The Wild, Wild Web: Web Browser Security, Performance, and Privacy

Rick Moen, rick@linuxmafia.com

How did we get in this mess?

An ultra-brief review:
[Not Really] The History of the Web

- 1990: Tim Berners-Lee invents Web servers/browsers, using a NeXT box: Browser/editor is called 'WorldWideWeb' (later 'Nexus').

How did we get in this mess?

1990, later that afternoon: Advertising!

1990, teatime: And worms, viruses, trojans...

1990, supper time: 90% of world's desktop publishers declare themselves 'webmasters'.

How did we get in this mess?

1994: Netscape Navigator brings the Web to the masses. Lou Montulli invents HTTP cookies.

1997: Microsoft Corp. buys Front Page from Vermeer Technologies (mainly for its ability to segfault Navigator?).

How did we get in this mess?

- 1997: RFC 2109 says third-party HTTP cookies are a no-no. It is promptly ignored.
- ...and Web Bugs are invented to go with them, thus creating Doubleclick and kin.
- 2002 Macromedia invents Flash Cookies (LSOs), is itself gobbled by Adobe in '05.

How did we get in this mess?

• Maybe ~2002, or whenever: Faced with the Web's overwhelming popularity, most sysadmins pretty much give up on influencing what users do to (and with, and over) port 80/tcp = HTTP. Port 80, accessible everywhere as a 'good' [sic] network service, becomes the primary sewer of the Internet.

The Web and Its Discontents

By original design, HTTP is stateless: It sends your browser stuff on 80/tcp, then the connection closes. Finito!

This was the first thing to be worked around. State gets embodied via:

1. URL encoding
2. HTTP cookies
3. Data sent back within the returned HTML and stored server-side, client-side, or both.

The Web and Its Discontents

- Stored state isn't the problem. Excessive longevity and abuse are.
- Abuse 1.0 was HTTP cookies – e.g., classic DoubleClick scheme – but dozens of successors have joined them.
- Gee, look who bought DoubleClick (a point we'll come back to later).

The Web and Its Discontents

Samy Kankar's Evercookie, http://samy.pl/evercookie/

- Standard HTTP Cookies
- Local Shared Objects (Flash Cookies)
- Silverlight Isolated Storage
- Storing cookies in RGB values of auto-generated, force-cached PNGs using HTML5 Canvas tag to read pixels (cookies) back out
- Storing cookies in Web History
- Storing cookies in HTTP ETags
- Storing cookies in Web cachewindow.name caching
- Internet Explorer userData storage
- HTML5 Session Storage
- HTML5 Local Storage
- HTML5 Global Storage
- HTML5 Database Storage via SQLite.

The Web and Its Discontents

- Keystone of the whole problem: Javascript abuse. (It's overfeatured and out of control, e.g. repeated security exploits, malware vector.)
- Typical Javascript engine: Huge attack surface, easy vector for third-party snooping. Of course, there are worse things (**cough** ActiveX, VBScript **cough**).
- Prescription: Limit that sucker (NoScript).

Why Care?

- Because we can. (My browser, my rules.)
- The best to prevent data from being abused is to not hand it out.
- Information has value. Want mine? Make me an offer. (Example of eBay pricing.)
- Nonetheless, 99% of people hearing this lecture will nod and do nothing. But next time you grumble over sluggish loads and bloat, remember.

Let's Fix Firefox

- Why not Chrome? Opera? Safari? (Because they're proprietary, silly.)
- Why not Chromium? (Pretty good browser. Extensions interface is relatively weak. Google, Inc. is in some conflict of interest. OTOH, good ideas there (“crash control”) sandboxing
- Why Firefox? Some conflict of interest. (Look where their funding comes from.) Unexcelled extensions interface. A bit bloated. (Cf. Swiftweasel, open-source riff on Swiftfox.)

Let's Fix Firefox

Recommended Extensions:

- NoScript – selective control over JavaScript
- Adblock Plus (“ABP”) – ad filtering
- OptimizeGoogle – improves Google search
- User Agent Switcher – set user-agent on the fly
- Objection – cleans Flash cookies
- Beef Taco (Targeted Advertising Cookie Opt-out) --

(Details to come.)

Why aren't at least some of these bundled with Firefox? Reasons include complicating of release schedules. (One cannot help wondering about avoiding biting the hand that feeds, though.)

Let's Fix Firefox

Often recommended, but not here:

- TACO (now called Abine) – Beef Taco is fork of TACO 2.0. TACO 3.0 aka Abine is proprietary, feature-rich, and supported by a benevolent, helpful company that cooperates with the open-source fork!
- BetterPrivacy – proprietary, lets user manage Flash cookies and DOM Storage objects.

Let's Fix Firefox

Other dumb ideas:

- Enumerating badness
  - Microsoft IE 'trusted zones' (haha).
  - Malware checkers.
- “Opening” a file from public networks without knowing what will happen.
- Using any old DNS nameservers and hoping for the best.

Let's Fix Firefox

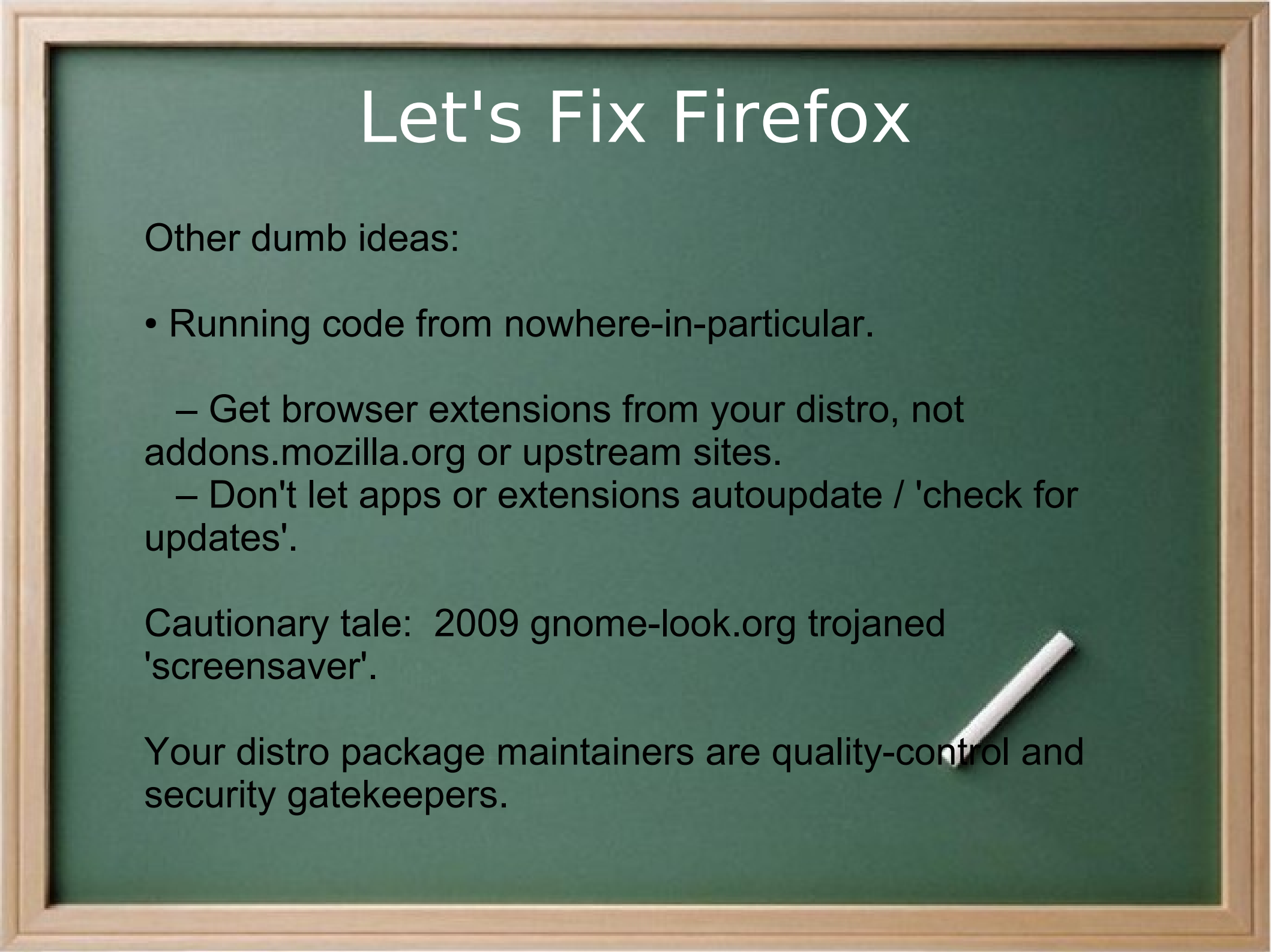
Other dumb ideas:

• Running code from nowhere-in-particular.

– Get browser extensions from your distro, not addons.mozilla.org or upstream sites.
– Don't let apps or extensions autoupdate / 'check for updates'.

Cautionary tale: 2009 gnome-look.org trojaned 'screensaver'.

Your distro package maintainers are quality-control and security gatekeepers.



Let's Fix Firefox

Cautionary tale – 2009 squabble between NoScript and Adblock Plus:

ABP blocks advertising. NoScript Web pages include ads. ABP blocks them, NoScript evades filters, ABP escalates, breaking NoScript site viewing. NoScript sabotages ABP filter.... Lather, rinse, repeat.

Meanwhile, distro packages of both omit all of this soap opera.

NoScript

- Fairly sophisticated by default. Little need to tweak.
- A few sites will briefly be headaches. You can figure out which JavaScript is actually useful, or if impatient you can “Allow All This Page” or such.
- NoScript is the single biggest win I've found.

http://noscript.net/

Adblock Plus

- Supports 'subscriptions' of ad blocklists. EasyList recommended (exception to my rule about disabling autoupdate).
- Again, little to tweak. Just cleans up and speeds sites.

http://adblockplus.org/en/

OptimizeGoogle

- Anonymises Google userid.
- Removes ads
- Adds links to try other search engines.
- Removes link tracking.
- (Many other improvements. Most are disabled by default, so spend time on Preferences.)

http://www.optimizegoogle.com/
Maintained fork of CustomizeGoogle, which became unmaintained in 2008:
(http://www.customizegoogle.com/)

Lesson: If it dies, look for a fork.

User Agent Switcher

- Gets you into many sites that block you for dumb reasons.
- Lets you make a statement in Web server logfiles, e.g.: "W3C standards are important. Stop f---ing obsessing over user-agent already"

http://chrispederick.com/work/user-agent-switcher/

Objection

- Keeps Flash cookies (LSOs) under control.
- Open-source replacement for that aspect of BetterPrivacy (which is proprietary).

http://objection.mozdev.org/

Hackish alternative for LSOs

```
$ crontab -l

# m h  dom mon dow   command
  0 *  *   *   *     /home/rick/bin/delete-flash-cookies.sh

$ cat /home/rick/bin/delete-flash-cookies.sh

#!/bin/sh
mv ~/.macromedia/Flash_Player/macromedia.com/support/flashplayer/sys/settings.sol\
~/.macromedia/Flash_Player/macromedia.com/support/flashplayer/
rm -rf ~/.macromedia/Flash_Player/macromedia.com/support/flashplayer/sys/*
mv ~/.macromedia/Flash_Player/macromedia.com/support/flashplayer/settings.sol\
~/.macromedia/Flash_Player/macromedia.com/support/flashplayer/sys/
rm -rf ~/.macromedia/Flash_Player/#SharedObjects/ZR7UJY6C/*

$
```

Beef Taco

It's just a set of long-lived, neutered advertising-domain cookies to pre-empt the real ones. Simple, effective.

http://jmhobbs.github.com/beef-taco/

DOM Storage

• New with Firefox 3.x, in sqlite database files. Doesn't seem to get data if you use NoScript, but nice to be able to query and manage contents. Limit seems to be 5 MB. (http://kb.mozillazine.org/Dom.storage.default_quota). Compare 100kB per domain for Flash cookies, 4kB per entry for HTTP cookies.

• Nothing currently in mine:

```
$ echo 'select * from webappsstore;' | sqlite3 \
/home/rick/.mozilla/firefox/sb0oeeg0.default/webappsstore.sqlite
$
```

Misc. Browser Preferences

- Advanced, Enable JavaScript, deselect all.
- Privacy, “Accept third-party cookies”, uncheck.
- Privacy, “Always clear my private data”, Settings, check all (but adjust according to taste).
- Security, Exceptions, “Warn me when sites try to install add-ons”, remove all.
- Security, “suspected attack site” & “suspected forgery”, disable. Nanny antiphishing/antimalware site.
- Advanced, General, “Warn... reload or redirect”, enable.
- Advanced, Update, set to “Ask me what I want to do” for all.

Misc. Information Leakage

- Internal leakage between domains
- Cross-app data transfer (e.g., via Flash plug-in)
- Stealing of Web history, e.g., injecting invisible links using JavaScript that exploit CSS link color attribute's dependency on the link-visited flag.
- Cookie theft, and thus session theft (another reason for https).
- Search bars (another reason Awesomebar isn't my cuppa).
- Browser page prefetching.
- List of sites exempted from password caching.
- Data logged at your DNS nameserver. Why aren't you running Unbound locally?

All Sorts of Further Resources

- Marcus Ranum on why “enumerating badness” is dumb:

http://www.ranum.com/security/computer_security/editorials/dumb/

- Samy Kankar's Evercookie

http://samy.pl/evercookie/

(Also visit Sam's home page with JavaScript enabled, to see what he can probe from your Web browser.)

- How distinctive is your browser signature? EFF Panopticlick.

https://panopticlick.eff.org/

- More opinionated views about Firefox configuration.

http://linuxmafia.com/~rick/firefox.html

- Unbound and other nameserver software for *ix

http://linuxmafia.com/faq/Network_Other/dns-servers.html

Son of Further Resources

• Karsten Self on why to set a custom user-agent
http://linuxmafia.com/faq/Web/user-agent-string.html

In the finest Alice's Restaurant tradition, if one person does this, they may think he's sick, and they'll deny him the Web page. If two people do it, in harmony, well, they're free speech fairies, and they won't serve them either. If three people do it, three, can you imagine, three people setting their user-agent strings to "Stop f---ing obsessing over user-agent...". They may think it's an organization. And can you imagine fifty people a day? Friends, they may think it's a movement. And that's what it is...

• Swiftweasel, Firefox compiled with buffer-overflow protection, etc.
http://swiftweasel.tuxfamily.org/

A Word from Our Sponsor

This talk sucked! You can do better. (I wrote this presentation in two days, after our originally scheduled speaker had to cancel.)

SVLUG needs your presentation. You know you want to!