A Browser Developer's Research Wish List

Robert O'Callahan
Mozilla Corporation
About Me

- Research career
- Mozilla career
  - Contributor
  - Developer
  - Manager
• A very quick overview of Mozilla development
• Problems that need research attention
Browsers Are Hard

HTTP  HTML  CSS  JPEG
DOM  JS  NPAPI  XML
HTML5  CSS3  Opentype  SVG
XSLT  XPath  WebM  IndexedDB  WebSockets
WebApp  MathML  WebGL  WebWorkers  SMIL
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 1</title>
<link REL="stylesheet" HREF="soccer.css" TYPE="text/css">
</head>
<body style="background-attachment: fixed" background="images/puyesl_08.gif">
<p>&nbsp;</p>
<p>&lt;p&gt;&lt;font size="3" face="Tahoma">Welcome To</font>&nbsp;&lt;/b&gt;&lt;/font&gt;&lt;b&gt; &lt;/b&gt;&lt;/p&gt;
&lt;p&gt;&lt;font color="#FF0066" size="5" face="Tahoma">POMONA UNITED YOUTH SOCCER LEAGUE</font&gt;&lt;/p&gt;
&lt;p&gt;&lt;font size="3" face="Tahoma">Weekly news : Updated AGOSTO 26, 2008 &lt;/font&gt;&lt;b&gt;&lt;br&gt;&lt;/b&gt;&lt;/p&gt;
&lt;p&gt;&lt;font color="#FF0066" size="6" face="Tahoma">NO HABRA JUEGOS PARA LABOR DAY WEEKEND!!!!!</font&gt;&lt;/p&gt;
&lt;p&gt;&lt;font color="#FFFF00" size="6" face="Tahoma">***ENTRENAON DE LA SELECCION DEL 98</font&gt;&lt;/p&gt;
Browsers Are Hard

- Severe performance requirements
- Severe security challenges
Browsers Are Hard
Mozilla

- Nonprofit
- Relatively small (~300 FTE)
- Large community
- > 300M users (~25% worldwide)
- Long-ish history (to 1998 and earlier)
Code

- C: 0.88M lines (many third party libs)
- C++: 1.5M lines
- .h: 0.98M lines
- JS: 0.19M lines
Being Open

• Making it easy for anyone to contribute to any level means opening everything online
  • Code
  • Data, e.g.
    – Bugs
    – Crash data
    – Test farm data
  • Decision-making

• Need to be distributed

• Need low barriers to entry
Distributed Version Control

- Mercurial (hg)
  - Like git
- Mercurial Queues (mq)
- Make it easy to factor work into many logically separate changes
Patch Lifecycle

- Bug filed in bugzilla.mozilla.org (including for new features)
- Patch attached, discussed, and formally reviewed
- Checkin, close bug
Automated Tests

- Multiple test frameworks
- Correctness and performance
- Run on every "push"
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thu Jun 3</td>
<td>16:46</td>
<td>Bug 563878. Part 4. Add AppUnitsPerDevPixel for 83d0a0f602c1f32d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thu Jun 3</td>
<td>16:46</td>
<td>Bug 563878. Part 3. Fix FindViewContaining. r=mckee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thu Jun 3</td>
<td>16:46</td>
<td>Bug 563878. Part 2. Some view/ clean-up. r=mc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thu Jun 3</td>
<td>16:46</td>
<td>Bug 563878. Part 1c. Misc layout cleanup. r=mc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thu Jun 3</td>
<td>16:46</td>
<td>Bug 563878. Part 1b. Make nsIContextManager. r=mc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thu Jun 3</td>
<td>16:46</td>
<td>Bug 563878. Part 1a. Make nsIWidget. r=mc</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Test Results**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS X 64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Bug 535358**

- s: talos-r3-fad64-037
- 1089 ERROR TEST-UNEXPECTED-FAIL | /tests/browser/base/content/test/test_contextmenu.html | checking item #10 (context-selectall) enabled state - got false, expected true

**Rev3 Fedora 12x64 mozilla-central opt test mochitests-1/5**

- test Started: 17:37
- finished: 17:44, took 7mins
- mochitest-plain-1: 63404/1/815

**View Brief Log**
**View Full Log**
**Add a comment**
Try-server

- “Push to try”
- Very heavily used
<table>
<thead>
<tr>
<th>Status</th>
<th>Build</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bo</td>
<td></td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Bd</td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Co</td>
<td></td>
<td>(12345 oth)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Build</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bo</td>
<td></td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Bd</td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Co</td>
<td></td>
<td>(12345 oth)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T</td>
</tr>
</tbody>
</table>

me@kylehuey.com - Sun Jun 6 00:06:55 2010 (compare: □)

<table>
<thead>
<tr>
<th>Status</th>
<th>Build</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bo</td>
<td></td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Bd</td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Co</td>
<td></td>
<td>(12345 oth)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Build</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bo</td>
<td></td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Bd</td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Co</td>
<td></td>
<td>(12345 oth)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T</td>
</tr>
</tbody>
</table>

eakhgari@mozilla.com - Sat Jun 5 23:48:59 2010 (compare: □)

<table>
<thead>
<tr>
<th>Status</th>
<th>Build</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bo</td>
<td></td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Bd</td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Co</td>
<td></td>
<td>(12345 oth)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Build</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bo</td>
<td></td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Bd</td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Co</td>
<td></td>
<td>(12345 oth)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Build</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
<th>OS</th>
<th>Status</th>
<th>Date</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bo</td>
<td></td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Bd</td>
<td></td>
<td>(12345 oth)</td>
<td></td>
<td>Co</td>
<td></td>
<td>(12345 oth)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T T</td>
<td></td>
<td></td>
<td></td>
<td>T T T T T T</td>
</tr>
</tbody>
</table>
Fuzz Testing

- Best bug-finding methodology so far
- Skilled operators
- Automated reduction
Adding Value To Tests

- Assertions
  - Debug only
- Leak detection
- Valgrind
- Race detection (hasn't worked?)
- Combined concrete/symbolic execution?
Crash-Stats

- Google Breakpad
- [http://crash-stats.mozilla.org](http://crash-stats.mozilla.org)

- Long tail of low frequency, non-reproducible, inexplicable crashes
  - Sometimes due to environmental differences
  - Correlate environmental factors with crashes
    - E.g., list of loaded DLLs
  - Malware
Dehydra

- GCC plugin for AST-level access
  - Custom checkers written in JS
    - e.g. “override”
  - Dead code detection
  - Syntax-aware source code browsing (DXR)
- Refactoring using Pork (based on Elsa)
  - Renaming
  - Not much used
A Wish List
Performance Analysis
Performance Analysis

- Reduce noise
- Find significant metrics
  - e.g. instruction counts, cache misses
- Intelligent profile diffing
Nondeterministic Test Failures

--

tnikkel@gmail.com - 2010/06/05 14:51:30

Bug 513558

s: talos-3-fd64-037
1089 ERROR TEST-UNEXPECTED-FAIL | /tests/browser/base/content/test/test_contextmenu.html | checking item #10 (context-selectAll) enabled state - got false, expected true

Rev3 Fedora 12x64 mozilla-central opt test mochitests-1/5 [testStarted] 17:37, finished 17:44, took 7mins
  moztest-plain-1: 63404/1/815

Firefox - Tinderboxpushlog

http://tests.themasta.com/tinderboxpushlog/

firefox | Firefox3.6 | MozillaTry | more...

Timezone: local | MVT

Linux

Bo Bd Mo (1 2 3 4 5 oth oth) Md (1 2 3 4 5 oth oth) Co Co Cd Cd Ro Ro Rd Rd Jo Jo Jd Jd Xo Xo Xd Xd T T T T T T

Linux

Bo Bd Mo (1 2 3 4 5 oth oth) Md (1 2 3 4 5 oth oth) Co Co Cd Cd Ro Ro Rd Rd Jo Jo Jd Jd Xo Xo Xd Xd T T T T T T

Linux

Bo Bd Mo (1 2 3 4 5 oth oth) Md (1 2 3 4 5 oth oth) Co Co Cd Cd Ro Ro Rd Rd Jo Jo Jd Jd Xo Xo Xd Xd T T T T T T

Linux

Bo Bd Mo (1 2 3 4 5 oth oth) Md (1 2 3 4 5 oth oth) Co Co Cd Cd Ro Ro Rd Rd Jo Jo Jd Jd Xo Xo Xd Xd T T T T T T
VM Record And Replay

- It really works
- Best advance in debugging since …
- Need improvements
  - Overhead and reliability
  - “Always On”
  - Easy sharing
  - Application-specific extensibility (e.g. DumpJSStack())
- Combine with finer-grained R&R?
Static Analysis

• So far, no useful advanced generic analysis
• sixgill looks promising
  • Brian Hackett's PhD thesis
  • Low-annotation array bounds checking for C++
  • Works on Firefox
  • http://sixgill.org
Program Analysis And Code Review

- Unreported bugs in shipped code: low priority
- Bugs in new code: high priority
  - Regression bugs: highest priority!
- Code review is the one time we look at code to try to find bugs!
  - Use analyses to assist code review
  - Add analyses to try-server
  - Even false positives could improve review quality
  - Reviewer more likely to believe results?
Bug Finding

• Code review is a cheap time to fix bugs
• Finding a bug too late may mean it's not worth fixing
• Bug finding is not our bottleneck
  • Need to reduce cost of fixing bugs
  • (Potential) regressions are a big part of that cost
Verifying Refactorings

- DVCSs enable breaking up changes into small patches
  - Facilitates code review
  - Facilitates bisection search
  - We could use better tools for this!
- Many patches are (intended to be) behaviour-preserving refactorings
Verifying Refactorings

• Verify operational equivalence for refactoring patches
  • Check for performance effects?
• Tremendously useful because these patches consume review time
• Easy incremental research progress
• Easier and more important than automated refactoring
Code Complexity

- Simple, buggy code is better than complex, less buggy code
  - All code will need to be fixed and improved, and that will be easier for the simple code
- Less skilled developers write overly complex code
- “Is this patch the simplest possible change?”
- Depends on entire system
  - E.g. failure to reuse existing code
Programming Languages

- Finding and fixing mountains of bugs is not sustainable
- Need approaches that prevent classes of bugs
- At some point we will need to change to better languages
- Lots to say, but out of scope
Final Plea

- Do problem-driven research, not solution-driven research
- Help!
- Thanks for inviting me :-}