Techniky získavania citlivých údajov z Apple iOS zariadení

Ing. Eugen Antal Ing. František Baranec

Slovenská Technická Univerzita v Bratislava
Fakulta elektrotechniky a informatiky
Ústav Informatiky a Matematiky

EurOpen 30.09.2013

Obsah

- Apple iOS
- Jailbreak, typy zraniteľností
- Forenzná analýza
- IB aplikácie vybraných SVK bánk

iOS a Apple zariadenia

- Apple Inc.
- Unix jadro;
- iPhone, iPod Touch - 2007;
- iPad - 2010;
- iOS 7 - sept. 2013;
- uzavretá platforma;
- prísne Apple smernice.

Niektoré bezpečnostné prvky

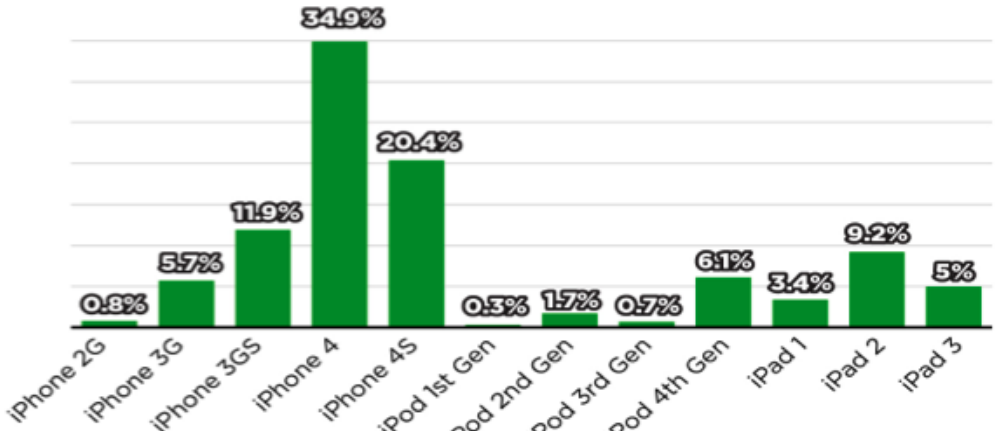
- Secure boot chain;
  - Podpísané komponenty bootovacieho procesu.
  - Integrita bootovania.
  - Po spustení sa vykoná kód z BootROM.
- DEP (data-execution protection);
  - Funkcia procesora.
  - Zamedzenie možnosti spustenia kódu.
  - Možnosť využitia - prísne kontrolované podmienky.

Niektoré bezpečnostné prvky

- Code signing;
  - Nutnosť podpisu certifikátom.
  - Podpísané pri distribúcii Apple store.
  - Zabraňuje zmenu kódu.
- Data protection;
  - Dodatočné šifrovanie.
  - AES (HW).
  - Odvodené od hesla, neukladá sa.

Jailbreak

- Vypnutie bezpečnostných prvkov iOS.
- Potreba nájsť HW či SW zraniteľnosť.
- Modifikovanie kernelových záplat.
- Root prístup.
- Cydia, Installous - neoficiálne aplikácie.
- Odblokovanie telefónu.



Typy Jailbreaku

Tethered Jailbreak (pripojený)

- Zmizne po reštarte.
- Pripojenie cez USB - názov.
- limera1n - zraniteľnosť v jadre USB ovládača.

Untethered Jailbreak (nepripojený)

- Permanentné.
- Bootchain, HW zraniteľnosť.

Kombinácia tethered a exploit na zachovanie stálosti.

Typy zraniteľností

Bootrom level

- Bootrom (HW súčasť zariadenia) - nemožno odstrániť.
- Neodstraňuje SW aktualizácia - ideálne pre Jailbreak.
- limera1n - do A5 procesor (iPhone 4S, iPad 2)
- Začiatok bootchain - AES HW heslá.

iBoot level

- Odstrániť SW aktualizáciou.
- Tiež začiatok bootchain.

Userland level

- Na úrovni iOS prostredia.

Forenzná analýza

- Súhrn techník a nástrojov.
- Hľadanie dôkazov na elektronických zariadeniach.
- Nesmie dôjsť k modifikácii údajov.
- Zdroje FA na iOS:
  - zo zálohy (iTunes, iCloud);
  - zo zariadenia.

FA zo zálohy 1/2

- Logická kópia súborového systému.
- AFC protokol (Apple file connection).
- AFC zálohuje:
  - kontakty, SMS, história hovorov;
  - kalendáre, fotky;
  - nastavenie siete, databázové súbory;
  - **Keychain**;
  - detaily zariadenia (UDID, sériové čísla, SIM).
- AFC nezálohuje:
  - obsah synchronizovaný z iTunes
  - (videá, skladby, ...)

FA zo zálohy 2/2

Sada existujúcich nástrojov:

- iPBA 2 (iOS Backup Analyzer);
- iPhone Backup Extractor, iPhone Backup Browser.

Záloha:

- nešifrovaná - všetky údaje;
- nešifrovaná + data protection;
  - Kľúče v Backup keybag - šifrovaný pomocou *0X835 key*.
  - *0X835 key* získať zo zariadenia (Jailbreak, custom OS).
- šifrovaná;
  - iTunes heslo uložené v Keychaine zariadenia.

FA na fyzickom zariadení

- Bit-by-bit kópia súborového systému.
- Možnosť obnovenia vymazaných dát.
- Priamo nie je možné spustiť nástroj na analýzu.
  - Opatrenia: DEP, Sandbox, DataProtection ...
  - Jailbreak.
  - Nabootovanie custom OS.
    - DFU (Device Firmware Upgrade) mód.
    - limera1n v BootRom do A5.

IB aplikácie

- Získať citlivé informácie.
- Keychain a súbory.
- Aplikácie:
  - Platby a účty - SLSP;
  - Tatra banka - TB;
  - BankAir - UniCredit
- UniCredit - žiadne čitateľné údaje.
- TB, SLSP - internet banking ID
  DoS cez web rozhranie.

Q & A

Ďakujem za pozornosť.