Mobile apps doubleheader: BADASS Angry Birds

From 6 weeks to 6 minutes: protocols exploitation in a rapidly changing world

Exploring and Exploiting Leaky Mobile Apps with BADASS

GTE/GCHQ

GA5A/CSEC

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
Coming up…

1) BADASS - From 6 weeks to 6 minutes: protocols exploitation in a rapidly changing world

2) We Know How Bad You Are At “Angry Birds”: Exploring and Exploiting Leaky Mobile Apps with BADASS (OtH)
BADASS

- Protocols Exploitation at GCHQ
- Mobile Applications – a challenge
- BADASS - BEGAL Automated Deployment And Survey System
- UNIQUELY CHALLENGED – Rapid deployment
- SEM – more complex extractions
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
New TDI Process 2010

VOB
Datastore (x 2!)
BADASS
Matrix reports
Spreadsheets
Etc..
Mobile Applications – Some Stats

Jobs in GTE Task tracker

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
Why?

Many different platforms (iOS, Android, WP7, Blackberry)

App store business model – everyone is writing software

Much greater diversity of software
(Basket) Case Studies

GMM – 18 months from analysis to deployment

TDIs – typical time from rule completion to deployment ~ 3 months
Intro to BADASS

BEGAL Automated Development / Deployment
And Something Something

Protocols Analyst

Web Front End

Rules to TPS

Rules

Event SLRs

Rules

BEGAL AEG running on software PPF

BEGAL AEG running on hardware PPF

DB

PCAP Tester

HW Tester

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on or email
Produced an invalid result in the FKB pcap test, and testing has been suspended.

Deployment status: DEPLOYED

Deployment Progress (TPS):

Version definition:

```
< surveypRule>
  <ruleName>N_Googlemobilemaps-000e-Body</ruleName>
  <action>
    <actionType>EVENT</actionType>
    <eventFormat>PRESENCE</eventFormat>
    <eventLogicalDestination>presence</eventLogicalDestination>
    <presenceEventIdentifierType>N_Googlemobilemaps-000e-Body</presenceEventIdentifierType>
    <presenceEventSourceId>true</presenceEventSourceId>
    <presenceEventTIType>TDI</presenceEventTIType>
    <presenceEventGenerationType>MACHINE</presenceEventGenerationType>
  </action>
  <criterionSet>
    <criterion>
      <spiTasking>
        <selectorType>string</selectorType>
        <selector>gmi/imap</selector>
        <bitM12K true"/>       
        <position>-1</position>
        <protocolLayer>APPLICATION_LAYER</protocolLayer>
```
<table>
<thead>
<tr>
<th>Hexdump</th>
<th>ASCII</th>
</tr>
</thead>
</table>

**Network layer**; protocol=TCP srcport=50323 destport=80
0000: 4500 0177 8258 4000 4006 4859 0a40 add5 F..w.X8.8.HY.0...
0010: d155 e564 .u.d

**Transport layer**; srcport=50323 destport=80
0014: c493 0050 9a1d 405b 5638 0c5d 8018 7d7b ...F...[V...])x
0024: ab27 0000 0101 080a ffff c224 b680 c3b2 ............$....

**Application layer**
0024: 404f 5054 4c6f 6d69 6e64 6566 696c 6573 7435 7385 0000 0177 8258 4000 4006 4859 0a40 add5 F..w.X8.8.HY.0...
0034: 4500 0177 8258 4000 4006 4859 0a40 add5 F..w.X8.8.HY.0...
0044: 5454 3132 3a 5153 5a54 5f5a 5f5b 5c5d 8018 7d7b ...F...[V...])x
0054: 2c55 0000 0101 080a ffff c224 b680 c3b2 ............$....

**Keep-Alive**

---

**This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on email**
Things worth mentioning

- Testing – increased confidence in rules produced by GTE
- Training – can use web interface to educate, and to prevent common mistakes
- Deduping effort – knowledge of what has already been done
- Became corporate TDI repo through back door
- Devolved management of protocols – no one person has to oversee all of them
UNIQUELY CHALLENGED

BADASS (BEGAL TDI Rules)

10G

10G

10G

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
UNIQUELY CHALLENGED

Rules to Task

Rule Library

Show: All Rules

Filter:

Selected Rules -> Destinations

Add Rule to Selection

Remove Rule from Selection

Deploy to Corporate MVR?
One person has complete oversight of a technology from analysis to deployment – important for rapidly changing protocols.
SEM – the future

Developed by ICTR at GCHQ

Complex events - More than just TDIs

Social interactions

Geo

Network Events
Over to Marty…
Coming up…

• Quick Overview: Ads and Analytics in the Mobile Realm
• Ads (Mobclix, AdMob, Mydas)
• Analytics (Dataflurry)
• Updates to Android IDs
• Windows Phone 7 User and Device IDs
• Abusing BADASS for Fun and Profit
Ads and Analytics in the Mobile Realm

Q: Why bother looking at mobile ads and analytics?

A: Developers use them to make money!

Ads and analytics support the developer with:

- App Development
- User Experience
- App Marketing

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on...
Ads and Analytics in the Mobile Realm

Ads are used as a means of generating revenue for a developer

- Advertisers need information about the device/user to properly target ads
- Unlikely to see ads in an app that charges
- Many developers are releasing dual versions of apps: ad-supported and paid
Ads and Analytics in the Mobile Realm

Analytics are used as a means of generating usage metrics for a developer

• “Anonymous usage statistics”
• Present in both paid and free apps
• Developer is presented with aggregate data for an app
WSJ: Mobclix, the ad exchange, matches more than 25 ad networks with some 15,000 apps seeking advertisers. The Palo Alto, Calif., company collects phone IDs, encodes them (to obscure the number), and assigns them to interest categories based on what apps people download and how much time they spend using an app, among other factors. By tracking a phone's location, Mobclix also makes a "best guess" of where a person lives, says Mr. Gurbuxani, the Mobclix executive. Mobclix then matches that location with spending and demographic data from Nielsen Co.
GET /?p=android
&i={GUID}
&s=320x50 (ad size)
&av=1.4.2
&u={IMEI}
&andid={Android ID}
&v=2.3.0
&ct=null
&dm={Phone Name}
&hwdm={Phone HW Model}
&sv={OS Version}&ua={User-Agent}
&o=0&ap=0
&ll=51.903699%2C-2.078062
&l=en_GB HTTP/1.1
Cookie:
User-Agent: ...
Host: ads.mobclix.com
Connection: Keep-Alive
GET /?p={platform}
&i={GUID}
&s=320x50 (ad size)
&av=1.4.2
&u={IMEI}
&andid={Android ID}
&v=2.3.0
&ct=null
&dm={Phone Name}
&hwdm={Phone HW Model}
&sv={OS Version}
&ua={User-Agent}
&o=0
&ap=0
&ll=51.903699%2C-2.078062
&l=en GB HTTP/1.1
Cookie: User-Agent: ...
Host: ads.mobclix.com
Connection: Keep-Alive

Ads: Mobclix

- GET request indicates platform and the device identifier
  - the order of the p argument in the GET can vary between platforms
- Il is lat,long; not always present
- Uses multiple URLs for activities:
  - Ads: ads.mobclix.com
  - Analytics: data.mobclix.com/post/sendData
  - Feedback: data.mobclix.com/post/feedback
  - Config: data.mobclix.com/post/config

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on ___ or email ___.
Cross-Platform Ads: Mobclix

GET /?p={platform} &i={GUID} &s=320x50 (ad size) &av=1.4.2 &u={IMEI} &andid={Android ID} &v=2.3.0 &ct=null &dm={Phone Name} &hwdm={Phone HW Model} &sv={OS Version} &ua={User-Agent} &o=0 &ap=0 &ll=51.903699%2C-2.078062 &l=en_GB HTTP/1.1
Cookie: User-Agent: ...
Host: ads.mobclix.com
Connection: Keep-Alive

<table>
<thead>
<tr>
<th>Argument</th>
<th>iPhone</th>
<th>Android</th>
<th>WP7*</th>
</tr>
</thead>
<tbody>
<tr>
<td>{platform}</td>
<td>iphone</td>
<td>android</td>
<td>?</td>
</tr>
<tr>
<td>{u}</td>
<td>UDID</td>
<td>AndID, or IMEI when {andid} is set</td>
<td>?</td>
</tr>
<tr>
<td>{andid}</td>
<td>N/A</td>
<td>AndID</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*: WP7 Mobclix SDK still in beta
Cross-Platform Ads: AdMob

GET /p/i/e2/9b/e29b1e7503a5b24b3e693ece2c887173.png HTTP/1.1
Host: mm.admob.com
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; HW iPhone1,2; en_us) AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-20090617)
X-Admob-Isu: 7355c9d9f7d1033e0fe3ee13513366ad69170013
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: uuid=81a66cc2cf3f554e02f089c04d8d4fcb;
admobuu=48617727332748471264744376038126
Connection: keep-alive

The isu can appear both as an argument in a POST or in the X-ADMOB-ISU HTTP header extension. The value itself is 32-40 bytes long.

Hosts using this value consistently: r.admob.com, mm.admob.com, mmv.admob.com, and a.admob.com
Cross-Platform Ads: AdMob

GET /p/i/e2/9b/e29b1e7503a5b24b3e693ece2c887173.png HTTP/1.1
Host: mm.admob.com
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; HW iPhone1,2; en_us) AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-20090617)
X-Admob-Isu: 7355c9d9f7d1033e0fe3ee13513366ad69170013
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: uuid=81a66cc2cf3f554e02f089c04d8d4fcb;
admobuu=48617727332748471264744376038126
Connection: keep-alive

The platform can be identified by the User-Agent string:
  • iPhone: AdMob-iSDK-20yyymmdd
  • Android: AdMob-ANDROID-20yyymmdd
  • WP7: possibly AdMob-WINDOWSPHONE7-20yyymmdd; observed 20yyymmdd-WINDOWSPHONE7-AldaritSuperAds

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
Cross-Platform Ads: AdMob

POST /ad_source.php HTTP/1.1
Accept: */*
Content-Length: 277
Accept-Encoding: identity
Content-Type: application/x-www-form-urlencoded
User-Agent: {User-agent}
Host: r.admob.com
Connection: Keep-Alive
Cache-Control: no-cache

...rt=0
&u={User-Agent}
&isu={isu}
&ex=1
&client_sdk=1
&l=en
&f=jsonp
&z=1304518478
&s=a14d248b5738462
&v=20101123-WINDOWSPHONE7-AldaritSuperAds

<table>
<thead>
<tr>
<th>Argument</th>
<th>iPhone</th>
<th>Android</th>
<th>WP7</th>
</tr>
</thead>
<tbody>
<tr>
<td>{isu}*</td>
<td>iPhone UDID, or MD5 hash of the int val of the UDID</td>
<td>MD5 hash of the int val of the Android ID</td>
<td>SHA1 hash of the int val of the Device ID</td>
</tr>
</tbody>
</table>

*: isu can appear both as an argument in a POST or in the X-ADMOB-ISU HTTP header extension.
Cross-Platform Ads: Mydas

GET /getAd.php5?
sdkapid=35447
&auid={Phone IMEI}
&ua={User-Agent}
&mmisdk=3.6.3-10.10.26.
&kw={keywords for app}
&mode=live
&adtype=MMBannerAdTop
HTTP/1.1

<table>
<thead>
<tr>
<th>Argument</th>
<th>iPhone</th>
<th>Android</th>
<th>WP7</th>
</tr>
</thead>
<tbody>
<tr>
<td>{auid}</td>
<td>?</td>
<td>IMEI</td>
<td>Base64-encoded integer value of Device ID</td>
</tr>
<tr>
<td>HTTP Host</td>
<td>?</td>
<td>androidsdk.ads.mp.mydas.mobi</td>
<td>ads.mp.mydas.mobi</td>
</tr>
</tbody>
</table>

Host: androidsdk.ads.mp.mydas.mobi
Accept-Encoding: gzip
Accept-Language: en-GB, en-US

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
Analytics firm Flurry estimates that 250,000 Motorola Droid phones were sold in the United States during the phone's first week in stores.
Managing User Privacy Expectations

Although some users may be concerned about their privacy, all data is gathered anonymously. On Pinch Media’s own website, the company states that when Pinch Analytics is installed within an application, the following information is sent back on each application run:

- A hardware identifier not connectable to any personal information
- The model of the phone (HTC, Samsung, LG, Droid 2, and so on) and operating system (2.1, 2.2, and so on)
- The application’s name and version
- The result of a check to see if the device has been jailbroken
- The result of a check to see if the application has been stolen and the developer hasn’t been paid
- The length of time the application was run
- The user’s location (if the user explicitly agrees to share it)
Analytics: Dataflurry

Chapter 17 Using Android Analytics

- The gender and age of the user (if the application uses Facebook Connect)

None of this information can identify the individual. No names, phone numbers, email addresses, or anything else considered personally identifiable information is ever collected. The information sent from applications, when it arrives at the servers, is quickly converted to aggregated reports—unprocessed data is processed as quickly as possible. The aggregated reports show counts and averages, not anything user specific. For instance, a developer can see the following information:

- The number of distinct users who’ve accessed the application
- The average length of time the application was used
- The percentage of phones using each operating system
- The percentage of each model of phone (3G, 3GS, and so on)
- A breakdown of user locations by country, state, and major metropolitan area (for example, 20,000 in USA, 700 in New York state, 500 in New York City)
- The percentage of users of each gender
- The percentage of users by “age bucket” (21–29, 30–39, and so on)
Analytics: Dataflurry Example (Device Identifier)

POST http://data.flurry.com/aar.donull HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Content-Type: application/octet-stream
Content-Length: 1395
Connection: close

............0?..n..IPF9LEEU8YW9ICKDSIUQ..2.0.74..BBPIN574646979........0?........0?.......device.m
odel..Black
Motion..do
.524280..en
code
1.1.micro
cale..en-
GB..micro
2.1.wire
+44123456
ax.bluetooth
javax.micro
.partial
.arm
javax.micro
true.
javax.micro
android
javax.micro
recordControl
on.pim.PIN
javax.micro
wireless.messaging.TextMessage..true.
javax.wireless.messaging.MultipartMessage..true.

• BlackBerry: BBPIN574646979 ➔ 22406AC3
• Android: AND{AndroidID, 16 hex bytes}
• iPhone: IPHONE{iPhoneUDID, 40 hex bytes}
• Symbian: ID{SomeIDNumber, 8-10 digit int}
• IMSI: IMSI{IMSI}
• IMEI: IMEI{IMEI, 15 digit int}
Analytics: Dataflurry Example (Device Metadata)

POST http://data.flurry.com/aar.donull HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Content-Type: application/octet-stream
Content-Length: 1395
Connection: close

.........0?..n..IPF9LEEU8YW9ICKDSIUQ..2.0.74..BBPIN574646979....0?........0.......device.model..Blackberry8900..device.manufacturer..Research In Motion..device.os.version..5.2.0.31..runtime.total.memory..169452204..storage.available..524280..audio.encodings,,encoding=audio/amr_encoding=pcm

Handset is RIM BlackBerry 8900 with OS 5.2.0.31
device.model Blackberry8900
device.manufacturer Research In Motion
device.os.version 5.2.0.31
runtime.total.memory 169452204
storage.available 524280

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
Analytics: Dataflurry Example (Device Metadata)

POST http://data.flurry.com/aar.donull HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Content-Type: application/octet-stream
Content-Length: 1395
Connection: close

Phone Number and Carrier Information
wireless.messaging.sms.smsc +441234567890
wireless.messaging.mms.mmsc
http://mms.mycarrier.co.uk/servlets/mms

cale..en-
GB..microedition.platform..BlackBerry8900/5.0.0.411..microedition.profiles..MIDP-
2.1..wireless.messaging.sms.smsc.
+441234567890..wireless.messaging.mms.mmsc.&http://mms.mycarrier.co.uk/servlets/mms..jav
ax.bluetooth.LocalDevice..true.)javax.microedition.content.ContentHandler..true.)
.true.)javax.microedition.io.file.FileConnection..true.
$javax.microedition.location.Location..true.-
javax.microedition.media.control.VideoControl..true..javax.microedition.media.control.Re
cordControl..true.,javax.microedition.payment.TransactionModule..false..javax.microediti
on.pim.PIM..true.
$javax.microedition.sip.SipConnection..false.*javax.microedition.sip.SipServerConnection
..false..javax.obex.Operation..true.*javax.wireless.messaging.MessageConnection..true.
$javax.wireless.messaging.MultipartMessage..true.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on...
Analytics: Dataflurry Breakdown

*DJPTCYNVVIV5H9D3R5IK.
.1.1.1....IPHONEa7deb7b28a94c880f6f80f6b02bee4161d157122.
..Level
restarted....From complete menu..Level..-10-19........D............Level
restarted....From pause menu..Birds used..3..Birds available..3..Level..-10-19..Attempts..1..................Level complete....

Dataflurry App Metadata

Contains a unique identifier for the application and the version number
Analytics: Dataflurry Breakdown

*DJPTCYNVVIV5H9D3R5IK.
.1.1.1..IPHONEa7deb7b28a94c880f6f80f6b02bee4161d157122...-/.....----------device.model.1..i0S4De
vice......1.1.1...-.wVH.......VG....................

**Dataflurry Device Metadata**

Contains a unique identifier for the handset and properties of the handset

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on... or email...
Analytics: Dataflurry Breakdown

*........................................*... DJPTCYNVVIV5H9D3R5IK.
.1.1.1. TPHONEa7deh7b28a94c880f6f80f6b0d157122.

App Analytics Metadata

Developer-specified application analytics

Level started....Level started....From...complete menu..Level..-10-19....D...........Level restarted....From..pause menu..Birds used..3..Birds available..3..Level..-10-19..Attempts..1....................Level complete....
Analytics: DataFlurry Device Metadata

**Device Hardware**
- `device.model`
- `device.manufacturer`

**Phone Information**
- `wireless.messaging.sms.smsc`
- `wireless.messaging.mms.mmsc`
- `IMSI`
- `IMEI`

**OS Information**
- `build.brand`
- `build.id`
- `device.os.version`
- `version.release`

**Cell Network Metadata**
- `network.mcc`
- `network.mnc`
- `network.lac`
- `network.cellid`
- `com.sonyericsson.net.cellid`
- `com.sonyericsson.net.lac`
- `com.sonyericsson.net.mcc`
- `com.sonyericsson.net.mnc`
- `CellID`
- `cellid`
- `LAC`
- `Lac`
- `lac`
- `MCC`
- `Mcc`
- `mcc`
- `MNC`
- `Mnc`
- `mnc`
- `com.nokia.mid.countrycode`
- `com.nokia.mid.cellid`
- `com.nokia.mid.networkid`
- `com.nokia.network.access`
Analytics: Dataflurry Device Metadata

- device.model
- device.manufacturer
- device.os.version
- device.software.version
- build.brand
- build.id
- version.release
- runtime.total.memory
- storage.available.size
- audio.encodings
- microedition.commports
- microedition.configuration
- microedition.encoding
- microedition.global.version
- microedition.locale
- microedition.platform
- microedition.profiles
- wireless.messaging.sms.smsc
- wireless.messaging.mms.mmsc
- java.bluetooth.LocalDevice
- java.microedition.content.ContentHandler
- java.microedition.global.ResourceManager
- java.microedition.io.SocketConnection
- java.microedition.io.file.FileConnection
- java.microedition.location.Location
- java.microedition.media.control.VideoControl
- java.microedition.media.control.RecordControl
- java.microedition.payment.TransactionModule
- java.microedition.pim.PIM
- java.microedition.sip.SipConnection
- java.microedition.sip.SipServerConnection
- java.obex.Operation
- java.wireless.messaging.MessageConnection
- java.wireless.messaging.TextMessage
- java.wireless.messaging.MultipartMessage
- pur.date
- rel.date
- pur.price
- store.id
- bluetooth.api.version
- fileconn.dir.memorycard
- fileconn.dir.photos.file
- fileconn.dir.photos.name
- fileconn.dir.private.file
- fileconn.dir.videos.file
- fileconn.dir.photos.name
- fileconn.dir.tones
- fileconn.dir.tones.name
- microedition.chapi.version
- microedition.io.file.FileConnection.version
- microedition.jtwi.version
- microedition.m3g.version
- microedition.pim.version
- microedition.location.version
- supports.audio.capture
- supports.mixing
- supports.recording
- supports.video.capture
- video.snapshot.encodings
- microedition.media.version
- streamable.contents
- video.encodings
- com.sonyericsson.net.cellid
- com.sonyericsson.net.lac
- com.sonyericsson.net.mcc
- com.sonyericsson.net.mnc
- microedition.timezone
- microedition.hostname
- IMEI
- IMSI
- network.mcc
- network.mnc
- network.lac
- network.cellid
- CellID
- cid
- LAC
- lac
- MCC
- Mcc
- MNC
- Mnc
- comports.maxbaudrate
- com.nokia.mid.countrycode
- com.nokia.mid.cellid
- com.nokia.mid.networkid
- com.nokia.network.access
- version.release
- country.code
- default.timezone
- storage.available
Mobile Gateway HTTP Headers and Data Aggregators: DataFlurry

POST /aar.do HTTP/1.0
Connection: Keep-Alive
User-Agent: SonyEricssonS500i/R8BA Profile/MIDP-2.0 Configuration/CLDC-1.1 UNTRUSTED/1.0
Host: data.flurry.com
Accept: */*
Accept-Charset: utf-8, iso-8859-1
Content-Type: application/octet-stream
Content-Length: 2327
Via: infoX WAP Gateway V300R001, Huawei Technologies
x-up-calling-line-id: +44
x-forwarded-for:
x-huawei-IMSI:

..........%..%....KHFP142N4PHQBQ8R7XEH..1.5.0..IMEIIMEI 35808401-728365-6-65 ....!
$5....%....*....microedition.platform..SonyEricssonS500i/R8BA024....1.5.0....%.
.N(......;0........onChatMessageSent...(onChatNewSession...Q.
Analytics: Other Methods & Providers

Many apps send a beacon out when the app is started
• Can be first- or third-party
• Typically includes phone ID; can include IMEI, geo, etc.
• Examples: Qriously, Com2Us, Fluentmobile, Papayamobile

BB App World will geolocate users using MCC and MNC to determine what content to show in the app store
Android ID Changes

Typically, Android IDs have followed the format below:

<table>
<thead>
<tr>
<th>ANDROID_ID</th>
<th>2 0 0</th>
<th>Hex encoded IMEI (inc. check digit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 2</td>
<td>MEID?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>X X X X X X X X X X X X X X X X</td>
<td></td>
</tr>
</tbody>
</table>

Seeing Android IDs starting to use the full 64-bits and decent distribution

Special case: 9774d56d682e549c is a non-unique Android ID (related to a Froyo release bug)
Windows Phone 7 Device IDs

App descriptions in the Marketplace will indicate whether a given app will use the account identifier or the phone identifier, both or neither.

Device IDs are 20-byte values (40-byte hex strings) represented in the following ways:
- A1A2A3A4A5B1B2B3B4B5C1C2C3C4C5D1D2D3D4D5 is the usual ASCII representation, typically in upper-case
- A1A2A3A4-A5B1B2B3-B4B5C1C2-C3C4C5D1-D2D3D4D5
- A1-A2-A3-A4-A5-B1-B2-B3-B4-B5-C1-C2-C3-C4-C5-D1-D2-D3-D4-D5
- Base64 encoding the integer value of the identifier. The resulting string looks like oAkpKWXsrO0tCHw8TF0dLT1NU=
- Long number string (i.e. 19621225364332011917921824118918419013320401482152118)
Windows Phone 7 App IDs

All traffic from a Win7 handset appears to carry the GUID associated with the app in the HTTP Referer field.

POST /Service/ServiceElleStyleTag.svc HTTP/1.1
Accept: */*
Referer: file:///Applications/Install/BB7CD1F6-BCDA-DF11-A844-00237DE2DB9E/Install/
Content-Length: 243
Accept-Encoding: identity
Content-Type: text/xml; charset=utf-8
SOAPAction: "urn:ServiceElleStyleTag/GetPlaces"
User-Agent: NativeHost
Host: styletag.elle.fr
Connection: Keep-Alive
Cache-Control: no-cache

<s:Envelope

If the Referer field is formatted in this way only for WP7 apps, it may be possible to use this as a mobile TDI against the Live account.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on or email
Windows Phone 7 MSN Ads

Apps that use MSN’s Mobile Ad service associate with the handset’s Live account instead of the handset itself.

GET /v3/Delivery/Placement?
pubid=break001wp7
&pid=USM3PB
&adm=1
&cfmt=text,image&sft=jpeg,png,gif&w=480&h=80
&fmt=json
&cltp=app
&dim=le
&nct=1&lc=en-GB&idtp=anid
&uid=63388195C29A61B3EA2E62EEFFFFFF HTTP/1.1
Accept: */*
Referer: file:///Applications/Install/D1CD2DCB-7CD5-DF11-A844-0237DE2DB9E/Install/
Accept-Encoding: identity
User-Agent: NativeHost (or occasionally, User-Agent: Windows Phone Ad Client (Xna)/5.1.0.0)
Host: mobileads.msn.com
Connection: Keep-Alive
Windows Phone 7 Marketplace

The WP7 Marketplace also associates with the handset’s Live account, and can include enough metadata to indicate that the account is active on a handset.

GET /v3.2/en-GB/apps?
orderBy=downloadRank
&cost=paid&chunkSize=10
&clientType=WinMobile%207.0
&store=Zest
&store=020GB
&store=HTC HTTP/1.1
User-Agent: ZDM/4.0; Windows Mobile 7.0;
Host: catalog.zune.net (or origin-catalog.zune.net)
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ANON=A=63388195C29A61B3EA2E62EEFFFFFFE&F=1
NAP=V=1.9&E=ac2&C=WbPWets1RmtLDSMaoaSy121N44id48LnRByEVrcQ0q8wd6Ds0g&W=1

The “store” arguments can help identify the handset manufacturer and the carrier.

This is the ANON cookie value for the Live account associated with the handset.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on... or email...
Abusing BADASS for Fun and Profit

Mediallytics traffic from Android uses MD5 sum of the Android ID string
Example: 200142d4dfcd56a9 = DEA9F697DEB0CBBB8433018A0B723BF9

POST /event HTTP/1.1
Content-Length: 543
Content-Type: application/x-www-form-urlencoded
Host: t.mediallytics.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

v=2 &h=0&tok=CAFEBABE
&sys=Android
&svsv=2.3.3
&dev=dea9f697deb0cbbb8433018a0b723bf9
&model=google+Nexus+One
&app=77327b6f00e7aa0f452d9d3ac3e2d1618e0f3aaa
&appv=2.5.3-BB70302
&data=...

Odds are that they’re using something similar for iPhones....
Abusing BADASS for Fun and Profit

We can use the FKB PCAP testing step as a launching point for a fishing expedition...

We use a very basic regular expression and restrict the traffic by requiring “Host: t.medialytics.com” (not pictured). Initially, we don’t add a validator for sys=Android.

This should give us traffic for Android, iPhone and any other platform they’re using MD5 sums against.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
Abusing BADASS for Fun and Profit

BADASS can show us packet dumps of traffic that completely matched the rule, and traffic that matched on the selector but failed on the rule.

Green indicates the selector hitting in the packet payload.

Yellow indicates where part of the rule hit. In this case, it’s the “Host: t.medialytics.com” validator and where a User-Agent extractor hit in the traffic.

The lack of other highlighted regions indicates that there was no hit on the “dev” presence identifier…

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on...
Abusing BADASS for Fun and Profit

... but that doesn’t mean that the dev identifier isn’t there! It’s just formatted differently.

<table>
<thead>
<tr>
<th>hexadecimal</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>01f8: 6d4c 624f 754e 6441 7259 0d0a 436f 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0208: 656e 742d 4469 7370 6f73 6974 696f 6e3a 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0218: 2066 6f72 6d2d 6461 7461 3b20 6e61 6d65 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0228: 3d22 7379 7322 0d0a 0d0a 6950 686f 6e65 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0238: 204f 530d 0a2d 2d30 784b 6854 6d4c 624f 754e 6441 7259 0d0a 436f 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0248: 754e 6441 7259 0d0a 436f 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0258: 4469 7370 6f73 6974 696f 6e3a 2066 6f72 6d2d 6461 7461 3b20 6e61 6d65 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0268: 6d2d 6461 7461 3b20 6e61 6d65 3d22 7379 7322 0d0a 0d0a 6950 686f 6e65 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0278: 7376 220d 0a0d 0a34 2e32 2e31 0d0a 2d2d 6e61 6d65 3d22 7379 7322 0d0a 0d0a 6950 686f 6e65 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0288: 3078 4b68 546d 4c62 4f73 4e64 4172 590d 7379 7322 0d0a 0d0a 6950 686f 6e65 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>0298: 0a43 6f6e 7465 6e74 2d44 6973 706f 7369 7465 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>02a8: 7469 666e 3a20 666f 726d 6e72 616d 653d 2d2d 7379 7322 0d0a 0d0a 6950 686f 6e65 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>02b8: 206e 616d 653d 2d2d 7379 7322 0d0a 0d0a 6950 686f 6e65 6e74 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>02c8: 3461 3563 3965 3338 3933 3739 3833 3433 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>02d8: 3166 6364 6437 3033 6535 6431 3566 620d mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
<tr>
<td>02e8: 0a2d 2d30 784b 6854 6d4c 624f 754e 6441 mlBoUyNdArY...Content-Disposition: Form-data; name=&quot;sys&quot;...iPhone OS.--0xKhTmLbOuNdArY...Content-Disposition: form-data; name=&quot;dev&quot;...4a5c9e38937988431fcdd703e5d15fb.---0xKhTmLbOuNdArY</td>
<td></td>
</tr>
</tbody>
</table>

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on...
Abusing BADASS for Fun and Profit

Using the FKB PCAP test in this manner has shown us that:

1. Medialytic traffic can appear as form-data
2. Our theory about iPhone traffic having a similar structure holds
3. iPhone traffic is using the MD5 sum against the UUID
4. We can create a rule against the iPhone variant with ease ("sys=iPhone OS" vs. "sys=Android")

and most importantly:

1. Creativity, iterative testing, domain knowledge, and the right tools can help us target multiple platforms in a very short time period.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
To bring us full-circle...

AdMob

Dataflurry
(Flurry/Pinch Media)

MobClix

Medialytics
(Medialets)

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on