

DEFCON 16

EXPLOITING A HUNDRED- MILLION HOSTS BEFORE BRUNCH

Stefan Frei & Gunter Ollmann [here]

Thomas Dübendorfer & Martin May [not here]

Abstract

- If you were to "hack the planet" how many hosts do you think you could compromise through a single vulnerable application technology? A million? A hundred-million? A billion? What kind of application is so ubiquitous that it would enable someone to launch a planet-wide attack? - why, the Web browser of course! We've all seen and studied one side of the problem - the mass- defacements and iframe injections. But how many vulnerable Web browsers are really out there? How fast are they being patched? Who's winning the patching race? Who's the tortoise and who's the hare? Our latest global study of Web browser use (tapping in to Google's massive data repositories) has revealed some startling answers along with a new perspective on just how easy it would be to "hack the planet" if you really felt like it.

The Situation...

- ④ The Internet is getting more and more hostile...
 - Profit motivated attacks driving new “Hackonomy”
- ④ Mass-defacements with injected drive-by downloads
 - iframe embedding, XSS, SEO/page-rank manipulation
- ④ Stream of sever-side figures in the news
 - 1,200,000 SEO injected iframes
 - Avg. 100,000 new/repeat defacements per week
- ④ What about the other side?
 - How many “victims” could you get if you really tried?

The Measurement...

⊙ Idea

- The USER-AGENT string reveals major & minor version of browser...
- Web servers log the user-agent information...
- Browser version correlates to patch level

⊙ Observation

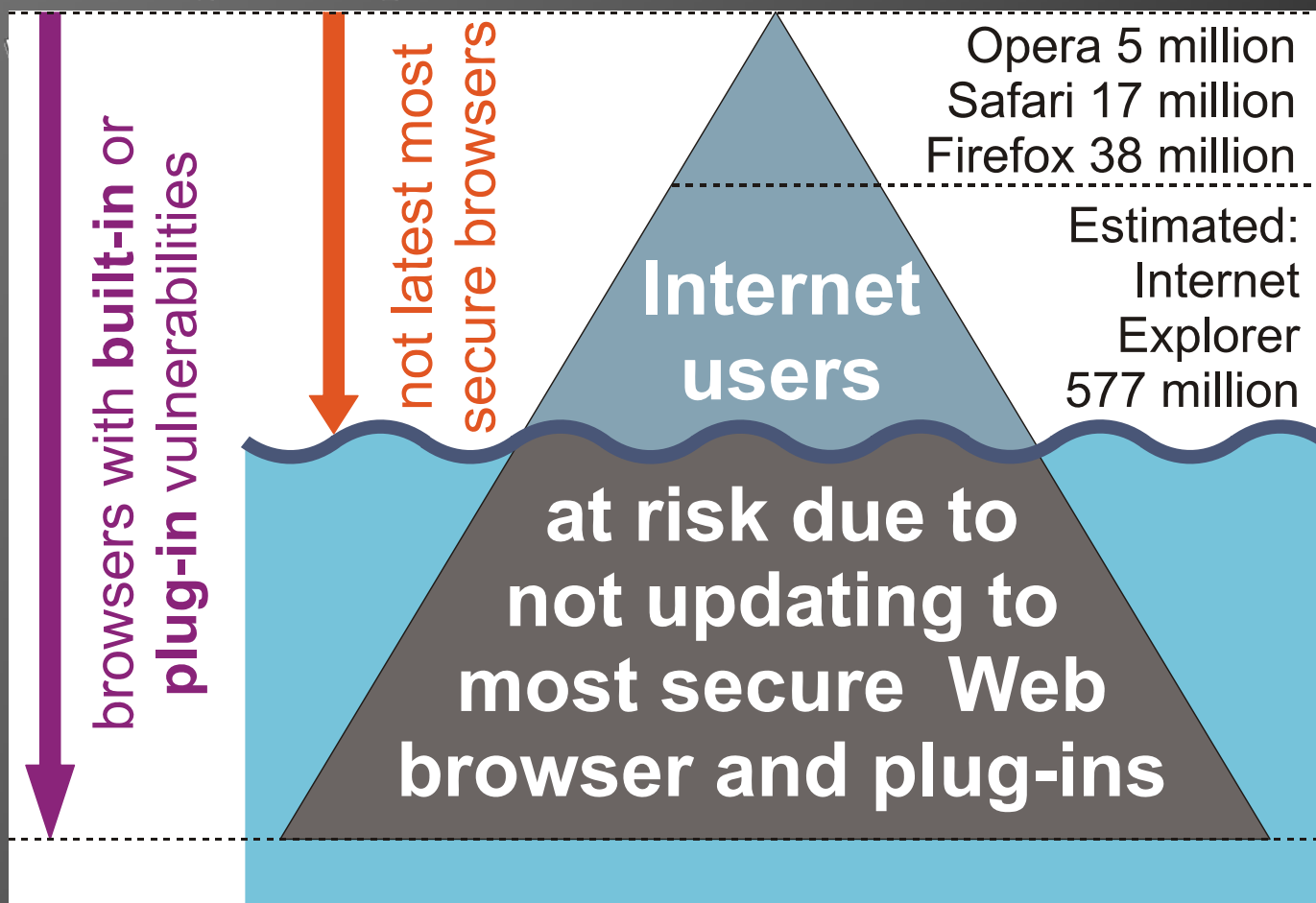
- Google has lots of Web servers...

⊙ Measurement

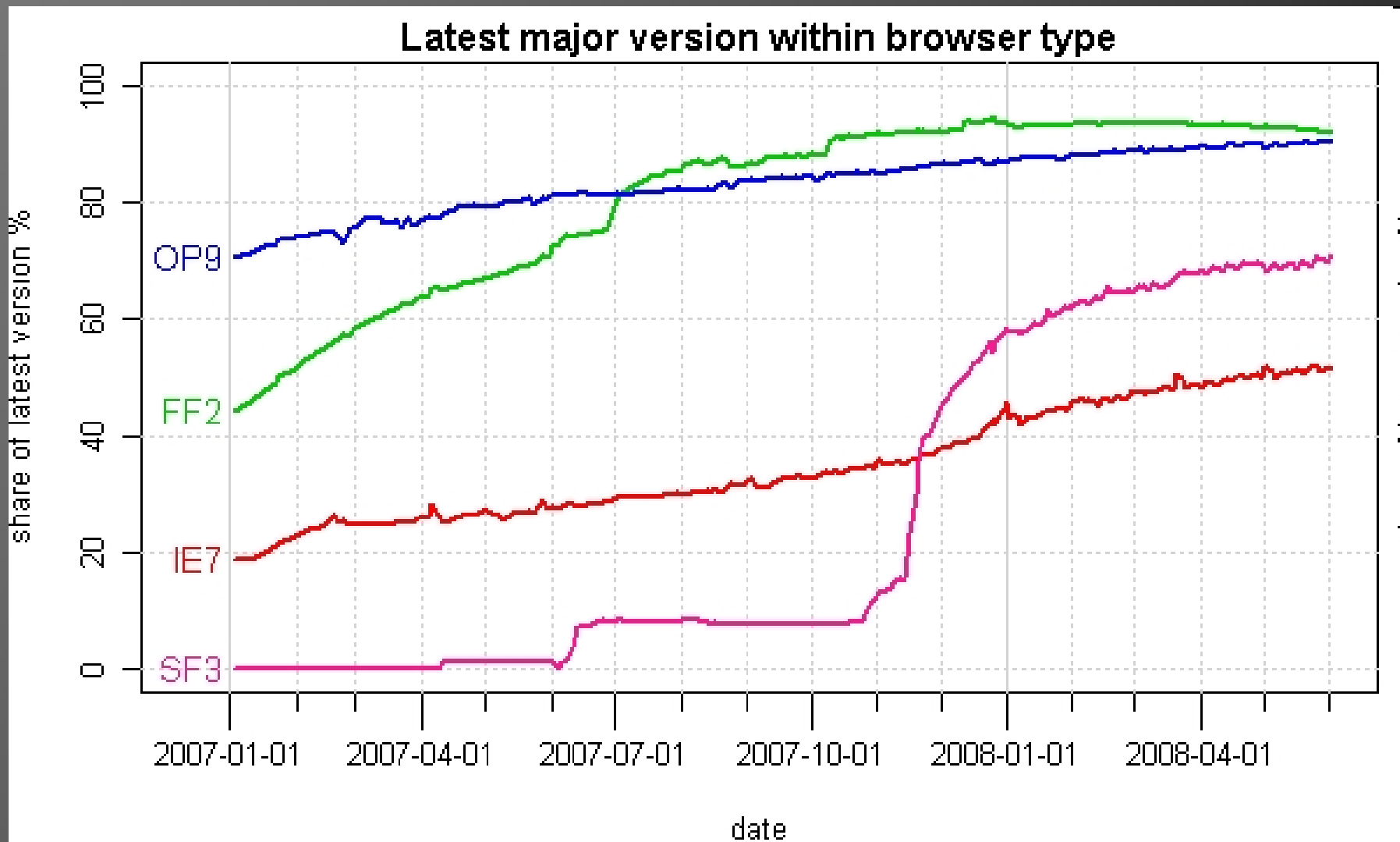
- Analysis of Google web logs between January 2007 to June 2nd, 2008 - *Big thanks to Google!*
- Passive unbiased measurement of truly global scale.

Insecurity Iceberg

- 637 million (or 45.2%) web users are not surfing using the latest most secure browser

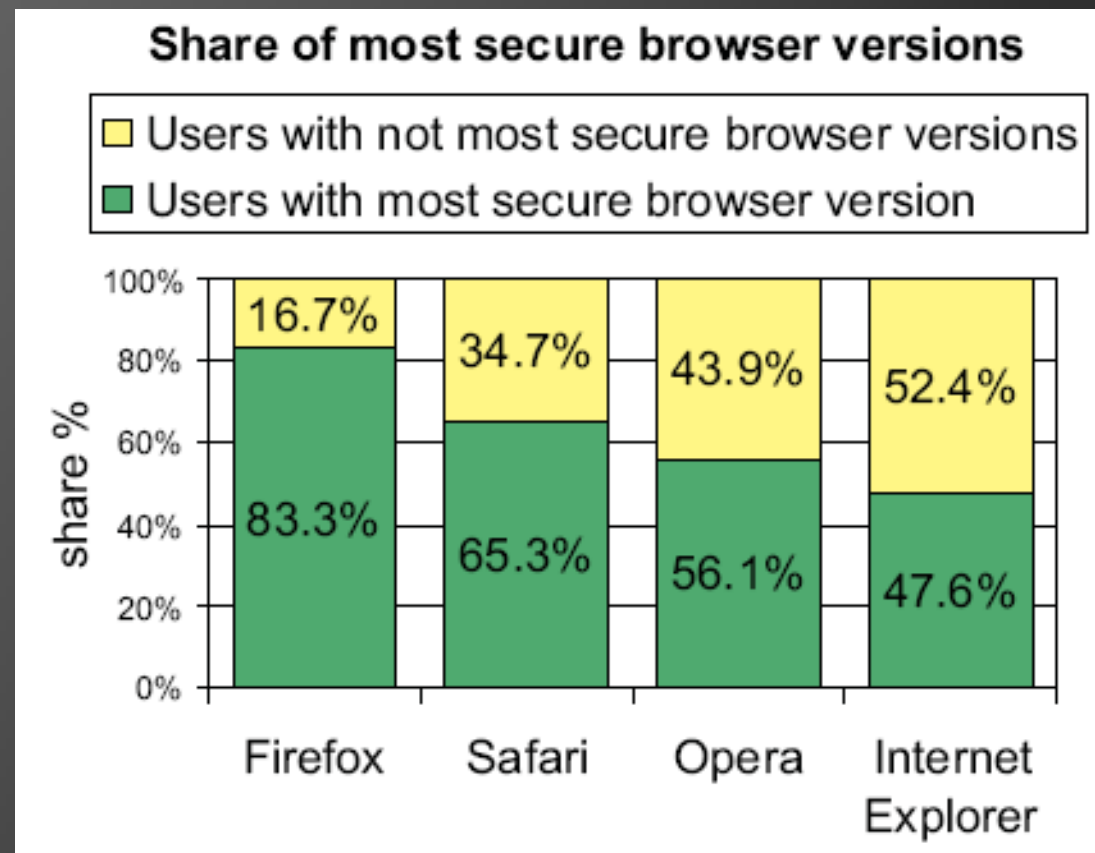


Share of Latest Major Version



Most Secure Browser

- Most secure browser designates the latest official public release of a vendor's Web browser at a given date.



Estimating Vulnerable Population

Estimate A

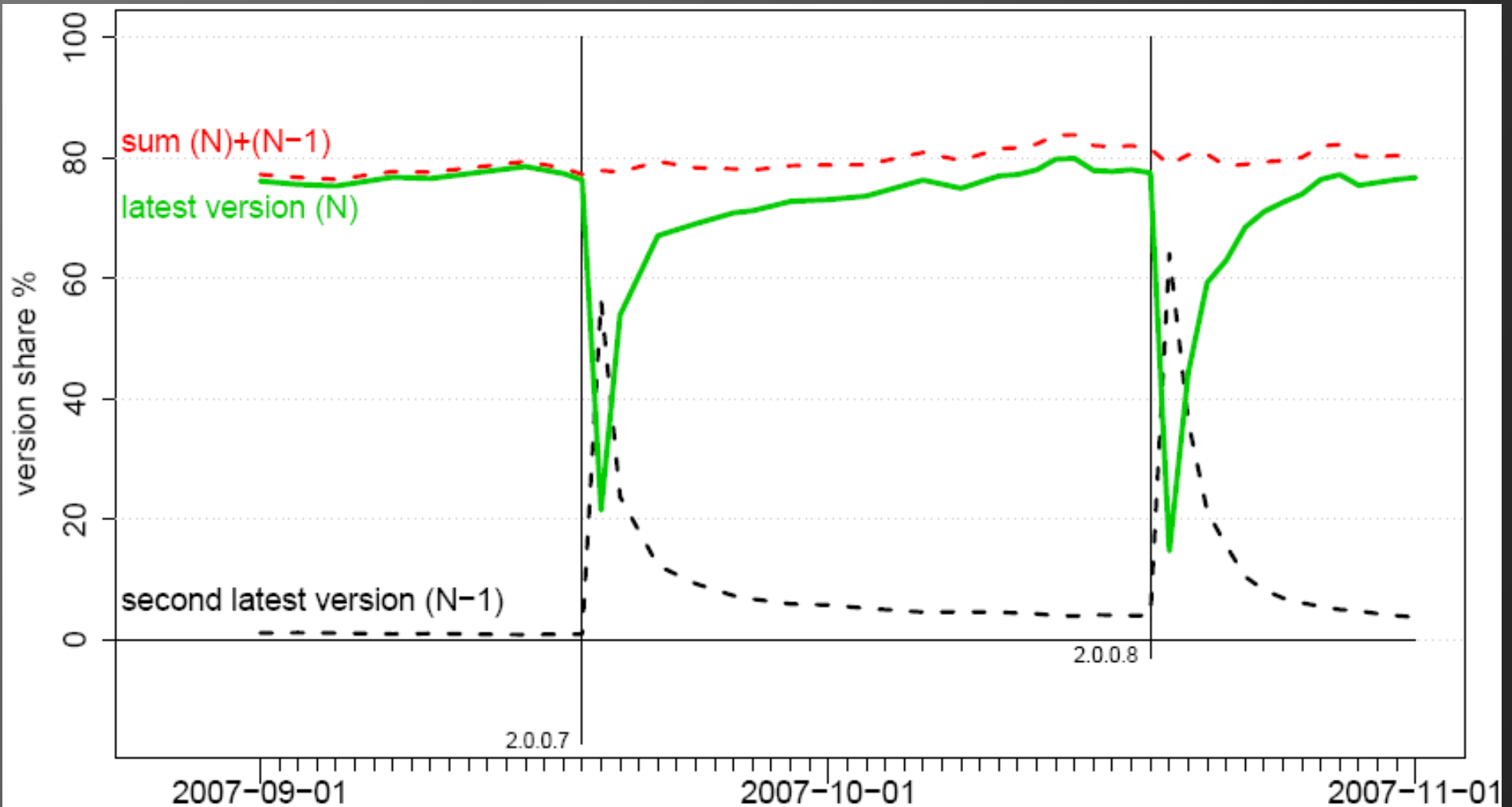
- Secunia PSI (biased) values for IE7 unpatched share, using Google data for FF2, SF3, OP9: 609 million.

Estimate B

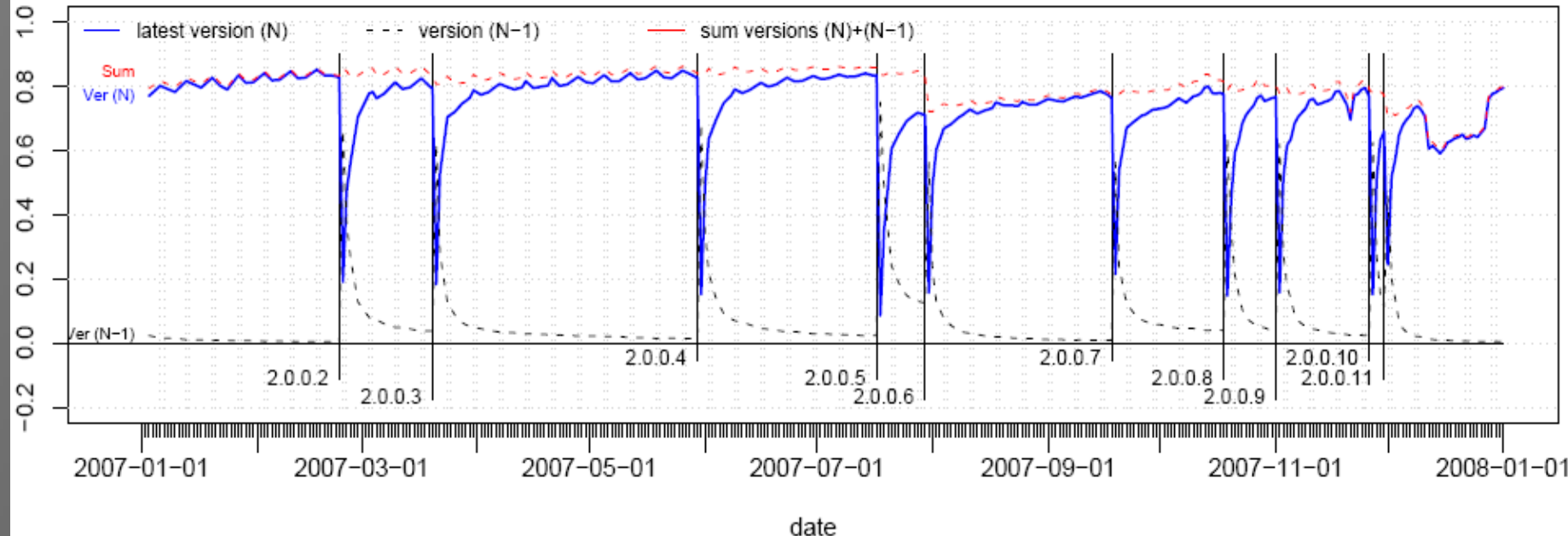
- Correcting PSI bias (factor 2.1 found by comparing FF2, SF3, OP9 PSI with Google): 637 million

Browser Type	IE w/o IE7	IE7	FF	SF	OP	Total
Share of browsers in daily use in percent (cf. Table 1)	37.2%	41.1%	16.1%	3.4%	0.8%	98.6%
Browsers in daily use worldwide in million	523.8	578.7	226.7	47.9	11.3	1388.3
Estimate A						
Share of not most secure browser versions in percent	100.0%	4.4%	16.7%	34.7%	43.9%	43.3%
Not most secure browser versions in million	524	25	38	17	5	609
Estimate B - correcting the bias of PSI (IE7 x 2.1)						
Share of not most secure browser versions in percent	100.0%	9.2%	16.7%	34.7%	43.9%	45.2%
Not most secure browser versions in million	524	53	38	17	5	637

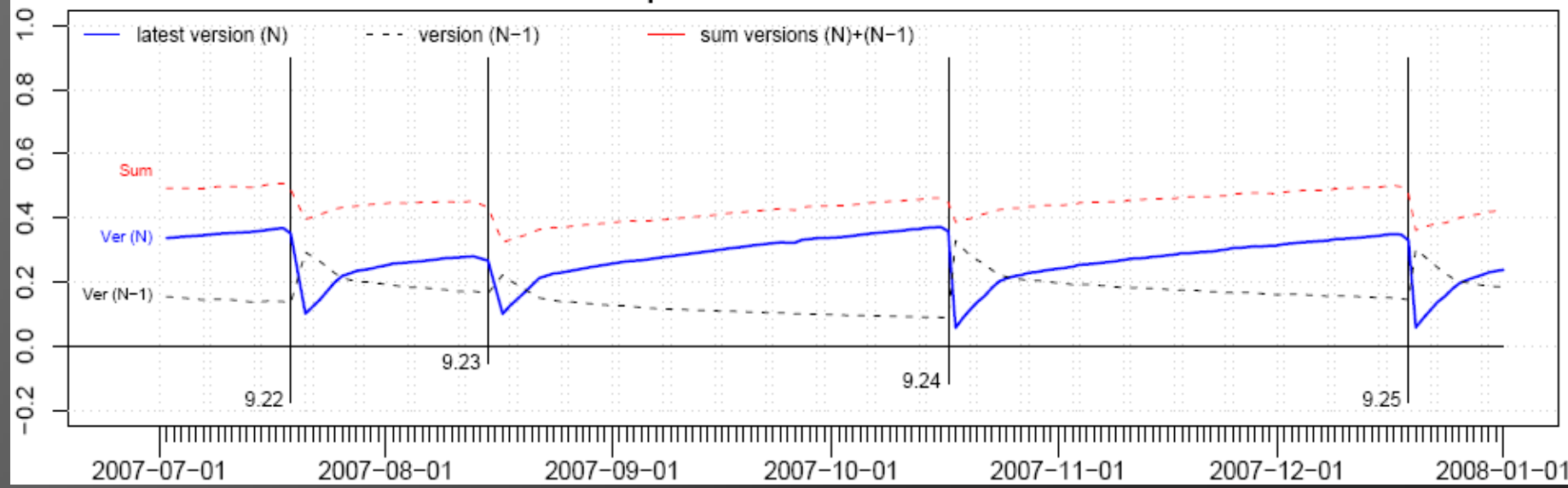
Firefox – Version Flux



Firefox most secure versions

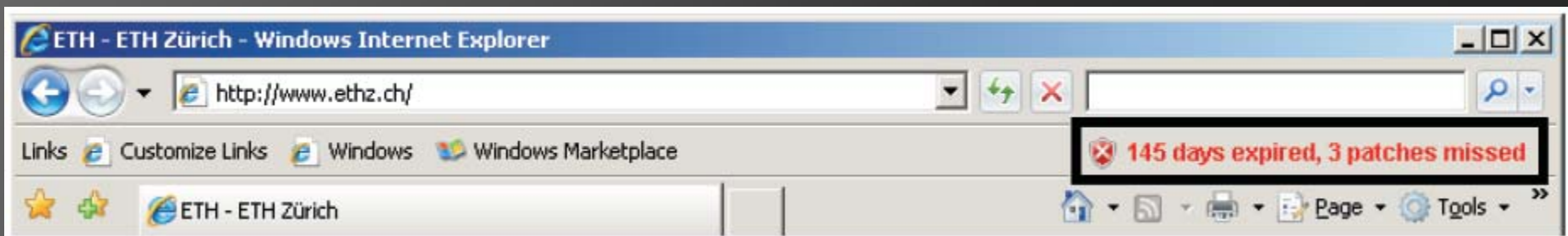


Opera most secure versions



Patch/Upgrade Faster?

- ⦿ Users don't know when and why to patch or upgrade
 - Even automated patching systems seen as “bother-ware”
- ⦿ How can they be helped along... nudged in the right direction?
 - Scare the sh*t out of them?
- ⦿ Why not try a “best before” date control system
 - Works for food
 - Easy to extrapolate consequences of “expired” goods

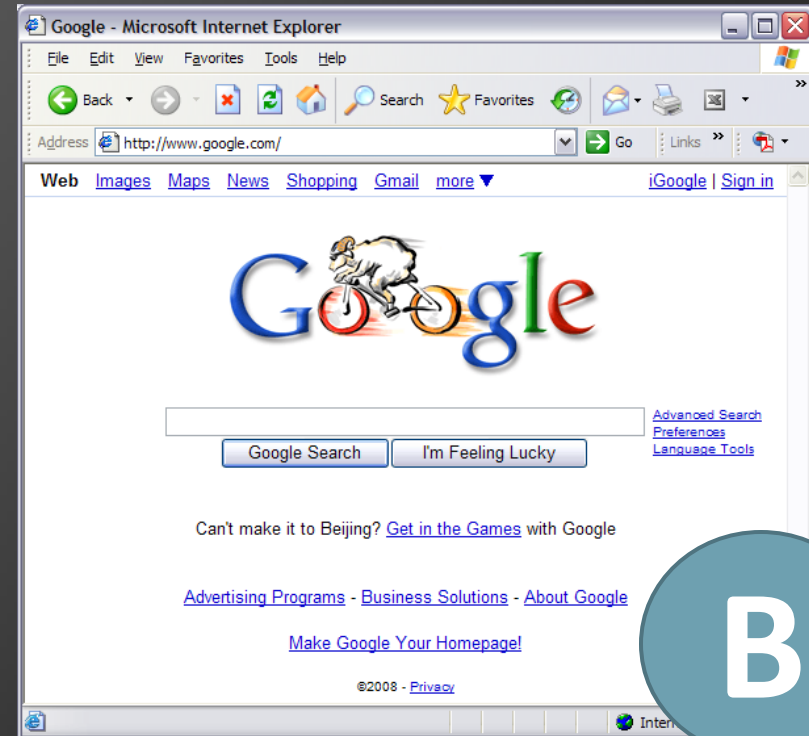
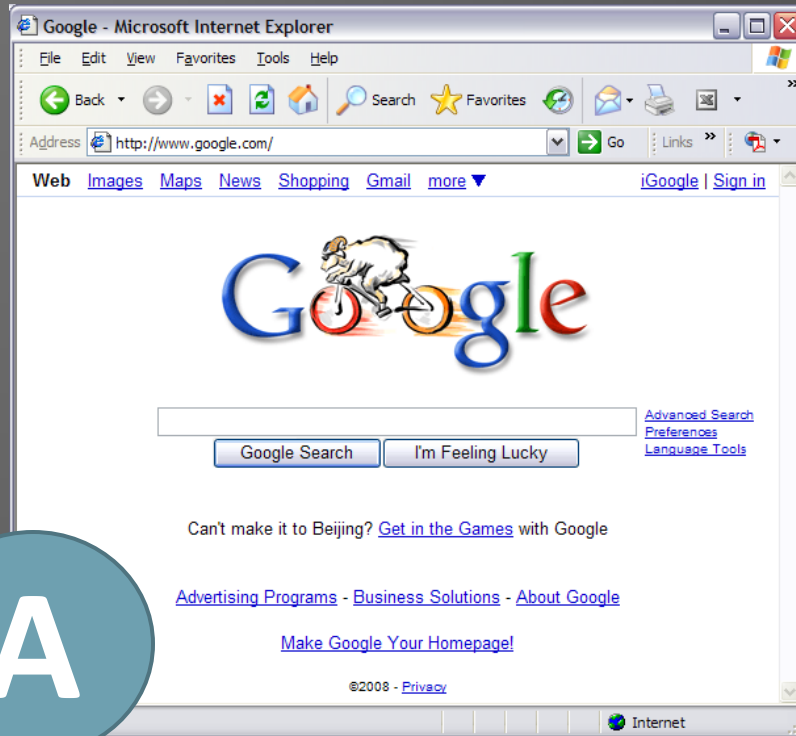


Conclusions

- ④ “Hack the planet” doesn’t require a 0-day
 - A well-spread malicious iframe with an old exploit would work
- ④ Browser patching is a complex problem
 - ...and we think Firefox leads the pack
- ④ Patching technology is only part of the solution
 - It’s a question of ergonomics
- ④ If you have to prompt the user, it just means the “expert” didn’t know what to do...

Are you an expert?

- Which browser below is missing 8 patches?
- Which one is still using Flash v.6?



- How are 1.4 billion users supposed to tell?

Thanks!

Questions?

Contact: insecurity-iceberg@ee.ethz.ch

<http://www.techzoom.net/insecurity-iceberg>