale notifikaci o Restore (tedy ani o potenciálně neoprávněném přístupu k záloze).
- Na iCloudu je zálohován pouze aktuální stav zařízení. Záloha uložená na iCloudu může být archivována na počítači http://support.apple.com/kb/HT4910 . Účelem archivu je napravení chyby uživatele, který si omylem něco smaže.

Obnovení ze zálohy

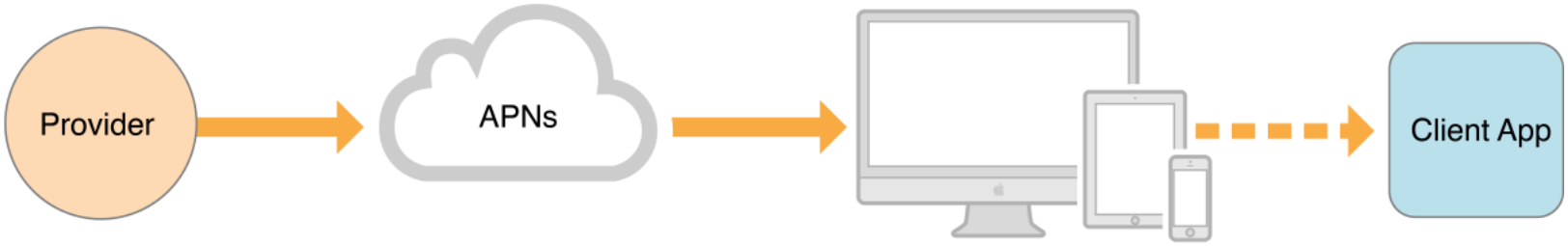
- iTunes a iOS umožňují obnovit zálohu na jiné zařízení stejného typu, nesmí mít ale starší verzi iOS. Obnovuje se celý systém, nelze obnovit pouze vybraná data (například pouze data určité aplikace).
- Obnova z iTunes se děje po připojení kabelu a volbě File>Devices>Restore from Backup
- Obnova z iCloud se děje pouze přes wifi.
- Pokud je třeba obnovit zálohu na nové zařízení (mám nový iPhone), pak v počátečním průvodci „Set up your device“ stiskneme tlačítko Restore from iCloud Backup nebo Restore from iTunes Backup
- Pokud se obnovuje na původní (staré) zařízení, je nutné nejprve smazat všechna data a nastavení ze zařízení Settings>General>Reset>Erase all content and settings (Nastavení>Obecné>Obnovit>Smazat data a nastavení). Předtím je vhodné se přesvědčit, že záloha existuje

Data in move

- Apple Push Notification Services
- iMessage

Apple Push Notification Service

- Notifikace je krátká zpráva, složená ze 2 částí – device token (adresa doručení) a těla zprávy (JSON property list, max 256 byte)
- Notifikace je jednosměrná, od providera (serveru dodavatele mobilní aplikace) přes APN k zařízení



Architektura APNs

- Architektura APNs má 3 subjekty:
  - Provider
    - má privátní klíč a certifikát od Apple. Certifikát obsahuje hodnotu bundle ID aplikace, je použitelný pouze pro tuto aplikaci.
    - Má device token (získaný od klientské aplikace) identifikující cílové zařízení.
  - Zařízení a aplikace
    - zařízení má privátní klíč a Push certifikát zařízení zařízení získaný při registraci zařízení u Apple.
    - aplikace získá device token během registrace k APN (typicky po instalaci) a poskytne ho providerovi. Device token je zašifrovaný klíčem APN.
    - zařízení použije device token při připojení k APN, které poté udržuje permanentní.
  - APNs
    - mají certifikáty CA, certifikáty a klíče pro validaci spojení a autentizaci poskytovatelů a zařízení. Vytváří device tokeny. Udržuje CRL pro certifikáty providerů a odmítne spojení pro odvolané certifikáty.

Device (Push) certifikát

- Při prvním připojení zařízení a jeho registraci a aktivaci u Apple vydá certifikační server běžící na serveru *albert.apple.com* device (*Push) certifikát*.
- Certifikát je podepsán autoritou *Apple Iphone Device CA* jejíž certifikát není „zadrátován v systému“ ☹ (certificate pinning).
- Certifikát se používá pro autentizaci klienta při sestavení TLS spojení s Push serverem.
- Push komunikace se používá pro notifikace, iMessage a FaceTime

Device token

- Device token je identifikátor zařízení (různý od UDID), přidělený APN při prvním připojení zařízení. Zařízení sdílí svůj token s providerem (aplikačním serverem), který jej používá pro každou odeslanou notifikaci.
- Pro iMessage je Device token příjemce poskytnut zařízení odesílající iMessage prostřednictvím adresářových služeb Apple

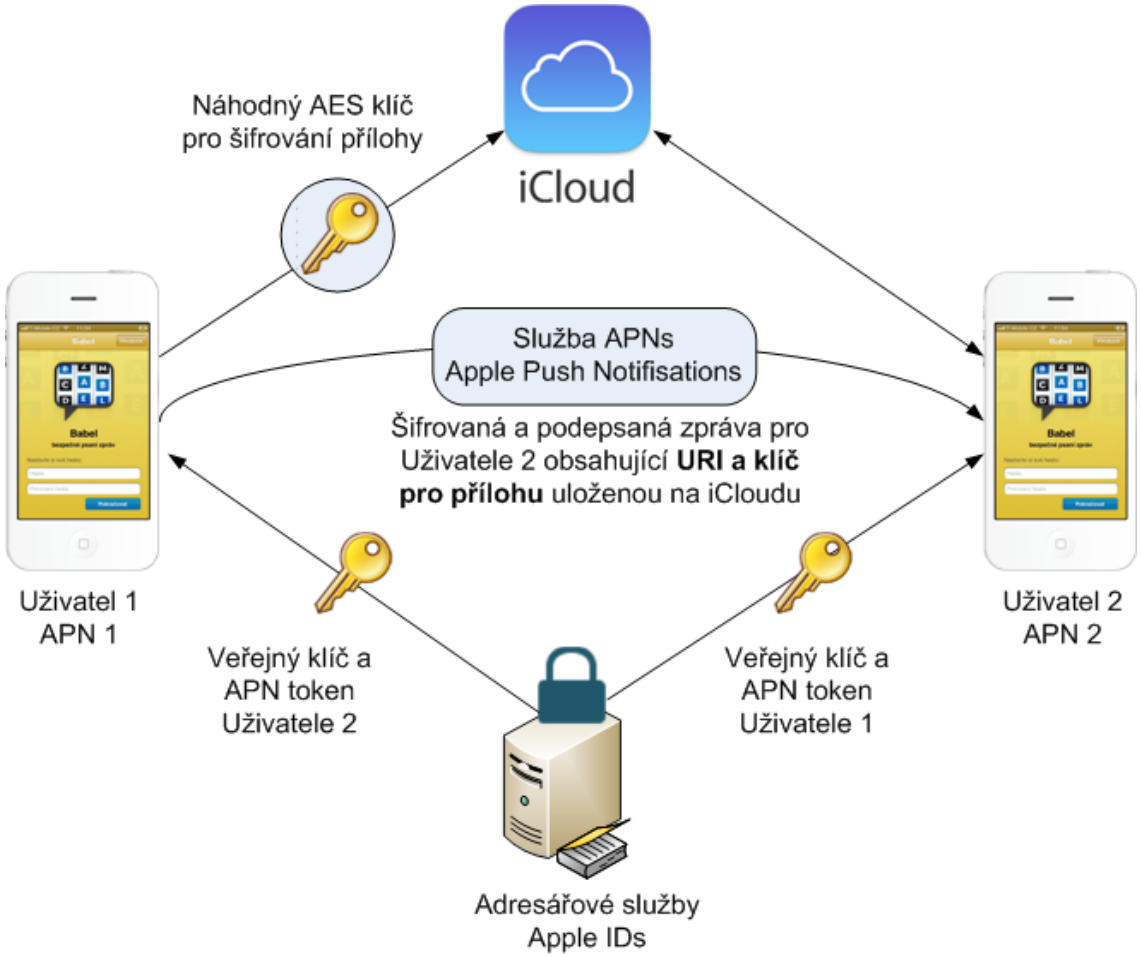
Připojení iPhone k Push serveru

- iPhone nejprve pošle dotaz typu TXT:
  nslookup -query=txt push.apple.com, vrátí se mu číslo X <= 255 s významem max. počet DNS adres (count=50)
- zprávy používají Push protokol s použitím TLS na serverový TCP port 5223 (není to XMPP, ale binární protokol), kde je klastr serverů se jmény:
  rnd[0-X]-courier.push.apple.com. Tato jména se překládají na veřejnou IP adresu Apple 17.Y.0.0
  Komunikace je chráněna TLS, s klientskou autentizací Push certifikátem.
- Detailní popis Push protokolu např. na http://theiphonewiki.com/wiki/Apple_Push_Service_Protocol

iMessage

- iMessage je služba pro přenos textových zpráv a příloh mezi zařízeními s iOS a OS X.
- Mezi zařízeními Apple se přenáší „několik miliard“ (=2-10) iMessage/den
- iMessage jsou zašifrovány mezi koncovými body přenosu
- iMessage používají 2 kanály – Apple Push Notification Service a iCloud pro přílohy a dlouhé zprávy (více než 256 byte)
- iMessage jsou na serveru smazány po doručení, pokouší se doručit na off-line zařízení maximálně 7 dní

iMessage


Náhodný AES klíč
pro šifrování přílohy
iCloud
Služba APNs
Apple Push Notifisations
Šifrovaná a podepsaná zpráva pro
Uživatele 2 obsahující **URI a klíč**
pro přílohu uloženou na iCloudu
Uživatel 1
APN 1
Uživatel 2
APN 2
Veřejný klíč a
APN token
Uživatele 2
Veřejný klíč a
APN token
Uživatele 1
Adresářové služby
Apple IDs

iMessage – adresářové služby

- Po aktivaci iMessage v *Nastavení > Zprávy > iMessage* jsou na zařízení generovány 2 klíčové páry (RSA 1280 pro šifrování AES klíčů a ECDSA 256 pro podpis zpráv). Privátní klíče jsou uloženy v keychain, veřejné klíče jsou zaslány do Apple IDS.
- IDS server **.ess.apple.com* (* = init, registration, service a další) poskytují službu adresáře s veřejnými klíči zařízení pro šifrování iMessage.
- Apple ID uživatele obsahuje pro jednotlivá zařízení:
  - APN (ID zařízení)
  - veřejný klíč zařízení
  - telefonní číslo
  - e-mail adresu
- ESS poskytuje klientskému zařízení:
  - device (Push) token, identifikuje zařízení, každé cílové URI má unikátní token
  - veřejný Klíč 1: ECDSA 256 bitů, určený k ověření podpisu zprávy (eventuálně) zaslané (zpět) z cílového URI
  - veřejný Klíč 2: RSA 1280 (divné číslo) určené k šifrování AES klíče, kterým je šifrována iMessage

  Pozn: korespondující privátní klíče jsou uloženy v keychain druhé strany

Touch ID

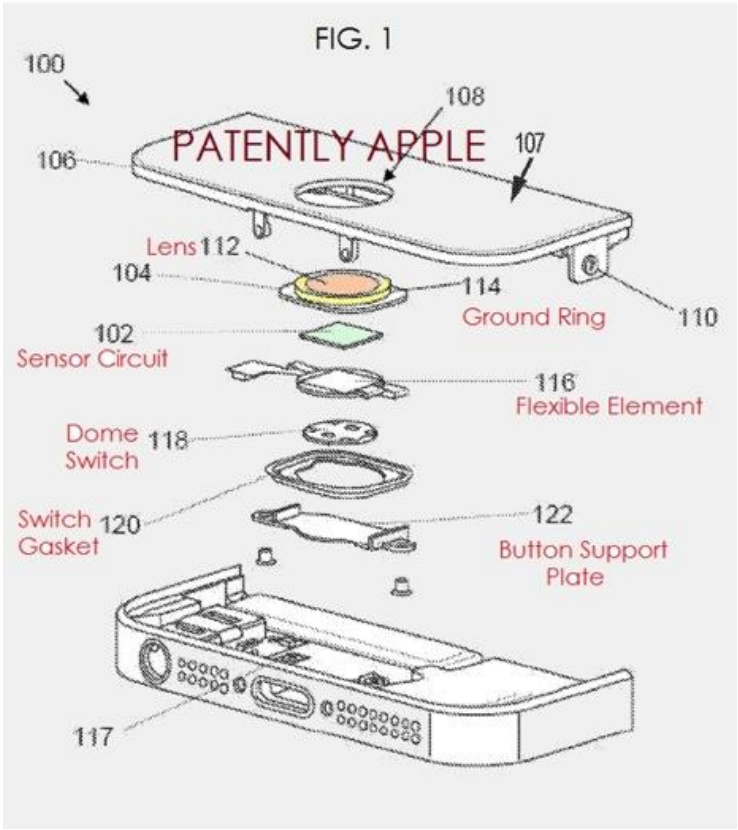
- Touch ID je systém pro čtení otisku prstů, zabudovaný do tlačítka Home iPhone 5s. Čte otisky prstů z libovolného úhlu a (možná kontroverzně) učí se z úspěšně akceptovaných otisků další data a rozšiřuje tak mapu otisku.
- Senzor má rozlišení 500 ppi v rastru 88 x 88 bodů, je ukryt pod safírovým sklíčkem a obklopen kovovým kroužkem, který má funkci kapacitního snímače. Pouze, když kroužek detekuje přiložení prstu, je snímač aktivní (to je určité bezpečnostní opatření) a (údajně) vysílá signál, který proniká do živé části kůže, kde skenuje kožní póry, údolí a hřbety otisků..
- Technologii získal Apple akvizicí společnosti AuthenTec v roce 2012 za 356 mil. USD.

Touch ID

Nasnímaná data jsou zaslána do Secure Enclave, kde jsou pomocí ztrátové a jednocestné transformace převedena do vektorové reprezentace, poté jsou zdrojová data snímače smazána z paměti.

Vektorová data nejsou spojena s žádnou identitou, jsou uložena v zašifrovaném tvaru v Secure Enclave a nikdy neopustí zařízení. Nejsou rovněž zálohována na iCloud nebo iTunes.

Apple's Touch ID Patent: Fingerprint Recognition Sensor



Secure Enclave

Enkláva (pojem mezinárodního práva) je území státu kompletně uzavřené v území jiného státu.

- Secure Enclave je bezpečnostní koprocesor, umístěný na čipu procesoru Apple A7. Má vlastní boot a vlastní proces aktualizace software, oddělený od aplikačního procesoru.
- Secure Enclave je zárodek bezpečného HW, obsahuje HW generátor náhodných čísel, používá šifrovanou paměť, provádí kryptografické operace pro ochranu dat a klíčů a to i v případě, že by jádro systému bylo kompromitováno.

Secure Enclave

- Každá Secure Enclave má unikátní UID, který není známý Apple a není přístupný ostatním částem systému.
- Při každém startu zařízení je vytvořen náhodný klíč, zkombinován s UID a použit k šifrování oblasti paměti určené pro Secure Enclave. Pokud Secure Enclave ukládá soubory do souborového systému, diverzifikuje klíče pomocí UID a čítače, který brání útoku na opakování.
- Secure Enclave zpracovává otisky prstů, porovnává je s uloženými vzory a při shodě umožňuje přístup/nákup.
- A7 komunikuje s Touch ID prostřednictvím sériové sběrnice, posílá data, ale není schopen je číst, neboť jsou šifrována pomocí klíče relace, odvozeného ze sdíleného klíče zařízení, který sdílí Secure Enclave a Touch ID

Touch ID FAR

- Touch ID umožní rozeznat až 5 různých otisků prstů, pokud je uložen jen jeden, nabývá FAR hodnoty 1:50.000 - to je více možností, než standardní 4 místný PIN, kde pravděpodobnost náhodného uhodnutí je 1:10.000).
- Při uložení vzorků 5 prstů je FAR stejné, jako u 4 místného PIN.
- Počet pokusů je omezen na 5, poté je vyžadováno zadání hesla. Pravděpodobnost přijetí náhodného otisku (uloženo 5 vzorků, použito 5 pokusů) je v nejhorším případě 1:2.000.

Touch ID a heslo

Hlavní výhodou je možnost použití kvalitního dlouhého hesla, které by nebylo vhodné k rutinnímu zadávání.

Nejedná se o vícefaktorovou autentizaci, ale o náhradu zadávání hesla v běžných případech. Přesto je nutné heslo znát a zadat v následujících případech:

- iPhone 5s byl zapnut, nebo restartoval
- iPhone 5s nebyl odemčen více než 48 hodin
- Bylo neúspěšně vyčerpáno všech 5 pokusů v řadě při ztotožnění otisku prstu
- Pokud má být přidán další otisk
- iPhone 5s obdržel příkaz remote lock

odemčení iPhone 5s s Touch ID

- Odemčení není pouze vlastní odemčení „desktopu“, jako u PC, ale současně je to proces obnovení klíče Data Protection, kterým jsou zašifrována data s třídou ochrany Complete. Příslušný klíč Data Protection je standardně obnoven na základě zadání hesla, po zamčení zařízení je klíč zničen a data s třídou ochrany Complete jsou nedostupná.
- V případě aktivace Touch ID je postup jiný – Data Protection klíč není při zamčení zničen, ale zašifrován klíčem Touch ID. Klíč je rozšifrován po zadání platného otisku. Data Protection klíč je uložen v nepersistentní paměti, takže je zničen při rebootu zařízení a také po 48 hodinách nebo 5 neplatných pokusech Touch ID.

Touch ID a aplikace

- Touch ID lze též aktivovat k on-line nákupům na iTunes Store, App Store a iBook Store, místo zadání Apple ID hesla.
- Apple nedává žádný přístup třetím stranám k použití Touch ID a Secure Enclave ☹.
- Spekuluje se, že Touch ID bude použit pro mobilní platby vázané na autorizaci v rámci existující infrastruktury Apple iTunes.

Jailbreak

Jak zabránit iOS a iPhone, aby byly relativně bezpečné

- Jailbreak je postup vedoucí k odstranění omezení, které zabraňují zařízením s iOS instalovat aplikace, které nebyly autorizované společností Apple (instalovat aplikace z jiných zdrojů, než AppStore), změnit UI, odstranit omezení na operátora.
- Jailbreaking je typ eskalace práv, který dává root přístup k systému souborů a manažeru přímo prostřednictvím aplikace, nebo z jiného počítače s použitím SSH..
- Apple schvaluje aplikace na základě jejich shody s iOS Developer program license Agreement, nicméně důvod k odmítnutí aplikace nemusí být pouze bezpečnostní nebo funkčně provozní (stabilita, drancování baterie používáním wifi a 3G, dostupnost služeb…), případně obsahující závadný materiál dle „racionálního úsudku Apple“, ale poměrně široce vyhovující zájmům společnosti Apple. Mezi zakázané aplikace patří např. aplikace, které suplují některé funkce AppStore, mění UI iOS, používají notifikace k neschváleným účelům, analyzují a měří wifi sítě apod.

iOS Jailbreak x Android root

Jailbreak je jiný koncept než Android root. Jailbreaking musí překonat více omezení současně:

- Prevence bootování pozměněného, nebo zcela jiného OS
- Prevence instalace nepodepsaných aplikací
- Restrikce práv root access (superuser) pro uživatelské aplikace

Cydia – appstore pro jb iOS

K nahrání alternativních aplikací byl vytvořen store Cydia https://cydia.saurik.com/ a příslušná mobilní aplikace na JB telefony.

Cydia se nahrává pomocí JB nástrojů, jako jsou evasiOn: http://evasi0n.com/ nebo or redsnOw

Poznámka

Cydia pomonella (obaleč jablečný) je známý červ v jablku

Scénář útoku

- iOS zařízení má útočník fyzicky k dispozici, je zamčeno kvalitním heslem a nebylo na dálku vymazáno. Útočník vypne zařízení a vyndá SIM, aby zabránil vymazání na dálku.
- Nejprve se provede jailbreak a nainstaluje SSH server, nakopíruje se skript pomocí SSH spojení, který najde hesla, pokud nejsou chráněna i kódem pro odemčení obrazovky. Jedná se o hesla, která musí být k dispozici bez zadání kódu pro odemčení obrazovky – zejména síťová hesla pro wifi, IPSec, PPP.
- SIM PIN je také uložen v keychain
- FAQ o slabinách keychain lze nalézt v http://sit.sit.fraunhofer.de/studies/en/sc-iphone-passwords-faq.pdf

Existence JB zvyšuje bezpečnost

Apple historicky vydal řadu záplat, zabraňujících zneužitelnosti slabin v iOS pomocí jailbreakových utilit, v současnosti je systém iOS 7.1 na procesoru A7 bez JB.

BootROM prostředí a jeho případné slabiny samozřejmě nelze aktualizovat pomocí záplat iOS.

Kdyby nebyl jailbreak, netlačil by Apple bezpečnost iOS a iDevice tak rychle dopředu.

Co udělat před prodáním nebo předáním iOS zařízení

- Zálohovat zařízení
- Smazání kompletního obsahu a nastavení iPhone – Nastavení>Obecné>Obnovit>Smazat data a nastavení.
- Pokud jste to takto neudělali a iPhone již nemáte a pokud je aktivována služba Find My iPhone, je nutné zadat Apple ID a heslo. Zařízení bude smazáno a odpojeno od mého účtu
- Pokud jste to takto neudělali, změňte si alespoň Apple ID heslo, aby nový majitel nemohl smazat vaše iCloud data.
- Pozor, nemazat obsah (kontakty, fotky, …) ručně, pokud jste připojeni k službě iCloud, byly by smazány i zde.

Co udělat vždy

- Chránit zařízení silným heslem
- aktivovat Touch ID, abychom se nezbláznili z předchozího opatření
- aktivovat smazání všech dat při 10 neúspěšných pokusech zadat heslo (záloha!)
- aktivovat Find My iPhone pomocí iCloudu + Remote Wipe
- chránit PC s iTunes (zálohy)
- zálohovat PC (archiv iTunes záloh)
- ve firmě pokud možno použít MDM/MAM systém a nastavit bezpečnostní politiky

a především…

- ….zůstat iOvce (neinstalovat JB…)

Dotazy?

Ivo Rosol
ředitel vývojové divize
OKsystem s.r.o.
rosol@oksystem.cz

www.getbabel.com

www.okbase.cz

www.oksmart.cz