Where do security bugs come from?

MIT 6.858 (Computer Systems Security), September 18th, 2014

Paul Youn

- Technical Director, iSEC Partners
- MIT 18/6-3 ('03), M.Eng '04

Agenda

- What is a security bug?
- Who is looking for security bugs?
- Trust relationships
- Sample of bugs found in the wild
- Memory corruption issues
- Stuxnet
- I'm in love with security; whatever shall I do?

What is a Security Bug?

- What is security?
- Class participation Tacos, Salsa, and Avocados (TSA)

What is security?

"A system is secure if it behaves precisely in the manner intended – and does nothing more" – Ivan Arce

- Who knows exactly what a system is intended to do? Systems are getting more and more complex.
- What types of attacks are possible?

First steps in security: define your security model and your threat model

Threat modeling: T.S.A.

- Logan International Airport security goal #3: prevent banned substances from entering Logan
- Class Participation: What is the threat model?
  - What are possible avenues for getting a banned substance into Logan?
  - Where are the points of entry?
- Threat modeling is also critical, you have to know what you're up against (many engineers don't)

Engineering challenges

- People care about features, not security (until something goes wrong)
- Engineers typically only see a small piece of the puzzle
- “OMG PDF WTF” (Julia Wolf, 2010)
  - How many lines of code in Linux 2.6.32?
  - How many lines in Windows NT 4?
  - How many in Adobe Acrobat?

Engineering challenges

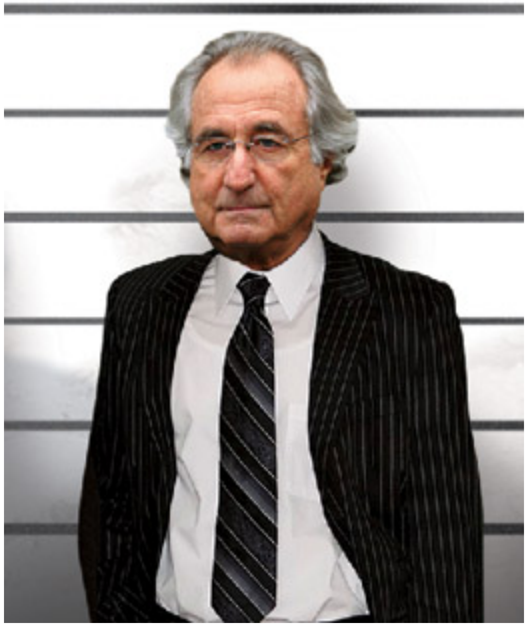
- People care about features, not security (until something goes wrong)
- Engineers typically only see a small piece of the puzzle
- “OMG PDF WTF” (Julia Wolf, 2010)
    - How many lines of code in Linux 2.6.32?
        - 8 – 12.6 million
    - How many lines in Windows NT 4?
        - 11-12 million
    - How many in Adobe Acrobat?
        - 15 million

Who looks for security bugs?

- Criminals
- Security Researchers
- Pen Testers
- Governments
- Hacktivists
- Academics

Criminals

- Goals:
  - Money (botnets, CC#s, blackmail)
  - Stay out of jail
- Thoroughness:
  - Reliable exploits
  - Don't need 0-days (but they sure are nice)
- Access:
  - Money
  - Blackbox testing



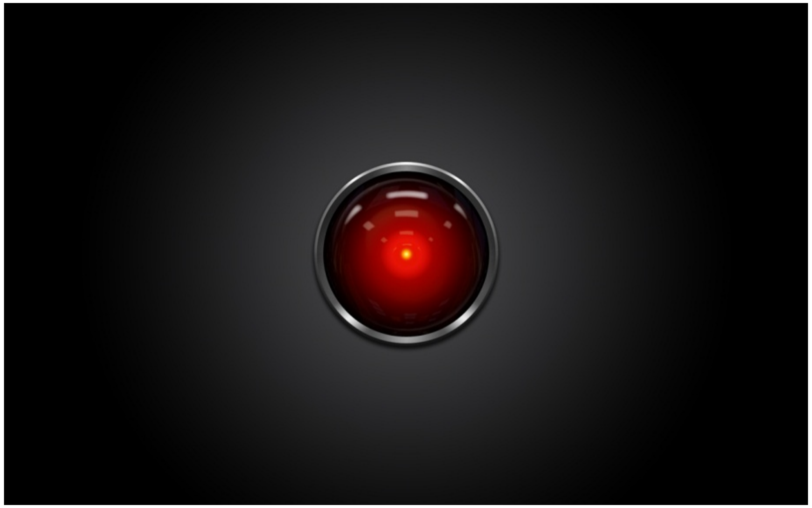
Security Researchers

- Goals:
  - Column inches from press, props from friends
  - Preferably in a trendy platform
- Thoroughness:
  - Don’t need to be perfect, don’t want to be embarrassed
- Access:
  - Casual access to engineers
  - Source == Lawyers

Pen Testers

- Goals:
  - Making clients and users safer
  - Finding vulns criminals would use
- Thoroughness:
  - Need coverage
  - Find low-hanging fruit
  - Find high impact vulnerabilities
  - Don't fix or fully exploit
- Access:
  - Access to Engineers
  - Access to Source
  - Permission

Governments



- Goals:
  - Attack/espionage
  - Defend
- Thoroughness:
  - Reliable exploits
- Access:
  - Money
  - Talent
  - Time

Hacktivists

- Goals:
  - Doing something "good"
  - Stay out of jail
- Thoroughness:
  - Reliable exploits
  - Don't need 0-days
- Access:
  - Talent
  - Plentiful targets

Academics

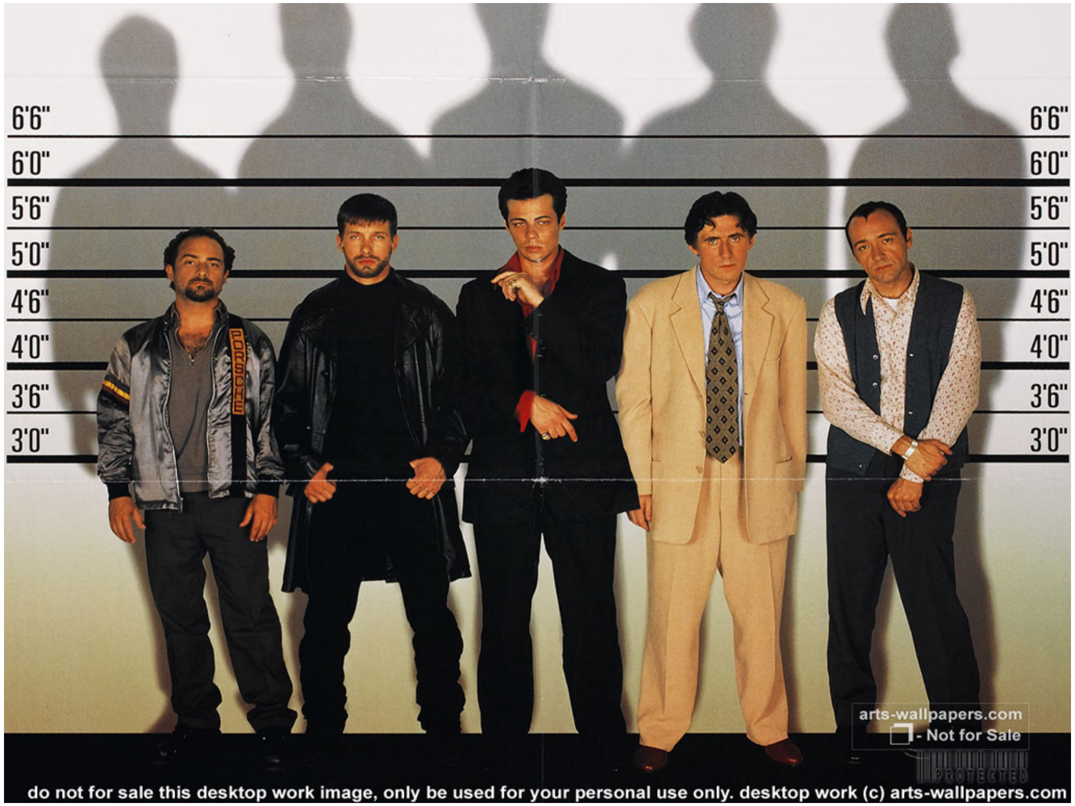
- Goals:
  - Finding common flaws and other general problems
  - Developing new crypto
  - Make something cool and useful
  - Make everyone safer
- Thoroughness:
  - Depth in area of research
- Access:
  - Creating new things
  - Blackbox

Techniques

- With access:
  - Source code review
  - Engineer interviews
  - Testing in a controlled environment
- Without access:
  - Blackbox testing
  - Fuzzing (give weird inputs, see what happens)
  - Reverse Engineering
  - Social Engineering

Overall Goals

- All are looking for the similar things: vulnerable systems
- Let's dive in and look at vulns that we all look for


6'6"
6'0"
5'6"
5'0"
4'6"
4'0"
3'6"
3'0"
PORSCHE
arts-wallpapers.com
- Not for Sale
PROTECTED
do not for sale this desktop work image, only be used for your personal use only. desktop work (c) arts-wallpapers.com

Bad Engineering Assumptions

Therac-25 (the engineer)

- Two modes of operation: image and radiation treatment
- Intended invariant: in radiation treatment mode, a protective focusing shield must be in place

Therac-25

Shield code was something like:

```
//global persistent variable, single byte value
ub1  protectiveShield; //zero if shield isn’t needed
…
//do we need a shield?
if(treatmentMode) then
{
       protectiveShield++;
} else {
       protectiveShield = 0;
}
…
if(protectiveShield) {
       putShieldInPlace();
} else {
       removeShield();
}
```

Therac-25

- Flawed assumption: protectiveShield would always be non-zero in treatment mode
- Impact: people actually died

Therac-25

- Flawed assumption: protectiveShield would always be non-zero in treatment mode
- Impact: people actually died
- My classmate's conclusion: "I learned to never write medical software"

Bad Assumptions

- Amazon allows you to add a credit card or email address with name, email address, physical address
- Amazon allows you to send a password reset to a registered email address
- Amazon lets you see the last four digits of registered credit card numbers
- Apple grants account access with the last four digits of a registered credit card (D’oh!)
- Gmail reset to Apple account

Bad Assumptions

- **Amazon allows you to add a credit card or email address with name, email address, physical address**
- Amazon allows you to send a password reset to a registered email address
- Amazon lets you see the last four digits of registered credit card numbers
- **Apple grants account access with the last four digits of a registered credit card (D'oh!)**
- Gmail reset to Apple account

Bad Assumptions

Conclusion: components that affect your system are often beyond your control (Facebook, Amazon, Apple). Consider the full threat model.

Bad Assumptions

Conclusion: components that affect your system are often beyond your control (Facebook, Amazon, Apple). Consider the full threat model.

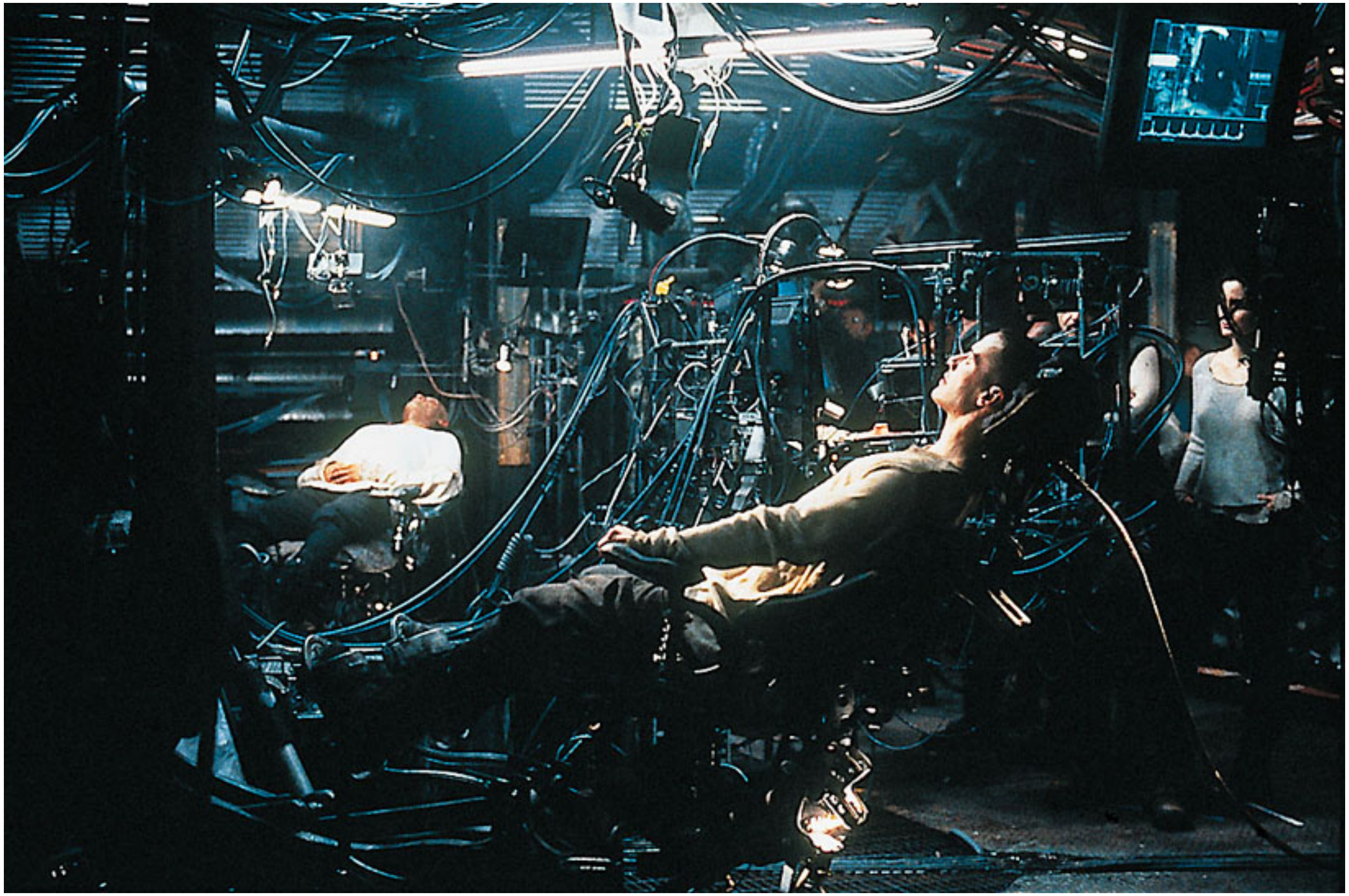
Question: is your personal email account password stronger or weaker than your online banking passwords?

Designing Systems

Think like a security researcher:

- What assumptions are being made?
- Which assumptions are wrong?
- What can you break if the assumption is wrong?

Memory Management is Hard



Can you hear me now?

High overhead security protocol:

- Avoid renegotiation
- Alice: “You there? If so, say ‘boo!’”
- Bob: “boo!”
- Alice and Bob know they’re good

Can you hear me now?

Alice sends in ping packet containing:

- Type of packet (ping)
- Length of data
- Data

Can you hear me now?

Bob parses input from Alice's provided data into:

```
typedef struct ping {
    int type;
    unsigned int length;
    unsigned char *data;
}
```

Can you hear me now?

Bob prepares a response:

```
char *response;
response = malloc(2 + aliceData.length);
memcpy(response, aliceData.length, 2);
memcpy(&response[2], aliceData.data,
    aliceData.length);
/* send echoed response back to Alice*/
```

What went wrong

Bob prepares a response:

```
char *response;
response = malloc(2 + aliceData.length);
memcpy(response, aliceData.length, 2);
memcpy(&response[2], aliceData.data,
     aliceData.length);
/* send echoed response back to Alice*/
```

Bad assumptions

- User supplied data length didn’t have to match the actual data size
- Server (Bob) never checks the length is accurate
- User can read up to 64k of server memory (including private keys)

Heartbleed sucked

What the heck do you do after you've broken the internet?

- How do you "responsibly" disclose?
- Who do you tell?

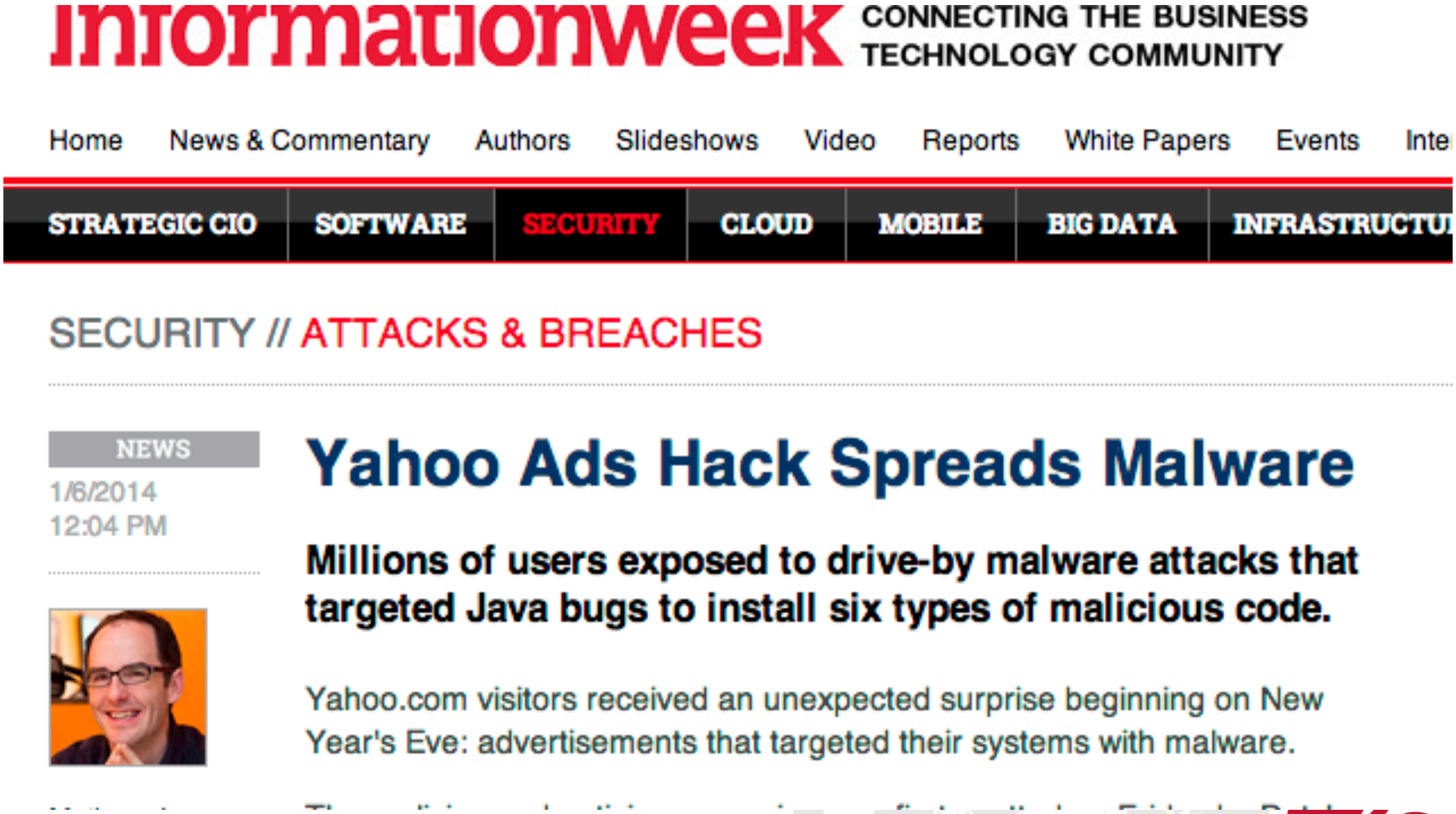
Heartbleed sucked a lot

- No sign of exploitation
- Signs that state actors have been exploiting this for a while (monitor diffs in OpenSSL)
- What have we learned?
  - TLS keys on your most exposed boxes: not so smart
  - Fundamental protocols have problems

http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html
http://vrt-blog.snort.org/2014/04/heartbleed-memory-disclosure-upgrade.html

Let's steal

Crime Pays: Botnet edition



InformationWeek CONNECTING THE BUSINESS TECHNOLOGY COMMUNITY

SECURITY // ATTACKS & BREACHES

NEWS
1/6/2014
12:04 PM

Yahoo Ads Hack Spreads Malware

Millions of users exposed to drive-by malware attacks that targeted Java bugs to install six types of malicious code.

Yahoo.com visitors received an unexpected surprise beginning on New Year's Eve: advertisements that targeted their systems with malware.

http://www.informationweek.com/security/attacks-and-breaches/yahoo-ads-hack-spreads-malware/d/d-id/1113325

Crime Pays: Botnet edition

- Improperly sanitized user input is executed as javascript in the browser on that origin.
- Yahoo: malicious ads automatically directed users to an exploit kit called "Magnitude" via the XSS vulnerability
- "Magnitude" exploited recent Java vulnerabilities
- Estimated 27,000 infections *per hour* from December 30th to January 3rd
- PSA: disable Java in your web browser and enable "click-to-play" (Chrome)

The Confused Deputy: 3s a crowd

- Tricking an authority into letting you do something you shouldn't be able to do
- Most security problems could fall under this broad definition

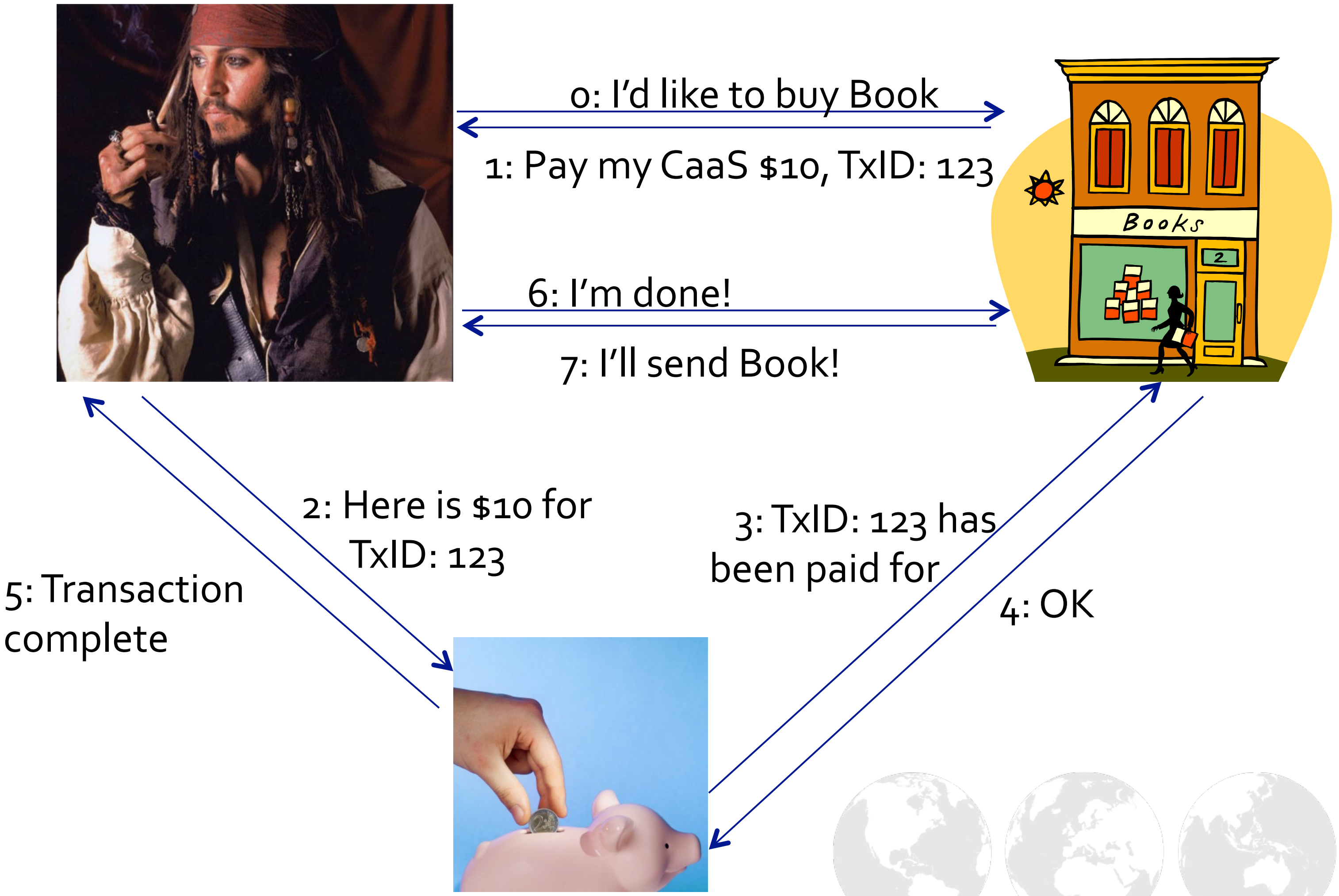
The Confused Deputy

"How to Shop for Free Online"* (security researcher and academic)

- Three-party payment systems (Cashier as a Service):
  - Merchant (seller)
  - Payment provider
  - ~~Cheater~~ User
- Communication between parties go through the user

* http://research.microsoft.com/pubs/145858/caas-oakland-final.pdf

The Confused Deputy



0: I'd like to buy Book

1: Pay my CaaS $10, TxID: 123

2: Here is $10 for TxID: 123

3: TxID: 123 has been paid for

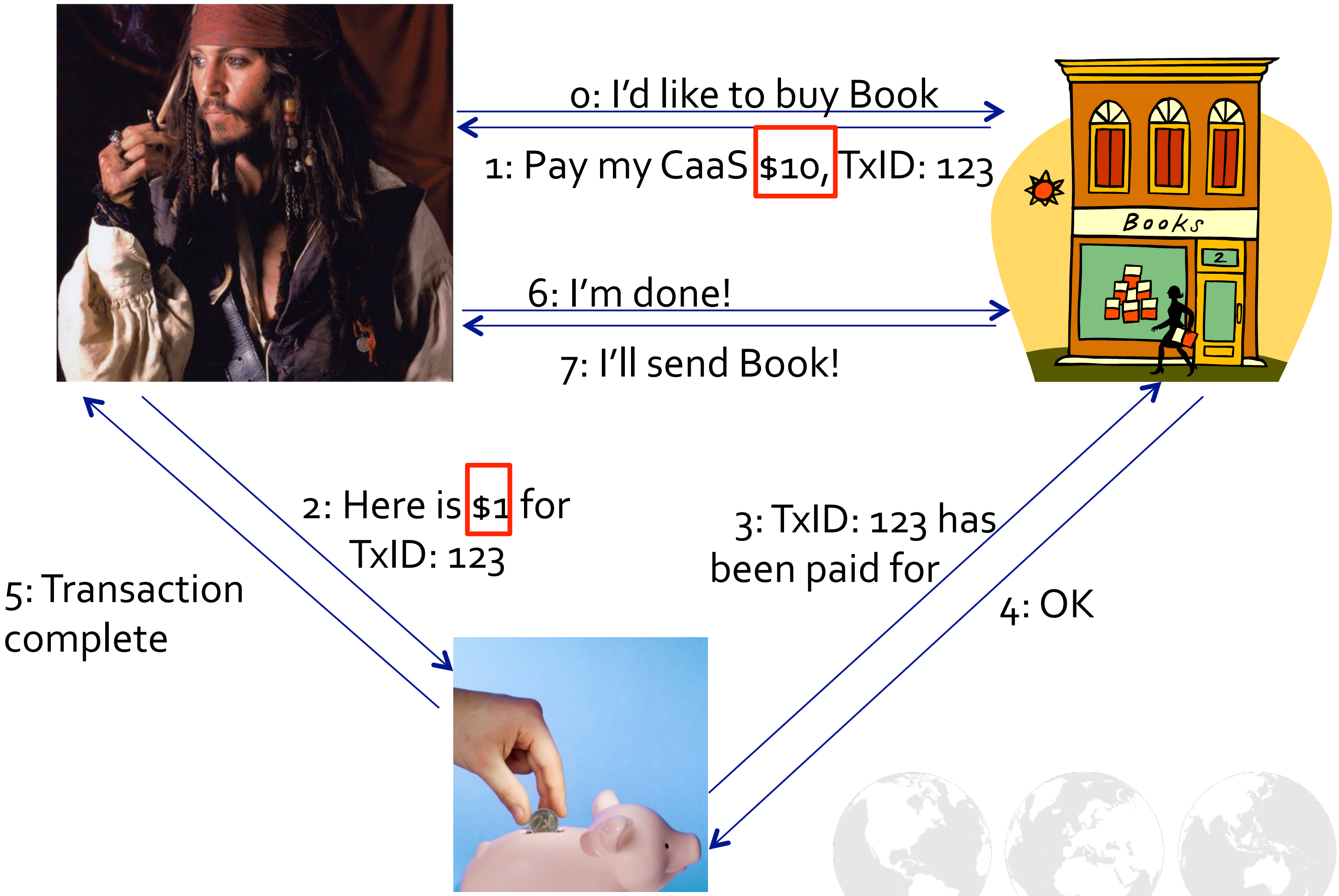
4: OK

5: Transaction complete

6: I'm done!

7: I'll send Book!

The Confused Deputy



0: I'd like to buy Book

1: Pay my CaaS $10, TxID: 123

2: Here is $1 for TxID: 123

3: TxID: 123 has been paid for

4: OK

5: Transaction complete

6: I'm done!

7: I'll send Book!

The Confused Deputy

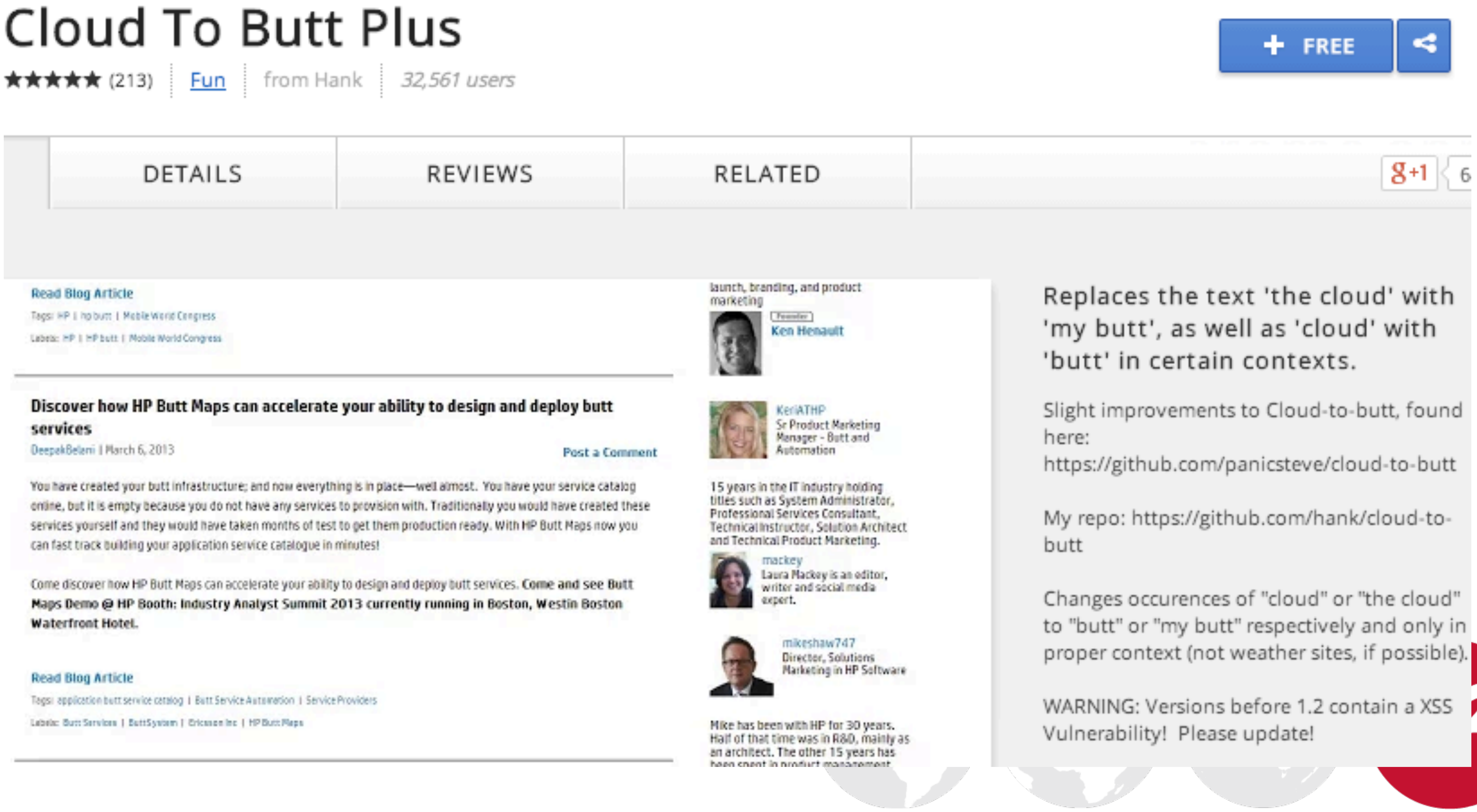
- The merchant thinks something ties the payment amount to the transaction
- Impact: shopping for free
- Solutions?
- Read the paper, lots of things can and do go wrong

Unexpected Interactions

Password Managers

- Passwords attacks get better over time:
  - More computing power
  - More real passwords
- 2FA isn't ubiquitous enough
- You can generate a few good passwords
- You can't generate a good, unique, one for every website you use

Browser Extensions



Cloud To Butt Plus

★★★★★ (213) | Fun | from Hank | 32,561 users

Read Blog Article

Tags: HP | hp butt | Mobile World Congress

Labels: HP | HP butt | Mobile World Congress

Discover how HP Butt Maps can accelerate your ability to design and deploy butt services

DeepakBelani | March 6, 2013

Post a Comment

You have created your butt infrastructure; and now everything is in place—well almost. You have your service catalog online, but it is empty because you do not have any services to provision with. Traditionally you would have created these services yourself and they would have taken months of test to get them production ready. With HP Butt Maps now you can fast track building your application service catalogue in minutes!

Come discover how HP Butt Maps can accelerate your ability to design and deploy butt services. **Come and see Butt Maps Demo @ HP Booth: Industry Analyst Summit 2013 currently running in Boston, Westin Boston Waterfront Hotel.**

Read Blog Article

Tags: application butt service catalog | Butt Service Automation | Service Providers

Labels: Butt Services | ButtSystem | Ericsson Inc | HP Butt Maps

launch, branding, and product marketing

Founder

Ken Henault

KeriATHP

Sr Product Marketing Manager - Butt and Automation

15 years in the IT industry holding titles such as System Administrator, Professional Services Consultant, Technical Instructor, Solution Architect and Technical Product Marketing.

mackey

Laura Mackey is an editor, writer and social media expert.

mikeshaw747

Director, Solutions Marketing in HP Software

Mike has been with HP for 30 years. Half of that time was in R&D, mainly as an architect. The other 15 years has been spent in product management

Replaces the text 'the cloud' with 'my butt', as well as 'cloud' with 'butt' in certain contexts.

Slight improvements to Cloud-to-butt, found here: https://github.com/panicsteve/cloud-to-butt

My repo: https://github.com/hank/cloud-to-butt

Changes occurences of "cloud" or "the cloud" to "butt" or "my butt" respectively and only in proper context (not weather sites, if possible).

WARNING: Versions before 1.2 contain a XSS Vulnerability! Please update!

Browsers have a hard job

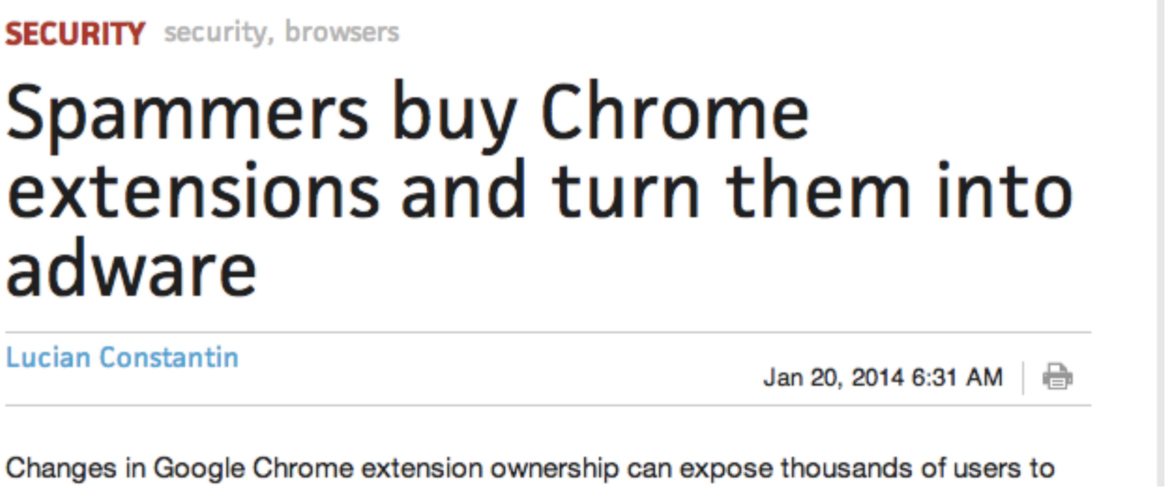
- Same-origin policy:
  - Prevents different domains from interacting in a meaningful* way with other domains
  - Visiting https://www.isecpartners.com doesn't allow us to read your gmail if you're logged in and have cookies
- Browsers, Flash, ~~Java~~, Javascript all implement the same-origin policy

Extensions don’t care

- Interact with all webpages in meaningful ways
- A security vulnerability may break your internet

Extensions don't care

- Interact with all webpages in meaningful ways
- A security vulnerability may break your internet
- Extensions are being sold to bad guys: http://www.pcworld.com/article/2089580/spammers-buy-chrome-extensions-and-turn-them-into-adware.html



SECURITY security, browsers

Spammers buy Chrome extensions and turn them into adware

Lucian Constantin

Jan 20, 2014 6:31 AM

Changes in Google Chrome extension ownership can expose thousands of users to

Security goals

- Securely send passwords to the correct party
- General application security
- Be easy to use
- Generate strong passwords
- Securely store passwords

Security goals

- **Securely send passwords to the correct party**
- **General application security**
- **Be easy to use**
- Generate strong passwords
- Securely store passwords

Oops

- Application security fail: 1Password
- Performed silent updates over HTTP of unsigned packages
- Ran as a privileged user

Ease of "use"

- Auto-fill and auto-submit functionality
  - MaskMe: auto-fill
  - LastPass: auto-fill and auto-submit
  - 1Password: neither
- Automation makes exploitation easier

Attack surfaces examined

- Distinguish between HTTP and HTTPS
- Fill credentials in iframes
- Cross-domain submission
- Distinguish between subdomains
- Identify login pages

HTTP vs HTTPS

- SSL stripping attacks could expose your password
- Active network attacker:
  - https://example.com is redirected to http://example.com
  - Password manager auto-fills
  - Fake page auto-submits

HTTP vs HTTPS

- SSL stripping attacks could expose your password
- Active network attacker:
  - https://example.com is redirected to http://example.com
  - Password manager auto-fills
  - Fake page auto-submits
- MaskMe was vulnerable

Fill credentials in iframes

- Would greatly increase the magnitude of an attack
- Visiting a malicious page could compromise large sets of credentials very quickly

Fill credentials in iframes

- Would greatly increase the magnitude of an attack
- Visiting a malicious page could compromise large sets of credentials very quickly
- No examined password managers were vulnerable on Windows (later researched showed vulnerability in Safari’s LastPass extension)

Cross-domain submission

- If a login form is encountered on https://example.com, would the manager fill it in and submit to https://www.isecpartners.com?

Cross-domain submission

- If a login form is encountered on https://example.com, would the manager fill it in and submit to https://www.isecpartners.com?
- Find a vulnerability or feature that lets you create a login form on a domain
- Malicious login form submits across origin to https://www.isecpartners.com

Cross-domain submission

- If a login form is encountered on https://example.com, would the manager fill it in and submit to https://www.isecpartners.com?
- Find a vulnerability or feature that lets you create a login form on a domain
- Malicious login form submits across origin to https://www.isecpartners.com
- All examined password managers would happily submit passwords across domains

Distinguishing subdomains

- Not all subdomains are equally sensitive
- blog.*, forum.*, or mail.*
- Treating subdomains as equivalent increases attack surface

Distinguishing subdomains

- Not all subdomains are equally sensitive
- blog.*, forum.*, or mail.*
- Treating subdomains as equivalent increases attack surface
- All examined password managers treated subdomains as equivalent

Identify login pages

- Even finer grained control than distinguishing subdomains
- Most web applications have a small set of login pages

Identify login pages

- Even finer grained control than distinguishing subdomains
- Most web applications have a small set of login pages
- None of the examined password managers attempted to track specific login pages

Tying it together

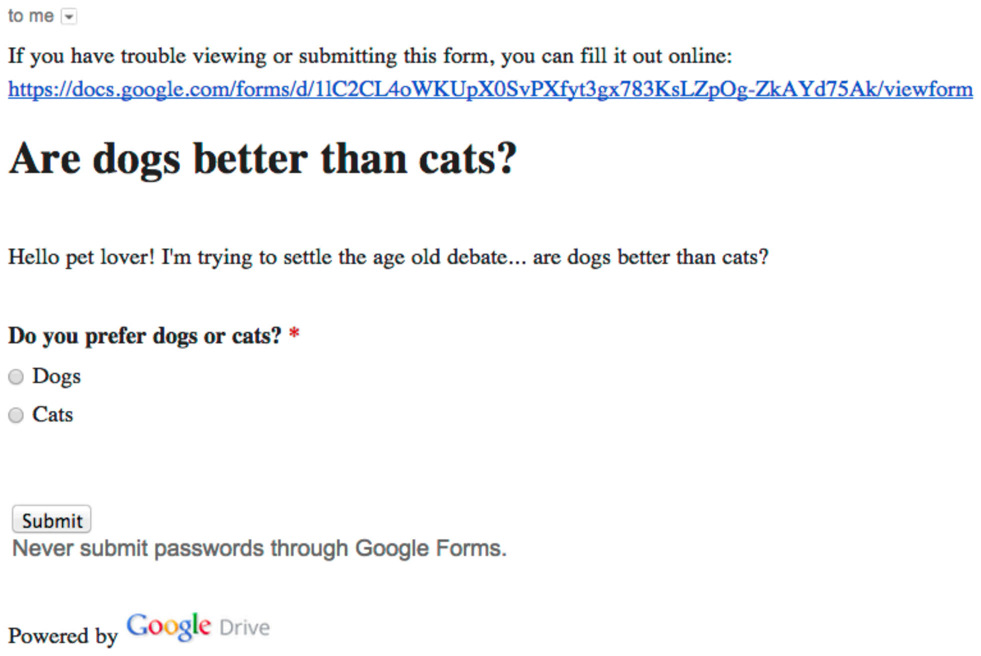
- Goal: introduce a login page that triggers auto-fill or auto-submit on a valuable domain

Tying it together

- Goal: introduce a login page that triggers auto-fill or auto-submit on a valuable domain
- Have:
  - Password managers are willing to submit across origin
  - Password managers will fill in any login form on any subdomain encountered

Tying it together

- Goal: introduce a login page that triggers auto-fill or auto-submit on a valuable domain
- Vector: HTML email
  - Google
  - Yahoo!
  - Outlook



If you have trouble viewing or submitting this form, you can fill it out online:
https://docs.google.com/forms/d/1lC2CL4oWKUpX0SvPXfyt3gx783KsLZpOg-ZkAYd75Ak/viewform

Are dogs better than cats?

Hello pet lover! I'm trying to settle the age old debate... are dogs better than cats?

Do you prefer dogs or cats? *

○ Dogs

○ Cats

Never submit passwords through Google Forms.

Powered by Google Drive

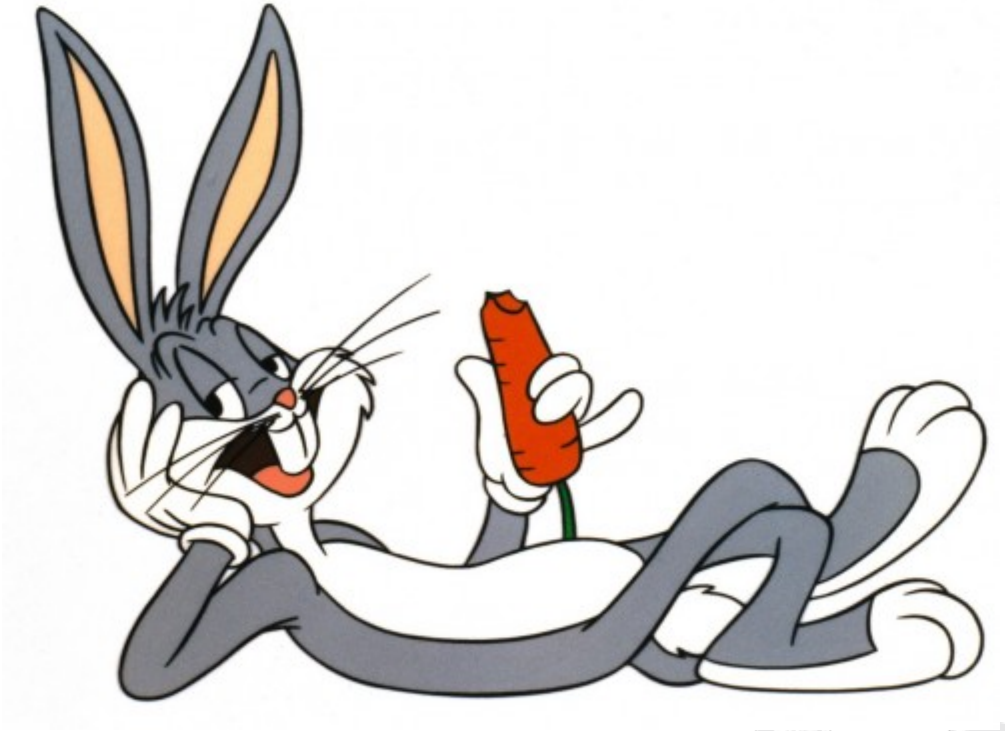
How bad

- Outlook (live.com):
  - Resisted the attack
  - Prevented cross-origin submissions of any kind
- Google:
  - Warned of cross origin submission
  - Stole passwords
- Yahoo!
  - Stole passwords without any warning

Even worse: mobile

- No extensions exist
- Javascript Bookmarklets: run tricky security code on a completely hostile website (what could possibly go wrong)
- Additional academic research that followed:
  - Berkeley: http://devd.me/papers/pwdmgr-usenix14.pdf
  - Joint Stanford/U of T: http://crypto.stanford.edu/~dabo/pubs/papers/pwdmgrBrowser.pdf

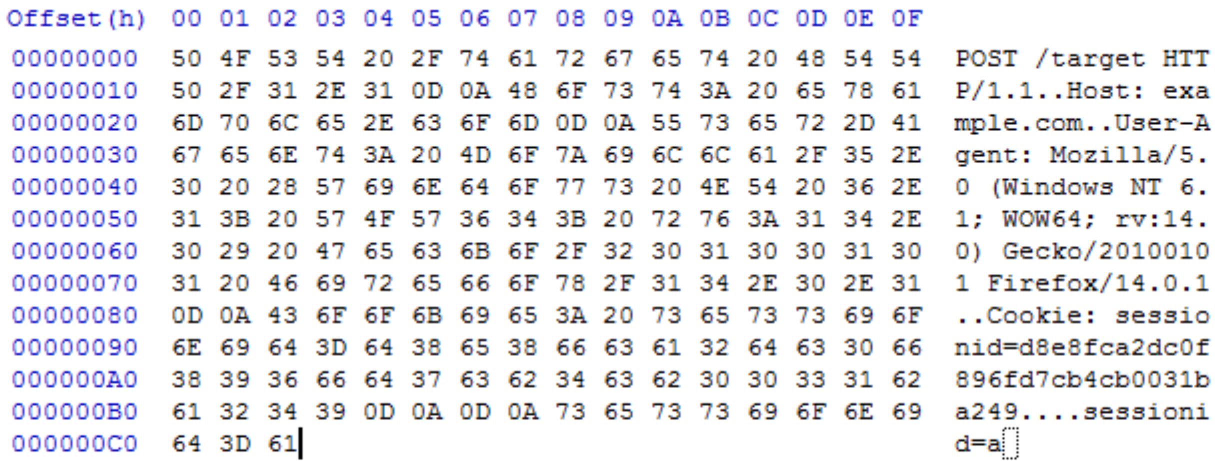
(more) Bugs you could have found



CRIME

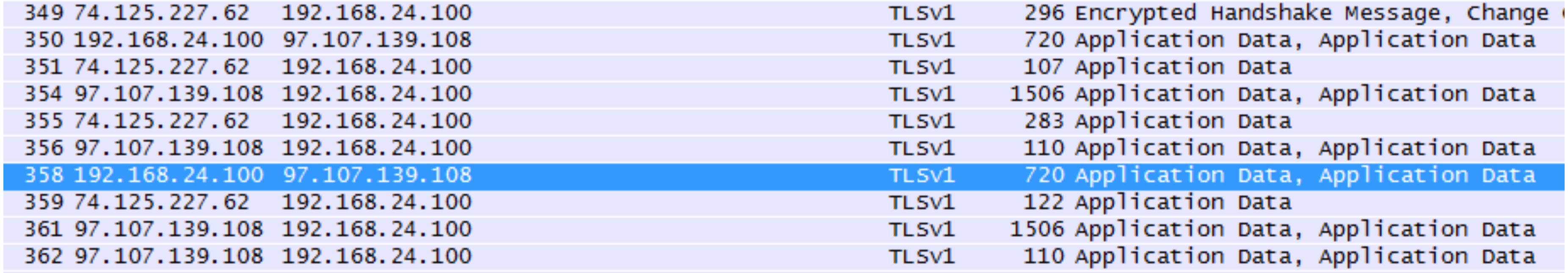
```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

username=tom&password=hunter2
```

HTTP



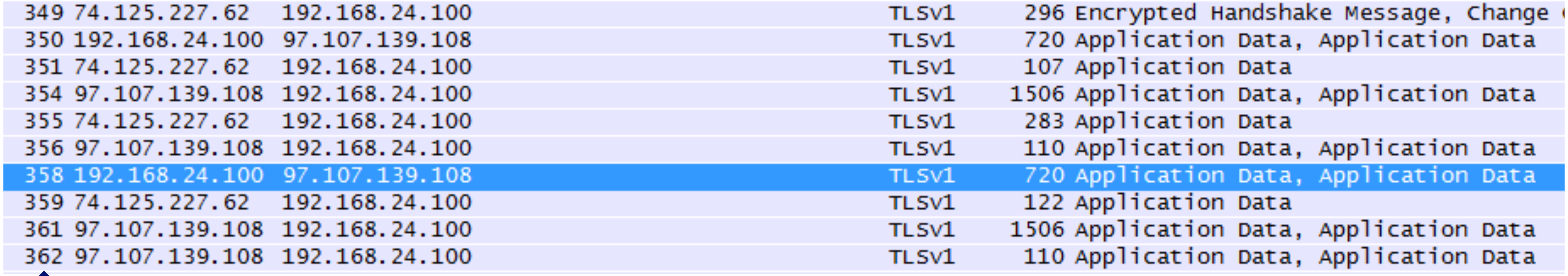
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  50 4F 53 54 20 2F 74 61 72 67 65 74 20 48 54 54  POST /target HTT
00000010  50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 65 78 61  P/1.1..Host: exa
00000020  6D 70 6C 65 2E 63 6F 6D 0D 0A 55 73 65 72 2D 41  mple.com..User-A
00000030  67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E  gent: Mozilla/5.
00000040  30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E  0 (Windows NT 6.
00000050  31 3B 20 57 4F 57 36 34 3B 20 72 76 3A 31 34 2E  1; WOW64; rv:14.
00000060  30 29 20 47 65 63 6B 6F 2F 32 30 31 30 30 31 30  0) Gecko/2010010
00000070  31 20 46 69 72 65 66 6F 78 2F 31 34 2E 30 2E 31  1 Firefox/14.0.1
00000080  0D 0A 43 6F 6F 6B 69 65 3A 20 73 65 73 73 69 6F  ..Cookie: sessio
00000090  6E 69 64 3D 64 38 65 38 66 63 61 32 64 63 30 66  nid=d8e8fca2dc0f
000000A0  38 39 36 66 64 37 63 62 34 63 62 30 30 33 31 62  896fd7cb4cb0031b
000000B0  61 32 34 39 0D 0A 0D 0A 73 65 73 73 69 6F 6E 69  a249....sessioni
000000C0  64 3D 61                                         d=a
```

SSL



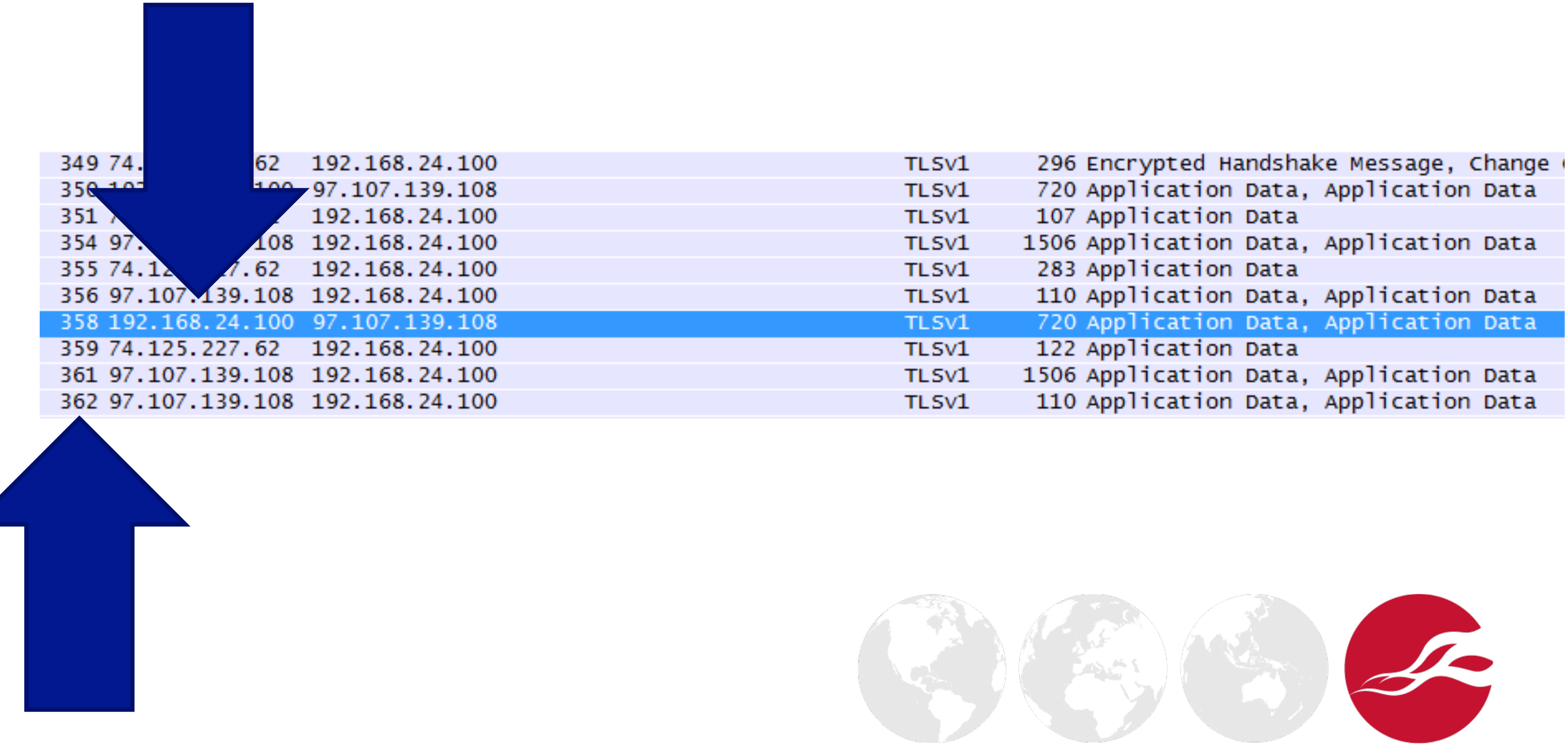
```
349 74.125.227.62   192.168.24.100   TLSv1    296 Encrypted Handshake Message, Change
350 192.168.24.100  97.107.139.108   TLSv1    720 Application Data, Application Data
351 74.125.227.62   192.168.24.100   TLSv1    107 Application Data
354 97.107.139.108  192.168.24.100   TLSv1   1506 Application Data, Application Data
355 74.125.227.62   192.168.24.100   TLSv1    283 Application Data
356 97.107.139.108  192.168.24.100   TLSv1    110 Application Data, Application Data
358 192.168.24.100  97.107.139.108   TLSv1    720 Application Data, Application Data
359 74.125.227.62   192.168.24.100   TLSv1    122 Application Data
361 97.107.139.108  192.168.24.100   TLSv1   1506 Application Data, Application Data
362 97.107.139.108  192.168.24.100   TLSv1    110 Application Data, Application Data
```

Time



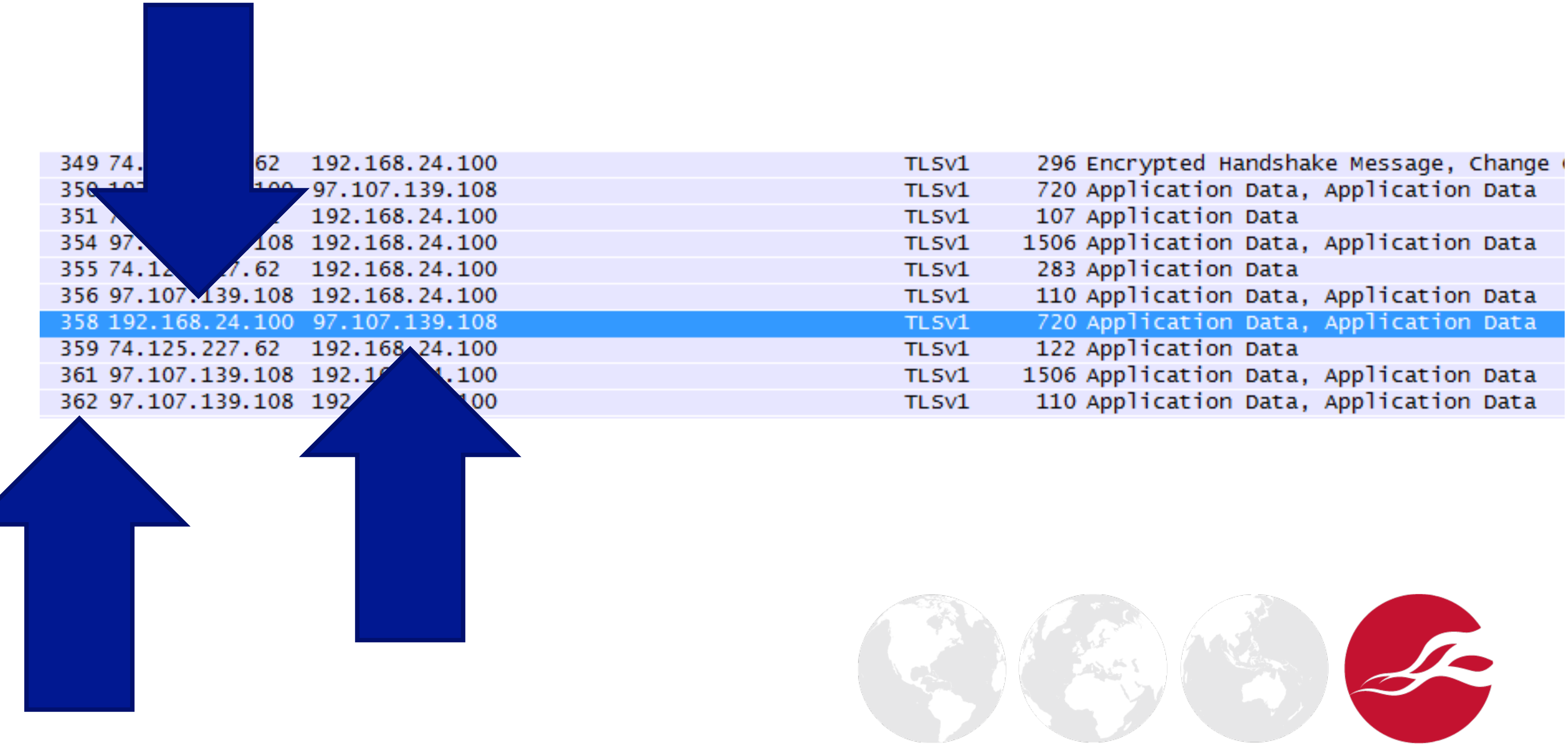
```
349 74.125.227.62   192.168.24.100                              TLSv1      296 Encrypted Handshake Message, Change
350 192.168.24.100  97.107.139.108                              TLSv1      720 Application Data, Application Data
351 74.125.227.62   192.168.24.100                              TLSv1      107 Application Data
354 97.107.139.108  192.168.24.100                              TLSv1     1506 Application Data, Application Data
355 74.125.227.62   192.168.24.100                              TLSv1      283 Application Data
356 97.107.139.108  192.168.24.100                              TLSv1      110 Application Data, Application Data
358 192.168.24.100  97.107.139.108                              TLSv1      720 Application Data, Application Data
359 74.125.227.62   192.168.24.100                              TLSv1      122 Application Data
361 97.107.139.108  192.168.24.100                              TLSv1     1506 Application Data, Application Data
362 97.107.139.108  192.168.24.100                              TLSv1      110 Application Data, Application Data
```

From



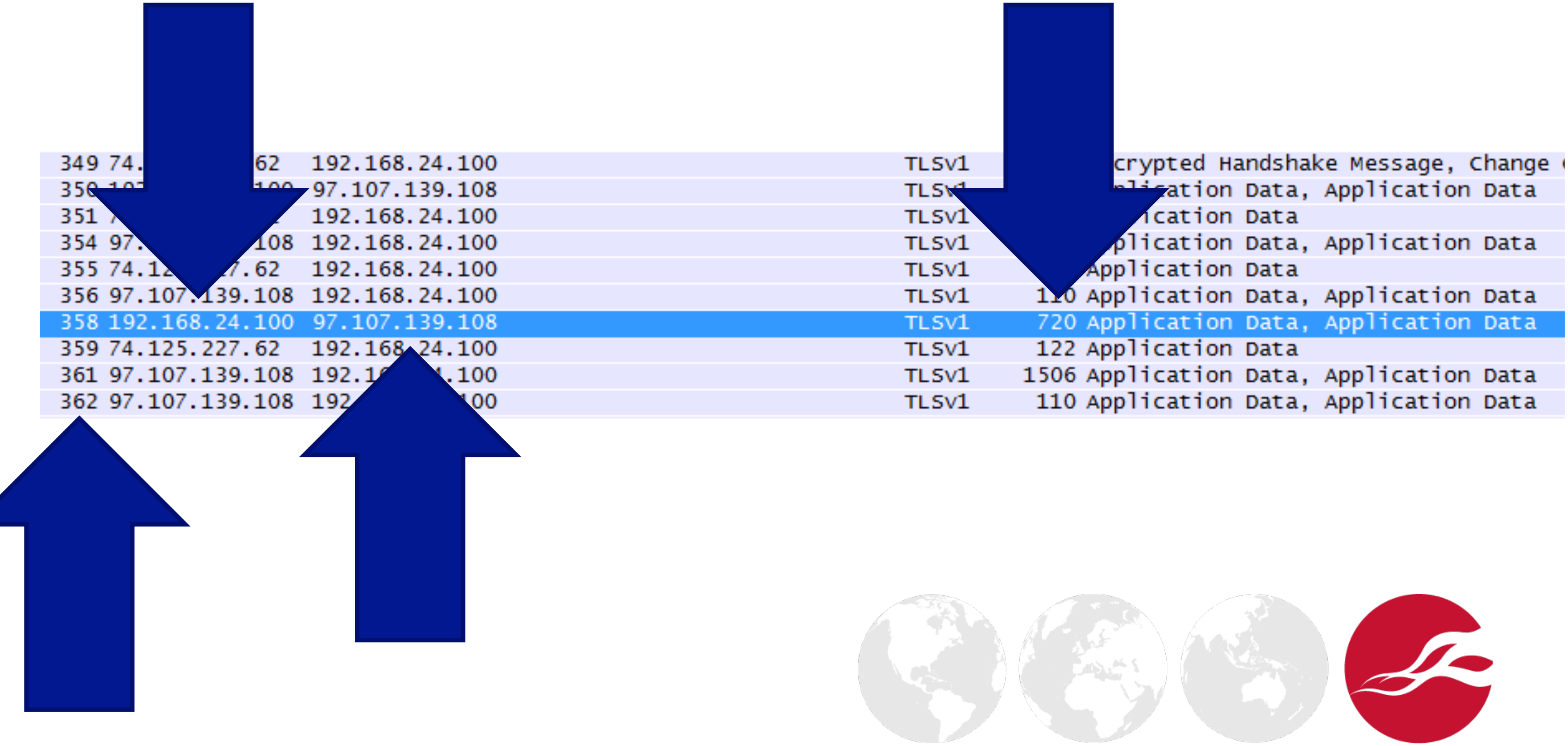
```
349 74.       62   192.168.24.100                                TLSv1       296 Encrypted Handshake Message, Change
350 10        100  97.107.139.108                                TLSv1       720 Application Data, Application Data
351 7          2   192.168.24.100                                TLSv1       107 Application Data
354 97.        108 192.168.24.100                                TLSv1      1506 Application Data, Application Data
355 74.12      7.62 192.168.24.100                               TLSv1       283 Application Data
356 97.107.139.108 192.168.24.100                                TLSv1       110 Application Data, Application Data
358 192.168.24.100 97.107.139.108                                TLSv1       720 Application Data, Application Data
359 74.125.227.62  192.168.24.100                                TLSv1       122 Application Data
361 97.107.139.108 192.168.24.100                                TLSv1      1506 Application Data, Application Data
362 97.107.139.108 192.168.24.100                                TLSv1       110 Application Data, Application Data
```

To



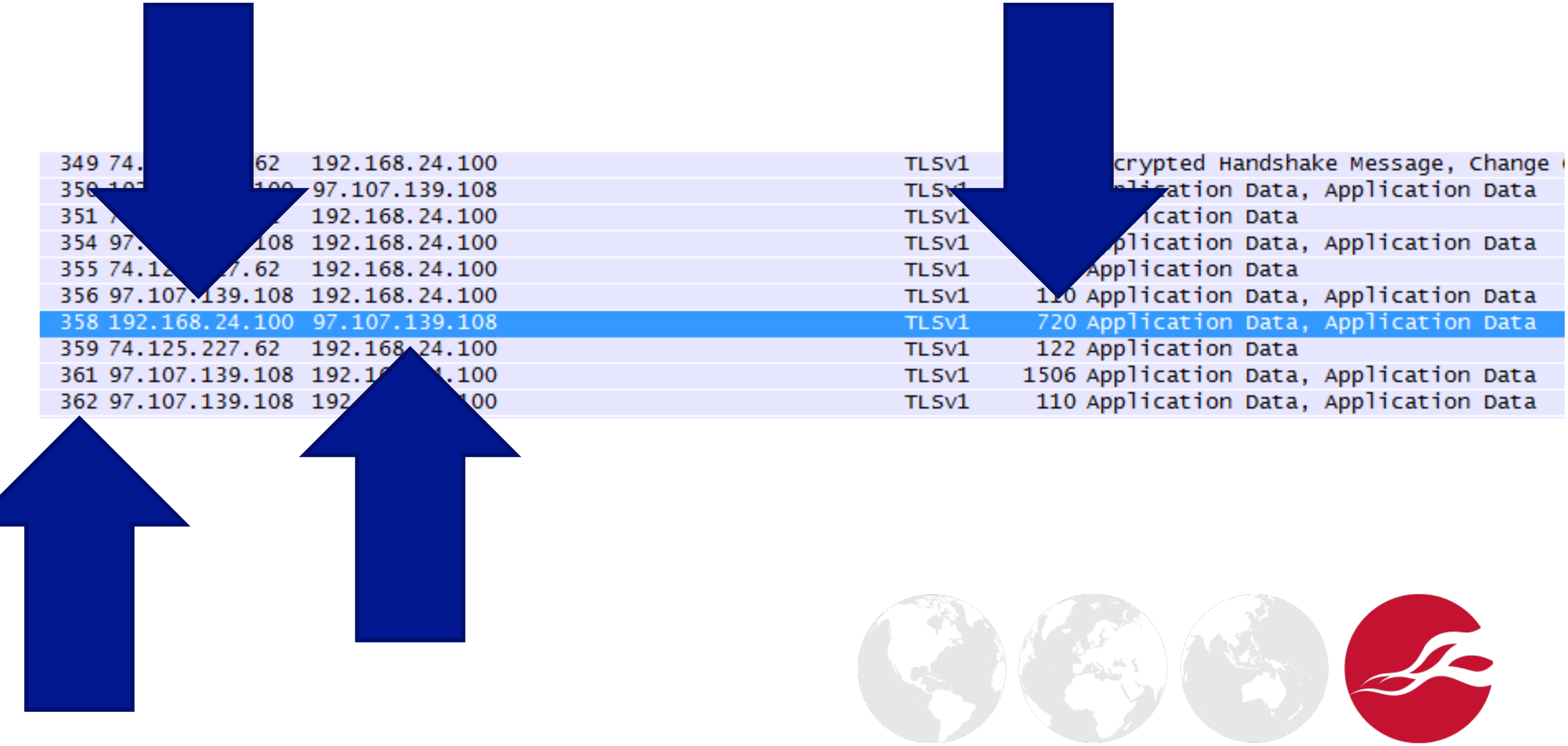
```
349 74.        62   192.168.24.100          TLSv1     296 Encrypted Handshake Message, Change
350            100  97.107.139.108          TLSv1     720 Application Data, Application Data
351 7               192.168.24.100          TLSv1     107 Application Data
354 97.         108 192.168.24.100          TLSv1    1506 Application Data, Application Data
355 74.12      7.62 192.168.24.100          TLSv1     283 Application Data
356 97.107.139.108  192.168.24.100          TLSv1     110 Application Data, Application Data
358 192.168.24.100  97.107.139.108          TLSv1     720 Application Data, Application Data
359 74.125.227.62   192.168.24.100          TLSv1     122 Application Data
361 97.107.139.108  192.1     .100          TLSv1    1506 Application Data, Application Data
362 97.107.139.108  192         00          TLSv1     110 Application Data, Application Data
```

Length



```
349 74.        62   192.168.24.100                                TLSv1          crypted Handshake Message, Change
350                 97.107.139.108                                TLSv1          lication Data, Application Data
351                 192.168.24.100                                TLSv1          ication Data
354 97.        108  192.168.24.100                                TLSv1          plication Data, Application Data
355 74.12     7.62  192.168.24.100                                TLSv1          Application Data
356 97.107.139.108  192.168.24.100                                TLSv1     110 Application Data, Application Data
358 192.168.24.100  97.107.139.108                                TLSv1     720 Application Data, Application Data
359 74.125.227.62   192.168.24.100                                TLSv1     122 Application Data
361 97.107.139.108  192.1      .100                               TLSv1    1506 Application Data, Application Data
362 97.107.139.108  192         00                                TLSv1     110 Application Data, Application Data
```

Traffic Analysis. Huge Field



```
349 74.       62   192.168.24.100                     TLSv1       crypted Handshake Message, Change
350                97.107.139.108                     TLSv        ation Data, Application Data
351 7              192.168.24.100                     TLSv1         ication Data
354 97.        108 192.168.24.100                     TLSv1        plication Data, Application Data
355 74.12     7.62 192.168.24.100                     TLSv1       Application Data
356 97.107.139.108 192.168.24.100                     TLSv1     1 0 Application Data, Application Data
358 192.168.24.100 97.107.139.108                     TLSv1     720 Application Data, Application Data
359 74.125.227.62  192.168 24.100                     TLSv1     122 Application Data
361 97.107.139.108 192.1     .100                     TLSv1    1506 Application Data, Application Data
362 97.107.139.108 192        00                      TLSv1     110 Application Data, Application Data
```

HTTP

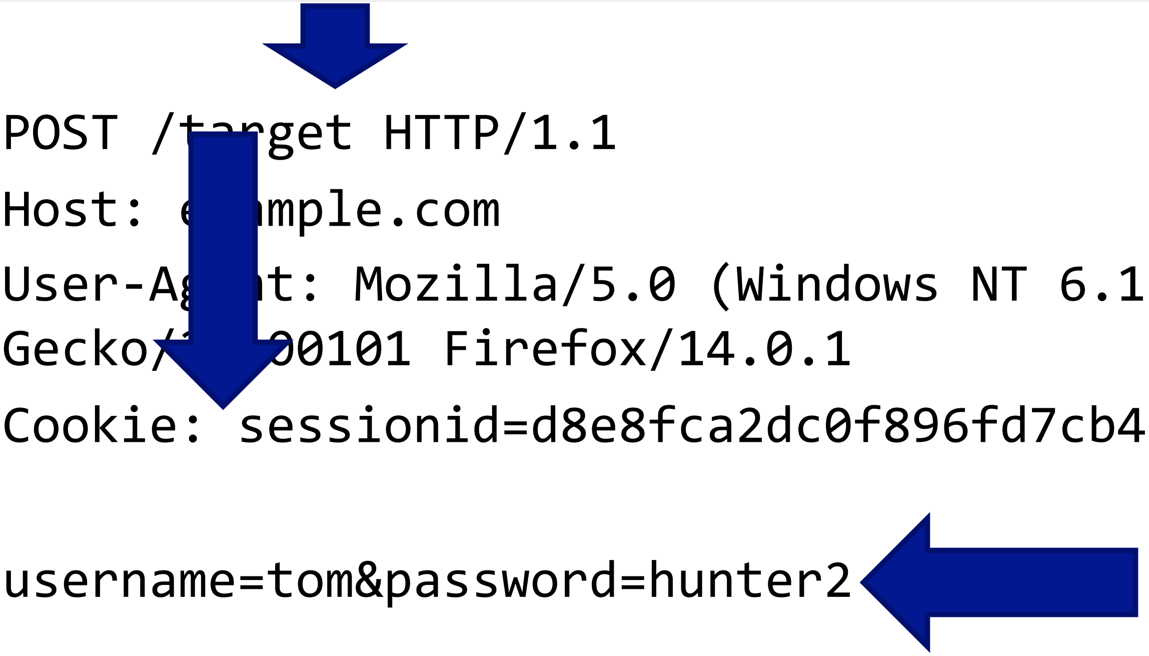
```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

username=tom&password=hunter2
```

HTTP

```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

username=tom&password=hunter2
```

Attacker wants to know this

Attacker Can Control



```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

username=tom&password=hunter2
```

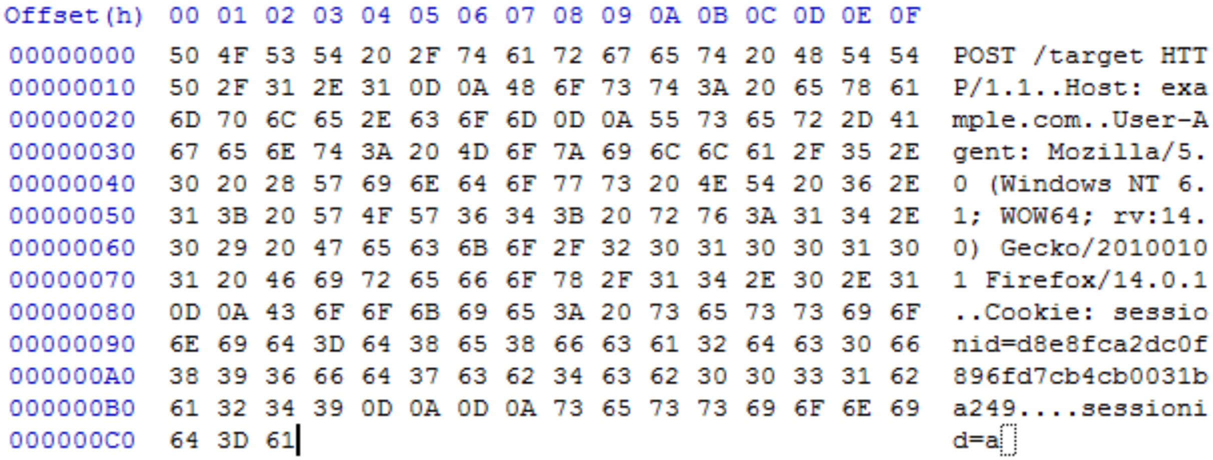
HTTP

```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

username=tom&password=hunter2
```

HTTP

```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

sessionid=a
```

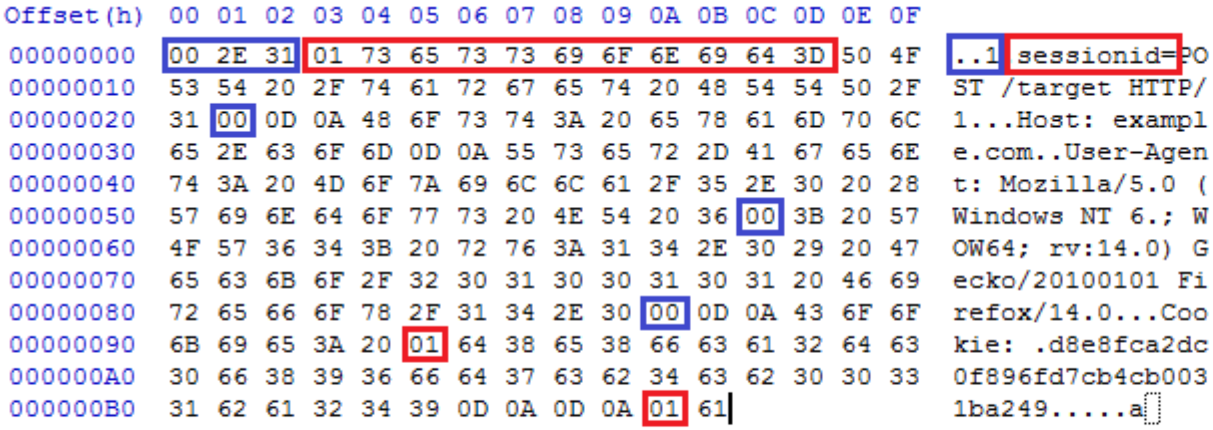
HTTP



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  50 4F 53 54 20 2F 74 61 72 67 65 74 20 48 54 54  POST /target HTT
00000010  50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 65 78 61  P/1.1..Host: exa
00000020  6D 70 6C 65 2E 63 6F 6D 0D 0A 55 73 65 72 2D 41  mple.com..User-A
00000030  67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E  gent: Mozilla/5.
00000040  30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E  0 (Windows NT 6.
00000050  31 3B 20 57 4F 57 36 34 3B 20 72 76 3A 31 34 2E  1; WOW64; rv:14.
00000060  30 29 20 47 65 63 6B 6F 2F 32 30 31 30 30 31 30  0) Gecko/2010010
00000070  31 20 46 69 72 65 66 6F 78 2F 31 34 2E 30 2E 31  1 Firefox/14.0.1
00000080  0D 0A 43 6F 6F 6B 69 65 3A 20 73 65 73 73 69 6F  ..Cookie: sessio
00000090  6E 69 64 3D 64 38 65 38 66 63 61 32 64 63 30 66  nid=d8e8fca2dc0f
000000A0  38 39 36 66 64 37 63 62 34 63 62 30 30 33 31 62  896fd7cb4cb0031b
000000B0  61 32 34 39 0D 0A 0D 0A 73 65 73 73 69 6F 6E 69  a249....sessioni
000000C0  64 3D 61                                         d=a
```

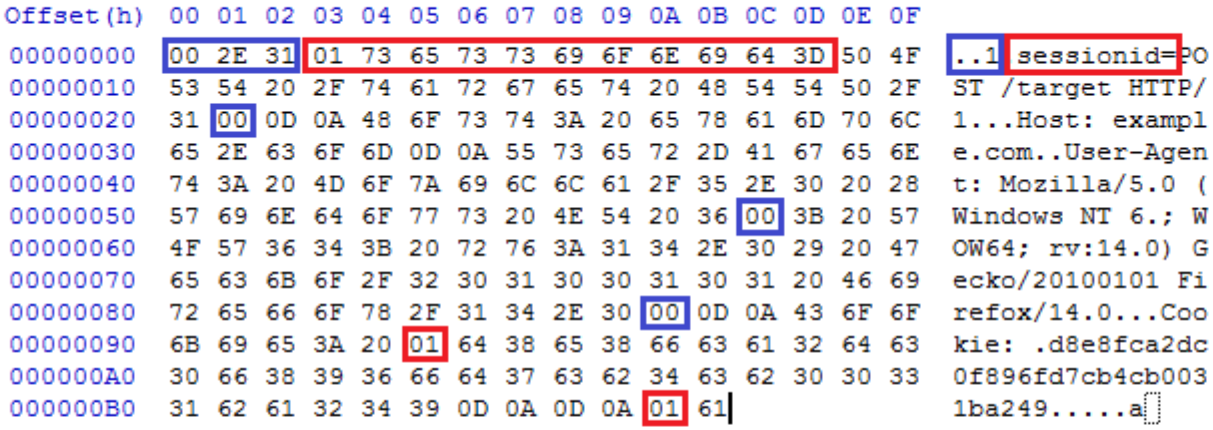
195 Bytes

HTTP



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  00 2E 31 01 73 65 73 73 69 6F 6E 69 64 3D 50 4F  ..1 sessionid=PO
00000010  53 54 20 2F 74 61 72 67 65 74 20 48 54 54 50 2F  ST /target HTTP/
00000020  31 00 0D 0A 48 6F 73 74 3A 20 65 78 61 6D 70 6C  1...Host: exampl
00000030  65 2E 63 6F 6D 0D 0A 55 73 65 72 2D 41 67 65 6E  e.com..User-Agen
00000040  74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28  t: Mozilla/5.0 (
00000050  57 69 6E 64 6F 77 73 20 4E 54 20 36 00 3B 20 57  Windows NT 6.; W
00000060  4F 57 36 34 3B 20 72 76 3A 31 34 2E 30 29 20 47  OW64; rv:14.0) G
00000070  65 63 6B 6F 2F 32 30 31 30 30 31 30 31 20 46 69  ecko/20100101 Fi
00000080  72 65 66 6F 78 2F 31 34 2E 30 00 0D 0A 43 6F 6F  refox/14.0...Coo
00000090  6B 69 65 3A 20 01 64 38 65 38 66 63 61 32 64 63  kie: .d8e8fca2dc
000000A0  30 66 38 39 36 66 64 37 63 62 34 63 62 30 30 33  0f896fd7cb4cb003
000000B0  31 62 61 32 34 39 0D 0A 0D 0A 01 61              1ba249.....a
```

HTTP



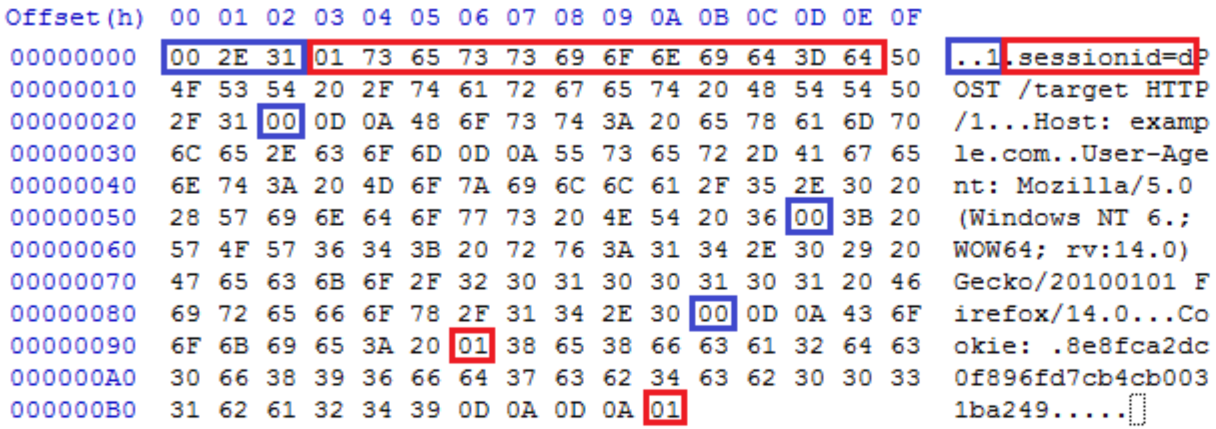
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  00 2E 31 01 73 65 73 73 69 6F 6E 69 64 3D 50 4F  ..1sessionid=PO
00000010  53 54 20 2F 74 61 72 67 65 74 20 48 54 54 50 2F  ST /target HTTP/
00000020  31 00 0D 0A 48 6F 73 74 3A 20 65 78 61 6D 70 6C  1...Host: exampl
00000030  65 2E 63 6F 6D 0D 0A 55 73 65 72 2D 41 67 65 6E  e.com..User-Agen
00000040  74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28  t: Mozilla/5.0 (
00000050  57 69 6E 64 6F 77 73 20 4E 54 20 36 00 3B 20 57  Windows NT 6.; W
00000060  4F 57 36 34 3B 20 72 76 3A 31 34 2E 30 29 20 47  OW64; rv:14.0) G
00000070  65 63 6B 6F 2F 32 30 31 30 30 31 30 31 20 46 69  ecko/20100101 Fi
00000080  72 65 66 6F 78 2F 31 34 2E 30 00 0D 0A 43 6F 6F  refox/14.0...Coo
00000090  6B 69 65 3A 20 01 64 38 65 38 66 63 61 32 64 63  kie: .d8e8fca2dc
000000A0  30 66 38 39 36 66 64 37 63 62 34 63 62 30 30 33  0f896fd7cb4cb003
000000B0  31 62 61 32 34 39 0D 0A 0D 0A 01 61              1ba249.....a
```

187 Bytes

HTTP

```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

sessionid=d
```

HTTP



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  00 2E 31 01 73 65 73 73 69 6F 6E 69 64 3D 64 50  ..1.sessionid=dP
00000010  4F 53 54 20 2F 74 61 72 67 65 74 20 48 54 54 50  OST /target HTTP
00000020  2F 31 00 0D 0A 48 6F 73 74 3A 20 65 78 61 6D 70  /1...Host: examp
00000030  6C 65 2E 63 6F 6D 0D 0A 55 73 65 72 2D 41 67 65  le.com..User-Age
00000040  6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20  nt: Mozilla/5.0
00000050  28 57 69 6E 64 6F 77 73 20 4E 54 20 36 00 3B 20  (Windows NT 6.;
00000060  57 4F 57 36 34 3B 20 72 76 3A 31 34 2E 30 29 20  WOW64; rv:14.0)
00000070  47 65 63 6B 6F 2F 32 30 31 30 30 31 30 31 20 46  Gecko/20100101 F
00000080  69 72 65 66 6F 78 2F 31 34 2E 30 00 0D 0A 43 6F  irefox/14.0...Co
00000090  6F 6B 69 65 3A 20 01 38 65 38 66 63 61 32 64 63  okie: .8e8fca2dc
000000A0  30 66 38 39 36 66 64 37 63 62 34 63 62 30 30 33  0f896fd7cb4cb003
000000B0  31 62 61 32 34 39 0D 0A 0D 0A 01                 1ba249.....
```

186 Bytes

HTTP

```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

sessionid=da
```

HTTP

```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

sessionid=da
```

188 Bytes

HTTP

```
POST /target HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249

sessionid=d8
```

187 Bytes

Fighting CRIME

- Browsers disabled TLS compression
- SPDY revised so request secrets are compressed in a separate context

BREACH

BREACH

- What about secrets in HTTP responses?
  - CSRF tokens
  - Any other sensitive information
- Similar to CRIME
- Requires a known secret prefix and the ability to inject into a response
- Difficult to identify false positives:
  - Secret: abcab1
  - Partial correct guess: abcab
  - Next character guesses that look right: “1”, “c”

BREACH: Mitigations

- Disable compression in responses (hahaha)
- Throttle the rather noisy attack (CRIME could MiTM and drop actual requests)
- Separate secrets into a separate file (such as javascript)
  - Difficult to implement
  - Hard to retrofit existing apps
- Randomize secrets per requests
  - Mainly for CSRF tokens, not for "attack at dawn"
  - Lots of performance
- Add some randomness to remove a fixed anchor

You Could Break the Internet!

- SSL/TLS!
- DNS!
- DNSSEC (Ho Boy, DNSSEC)
- IPv6 (Ho Boy, IPv6)

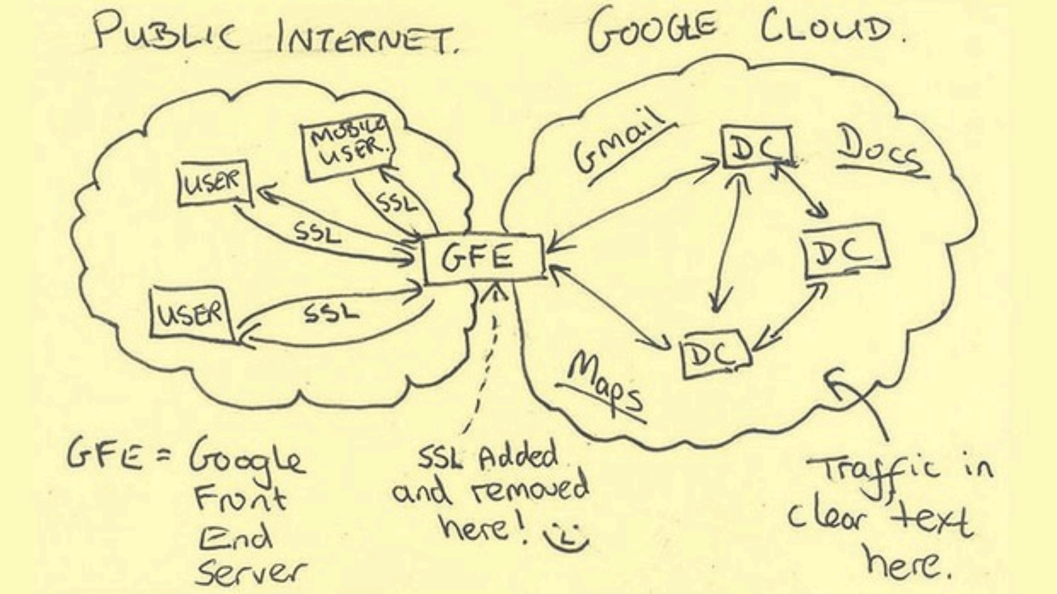
State Actors

Disclaimer

- I’m about to hate on the NSA
- The NSA people at the career fair can’t change policies
  - Intellectually stimulating work
  - They (hopefully) believe in benevolent usage
  - If you yell at them at the career fair, be honest: you’re doing it to make yourself feel better and not make a difference
- There are two sides to the coin, these are my opinions and not those of my employer
- I don’t think these have all been officially declassified

Snowden

- Some claims have been proven true, some proven false:
  - “Direct access to Google networks” [false]
  - Equivalent access [true]



PUBLIC INTERNET.
GOOGLE CLOUD.
USER
MOBILE USER.
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! :)
Traffic in clear text here.

- News filtered through media, snippets of documents

Government Muscle

- Very hard to resist cooperation:
  - LavaBit
  - Can’t publicly acknowledge cooperation of any kind
  - Terms and Conditions canaries

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

● High Speed Optical Cable

Covert, Clandestine or Coorperative Large Accesses

20 Access Programs Worldwide

● Regional

[redacted]
Geneva
Athens
Rome
Quito
San Jose

Caracas
Tegucigalpa
Bogota
Mexico City
Brasilia
Managua
[redacted]

Havana
Panama City
[redacted]

[redacted]
Lagos
[redacted]

Kinshasa
Lusaka
[redacted]
Budapest
Prague
Vienna
[redacted]

Sofia
[redacted]
Rangoon
[redacted]

[redacted]
Bangkok
New Delhi
[redacted]
Paris
[redacted]

Berlin
[redacted]
Frankfurt
[redacted]
Zagreb

[redacted]
Phnom Penh
Sarajevo
[redacted]

Pristina
Tirana
[redacted]
La Paz
[redacted]

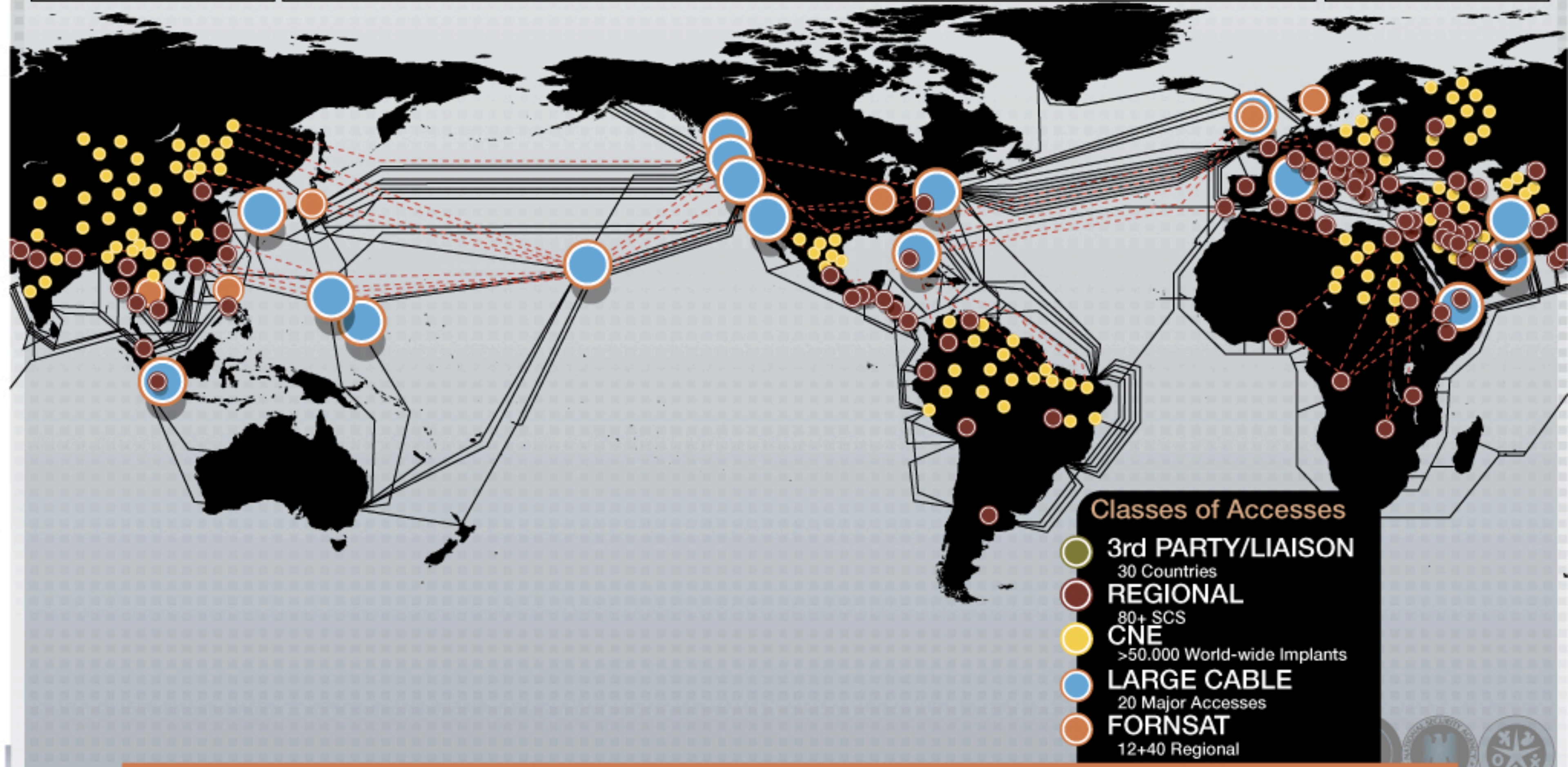
Guatemala City
[redacted]
Vienna Annex

[redacted]
RESC
[redacted]
Milan
[redacted]
Langley
Reston

● FORNSAT

STELLAR
SOUNDER
SNICK
MOONPEN
NY
LADYLOVE

INDRA
IRONSAND
JACKKNIFE
CARBOY
TIMBERLIN
E



Classes of Accesses

● 3rd PARTY/LIAISON
30 Countries

● REGIONAL
80+ SCS

● CNE
>50.000 World-wide Implants

● LARGE CABLE
20 Major Accesses

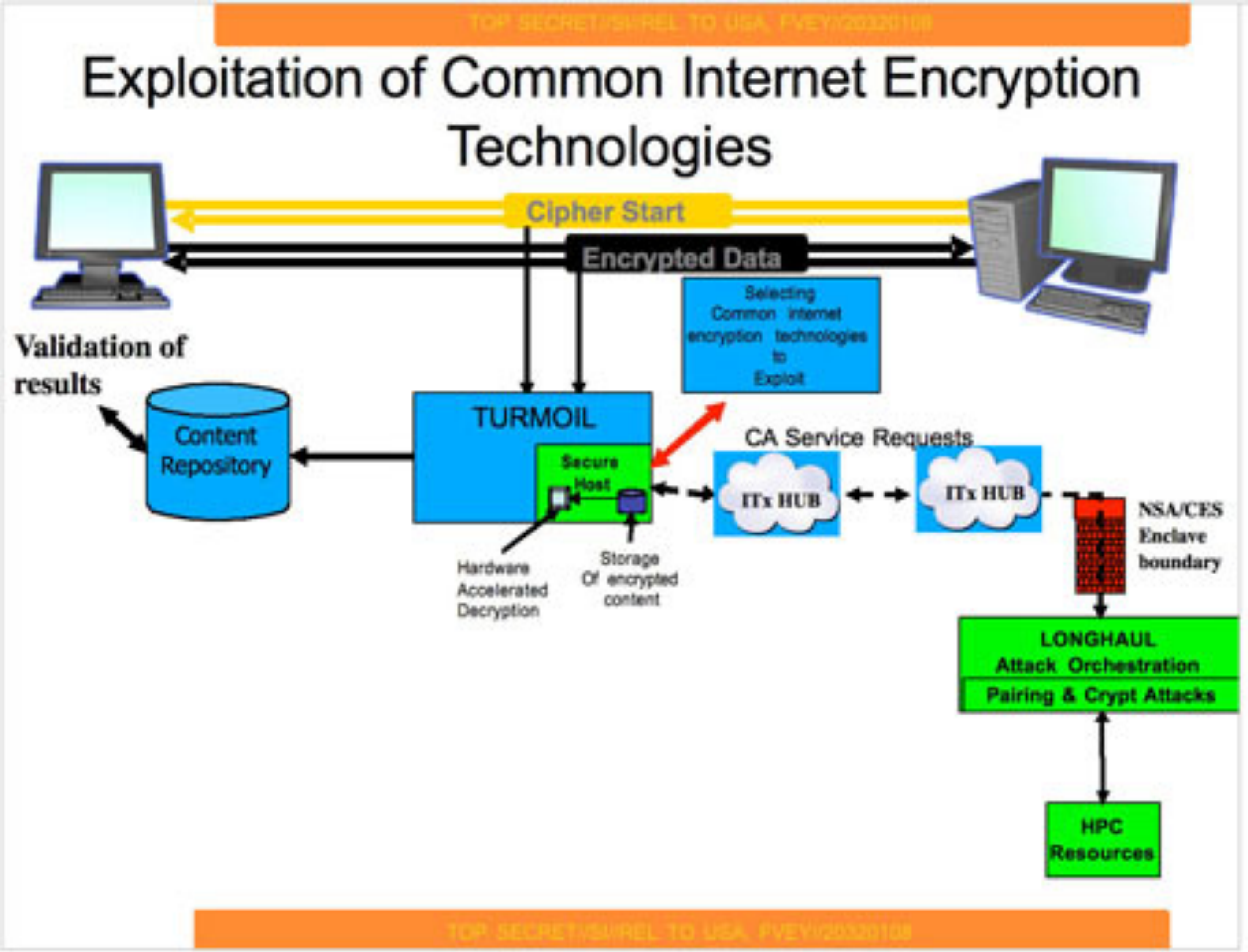
● FORNSAT
12+40 Regional

Bron: NSA

Government Muscle

- Cooperate => direct access, don't cooperate…
- From EFF lawsuit and list of acquired information, NSA is likely using optical taps
  - Catches phone calls, MPLS, even dedicated λ
  - Prevents leakage of targeting data to carriers
- Almost all US and many overseas carriers implicated
  - One map shows collection points around the world, including in non-ally countries. Secret taps?

TLS to Save The Day?



TOP SECRET//SI//REL TO USA, FVEY//20320108

Exploitation of Common Internet Encryption Technologies

TOP SECRET//SI//REL TO USA, FVEY//20320108

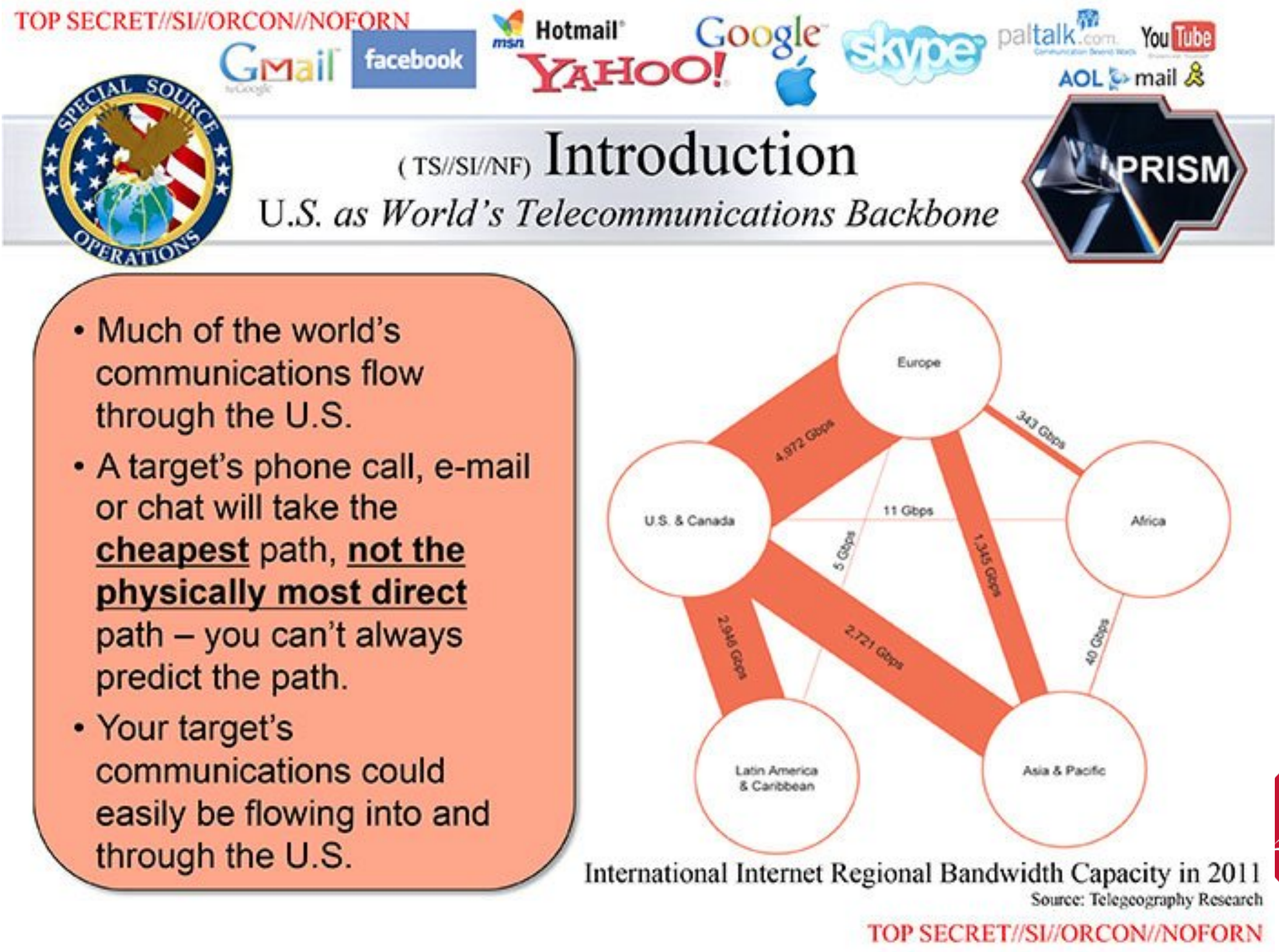
Crypto Attacks?

- Likely Pokemon private keys from edge servers (gah, why did we put them there)
  - Heartbleed
  - Standard network attacks
- POSSIBLE crypto attacks
  - MD5 collision used in Stuxnet (also had valid certs)
  - They have certs in your browser (noisy) and Google can detect it

Crypto Attacks?

- NIST creates all standards for encryption used (mostly) by everyone
- DUAL_EC_PRNG used to generate random values
- Prediction resistance based on solving ONE instance of elliptic curve discrete log
- The algorithm designer knew this before
- NSA discovered novel MD5 collision attacks better than other techniques

Global impact



TOP SECRET//SI//ORCON//NOFORN

Gmail
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
PRISM

(TS//SI//NF) Introduction

U.S. as *World's Telecommunications Backbone*

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

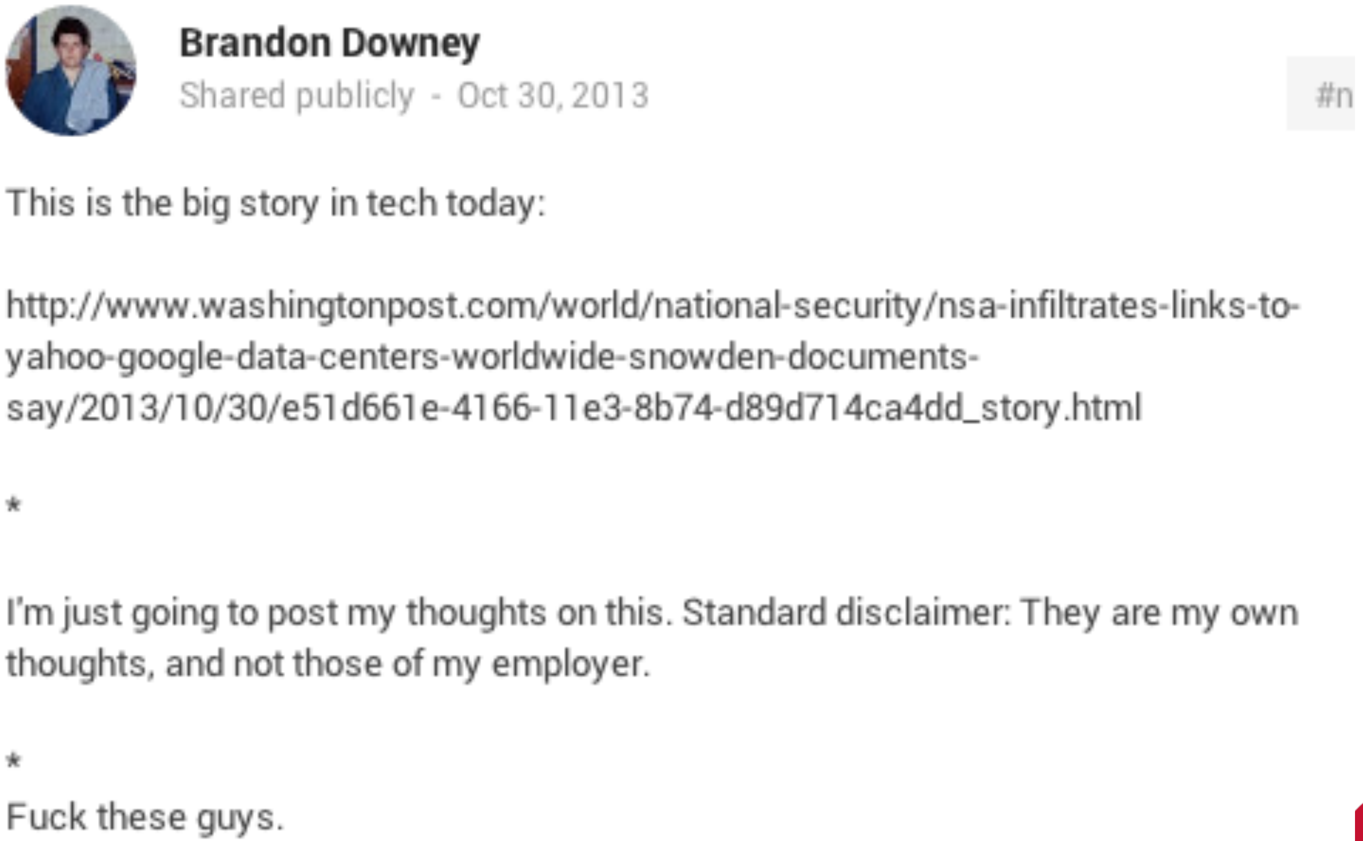
Europe
U.S. & Canada
Africa
Latin America & Caribbean
Asia & Pacific
4,972 Gbps
343 Gbps
11 Gbps
5 Gbps
1,345 Gbps
2,946 Gbps
2,721 Gbps
40 Gbps

International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

Blowback



Brandon Downey
Shared publicly - Oct 30, 2013

#n

This is the big story in tech today:

http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

*

I'm just going to post my thoughts on this. Standard disclaimer: They are my own thoughts, and not those of my employer.

*

Fuck these guys.

Blowback

- Hard for folks to trust US network equipment
- Hard for folks to trust US service offerings
- “If one would give me six lines written by the hand of an honest man, I would find something in them to have him hanged.”
  – Cardinal Richelieu

You're too young to get this reference

Flame (Stuxnet's Cousin)

- Spyware
- Does crazy things like:
  - Get all the GPS tags from all your photos
  - Get your contact list from any Bluetooth attached phone
  - Screenshots, keystroke logging, audio recording

MD5 is Broken (an Interlude)

- MD5 is broken because you can find collisions
- Specifically, chosen-prefix collision
- Demonstrated to be feasible in 2008 to generate a rogue CA (http://marc-stevens.nl/research/papers/CR09-SSALMOdW.pdf)
- Attack required 3 days running on 215 PS3s to find a collision
- Everyone panics, CAs stop using MD5 entirely

Flame (Stuxnet's Cousin)

- Microsoft forgot about one Microsoft Terminal Server still issuing MD5 certificates
- Attackers devised a new way to find MD5 collisions
- Harder challenges, 1 ms time window to get the right timestamp
- Created an arbitrary MS root certificate for signing anything

Flame (Stuxnet's Cousin)

- Microsoft forgot about one Microsoft Terminal Server still issuing MD5 certificates
- Attackers devised a new way to find MD5 collisions
- Harder challenges, 1 ms time window to get the right timestamp
- Created an arbitrary MS root certificate for signing anything
- .... Like Windows Updates

Flame (Stuxnet’s Cousin)

- “Oh Hai! I’m a Windows Update server!”
- “Oh Hello, I need an update.”
- “Here, have delicious delicious Flame!”
- “You silly goose, this is signed by MS! I’ll install it!”

I Love Security, What’s Next?

- Ethics in security
- Possible careers

Ethics in Security

- Big ethical debates used to be:

Responsible vs Full Disclosure

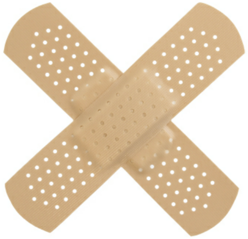
Ethics in Security

- Big ethical debates used to be:

  Responsible vs Full Disclosure

- Debate has shifted to:

  Disclosure vs Selling Weapons



Ethics in Security

- A single iOS 0-day sold for a purported 250k, allegedly to the US government
- Think jailbreakme.com
- Most profitable way to be a hacker is likely to sell exploits
- Be afraid, be very afraid (tin foil available up front)
- But remember, there are many ways to make money by being unethical, you still shouldn't do it

Careers in Security

- Shape your job around your ethical standpoint, not vice versa

Careers in Security

- Shape your job around your ethical standpoint, not vice versa
- Write security relevant software

Careers in Security

- Shape your job around your ethical standpoint, not vice versa
- Write security relevant software
- Write (more) secure software

Careers in Security

- Shape your job around your ethical standpoint, not vice versa
- Write security relevant software
- Write (more) secure software
- Be a criminal

Careers in Security

- Shape your job around your ethical standpoint, not vice versa
- Write security relevant software
- Write (more) secure software
- Be a criminal
- Academia

Careers in Security

- Shape your job around your ethical standpoint, not vice versa
- Write security relevant software
- Write (more) secure software
- Be a criminal
- Academia
- Independent researcher

Careers in Security

- Shape your job around your ethical standpoint, not vice versa
- Write security relevant software
- Write (more) secure software
- Be a criminal
- Academia
- Independent researcher
- Pen testing!

Pen Testing (at iSEC Partners)

- See new companies every 2-3 weeks and touch a wide variety of technologies
- Do awesome research (be a pen tester and a security researcher)
- Have a big impact by making the world safer
- Spend most of your time being clever and thinking
- See us at the job fair on Friday!

Thanks for listening!

iSECpartners part of nccgroup

paul@isecpartners.com

See me up front, or stop by our booth at the career fair!

Help with material from:

- Aaron Grattafiori (Principle Security Consultant, iSEC Partners)
- Alex Stamos (Co-Founder iSEC Partners, Artemis Internet, CSO Yahoo Inc.)

Images:

http://www.babylifestyles.com/images/blog/2009/05/stork.gif

http://cdn3.mixrmedia.com/wp-uploads/wirebot/blog/2010/01/jacked_in.jpg

http://www.dan-dare.org/FreeFun/Images/CartoonsMoviesTV/BugsLifeWallpaper800.jpg

http://cdn.tss.uproxx.com/TSS/wp-content/uploads/2008/03/ep60_mcnultybunk_506_03.jpg

http://desertpeace.files.wordpress.com/2010/11/spy-vs-spy.jpg

http://upload.wikimedia.org/wikipedia/commons/thumb/d/d7/Don_Knotts_Jim_Nabors_Andy_Griffith_Show_1964.JPG/220px-Don_Knotts_Jim_Nabors_Andy_Griffith_Show_1964.JPG

http://worldofstuart.excellentcontent.com/bruceworld/pics/depp-pirate.jpg

http://keetsa.com/blog/wp-content/uploads/2007/09/nuclear_explosion.jpg

http://www.asianbite.com/photos/psy-gangnam-style_27980.jpg

http://upload.wikimedia.org/wikipedia/commons/d/d3/Cbc_encryption.png

http://www.neatorama.com/wp-content/uploads/2010/11/bugs-bunnyreclining-499x367.jpg

http://www.langner.com/en/wp-content/uploads/2011/12/IR-1-cascade-model1.jpg

http://bdnpull.bangorpublishing.netdna-cdn.com/wp-content/uploads/2012/06/Natanz_Ahmadinejad-Visit_4-computers-250x241.jpg

http://www.politico.com/blogs/bensmith/0509/Secret_CIA_document_on_White_House_Flickr_feed.html

http://www.sirlin.net/storage/street_fighter/dhalsim_yoga_flame.gif?__SQUARESPACE_CACHEVERSION=1226558938179

http://www.cosmosmagazine.com/files/imagecache/feature/files/20080314_sherlock_holmes.jpg

http://www.inquisitr.com/wp-content/2012/08/original3-e1346095350417.jpg

http://www-bgr-com.vimg.net/wp-content/uploads/2011/06/lulzsec-hackers110624115314.jpg

http://img.timeinc.net/time/photoessays/2009/blame_25/blame_25_madoff.jpg

http://www.imgbase.info/images/safe-wallpapers/miscellaneous/1_other_wallpapers/16562_1_other_wallpapers_hal_9000.jpg

http://www.thecfpgroup.com/images/engineers.gif

http://www.moviefanatic.com/gallery/ryan-gosling-in-drive/

http://www.allmovieposter.org/poster/the-usual-suspects-poster-15.jpg

Game of thrones

http://www.npr.org/blogs/money/

http://disneyexaminer.com/wp-content/uploads/2014/07/marvel-guardians-of-the-galaxy-spoiler-free-review-drax-the-destroyer.jpg

UK Offices

Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

European Offices

Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland

North American Offices

San Francisco
Atlanta
New York
Seattle

Australian Offices

Sydney