Zsebünkre megy a játék

Veres-Szentkirályi András
vsza@silentsignal.hu

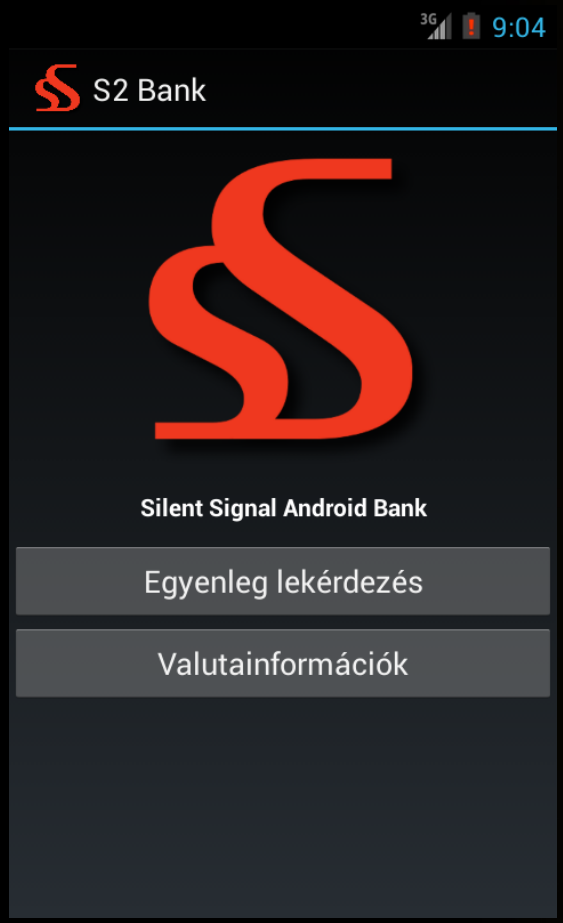
smartmobil
2013. április 4.

Zsebünkre megy a játék

- Webalkalmazás (2000) → okostelefon app (2010)
- Egyre nagyobb bizalom
  - adat és
  - kód irányába is!
- Mit adtak nekünk a böngészők?
  - Szegény ember kétfaktoros autentikációja: SMS
  - Biztonságos kapcsolódás: SSL/TLS
  - Kontrollált kódfuttatás: szerveroldali nyelvek

http://xkcd.com/1174/

Állatorvosi ló: S2 Bank app



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: statikus kódanalízis

- APK kicsomagolása
- DEX $\rightarrow$ JAR konverzió
- JAR visszafejtése
- (ProGuard hatásának bemutatása)

2. demo tanulságai

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

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!
Facebook
vsza@silentsignal.hu
web
e-mail
SILENT SIGNAL
VÉSZJELZÉS HELYETT...
WWW.SILENTSIGNAL.HU