Android WebKit Development: A cautionary tale

Joe Bowser
Nitobi
E-Mail: joe.bowser@nitobi.com
About this talk

- This talk is not explicitly about PhoneGap
- This is a technical talk
  - It is expected that you have looked at the Android SDK (ApiDemos, Hello World)
  - This will make more sense if you have gone to the other PhoneGap talks today as well
- There will be screenshots
- This won't be just a rant! (I promise)
- This won't be an Apple Fanboy Talk
About the Speaker

- First commit on PhoneGap-Android
- Did minor work on other Open Source Projects
- Worked with Android since 2008 (Version 1.0, T-Mobile G1 release days)
- Co-founded Vancouver Hack Space (hackspace.ca)
- Currently still work with PhoneGap (I do dogfood my stuff), but also work with the ADK and other Hardware-Related stuff on my spare time
- I definitely do NOT work for Google, I just get to hear people's complaints about the Android Browser
- All my experiences with this are from OUTSIDE Google
- I feel your pain!!!
Android Web Development

- When someone develops a mobile web app, they will have to deal with the Android Browser.
- Android Browser is an application that is different on EVERY SINGLE device released by a manufacturer.
- Android Browser handles copy/paste functionality, dialog boxes, text boxes, “Native-Style” UI.
- Android Browser is written in Java and is the visible app for users.
FAIL

Acid3

100/100

To pass the test, a browser must use its default settings, the animation has to be smooth, the score has to end on 100/100, and the final page has to look exactly, pixel for pixel, like this reference rendering.
But doesn't Android use WebKit

- Android DOES use WebKit, through Android Browser
- WebKit is NOT a browser
- WebKit is NOT written in Java
- WebKit can't create Dialog Boxes or any of the other Native UI elements
  - Webkit can render HTML and Javascript, but these are NOT consistent with the look and feel of Android's UI
- WebKit renders graphics in a completely different way than the rest of Android, and these graphics are pushed onto a surface for Java applications to layer components over top of
What is WebKit?

- From webkit.org:
  - Webkit is a modular open source browser engine, but it is NOT A BROWSER
  - WebKit is a fork of KHTML, and is used everywhere
    - Android, iOS, Blackberry OS 6, Chrome, Safari, etc
  - WebKit is written in C++
  - WebKit is NOT the solution to every problem
Android Layer Cake
Android Browser's Cake

- The world of Android WebKit looks something like this
- WebKit displays pages using the Android WebView
- WebView is a complex view that consists of other views
- The implementation of WebView directly influences how WebKit interacts with the Android UI
- It is often not clear where the differences between WebView end and WebKit begin, making issues with Android WebView and Android WebKit harder to track down
- Android WebView is part of the Android Apache source, Android WebKit is LGPL/MIT
But I'm writing Web Apps?

- Writing Web Applications using HTML, CSS and Javascript can get most applications done very quickly
- The applications have to use whatever version of WebKit is on the Android Device
- Every Manufacturer has a different implementation of webkit that are optimized for their device
- Every device released has a slightly different version as well
- Buying every device on the market is prohibitively expensive and many companies have cashed in on this fact with their own solutions
  - Some companies provide Device Rental
  - Device Anywhere
Common complaints about Android and WebKit
Serious Differences

- **Android Versions**
  - Old Android 1.x issues
    - Touch Events don't exist
    - No Storage by default
  - Android 2.1+
    - No REAL Multi-Touch (very glitchy, works in serial, crashes device)
  - Android 2.3 doesn't have a working addJavascriptInterface
  - Android 3.0+ can't handle “#” or “?” in some URLs (Seriously)

- **Manufacturer Differences**
  - HTC phones don't have a working console.log
  - HTC, Samsung and Motorola all have their own copy-paste behavior

- Different screen sizes between devices
What about testing?

- Android has the Compatibility Test Suite (CTS)
- The CTS covers Android, but does not cover WebKit
- The CTS tests don't appear to make or break whether a device is released, but do determine whether it's a Google Branded Device
- CTS may be why there's no low-end Android 2.3 devices
  - Low-RAM devices uses the JSC Javascript Engine instead of V8, which breaks the WebKit bridge, which allows developers to hook Java objects as Javascript Globals
  - CTS 2.3 has a test for the method addJavascriptInterface, which uses the WebKit bridge
Android is open source, how about fixing it

- Android Open Source Development is HARD
- Android does have a way to commit bug fixes (gerrit)
- WebKit is WebKit
  - Very different than Mozilla and other more developer-friendly projects (no good “First Bug” tags)
  - It IS possible to fix bugs in WebKit, but it's very difficult to track WebKit development
- A good place to start if you go down this path are the Google Groups
  - Android-Building : How to build the AOSP
  - Android-Platform : Discussions on what should be changed in the Android Platform
How do we, as Application Developers deal with all of this?

- Test on as many different devices as possible
- The Android Emulator (as slow as it may be) is your friend with these bugs
  - Sony Ericsson (developer.sonyericcson.com)
  - Samsung (Galaxy Tab only, through the Android manager)
  - Motorola (developer.motorola.com)
  - LG (through Android Manager)
  - Kyocera (through Android Manager)
- Use tools like weinre
- Avoid CSS 3D Transforms – They STILL don't work (as of Android 3.1)
Will it get better?

**Issue 7589: Android dev team ignores its own bugtracker**

160 people started this issue and may be notified of changes.

**Status:** Unassigned

**Owner:**

This bugtracker is seriously underused. Issues reported here are stagnant and receive hardly any attention.

Users are ignored and no communication is happening.

And most importantly: Errors reported here are never worked on or even fixed.

Please describe the problem in detail. Be sure to include:

- **Steps to reproduce the problem.**
  Find a bug in Android.
  Confirm it is already known in this database.
  Marvel in disbelief at the <100 comments and <100 stars and its age >> 1 year.
  Wonder why the bugtracker exists in the first place if none of the developers bother to do anything about the bugs.
  Wonder if anyone at google actually cares about their users.
  Star the item in the vain hope to get it recognized and fixed.

- **What happened.**
  nothing.

- **What you think the correct behavior should be.**
  The bug is assigned to a developer, fixed and rolled out in the next version.

**Comment 1** by project member bad_@android.com, Apr 7, 2010

If you would like us to work on a bug, please use the following process:

1. Describe the bug or desired feature in as much detail as you possibly can.
2. Explain, again in as much detail as you possibly can, just how device the presence of the bug or absence of the feature is. Expressions of disbelief will enhance our understanding.
3. If appropriate, threaten to initiate a class-action lawsuit. Actually, I’m just kidding -- it’s always appropriate to threaten lawsuits.
I believe that one day it will

- There are various bugs in the tracker that I think should be fixed:
  - 17485 – Poor performance of WebView (3D CSS Transforms)
  - 12987 – Javascript to Java Bridge throws Exceptions on Android 2.3
  - 16312 – addJavascriptInterface: no type checking
  - URLs should be rock-solid (should not break the browser if you use a ? or a # in it)

- There are features that I would like to see
  - Running Javascript from Java (webView.loadUrl("javascript: foo()") is considered harmful)
Success

- Success from outside developer influence
  - Android Web Applications section added due to large number of PhoneGap applications
  - Android SQLite Storage Added in Android 2.1
  - Android DOM storage added shortly after
- Successful patches to WebKit
  - Android accepts patches from 3rd Parties
  - Android WebKit development is out in the open
  - Android Browser is still a part of the Apache-Licenced closed dev model
WebKit Gerrit

<table>
<thead>
<tr>
<th>ID</th>
<th>Subject</th>
<th>Owner</th>
<th>Project</th>
<th>Branch</th>
<th>Updated</th>
<th>V</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>1acafsca</td>
<td>Fix missing nil</td>
<td>Bruce Beaugrand</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>May 12</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1bb534ab</td>
<td>Remove unused function that relies on an obsolete API (MERGED)</td>
<td>Jean-Baptiste Queyrat</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>May 12</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1af3234d</td>
<td>Port toward newer versions of skia, (MERGED)</td>
<td>Jean-Baptiste Queyrat</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>May 12</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1af44ebd</td>
<td>&quot;No to fix Safari (MERGED)</td>
<td>Jean-Baptiste Queyrat</td>
<td>platform/external/webkit</td>
<td>master (fixSafari/noS)</td>
<td>May 12</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1afdf31f</td>
<td>Switch to SA/SafeUnref for better portability, (MERGED)</td>
<td>koan-sin tan</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>May 12</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>15f303be</td>
<td>WebP (R81223): Fix build with GCC 4.6</td>
<td>Joao de Almeida</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Apr 29</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1e7745f7</td>
<td>Don’t use deleted Node object in serialize/Script/WidthAndScale</td>
<td>Johan Rosentwig</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Apr 8</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1d06c0669</td>
<td>3D keycorder, add</td>
<td>LGD AOSP</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Feb 23</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1d394401f</td>
<td>3D keycoder Add</td>
<td>LGD AOSP</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Feb 17</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1d394401f</td>
<td>Enable filter selections to be rendered correctly even at small sizes,</td>
<td>Harold Baier</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Dec 19</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1e89222c4</td>
<td>Allow scrolling of frameworks even when refreshing is enabled</td>
<td>Harold Baier</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Dec 29</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>17ff08279</td>
<td>Fix compilation error, (MERGED)</td>
<td>Rens Bolderd</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Dec 1, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1a82e25e5</td>
<td>[Project][Branch][Component] Summary (ABANDONED)</td>
<td>Rain Chen</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Dec 1, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1900c78b1</td>
<td>[Project][Branch][Component] Summary (ABANDONED)</td>
<td>Rain Chen</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Dec 1, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1a8f6a4e1</td>
<td>[Project][Branch][Component] Summary (ABANDONED)</td>
<td>Rain Chen</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Nov 1, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1a95e5357</td>
<td>Reverse crash fix caused by incorrect reference counting leading</td>
<td>Sagar Shek</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Sep 10, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1b6d41c8e</td>
<td>Map fix 2337068: &lt;code&gt;URL&lt;/code&gt; + &lt;img&gt; URL = URL that starts</td>
<td>Melanie Clements</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Aug 31, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1bff3e368</td>
<td>Map fix 2337068: &lt;code&gt;URL&lt;/code&gt; + &lt;img&gt; URL = URL that starts</td>
<td>Melanie Clements</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Aug 30, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1d72f4e2d</td>
<td>Properly define LOG TAG in v8iesting</td>
<td>Jim Huang</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Aug 25, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1769a225e5</td>
<td>Merge runtime branch into and webkit (ABANDONED)</td>
<td>Melanie Clements</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Aug 20, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1a5f0a4e0</td>
<td>activeDocumentLoader( ).cause Crash in WebCoreFrameBridge.cpp (MERGED)</td>
<td>Kenneth Anderson</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Aug 17, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1b72f7dfe4</td>
<td>Fix missing NIL (MERGED)</td>
<td>Bruce Beans</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>Jul 6, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1b6f86d12</td>
<td>Check for the absence of a frame. This crashes in the situation where</td>
<td>Jean-Baptiste Queyrat</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>May 15, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1ff8d0d46</td>
<td>A leak in RenderTheme/Android, (ABANDONED)</td>
<td>Julien Chafflaix</td>
<td>platform/external/webkit</td>
<td>master</td>
<td>May 17, 2010</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
How do I make the Mobile Web better

- Write more code – Work on PhoneGap, writer Apps, work on WebKit directly
- Use PhoneGap and other Web Technologies when appropriate
- Write tests and show them to people. Writing comments like “This doesn't work” isn't as helpful as explaining why and showing a stack trace
- Remember that while some parts of HTML5 code for the iPhone won't work on Android, that code will work properly on the iPhone
- Don't Give Up
If I wanted to hack on Android WebKit, how would I do it

- DISCLAIMER: I have not committed ANY code to WebKit, I only got this working a few months ago
- This will be a step-by-step guide to debugging WebKit on the AOSP
- This will be based on Screenshots, because I can't guarantee that the AOSP will compile, or that it will run (I do not work for Google)
- There are probably far better ways to do this, this is the way that I've pieced together from reading the Google Groups
- Make sure that you have a proper build setup first before doing this, otherwise you will spend hours chasing down build dependencies
- See source.android.com for more information
Step One: Get the Source code for AOSP

- Setup build environment (Ubuntu 10.04 works best)
- Install Dependencies
- See source.android.com for more info

```
repo init -u git://android.git.kernel.org/platform/manifest.git
repo sync
```
Step Two: Edit the buildspec.mk

- Copy the file from build/buildspec.mk.default to buildspec.mk (in the root directory of your AOSP build)

- Edit the file and add the following:
  
  DEBUG_MODULE_libwebcore:=true
  DEBUG_MODULE_libxml2:=true
  TARGET_CUSTOM_DEBUG_CFLAGS:=-O0 -mlong-calls
  ADDITIONAL_BUILD_PROPERTIES += debug.db.uid=100000

- This allows WebKit to be built in DEBUG mode
Step Three: Edit the Android.mk in external/webkit

- This is VERY IMPORTANT
- Your AOSP build will break if this is not done, since libwebkit will be huge with debugger symbols
- Uncomment this line:
  ```
  LOCAL_PRELINK_MODULE := false
  ```
Step Four: Build the Project, take a nap

- Run the following in the root directory:
  ```
  source build/envsetup.sh
  lunch full-eng
  make -j2 # Note: The more cores you have, the faster this will run
  ```
- This will take a very long time on most systems
Step Five: Start the Emulator

- Set the ANDROID_PRODUCT_OUT variable
  
  ```
  export ANDROID_PRODUCT_OUT="/home/(username)/aosp-official/out/product/generic/
  ```

- Start the emulator
  
  ```
  emulator
  ```
Step Six: Run a WebKit Application

- I like running PhoneGap
- I run PhoneGap in Eclipse because I'm a n00b who can't use Command-Line debugger tools for Java
- This is identical to the standard workflow for debugging a Java application
  - See developer.android.com for more info on how to do this
- To check out PhoneGap Android, use git and check this out:
  
git clone git://github.com/phonegap/phonegap-android.git
Step Seven: Hook up a Java Debugger to the Java Application

- This is the same thing as debugging a Java Application in Android
- Set your breakpoints in Eclipse
- Then instead of running your Android Application, Debug your Android Application
- See [http://developer.android.com](http://developer.android.com) for more details on how to do this
Step Eight: Hook up a C Debugger to WebKit

- Run the following command on your computer:
  adb forward tcp:5039 tcp:5039

- Run the following command on your running emulator:
  gdbserver 10.0.2.2:5039 --attach pid

- Run the following commands in gdb/ddd:
  ```
  set solib-absolute-prefix /home/(yourdir)/aosp-official/out/target/product/generic/symbols
  set solib-search-path /home/(yourdir)/aosp-official/out/target/product/generic/symbols/system/lib
  file /home/(yourdir)/aosp-official/out/target/product/generic/symbols/system/app_process
  ```
If you're successful, and you use old tools like DDD....
Obviously, most people won't bother to do this, but..

- This can give you a solid understanding of how WebKit works on the phone
- There are easier ways to do this, but showing a debug screen of WebKit impresses people
- This is how to debug WebKit, not V8 or any of the other libraries you can plug into WebKit
- This only works on a stable AOSP branch (Gingerbread), edge has WebKit built against proprietary Honeycomb source
- Even though I can do this, I don't really have any idea what is going on past this point
  - This could probably be made easier by using an Eclipse C/C++ debugger
  - I'd rather learn more gdb/ddd skills
Summary

- Web Development is easy
- Developing the fundamental tools required for the Web Development Ecosystem to exist is HARD
- Haters need to stop hating! Every time you get frustrated with WebKit bugs, attempt this process
- Android WebKit has different versions, but phone manufacturers know this and often provide emulators of the builds that they ship
- It's not always WebKit’s fault on Android (in fact, it is very rarely WebKit's fault, it could be JSC, or Android Browser or the other components of WebKit)
- Keep Calm and Carry On
Questions?