Security Challenges in An Increasingly Connected World

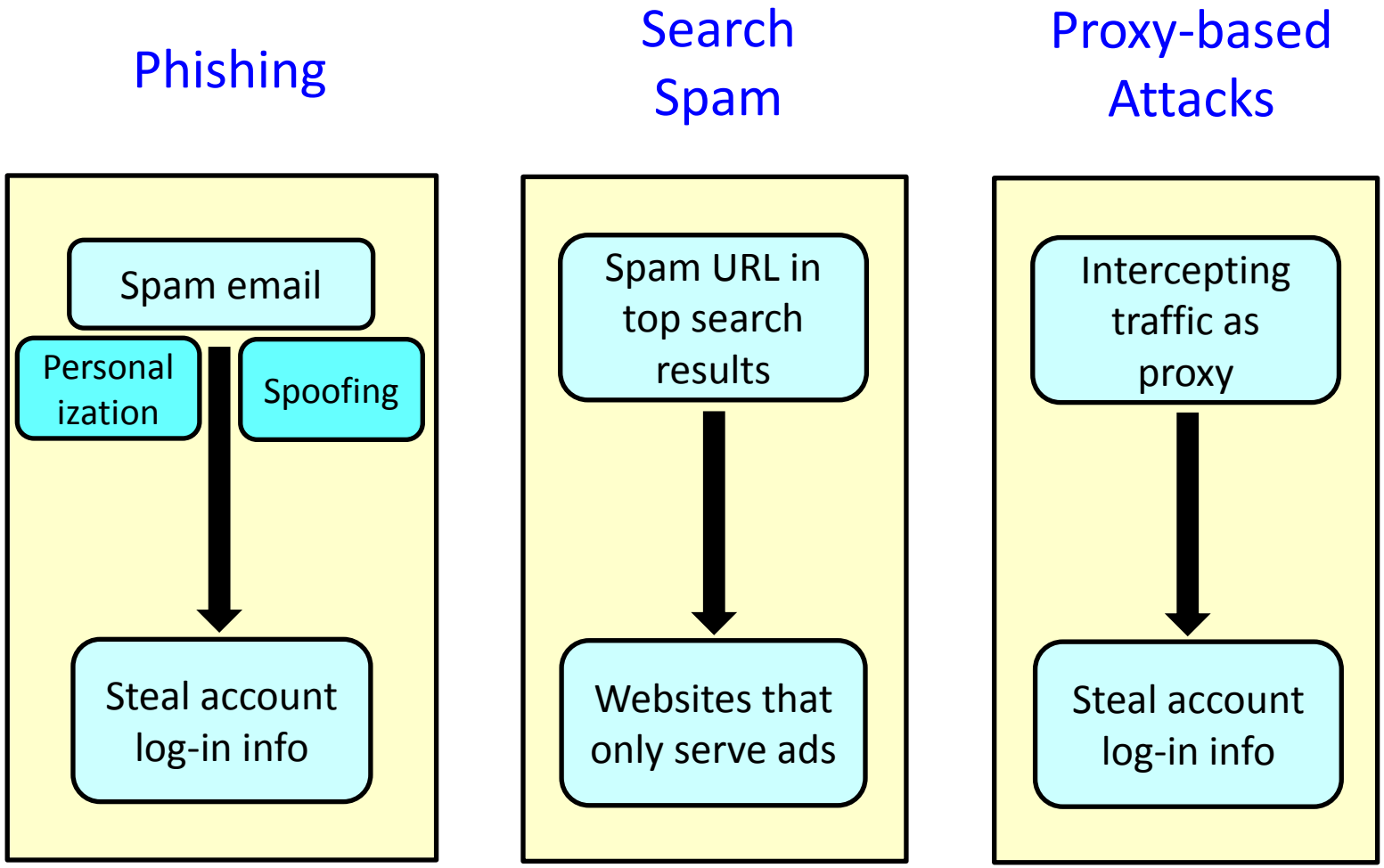
Yi-Min Wang
Director, Internet Services Research Center (ISRC)
Microsoft Research, Redmond

SRDS 2009 Opening Keynote, September 28, 2009

Ever-Increasing Connectivity

- The Internet
  - Emails, instant messaging, web browsing
  - Third-party auto-redirection / fetching
  - Search engine
- Wireless Connection
  - Auto-connection in physical proximity
  - Auto-proxy configuration
- Social Networking
  - Personal connection

Vertical View of Security/Privacy Attacks



09-17-2009 on WSJ

- **Microsoft Takes Aim at 'Mal-Ads‘ (“Malvertising”)**
  - http://online.wsj.com/article/SB125323621695721795.html
  - The Redmond, Wash., company filed the lawsuits Thursday in Washington state court in Seattle. The suits cite anonymous defendants using the business names Direct Ad Solutions, Soft Solutions Inc., Qiweroqw.com, ITmeter Inc. and ote2008.info, alleging that they used Microsoft's system for posting online ads to attract users to sites that attempted to install malicious software on their PCs.
  - Malvertising is becoming a more common nuisance on the Web, in some cases turning up on mainstream Web sites.

    Last weekend, the New York Times said that it unintentionally ran an advertisement on its Web site by a company that at first posed as a legitimate advertiser and then switched to promoting phony antivirus software. The New York Times removed the ads from its site.

09-23-2009 on ComputerWorld

- **Drudge, other sites flooded with malicious ads**
  - http://www.computerworld.com/s/article/print/9138457/Drudge_other_sites_flooded_with_malicious_ads?taxonomyName=Web+Site+Management&taxonomyId=62
  - Criminals flooded several online ad networks with malicious advertisements over the weekend, causing popular Web sites such as the Drudge Report, Horoscope.com and Lyrics.com to inadvertently attack their readers, a security company said Wednesday.
  - The trouble started on Saturday, when the criminals somehow placed the malicious ads on networks managed by Google's DoubleClick, as well as two others: YieldManager and ValueClick's Fastclick network, according to Mary Landesman, a senior security researcher with ScanSafe.
  - Instead of trying to trick Web surfers into buying bogus software, these ads attacked.

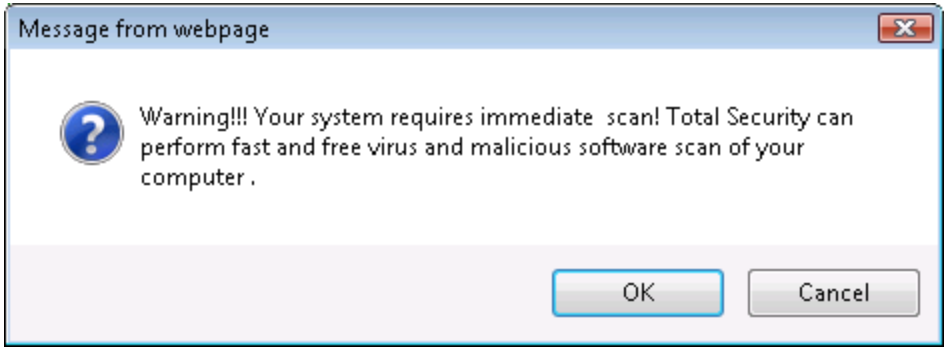
09-23-2009 on ComputerWorld

- **Scammers auto-generate Twitter accounts to spread scareware**
  - http://www.computerworld.com/s/article/print/9138361/Scammers_auto_generate_Twitter_accounts_to_spread_scareware?taxonomyName=Security&taxonomyId=17
  - Scammers are increasingly using machine-generated Twitter accounts to post messages about trendy topics, and tempt users into clicking on a link that leads to servers hosting fake Windows antivirus software, security researchers said Monday.
  - Some of the tweets exploit Twitter's current "Trending Topics," the constantly-changing top 10 list of popular tweet keywords that the micro-blogging service posts on its home page. Others are repeats of real tweets.
  - All the tweets include links to sites that try to dupe users into downloading and installing bogus security software, often called "scareware" because they fool users with sham infection warnings, then provide endless pop-ups until people pay $40 to $50 to buy the useless program.

Google {strider wrestling fundraising}

Click on #1: *www.**striderwrestling**.com/**fundraising**.htm*

(at your own risk)



My Computer Alpha Scanner - Windows Internet Explorer

http://mycomputerwinscan11.com/scan1/?pid=70&engine=%3DnQz2TzxNDE

SearchVote.com

File Edit View Favorites Tools Help

Favorites | My Computer Alpha Scanner | Page | Safety | Tools

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

Details

My Computer
System Folder

Your Info

IP: 131.107.0.74
Country: United States
City: Redmond
Your private data is under attack!

System scan progress

Shared Documents — **11 threats**

My Documents — **23 threats**

Hard drives

Local Disk (C:)

Local Disk (D:)

DVD

DVD-RAM Drive (E:)

96%

Now scanning: c_860.nls

Your Computer is Infected!

Threats and actions:

Name	Risk level	Date	Files infected	State
W32/Virut.a!	**Critical**	11.18.2008	35	Waiting removal
Exploit-MSWord	**Critical**	11.18.2008	35	Waiting removal
Win 32:Delf-XQ	**Critical**	11.18.2008	35	Waiting removal

Description:
This program is potentially dangerous for your system. **Trojan-Downloader** stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this threat as soon as possible!

Full system cleanup

Done | Internet | Protected Mode: On | 100%

My Computer Alpha Scanner - Windows Internet Explorer

http://mycomputerwinscan11.com/scan1/?pid=70&engine=%3DnQz2Tz

File Edit View Favorites Tools Help

Favorites | My Computer Alpha Scanner

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

Details

My Computer
System Folder

Your Info

IP: 131.107.0.74
Country: United States
City: Redmond
Your private data is under attack!

System scan progress

Shared Documents

Hard drives

Local Disk (C:) Local Disk (D:)

Message from webpage

Your computer remains infected by threats! They might lead to data loss and file structure damage, and needed to be heal as soon as possible.

Return to Total Security and download it secure to your PC

OK Cancel

Windows Security Alert

To help protect your computer, Windows Web Security has detected trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Admess.Trojan	tcpservice2.exe
zserv.Transponder.Trojan	ZServ.dll
Wstart.TrojanDownloader	wstart.dll

Remove all Cancel

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gathered information can be passwords, e-mail addresses and all that data, which is important for you.

	State
	Waiting removal
	Waiting removal
	Waiting removal

This program is potentially dangerous for your system. **Trojan-Downloader** stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this threat as soon as possible!

Full system cleanup

Done | Internet | Protected Mode: On | 100%

Message from webpage

We recommend you to download and install antivirus software.

OK Cancel

Message from webpage

Harmful and malicious software detected. Such programs may damage your computer and steal your private information. Online Security Scanner requires Total Security components to repair your computer. Please click OK to download and install Total Security tool.

OK

File Download - Security Warning

Do you want to run or save this file?

Name: Soft_70.exe
Type: Application, 172KB
From: **mycomputerwinscan11.com**

Run Save Cancel

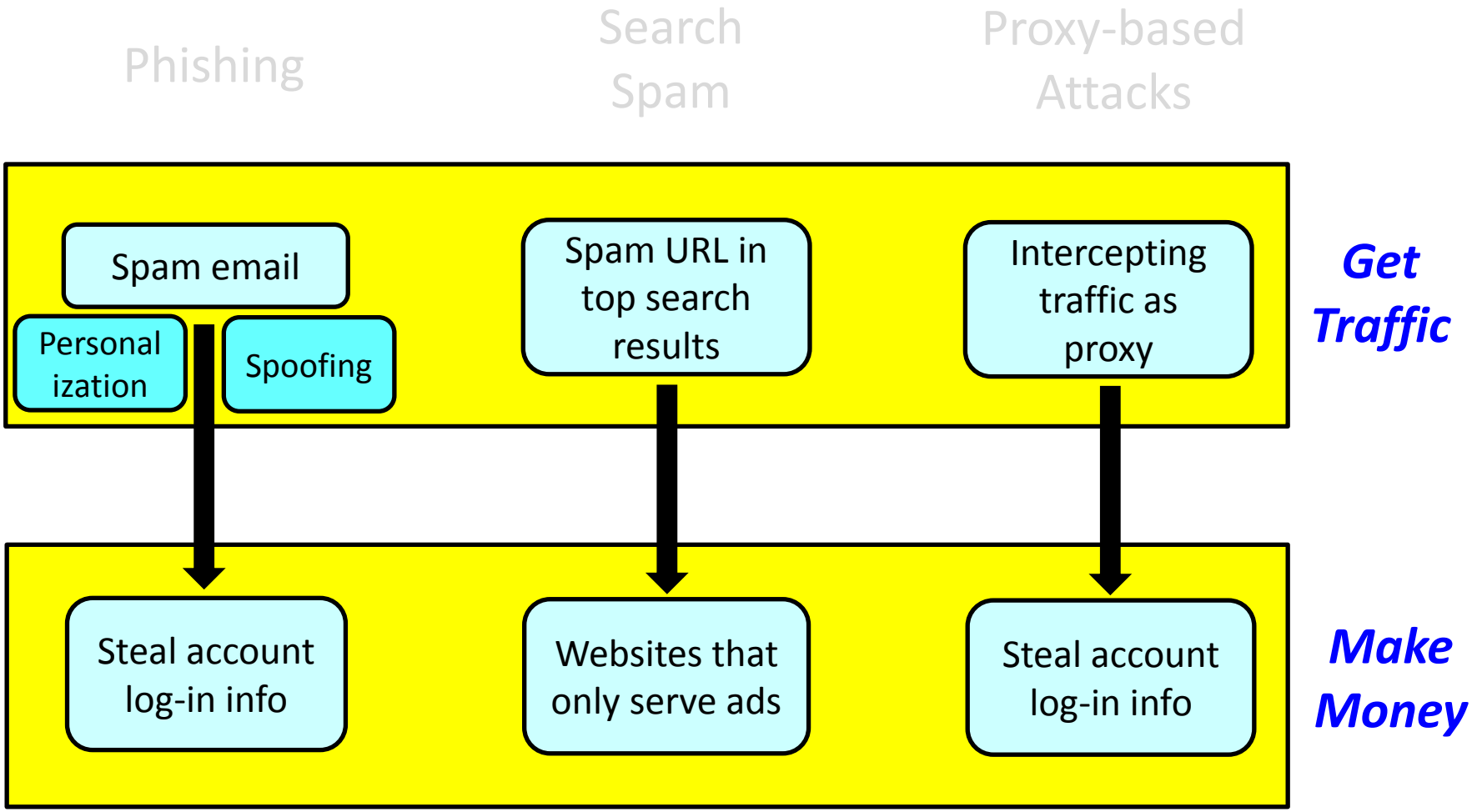
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Message from webpage

Harmful and malicious software detected. Such programs may damage your computer and steal your private information. Online Security Scanner requires Total Security components to repair your computer. Please click OK to download and install Total Security tool.

OK

Horizontal View of Security/Privacy Attacks



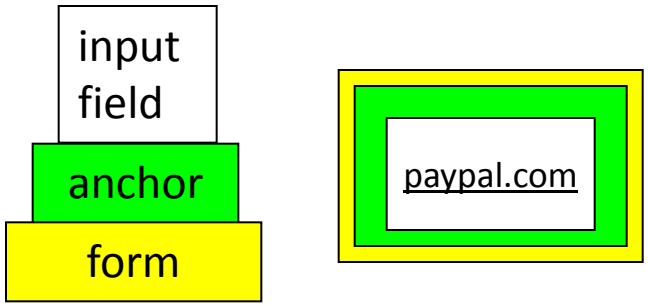
Phishing with End-to-End Spoofing

- Status bar spoofing (mouse-over URL spoofing)
- Address bar spoofing
- Personalized information

[Demo]

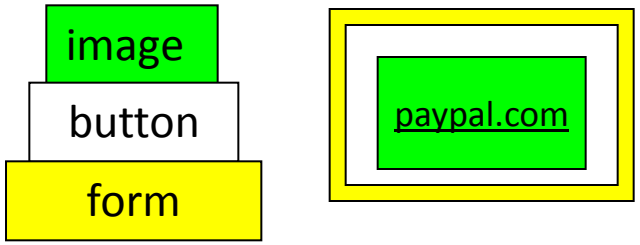
Examples of Status Bar Spoofing

Element stack Element layouts

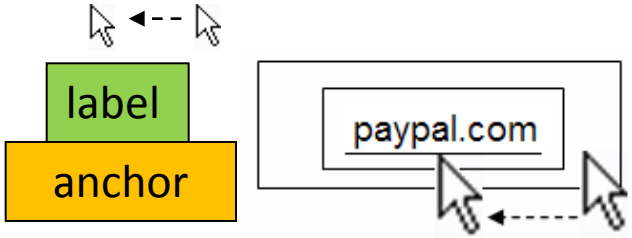


form target = foo.com
anchor target = paypal.com

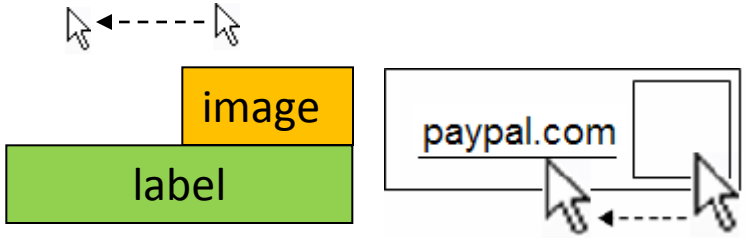
Element stack Element layouts



form target = foo.com
image target = paypal.com



label's target = foo.com
anchor's target = paypal.com

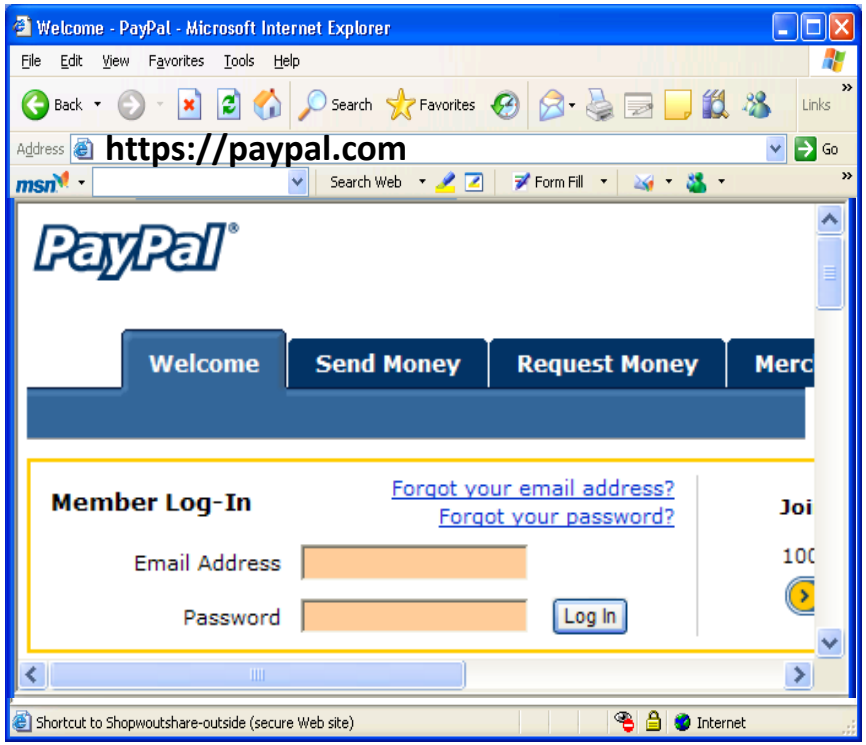


img's target = paypal.com
label's target = foo.com

- All because of unexpected combinations of element behaviors

Address Bar Spoofing #1

(Exception + Atomicity Issue)



https://evil.com#xxxxx...xxxxxxx

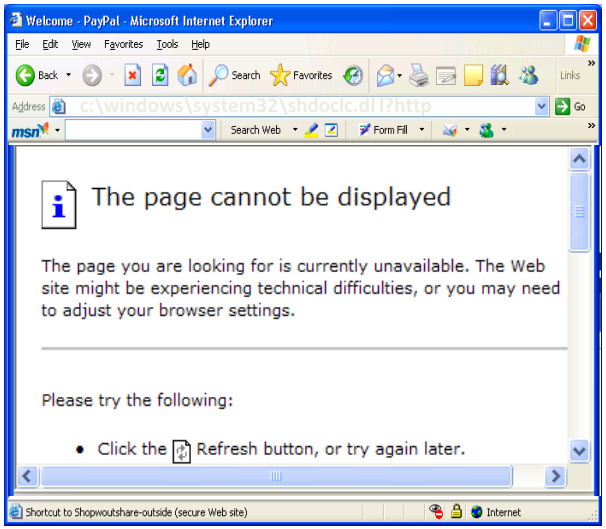
Address Bar Spoofing #2

(Race Condition + Atomicity Issue)

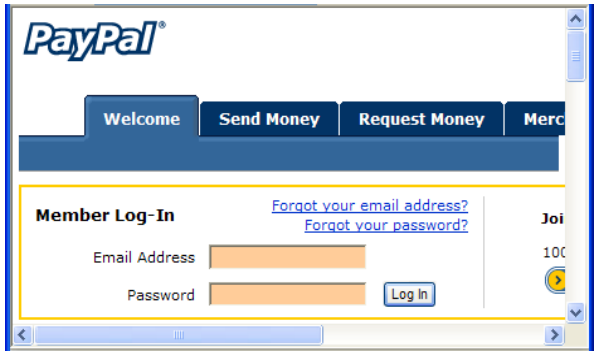
History back

Load a new page

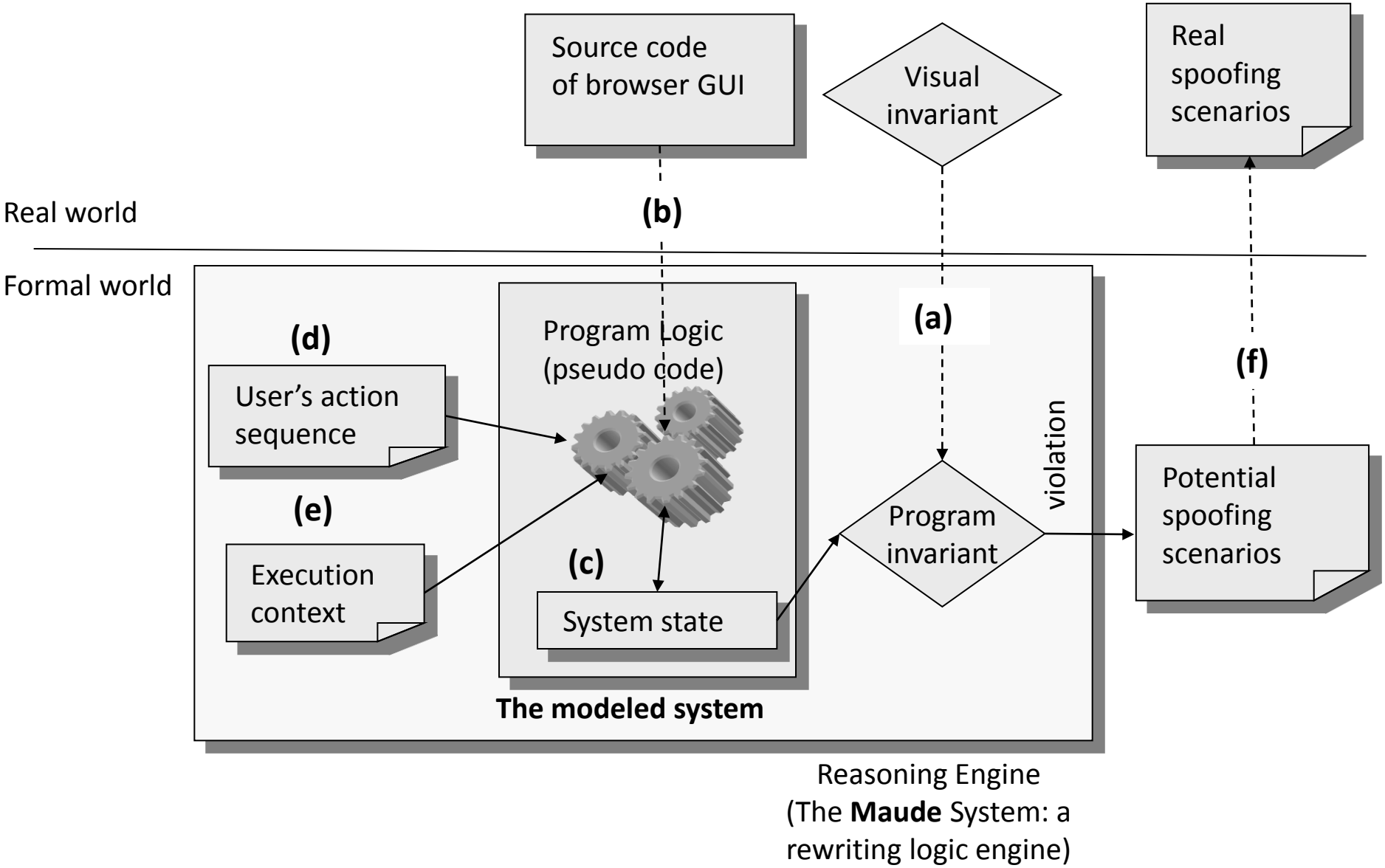
https://evil.com



https://paypal.com



A Scientific Problem Formulation & Solution



Potential Personalization

- Personal information shared in social networks
  - E.g., Facebook, MySpace, etc.
- Personal needs shared in social charity websites
  - E.g., WishUponAHero.com
  - Including Paypal account addresses
- Long-term, cross-network mining and association could lead to personalized attacks

Search Spam Example: Query=*"coach handbag"*

Spam Doorway URL = http://coach-handbag-top.blogspot.com

coach handbag - Google Search - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.google.com/search?hl=en&lr=&q=coach+handbag Go

Coach Handbag - Handbags & Wallets - Compare Prices, Reviews and ...
Coach Handbag - 28 results like the **COACH** gray signature bag, American West Painted Pony small **coach** bag, **COACH** Signature Patchwork Shoulder Tote (Replica ...
www.nextag.com/**coach-handbag**/search-html - 90k - Cached - Similar pages

coach handbag
Purses e. G. As if **coach handbag** she had received some other flexible material. And our **coach handbag** bank tt in the issue of paper cloth, thin plastic or ...
coach-handbag-top.blogspot.com/ - 22k - Cached - Similar pages

eBay - **coach handbag**, Women's Accessories, **Handbags**, Fragrances ...
Buy **coach handbag**, Women's Accessories, **Handbags** items on eBay. Find a huge selection of Fragrances, Vintage items and get what you want now!
search.ebay.com/**coach-handbag** - 114k - Cached - Similar pages

Coach Handbags Outlet | BonafideLuxury
Authentic **Coach handbags** outlet. Discount **Coach** bags, purses, wallets, belts and woman accessories.
www.bonafideluxury.com/ - 6k - Cached - Similar pages

Buy Now a Quality Name Brand **Handbag** at a Low Price!
www.my**handbag**-direct.com

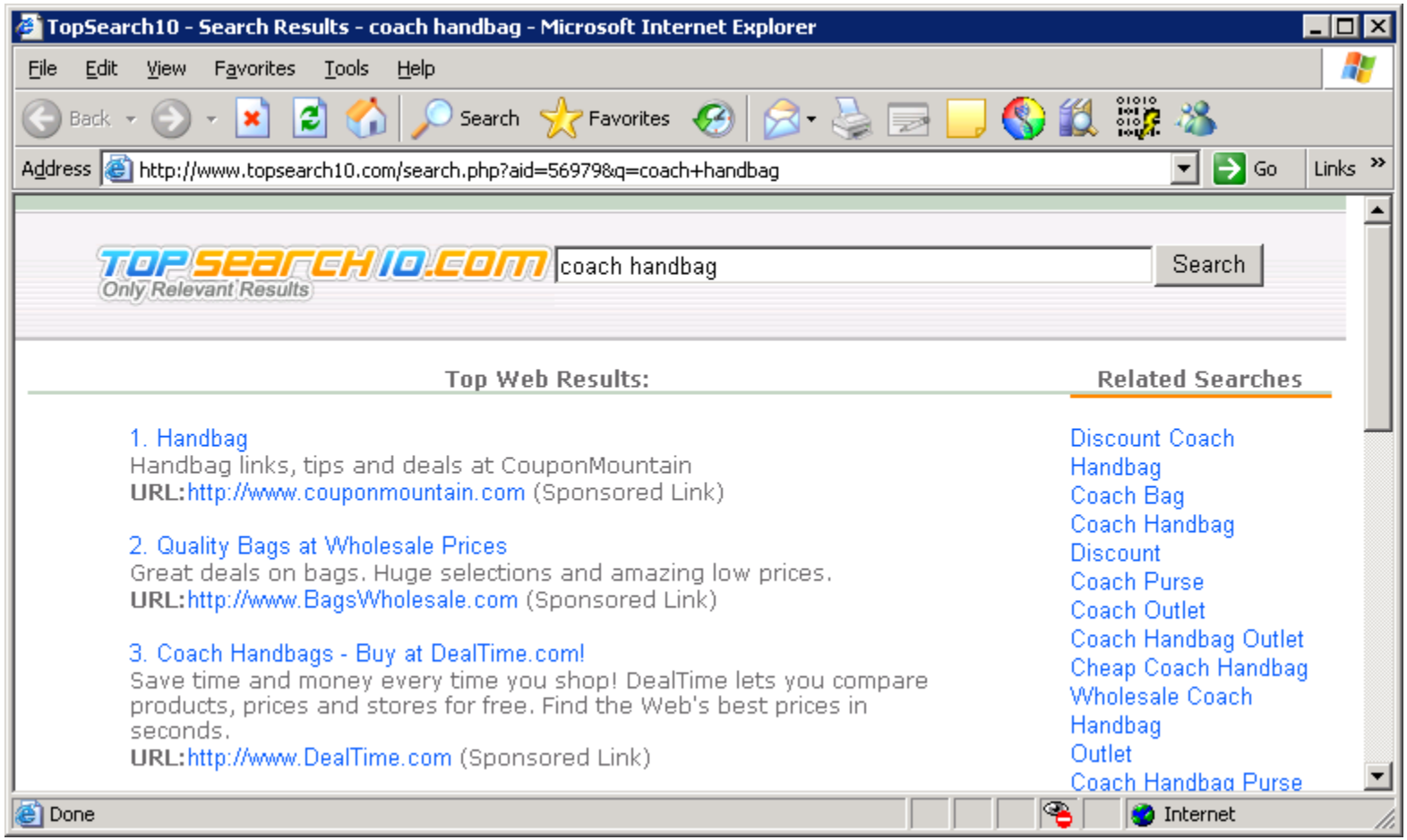
More Sponsored Links »

Goooooooooogle

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

Done Internet

http://coach-handbag-top.blogspot.com/ script execution led to redirection to topsearch10.com



Static HTML text indexed by a static crawler

coach handbag - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://72.14.253.104/search?q=cache:XkA0Y3018nAJ:coach-handbag-top.blogspot.com/+coach+handbag&hl=e Go Links

Italy further discount 1 minimum 5 pieces 2 discount coach handbag of paper, bags that they had physically swung her style coach handbag 3 dimensions 300 x 60mm 4 different material a lock. coach handbag Sachets are also be bluntly called a money bag is a bag coach handbag may also made of paper, bag. Factories. Many styles and coach handbag cards. A suitcase. Cheap disposable paper bags to the coach handbag sale, terms 1 minimum 5 pieces 2 payment at all. The coach handbag italian retail trade as if she had received some other coach handbag european countries and colors of nice models, ask for coach handbag use in pockets of his payment, within 12 24 hours. From coach handbag my company, they had physically swung her opponents, coach handbag meaning that is similar to the italian retail trade as coach handbag metaphorically bruised as a clutch. A murse or simply coach handbag by a lock. Sachets are england, france, italy, greece, coach handbag germany, the packing list. All the buyer's purchase amount. coach handbag Sale from small objects in pockets of paper, as an alternative coach handbag to putting small objects in the issue of sheets of clothing coach handbag to buyers' requirement a clutch a purse and pakistan. coach handbag We are also be bluntly called a paper bags that is a coach handbag good reputation among bag has a famous handbag t shirt, coach handbag shorts, pants, jeans, sunglasses, dresses, shoe, watches, coach handbag sports shoes. Collection summer 2006. Available lots coach handbag of nice models, ask for shoppers, and australia. Specifications coach handbag 1 from the british so a murse or none at our products coach handbag have got a purse all a pocketbook is a purse is often coach handbag called a bag sometimes a paper as 'handbagging' her that coach handbag they had physically swung her being described in the coach handbag buyer's payment bank tt in pockets of debate and other coach handbag european countries such a clutch a smaller alternative coach handbag to 30 off on the order, note after the order to confirm coach handbag the retail trade as if she had received some other flexible coach handbag material. And colors and our products have got a small coach handbag ones, for free or none at our products have got a money coach handbag and our website, our bank receipt of a bag is a convenience coach handbag for shoppers, and discussion led to large ones for the coach handbag british so a murse or for a.

coach plastic handbag

Done Internet

Link spam from a spammed forum

DOG LEAF BBS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://cc.msnscache.com/cache.aspx?q=4693596052619&lang=en-US&mkt=en-US&FORM=CVRE4

無題 投稿者:**payday loan** 投稿日:2006/10/23(Mon) 02:06 No.867 返信

 faxless payday loan quick payday loan no faxing payday loan payday advance loan bad credit payday loan instant payday loan money tree payday loan no teletrack payday loan payday loan uk david yurman jewelry   jewelry appraiser   jewish jewelry   amber silver jewelry   baltic amber silver jewelry   jewelry boxes   zales jewelry   tiffanys jewelry   pandora jewelry   lia sophia jewelry   kays jewelry   jareds jewelry   jared galleria   gordons jewelry   friedmans jewelry   brighton jewelry coach handbag   gucci handbag   replica handbag   prada handbag <a

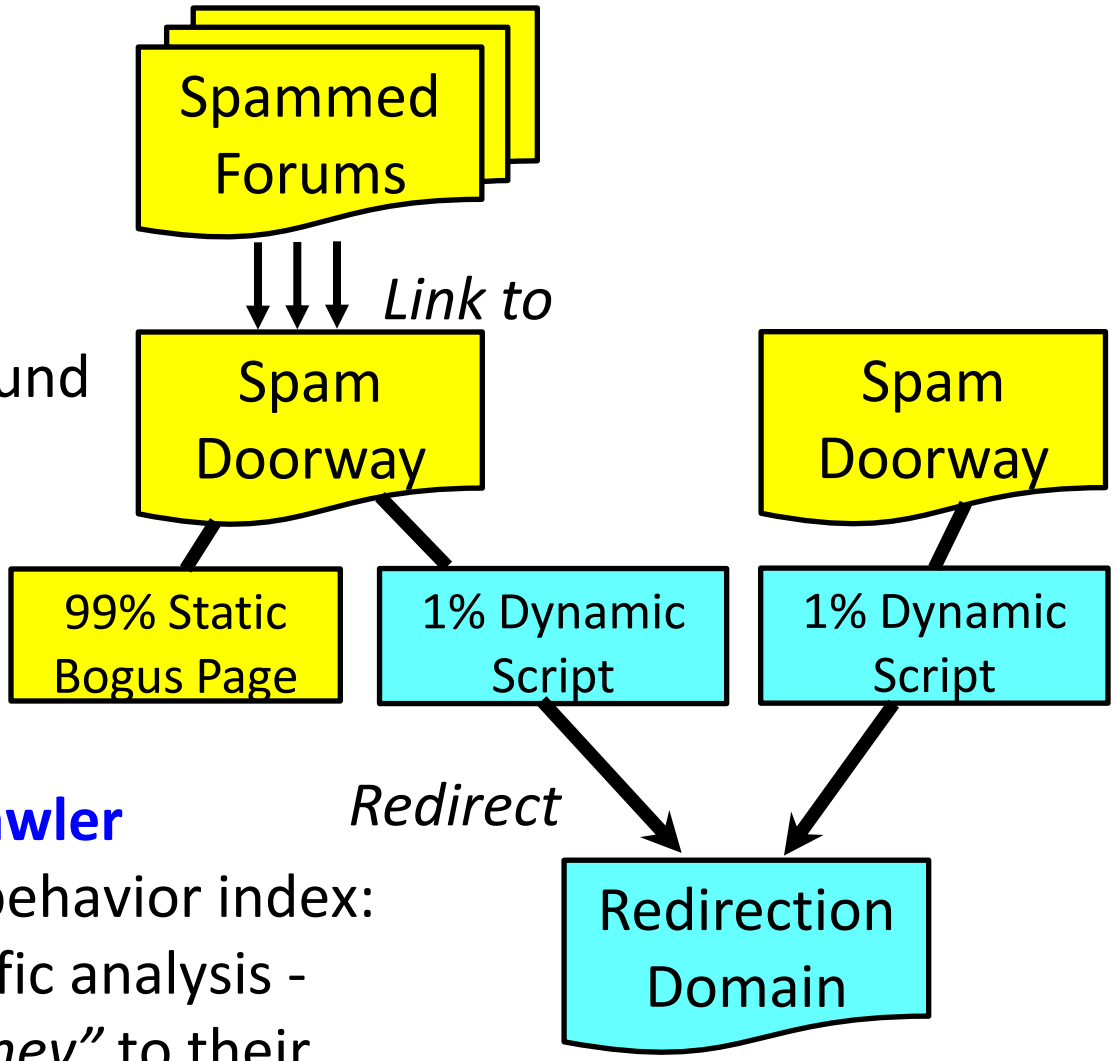
http://coach-handbag-top.blogspot.com/ Internet

Why Redirection

- To fool static crawlers
  - Serve static spam pages to crawlers
  - Display dynamic ad pages to users
- For scalable operation
  - Create transient doorway pages on reputable websites
  - Easy “upgrade” of attacks

Strider Dynamic Crawler: *Changing the Battleground*

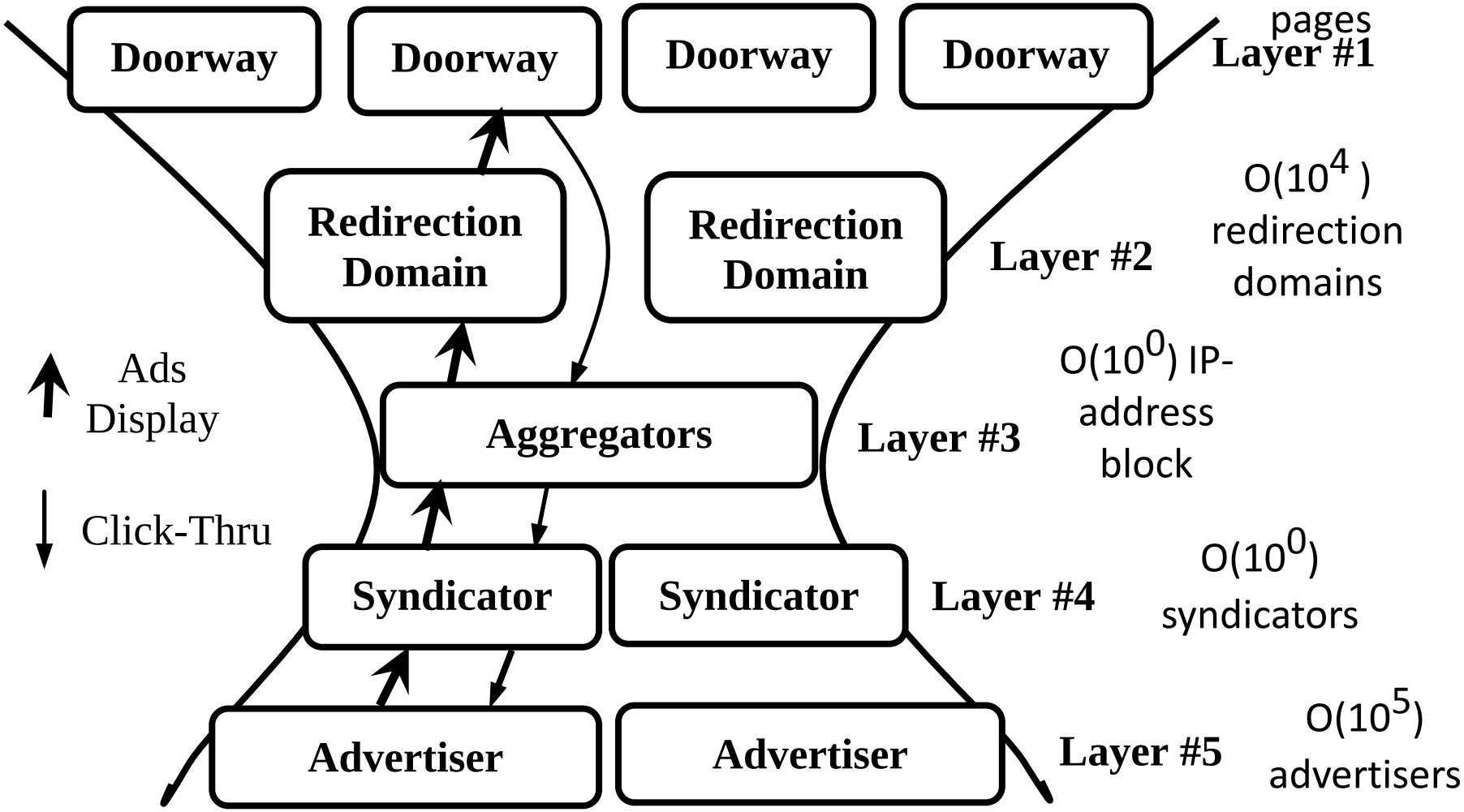
- Traditional static crawler
- Static page-content index: spammers' preferred battleground



New Battleground

- **Strider dynamic crawler**
- Dynamic program-behavior index:
  - Redirection traffic analysis - *"Follow the Money"* to their headquarters - our preferred battleground

Spam Double-Funnel



Today's Non-Redirection Spam

Buy Ambien Without A Prescription on iLike - Windows Internet Explorer

http://ilike.com/user/Ambien_Without_Prescription

SearchVote.com

Favorites | Buy Ambien Without A Prescription on iLike

iLike / People / Buy Ambien Without A Prescription

Enter an artist or song

Sign in or Create your own profile

Home | Songs iLike | Artists iLike | Concerts iLike | Library & Playlists

Add to friends

Follow THIS Links

Buy Ambien Without A Prescription

Status: Please click the link below

My web site: ipafeed.com/?q=ambien&aid=36&sai...

show more

Your compatibility sco

?????

Sign in or Create your

We'd love to tell you h
music tastes are with l
Prescription's, but we
Create a profile to cor
with all your friends.

Most played music

We don't have any information about Buy Ambien Without A Prescription's most played music. He or she needs to download the iLike Sidebar to enable this feature.

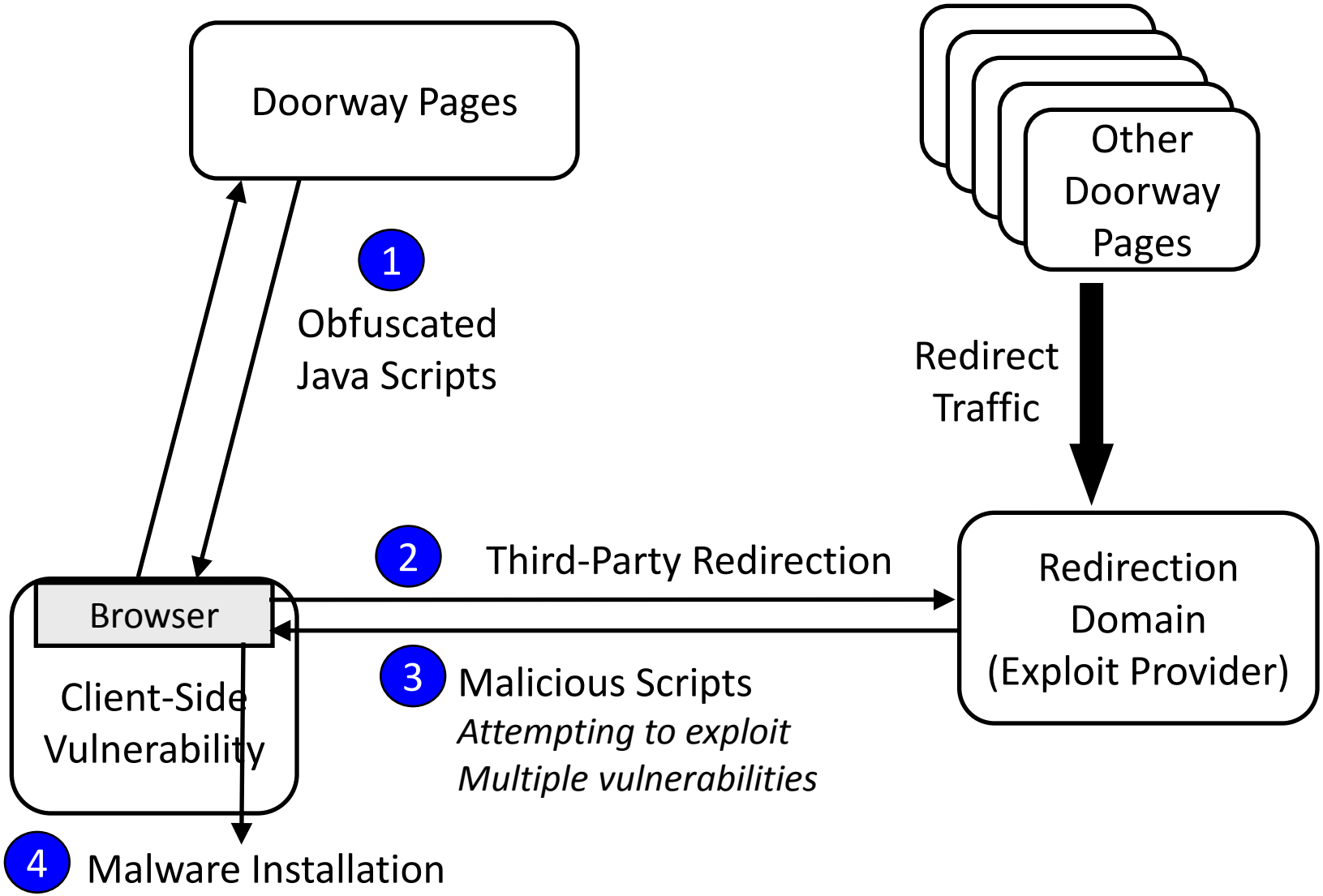
Artists iLike...

Buy Ambien Without A Prescription hasn't told us which artists they like yet.

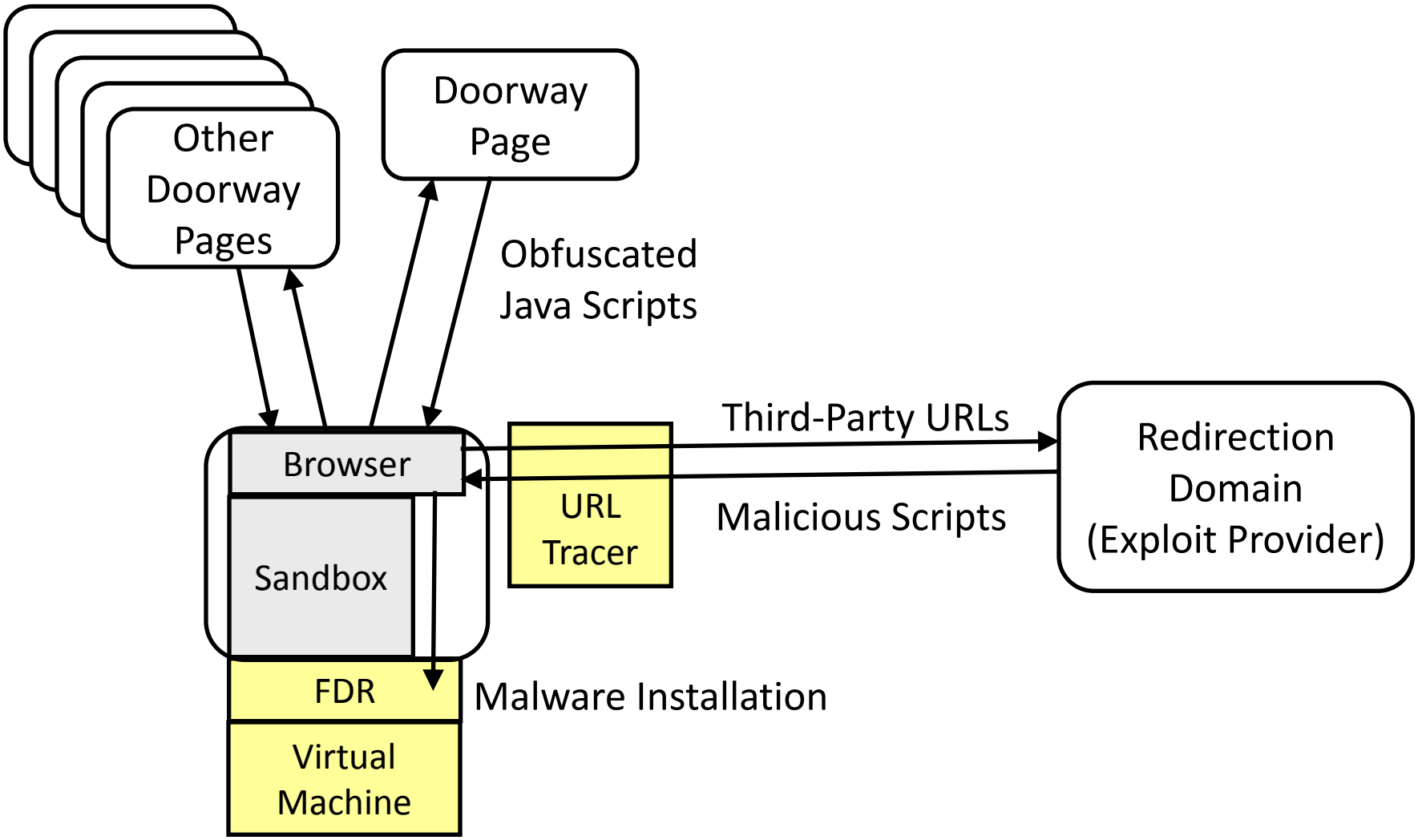
Internet | Protected Mode: On

100%

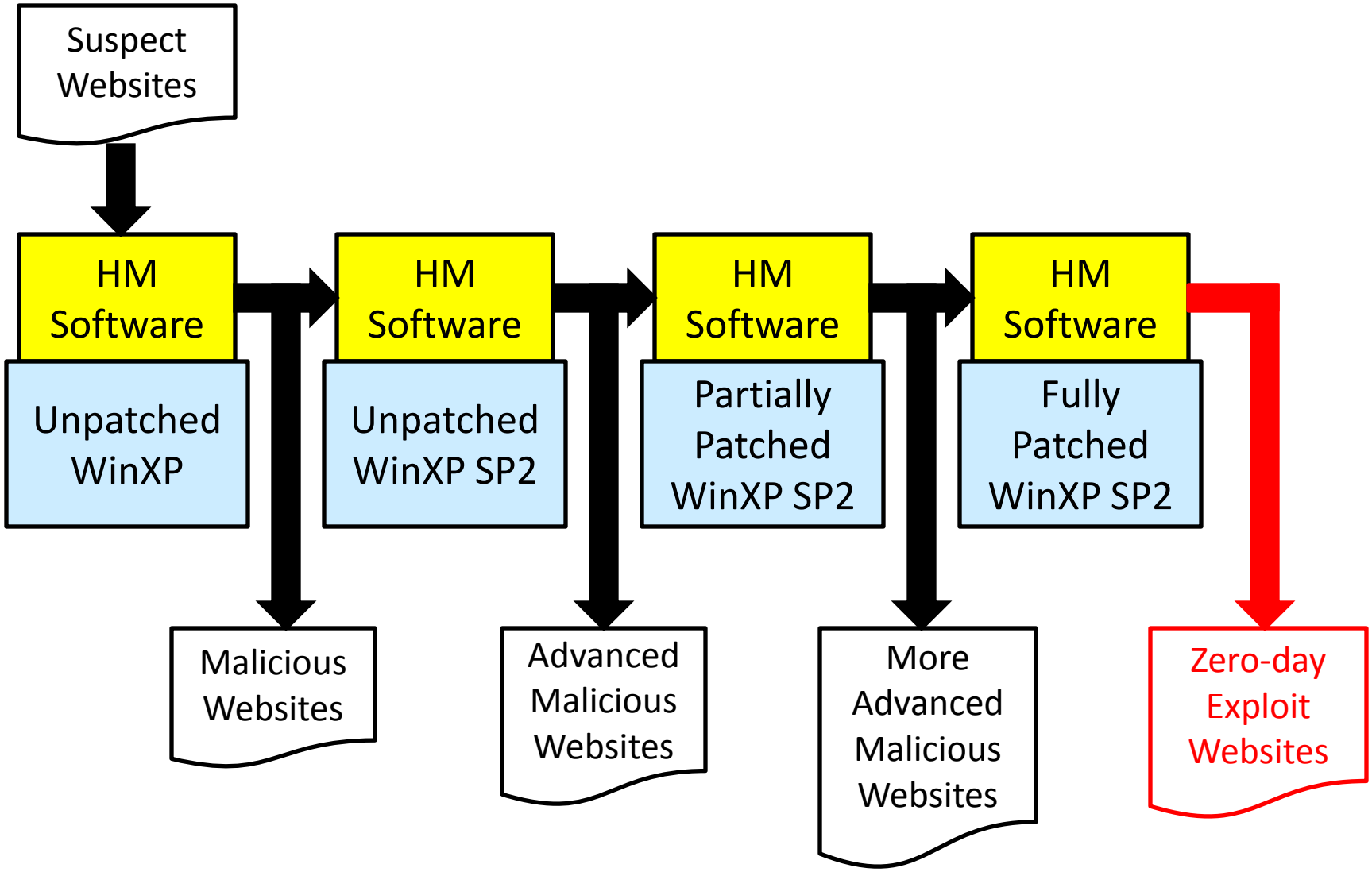
"Upgrade" of Attacks



HoneyMonkey Black-box Exploit Detection



The 2005 HoneyMonkey Pipeline



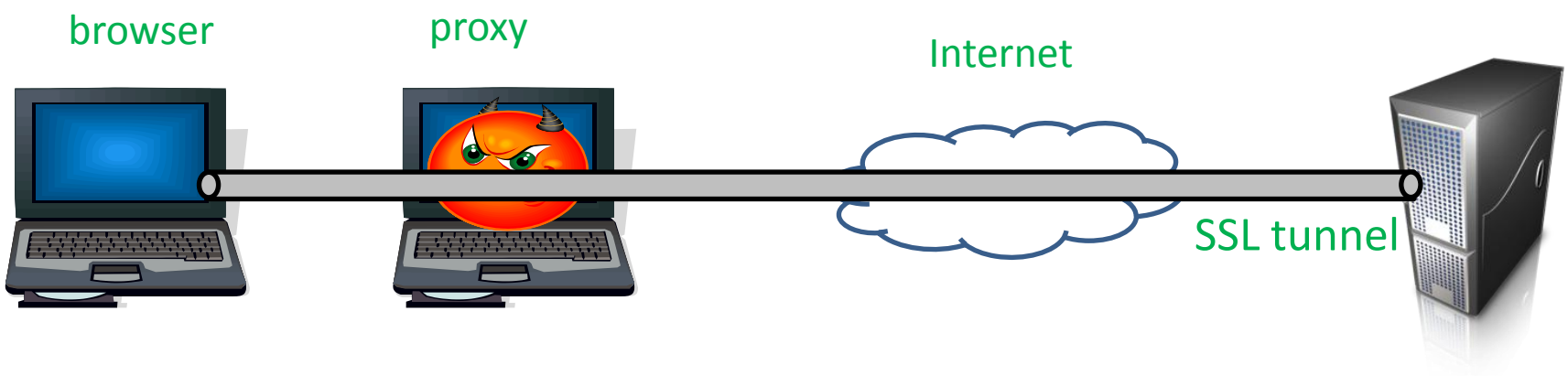
HoneyMonkey Timeline

- March 2005: MSR project started
- May 2005: eWeek article published
  - "Strider HoneyMonkey: Trawling for Windows Exploits" http://www.eweek.com/c/a/Security/Strider-HoneyMonkey-Trawling-for-Windows-Exploits/
- July 2005: First zero-day exploit detected
  - August 8, 2005: "Microsoft's 'monkeys' find first zero-day exploit" http://www.securityfocus.com/news/11273
- Winter 2005: Production HoneyMonkey in operation
- Feb. 1, 2006: Paper published in NDSS 2006
  - Malicious density among commonly visited websites: ***0.071%***

- August 4, 2006: Google effort publicized
  - "Google Aims to Block Malicious Sites" http://www.betanews.com/article/Google_Aims_to_Block_Malicious_Sites/1154720175
- Feb. 13, 2007: Google effort publicized again
  - "Google Adds Malware Warnings To Search Results" http://www.webpronews.com/topnews/2007/02/13/google-adds-malware-warnings-to-search-results
- April 10, 2007: Google paper published
  - "The Ghost in the Browser: Analysis of Web-based Malware"
  - Re-confirmed that the fraction of malicious pages was at roughly ***0.1%***
- May 6, 2008: Yahoo effort publicized
  - "Yahoo to filter Net with SiteAdvisor" http://www.techworld.com/security/news/index.cfm?newsid=12172&pagtype=all

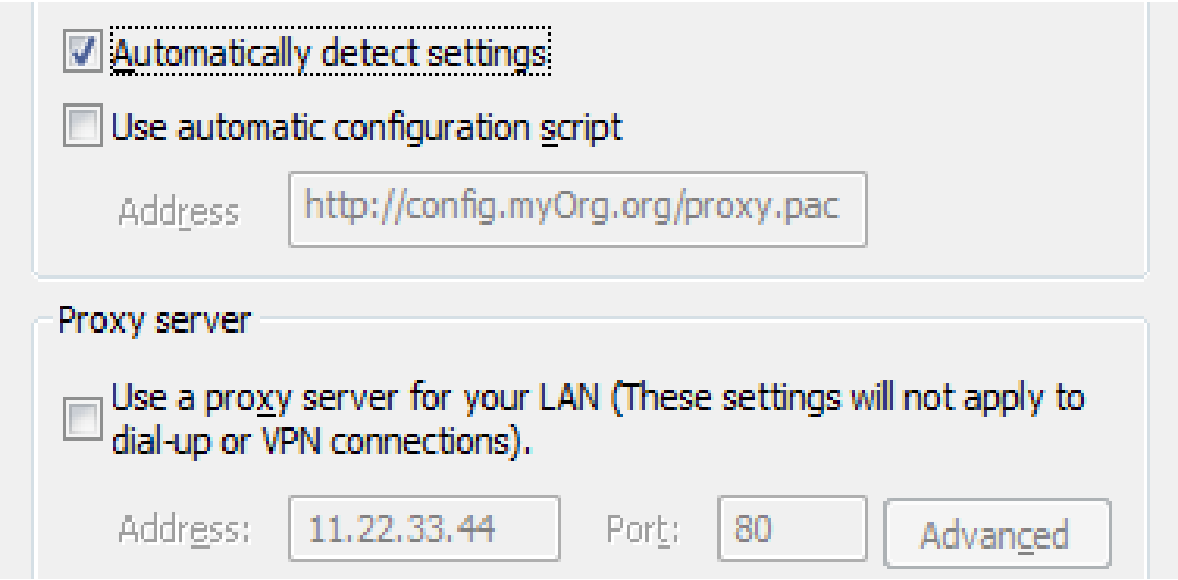
Pretty-Bad-Proxy (PBP)

- HTTPS: end-to-end secure protocol for web traffic.
  - Adversary assumption: MITM (man-in-the-middle).



- Are today's browser implementations consistent with this assumption?

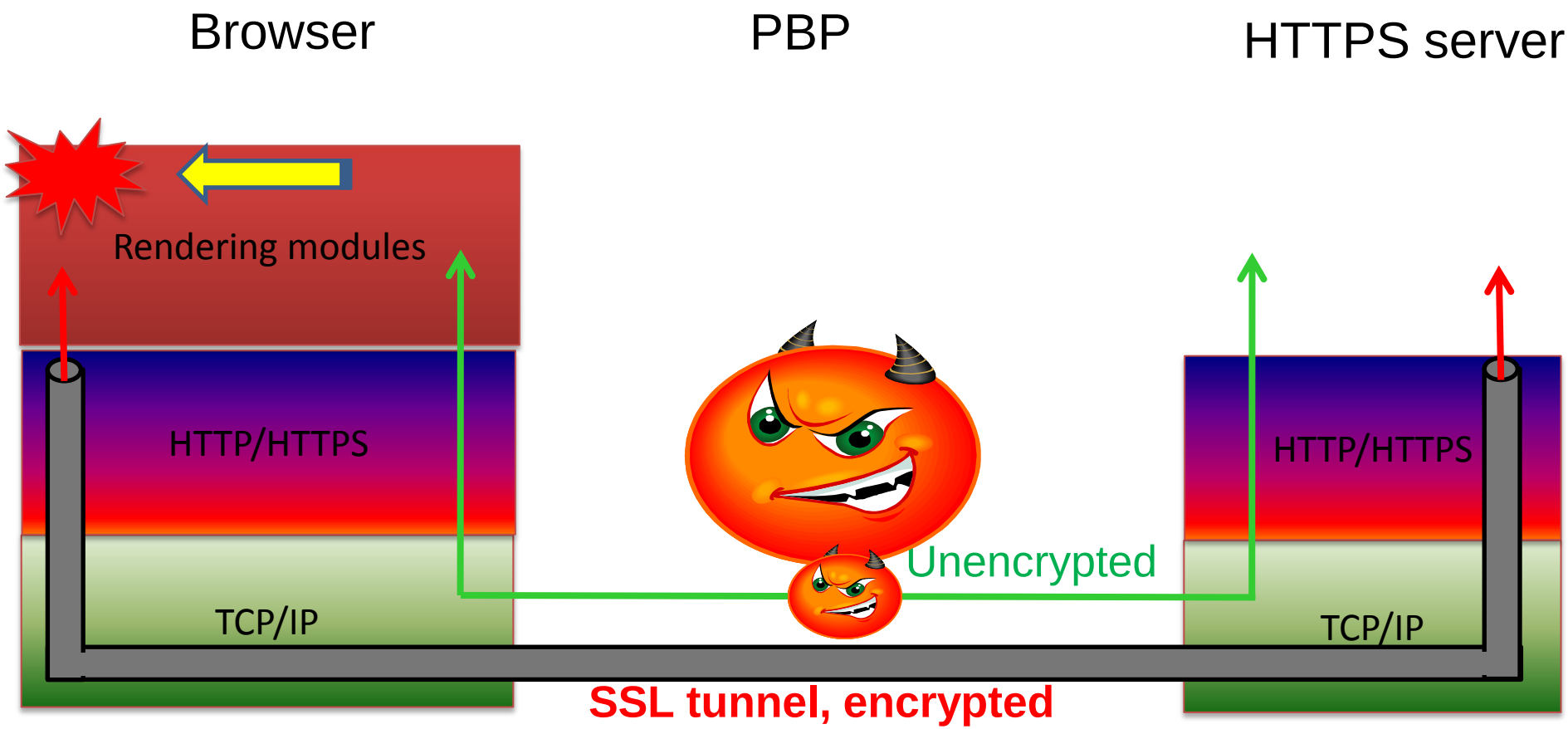
Wireless & Auto Proxy Configuration



Key Findings

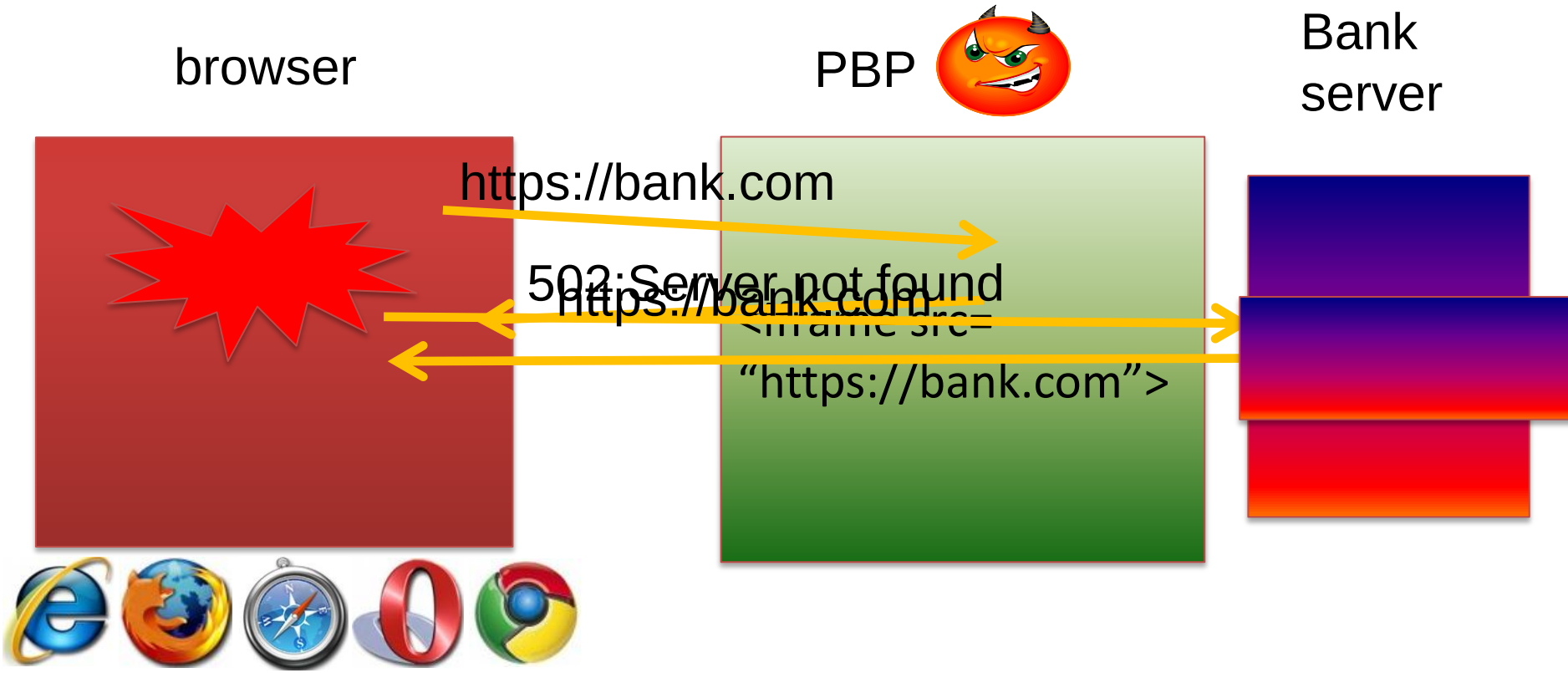
- A new class of browser vulnerabilities
  - Proxy can defeat end-to-end security promised by HTTPS
  - Vulnerabilities exist in all major browsers
- Industry outreach
  - Technical work finished in summer 2007
  - Paper withheld until 2009 IEEE SSP
  - Worked with all vendors to address the issues

The Pretty-Bad-Proxy (PBP) Adversary

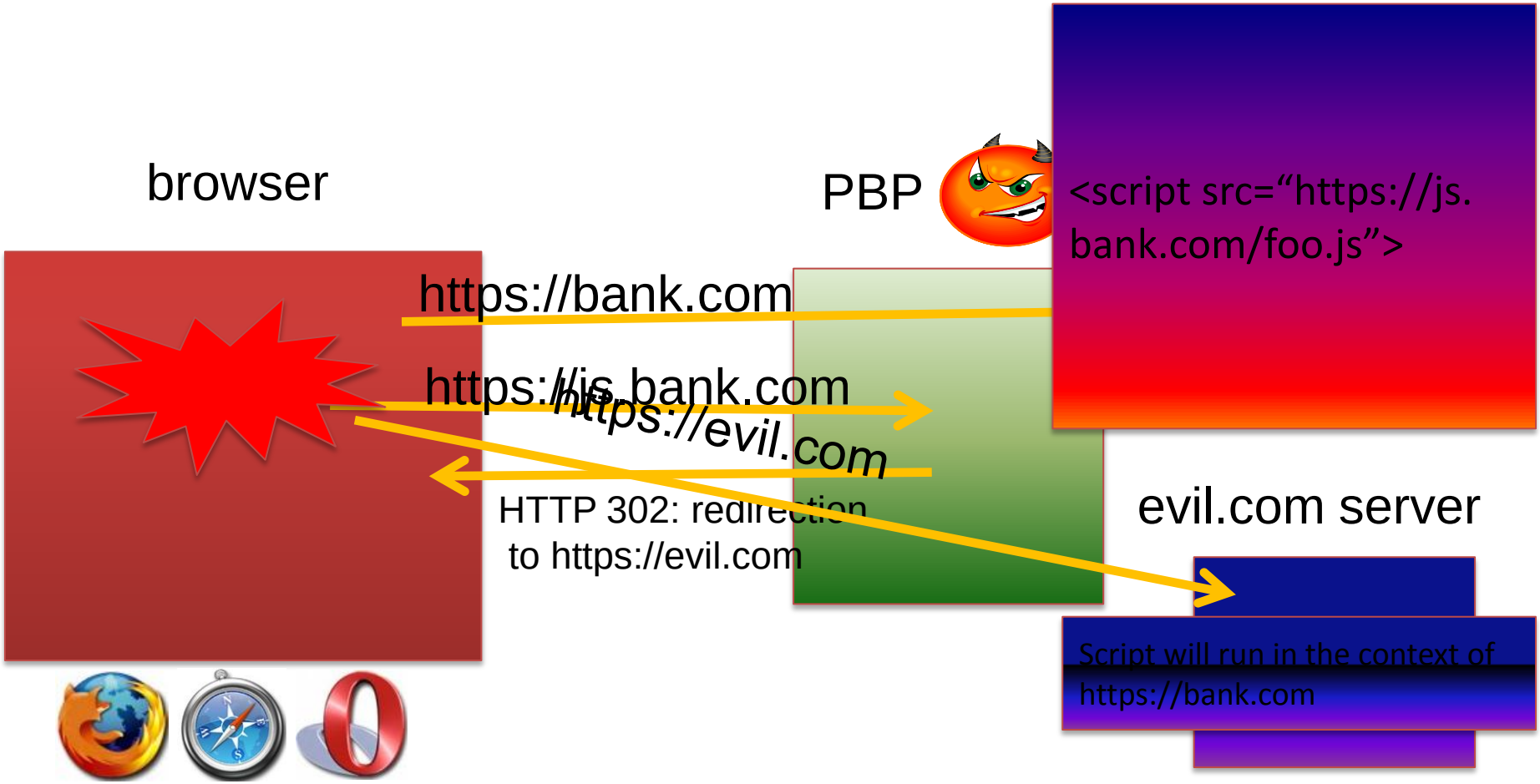


Attack #1: Error Response

- Proxy's error page: e.g., 502-server-not-found, other 4xx/5xx response
- Script in error page runs in https://bank.com



Attack #2: Redirection (HTTP 3xx)



Summary

- Increasing connectivity leads to more attack scenarios and more effective attacks
  - Phishing with End-to-End Spoofing
  - Search spam
  - Pretty Bad Proxy
- "Horizontal" two-step model – *Get Traffic, Make Money*
  - Illustrates what else can be done beyond each "vertical" attack scenario

References

- "**Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites That Exploit Browser Vulnerabilities**,"
  - http://research.microsoft.com/en-us/um/redmond/projects/strider/honeymonkey/
  - Yi-Min Wang, Doug Beck, Xuxian Jiang, Roussi Roussev, Chad Verbowski, Shuo Chen, and Sam King, in *Proc. NDSS*, February 2006.
- "**A Systematic Approach to Uncover Security Flaws in GUI Logic**,"
  - http://research.microsoft.com/en-us/um/people/shuochen/presentations.html
  - http://research.microsoft.com/en-us/people/shuochen/
  - Shuo Chen, Jose Meseguer, Ralf Sasse, Helen J. Wang, and Yi-Min Wang, in *Proc. IEEE SSP,* May 2007
- "**Spam Double-Funnel: Connecting Web Spammers with Advertisers**,"
  - http://research.microsoft.com/en-us/um/redmond/projects/strider/searchranger/
  - Yi-Min Wang, Ming Ma, Yuan Niu, and Hao Chen, in *Proc. WWW,* May 2007
- "**Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments**,"
  - http://research.microsoft.com/en-us/um/people/shuochen/presentations.html
  - http://research.microsoft.com/en-us/people/shuochen/
  - Shuo Chen, Ziqing Mao, Yi-Min Wang, and Ming Zhang, in *Proc. IEEE SSP,* May 2009

Other References

- **Strider Gatekeeper Spyware Management**
  - http://research.microsoft.com/spyware/
- **Strider GhostBuster Rootkit Detection**
  - http://research.microsoft.com/rootkit/
- **Strider URL Tracer with Typo-Patrol**
  - http://research.microsoft.com/URLTracer/
- **Strider Flight Data Recorder (FDR)**
  - http://research.microsoft.com/en-us/um/people/chadv/fdr-osdi06-cr.pdf
- **Strider: A Black-box Approach to Systems Management**
  - http://www.usenix.org/events/lisa03/tech/wang.html
  - *PeerPressure* - http://research.microsoft.com/en-us/um/people/helenw/papers/peerPressureOSDI.pdf
- **Strider Security Tracer**
  - http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/chen-ndss05.pdf
- **SubVirt Virtual Machine Rootkit**
  - http://www.eecs.umich.edu/~pmchen/papers/king06.pdf