

Okostelefon biztonság

Veres-Szentkirályi András
vsza@silentsignal.hu



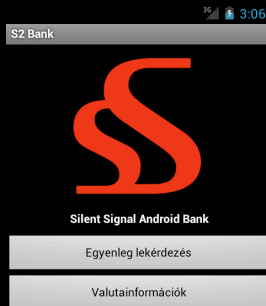
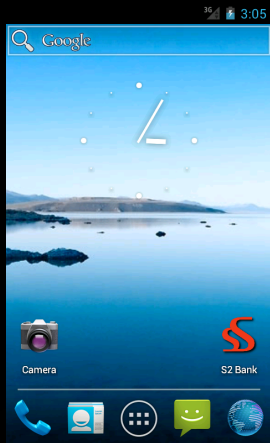
App!2012

2012-11-20

Bevezetés

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

Állatorvosi ló



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 bízunk 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: dinamikus kódanalízis

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

3. 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 higgyünk,
 - ▶ próbáljuk ki!

Köszönöm a figyelmet!

Facebook

vsza@silentsignal.hu

web

e-mail