mozilla

Open Approaches to Secure Software

Window Snyder

Chief Security Something-or-Other

Overview

Who am I?

A security process tested by millions

Metrics, Transparency and Opacity

Security UI

Vendors listen to you

Window Snyder

Mozilla - Head of Security (or something)

security strategy, engineering, response, communication

Microsoft - Senior Security Strategist

worked with product teams to improve security

sign off for security for Windows XPSP2, 2003

engaged security community

@stake - Director of Security Architecture

created methodologies for app sec analysis

About Mozilla

Mozilla is...

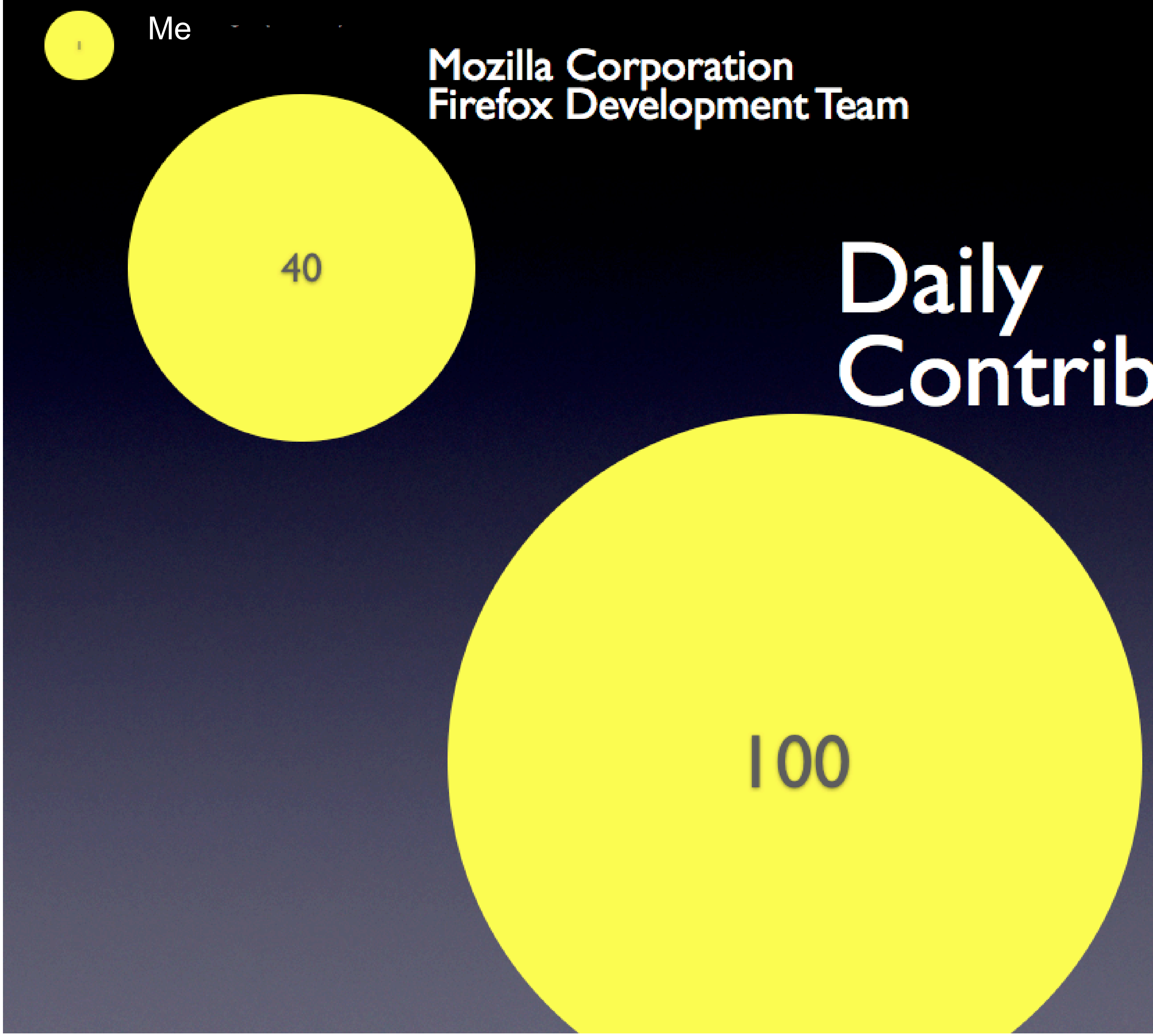
- a global effort to promote choice & innovation on the Internet
- the foremost advocate for users on the Web
- an open source project with thousands of code contributors and tens of thousands of non-code contributors
- home of the Firefox Web browser
- more than 100 million users worldwide

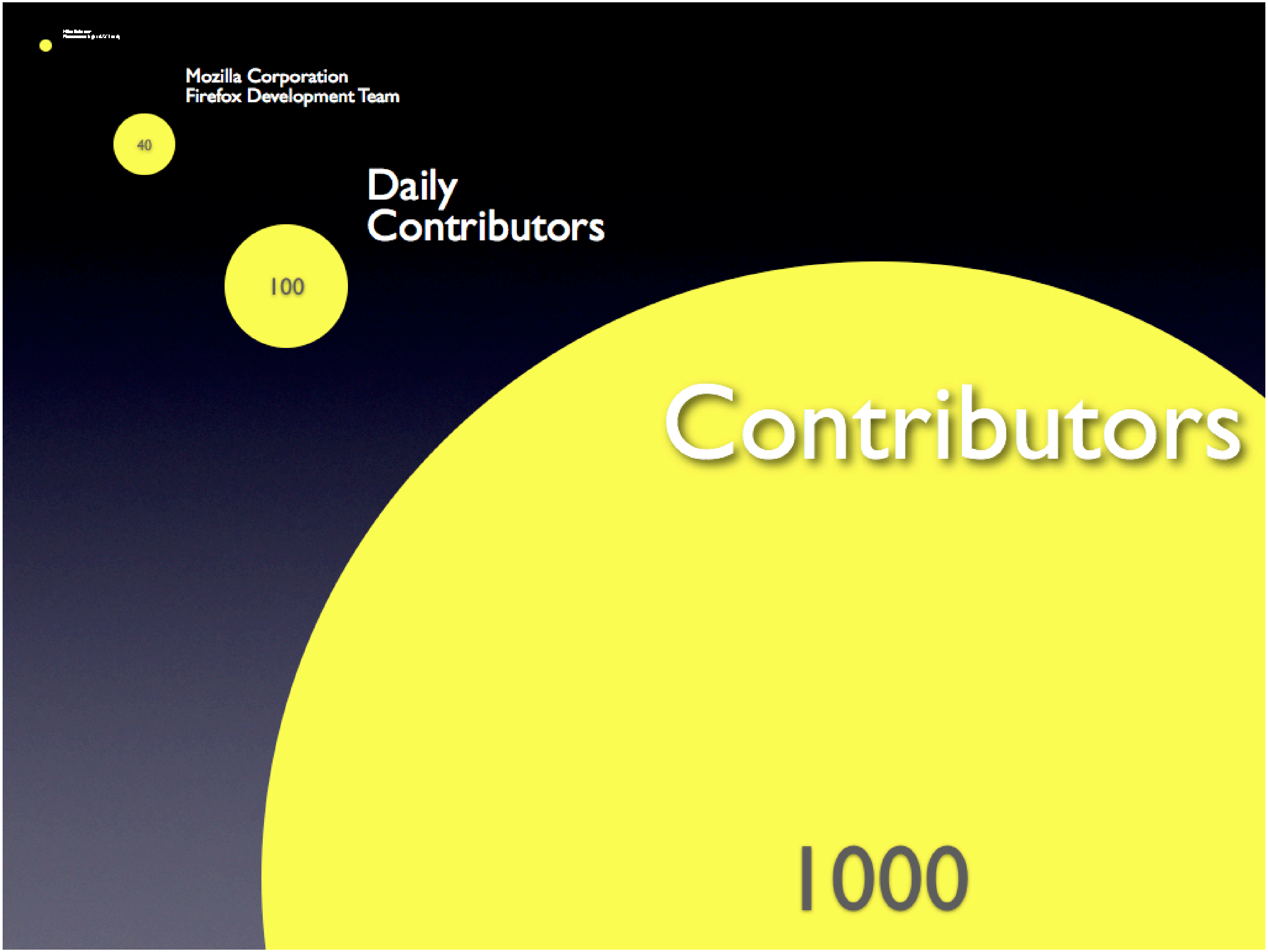
Me

Me

Mozilla Corporation
Firefox Development Team

Daily Contributors





Mozilla Corporation
Firefox Development Team

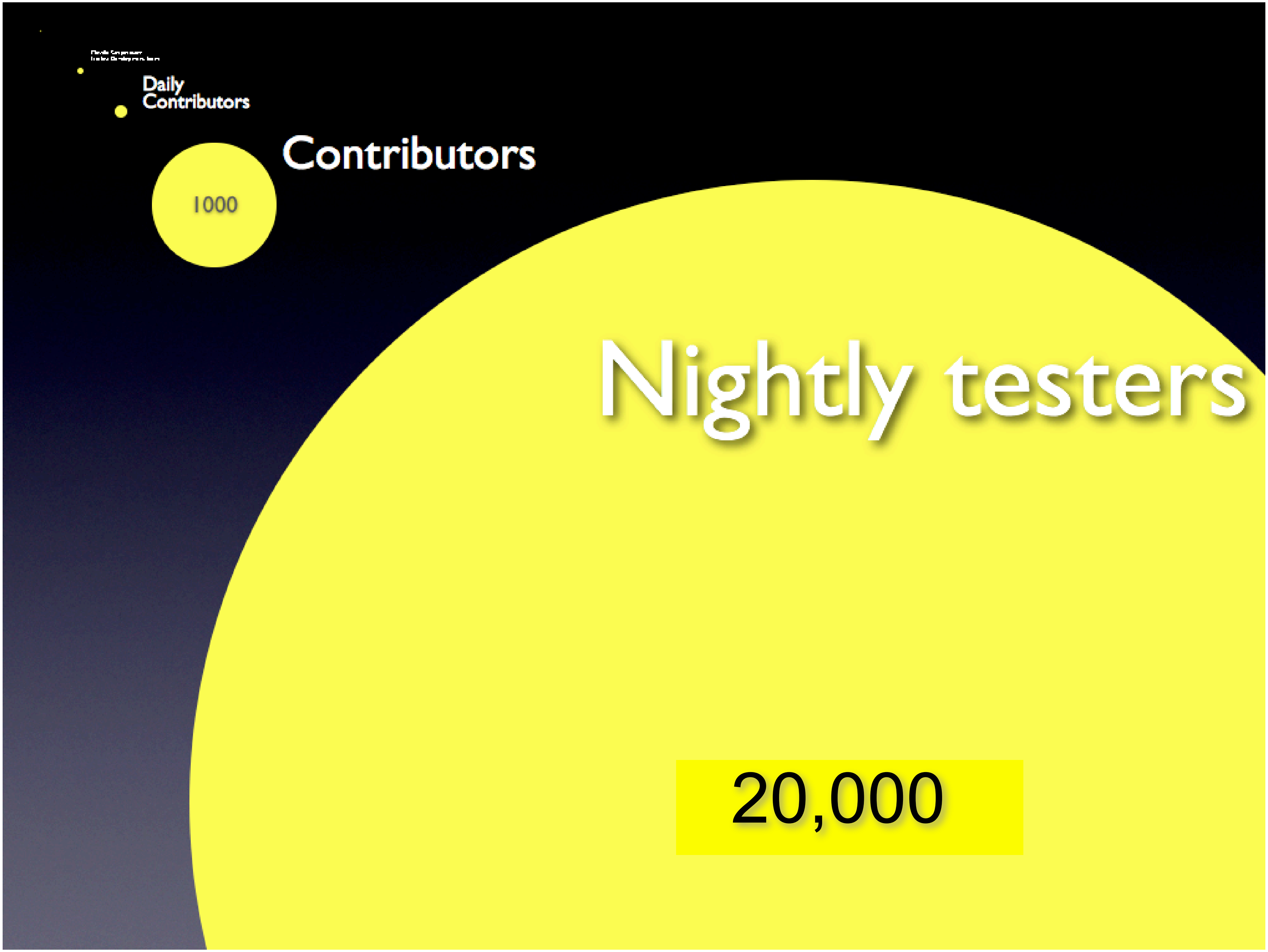
40

Daily
Contributors

100

Contributors

1000



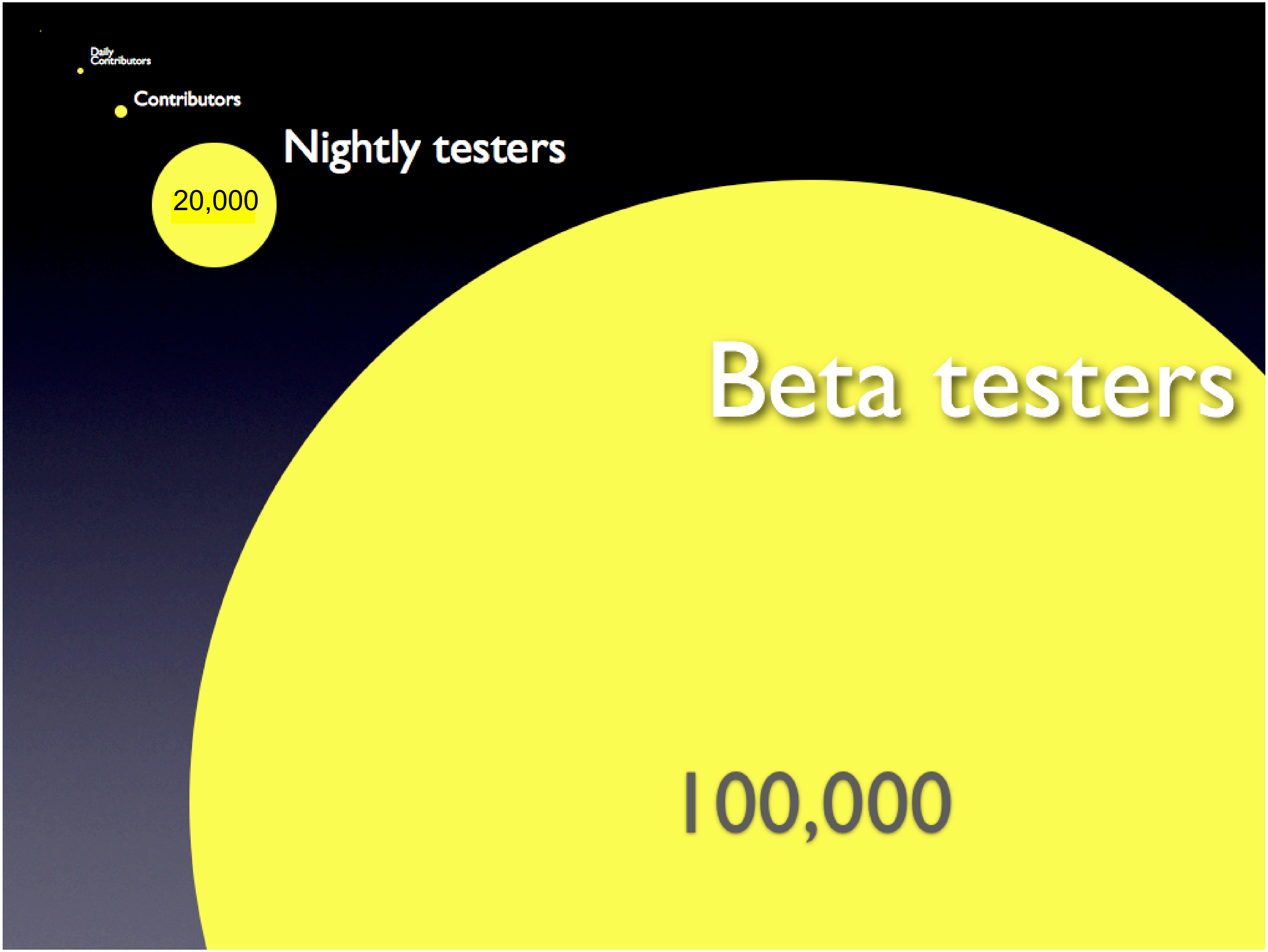
Daily Contributors

Contributors

1000

Nightly testers

20,000



Daily Contributors

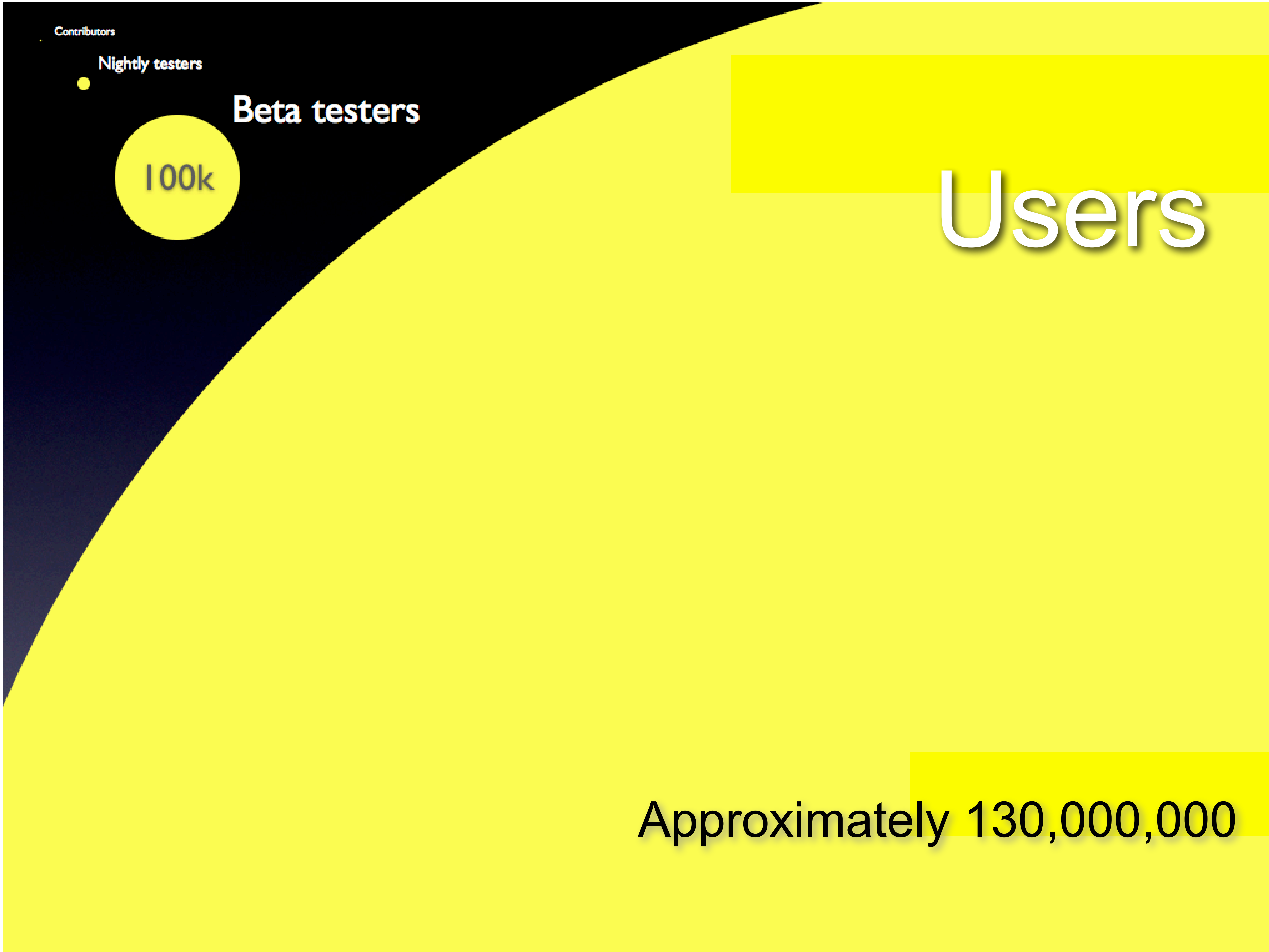
Contributors

Nightly testers

20,000

Beta testers

100,000



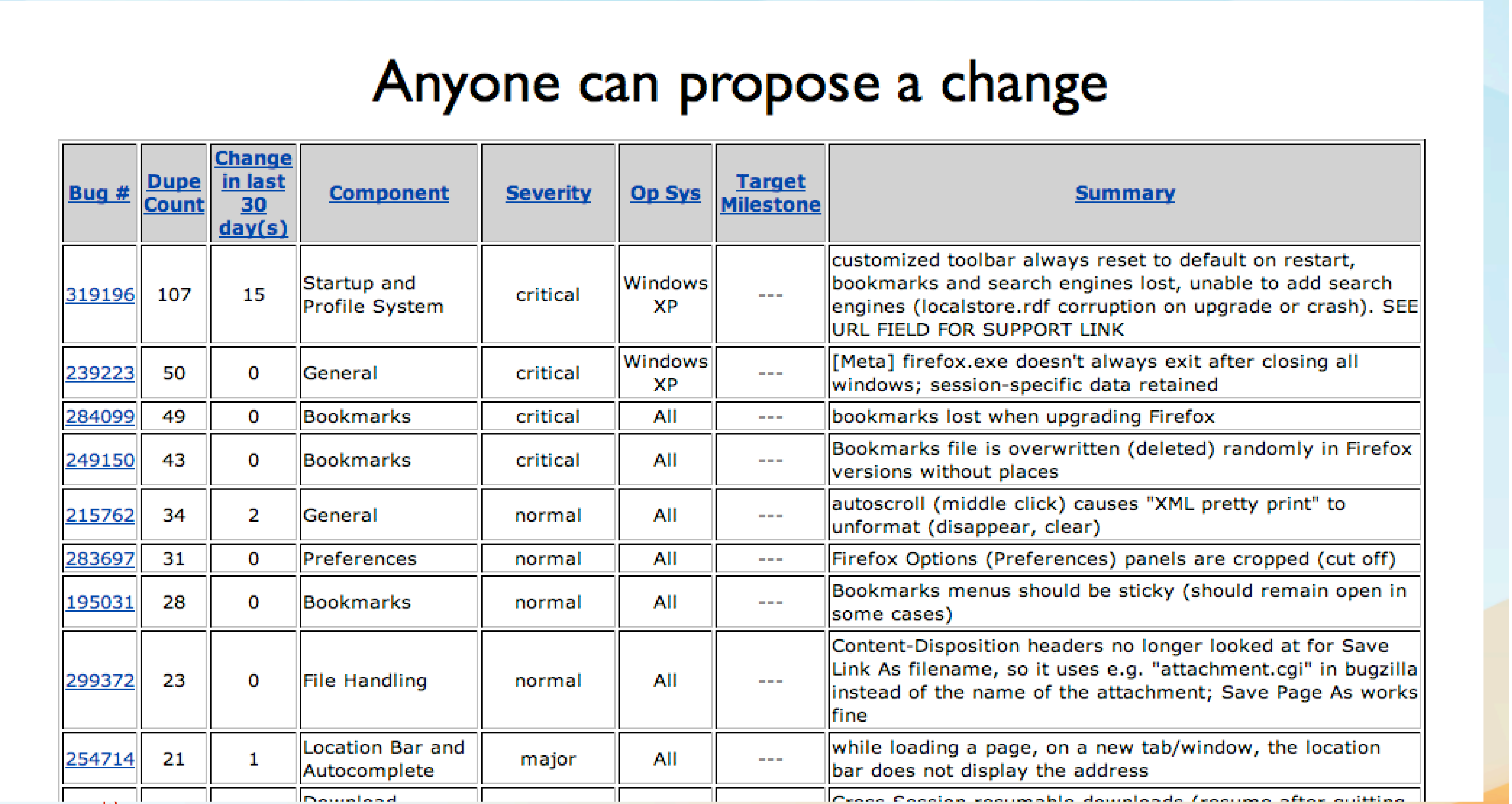
Users

Approximately 130,000,000

Aliens run Firefox…

(Market share numbers unavailable.)

How it all works…

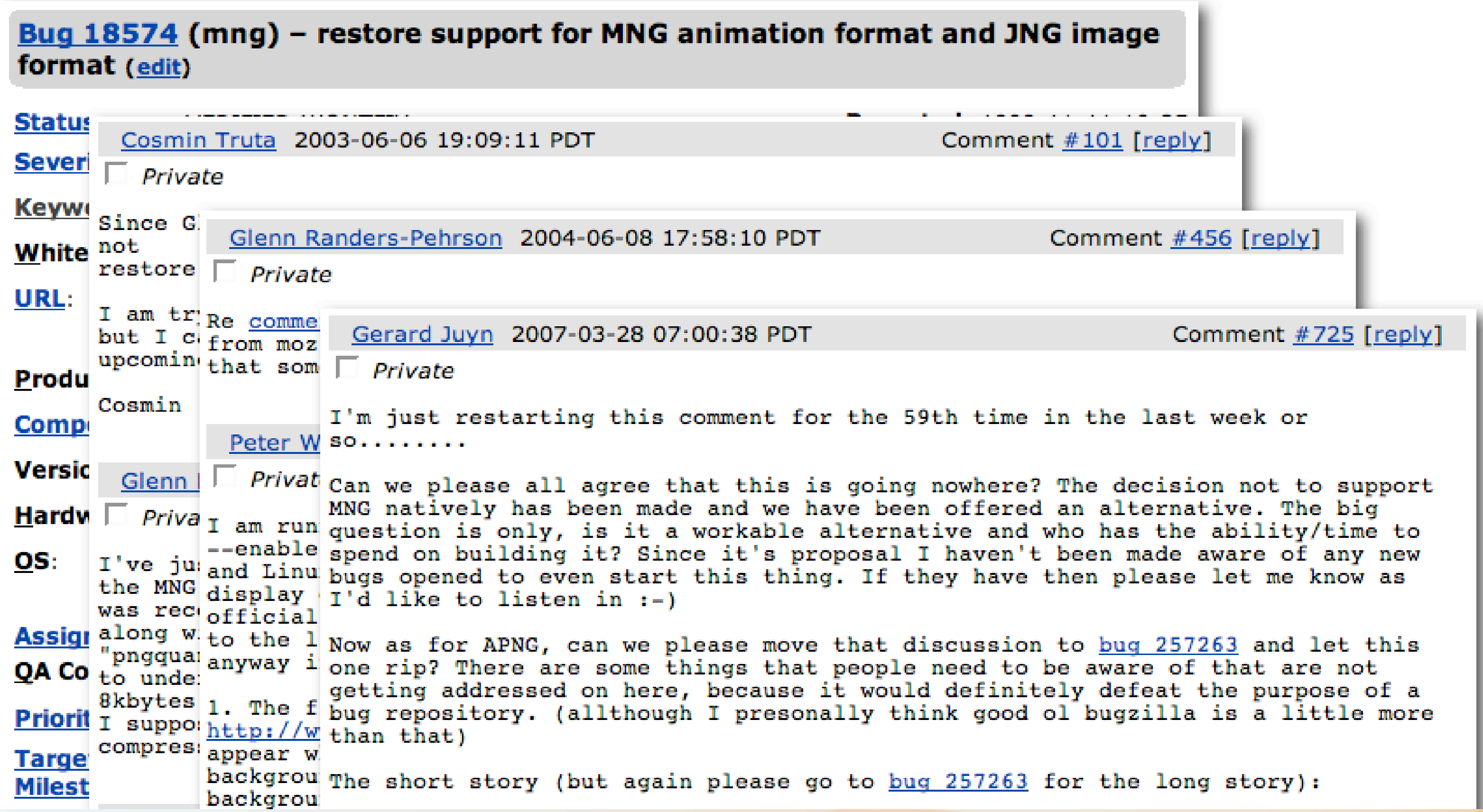


Anyone can propose a change

Bug #	Dupe Count	Change in last 30 day(s)	Component	Severity	Op Sys	Target Milestone	Summary
319196	107	15	Startup and Profile System	critical	Windows XP	---	customized toolbar always reset to default on restart, bookmarks and search engines lost, unable to add search engines (localstore.rdf corruption on upgrade or crash). SEE URL FIELD FOR SUPPORT LINK
239223	50	0	General	critical	Windows XP	---	[Meta] firefox.exe doesn't always exit after closing all windows; session-specific data retained
284099	49	0	Bookmarks	critical	All	---	bookmarks lost when upgrading Firefox
249150	43	0	Bookmarks	critical	All	---	Bookmarks file is overwritten (deleted) randomly in Firefox versions without places
215762	34	2	General	normal	All	---	autoscroll (middle click) causes "XML pretty print" to unformat (disappear, clear)
283697	31	0	Preferences	normal	All	---	Firefox Options (Preferences) panels are cropped (cut off)
195031	28	0	Bookmarks	normal	All	---	Bookmarks menus should be sticky (should remain open in some cases)
299372	23	0	File Handling	normal	All	---	Content-Disposition headers no longer looked at for Save Link As filename, so it uses e.g. "attachment.cgi" in bugzilla instead of the name of the attachment; Save Page As works fine
254714	21	1	Location Bar and Autocomplete	major	All	---	while loading a page, on a new tab/window, the location bar does not display the address
			Download				Cross Session resumable downloads (resume after quitting

How it all works…

Anyone can *comment* on a proposal for a change



Bug 18574 (mng) – restore support for MNG animation format and JNG image format (edit)

Status
Severi
Keyw
White
URL:
Produ
Comp
Versic
Hardw
OS:
Assigı
QA Co
Priorit
Targe
Milest

Cosmin Truta 2003-06-06 19:09:11 PDT Comment #101 [reply]

□ Private

Since G
not
restore

I am tr
but I c
upcomin

Cosmin

Glenn

□ Priva

I've ju
the MNG
was rec
along w
"pngqua
to unde
8kbytes
I suppo
compres

Glenn Randers-Pehrson 2004-06-08 17:58:10 PDT Comment #456 [reply]

□ Private

Re comme
from moz
that som

Peter W

□ Privat

I am run
--enable
and Linu
display
official
to the l
anyway i

1. The f
http://w
appear w
backgrou
backgrou

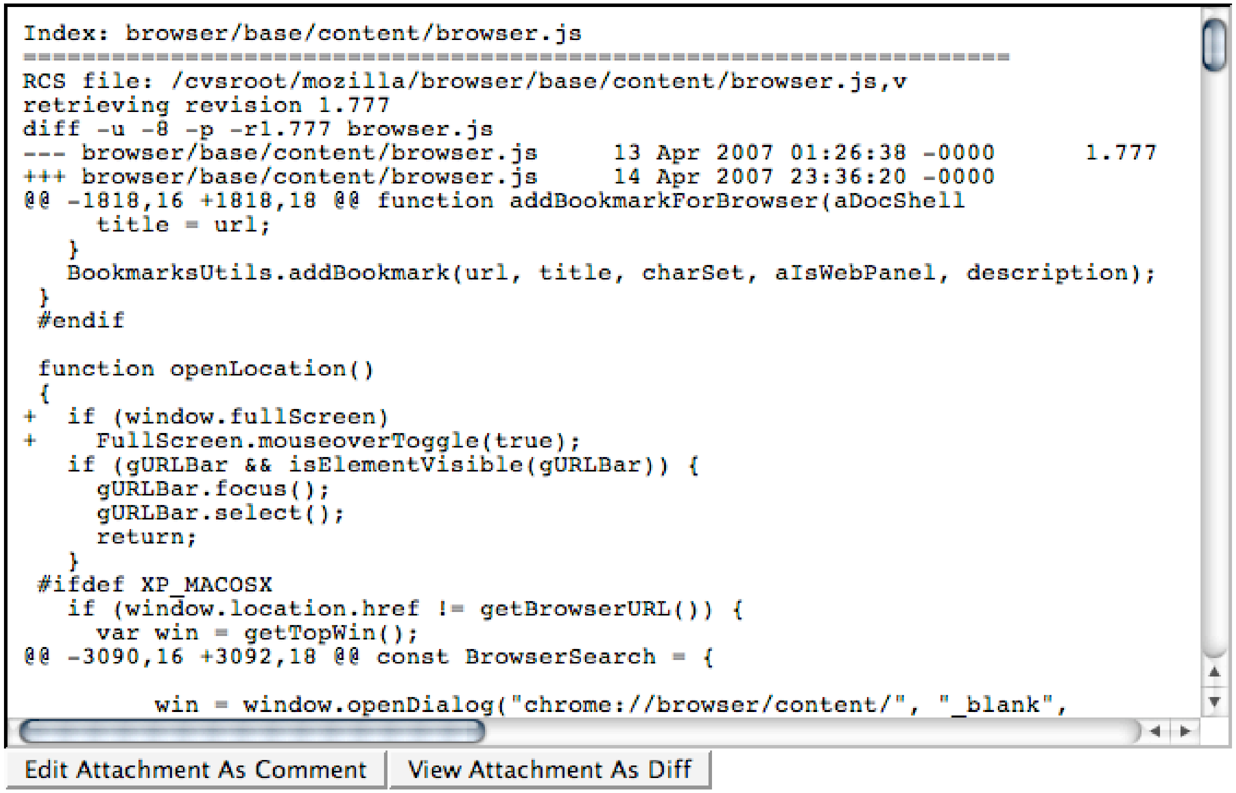
Gerard Juyn 2007-03-28 07:00:38 PDT Comment #725 [reply]

□ Private

```
I'm just restarting this comment for the 59th time in the last week or
so........

Can we please all agree that this is going nowhere? The decision not to support
MNG natively has been made and we have been offered an alternative. The big
question is only, is it a workable alternative and who has the ability/time to
spend on building it? Since it's proposal I haven't been made aware of any new
bugs opened to even start this thing. If they have then please let me know as
I'd like to listen in :-)

Now as for APNG, can we please move that discussion to bug 257263 and let this
one rip? There are some things that people need to be aware of that are not
getting addressed on here, because it would definitely defeat the purpose of a
bug repository. (allthough I presonally think good ol bugzilla is a little more
than that)

The short story (but again please go to bug 257263 for the long story):
```

How it all works…

Anyone can submit a change to the code



```
Index: browser/base/content/browser.js
===================================================================
RCS file: /cvsroot/mozilla/browser/base/content/browser.js,v
retrieving revision 1.777
diff -u -8 -p -r1.777 browser.js
--- browser/base/content/browser.js     13 Apr 2007 01:26:38 -0000      1.777
+++ browser/base/content/browser.js     14 Apr 2007 23:36:20 -0000
@@ -1818,16 +1818,18 @@ function addBookmarkForBrowser(aDocShell
     title = url;
   }
   BookmarksUtils.addBookmark(url, title, charSet, aIsWebPanel, description);
 }
 #endif

 function openLocation()
 {
+  if (window.fullScreen)
+    FullScreen.mouseoverToggle(true);
   if (gURLBar && isElementVisible(gURLBar)) {
     gURLBar.focus();
     gURLBar.select();
     return;
   }
 #ifdef XP_MACOSX
   if (window.location.href != getBrowserURL()) {
     var win = getTopWin();
@@ -3090,16 +3092,18 @@ const BrowserSearch = {

         win = window.openDialog("chrome://browser/content/", "_blank",
```

How it all works…

Not everyone can *approve* a change

Approach to Security - Transparency

- Community supports security testing and review efforts
- Code and developer documentation is available to anyone
- Security researches can spend their time in analysis and not in reconnaissance
- External parties can check our work, do not need to rely on what we tell them
- Design online, open meetings (MSFT takes great notes!)
- Real time updates on vulnerabilities

Security Process

Self-organizing Security Group is about 95 people representing all aspects of the community

Features are security reviewed to ensure compatibility with the overall security model

Designed with security in mind

Security testing is continuous throughout development process

Security updates every 6-8 weeks

Security Updates

Most vendors ship security updates for vulnerabilities reported externally

- The bugs found internally (though QA, engaging penetration testers, etc) are rolled up in service packs in major releases
- Bugs get the benefit of a full test pass
- Takes a very long time for the fix to reach the user
- Can’t tell from the outside how many bugs get fixed this way

Mozilla is continuously looking for vulnerabilities

Shipped in security updates on regular schedule

Don’t have to wait for a major release to get the benefit of the security work we’re doing

Try this at home…please!

Evaluate whether the benefit of the monster test pass for service packs and major revisions is really required for security fixes

It’s not nice to force customers to pay for an upgrade to get security fixes

Just because they were found internally doesn’t mean they are not known externally

Customers shouldn’t have to be exposed for a year if the fix is already checked in and just waiting for the right ship vehicle to be ready

Lies, damned lies, and statistics

Numbers make you look smarter!

Managers (and customers) Need Data

Answers questions like:

“Should I be worried?” (Yes.)

“Are we getting better?”

“What is the top priority?”

“When will we get there?”

Metrics for Success

“Show me how you’ll measure me, and I’ll show you how I’ll perform.” – Eli Goldratt; physicist

How should we measure success and prioritize effort?

Just counting bugs doesn’t work.

And it doesn’t help the industry:

- Provides incentive to group bugs unhelpfully
- Provides incentive to keep quiet about bugs not otherwise disclosed

You don’t want those incentives!

Metrics for Success (cont.)

What metrics describe user safety for Mozilla?

Mozilla’s metrics:

- Severity
- Find Rate/Fix Rate
- Time to Fix
- Time to Deploy

What are your vendor’s metrics?

Severity

Helps us prioritize what to fix first, and when to ship an emergency update

Every bug with any security risk gets fixed, even low – often easier to fix than prove exploitable

No industry standard for severity ratings – but there probably should be!

Consistent with ourselves over time

Mozilla Severity Ratings

Critical: Vulnerability can be used to run attacker code and install software, requiring no user interaction beyond normal browsing

High: Vulnerability can be used to gather sensitive data from sites in other windows or inject data or code into those sites, requiring no more than normal browsing actions

Mozilla Severity Ratings (cont.)

Moderate: Vulnerabilities that would otherwise be High or Critical except they only work in uncommon non-default configurations or require the user to perform complicated and/or unlikely steps

Low: Minor security vulnerabilities such as Denial of Service attacks, minor data leaks, or spoofs

Find Rate

How many security bugs have we found? How severe in aggregate?

What methods were most productive? Quantity and severity both count

Are some methods inefficient?

- Automated source code analysis: high number of false positives (one tool was 0 for ~300!)

Who is really good at finding security bugs?

How do we scale?

Fix Rate

How long does it take to fix bugs?

Which are hardest to fix?

Which components have the highest concentration of bugs?

Can we fix many bugs with a single architecture change?

Are we finding faster than we can fix?

Regressions? (part of the cost of the fix)

Window of Risk

Two factors:

1. How long does it take to fix the security vulnerability?

2. How long does it take for users to get the patch installed?

Users don’t care why they’re vulnerable, and neither do attackers

Time to Fix

Once a vulnerability is identified, how long does it take a vendor to ship a patch?

Are we getting better over time?

Community Support

- Nightly builds tested by 20,000 people
- Users, developers, security researchers

Time to Deploy

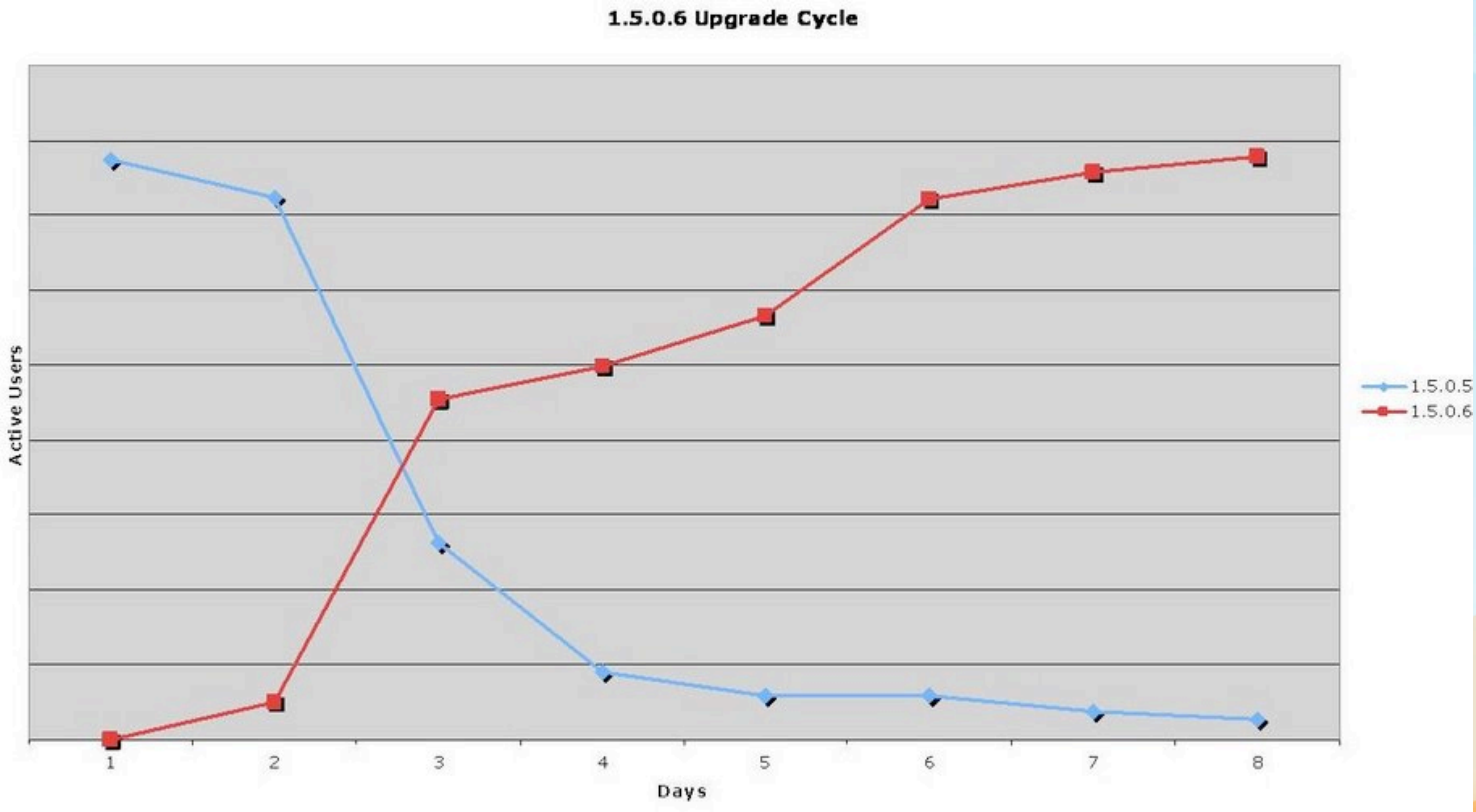
How long does it takes for users to get a patch installed once the fix is available from the vendor?

Auto-update is:

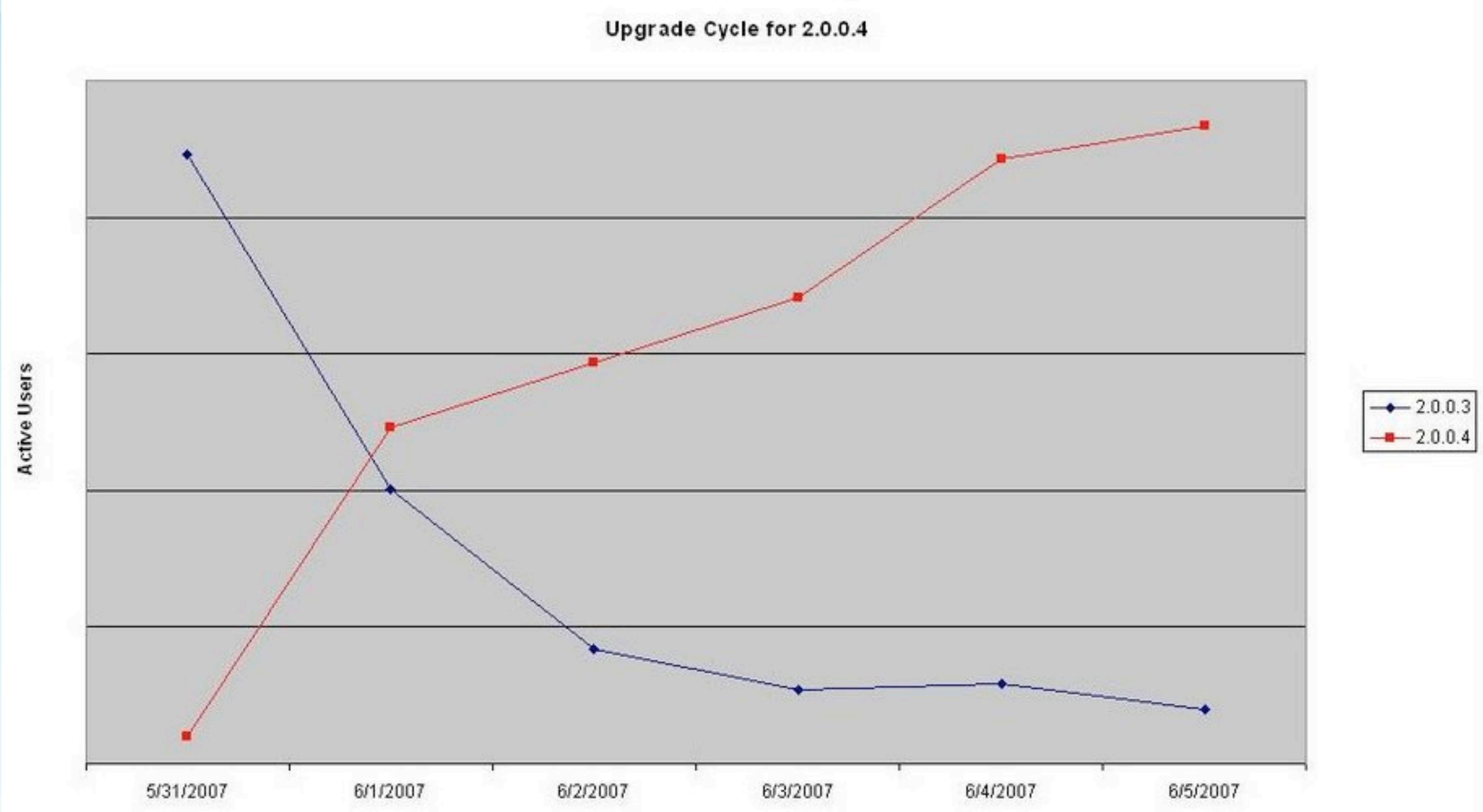
- vital for users; and
- a source of useful data for us

Measuring active users via AUS requests

Upgrade Cycle for 1.5.0.6



Upgrade Cycle for 2.0.0.4



Time to Deploy

Reduced time to deploy by 25% this year

Users get patches faster, stay safer

90% of active users updated within six days

Ask your vendor…

These metrics apply to most software projects

Reduce FUD about number of vulnerabilities

Maybe there are more because they've gotten better at finding them…

Track progress over time – make pretty charts

Develop confidence that your vendor is doing reasonable things

Predict the future!

Security UI 101 for the Software Industry

Users should not have to be experts on PKI to shop safely online

Users aren’t dumb. They are trying to accomplish a task and poor security UI gets in the way.

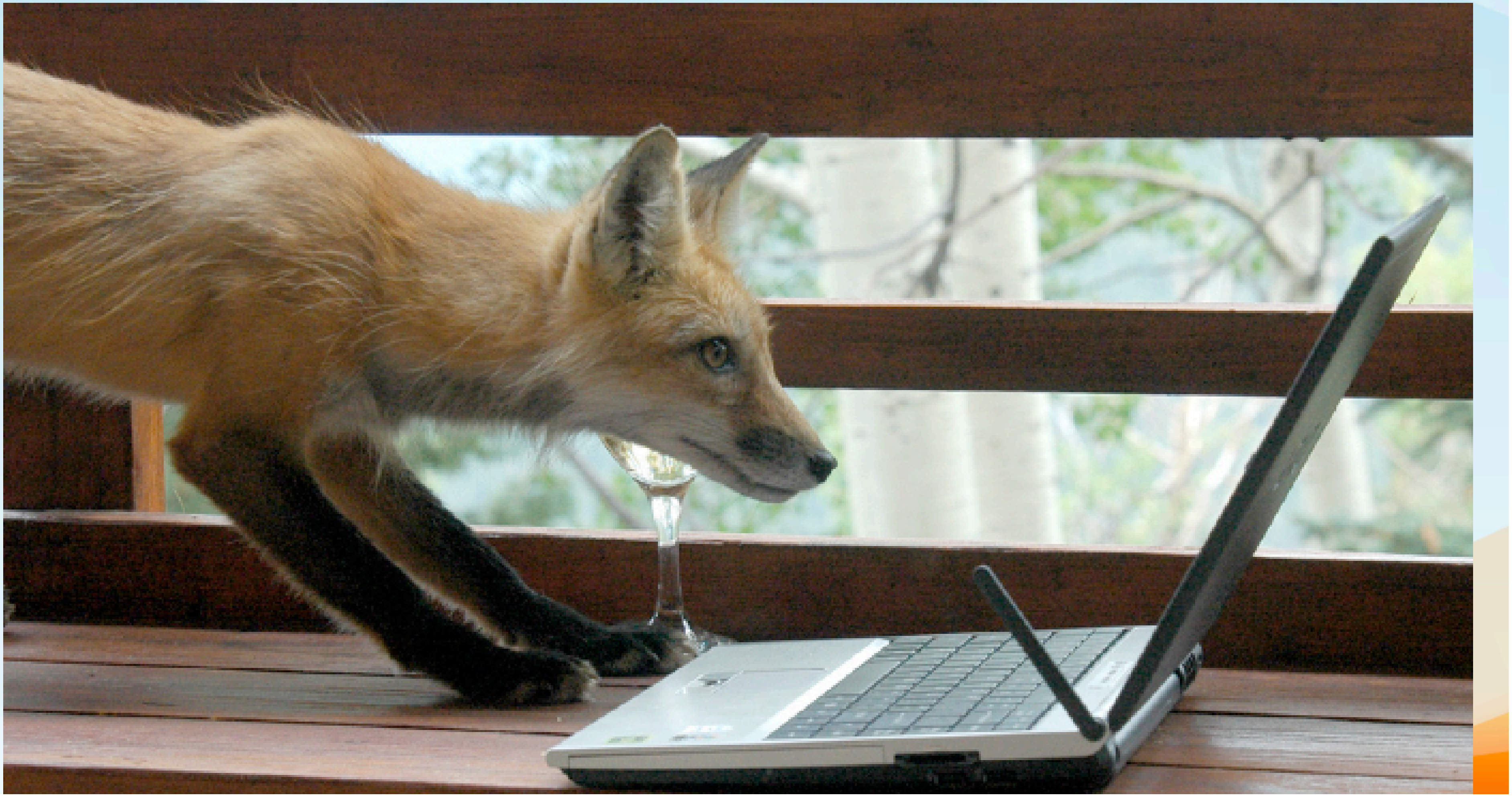
We can do better…

Be Meaningful

Use clear language and concepts. Avoid ambiguity.

Be Relevant

Focus on what matters to users, not the systems.



Be Robust

Don’t build trust around indicators that can be easily subverted.

Be Available

Do not expect users to recognize the absence of an indicator.

Be Brave

Sometimes you have to make the call for the user.

Designing Products for Security

What are the key user tasks for security?

How can we make them better?

How can we help users help us help users?

Key User Task: Apply an Update

We want to optimize time-to-deploy, remember!

The “last mile” is in the hands of the user

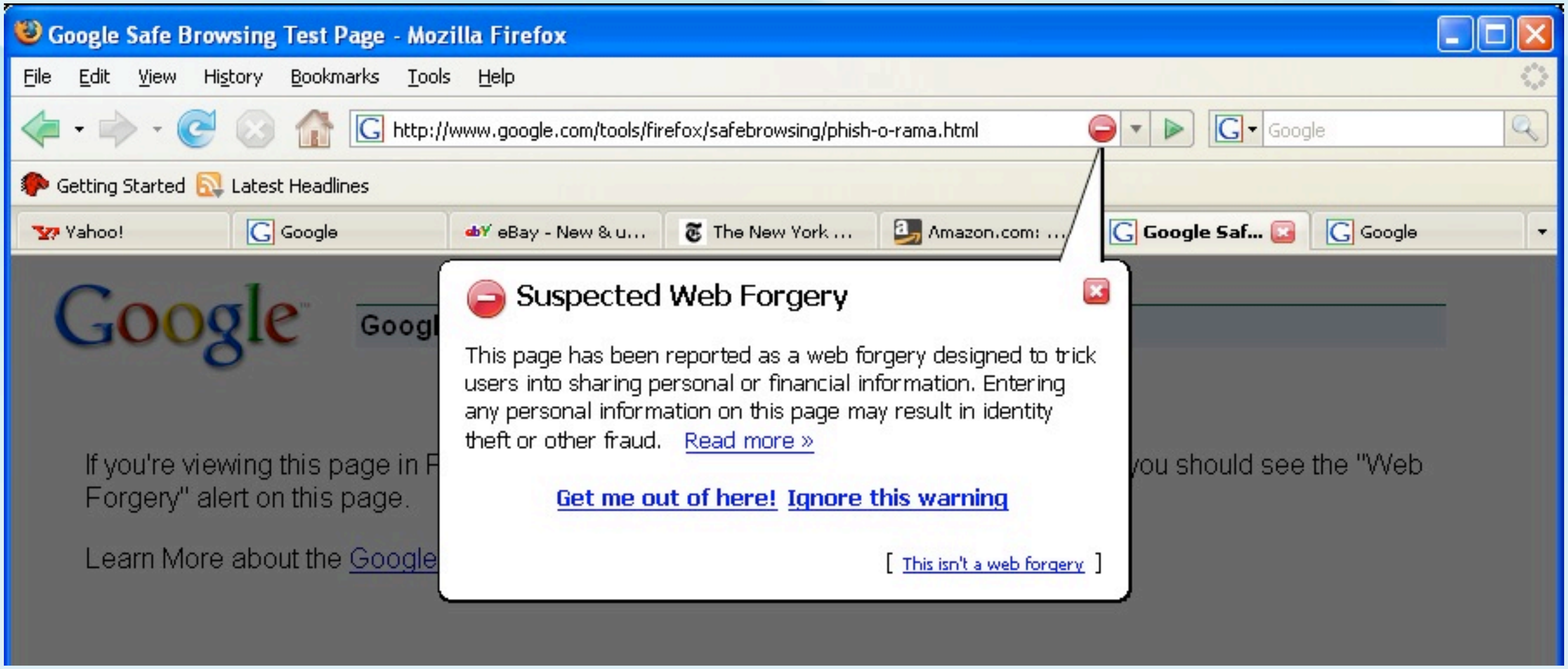
Why do users decline updates?

- Too intrusive (“when I’m done with this blog post”)
- Worried about things breaking

Session restore is a security feature

API stability is a security feature

Help users help us help users.



Google Safe Browsing Test Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.com/tools/firefox/safebrowsing/phish-o-rama.html
Google
Getting Started
Latest Headlines
Yahoo!
Google
eBay - New & u...
The New York ...
Amazon.com: ...
Google Saf...
Google
Google
Googl

Suspected Web Forgery

This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Read more »

Get me out of here! Ignore this warning

[This isn't a web forgery]

If you're viewing this page in F… you should see the "Web Forgery" alert on this page.

Learn More about the Google…

Report a Web Forgery image

Crash reporting image

Security Communication

Builds confidence that the vendor is doing something reasonable

Helps security researchers evaluate a product's security strength

Turns marketing claims into measurable progress

Encourages us to give them the benefit of the doubt

Vendors listen to you

You can change how vendors communicate about security

Encourage them to publish security metrics

Customer feedback was the key driver behind Windows XP SP2 for Microsoft

Community feedback contributes to a stronger process

Others can leverage what we learn from this

Thank You

window@mozilla.com