

[Personalize this page](#) | [Sign in](#)

<form action="/search" name="f">

Web [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

<input name="hl"> en

<input name="q" size="55" maxlength="2048">

[Advanced Search](#)

[Preferences](#)

[Language Tools](#)

<input name="btnG">

Google Search

<input name="btnI">

I'm Feeling Lucky

[Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2007 Google

# Reflections on trusting the same-origin policy

... and other web+network trust issues

# me

## The North American Network Operators' Group

---

### General Information

- [What Is NANOG?](#)
- [Charter](#)
- [NANOG Endorsed by FARNET Membership, 26 October 1994](#)
- [Other Regional Networking Organizations](#)

### Meetings

- [Next Meeting: Tentatively scheduled for October 27-28 in Phoenix!](#)
- [Past Meetings and Presentations](#)
- [Tips for Hosting a NANOG Meeting](#)
- [Search Engine for the NANOG Notes](#)  
From Stan Barber, Academ Consulting Services

### Mailing List



- [Charter/AUP](#)
- [How to Join the NANOG Mailing List](#)
- [Searchable NANOG Mailing List Archive](#) from CCTec
- [NANOG Mailing List Archives](#) from Merit

- Andre Girona
- 15 years Unix+Internet experience
- First ran `www` in summer of 1993
- Cisco certified, NANOG attendee since '97
  - That means I'm a network guy more than a systems guy, programming guy, or security guy
- Phoenix native

# Past work

table 1008x501

## Vulnerability Research at lockdatasystems since 1997

table 537x295			<table border="1"><tr><td><a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a></td><td>File Size=660 bytes</td><td>profile</td></tr><tr><td><a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a></td><td>File Size=792 bytes</td><td>services</td></tr><tr><td><a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a></td><td>File Size=1 kb</td><td>products</td></tr><tr><td><a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a></td><td>File Size=2 kb</td><td>development</td></tr><tr><td><a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a></td><td>File Size=2 kb</td><td>who we are</td></tr><tr><td><a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a></td><td>File Size=2 kb</td><td>contact lds</td></tr></table>	<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=660 bytes	profile	<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=792 bytes	services	<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=1 kb	products	<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=2 kb	development	<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=2 kb	who we are	<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=2 kb	contact lds
<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=660 bytes	profile																			
<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=792 bytes	services																			
<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=1 kb	products																			
<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=2 kb	development																			
<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=2 kb	who we are																			
<a href="http://web.archive.org/web/20010331130919/http://www.lidsys.net/">Href=http://web.archive.org/web/20010331130919/http://www.lidsys.net/</a>	File Size=2 kb	contact lds																			
File Size=9 kb	File Size=8 kb	File Size=2 kb																			

lockdata systems

71broadway.newyork.ny.10006 T 212.863.9042 F 212.863.9041 E info@lidsys.net

- CatOS version 2.1
- IPv4 Vulnerability

File Size=20 kb

Several Cisco zero-day denial-of-service (IOS, CatOS)

# I'm bringing network back

- Routers are sexy
- Webapp security doesn't make network security obsolete or any less interesting / important
- There are plenty of innovations left in both camps
- There is plenty of cross-over between the two



# BGP

- Routing protocol
- 1993 CIDR
- Attributes

- Well-known or optional

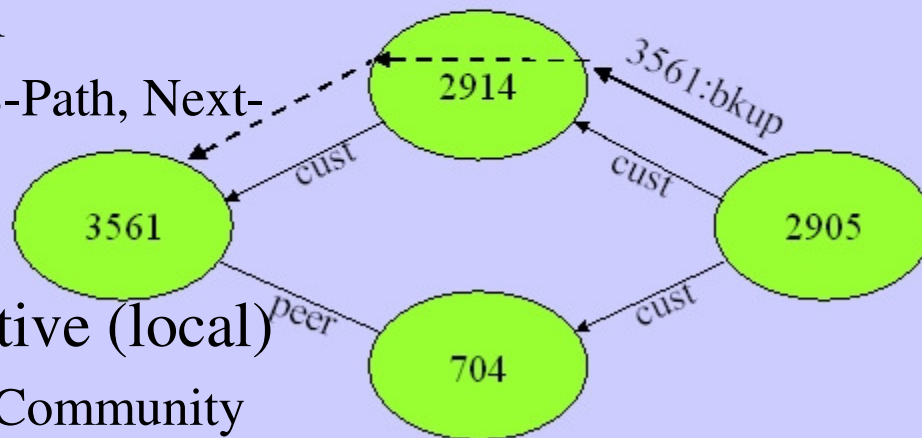
- Well-known: Origin, AS-Path, Next-hop, local-preference

- Transitive or non-transitive (local)

- Optional and transitive: Community
- Optional and non-transitive: MED

## Influence your Neighbor's Neighbor

- Can be used to give clues to peers and beyond
- Intermediate ASs must allow color to transit



# MPLS



- Enno Rey: LayerOne 2006 – MPLS Security
- Injection of label traffic from the Internet

# Wireless

Airport ad-hoc viruses +  
Karma =

World MITM

- *First New York, then San Francisco, New Orleans, Rio de Janeiro, Rome, Kinshasa, Karachi, Bangkok, and Beijing (from the movie, 12 Monkeys)*

## Your Wi-Fi can tell people a lot about you

By Joris Evers

Staff Writer, CNET News.com

Published: March 1, 2007, 6:40 PM PST

 TalkBack  E-mail  Print  del.icio.us  Digg this

**ARLINGTON, Va.--Simply booting up a Wi-Fi-enabled laptop can tell people sniffing wireless network traffic a lot about your computer--and about you.**

Soon after a computer powers up, it starts looking for wireless networks and network services. Even if the wireless hardware is then shut-off, a snoop may already have caught interesting data. Much more information can be [plucked out of the air](#) if the computer is connected to an access point, in particular an access point without security.

**"You're leaking all kinds of information that an attacker can use."**

--David Maynor,  
CTO, Errata Security

"You're leaking all kinds of information that an attacker can use," David Maynor, chief technology officer at Errata Security, said Thursday in a presentation at the Black Hat DC event here. "If the government was taking this information from you, people would be up in arms. Yet you're leaking this voluntarily using your laptop at the airport."

There are many tools that let anyone [listen in on wireless network traffic](#). These tools can capture information such as usernames and passwords for e-mail accounts and instant message tools as well as data entered into unsecured Web sites. At the annual Defcon hacker gathering, a "wall of sheep" always [lists captured log-in credentials](#).

Errata has developed another network sniffer that looks for traffic using 25 protocols, including those for the popular instant message clients as well as DHCP, SMNP, DNS and HTTP. This means the sniffer will capture requests for network addresses, network management tools, Web sites queries, Web traffic and more.

"You don't realize how much you're making public, so I wrote a tool that tells you," said Robert Graham, Errata's chief executive. The tool will soon be released publicly on the [Black Hat Web site](#). Anyone with a wireless card will be able to run it, Graham said. Errata also plans to release the source code [on its Web site](#).

# This old vulnerability: CLID

## Caller ID trust

- Spoofing CLID
  - Lax VoIP providers
  - Security screens (a misnomer?)
- Spoofing ANI
- Beige-boxing

**craigslist**<sup>B</sup>  
Listing online? Protect your privacy.

Your craigslist number is (602) 635 4371 x 520

When should we discontinue this craigslist number

Tell us where should we send your calls  \*  
10 digit US number

Click 'Submit' to activate your craigslist number  [Terms](#)

You can also get a FREE craigslist number by calling (415) 234 5678

Like craigslist? [Tell your friends](#) [craigslist factsheet](#) [Terms](#) [Privacy](#) © 2006-2007 craigslist

# Telespoof

- Home
- FAQs
- Rates
- Sign Up
- Login
- Contact Us
- Media Coverage

### Spoof Caller ID With Telespoof.com

Telespoof.com offers the first domestic and international Caller ID spoofing service, allowing business professionals to remain anonymous when calling from anywhere in the world, to anywhere in the world. We like to think of it as "mobile invisibility", the highest quality Caller ID spoofing service available anywhere in the world.

Our service is for business professionals within the U.S. including, but not limited to; Private Investigators, Skip Tracers, Law Enforcement, Collection Agencies and Lawyers, giving them freedom to choose any number as the Caller ID. Telespoof allows you to be whoever you want to be.

With toll free numbers in the U.S. and a web based interface, Telespoof offers clients access from wherever they may be. This means it is not required to be at a computer to use the service, yet the option is available for convenience.

While similar services have come and gone, Telespoof has proven its commitment to our clients and to remaining the longest lasting and most reliable source for Caller ID spoofing, after almost two years of operation.

Simply put, Telespoof will help you reach the person you want, safely and more cost efficiently. Stay anonymous and stay in business.

### Latest news:

October 28, 2006:  
Telespoof celebrates its second anniversary today, making us the longest lasting Caller ID spoofing service provider ever.

[Read more](#)

**SPOOF CARD FEATURES:**

- Caller ID Spoofing
- Voice Changer
- Call Recording
- Web Control Panel

No computer needed! Simply dial the toll free number from the calling card you purchase.



# Network Vulns: borken stuff

- Original SYN attack still works.. (juno-z)
- Mitnick hack: rlogin
  - Hosts.equiv, .rhosts
  - AIX rlogin –froot
  - Solaris 10/11: Oday was the case that they gave me
    - `telnet -l "-froot" 10.0.0.1`
- Smurf attack, DDoS
  - ICMP reflection
  - TCP amplification

[Full-disclosure] "0day was the case that they gave me" [Inbox](#) [Collapse all](#) [Print all](#) [Forward all](#)

☆ from [kcope <kingcope@gmx.net>](mailto:kingcope@gmx.net) [hide details](#) Feb 10 [Reply](#)

to full-disclosure@lists.grok.org.uk

date Feb 10, 2007 9:59 PM

subject [Full-disclosure] "0day was the case that they gave me"

"Alla pisteua gia sena,  
Alla phantasomouna,  
Nomisa pos magapouses,  
Kai geliomouna.  
Alla pisteua gia sena,  
Alla phantasomouna,  
Nomisa pos magapouses,  
  
Kai geliomouna."  
  
[http://www.com-winner.com/0day\\_was\\_the\\_case\\_that\\_they\\_gave\\_me.pdf](http://www.com-winner.com/0day_was_the_case_that_they_gave_me.pdf)  
[http://www.com-winner.com/Alla\\_pisteua.mp3](http://www.com-winner.com/Alla_pisteua.mp3)  
<http://www.com-winner.com/anothernicesong.mp3>

G0 f3tch y0ur Sol10 r00tkitz :)

Signed,  
Eliteboy

---

Full-Disclosure - We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
Hosted and sponsored by Secunia - <http://secunia.com/>

↑ Tyop?

# Advanced Network Vulns: trust

- BGP nastiness
  - Jack moves, AS loops, Stealing traffic
- Proxies
  - Tor (we'll get to this a little later...)
  - Firewall hole punching (Skype, chownat)
- MITM

Arp poisoning, DNS hijacking, cache poisoning, Wireless, STP takeover, HSRP/VRRP takeover, MPLS VPN / VPLS label modification / injection, VLAN / VPN hopping, CAM table overflow, Slipping windows

## EXAMPLE USAGE

```
Two machines exist across the Internet.
Machine nat1 is behind a NAT.
Machine nat2 is behind another NAT.
Machine nat1 is running a web server on port 80,
however it cannot be accessed because it is behind a NAT.
Machine nat1 wants to let nat2 connect to its web server.
```

```
In this case, nat1 runs:
./chownat.pl -d -s 80 nat2.com
```

```
And nat2 runs:
./chownat.pl -d -c 8000 nat1.com
```

```
nat2 connects to http://localhost:8000 in their local browser
and will access the http server nat1 has running on port 80
```

```
Similar scenario with ssh:
ssh server side:
./chownat.pl -d -s 22 nat2.com

client side:
./chownat.pl -d -c 1234 nat1.com
ssh -p 1234 user@localhost
```

NANOG Web  
Back to: [NANOG Home](#)

## Abstract: Peering Dragnet: Examining BGP Routes Received from Peers

Tom Scholl & Aman Shaikh, AT&T Labs  
Nathan Patrick, Sonic  
Richard Steenbergen, nLayer

In the hot-potato settlement-free peering world of today, there is an expectation that all peers play & advertise routes equally. However, in reality, some settlement-free peers may attempt to short cut and modify advertisements resulting in you hauling traffic a bit farther than needed. This presentation looks at ways this is done today, some specific examples of this as well as other interesting things you can learn by examining routes received (but maybe not accepted) at all points in a network.

### About the Presenters

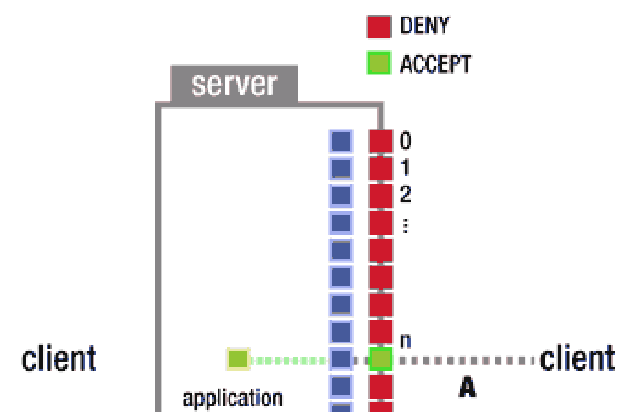
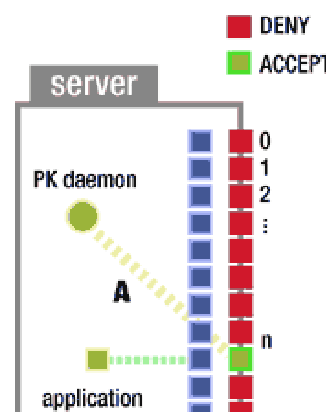
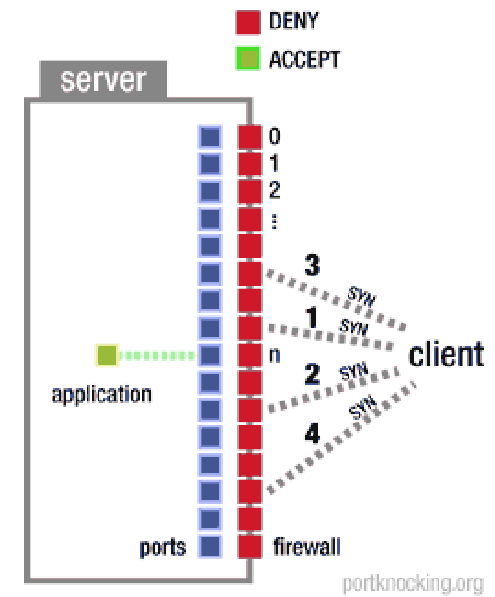
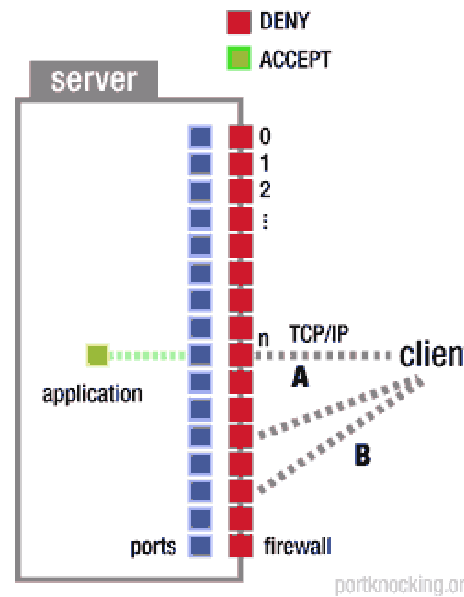
**Tom Scholl** is a Senior Technical Consultant in the global IP core network design & routing group in AT&T Labs. He works on network design and routing architecture as well as the SBC network integration. Tom has spent his last several years at what was SBC and prior to that, Ameritech. When not working, Tom can be found on IRC discussing routing, networking hardware and the NINAF protocol.

**Aman Shaikh** is a member of Network Performance and Engineering Department at AT&T Research where he works on IP route monitoring and several projects related to IP routing. His general research interests lie in the areas of IP routing and network management. Aman obtained his Ph.D. and M.S. from University of California, Santa Cruz. His home-page can be found at <http://www.research.att.com/~ashaikh>

**Richard Steenbergen** is the Co-Founder of nLayer Communications, where he currently serves as Chief Technical Officer and devotes a significant amount of time to the strategic management of peering relationships. Previously, he served as a Sr. Network Engineer for several large NSPs, and was the Sr. Software Engineer responsible for developing optimized routing technologies at netVmg, Inc.

# Network defenses

- Deep packet inspection at line-rate
    - Stop SYN DoS. Use IPS-like features
  - Secure Shell, Public key crypto
    - Stop using cleartext. Portknocking, GPG, OTR
  - Protecting the infrastructure
    - Reflection and amplification attacks
- <http://www.nanog.org/mtg-0405/mcdowell.html>



# Advanced network defenses

- Route filtering, SIDR, PGP-Whois
  - <https://Prefix.PCH.Net>
  - IETF SIDR WG
  - DHS SPRI
- Proxy scanners, pedantic perimeters
  - Separate DNS servers from infrastructure
  - Never allow outbound SYN from DMZ
  - Perform Firewall Differential Analysis
- SSL (DHE), Cisco port-security + DAI
  - Stop MITM attacks
  - Enforce local DNS/DHCP (not over WAN)

## Secure Inter-Domain Routing (sidr)

Last Modified: 2007-02-20

Additional information is available at [tools.ietf.org/wg/sidr](https://tools.ietf.org/wg/sidr)

### Chair(s):

- [Sandra Murphy <sandy@tislabs.com>](mailto:sandy@tislabs.com)
- [Geoff Huston <gh@apnic.net>](mailto:gh@apnic.net)

### Routing Area Director(s):

- [Ross Callon <rcallon@juniper.net>](mailto:rcallon@juniper.net)
- [Bill Fenner <fenner@research.att.com>](mailto:fenner@research.att.com)

### Routing Area Advisor:

- [Ross Callon <rcallon@juniper.net>](mailto:rcallon@juniper.net)

### Technical Advisor(s):

- [Steven Bellovin <smb@cs.columbia.edu>](mailto:smb@cs.columbia.edu)

### Mailing Lists:

General Discussion: [sidr@ietf.org](mailto:sidr@ietf.org)

To Subscribe: [sidr-request@ietf.org](mailto:sidr-request@ietf.org)

# Web vulns: extra borken stuff

## Steal Browser History Without JavaScript

Well, the server is back up and running (big thanks to id - during our upgrade there was a drive failure causing us to have to switch machines), and to celebrate I didn't want to come back with a boring post that would make you question why you read this site. So instead I decided to play around with some CSS tricks - bare with me for a minute. I don't know why, but I really think CSS is going to get worse over time. Anyway, as I was poking around I happened across one of the missing pieces of the puzzle to solve a simple problem in using CSS to hack - the lack of conditional logic.

Keeping this in mind it would be great if you could create a form of conditional logic in CSS. Well I finally figured out a way. Using a hybrid of a visited and display: attribute you can detect that the user has visited a page and more importantly perform an action based on that fact. The actions are somewhat limited if you can't use JavaScript, however, one action is enough. The reason being, when something is set to display:none it will actually cause the HTML tag that it references to not render. Setting the background: image attribute for the visible tag to use a URL of a logging CGI script allows you to send a request to a remote webserver based on the conditional logic as mentioned above.

Now, the only lacking part is the state management, and that can easily be tied together using a unique cookie, and/or an IP address in the QUERY\_STRING or anything else you want to use to identify the user. In this way, the remote website can steal history information from the user without ever once using JavaScript, or any client side programming. [Click here for a proof of concept of the CSS history theft without using JavaScript](#). This works nearly instantly, so it is far better than the JavaScript-less intranet hacking and pdp's version of the JavaScript CSS history hack in terms of speed. The only latency is the time it takes your browser to request the images associated with each URL you've visited - which is nearly instant since I don't return any data (and thanks to browser threading). The other nice thing about this is that it works beautifully in both Internet Explorer 7.0 and Firefox 2.0.0.2 (although it doesn't work in Opera 9.22).

So now we've eliminated the JavaScript pre-requisite from Intranet port scanning, cross site request forgeries, session riding and of course CSS history hacking. The only thing we can't yet do without JavaScript is read cross domain (and I stress the word yet). What else is left? I don't mean to sound ho-hum about this, but really, what else do we have to do? Are there any nay-sayers left?

- No order for HTTP headers (except method + version)
- Forms and cookies can be huge, unvalidated

# Advanced web vulns: trust<sup>2</sup>

- mhtml vulnerability: own the whole browser
- Firefox pop-up blocker reads local files
- Exponential Cross-Site Scripting (XSS <sup>n</sup>)
- Ajax and XHR now allow breaking of same-origin. ... so does any external JS/DHTML
- Flash does, too, if not configured properly. If configured properly: flash can be good!
- Anti-DNS Pinning (via JS, Flash, and Java applet)
- Cross-site cooking, Homograph attack
- HTTP request smuggling (and splitting, et al)
- HTML and Javascript network/port scanning

# Web+Network attacks

- IP address-based authentication
  - Spoofing and MITM (Wireless) break this
  - BGP and MPLS break this
  - **Proxies break this**
  - Layer One Session Hijacking
- XSS Shell
  - Combination of XSS proxy, History/cache enumeration, JS network/port scanning, clipboard grabbing, and even instant messaging!

## Solutions Worthy of Paranoia

There is hope, or rather, there are gruesome hacks, that can bring the splendor of seamless cross-browser `XMLHttpRequests` to your developer palette. The three methods currently in vogue are:

1. **Application proxies.** Write an application in your favorite programming language that sits on your server, responds to `XMLHttpRequests` from users, makes the web service call, and sends the data back to users.
2. **Apache proxy.** Adjust your Apache web server configuration so that `XMLHttpRequests` can be invisibly re-routed from your server to the target web service domain.
3. **Script tag hack with application proxy** (doesn't use `XMLHttpRequest` at all). Use the `HTML script` tag to make a request to an application proxy (see #1 above) that returns your data wrapped in JavaScript. This approach is also known as [On-Demand JavaScript](#).

The basic idea of all three hacks is the same: fool your user's web browser into thinking that the data is coming from the same domain as the web page.

A word of caution here: there is a good reason why `XMLHttpRequests` are restricted. Allowing them to freely access any domain from within a web page opens up users to potential security exploitation. Not surprisingly, these three hacks, which offload the request to your web server, potentially threaten to disparage your web server's identity, if not its contents. Caution is advised before deploying them.

- WS Proxy Injection

# Web+network attack examples

- Using Tor with .edu exit nodes over the Internet
  - StrictExitNodes 1
  - ExitNodes a.edu, b.edu, c.edu
- HTTP Referer checks stop proxies? Spoof the headers!
- My 0-days that you can bring home to mom
  - ProQuest: **vulnerable**
  - LexisNexis: **vulnerable**
  - ACM / IEEE: **vulnerable**

SHELVE Tsinghua University • Logout >

## Welcome to Safari

Welcome Tsinghua University User.

Logout

### RSS

Grab new Safari titles with our RSS 1.0 feed!

[RSS](#)

### Publishers on Safari

- O'Reilly
- Sams
- Prentice Hall
- Que
- Cisco Press
- Microsoft Press
- Peachpit Press
- New Riders Publishing
- Alpha Books
- Course Technology
- IBM Press
- Macromedia

## Safari Books Online library for programi

WHAT'S NEW >>>

**Search**  
across the full text of thousands of the best technical

**Browse**  
books by category to research any technical

**Read**  
books cover to cover online, or flip directly to the



# Web+network theoretical

- Credit card processors
  - Need to create accounts en-masse
  - Allow partners by IP prefix
- DISA.MIL publications
  - Uses reverse DNS lookup checks
  - I'm a .mil, let me in!
  - DSN directory
- Vulnerable? Very likely  
Others - Dialog, Hoover's, InfoTrac, LawTel, and PayScale

## IP Trust Relationships, XSS and You

[ntp](#) published an interesting conversation today on [sla.ckers.org](#) discussing IP trust relationships that web applications often have. It might sound crazy that one site should trust anything at all, but I've seen countless examples where certain IPs are simply ignored by security systems, purely because they are believed to be secure. First of all, insiders represent a majority of corporate hacks. Secondly, every day, on this website and on [sla.ckers.org](#) we are finding IPs that are untrustworthy, regardless of the brand associated with them.

To elaborate on ntp's thoughts, let me give you a 95% real world scenario that I've actually seen. There is an online credit card processor that actually uses IP based authentication for adding user accounts to your database. Not only is that scary, but it's highly probable that the usernames could include SQL injection. Not because the credit card processor would allow that through, but because the scripts that run on your server trust whatever is sent through the credit card processor. Now let's assume for a second that the credit card processor's machine is a windows box, and runs a remote desktop.

Someone at that company could easily be subverted into clicking a link (I tell them that for some reason I can't get a connection between their server and my own so they must log in to verify it). When they click the link, it performs actions on their behalf (beyond connecting to my machine). Normally that wouldn't be a big deal. They aren't authenticated to anything, and they may have never used that account before. However, because of IP trust relationships between their IP and every one of the merchants that they service, I now can add user accounts to as many accounts as I can reasonably do in the time the browser is left open. Not only that, but I can do SQL injection and pull other user accounts, delete databases or whatever I choose to the database.

Suddenly the trust relationship has allowed major security issues, due to the privileged nature of the credit card processor. Nasty. There are all sorts of these IP based trust relationships on the Internet, because there is really no other

# Web+Network defenses

- IP address-based authentication
  - Don't do that then! Check your firewalls! Use individual login accounts with passwords!
  - Check your IIS -> Directory Security tab -> IP address-based access control
    - AOL Proxies, Corporate NAT makes this superbad!
- XSS and CSRF protections
  - XSS for coders: Input validation with frameworks
  - XSS for operators: Output filtering with WAF's
  - CSRF: No GET's! POST with nonce (e.g. Viewstate)

# Reflections on trusting trust

- You can't trust compilers
- You can't trust people or groups
- You can't trust networks
- You can't trust browsers
- You can allow individuals access and make them accountable (sudo vs. su)

## My Reflections on Trust

I was a young Air Force lieutenant when Ken Thompson released his 1984 piece, [Reflections on Trusting Trust](#). Assigned to a data center in the Pentagon, I was working on the E2 evaluation of Honeywell Multics with the fine folks at the National Computer Security Center and contributing some words to the growing Rainbow Series books. We were in ongoing debates over the meaning of phrases such as "top-level specification" and "on behalf of" in the Orange Book (a mail thread that went on for several years) and trying to perpetuate the wave of talking about "trusted computers" instead of "secure computers."

We talked a lot about "how much trust do I get for how much analysis and testing" and "how much trust do I need for certain scenarios, like allowing a computer to automatically downgrade data from Top Secret to Secret." These kinds of concepts ended up in capability maturity models, testing models, and risk models.

I took Ken's words to heart and quickly made up my mind that we could really only move the trust bar up slightly (like from 10% to 20%), even with enormous expense. It was immediately obvious that getting up to, say, 75% would require so much calendar time that no one would wait for the result (and I think later experience with Orange Book evaluations, Common Criteria evaluations, and related programs have borne this out). Between hardware, software, firmware—and the completely unpredictable human factors—we really had no idea how even the most reviewed code would operate in relatively controlled environments (e.g., in a government facility where everyone was cleared), much less how it would operate in a hostile environment (hostile mobile code was not really a problem yet) where people might actively be up to nefarious deeds.

Why should you care about my reminiscing? Well, because I think a flavor of trust is still a major problem today and it's costing everyone a bunch of money that could be put into real long-term solutions.

As I talk with my operations friends these days, I'm seeing a subtle shift in their thinking. They're thinking more and more about appliances (web application firewalls, IDS and stuff like that), but not for direct security value. They seem to be thinking that since the software they install, whether purchased or built internally, will certainly have security problems, they have to install more bells and whistles so that operations can protect itself. This is beyond healthy paranoia, it's an unhealthy distrust of people who should be active partners, even if it's been earned by years of spectacular failures.

Then I started wondering why so many development organizations throw out requirements documents from product managers and just start over. Is it only because the requirements are so bad, or is it also because the developers just don't trust the managers to know what they're talking about?

And why do so many managers try to tell development organization how to create applications, instead of simply what the creation must accomplish? Do they simply not trust the developers to be aware of business objectives, or do they just not understand the creative processes involved?

And so on.

What an enormous amount of wasted cycles that could be used to greater organizational good.

We may never get to the point where we can implicitly trust software. But, can't we at get to the point where we can trust each other?



- Enforce a password policy
- Never make group accounts
- Watch accounts for activity, monitor policy
- Close or lock-out old/unused accounts

# My incident response strategy

- **Strike-back**
  - You want personal information? Yes, have some (unload tons)
  - Use SQL injection, create large lists with [Fakenamegenerator.com](http://Fakenamegenerator.com)
- **Lock-down**
  - Better to gather intelligence than lock-out usually
  - Allow user to input additional account information for authorization and then force them to change their password
- **Trace-back**
  - Check web/firewall/IPS/load-balancer logs, SIM/SIEM, NSM data
  - Notify the user/users/groups/orgs. Have them check their logs, too
- **Take-down**
  - Never operate alone. Use a service e.g. CastleCops PIRT

# The future of attacks

- Transitive attacks

- Web 2.0 (Blogger, Technorati, Sitemeter, Flickr, Zoomr, Feedburner, Newsgator, del.icio.us, et al)
  - Blogs
  - RSS
- IP address-based authentication / trust relationships
  - Network A – Network B – WebApp Y – Database Z
- Combination of the above

- Targeted attacks

- Profiling, stalking (e.g. Google hacking, social network sites, WiFi stalking, AOLstalker.com)
- Stealing search engine queries from orgs



# Example One: Project *Camwhore*

- This is a targeted attack

The screenshot shows the Encyclopedia Dramatica website interface. On the left is a navigation menu with sections for '4chan', 'Text Boards', and 'Image Boards'. The main content area features the site's logo and a navigation box. The article 'Camwhore' is displayed, including a warning about disabled account creation, a definition of a camwhore, and a list of contents. A small image of a person's mouth with a red lollipop is shown on the right side of the article.

4chan  
Front Page  
[Remove Frames]  
[Show Directories]  
[Show Worksafe Only]  
Text Boards +  
Image Boards -  
Anime & Manga  
Animals & Nature  
Random  
Anime/Cute  
Cosplay & EGL  
Food & Cooking  
Cute/Male  
Comics & Cartoons  
Hentai/Alternative  
Ecchi  
Technology  
Animated GIF  
Hentai  
High Resolution  
Weapons  
Mecha

navigation  
■ Main Page  
■ The TJC  
■ Recent changes  
■ Random page  
■ Help  
■ Pixel Ads  
■ Support ED

search  
Go Search

support

Log in / create account

article discussion edit history

**Account creation has been disabled again. Want an account? [look here](#). *Encyclopedia Dramatica* needs your help! Please see [Encyclopedia Dramatica:Support ED](#). Keep the lulz alive!**

## Camwhore

A variety of [attention whore](#), typically a young [woman](#) though occasionally a [twink](#), who will do anything on her [webcam](#) in exchange for [attention](#), money, items from Amazon.com [wishlist](#)s or just to be generally slutty. Camwhores typically suffer from [internet disease](#) and engage in constant [Shameless self promotion](#).

There are many reasons to camwhore and many kinds of camwhores. Often camwhores will remove their clothing if given enough of their preferred currency, which consists of money, attention or wishlist items.

**Contents** [hide]

- 1 Determining Status
- 2 Wishlists
- 3 Evolution of the term
- 4 Where to find them
- 5 The present state of camwhoredom
- 6 Some Noteworthy Camwhores

[scarlet](#) pretending to imitate a camwhore. Notice the focus on mouths and sucking.

- 4Chan: Togi-chan
- Encylopedia Dramatica / Camwhore
- Yahoo Profile -> Deviant Art -> Myspace



# Example One: Owning Myspace

Thursday, 25 January 2007

- Myspace hates hackers
  - Samy busted
  - Seclists.org shutdown by GoDaddy
- Myspace loves hackers
  - Allow XSS everywhere (allowing user-submitted HTML is bad, mmkay?)
  - Requires Javascript everywhere
- Myspace is confused

## MySpace Allegedly Kills Computer Security Website

Computer security guru [Evodor](#) (pictured) reports waking up yesterday to find his website [SecLists.org](#) essentially removed from the web by his domain registrar, GoDaddy. After a bunch of phone calls to GoDaddy, he eventually got them to explain why: Because MySpace asked them to.



SecLists provides public archives of over a dozen computer security mailing lists, including BugTraq and Full Disclosure. MySpace was apparently unhappy with a post that crossed Full Disclosure earlier this month, in which the author attached the spoils of a phishing attack against MySpace users, consisting of 56,000 user names and passwords.





# Example 2: Project *NSA Call DB*

- This attack is at first targeted and then [theoretically] becomes a transitive attack



- Another woman
- She makes news for getting arrested
- How to find her?

## Fan hacks into cell phone data for Linkin Park's lead singer, threatens wife, feds say

The Associated Press

Published: November

ALBUQUERQUE, New Mexico: A woman is accused of using a computer at a national laboratory to hack into a cell phone company's Web site to get a number for Chester Bennington, lead singer of the Grammy-winning rock group Linkin Park.

According to an affidavit filed by the Department of Defense Inspector General, Devon Townsend, 27, obtained copies of Bennington's cell phone bill, the phone numbers he called and digital pictures taken with

- E-Mail Article
- Listen to Article
- Printer-Friendly
- 3-Column Format
- Translate
- Share Article
- Add to Clipboard

# Example 2: Myspace again!

- Search for:

- Female
- Age 27
- In Albuquerque, New Mexico
- Works for Sandia National Labs
- Likes Linkin Park

Concert Goer's Companies	
Sandia National Laboratories Albuquerque, New Mexico US I could tell you what I do but then I'd have to kill you	November 27, 2000 to Present

Concert Goer

"Oh what a tangled web we  
weave...."

Female  
28 years old  
ALBUQUERQUE , NEW  
MEXICO  
United States

Last Login: 11/16/2006

Who I'd like to meet:

anybody who knows how to have a good time.

Famous people -- I've met Sum 41 and Chester Bennington of Linkin  
Park.

- **ONE RESULT**

<http://profile.myspace.com/index.cfm?fuseaction=user.viewprofile&friendID=36977809>

# Example 2: DoD Response

- A few more words about incident response

- Transitive attack could be as simple as:

Myspace – SNL browser – NSA DB

- Need-to-know basis
- A trap?
  - CIA involvement on Facebook

## CIA Gets in Your Face(book)



MAIL

RANTS + RAUES

By [Chaddus Bruce](#) | [Also by this reporter](#)

02:00 AM Jan, 24, 2007

If you're a Facebook member, a career as a government spook is only a click away.

Since December 2006, the Central Intelligence Agency has been using [Facebook.com](#), the popular social networking site, to recruit potential employees into its National Clandestine Service. It marks the first time the CIA has ventured into social networking to hire new personnel.

The [CIA's Facebook page](#) (login required) provides an overview of what the NCS is looking for in a recruit, along with a 30-second promotional [YouTube video](#) aimed at potential college-aged applicants. U.S. citizens with a GPA above 3.0 can apply.

# Summary

- Same-origin policy doesn't protect you
- Transitive attacks
- Targeted attacks
  
- There is a lot more out there than what I've talked about. The webapp security landscape is constantly and consistently getting worse and worse by the day

# References

- <http://ryanlrussell.blogspot.com/2007/01/web-of-trust.html>
- <http://ha.ckers.org/blog/20070122/ip-trust-relationships-xss-and-you/>
- <http://taossa.com/index.php/2007/02/08/same-origin-policy/>
- [http://www.layerone.info/2006/presentations/MPLS\\_Security-LayerOne-Enno\\_Rey.pdf](http://www.layerone.info/2006/presentations/MPLS_Security-LayerOne-Enno_Rey.pdf)
- <http://www.nanog.org/mtg-0610/scholl-shaikh.html>
- <http://www.theta44.org/karma/>
- <http://www.blackhat.com/html/bh-dc-07/bh-dc-07-speakers.html#Graham>
- <http://www.websense.com/securitylabs/blog/blog.php?BlogID=106>

Questions?