Android Hax

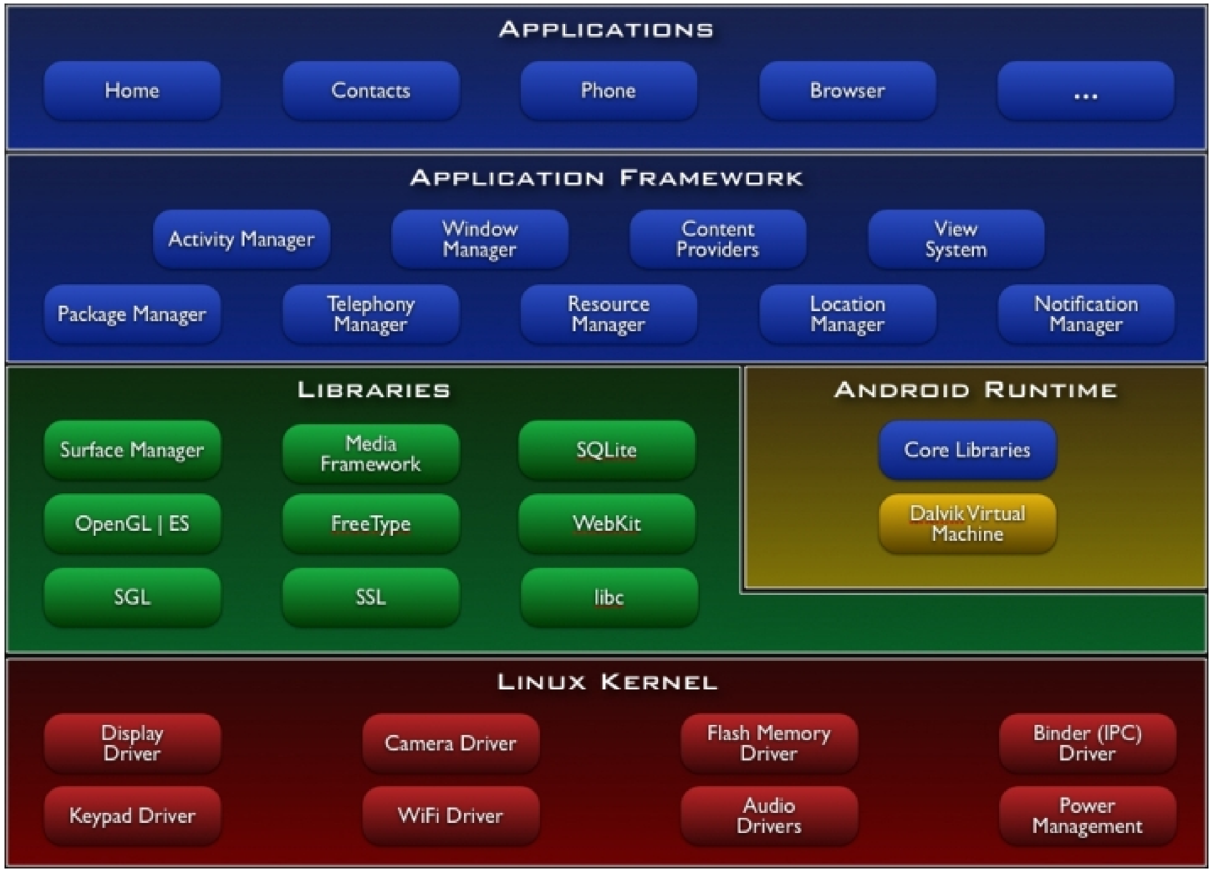
Jon Oberheide
jon@oberheide.org

Agenda

- **Android Security Overview**
- Market and the Mystical GTalkService
- The RootStrap PDP
- Wrap-Up / Q&A

Android Overview

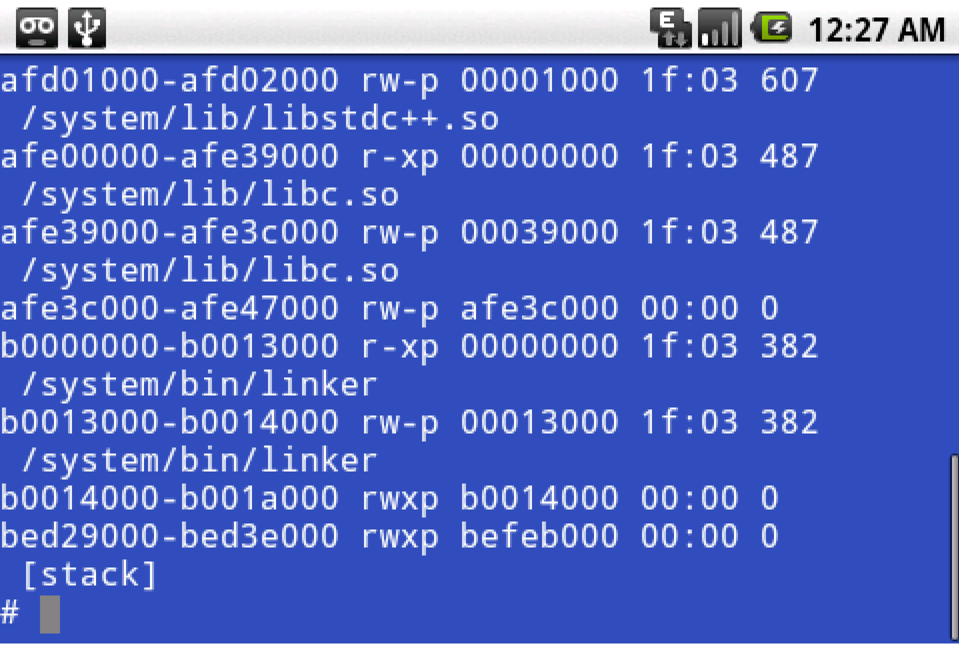
- Base platform
  - ARM core
  - Linux 2.6.3x kernel
- Native Libraries
  - libc, WebKit, etc
- Dalvik VM
  - Register-based VM
  - Runs dex bytecode
- Applications
  - Developed in Java
  - Runs on Dalvik VM
  - Linux process 1-1



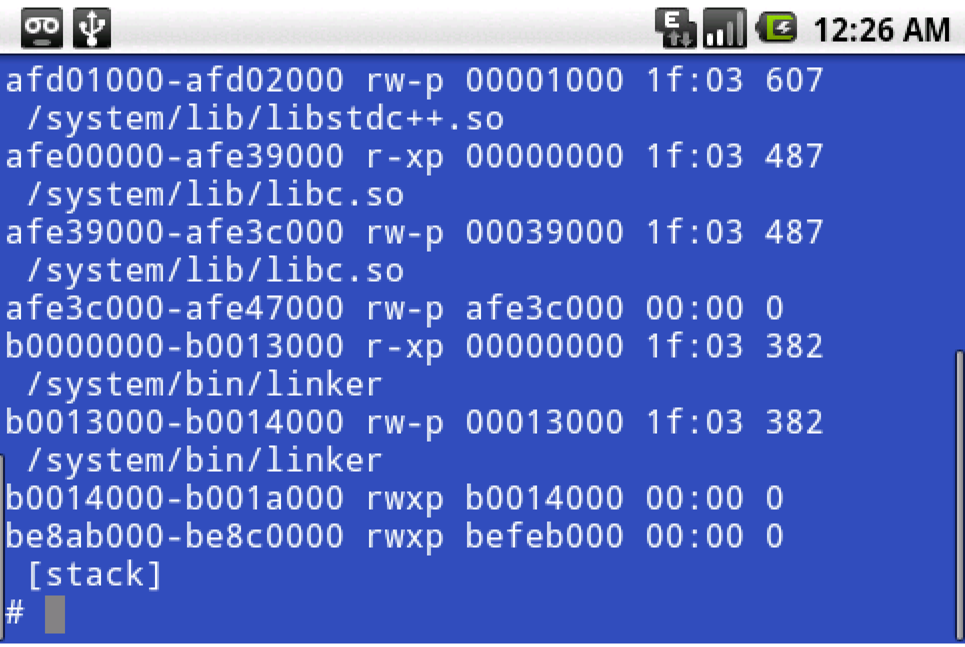
Hardware Features

- ARM11 TrustZone?
  - Unused!
- ARM11 Jazelle JVM?
  - Unused!
- ARMv6 eXecute-Never (XN)?
  - Unused!

Linux Environment

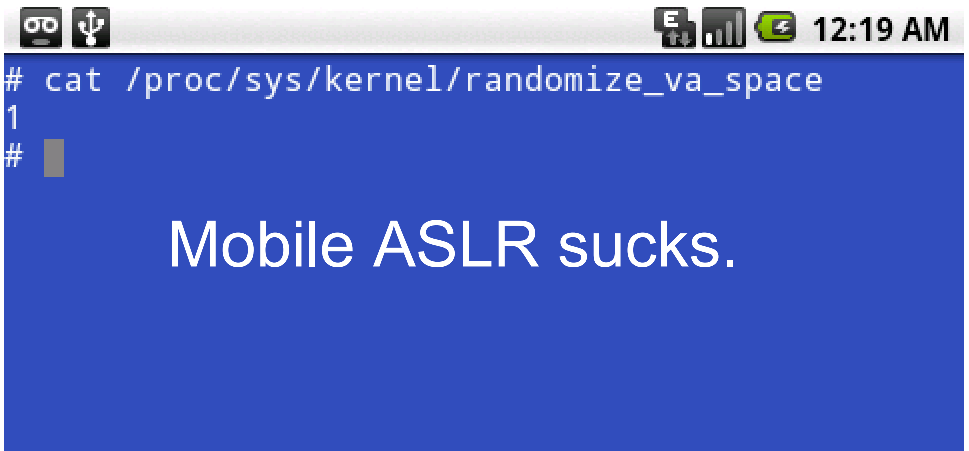


```
afd01000-afd02000 rw-p 00001000 1f:03 607
 /system/lib/libstdc++.so
afe00000-afe39000 r-xp 00000000 1f:03 487
 /system/lib/libc.so
afe39000-afe3c000 rw-p 00039000 1f:03 487
 /system/lib/libc.so
afe3c000-afe47000 rw-p afe3c000 00:00 0
b0000000-b0013000 r-xp 00000000 1f:03 382
 /system/bin/linker
b0013000-b0014000 rw-p 00013000 1f:03 382
 /system/bin/linker
b0014000-b001a000 rwxp b0014000 00:00 0
bed29000-bed3e000 rwxp befeb000 00:00 0
 [stack]
#
```



```
afd01000-afd02000 rw-p 00001000 1f:03 607
 /system/lib/libstdc++.so
afe00000-afe39000 r-xp 00000000 1f:03 487
 /system/lib/libc.so
afe39000-afe3c000 rw-p 00039000 1f:03 487
 /system/lib/libc.so
afe3c000-afe47000 rw-p afe3c000 00:00 0
b0000000-b0013000 r-xp 00000000 1f:03 382
 /system/bin/linker
b0013000-b0014000 rw-p 00013000 1f:03 382
 /system/bin/linker
b0014000-b001a000 rwxp b0014000 00:00 0
be8ab000-be8c0000 rwxp befeb000 00:00 0
 [stack]
#
```

Executable stack/heap!



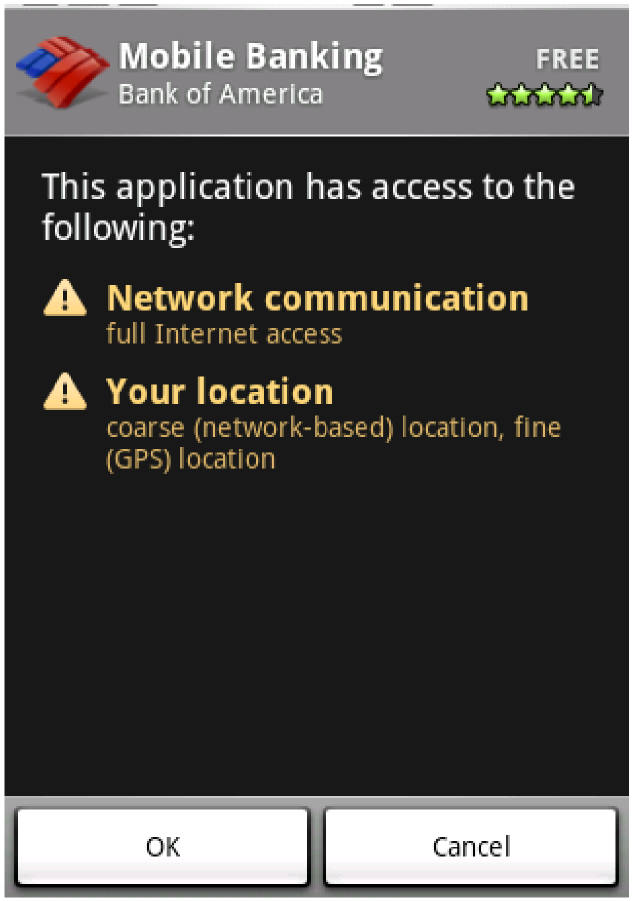
```
# cat /proc/sys/kernel/randomize_va_space
1
#
```

Mobile ASLR sucks.

Non-randomized mmap/brk!

Permission-Based Model

- Apps explicitly request pre-defined permissions
- Examples:
  - Cellular: calls, SMS, MMS
  - Network, bluetooth, wifi
  - Hardware settings: vibrate, backlight, etc
  - Location: coarse/fine
  - App data: contacts, calendar


Mobile Banking
Bank of America
FREE

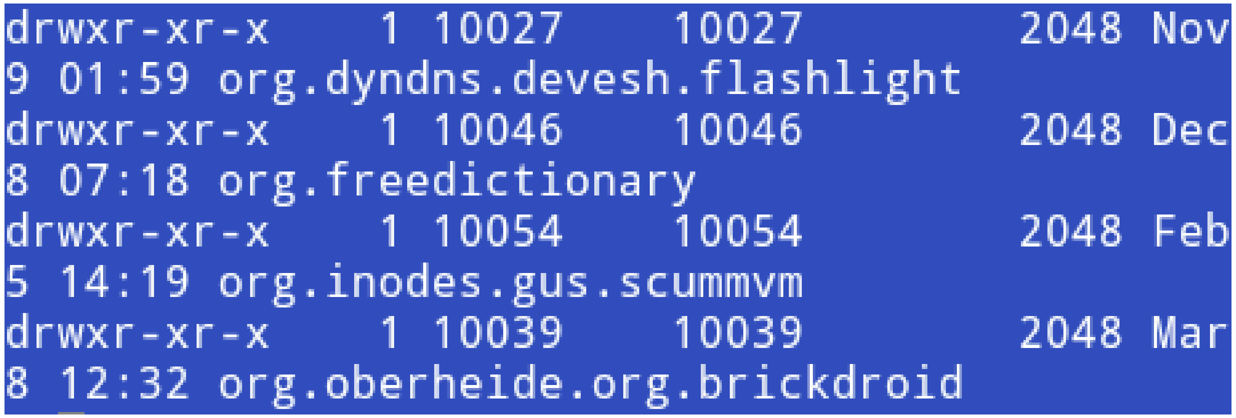
This application has access to the following:

Network communication
full Internet access

Your location
coarse (network-based) location, fine (GPS) location

App Sandboxing

- “Sandboxed” by standard UNIX uid/gid
  - generated unique per app at install



```
drwxr-xr-x    1 10027    10027          2048 Nov
9 01:59 org.dyndns.devesh.flashlight
drwxr-xr-x    1 10046    10046          2048 Dec
8 07:18 org.freedictionary
drwxr-xr-x    1 10054    10054          2048 Feb
5 14:19 org.inodes.gus.scummvm
drwxr-xr-x    1 10039    10039          2048 Mar
8 12:32 org.oberheide.org.brickdroid
```

- High-level permissions restricted by Android runtime framework

App Distribution

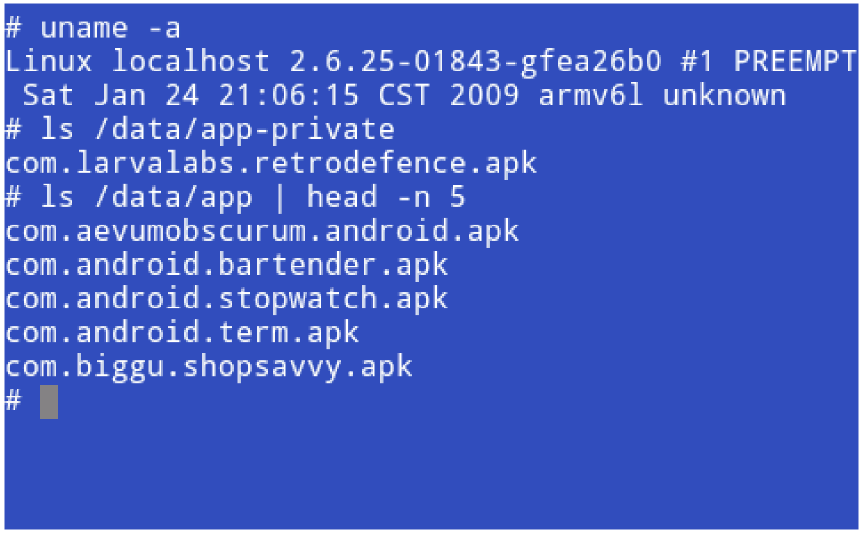
- Application signing
  - No CAs
  - Self-signed by developers
- Android Market
  - $25 signup, anyone can publish
  - Anonymous sign-up possible

App Piracy

- Trivial copy protection provided by market

Off?

- Apps stored in /data/app/
- Accessible to users



```
# uname -a
Linux localhost 2.6.25-01843-gfea26b0 #1 PREEMPT
 Sat Jan 24 21:06:15 CST 2009 armv6l unknown
# ls /data/app-private
com.larvalabs.retrodefence.apk
# ls /data/app | head -n 5
com.aevumobscurum.android.apk
com.android.bartender.apk
com.android.stopwatch.apk
com.android.term.apk
com.biggu.shopsavvy.apk
# 
```

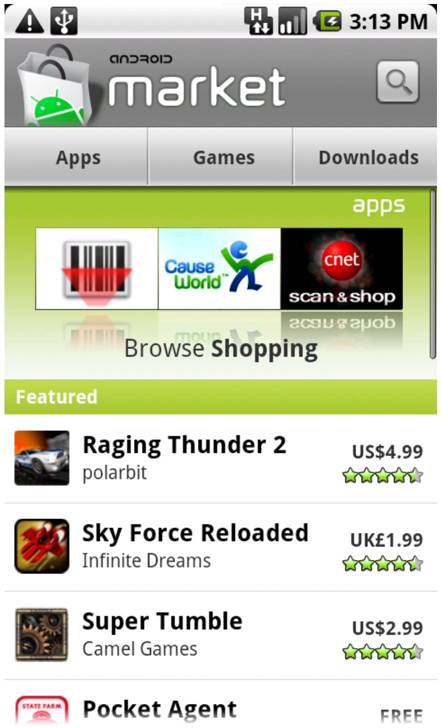
On?

- Apps stored in /data/app-private/
- Only accessible if rooted phone

Agenda

- Android Security Overview
- **Market and the Mystical GTalkService**
- The RootStrap PDP
- Wrap-Up / Q&A

Perceived Market Flow


3:13 PM

android market

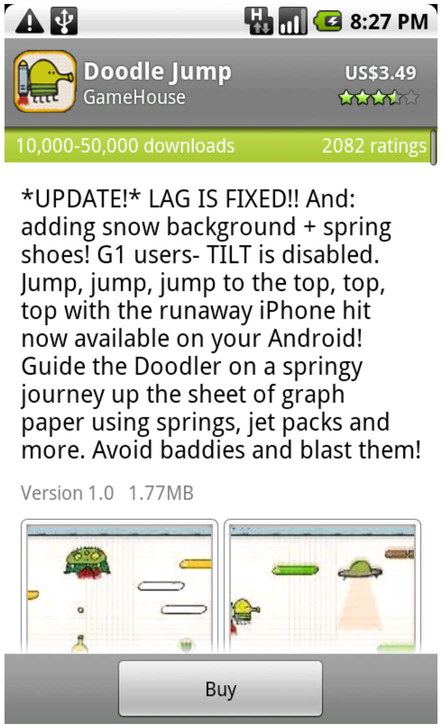
Apps | Games | Downloads

apps

Browse Shopping

Featured

Raging Thunder 2	polarbit	US$4.99
Sky Force Reloaded	Infinite Dreams	UK£1.99
Super Tumble	Camel Games	US$2.99
Pocket Agent		FREE


8:27 PM

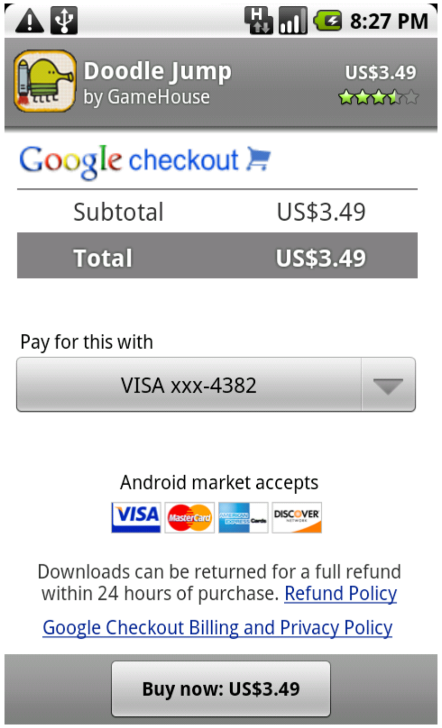
Doodle Jump
GameHouse
US$3.49

10,000-50,000 downloads 2082 ratings

UPDATE! LAG IS FIXED!! And: adding snow background + spring shoes! G1 users- TILT is disabled. Jump, jump, jump to the top, top, top with the runaway iPhone hit now available on your Android! Guide the Doodler on a springy journey up the sheet of graph paper using springs, jet packs and more. Avoid baddies and blast them!

Version 1.0 1.77MB

Buy


8:27 PM

Doodle Jump
by GameHouse
US$3.49

Google checkout

Subtotal	US$3.49
Total	US$3.49

Pay for this with

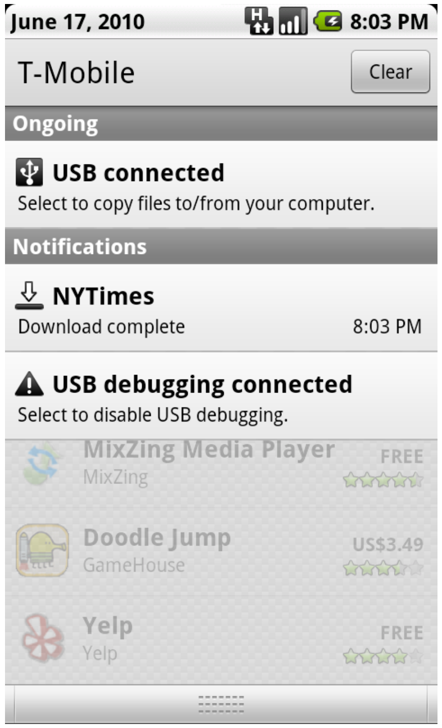
VISA xxx-4382

Android market accepts

Downloads can be returned for a full refund within 24 hours of purchase. Refund Policy

Google Checkout Billing and Privacy Policy

Buy now: US$3.49


June 17, 2010 8:03 PM

T-Mobile Clear

Ongoing

USB connected
Select to copy files to/from your computer.

Notifications

NYTimes
Download complete 8:03 PM

USB debugging connected
Select to disable USB debugging.

MixZing Media Player FREE
MixZing

Doodle Jump US$3.49
GameHouse

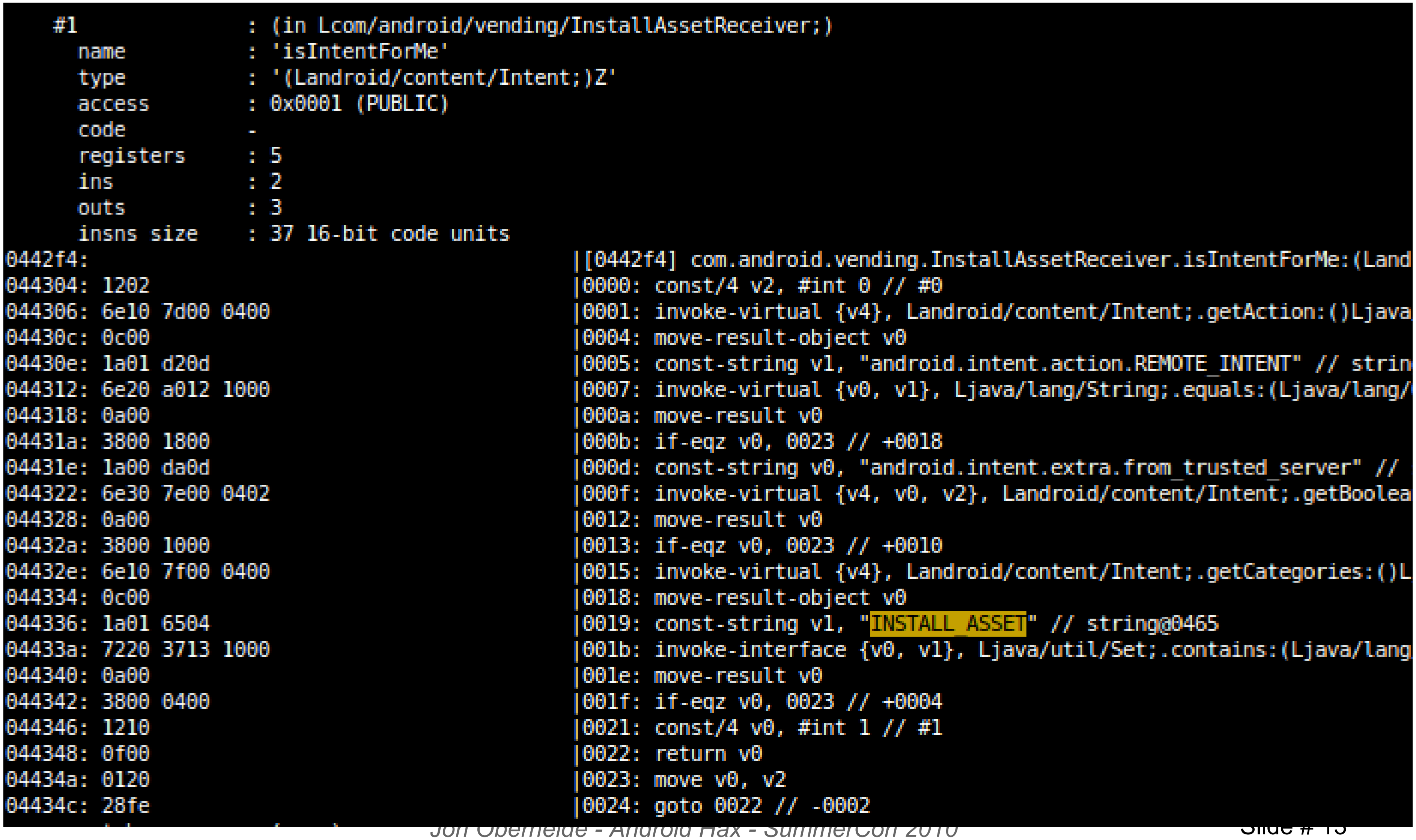
Yelp FREE
Yelp

BROWSE INSTALL PAY INSTALLED!

ACTUAL Market Flow

- Google is a sneaky panda!
  - You don't actually download / install the app through the market application
- When you click install in market app
  - Google servers push an out-of-band message down to you via persistent data connection
  - Triggers INSTALL_ASSET intent to start install
  - Intent handler fetches APK and installs

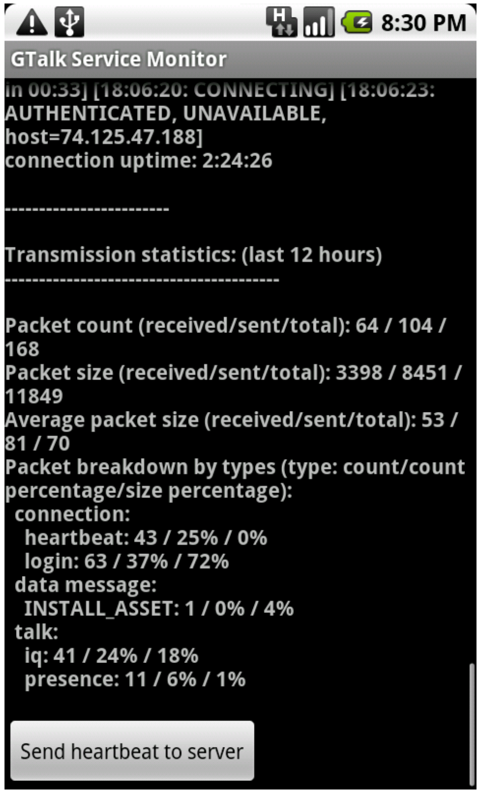
Dex Bytecode RE



```
    #1              : (in Lcom/android/vending/InstallAssetReceiver;)
      name          : 'isIntentForMe'
      type          : '(Landroid/content/Intent;)Z'
      access        : 0x0001 (PUBLIC)
      code          -
      registers     : 5
      ins           : 2
      outs          : 3
      insns size    : 37 16-bit code units
0442f4:                                        |[0442f4] com.android.vending.InstallAssetReceiver.isIntentForMe:(Land
044304: 1202                                   |0000: const/4 v2, #int 0 // #0
044306: 6e10 7d00 0400                         |0001: invoke-virtual {v4}, Landroid/content/Intent;.getAction:()Ljava
04430c: 0c00                                   |0004: move-result-object v0
04430e: 1a01 d20d                              |0005: const-string v1, "android.intent.action.REMOTE_INTENT" // strin
044312: 6e20 a012 1000                         |0007: invoke-virtual {v0, v1}, Ljava/lang/String;.equals:(Ljava/lang/
044318: 0a00                                   |000a: move-result v0
04431a: 3800 1800                              |000b: if-eqz v0, 0023 // +0018
04431e: 1a00 da0d                              |000d: const-string v0, "android.intent.extra.from_trusted_server" //
044322: 6e30 7e00 0402                         |000f: invoke-virtual {v4, v0, v2}, Landroid/content/Intent;.getBoolea
044328: 0a00                                   |0012: move-result v0
04432a: 3800 1000                              |0013: if-eqz v0, 0023 // +0010
04432e: 6e10 7f00 0400                         |0015: invoke-virtual {v4}, Landroid/content/Intent;.getCategories:()L
044334: 0c00                                   |0018: move-result-object v0
044336: 1a01 6504                              |0019: const-string v1, "INSTALL_ASSET" // string@0465
04433a: 7220 3713 1000                         |001b: invoke-interface {v0, v1}, Ljava/util/Set;.contains:(Ljava/lang
044340: 0a00                                   |001e: move-result v0
044342: 3800 0400                              |001f: if-eqz v0, 0023 // +0004
044346: 1210                                   |0021: const/4 v0, #int 1 // #1
044348: 0f00                                   |0022: return v0
04434a: 0120                                   |0023: move v0, v2
04434c: 28fe                                   |0024: goto 0022 // -0002
```

GTalkService Connection

- Persistent data connection
  - Speaks XMPP
  - Same connection now used for C2DM push service
- It's SSL, but...
- If you MITM or C2DM spoof
  - Remote intent / app install
- If you pop GTalkService servers
  - Push down code to all Android phones in the world?



```
in 00:33] [18:06:20: CONNECTING] [18:06:23:
AUTHENTICATED, UNAVAILABLE,
host=74.125.47.188]
connection uptime: 2:24:26

-----------------------

Transmission statistics: (last 12 hours)
---------------------------------------

Packet count (received/sent/total): 64 / 104 /
168
Packet size (received/sent/total): 3398 / 8451 /
11849
Average packet size (received/sent/total): 53 /
81 / 70
Packet breakdown by types (type: count/count
percentage/size percentage):
 connection:
  heartbeat: 43 / 25% / 0%
  login: 63 / 37% / 72%
 data message:
  INSTALL_ASSET: 1 / 0% / 4%
 talk:
  iq: 41 / 24% / 18%
  presence: 11 / 6% / 1%
```

Disclaimer

[redacted]

- Useful though if you want to fetch a large amount of apps and do some fuzzing, analysis, whatever
  - I've got a repo of ~10k apps

Agenda

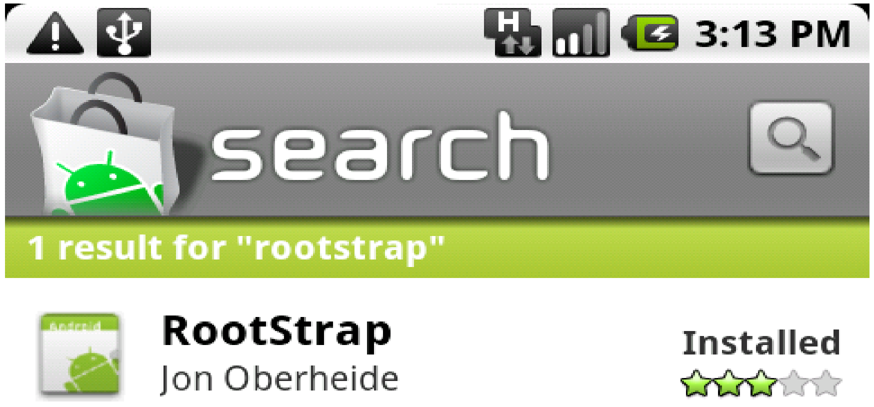
- Android Security Overview
- Market and the Mystical GTalkService
- **The RootStrap PDP**
- Wrap-Up / Q&A

Android Native Code

- Dalvik VM != sandbox
  - Not limited to executing dex bytecode
  - Can pop out of the VM to execute native code
- Linux kernel = swiss cheese
  - Wonderful attack surface
  - Any 3rd party app can root your phone by exploiting a kernel vulnerability via native code
- Native code packaged within APKs
  - But why limit execution of native code to build-time packaged modules?

RootStrap

- Enter, RootStrap
  - Silent runtime fetching and execution of remote ARM payloads
  - Not really a bot..more of a general purpose distributed computing platform ;-)
- Currently available in Android market

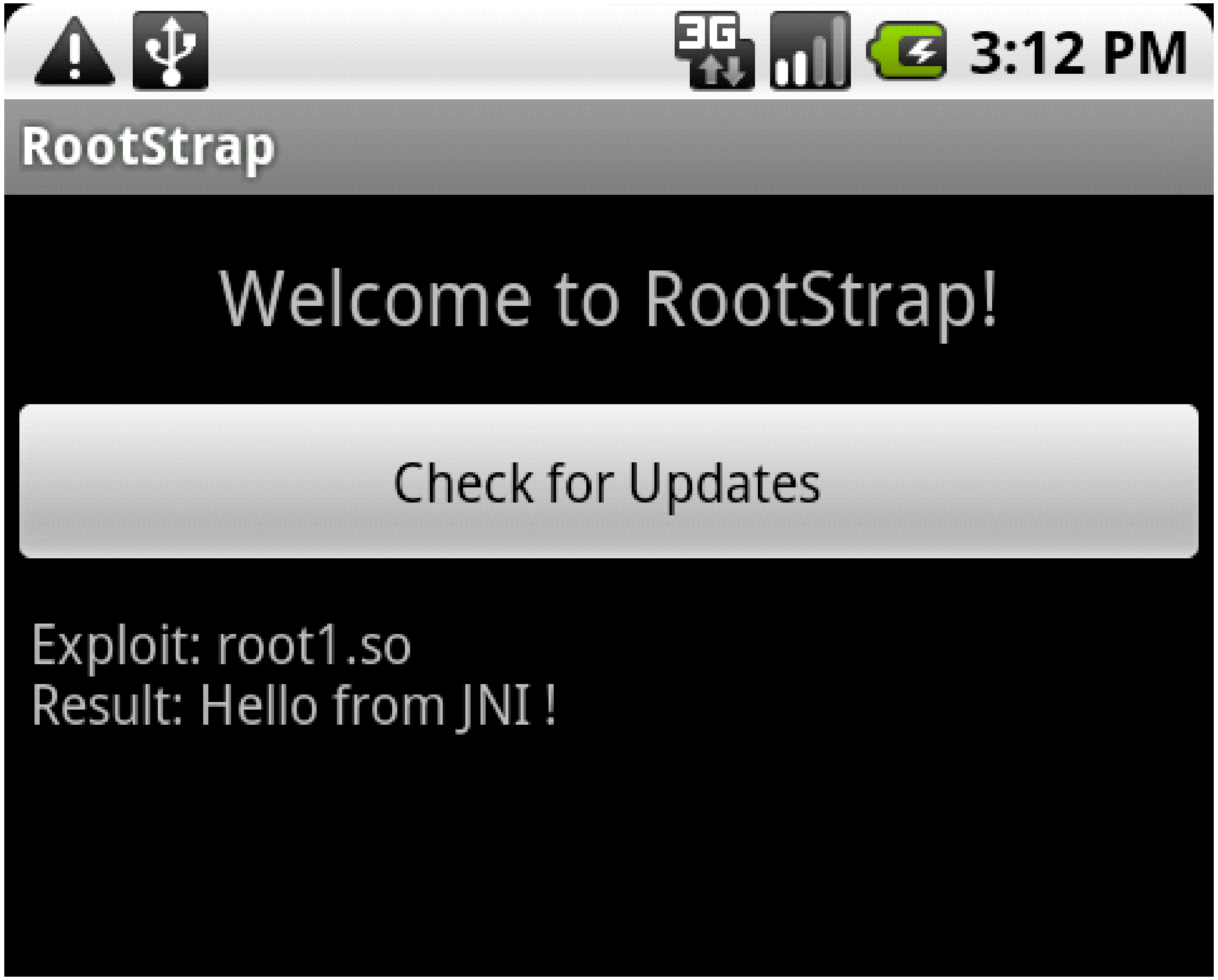

3:13 PM

search

1 result for "rootstrap"

RootStrap
Jon Oberheide
Installed

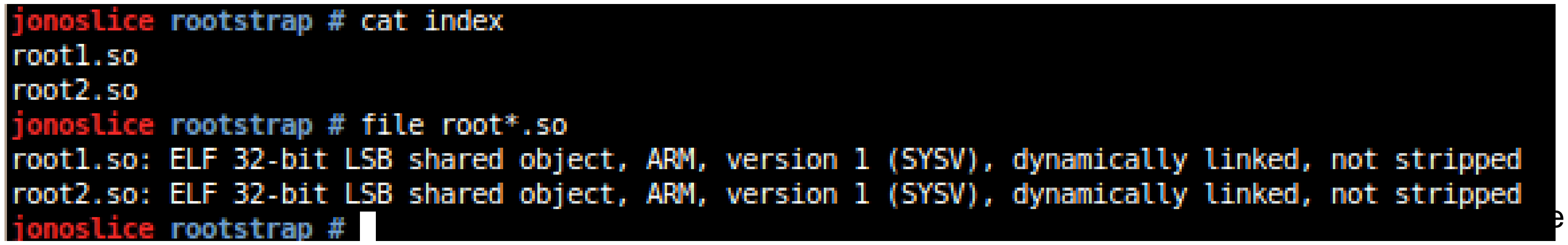
RootStrap Example



```
Exploit: root1.so
Result: Hello from JNI !
```

Native ARM Code Delivery

- Fetch index file
  - Lists available exploits and module names
  - http://jon.oberheide.org/rootstrap/index
- Yank down ARM modules
  - Dumped to Android app private storage
  - eg. /data/data/org.rootstrap/files, not ./libs
- Load via JNI and execute each payload
  - System.load(".../files/root1.so");
  - result = root1();



```
jonoslice rootstrap # cat index
root1.so
root2.so
jonoslice rootstrap # file root*.so
root1.so: ELF 32-bit LSB shared object, ARM, version 1 (SYSV), dynamically linked, not stripped
root2.so: ELF 32-bit LSB shared object, ARM, version 1 (SYSV), dynamically linked, not stripped
jonoslice rootstrap #
```

How to Build a Mobile Botnet

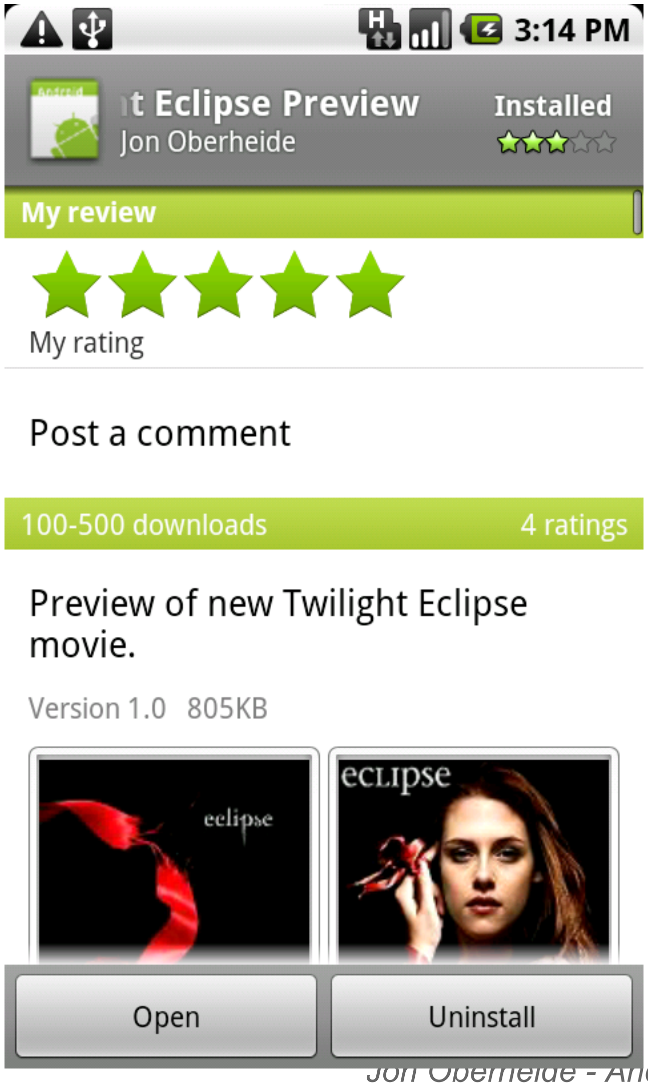
- Build some fun legit-looking games / apps
  - Include RootStrap functionality
  - Periodically phone home to check for new payloads
- As soon as new kernel vuln discovered, push out exploit payload
  - Before providers push out OTA patch
  - Trivial to win that race, slow OTA updates
- Rootkit a bunch of phones!

A Wolf in Vampire's Clothing?

- RootStrap app is boring and not sneaky
  - No one would intentionally download it
  - Need something legit looking to get a significant install base

- How about an RootStrap-enabled app claiming to be a preview for the upcoming Twilight Eclipse movie?!?

Fake Twilight Eclipse App



3:14 PM

ıt Eclipse Preview

Jon Oberheide

Installed

My review

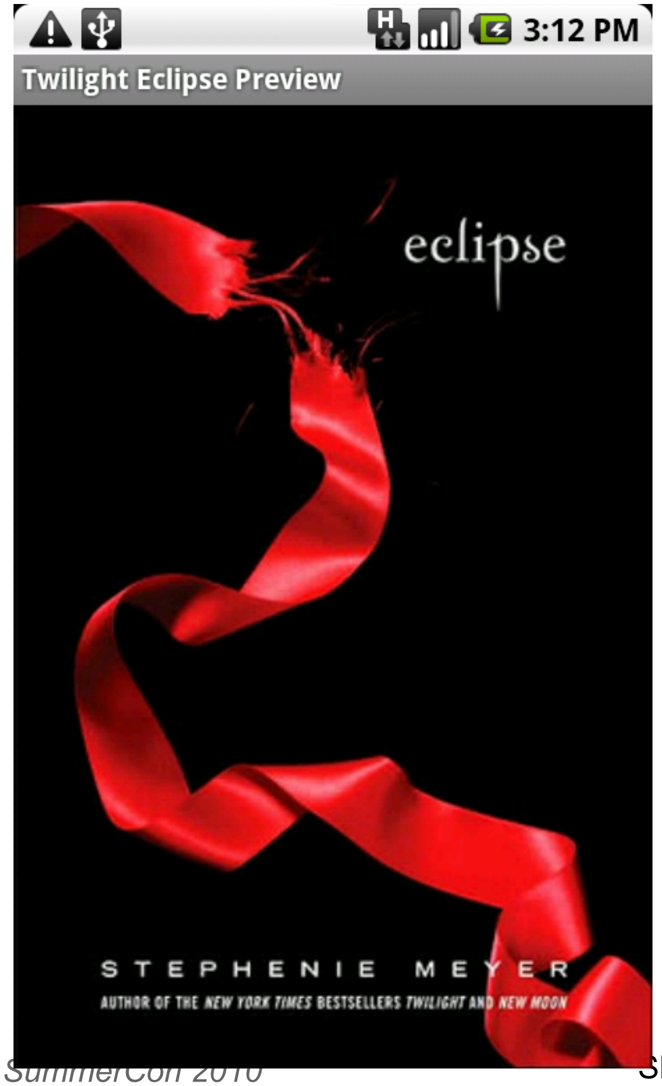
My rating

Post a comment

100-500 downloads 4 ratings

Preview of new Twilight Eclipse movie.

Version 1.0 805KB

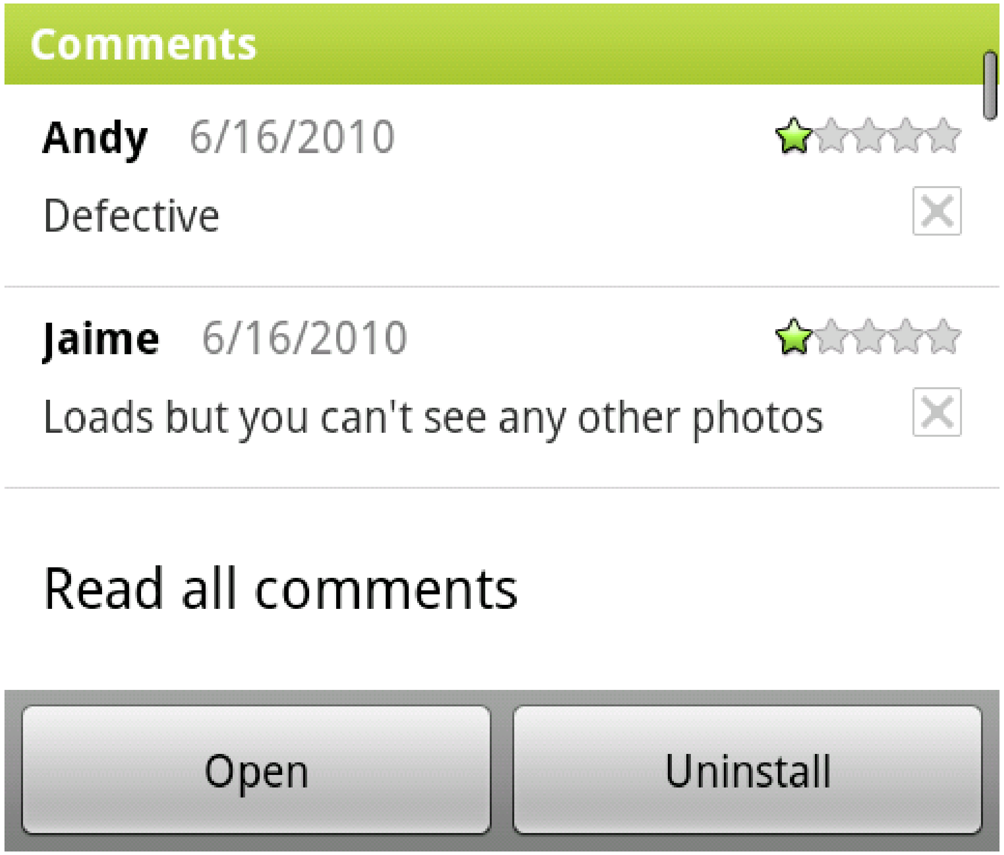


3:12 PM

Twilight Eclipse Preview

eclipse
STEPHENIE MEYER
AUTHOR OF THE NEW YORK TIMES BESTSELLERS TWILIGHT AND NEW MOON

Andy and Jaime Don't Like It :-(



Comments

Andy 6/16/2010

Defective

Jaime 6/16/2010

Loads but you can't see any other photos

- Still, 200+ downloads in under 24 hours
- With a legit-looking app/game, you could collect quite an install base for RootStrap

RootStrap Payloads

- sock_sendpage NULL deref
  - Old, but still works on some phones
  - fork/execve from JNI is a bit wacky
- Supervisor App vulns?
  - su without approval
  - “jailbroken” phone is less safe
- Meterpretux?

Agenda

- Android Security Overview
- Market and the Mystical GTalkService
- The RootStrap PDP
- **Wrap-Up / Q&A**

Wrap-Up

[redacted]

- Native code support sucks.
  - Not so easy to take away
  - Build-time signing / loader verification?
- Android homework
  - Poke at the GTalkService code paths
  - Write some RootStrap payloads
  - Port to other platforms?
  - Fuzz the new Android Acrobat app!

Q&A

QUESTIONS?

Jon Oberheide

@jonoberheide

jon@oberheide.org

http://jon.oberheide.org