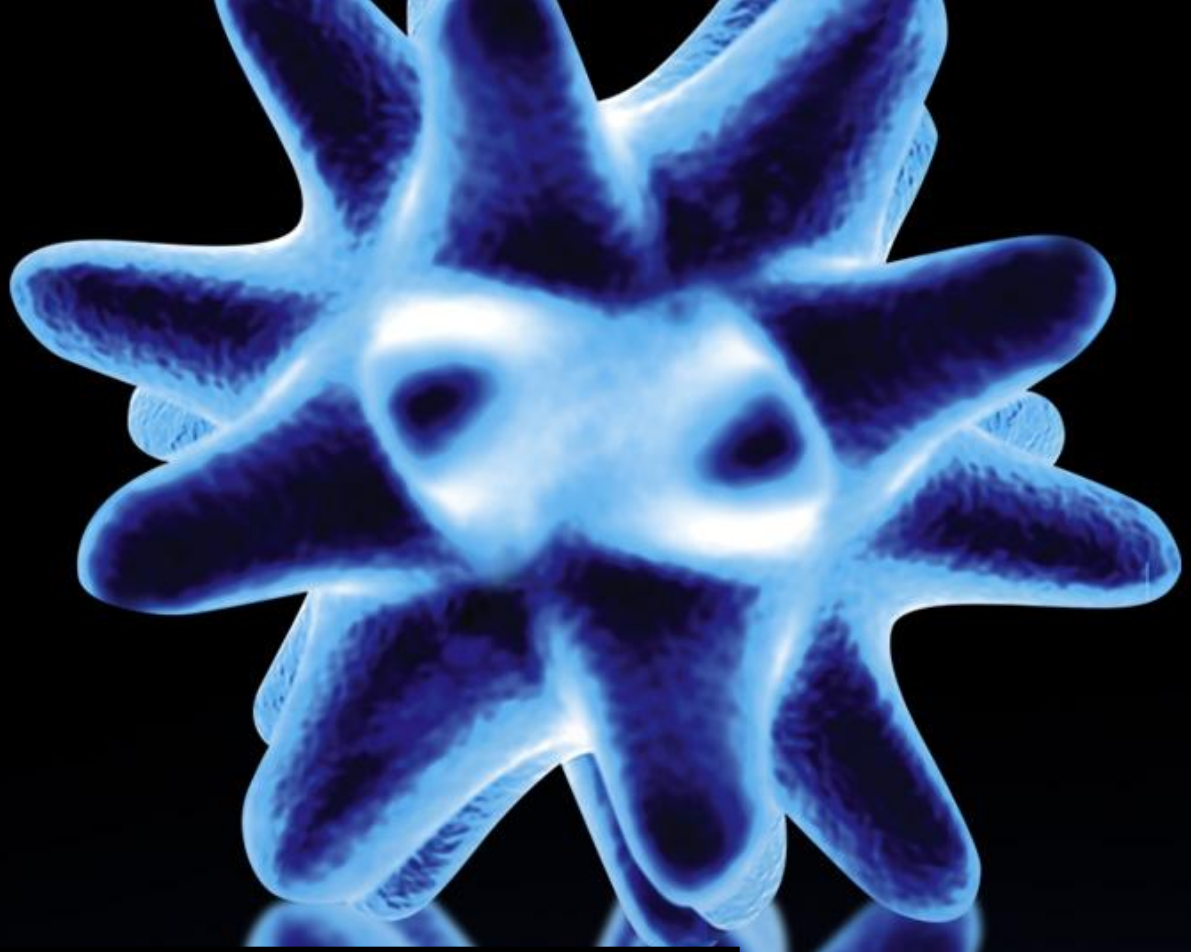
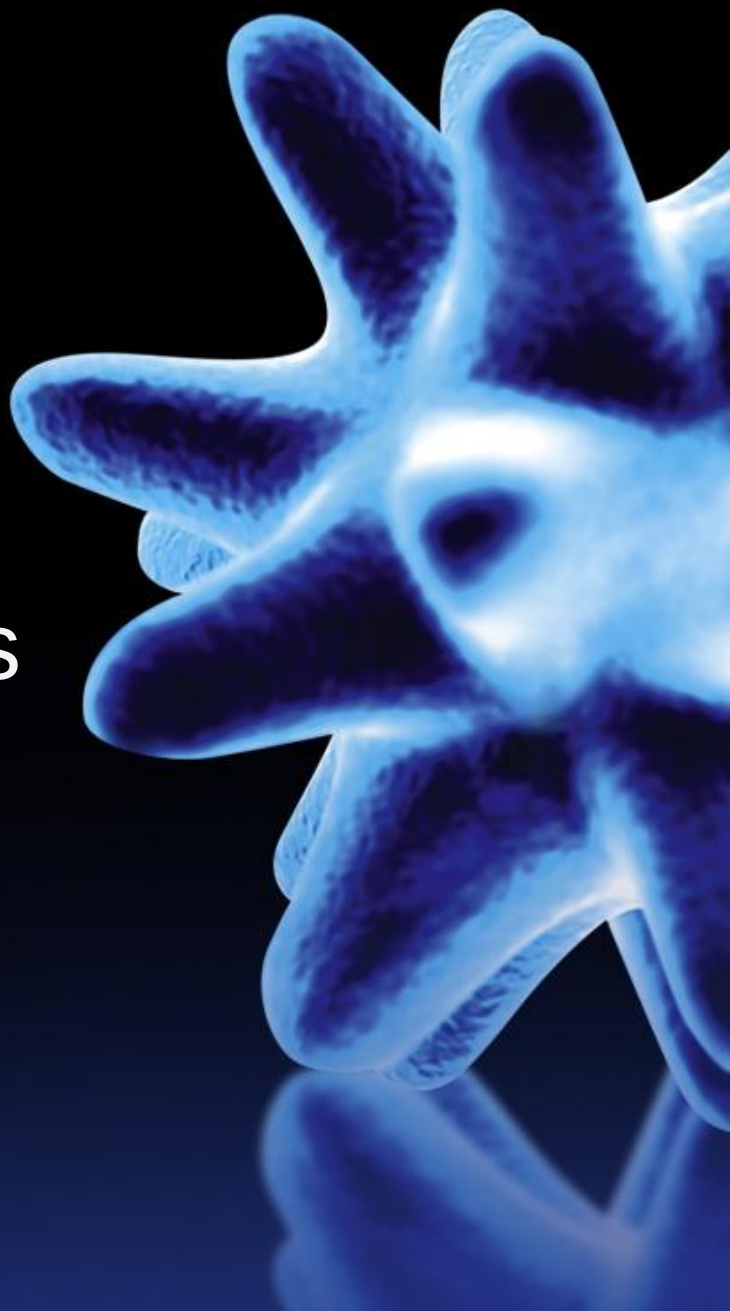
ethical hacking



Do Androids dream of electric sheep?,
avagy mennyire álmodhatunk biztonságos mobil eszközökről

Bemutatkozás



Veres-Szentkirályi András

Silent Signal

IT biztonsági szakértő

OSCP

vsza@silentsignal.hu

Miért Android?

2011 will be the year Android explodes

Posted by Seth Weintraub
December 22, 2010 2:50 PM

Ever-improving networks and a big hardware announcement that will send handset prices plummeting both point to smartphone growth in 2011 that could totally eclipse anything we've seen before.

kind of smartphone growth.) Image by
er via Flickr

et penetration of smartphones.

hones sold this year, compared to

Hárommilliárd letöltött appnál tart az Android

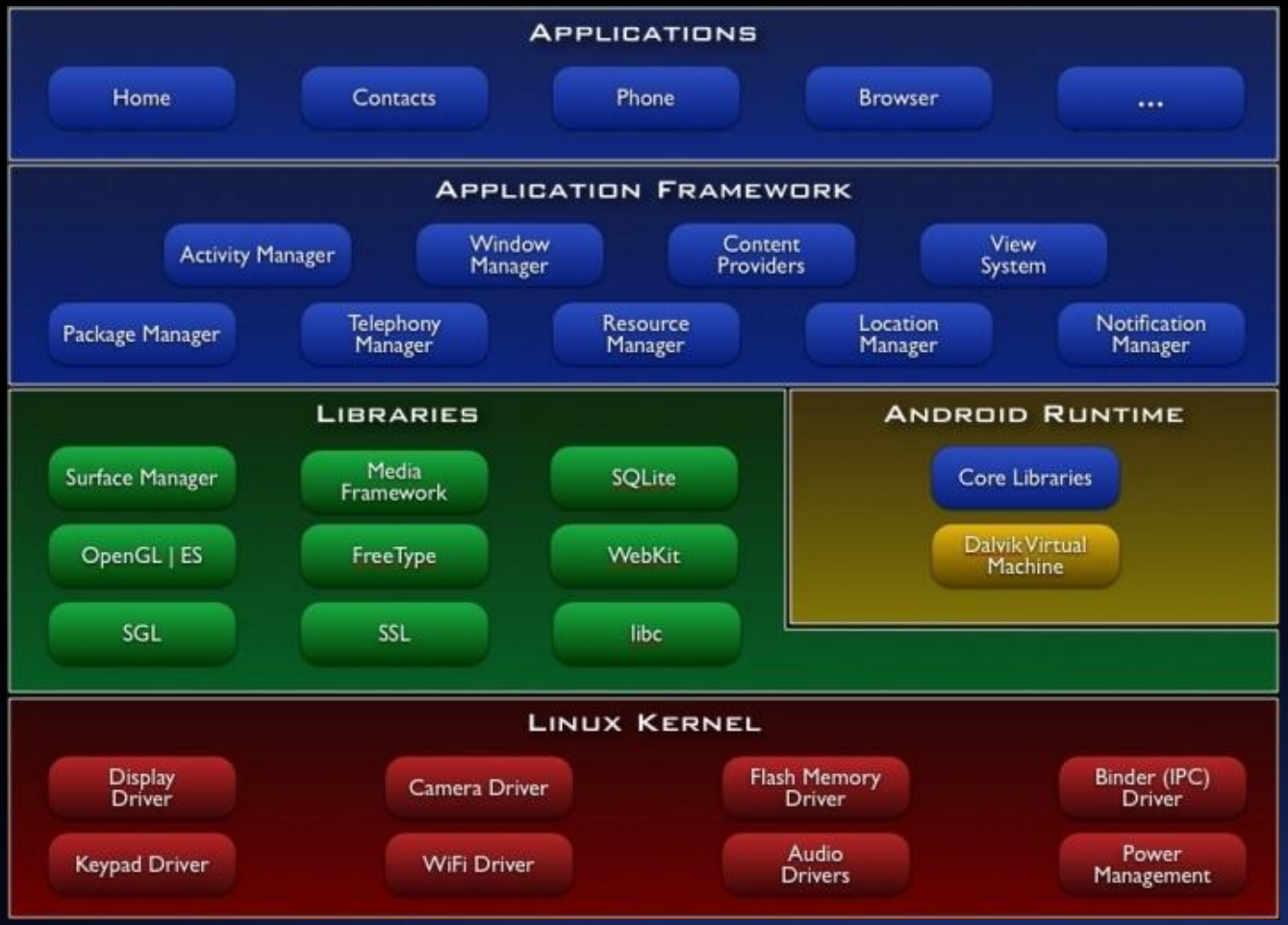
lica

2011. április 15., péntek 16:17 | aznap frissítve

A Google nyilvánosságra hozta, hogy mennyi alkalmazást töltöttek le eddig az androidos készülékekre. A tavalyi utolsó negyedévhez képest ötven százalékkal nőtt a letöltések száma és elérte a hárommilliárdot.

Azt is nyilvánosságra hozták, hogy naponta 350 ezer andoridos készüléket aktiválnak. A cég eddig nem hozta nyilvánosságra ezeket az adatokat.

Android 101


Applications
Home
Contacts
Phone
Browser
...
Application Framework
Activity Manager
Window Manager
Content Providers
View System
Package Manager
Telephony Manager
Resource Manager
Location Manager
Notification Manager
Libraries
Surface Manager
Media Framework
SQLite
OpenGL | ES
FreeType
WebKit
SGL
SSL
libc
Android Runtime
Core Libraries
Dalvik Virtual Machine
Linux Kernel
Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Kernel biztonság

Dalvik VM biztonság

Alkalmazás biztonság

- Telepítéskor
  - Egyedi UID+GID: kernel szeparál (?)
  - Jogosultságokat kér a felhasználótól
  - Saját könyvtár: /data/data/hu.csomag.nev

Skype

DEMO

Android Market működése

- Tévhit: keres → elfogad → letölt → telepít
- Valóság:
  - ProtoBuf API kérés Android Market felé
  - Háttérben futó GTalkService kap egy kérést a Google felől csomagtelepítésre és végrehajtja
  - Что вы видите на картинке?
    - ProtoBuf kérés spoofolás
    - GTalkService MITM
    - Szerver felőli hack: XSS, pwn

AppHacking: blackbox mód

Első lépések (DEMO)

- Néhány próbakeresést végzünk
- Elsőre látszik: semmi titkosítás

Address A	Port A	Address B	Port B	Packets	Bytes
android .hu	55662	.hu	http	10	1 412
android .hu	53631	.hu	http	10	1 652
android .hu	40276	.hu	http	10	1 496
android .hu	55756	.hu	http	10	1 690
android .hu	53679	.hu	http	11	1 282
android .hu	48279	.net	http	10	1 339
android .hu	33394	.hu	http	9	1 436
android .hu	33937	.hu	http	10	1 690
android .hu	53978	.net	http	10	1 340
android .hu	56630	.hu	http	11	1 282
android .hu	36584	hu	http	13	2 604

Protokollanalízis (DEMO)

Az ígéretes TCP folyamokat követve némi intuícióval gyorsan megfejthető a dolog.

```
POST /[redacted].server.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 227
Host: api.[redacted].hu
Connection: Keep-Alive

auth=MTA6ZGZrbDIzNG9tdm0yMw%3D%3D&encoder=json&charset=utf-8&request=%7B%22me
3A%223-667574C3A172%22%2C+%22page%22%3A%221%22%2C+%22limit%22%3A%2220%22%7D%7
Date: Mon, 11 Apr 2011 11:10:11 GMT
Server: Apache
W: w41
Content-Length: 786
Keep-Alive: timeout=3, max=100
Connection: Keep-Alive
Content-Type: text/html

{"success":true,"result":{"pages":1,"records":"2","searchID":"3-667574C3A172"
```

Ingyen API (DEMO)

Python a barátunk: JSON+Base64+HTTP

```
$ python req.py futár
date_to: 2011-04-22 00:00:00
position: Office manager
cities: Budapest
company: Kirowski Zrt.
id: 394692
```

Spoofing (DEMO + BYOP)

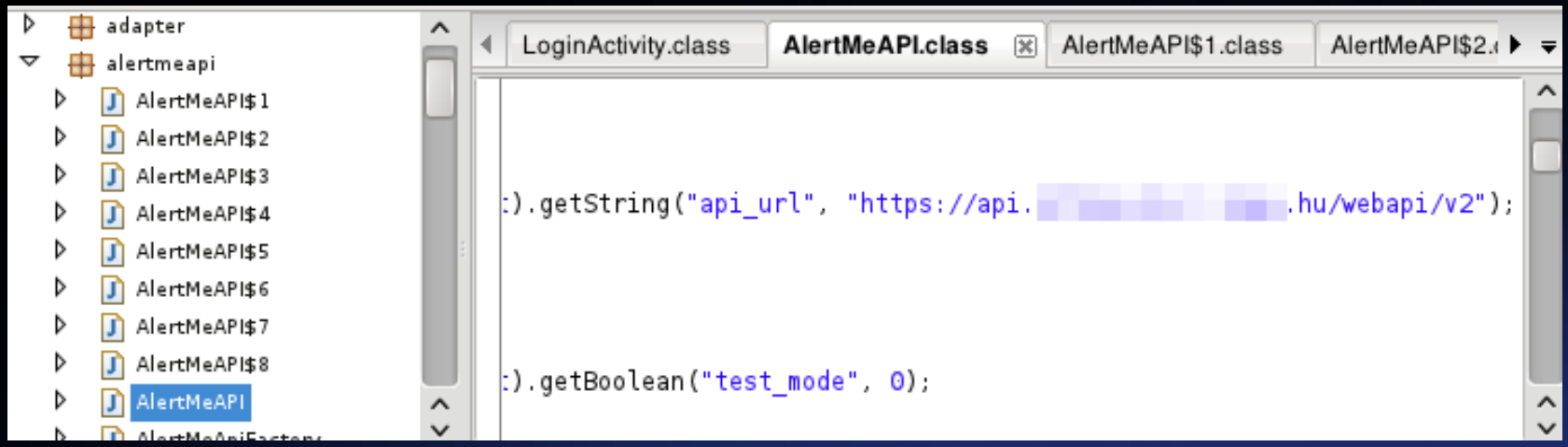
- „További alkalmazások” ablak: sima JSON
- WiFi esetén triviális
  - `iptables REDIRECT`
  - SQUID proxy
  - Python rewrite script
- Felhasználó
  - Jobban bízik az innen nyíló linkekben
  - Puszta érdeklődésből is rákattint

AppHacking: kódanalízis

- Tévhit: amit a binárisba teszünk, az titkos
- Valóság: majdnem tökéletes Java kód
- Eszközkészlet:
  - Wireshark/TCPdump: URL megszerzése
  - wget: APK letöltése + unzip: kicsomagolás
  - dex2jar: classes.dex JAR fájllá alakítása
  - JD-GUI: gyakorlatilag Java forráskód
  - A fentiek mind ingyenesen letölthetők

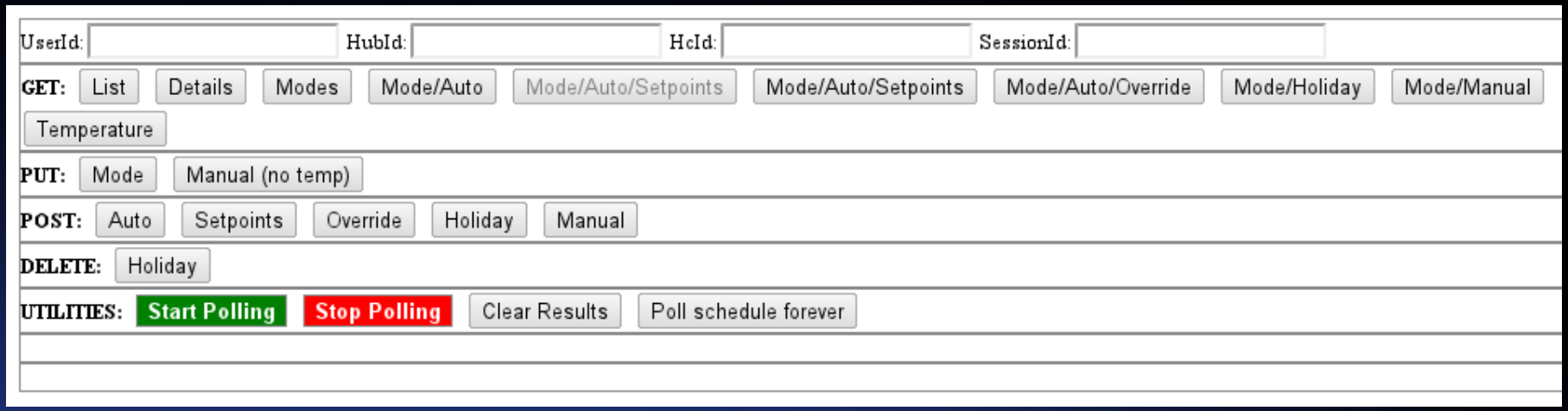
Kódanalízis kezdőknek (DEMO)

- Esettanulmány: otthonvédelmi rendszer
- HTTPS kommunikáció, tisztességes PKI
- „Talk is cheap, show me the code”
  - Előző dián látottak alapján kód visszafejthető



Kedves API (DEMO)

- Adott tehát egy URL
- Böngészővel és egy kis kreativitással érdekes felületek hozhatók elő…
- Ezeknek biztos elérhetőnek kell lenniük?



Összefoglalás

@p0sixninja
Joshua Hill

Looks like Apple added ASLR into iOS 4.3. This should make things more fun!!!

26 Jan via Twitter for iPhone

ESET Smart Security kérdés

Milyen kernel adja az Android alapját?

A: BSD

B: Linux

C: Windows CE

D: Windows NT

Köszönöm a figyelmet!