Veres-Szentkirályi András OSCP GWAPT

Zsebtolvajok a XXI. században

Bemutatkozás

- Etikus hackelés
  - Weboldaltól az RFID-ig
  - Konfiguráció-elemzéstől forráskód tesztekig
- Oktatás
  - Fejlesztőknek
  - Üzemeltetőknek
  - Vezetőknek
- Tanácsadás
- > 5 év szakmai tapasztalat minden szakterületen

Bemutatkozás

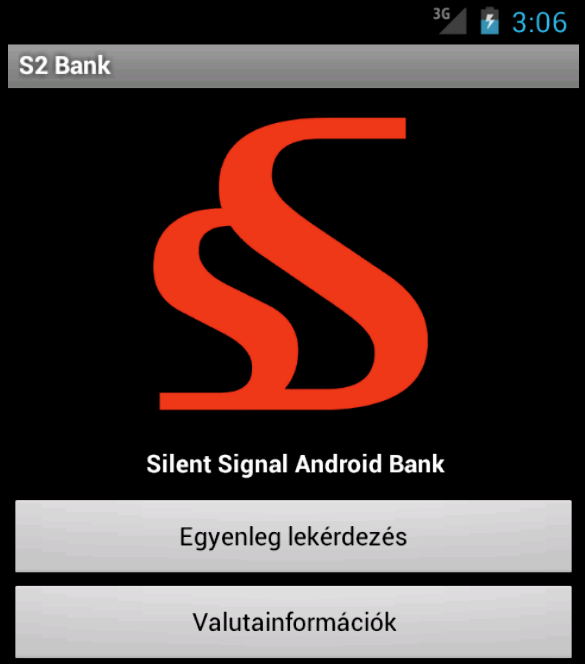
- Egy lépéssel a világ előtt: 0-day bejelentések
- Nemzetközi hackerversenyek
  - How Strong Is Your Fu?
    3. és 5. hely (> 1000 induló)
- **OSCP**, **GWAPT**, CISSP, OSCE, OSWP, GPEN
- Kiemelt ügyfeleink:
  - Pénzintézetek
  - KKV
  - Államigazgatás

WWW.SILENTSIGNAL.HU

Bevezetés

- Okostelefonok mindenütt
- Egyre nagyobb bizalom
  - adat és
  - kód irányába is
- Hányfaktoros is az a bizonyos autentikáció?
- Biztonságos a kapcsolódás módja?

Állatorvosi ló



Fejlesztők nézőpontja

- Új technológia
- Új keretrendszer
- Új protokoll(ok)

- „régi” hibák
- „elavult” best practice-ek
- „üzemeltető” fejlesztők

Támadók nézőpontja

- Új technológia
- Új keretrendszer
- Új protokoll(ok)

} támadási felület

- Sok felhasználó
- Sok on-line eszköz
- Kezdetleges rendszerszintű védelem

Etikus hackerek nézőpontja

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

- Gray-box tesztelés
  - nincs hozzáférés a forráskódhoz
  - van felhasználónév-jelszó páros
  - van egy APK fájl
    - mennyire megszerezhető?
    - mennyire Android-specifikus a következmény?
  - nem teljes körű a vizsgálat
  - nem csak első vérig

WWW.SILENTSIGNAL.HU

Tesztelési menetrend

„Mesterlövésztől a közelharcig”

1. Statikus kódanalízis
2. Dinamikus kódanalízis
3. Passzív hálózati támadás
4. Aktív hálózati támadás + DEMO

Statikus kódanalízis

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

- APK-ból Dalvik bájtkód kinyerhető
  - Dalvik bájtkód átalakítható JAR-rá
  - innentől meglévő eszközökkel fejtegethető
- Kliens működése megismerhető
  - következtetés a szerver működésére
- Árulkodó osztály- és változónevek
  - „ellenszer” a ProGuard
  - fontos kérdés a debugolhatóság

WWW.SILENTSIGNAL.HU

Dinamikus kódanalízis

- APK-ból kinyert kód változtatás után újrafordítható és futtatható
- Digitális aláírás? CA nélkül?
- Kliens működése befolyásolható
  - saját hoszt, IP cím, telefonszám, APN…
  - saját kriptográfiai adatok: hash, kulcs, cert
  - DEBUG=1 és társai
- Megbízunk a kliensünkben?

Passzív hálózati támadás

- Titkosítatlan csatornák? 2012-ben?
- Elég az autentikációt titkosítani?
- Visszajátszhatók a tranzakciók?
- Az API-k nagy része ma HTTP feletti
  - Basic auth?
  - Cookie?
    - Secure?
  - WSSE?

Aktív hálózati támadás

- Elég, ha „titkosított” a kapcsolat?
- Mitől hitelesített a csatorna?
  - Ismert CA által aláírt tanúsítvány
    - szűk beépített lista
    - kiben bízunk meg valójában?
  - Saját megoldás
- Hol tároljuk a kriptográfiai adatokat?
- Konfigurációmenedzsment?

Összefoglalás

- Kezeljük helyén az elhangzottakat!
- Ne dobjuk ki a fejlesztési tapasztalatokat
  - sem webes (API),
  - sem vastagkliens (telefon) oldalról!
- Ha valamiben nem vagyunk biztosak,
  - ne tippeljünk,
  - dokumentációnak se higyjünk vakon,
  - próbáljuk ki, **teszteljük le**!

Köszönöm megtisztelő figyelmüket!

Facebook

vsza@silentsignal.hu

web

e-mail

WWW.SILENTSIGNAL.HU