Low Cost, High Performance, Strong Security: Pick Any Three

Chris Palmer

iSEC Partners

https://www.isecpartners.com/

iSEC PARTNERS

Why Listen to This Guy?

- Experienced web developer
- Experienced web application security consultant
  - I see lots of web apps of all types
  - Large companies, startups, all different types of risk/threat profiles
  - All different skill levels of developers
  - All different technical needs

iSEC PARTNERS

My Goal

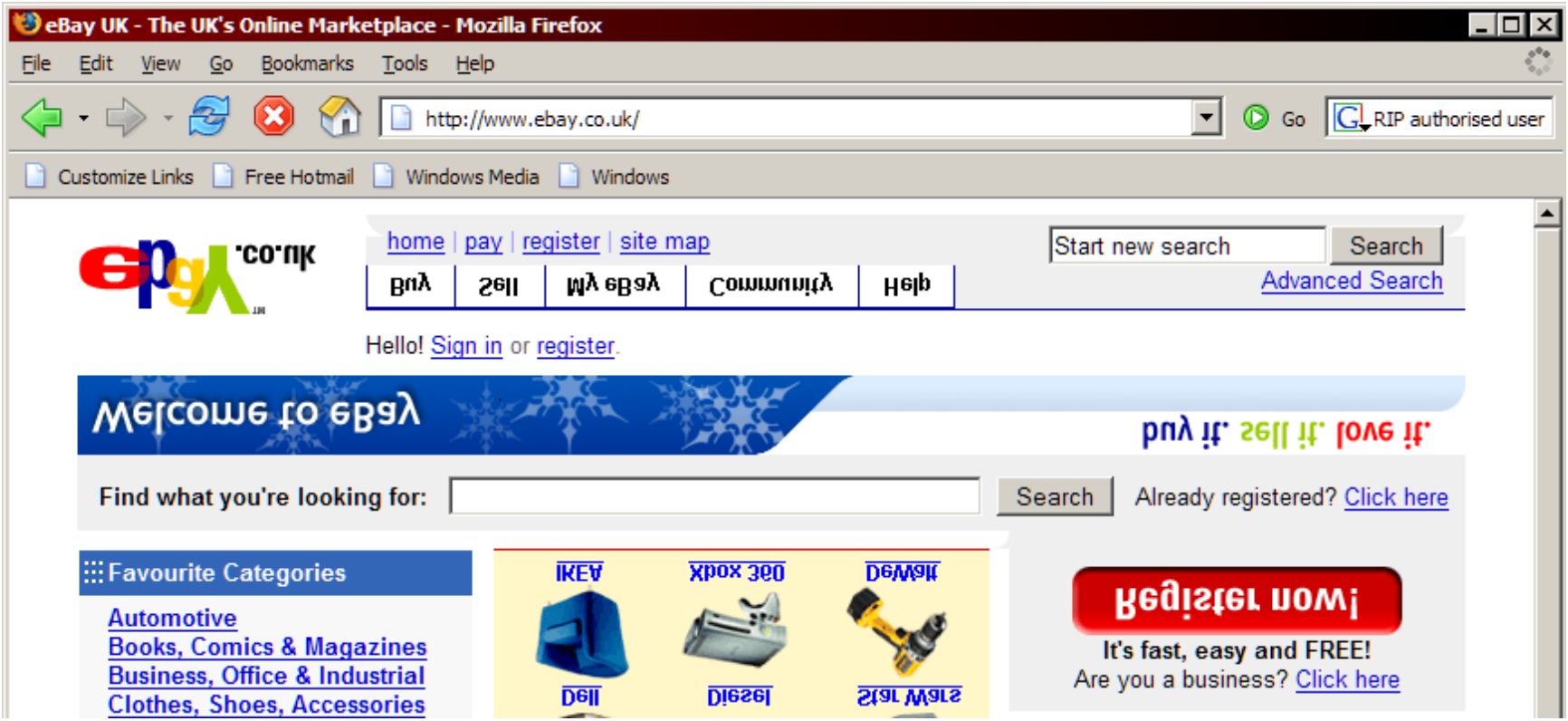
- Find ways to improve site performance so that you can consider HTTPS deployment.

Security Guarantees of HTTP

This slide intentionally left blank.

iSEC PARTNERS

How Is This Possible?

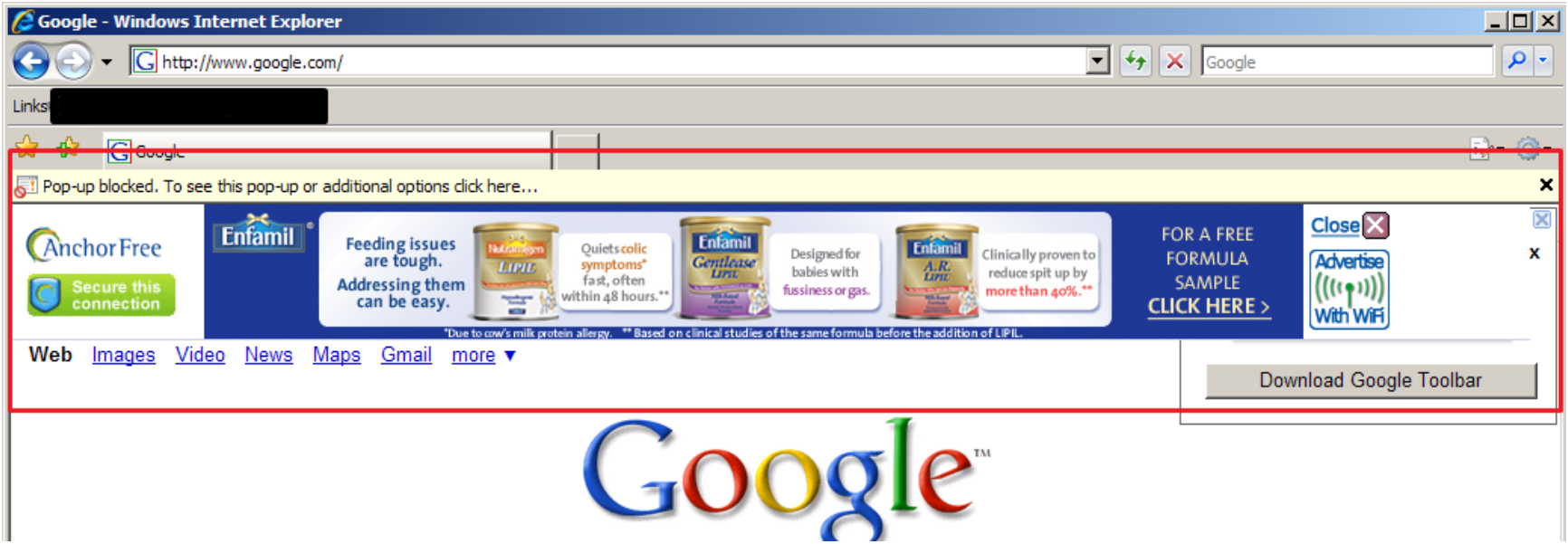


iSEC PARTNERS

The Upside-down-ternet

- http://www.ex-parrot.com/~pete/upside-down-ternet.html
- Simple router configuration and HTTP proxy that runs a script to invert any image.
- See also: Wifi hotspots paid for by injecting advertising into the pages users view.

Network Attacks: A Business Model



iSEC PARTNERS

Security Guarantees of HTTPS

- Server authentication
  - You are talking to the true example.com
- Data integrity
  - You got the true page back from example.com
- Data confidentiality
  - Nobody can decrypt your sensitive example.com information

So Why Not Use HTTPS Exclusively?

- “It’s too slow.”
- Okay, what’s your performance target?
- “I don’t know.”
- Then HTTPS is not too slow.

iSEC PARTNERS

So Why Not Use HTTPS Exclusively?

- “It’s too slow.”
- Okay, what’s your performance target?
- “98% of responses in < 5 seconds.”
- Okay, have you profiled your application to find the slowest parts?
- “No.”
- Then HTTPS is not too slow.

Performance Ueber Alles?

- The proposition is that, since performance is so important, we must disable all security since it's "too slow".
- In effect, HTTP is considered an optimization of HTTPS.
- But is it an effective optimization?

Is Turning Off All Security an Effective Optimization?

- For most of my clients, and most web sites I see, there is much low-hanging fruit for optimization — orders of magnitude more effective than disabling security.
- Usually, the equation is reversed: You should have a really compelling performance requirement (e.g. 99% of responses in < 400ms!) to disable security.

iSEC PARTNERS

People With Such Severe SLAs Include:

- Probably not you

iSEC PARTNERS

What Does HTTPS Actually Cost?

- 3+ RTT handshake. Yeah, I know.
  - So use HTTP/1.1 persistent connections, and reduce the number of requests/responses.
  - Definitely turn on TLS session resumption!
- Asymmetric (public key) cryptography.
  - Amortizable with session resumption.
- Symmetric cryptography.
  - Very cheap (Moore's Law).
  - Reduce the size of your messages.

What Does HTTPS Actually Cost?

- The handshake latency is the real cost.
- You amortize it by making the best use of your TCP connection and TLS session.
- The more effective optimizations discussed below are:
  - Orders of magnitude more effective than disabling security.
  - Very effective, *and rarely applied*, even for insecure sites. Even for high-traffic sites!

iSEC PARTNERS

More Effective Optimizations

- In addition to profiling and optimizing the client, server, and backend code (how chubby is your AJAX library?),
- you can find lots of optimization opportunities in the network traffic profile.
- After all, it's a *web* app, right? Let's check the web part.

Previous Work

- Gmail: http://gmailblog.blogspot.com/2008/05/need-for-speed-path-to-faster-loading.html
- Yahoo: http://developer.yahoo.com/performance/rules.html

Gmail: Major Improvements

- “““…we found that there were between fourteen and twenty-four HTTP requests required to load an inbox… it now takes as few as four requests from the click of the “Sign in” button to the display of your inbox.””””

iSEC PARTNERS

Gmail: Major Improvements

iSEC PARTNERS

Gmail: Some Bad Advice

- http://mail.google.com/support/bin/answer.py?hl=en&ctx=mail&answer=74765
- “If you trust the security of your network, you can turn this feature off at any time.”
- If you trust the security of your parking garage, you can unlock your car door at any time. – Nathan Wilcox
- The Internet is not a secure network.

iSEC PARTNERS

Yahoo UI Blog

- http://yuiblog.com/blog/2006/11/28/performance-research-part-1/
- “You may be wondering why you’re reading a performance article on the YUI Blog. It turns out that most of web page performance is affected by front-end engineering, that is, the user interface design and development.”

Yahoo UI Blog

- “Reducing the number of HTTP requests has the biggest impact on reducing response time and is often the easiest performance improvement to make.”

Reduce Network Traffic

- DON’T have giant cookies, giant request parameters (e.g. .NET ViewState).
- DO compress responses (gzip, deflate).
- DO minify HTML, CSS, and JS.
- DO use sprites. DO compress images at the right compression level, and DO use the right compression algorithm for the job.
- DO maximize caching.

Reduce Network Traffic

- DO enable TLS session resumption on the TLS server.
  - http://rdist.root.org/2009/03/10/note-to-wordpress-on-ssl/

Reduce Network Traffic

- Do you find yourself serving images from 6 different hostnames to get the browser to maximally parallelize your 40 image loads?
- Perhaps the problem is the 40 images.
- eBay.com: 370KiB, 57 request/response pairs, 20+ TCP connections, 7 DNS resolutions.
  - > 4s to load, then 17s later, does > 5s more loading.

Reduce Network Traffic

- Is your front page 1MiB?
- Gap.com (977,657 bytes), nytimes.com (741,148 bytes, > 8 seconds)
- Even if the page really presented that much information (500 pages of ASCII text), people don't sit there and read 500 pages in one go.
- Sure, a lot of it is images… Can people process that much visual information at once? No.

Design and Usability

- As much as that 1MiB page is flooding the network,
- it’s flooding people’s brains even more.

Pick Any Three

- Reducing the size and frequency of network communications allows you to:
  - Get faster page loads—which often means more sales!
  - Suddenly be able to afford the relatively small cost of HTTPS.
  - Save money — lower ISP bills.
    - Give a DoS attacker less of a multiplier…

“But the Site Must Be Visually Rich!”

- Tell that to Larry and Sergey.
- Google made more money than the Beatles with little 3-line text ads.
- Look at their home page, a search results page, and then their stock price and market capitalization.

“But the Site Must Be Visually Rich!”

- Sure, okay. But have you optimized the network traffic as much as possible, given this requirement?
- Visually noisy sites in my experience usually pay a higher network cost than they have to.

A Unifying Principle

- Good security, good performance, good usability, good design all agree on the same basic principle:
- Present people relevant information, allowing them to make good choices at the right time without distractions.

iSEC PARTNERS

Tools to Get the Job Done

- Shameless plug: httprof
  - http://code.google.com/p/httprof
- YSlow and HTTPFox (Firefox plugins)
- WebScarab: https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- Wireshark

iSEC PARTNERS

Demonstrating That the Internet Is Not Secure

- The Upside-Down-Ternet
- Cain and Abel
- Metasploit: http://blog.metasploit.com/2008/07/bailiwicked.html
- Ettercap
- Wireshark, tcpdump
- BGP forgeries: http://iar.cs.unm.edu/

iSEC PARTNERS

Conclusion

- Usability, design, security, and performance are all friends — not enemies.
- If you can't afford HTTPS, you can't afford to be in business.
- Luckily, you *can* afford HTTPS!

iSEC PARTNERS

Future Work

- Improve the security UI of browsers.
  - Usability is our biggest security problem right now!
  - And vice-versa!
- Improve the quality of browsers' treatment of TLS/SSL and PKI.

iSEC PARTNERS

Thank You

Questions?

Chris Palmer

chris@isecpartners.com

iSEC PARTNERS