Zsebtolvajok a XXI. században

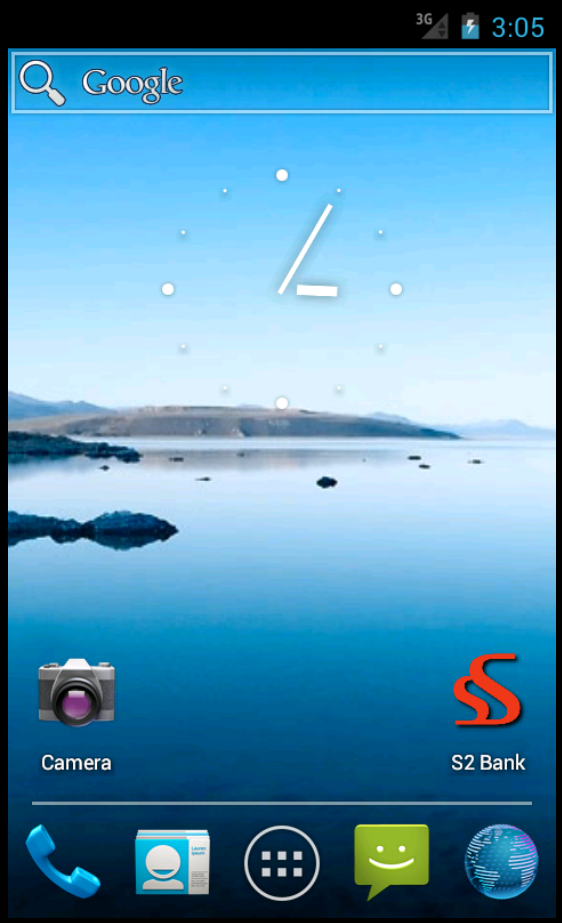
Veres-Szentkirályi András
vsza@silentsignal.hu

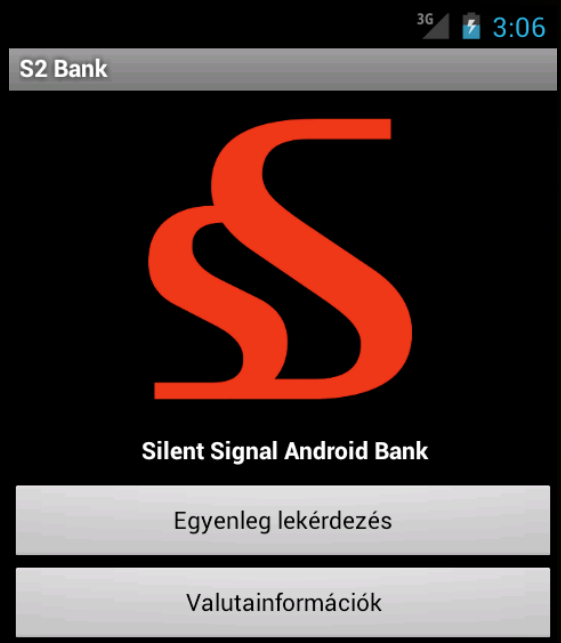
Silent Signal
szakmai délután
2012-03-23

Bevezetés

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

Állatorvosi ló





SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU

Mobil alkalmazás audit gray-box megközelítéssel

- nem áll rendelkezésre forráskód
- van felhasználónév-jelszó páros (s2/s2)
- van egy APK fájl
- nem teljes körűen!
- nem csak első vérig!

1. demo: aktív hálózati támadás

- APK kicsomagolása
- Kulcstár felfedezése
- Kulcsok vizsgálata
- MITM támadás

1. demo tanulságai

- Kulcstárban sem bízzunk vakon
- Fejlesztői kulcs is lehet kockázat
- A hálózat sosem megbízható

2. demo: passzív hálózati támadás

- Hálózat lehallgatása
- Süti megszerzése
- Munkamenet megszerzése

2. demo tanulságai

- Minden legyen titkosított és hitelesített!
- HTTP mindig HTTP marad
- Látott valaki kilépés gombot?

3. demo: statikus kódanalízis

- APK kicsomagolása
- DEX–JAR konverzió
- JAR visszafejtése
- (ProGuard hatásának bemutatása)

3. demo tanulságai

- „Ami a kódban van, az titkos” – tévhit
- Obfuszkáció
  - Defense in Depth?
  - Security by Obscurity?
  - Debug / Configuration Management?

4. demo: dinamikus kódanalízis

- APK visszafejtése köztes kódra
- Módosítást követően újraépítés
- Kód aláírása
- Telepítés emulátorba

4. demo tanulságai

- Attól, hogy valami obfuszkált, még módosítható
- URL-ek, telefonszámok, debug flagek érdekesek
- A digitális aláírás más ellen véd

Összefoglalás

- Kezeljük a 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 feltétlenül higyjünk,
  - próbáljuk ki!


Köszönöm a figyelmet!
vsza@silentsignal.hu
http://silentsignal.hu
SILENT SIGNAL
VÉSZJELZÉS HELYETT...
WWW.SILENTSIGNAL.HU