Bezpečnosť mobilných aplikácií (iPhone)

Juraj Bednár
juraj.bednar@digmia.com

Čo je počítač?

Aplikačná bezpečnosť

- Z pohľadu aplikácie
  - Keď dodáme túto aplikáciu, aká je jej bezpečnosť
- Trochu užívateľského pohľadu
  - Dokumentovať riziká
    - Ukradnutie
    - Malware
    - ...

Aplikačná bezpečnosť

- Robí sa podľa metodológií ako napr. OWASP
- Mobilné aplikácie nie sú na trhu dostatočne dlho
  - Pre klient-server app sa dá použiť subset OWASPu
    - V závislosti od aplikácie je možné preskočiť časti ako napríklad XSS alebo JavaScript útoky
    - SQL Injection a iné časti je dobré použiť
  - Veľa potenciálnych bodov nepokrýva žiadna akceptovaná metodika

Bezpečnosť mobilných app všeobecne

- Ukladanie
  - Citlivých dát
    - Fotografie, privátne dáta, dokumenty
    - Prístupové kľúče
  - Menej citlivé
    - Cache (môže byť citlivé)
    - Obrázky, kód
    - Necitlivé konfiguračné nastavenia
- Malware
- Ukradnutie zariadenia
- Autentifikácia (namiesto SMS autentifikácie)

iPhone

- Aplikácie oficiálne idú cez AppStore
- Možnosť “jailbreaknút”” a nainštalovať iný SW
- Časté bezpečnostné chyby (PDF, Safari, ...)
  - Užívatelia málokedy updatujú
    - Nie je to povinné
    - Je to zložité, častokrát sa stratia dáta
    - Malá pridaná hodnota “point releasov” pre väčšinu užívateľov
    - O “hacknutí” a zabezpečení telefónu málokto rozmýšľa
- Operačný systém založený na BSD a OSX
- Veľa inštalácií rovnakého systému – známe prostredie

iPad

- Rovnaké aplikácie, rovnaký OS, rovnaké chyby
- Viac interakcie s užívateľom, ale tiež veľmi nízka viditeľnosť “do systému”

iPhone keystore

- Databáza kľúčov a citlivých informácií
- Uložená v SQLite3 databáze
- Zašifrovaný kľúčom unikátnym pre zariadenie
  - Tento kľúč zariadenie nikdy nevydá, vie len spraviť operáciu (TPM)
  - Backup je možné obnoviť len na rovnakom kuse zariadenia (pri reklamácii výmenou zariadenia to nie je možné)
  - Ak má útočník prístup do userlandu telefónu, vie si samozrejme vyžiadať dešifrovanie akéhokoľvek ciphertextu

iPhone keystore

- “Šifrované backupy”
  - iTunes nastaví symetrický šifrovací kľúč do telefónu (neukladá si ho)
  - Backupy sú od tohto momentu šifrované (telefónom) na tento symetrický kľúč
  - Jeho brute-force (keďže kľúč volí užívateľ, ...) sa dajú z iPhone backupu získať senzitívne informácie
- Ako bezpečne ukladať dáta?
  - Časť do keystoru, XOR s random dátami ukladanými mimo časti, ktorá sa zálohuje
  - Radšej nech sa užívateľ reautentifikuje alebo musí začať “from scratch”, ako riskovať únik citlivých informácií.

Všeobecne k ukladaniu citlivých autentifikačných informácií

- V prípade ukradnutia telefónu má väčšinou útočník čas na bruteforce
  - Používať schémy, ktoré bruteforce maximálne sťažujú (padding ho uľahčuje, off-line overovanie tiež)
  - Server by mal pri akomkoľvek podozrení odmietnuť ďalšie požiadavky a žiadať reautentifikáciu alebo novú výmenu kľúčov

Malware

- iPhone je štandardná platforma, stačí písať malware pre jeden typ OS
- Ak je aplikácia pre viacero mobilných platforiem, efektivita sa prudko znižuje
- Malware je možný, vie robiť to, čo bežný unix proces (čítať súbory, posielať signály, debuggovať cudzí kód, čítať cudziu pamäť)
  - Dvaja užívatelia

Malware

- Riziko je cca rovnaké ako pri klasickom PC
  - + štandardná platforma (nie milión príchutí windowsu)
  - - užívatelia nemôžu “spúšťať” ľubovoľné 3rd party aplikácie. Treba exploitovať.
- Malware je prakticky neviditeľný
  - Žiadny antimalware
  - Užívateľ nevidí systémové informácie, nemá shell
  - Môže bežať malware mesiace, bez toho, aby si to všimol
- Malware je zatiaľ cielený, rozšírené malware pre iPhone prakticky neexistujú.

Forenzná analýza

- Dump FS je možný
- Štandardný UNIX prístup
- Telefón obsahuje väčšinou veľmi citlivé informácie

Disassemblovanie a analýza kódu

- Štandardná architektúra (ARM)
- Objective-C veľmi uľahčuje disassemblovanie
  - Všetky volania metód idú cez jednu low-level funkciu
    - Možnosť rekonštrukcie objektovej štruktúry, symbolických názvov (analýza sa dá ľahko automatizovať)
  - Binárky obsahujú veľmi veľa debug informácií (častokrát X-Code pridá cesty k zdrojákom, ktoré boli kompilované)
- Neexistuje ekvivalent kdump, strace, truss
- Možnosť online debugovania cez gdb (krokovanie, čítanie pamäte)
- Možnosť odchytávania sieťovej prevádzky (tcpdump)
- Možnosť odchytenia kľúčov (client-side certifikát pre SSL nepomôže, overovanie server-side SSL možné podvrhnúť a malware vie spraviť man in the middle)

Distribučný kanál

- AppStore
- Developer účet vie tlačiť nové verzie
- Užívatelia málokedy upgradujú OS, aplikácie upgradujú častejšie

Thanks to

- Tomáš Zaťko
- Martin Mocko (assembler guru)

Otázky?

Juraj Bednár
juraj.bednar@digmia.com