Android Hax

Jon Oberheide
jon@oberheide.org
Agenda

• Android Security Overview
• Market and the Mystical GTalkService
• The Root Strap 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!
Mobile ASLR sucks.
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
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

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

*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

Downloads can be returned for a full refund within 24 hours of purchase. Refund Policy
Google Checkout Billing and Privacy Policy

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: 044304: 1202
044306: 6e10 7d00 0400
04430c: 0c00
04430e: 1a01 d20d
044312: 6e20 a012 1000
044318: 0a00
04431a: 3800 1800
04431e: 1a00 da0d
044322: 6e30 7e00 0402
044328: 0a00
04432a: 3800 1000
04432e: 6e10 7f00 0400
044334: 0c00
044336: 1a01 6504
04433a: 7220 3713 1000
044340: 0a00
044342: 3800 0400
044346: 1210
044348: 0f00
04434a: 0120
04434c: 28fe

0442f4] com.android.vending.InstallAssetReceiver.isIntentForMe:(Landroid/content/Intent;)Z
0000: const/4 v2, #int 0 // #0
0001: invoke-virtual {v4}, Landroid/content/Intent;.getAction():Ljava/lang/String;
0004: move-result-object v0
0005: const-string v1, "android.intent.action.REMOTE_INTENT" // string@0x0465
0007: invoke-virtual {v0, v1}, Ljava/lang/String;.equals:(Ljava/lang/
000a: move-result v0
000b: if-eqz v0, 0023 // +0018
000d: const-string v0, "android.intent.extra.from_trusted_server" // string@0x0465
000f: invoke-virtual {v4, v0, v2}, Landroid/content/Intent;.getBoolean;
0012: move-result v0
0013: if-eqz v0, 0023 // +0010
0015: invoke-virtual {v4}, Landroid/content/Intent;.getCategories():Ljava
0018: move-result-object v0
0019: const-string v1, "INSTALL ASSET" // string@0x0465
001b: invoke-interface {v0, v1}, Ljava/util/Set;.contains:(Ljava/lang/
001e: move-result v0
001f: if-eqz v0, 0023 // +0004
0021: const/4 v0, #int 1 // #1
0022: return v0
0023: move v0, v2
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?
Disclaimer

• 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 ;-)
RootStrap Example

Welcome to RootStrap!

Check for Updates

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();
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?

• Root Strap 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 Root Strap-enabled app claiming to be a preview for the upcoming Twilight Eclipse movie?!?
Fake Twilight Eclipse App

Post a comment

100-500 downloads  4 ratings

Preview of new Twilight Eclipse movie.

Version 1.0  805KB
Andy and Jaime Don't Like It :-(

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

Comments

<table>
<thead>
<tr>
<th>Andy</th>
<th>6/16/2010</th>
<th>🌟🌟🌟🌟</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defective</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Jaime</th>
<th>6/16/2010</th>
<th>🌟🌟🌟🌟</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loads but you can't see any other photos</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

• 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!
QUESTIONS?

Jon Oberheide
@jonoberheide
jon@oberheide.org
http://jon.oberheide.org