

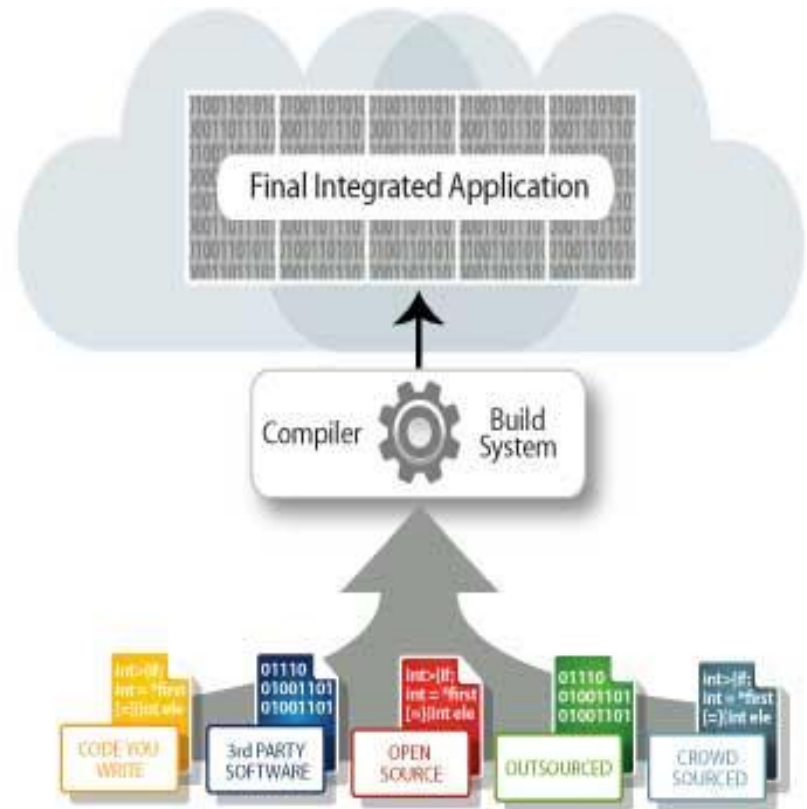


Avoiding the Pandora Pitfall
Secure Coding Practices for
Android Application Privacy

Joe Brady
Sr. Solutions Architect
November 29, 2011

About Veracode

- ✦ Founded in 2006 by application security experts and industry veterans
- ✦ Patented static binary analysis innovation removes dependence on source code for automated code scanning
- ✦ Cloud platform combines static analysis, dynamic analysis, policy management, elearning and application intelligence capabilities
- ✦ Offer automated analysis of mobile apps including iOS and Android
- ✦ Massively parallel architecture for rapid automated scanning of thousands of applications
- ✦ Recognized as leaders in Gartner's static application security testing MQ



"Only one vendor, Veracode, has an offering that can perform true binary analysis" **Gartner**



Mobile Security
Landscape

Privacy
Implications

1

2

3

4

Case Studies

Q&A



**Risk - noun \`risk\
The possibility of loss or injury**

PC Sensitive Data

Financial data

Corporate data

Computing power

Email

Contact List

Photos

...

Video Images

MMS

Location
Information

Call Logs

Outbound
Dialing

SMS

Audio Data



Mobile Mitigations

Patch methodology

Process isolation

Reasonable permission
model

Home disk encryption

Code signatures

Firewalls

Patch
Methodology


Anti-Virus

DEP

HIDS / NIDS

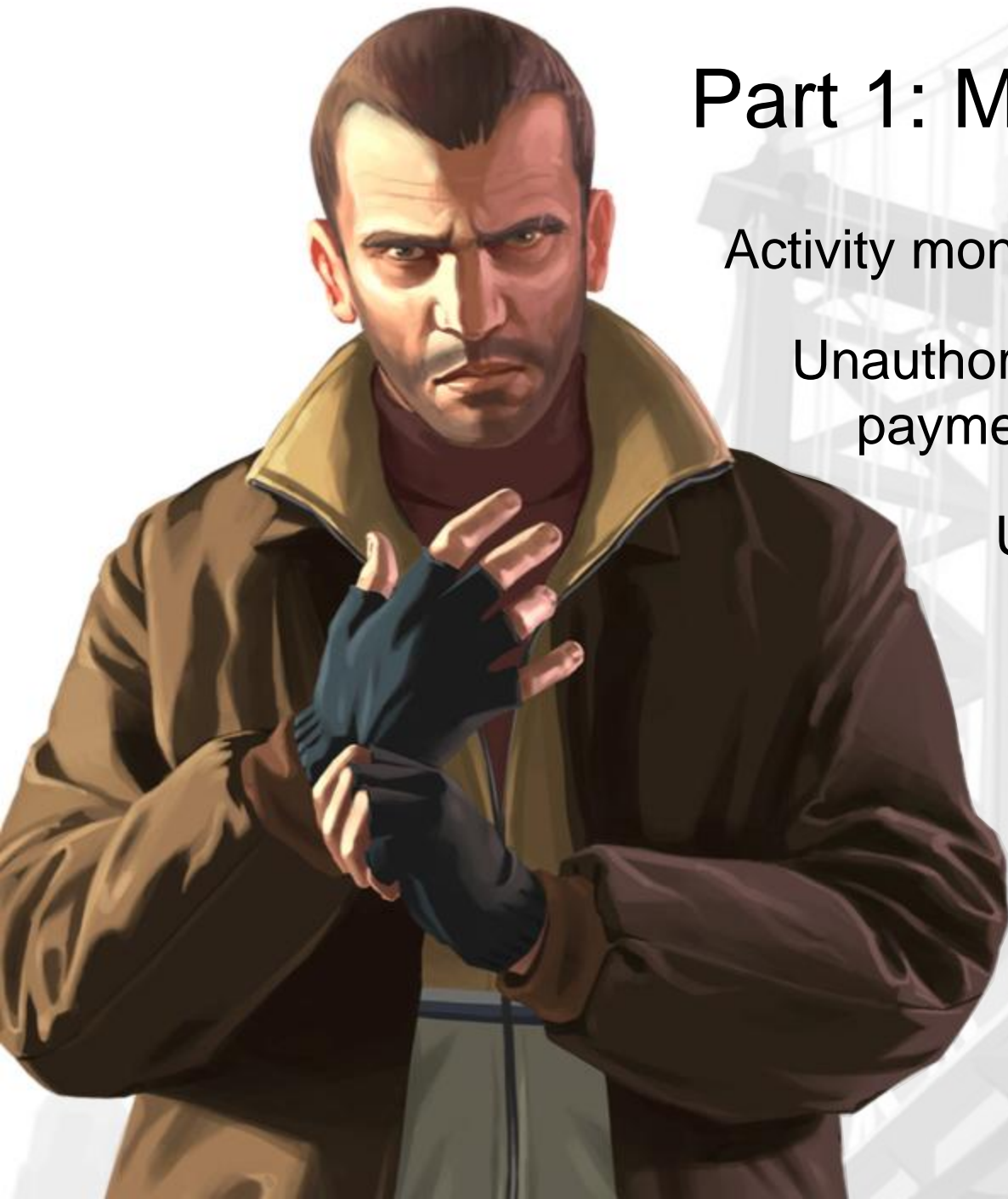
ASLR

Strong Disk
Encryption



10.9 billion mobile apps downloaded
in 2010, according to IDC

Expected to rise to
76.9 billion apps by 2014



Part 1: Malicious Code

Activity monitoring and data retrieval

Unauthorized dialing, SMS, and payments

Unauthorized network connectivity (exfiltration or command & control)

UI impersonation

System modification (rootkit, APN proxy config)

Logic or time bomb

Part 2: Code Vulnerabilities

Sensitive data leakage (inadvertent or side channel)

Unsafe sensitive data storage

Unsafe sensitive data transmission

Hardcoded password/keys





Case Study: *Hardcoded Passwords*



Case Study: *Unsafe Data Transmission*

Print

Tweet

Like

41

Alert

Security shocker: Android apps send private data in clear

Facebook's persistent SSL isn't

By Dan Goodin in S... • Get more from

Posted in Security 24th ... 11:00:21

Official Facebook
application
Transmitted everything
except password in clear
text

Photos, private messages,
wall posts, etc

Even with Web-SSL Enabled

Google Calendar
Transmitted appointment
data in clear text

Or better yet...

Just disable cert checking all together!

As Seen In The WILD!

```
TrustManager that does not validate certificate chains
TrustManager[] trustAllCerts = new TrustManager[]{
    new X509TrustManager() {
        public java.security.cert.X509Certificate[] getAcceptedIssuers() {
            return null;
        }
        public void checkClientTrusted(
            java.security.cert.X509Certificate[] certs, String authType) {
        }
        public void checkServerTrusted(
            java.security.cert.X509Certificate[] certs, String authType) {
        }
    }
};

// Install the all-trusting trust manager
try {
    SSLContext sc = SSLContext.getInstance("SSL");
    sc.init(null, trustAllCerts, new java.security.SecureRandom());
    HttpsURLConnection.setDefaultSSLSocketFactory(sc.getSocketFactory());
} catch (Exception e) {
}

// Now you can access an https URL without having the certificate in the truststore
try {
    URL url = new URL("https://hostname/index.html");
} catch (MalformedURLException e) {
}
```

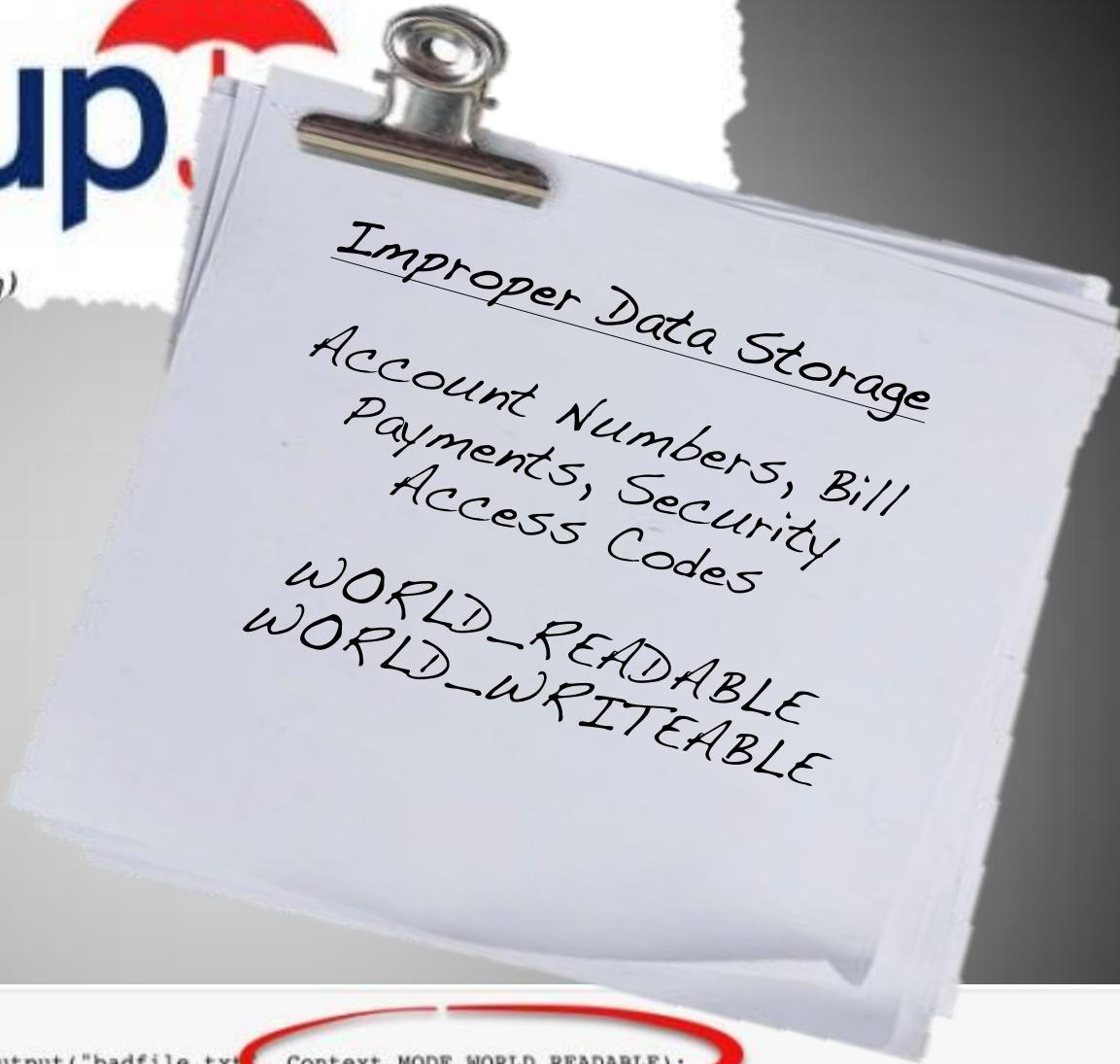


Case Study: *Unsafe Data Writes*

Citigroup



(Image courtesy of contact-centres.com)



```
void createFileBadPerms() {  
try {  
    FileOutputStream fos = this.con.openFileOutput("badfile.txt", Context.MODE_WORLD_READABLE);  
    ObjectOutputStream oos = new ObjectOutputStream(fos);  
    String text = "This is a test text string object.. we are going to serialize and write this in an unsafe manner";  
    oos.writeObject(text);  
    oos.close();  
} catch (FileNotFoundException e) {  
    e.printStackTrace();  
} catch (IOException e) {  
    e.printStackTrace();  
}  
}
```


skype™ mobile

Improper Data Storage

SQLite3 Database

Contact List
Chat Logs

WORLD-READABLE
WORLD-WRITEABLE

```
SQLiteDatabase db = context.openOrCreateDatabase(DATABASE_NAME, Context.MODE_WORLD_READABLE | Context.MODE_WORLD_WRITEABLE, null);  
createDatabase(db);
```



Case Study: *Data Exfiltration*



WSJ Breaks Story on Pandora Investigation

Mobile-App Makers Face U.S. Privacy Investigation

By AMR EFRATI, SCOTT THURM and DIONNE SEARCEY

Federal prosecutors in New Jersey are investigating whether numerous smartphone applications illegally obtained or transmitted information about their users without proper disclosures, according to a person familiar with the matter.



Online music streaming service Pandora, which plans an initial public offering, says in an SEC filing that it has been subpoenaed in an investigation probing information-sharing by mobile applications. *John Letzing and Stacy DeLoe discuss.*

Securities and Exchange Commission filing. The Oakland, Calif., company said it had been informed it is "not a specific target of the investigation." Pandora said it believed similar subpoenas had been issued "on an industry-wide basis to the publishers of numerous other smartphone applications."

A Pandora spokeswoman declined to comment.

The Wall Street Journal reported in December that popular applications on the iPhone and Android mobile phones, including Pandora, transmit information about the phones, their users and their locations to outside advertising networks.

Smartphone apps—of which there are thousands—programs that allow, say, a user to read an e-book, get sports scores or search for a restaurant.

The Journal tested 101 apps and found that many of them transmitted information about the phone's unique device identifier to third parties.

The criminal investigation is examining whether the app makers fully described to users the types of data they collected and why they needed the information—such as a user's location or a unique identifier for the phone—the person familiar with the matter said. Collecting information about a user without proper notice or authorization could violate a federal computer-fraud law.

Online music service Pandora Media Inc. said Monday it received a subpoena related to a federal grand-jury investigation of information-sharing practices by smartphone applications.

Pandora disclosed the subpoena, issued "in early 2011," in a Securities and Exchange Commission filing. The Oakland, Calif., company said it had been informed it is "not a specific target of the investigation." Pandora said it believed similar subpoenas had been issued "on an industry-wide basis to the publishers of numerous other smartphone applications."

“Federal prosecutors in New Jersey are investigating whether numerous smartphone applications illegally obtained or transmitted information about their users without proper disclosures”

No program execution

Full coverage of binary or
source

Wider range of bug discovery

Not limited by runtime data

-- JD-GUI

-- Veracode Engine

Static Analysis

JD-Gui Analysis

Java Decompiler - AdManager.class

File Edit Navigate Search Help

com.pandora.android-1 - updated dex2jar.jar

com

- admarvel.android
 - ads
 - AdFetcher
 - AdMarvelAd
 - AdMarvelDisplayContext
 - AdMarvelISWebViewS1
 - AdMarvelISWebViewSAdMarvelWebV
 - AdMarvelISWebView
 - AdMarvelViewS1
 - AdMarvelViewS2
 - AdMarvelView
 - AdMarvelWebView1
 - AdMarvelWebView
 - AdMarvelXMLElement
 - AdMarvelXMLReader
 - R
 - Rotate3dAnimation
 - analytics
 - common
 - admob.android.ads
 - ford.syncV4
 - google.ads
 - medialets
 - pandora
 - securestudies
- org
 - apache
 - slf4j

d.class AdManager.class

```
static String[] getTestDevices()
{
    return e;
}

public static String getUserId(Context paramContext)
{
    String str1 = "emulator"; String str2 = "AdMobSDK";

    Object localObject1 = f; if (localObject1 == null) { Object localObject3 = paramContext.getContentResolver();

    467     localObject1 = localObject3;

    469     str3 = "android_id"; localObject3 = Settings.Secure.getString((ContentResolver)localObject1, str3);

    474     localObject1 = localObject3; if (localObject1 != null) break label159;
    477     localObject1 = "emulator"; f = str1; localObject1 = "AdMobSDK"; localObject1 = "To get test ads on the emulator use AdManager.setTestDevices( new String[] { Admanager.TE

    487     int m = 3; int i1 = Log.isLoggable(str2, m);

    494     m = i1; if (m != 0)

    610     {
    612         localObject2 = "AdMobSDK"; localObject2 = new java/lang/StringBuilder; ((StringBuilder)localObject2).<init>(); str3 = "The user ID is "; Object localObject4 = ((String

    628         localObject2 = localObject4; localObject4 = ((StringBuilder)localObject2).toString(); localObject2 = localObject4; int i2 = Log.d(str2, (String)localObject2);
    629     } Object localObject2 = f; String str3 = "emulator"; if (localObject2 == str1);
    629     for (localObject2 = null; ; localObject2 = f) { return localObject2; label159: Object localObject5 = a((String)localObject2); localObject2 = localObject5; f = (String)loce
    }

    public static boolean isTestDevice(Context paramContext)
    {
    421     int m = 0; Object localObject1 = e;
    422     int n;
    423     if (localObject1 != null)
    425     {
    425         String str = getUserId(paramContext);

    431         localObject1 = str; if (localObject1 == null)
    434         {
    434             localObject1 = "emulator";
    431         }
    431         String[] arrayOfString = e; Object localObject2 = Arrays.binarySearch(arrayOfString, localObject1); localObject1 = localObject2; if (localObject1 >= 0) n = 1;
    431     } while (true) { return n; n = n; continue; n = n;
    }
```

AdMob Location Requests

The screenshot shows a Java decompiler window titled "Java Decompiler - AdManager.class". The left pane displays a package tree for "com.pandora.android-1 - updated dex2jar.jar", with "admob.android.ads" highlighted. The right pane shows the decompiled code for "AdManager.class".

```
String str1 = "url";
107 d = str1;
150 str1 = null; e = str1;
151 str1 = "AdMobSDK"; String str2 = "AdMob SDK version is 20100331-ANDROID-3312276cc1406347"; int m = Log.i(str1, str2);
}

static String a()
{
720 long l1 = h; long l2 = 1000L; l1 /= l2; String str1 = String.valueOf(l1); return str1;
}

static String a(Context paramContext)
{
697 String str1 = "AdMobSDK"; Object localObject1 = null; Object localObject2 = getCoordinates(paramContext);
701 Object localObject4 = localObject2;
String str2;
701 if (localObject4 != null) { localObject1 = new java/lang/StringBuilder; ((StringBuilder)localObject1).<init>(); double d1 = ((Location)localObject4).getLatitude(); double
704 localObject1 = localObject2; str2 = ","; localObject2 = ((StringBuilder)localObject1).append(str2);
706 localObject1 = localObject2; d1 = ((Location)localObject4).getLongitude(); double d3 = d1; localObject2 = ((StringBuilder)localObject1).append(d3); localObject1 = localO
709 localObject1 = localObject2; } localObject4 = "AdMobSDK"; int i1 = 3; int m = Log.isLoggable(str1, i1); i1 = m; if (i1 != 0) { Object localObject5 = "AdMobSDK"; localOb
}

private static String a(String paramString)
{
514 int m = 0; Object localObject1 = null; if (paramString != null) { int i1 = paramString.length();
518 int i4 = i1;
519 if (i4 <= 0); } try { localObject1 = "MD5"; Object localObject3 = MessageDigest.getInstance((String)localObject1);
520 localObject1 = localObject3; localObject3 = paramString.getBytes(); localObject5 = localObject3; int i5 = null; int i2 = paramString.length(); int i6 = i2;
531 ((MessageDigest)localObject1).update(localObject5, i5, i6);
652 localObject5 = "%032X"; localObject6 = null; localObject6 = new Object[localObject6]; i6 = 0; BigInteger localObject6 = new java/math/BigInteger; int i7 = 1; localOb
655 localObject1 = localObject4; localBigInteger.<init>(i7, localObject1); localObject6[i6] = localBigInteger; localObject4 = String.format((String)localObject5, localObject
}
}
```

Red circles highlight the following code elements:

- `Object localObject2 = getCoordinates(paramContext);`
- `double d1 = ((Location)localObject4).getLatitude(); double`
- `d1 = ((Location)localObject4).getLongitude(); double d3 = d1;`

The search bar at the bottom left contains the text "Location".

AdMob AndroidID Request

The screenshot shows the Java Decompiler interface with the following details:

- Window Title:** Java Decompiler - AdManager.class
- File List (Left):** com.pandora.android-1.jar, com, admovel.android, admob.android.ads, view, AdListener, AdManager\$1, AdManager, AdView\$1, AdView\$a, AdView\$b, AdView\$c\$1, AdView\$c, AdView\$d, AdView, SimpleAdListener, a, b, c, d\$2, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, ford.syncV4, google.ads, medialets, pandora.
- Code Editor (Right):** AdManager.class
Line 406: `return e;`
Line 467: `String str1 = "AdMobSDK";`
Line 469: `if (f == null) { Object localObject1 = unknown.getContentResolver();`
Line 474: `localObject2 = localObject1;`
Line 477: `localObject1 = Settings.Secure.getString((ContentResolver) localObject2, "android_id");` (Circled in red)
Line 487: `localObject2 = localObject1; if (localObject2 != null) break label108;`
Line 489: `f = "emulator"; int m = Log.i(108, "To get test ads on this emulator use AdManager.setTestDevices(new String[] { Admanager.TEST_EMULATOR });");`
Line 494: `boolean bool = Log.isLoggable(str1, 3);`
Line 610: `if (bool)`
Line 612: `{ StringBuilder localStringBuilder2 = new StringBuilder().append("The user ID is "); String str2 = f; StringBuilder localStringBuilder1 = localStringBuilder2.append(str2`
Line 628: `String str3 = localStringBuilder1.toString(); int n = Log.d(str1, str3);`
Line 628: `} } if (f == "emulator");`
Line 628: `for (Object localObject2 = null; ; localObject2 = f) { return localObject2; label108: f = a((String) localObject2); StringBuilder localStringBuilder3 = new StringBuilder().`
Line 628: `}`
Line 694: `public static boolean isTestDevice(Context unknown)`
Line 700: `{`
Line 721: `Object localObject = e;`
Line 722: `int m;`
Line 723: `if (localObject != null)`
Line 724: `{`
Line 725: `String str = getUserId(unknown);`
Line 731: `localObject = str; if (localObject == null)`
Line 732: `{`
Line 733: `localObject = "emulator";`
Line 734: `}`
Line 735: `}`
- Search Bar (Bottom):** Find: android_id, Next, Previous, Case sensitive
- Taskbar (Bottom):** Windows Start button, taskbar icons, system tray showing 8:44 AM.

Android Manifest Permissions

ACCESS_CHECKIN_PROPERTIES
ACCESS_COARSE_LOCATION
ACCESS_FINE_LOCATION
ACCESS_LOCATION_EXTRA_COMMANDS
ACCESS_MOCK_LOCATION
ACCESS_NETWORK_STATE
ACCESS_SURFACE_FLINGER
ACCESS_WIFI_STATE
ACCOUNT_MANAGER
AUTHENTICATE_ACCOUNTS
BATTERY_STATS
BIND_APPWIDGET
BIND_DEVICE_ADMIN
BIND_INPUT_METHOD
BIND_REMOTEVIEWS
BIND_WALLPAPER
BLUETOOTH
BLUETOOTH_ADMIN
BRICK
BROADCAST_PACKAGE_REMOVED
BROADCAST_SMS
BROADCAST_STICKY
BROADCAST_WAP_PUSH
CALL_PHONE
CALL_PRIVILEGED
CAMERA
CHANGE_COMPONENT_ENABLED_STATE
CHANGE_CONFIGURATION
CHANGE_NETWORK_STATE
CHANGE_WIFI_MULTICAST_STATE
CHANGE_WIFI_STATE
CLEAR_APP_CACHE
CLEAR_APP_USER_DATA
CONTROL_LOCATION_UPDATES
DELETE_CACHE_FILES
DELETE_PACKAGES
DEVICE_POWER
DIAGNOSTIC
DISABLE_KEYGUARD
DUMP
EXPAND_STATUS_BAR
FACTORY_TEST
FLASHLIGHT
FORCE_BACK
GET_ACCOUNTS
GET_PACKAGE_SIZE
GET_TASKS
GLOBAL_SEARCH
HARDWARE_TEST
INJECT_EVENTS
INSTALL_LOCATION_PROVIDER
INSTALL_PACKAGES
INTERNAL_SYSTEM_WINDOW
INTERNET
KILL_BACKGROUND_PROCESSES
MANAGE_ACCOUNTS
MANAGE_APP_TOKENS
MASTER_CLEAR
MODIFY_AUDIO_SETTINGS
MODIFY_PHONE_STATE
MOUNT_FORMAT_FILESYSTEMS
MOUNT_UNMOUNT_FILESYSTEMS
NFC
PERSISTENT_ACTIVITY
PROCESS_OUTGOING_CALLS
READ_CALENDAR
READ_CONTACTS
READ_FRAME_BUFFER
READ_HISTORY_BOOKMARKS
READ_INPUT_STATE
READ_LOGS
READ_PHONE_STATE
READ_SMS
READ_SYNC_SETTINGS
READ_SYNC_STATS
REBOOT
RECEIVE_BOOT_COMPLETED
RECEIVE_MMS
RECEIVE_SMS
RECEIVE_WAP_PUSH
RECORD_AUDIO
REORDER_TASKS
RESTART_PACKAGES
SEND_SMS
SET_ACTIVITY_WATCHER
SET_ALARM
SET_ALWAYS_FINISH
SET_ANIMATION_SCALE
SET_DEBUG_APP
SET_ORIENTATION
SET_PREFERRED_APPLICATIONS
SET_PROCESS_LIMIT
SET_TIME
SET_TIME_ZONE
SET_WALLPAPER
SET_WALLPAPER_HINTS
SIGNAL_PERSISTENT_PROCESSES
STATUS_BAR
SUBSCRIBED_FEEDS_READ
SUBSCRIBED_FEEDS_WRITE
SYSTEM_ALERT_WINDOW
UPDATE_DEVICE_STATS
USE_CREDENTIALS
USE_SIP
VIBRATE
WAKE_LOCK
WRITE_APN_SETTINGS
WRITE_CALENDAR
WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE
WRITE_GSERVICES
WRITE_HISTORY_BOOKMARKS
WRITE_SECURE_SETTINGS
WRITE_SETTINGS
WRITE_SMS
WRITE_SYNC_SETTINGS



Permissions

Phone Calls

Read Phone State and Identity

System Tools

Modify Global System Settings

Prevent Device From Sleeping

Bluetooth Administration

Change Wi-Fi State

Change Network

Connectivity

Automatically Start at Boot

Network Communication

Full Internet Access

Create Bluetooth Connections

View Network State

View Wi-Fi State

Your Personal Information

Read Contact Data

Add or Modify Calendar Events

and Send Email To

Guests

Just a bit deeper...

The Official **Google** Blog | Insights from Googlers into our products, technology, and the Google culture.

We've officially acquired AdMob!

5/27/2010 01:04:00 PM

Last Friday, [we said](#) that mobile advertising was moving fast. So are we! Today, we closed our acquisition of AdMob. Omar Hamoui has built a great team and great products at AdMob and we're thrilled to officially welcome them to Google.

We'll now begin the process of bringing our products and teams together in the best way, and building new products and features together. We're working to make this integration happen as fast and as seamlessly as possible. We'll actively keep our clients up-to-date as we bring our businesses together — stay tuned!

It's clear that mobile advertising is becoming a much larger part of our clients' and partners' strategies and with this acquisition, it's now a central part of our own business. In continuing to invest in this highly competitive area, we'll be bringing together our technology, resources and expertise in search advertising with AdMob's innovative solutions for advertising on mobile websites and in mobile applications.

Mobile search is central

One of the key ways that people find and access information on their mobile devices, just like on the desktop, is through search. As the use of mobile devices continues to grow, and as the number of searches increases in mobile environments, we're seeing more and more people use mobile devices to search. In fact, searches on mobile devices have grown more than 100% in the last year. And as more people use mobile devices to search, we're seeing more and more people search with smartphones and tablets. In fact, searches on mobile devices with smartphones and tablets (Pre) searched 62 percent of all searches on mobile devices.

Increasingly, people are using mobile devices to search for information. In fact, searches on mobile devices with smartphones and tablets (Pre) searched 62 percent of all searches on mobile devices.

Search This Blog
powered by **Google™**

Site Feed
+ **Google**
547K readers
BY FEEDBURNER

Blog Archive
Blog Archive ▾

Labels
[accessibility](#) (29)
[acquisition](#) (18)
[ads](#) (94)
[Africa](#) (16)
[Android](#) (24)
[apps](#) (358)
[April 1](#) (4)

Google purchases AdMob for \$750 million dollars. Closed May, 2010

ESPN, CBS Interactive, Geico, Starbucks...



100,000 – 500,000 installations

Permissions:

- FINE (GPS) LOCATION
- COARSE (NETWORK-BASED) LOCATION
- FULL INTERNET ACCESS

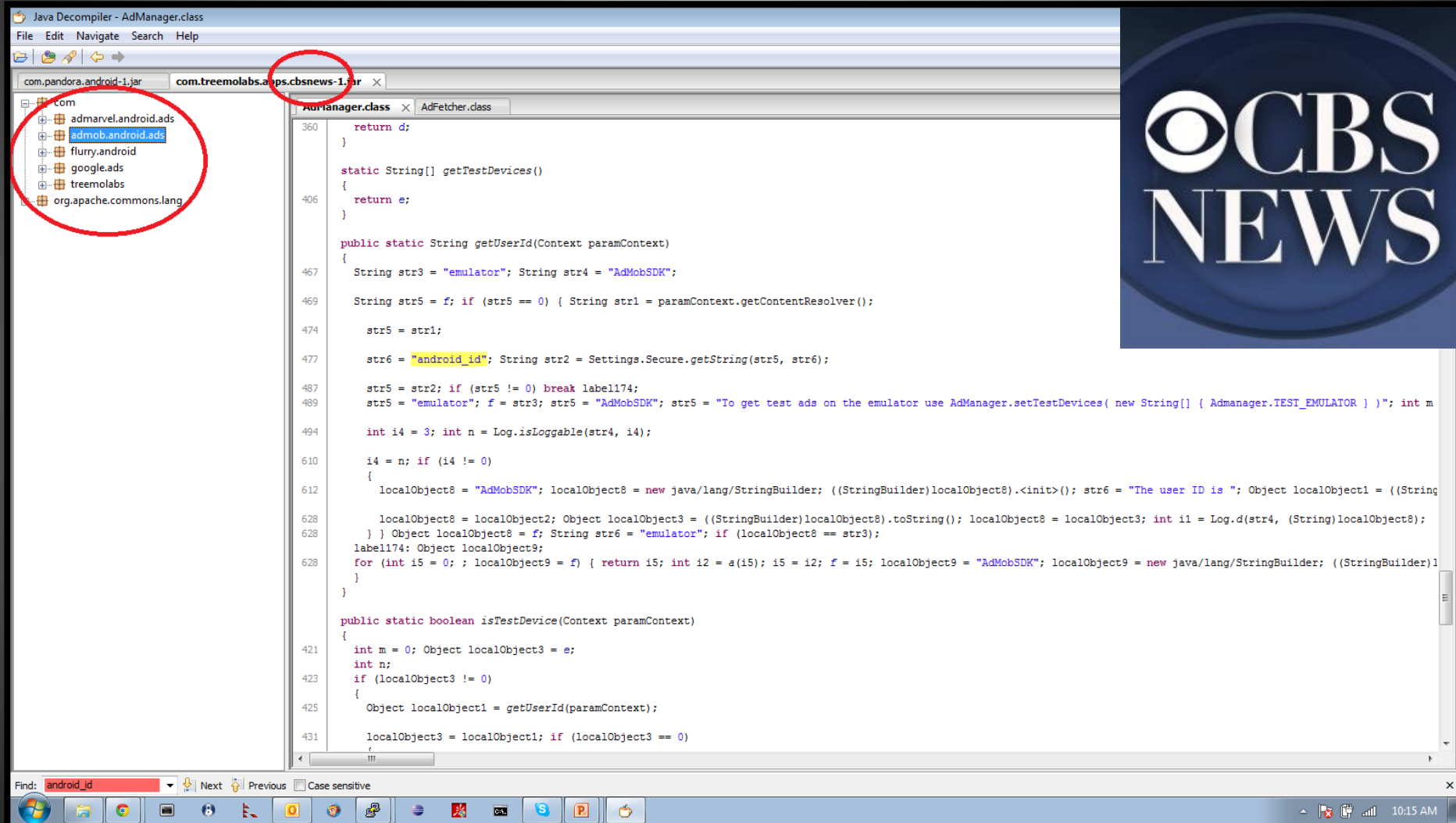


5,000,000 – 10,000,000 installation

Permissions:

- RECORD AUDIO
- CHANGE YOUR AUDIO SETTINGS
- FINE (GPS) LOCATION
- COARSE (NETWORK-BASED) LOCATION
- FULL INTERNET ACCESS
- MODIFY/DELETE USB STORAGE CONTENTS MODIFY/DELETE SD CARD CONTENTS
- PREVENT DEVICE FROM SLEEPING

CBS News Advertising Networks



Java Decompiler - AdManager.class

File Edit Navigate Search Help

com.pandora.android-1.jar com.treemolabs.ads.cbsnews-1.jar

- com
 - admarvel.android.ads
 - admob.android.ads
 - flurry.android
 - google.ads
 - treemolabs
 - org.apache.commons.lang

```
360     return d;
    }

    static String[] getTestDevices()
    {
        return e;
    }

    public static String getUserId(Context paramContext)
    {
        String str3 = "emulator"; String str4 = "AdMobSDK";

        String str5 = f; if (str5 == 0) { String str1 = paramContext.getContentResolver();

        str5 = str1;

        str6 = "android_id"; String str2 = Settings.Secure.getString(str5, str6);

        str5 = str2; if (str5 != 0) break label174;
        str5 = "emulator"; f = str3; str5 = "AdMobSDK"; str5 = "To get test ads on the emulator use AdManager.setTestDevices( new String[] { Admanager.TEST_EMULATOR } )"; int m

        int i4 = 3; int n = Log.isLoggable(str4, i4);

        i4 = n; if (i4 != 0)
        {
            localObject8 = "AdMobSDK"; localObject8 = new java/lang/StringBuilder; ((StringBuilder)localObject8).<init>(); str6 = "The user ID is "; Object localObject1 = ((String

            localObject8 = localObject2; Object localObject3 = ((StringBuilder)localObject8).toString(); localObject8 = localObject3; int i1 = Log.d(str4, (String)localObject8);
        } Object localObject8 = f; String str6 = "emulator"; if (localObject8 == str3);
        label174: Object localObject9;
        for (int i5 = 0; ; localObject9 = f) { return i5; int i2 = a(i5); i5 = i2; f = i5; localObject9 = "AdMobSDK"; localObject9 = new java/lang/StringBuilder; ((StringBuilder)l
        }

        public static boolean isTestDevice(Context paramContext)
        {
            int m = 0; Object localObject3 = e;
            int n;
            if (localObject3 != 0)
            {
                Object localObject1 = getUserId(paramContext);

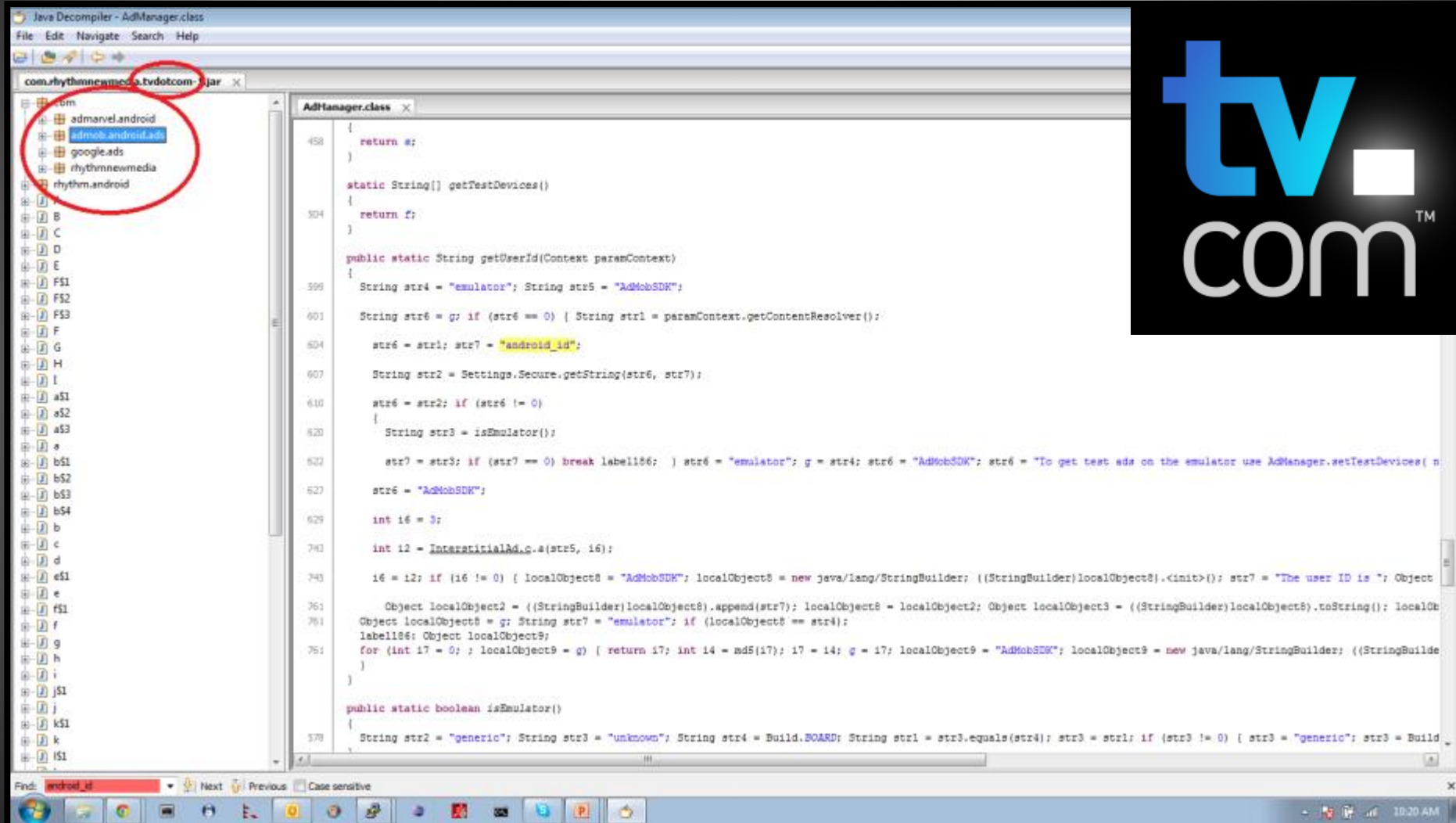
                localObject3 = localObject1; if (localObject3 == 0)
            }
        }
    }
}
```

Find: android_id Next Previous Case sensitive

10:15 AM



TV.com Advertising Networks



Java Decompiler - AdManager.class

com.rhythmnewmedia.tvdotcom.jar

com

- admanvel.android
- admob.android.ad
- google.ads
- rhythmnewmedia
- rhythm.android

AdManager.class

```
458     return s;
    }

    static String[] getTestDevices()
    {
        return f;
    }

    public static String getUserId(Context paramContext)
    {
        String str4 = "emulator"; String str5 = "AdMobSDK";

        String str6 = g; if (str6 == 0) { String str1 = paramContext.getContentResolver();

        str6 = str1; str7 = "android_id";

        String str2 = Settings.Secure.getString(str6, str7);

        str6 = str2; if (str6 != 0)
        {
            String str3 = isEmulator();

            str7 = str3; if (str7 == 0) break label186; } str6 = "emulator"; g = str4; str6 = "AdMobSDK"; str6 = "To get test ads on the emulator use AdManager.setTestDevices( n

        str6 = "AdMobSDK";

        int i6 = 3;

        int i2 = InterstitialAd.g.a(str5, i6);

        i6 = i2; if (i6 != 0) { localObject8 = "AdMobSDK"; localObject8 = new java/lang/StringBuilder; ((StringBuilder)localObject8).<init>(); str7 = "The user ID is "; Object

        Object localObject2 = ((StringBuilder)localObject8).append(str7); localObject8 = localObject2; Object localObject3 = ((StringBuilder)localObject8).toString(); localOb

        Object localObject8 = g; String str7 = "emulator"; if (localObject8 == str4);

        label186: Object localObject9;

        for (int i7 = 0; ; localObject9 = g) { return i7; int i4 = md5(i7); i7 = i4; g = i7; localObject9 = "AdMobSDK"; localObject9 = new java/lang/StringBuilder; ((StringBuilde

        )

        }

        public static boolean isEmulator()
        {
            String str2 = "generic"; String str3 = "unknown"; String str4 = Build.BOARD; String str1 = str3.equals(str4); str3 = str1; if (str3 != 0) { str3 = "generic"; str3 = Build
```

Find: android_id

Next Previous Case sensitive

10:20 AM



POSTED: APRIL 15, 2:32 PM ET | By SCOTT STEINBERG

Pandora Responds to Claims That Its Online Service Violates User Privacy

Recommend 2 recommendations. Sign Up to see what your friends recommend.



As discussed in an [earlier post](#), security firm Veracode alleges that online streaming music service provider Pandora has been secretly sharing users' information, including age, gender and location, with digital advertising firms.

In response to these accusations, the popular Internet radio service is removing third-party advertising platforms, including Google, AdMeld and Medialets. Despite insisting it has found zero evidence to support the charge that these companies acted beyond the confines of its ad policy, the company hopes to mollify fans by taking a proactive stance. New versions of its smartphone and mobile device apps lacking

support for these services are planned for free download via the Android Market and the Apple App Store soon.

Share Tweet 17

One
week
later...



<http://www.rollingstone.com/culture/blogs/gear-up/pandora-responds-to-claims-that-its-online-service-violates-user-privacy-20110415>

Privacy?



Here are Some Numbers...

53,000 - # Of Applications Analyzed

~48,000 Android Market

~5,000 3rd Party Markets

3 Average Number of Permissions Requested

117 Most Requested for Single Application

Permissions Requested

24% GPS information (11,929)

8% Read Contacts (3,626)

4% Send SMS (1,693)

3% Receive SMS (1262)

2% Record Audio (1100)

2% Read SMS (832)

1% Process Outgoing Calls (323)

.5% Use Credentials (248)

And Even More Numbers...

Total Third Party Libraries: ~83,000

Top Shared Libraries

- 38% com.admob (18,426 apps)
- 8% org.apache (3,684 apps)
- 6% com.google.android (2,838 apps)
- 6% com.google.ads (2,779 apps)
- 6% com.flurry (2,762 apps)
- 4% com.mobclix (2,055 apps)
- 4% com.millennialmedia (1,758 apps)
- 4% com.facebook (1,707 apps)

Code Reuse

Outsourcing

Third Party Libraries

Most Code Is

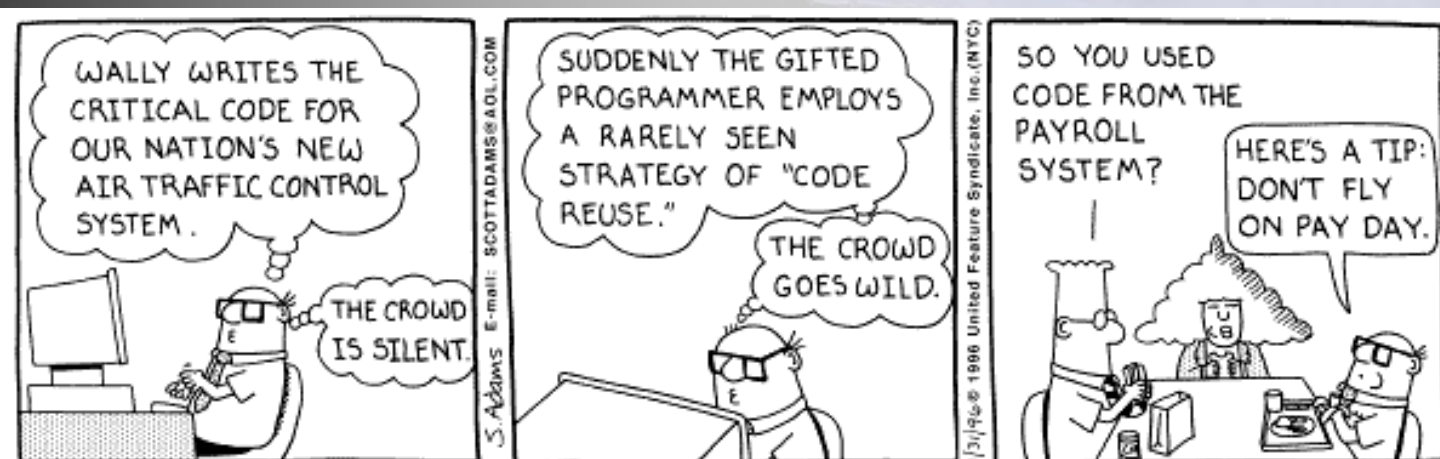
Reused

Outsourced

3rd Party Libraries (with source)

3rd Party Libraries (binary format)

Nobody really knows what their code does!



Risk Transference

Your code
Your libraries
Outsourced code
3rd party libraries
Purchased code
COTS code

Contract your vendors
to do the same

I'll Accept that Risk!

Pass it on over..

Joe Brady
jbrady@veracode.com

Tyler Shields
tshields@veracode.com
txs@donkeyonawaffle.org
@txs

Summary

Mobile Security Lessons

Mobile Applications
Are High Risk

Malicious Mobile
Code

Case Studies

No Hardcoded Passwords

Encrypt Data In Transit

Secure Data At Rest

Analyze Security of ALL
Code

(Includes Code Reuse)

Privacy
Only Take What You
Need

Honest With Your
Users

Wary of Risk
Transference