

Methodological issues in:

“The Security Impact of HTTPS Interception”

Stefan Savage  
University of California, San Diego

## First, another hypothetical measurement project

Is your phone listening in to you?

- It is frequently alleged that smart phone apps do “word spotting”, surreptitiously listening to your conversations and then selling that information to advertisers (e.g., right after talking about needing a car, you get a Honda ad)

How might you try test this theory empirically?

- Limitations/assumptions?

There are two alternative explanations for this effect:

- **Apophenia** – people tend to notice patterns where there are none (i.e., you notice the correlation between ad and interest, but not the non-correlations)
- **Correlated leakage** – people may not notice the signals they are giving off (e.g., visiting caranddriver.com, doing searches about cars, etc)
- How might you design an experiment to test for this?

## Context for today: TLS (aka HTTPS)

### Transport Layer Security

“The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications”

- What does that mean? What is being “claimed”?

#### Authenticity

- That the server is who they say they are (e.g., [www.amazon.com](https://www.amazon.com))

#### Confidentiality

- That no one but the client and server can read the content of the messages they exchange

#### Integrity

- That no one can alter the messages being exchange without being detected

Note: TLS is not only used for HTTPS but other protocols too; also not all HTTPS use is in a browser (e.g., apps)

# History of the Protocol

## SSL 1.0

- Internal Netscape design, early 1994? Bad enough that never released

## SSL 2.0

- Published by Netscape, November 1994
- Badly badly broken

## SSL 3.0

- Designed by Netscape and Paul Kocher, November 1996

## TLS 1.0

- Internet standard based on SSL 3.0, January 1999
- Not interoperable with SSL 3.0

## TLS 1.1 (2006), 1.2 (2008), 1.3 (2018)

- Add ciphersuites and various fixes (padding, prevent downgrade to 2.0, etc), remove features, forward security; recently ECH, PQ crypto

# TLS Handshake Protocol (10,000 foot level)

Negotiate version of the protocol and the set of cryptographic algorithms to be used

- Client offers sets of options it supports ([ClientHello](#)); server will select from among those
- Interoperability between different implementations of the protocol

Server provides public key to establish a shared secret ([ServerHello](#))

- Client picks random session key, encrypts with Server's public key and sends to server ([ClientKeyExchange](#)); server decrypts session key
- Client and server use session key for symmetric encryption and MAC (or combined via AEAD) going forward; end-to-end security (ish)

But how does client know the public key *really belongs to the domain*?

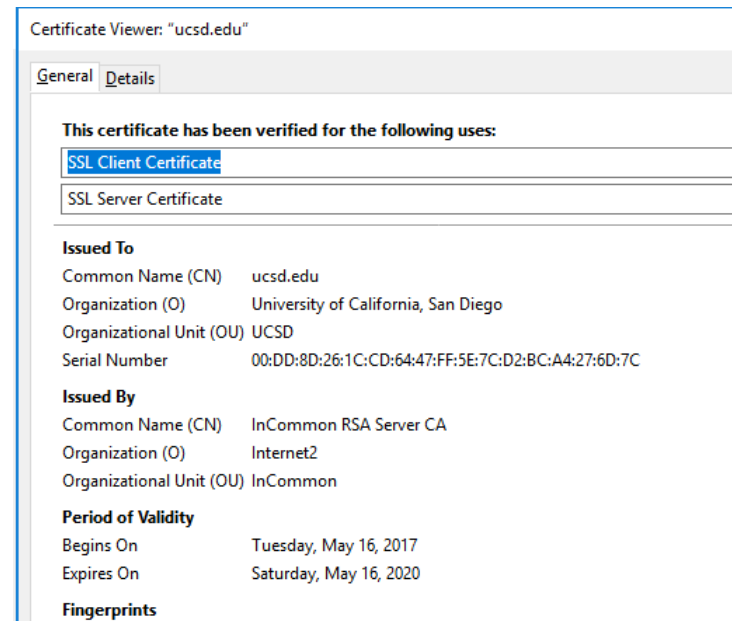
- I.e., the site claims its amazon.com... but is it?

# Certificate authorities

Third-parties who “attest” as to the integrity of the binding between a **name(s)** (e.g., amazon.com) and a **certificate** (which contains the name’s public key) – *digitally signed by CA*

## Certificate semantics:

- Subject (name, domain)
- Issuing CA
- Validity period
- Limitations on use (e.g. can it be used to sign other certificates)



# But why do I trust the CA's signature?

Each OS and/or Browser has a list of “Root CAs”

- Anything they sign is implicitly assumed ok (e.g., 153 root CAs in MacOS)

| Keychain Access                                                                                                                                                                                                                                                                                       |             |               |                              |              |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|------------------------------|--------------|--|
| All Items Passwords Secure Notes My Certificates Keys Certificates                                                                                                                                                                                                                                    |             |               |                              |              |  |
| <div><div></div><div><b>XRamp Global Certification Authority</b><br/>Root certificate authority<br/>Expires: Sunday, December 31, 2034 at 9:37:19 PM Pacific Standard Time<br/>This certificate is valid</div></div> |             |               |                              |              |  |
| Name                                                                                                                                                                                                                                                                                                  | Kind        | Date Modified | Expires                      | Keychain     |  |
| AAA Certificate Services                                                                                                                                                                                                                                                                              | certificate | --            | Dec 31, 2028 at 3:59:59...   | System Roots |  |
| AC RAIZ FNMT-RCM                                                                                                                                                                                                                                                                                      | certificate | --            | Dec 31, 2029 at 4:00:00...   | System Roots |  |
| ACCV/RAIZ1                                                                                                                                                                                                                                                                                            | certificate | --            | Dec 31, 2030 at 1:37:37 AM   | System Roots |  |
| Actalis Authentication Root CA                                                                                                                                                                                                                                                                        | certificate | --            | Sep 22, 2030 at 4:22:02...   | System Roots |  |
| AffirmTrust Commercial                                                                                                                                                                                                                                                                                | certificate | --            | Dec 31, 2030 at 6:06:06...   | System Roots |  |
| AffirmTrust Networking                                                                                                                                                                                                                                                                                | certificate | --            | Dec 31, 2030 at 6:08:24...   | System Roots |  |
| AffirmTrust Premium                                                                                                                                                                                                                                                                                   | certificate | --            | Dec 31, 2040 at 6:10:36...   | System Roots |  |
| AffirmTrust Premium ECC                                                                                                                                                                                                                                                                               | certificate | --            | Dec 31, 2040 at 6:20:24...   | System Roots |  |
| Amazon Root CA 1                                                                                                                                                                                                                                                                                      | certificate | --            | Jan 16, 2038 at 4:00:00 P... | System Roots |  |
| Amazon Root CA 2                                                                                                                                                                                                                                                                                      | certificate | --            | May 25, 2040 at 5:00:00...   | System Roots |  |
| Amazon Root CA 3                                                                                                                                                                                                                                                                                      | certificate | --            | May 25, 2040 at 5:00:00...   | System Roots |  |
| Amazon Root CA 4                                                                                                                                                                                                                                                                                      | certificate | --            | May 25, 2040 at 5:00:00...   | System Roots |  |
| Apple Root CA                                                                                                                                                                                                                                                                                         | certificate | --            | Feb 9, 2035 at 1:40:36 PM    | System Roots |  |
| Apple Root CA - G2                                                                                                                                                                                                                                                                                    | certificate | --            | Apr 30, 2039 at 11:10:09...  | System Roots |  |
| Apple Root CA - G3                                                                                                                                                                                                                                                                                    | certificate | --            | Apr 30, 2039 at 11:19:06...  | System Roots |  |
| Atos TrustedRoot 2011                                                                                                                                                                                                                                                                                 | certificate | --            | Dec 31, 2030 at 3:59:59...   | System Roots |  |
| Atos TrustedRoot Root CA ECC G2 2020                                                                                                                                                                                                                                                                  | certificate | --            | Dec 10, 2040 at 12:39:09...  | System Roots |  |
| Atos TrustedRoot Root CA ECC TLS 2021                                                                                                                                                                                                                                                                 | certificate | --            | Apr 17, 2041 at 2:26:22 AM   | System Roots |  |
| Atos TrustedRoot Root CA RSA G2 2020                                                                                                                                                                                                                                                                  | certificate | --            | Dec 10, 2040 at 12:41:22...  | System Roots |  |
| Atos TrustedRoot Root CA RSA TLS 2021                                                                                                                                                                                                                                                                 | certificate | --            | Apr 17, 2041 at 2:21:09 AM   | System Roots |  |
| Autoridad de Certificación Firmaprofesional CIF A62634068                                                                                                                                                                                                                                             | certificate | --            | Dec 31, 2030 at 12:38:15...  | System Roots |  |
| Baltimore CyberTrust Root                                                                                                                                                                                                                                                                             | certificate | --            | May 12, 2025 at 4:59:00...   | System Roots |  |
| Buypass Class 2 Root CA                                                                                                                                                                                                                                                                               | certificate | --            | Oct 26, 2040 at 1:38:03...   | System Roots |  |
| Buypass Class 3 Root CA                                                                                                                                                                                                                                                                               | certificate | --            | Oct 26, 2040 at 1:28:58...   | System Roots |  |
| CA Disig Root R2                                                                                                                                                                                                                                                                                      | certificate | --            | Jul 19, 2042 at 2:16:39 AM   | System Roots |  |
| Certainly Root E1                                                                                                                                                                                                                                                                                     | certificate | --            | Mar 31, 2046 at 5:00:00...   | System Roots |  |
| Certainly Root R1                                                                                                                                                                                                                                                                                     | certificate | --            | Mar 31, 2046 at 5:00:00...   | System Roots |  |
| Certigna                                                                                                                                                                                                                                                                                              | certificate | --            | Jun 29, 2027 at 8:13:05 AM   | System Roots |  |
| certSIGN ROOT CA                                                                                                                                                                                                                                                                                      | certificate | --            | Jul 4, 2031 at 10:20:04 AM   | System Roots |  |

## But... this all creates a problem for enterprises

Why?

Don't want network traffic to be opaque to security analysis

- Intrusion detection/prevention
- Data leakage prevention
- PII logging requirements
- Etc

Similar issues for endpoint Antivirus/EDR software  
(really **anything** that wants to interpose on traffic;  
e.g. INetNanny)

# TLS interception – two separate TLS connections

## Normal TLS

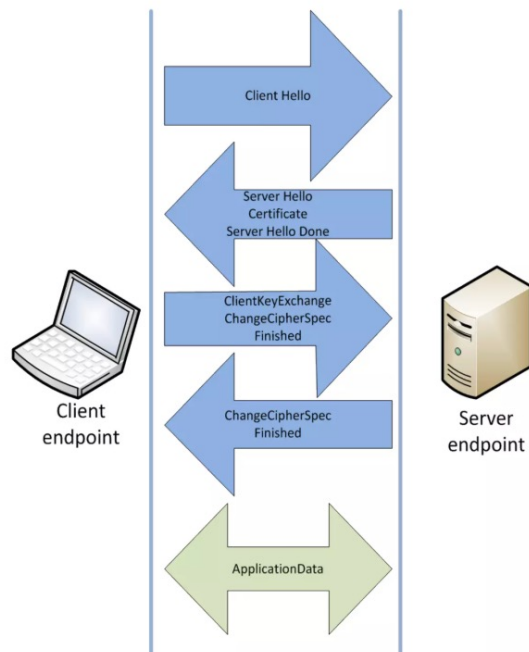


Figure 1. Sample two-party TLS handshake.

## TLS with interception

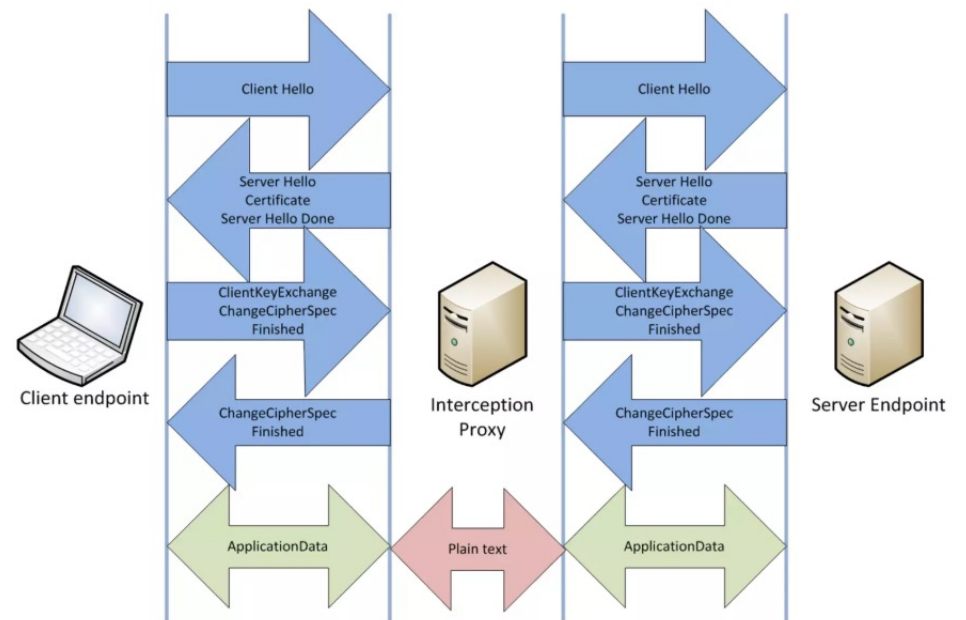


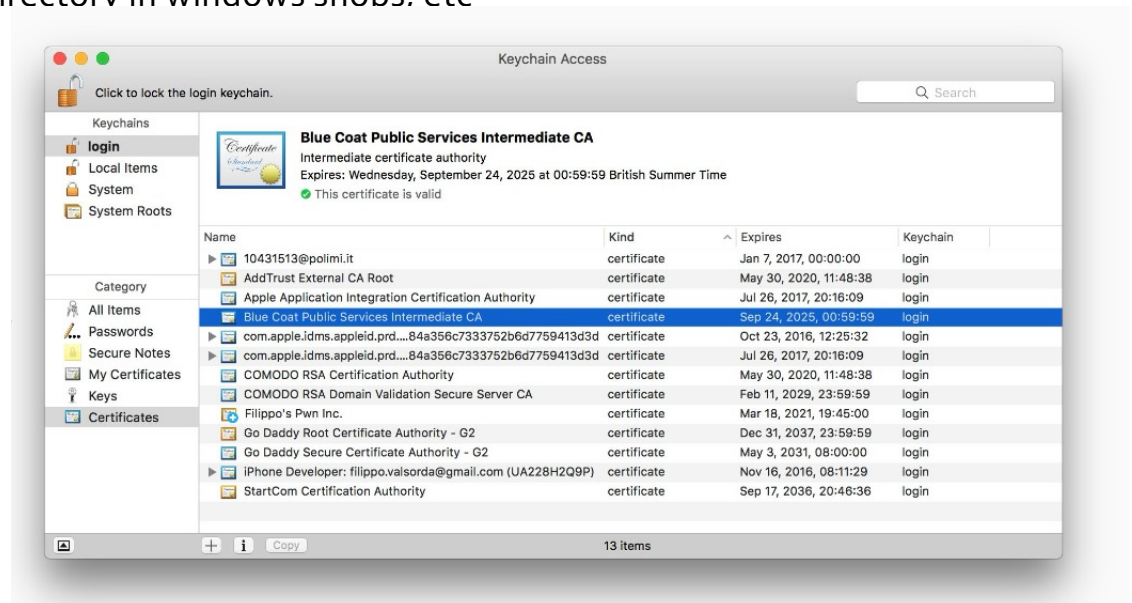
Figure 2. Sample SSL interception TLS handshakes.

## But won't the certificate check fail?

Yes, unless you:

- Install new rootCA on end hosts  
E.g., via MDM, via Active Directory in windows shops. etc
- Some root CAs issued subCAs for interception purposes (uncool)

If CA checks out,  
interception is *invisible*  
to both client and server



# Lots of products do this



**AVG**



1. [A10 vThunder](#)
2. [Arbor Networks Pravail](#)
3. [Baracuda Web Filter](#)
4. [BASCOM School Web Filter](#)
5. [Bloxx Web Filter](#)
6. [Blue Coat SSL Visibility Appliance](#)
7. [Check Point Data Loss Prevention \(DLP\), Anti Virus, Anti-Bot, Application Control, URL Filtering, Threat Emulation and IPS.](#)
8. [Cisco ScanCenter](#)
9. [Citrix NetScaler AppFirewall](#)
10. [Clearswift SECURE Web Gateway](#)
11. [ContentKeeper](#)
12. [Cymphonix Internet Management Suite](#)
13. [Dell SonicWALL](#)
14. [EdgeWave iPrism Web Security](#)
15. [ESET Smart Security](#)
16. [F5 BIG-IP](#)
17. [Fortinet FortiGate](#)
18. [Fidelis Security XPS](#)
19. [Finjan Vital Security \(pdf\)](#)
20. [GFI WebMonitor](#)
21. [GigaMon GigaSmart](#)
22. [IBM Security Network Protection](#)
23. [iboss Web Security](#)
24. [Imperva Incapsula](#)
25. [iSHERIFF Cloud Security](#)
26. [Juniper IDP devices](#)
27. [Kaspersky Anti-Virus](#)
28. [Komodia SSL Decoder](#)
29. [M86 Secure Web Gateway](#)
30. [McAfee Web Gateway and Firewall Enterprise \(pdf\)](#)
31. [Microsoft Forefront TMG](#)
32. [NetNanny](#)
33. [NextGig Netronome](#)
34. [Optenet WebFilter \(pdf\)](#)
35. [Palo Alto PAN-OS](#)
36. [Panda Cloud Internet Protection](#)
37. [PrivDog](#)
38. [Radware AppXcel](#)
39. [SafeNet eSafe Web Security Gateway](#)
40. [Sanqfor IAM \(pdf\)](#)
41. [Smoothwall Secure Web Gateway](#)
42. [Sophos Cyberoam](#)
43. [Sourcefire SSL Appliance](#)
44. [Squid](#)
45. [Symantec Web Gateway](#)
46. [Thomson Technologies Next Gen IPS](#)
47. [Trend Micro Deep Security \(pdf\)](#)
48. [Trustwave WebMarshal, Secure Web Gateway](#)
49. [Untangle NG Firewall](#)
50. [Venafi TrustAuthority](#)
51. [VSS Monitoring vinspector \(pdf\)](#)
52. [WatchGuard HTTPS Proxy](#)
53. [Wavecrest CyBlock](#)
54. [WebSense Content Gateway](#)
55. [WebTitan](#)
56. [Qbik WinGate](#)
57. [WolfSSL SSL Inspection](#)
58. [Zscaler](#)
59. [ZyXel Firewall](#)

## Ok, background done – now the key question

How often are HTTPS sessions being proxied?

How might you possibly measure this? (ignore paper for now)

- Identify popular middleboxes and develop network signatures (ala nmap) to identify them  
Pros/cons?
- Survey CISOs to ask if they do TLS interception  
Pros/cons?
- Client viewpoint  
Client records certificate they received from server X and sends to measurement server; compare certs received from X  
Pros/Cons?
- Client or server – some kind of timing side channel  
Maybe round-trip time to client for plain HTTP will be faster than HTTPS due to extra processing  
Pros/cons?

The client-side is where this happens, but they had server partners  
“When you have lemons, make lemonade”

# Basic idea – hunt for impossibility

Instead of “detect proxy” switch to “detect inconsistent browser”

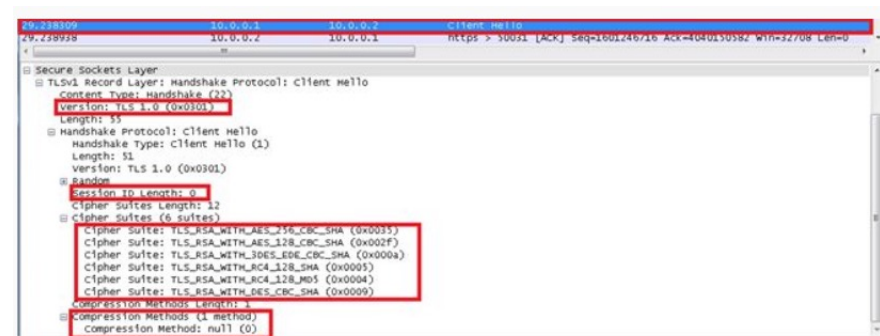
Two key pieces of information from client

- HTTP User-Agent string (browser version/OS)

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

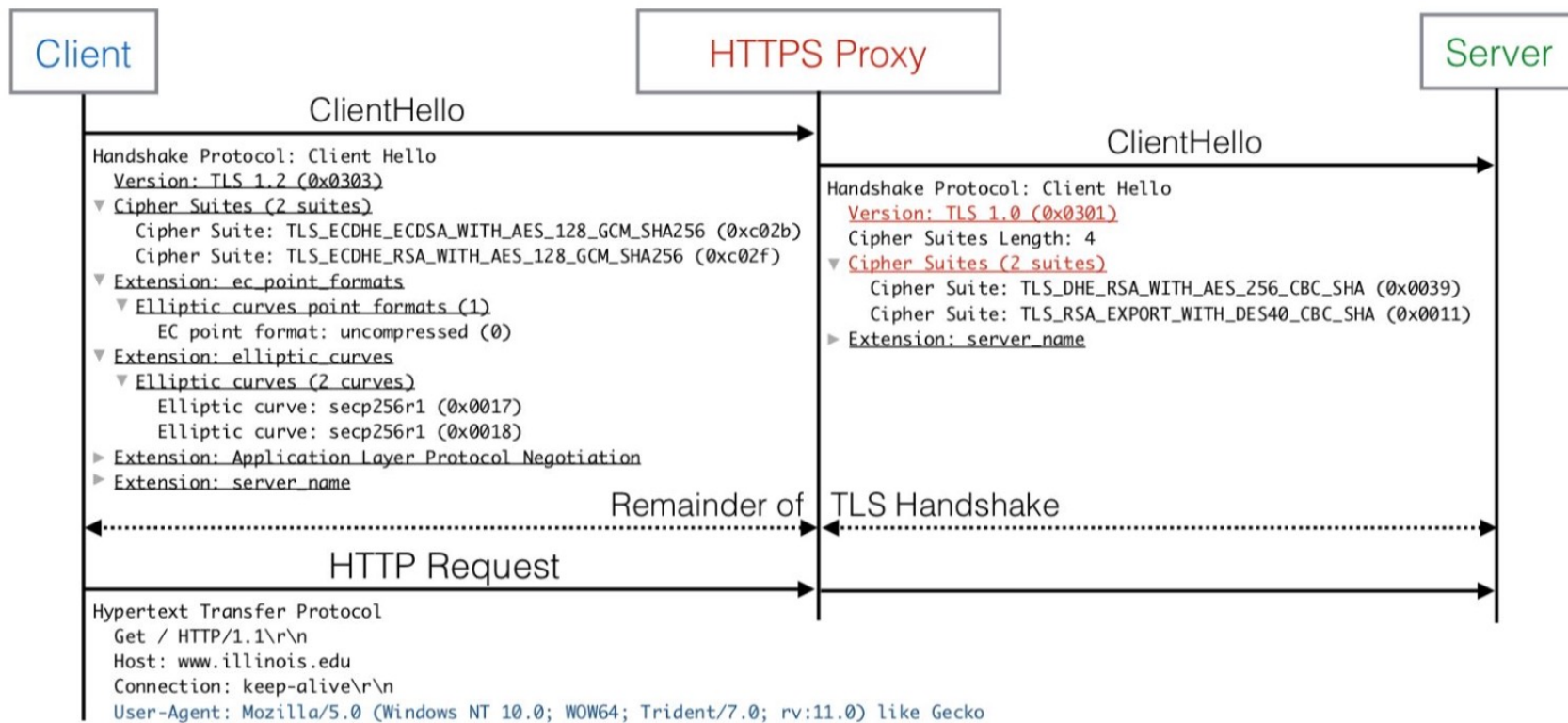
- Particular set of parameters in ClientHello

Identify which parameters were standard for each browser/version/OS



Do they match expectation?

# Impossibility example



## What are the key assumptions here?

### **We can obtain client connection data that is representative**

- We want to talk about prevalence, so people visiting universities may not cut it

### **We can effectively map ClientHello heuristics and User-Agents**

- Ideally these map one-to-one; worst case they are *non-deterministic*

### **The User-Agent header is correct**

- Easy to change; some software fakes it
- They don't check this... could they have? If so, how?

### **Proxy will not just match/duplicate client's ClientHello**

- Too many options, too much change; not worth it to preserve verisimilitude
- But what if they just match a popular one...?

### **Proxies differ in how they advertise ClientHello**

- Mainly matters for fingerprinting *kinds* of proxies

## Lets start with the first one

How to obtain representative client data?

Partners

- Cloudflare
- Firefox (update server)
- Google (“e-commerce servers”, but look at authors)

Some differences in how data collected

- **Cloudflare**: server logs
- **Firefox**: packet sniffer – don’t get User-Agent because **it is encrypted**  
Proxy: only specific Firefox versions configured to connect; so assume one of those
- **E-Commerce**: https tracking pixel inserted in site javascript  
International presence; likely skewed towards desktop (why?)  
“May suffer from falsified User-Agent Headers” – doesn’t explain; guesses?

# Mapping ClientHello and User Agents: Messy

## Firefox

- Almost the same across OS/hardware
- Fixed parameters (extensions, ciphers, curves, compression and fixed order)
  - Order distinct from other browsers (NSS)
- Users can remove ciphers, but can't add or reorder

## Safari

- No user customization, order is fixed; some unique features
- Modifications in minor releases (not included in User Agent)

## Chrome

- Lots of variability due to optimization (e.g., chacha20 > AES if no hw support for AES); multiple sets/orders valid for each browser version
- Users can also remove ciphers
- Less tight matching rules

## IE/Edge

- Even less consistent: admins can enable new ciphers, arbitrarily reorder ciphers
- Dumpster fire

# What do interception proxies actually do?

## Empirical ground truth

- Get trial versions of leading middleboxes and AVs and test  
Test how?
- Representative? What are potential sources of bias here?

Some DO match clients! (Bluecoat)

Test for “security”  
(more on this later)

| Product                        |
|--------------------------------|
| A10 vThunder SSL Insight       |
| Blue Coat ProxySG 6642         |
| Barracuda 610Vx Web Filter     |
| Checkpoint Threat Prevention   |
| Cisco IronPort Web Security    |
| Forcepoint TRITON AP-WEB Cloud |
| Fortinet FortiGate 5.4.0       |
| Juniper SRX Forward SSL Proxy  |
| Microsoft Threat Mgmt. Gateway |
| Sophos SSL Inspection          |
| Untangle NG Firewall           |
| WebTitan Gateway               |

| Product                  | OS  |
|--------------------------|-----|
| Avast ...                |     |
| AV 11                    | Win |
| AV 11.7                  | Mac |
| AVG ...                  |     |
| Internet Security 2015–6 | Win |
| Bitdefender ...          |     |
| Internet Security 2016   | Win |
| Total Security Plus 2016 | Win |
| AV Plus 2015–16          | Win |
| Bullguard ...            |     |
| Internet Security 16     | Win |
| Internet Security 15     | Win |
| CYBERSitter ...          |     |
| CYBERSitter 11           | Win |
| Dr. Web ...              |     |
| Security Space 11        | Win |
| Dr. Web 11 for OS X      | Mac |
| ESET ...                 |     |
| NOD32 AV 9               | Win |
| Kaspersky ...            |     |
| Internet Security 16     | Win |
| Total Security 16        | Win |
| Internet Security 16     | Mac |
| KinderGate ...           |     |
| Parental Control 3       | Win |
| Net Nanny ...            |     |
| Net Nanny 7              | Win |
| Net Nanny 7              | Mac |
| PC Pandora ...           |     |
| PC Pandora 7             | Win |
| Qustodio ...             |     |
| Parental Control 2015    | Mac |

## First big result: How much interception is inferred?

| Vantage Point | % HTTPS Connections Intercepted |        |           |
|---------------|---------------------------------|--------|-----------|
|               | No Interception                 | Likely | Confirmed |
| Cloudflare    | 88.6%                           | 0.5%   | 10.9%     |
| Firefox       | 96.0%                           | 0.0%   | 4.0%      |
| E-commerce    | 92.9%                           | 0.9%   | 6.2%      |

Fig. 2: **Detecting Interception**— We quantify HTTPS interception at three major Internet services. We estimate that 5–10% of connections are intercepted.

Much higher than any previous estimates

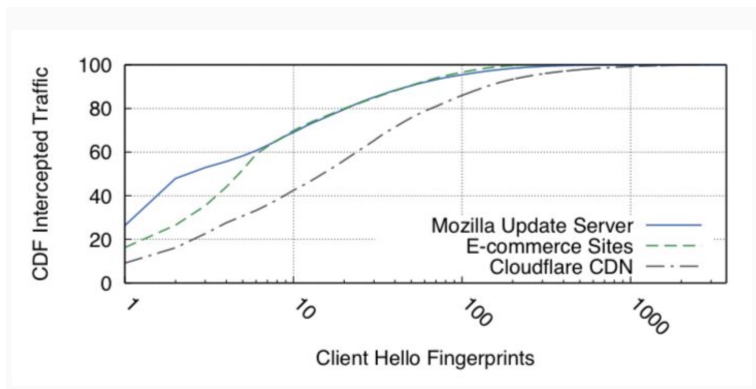
2.5x variation between vantage points

- Potential explanations? Testable?
- Implications?

Did you notice how results section is written?

- Why do you think this is?

## More on differences



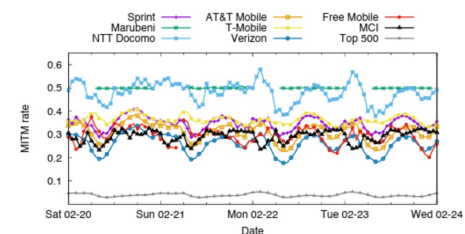
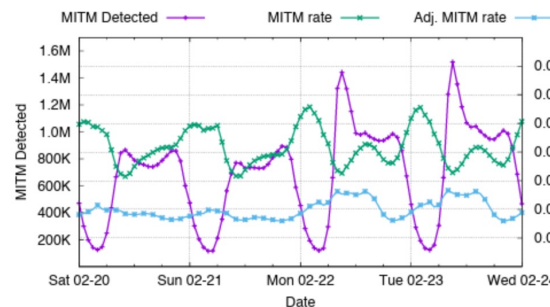
### Makeup of proxy fingerprints

- What product is being used to intercept?  
Note lots of unknowns; try to be conservative
- What kinds of conclusions/questions might you have here?

What is going on here?

| Fingerprint Description |                                                 | % Total |
|-------------------------|-------------------------------------------------|---------|
| E-commerce              | Unknown                                         | 17.1%   |
|                         | Avast Antivirus                                 | 10.8%   |
|                         | Unknown                                         | 9.4%    |
|                         | Blue Coat                                       | 9.1%    |
|                         | Unknown                                         | 8.3%    |
| Cloudflare              | Avast Antivirus                                 | 9.1%    |
|                         | AVG Antivirus                                   | 7.0%    |
|                         | Unknown. Likely AV; mainly Windows 10/Chrome 47 | 6.5%    |
|                         | Kaspersky Antivirus                             | 5.0%    |
|                         | BitDefender Antivirus                           | 3.1%    |
| Firefox                 | Bouncy Castle (Android 5)                       | 26.3%   |
|                         | Bouncy Castle (Android 4)                       | 21.6%   |
|                         | Unknown. Predominantly India                    | 5.0%    |
|                         | ESET Antivirus                                  | 2.8%    |
|                         | Dr. Web Antivirus                               | 2.6%    |

Fig. 6: **Top Interception Fingerprints**—We show the products responsible for the most interception at each vantage point.



## More on differences

| E-commerce Sites |             |             |                | Cloudflare    |             |             |                |
|------------------|-------------|-------------|----------------|---------------|-------------|-------------|----------------|
| Browser          | All Traffic | Intercepted | Of Intercepted | Browser       | All Traffic | Intercepted | Of Intercepted |
| Chrome           | 40.3%       | 8.6%        | 56.2%          | Chrome        | 36.2%       | 14.7%       | 48.8%          |
| Explorer         | 16.8%       | 7.4%        | 19.6%          | Mobile Safari | 17.5%       | 1.9%        | 3.3%           |
| Firefox          | 13.5%       | 8.4%        | 18.2%          | Explorer      | 14.9%       | 15.6%       | 21.2%          |
| Safari           | 10.2%       | 2.1%        | 3.4%           | Safari        | 8.9%        | 6.5%        | 5.3%           |
| Chromium         | 7.6%        | 0.1%        | 0.1%           | Firefox       | 8.5%        | 18.2%       | 14.2%          |
| Mobile Safari    | 7.6%        | 0.9%        | 1.1%           | Mobile Chrome | 8.4%        | 4.7%        | 3.6%           |
| Other            | 4.0%        | 4.0%        | 2.4%           | Other         | 5.6%        | 7.0%        | 3.6%           |
| OS               | All Traffic | Intercepted | Of Intercepted | OS            | All Traffic | Intercepted | Of Intercepted |
| Windows 7        | 23.3%       | 9.6%        | 56.6%          | Windows 7     | 23.9%       | 13.4%       | 29.2%          |
| Windows 10       | 22.5%       | 9.3%        | 14.3%          | Windows 10    | 22.9%       | 13.1%       | 27.4%          |
| iOS              | 17.3%       | 0.1%        | 1.1%           | iOS           | 17.5%       | 2.0%        | 3.2%           |
| Mac OS           | 15.8%       | 2.1%        | 6.5%           | Mac OS        | 16.0%       | 6.6%        | 9.6%           |
| Android          | 9.4%        | 1.0%        | 0.5%           | Android       | 9.5%        | 4.8%        | 4.2%           |
| Windows 8.1      | 6.9%        | 8.3%        | 15.8%          | Windows 8.1   | 4.9%        | 24.4%       | 11.0%          |
| Other            | 4.8%        | 21.4%       | 15.2%          | Other         | 5.3%        | 31.7%       | 15.4%          |

Fig. 13: **OS and Browser Breakdown**—We show the breakdown of all traffic, the amount of traffic intercepted, and percentage of all interception that each browser and operating system accounts for across both the e-commerce and Cloudflare vantage points.

## Massive tables

- What is interesting here? Anything?

## Where are these interceptions “from”?

| Network Type         | No Interception | Likely | Confirmed |
|----------------------|-----------------|--------|-----------|
| Residential/Business | 86.0%           | 0.4%   | 13.6%     |
| Cell Provider        | 94.1%           | 0.1%   | 5.8%      |

Fig. 12: **U.S. Network Breakdown**—We show the Cloudflare interception rates for types of U.S. networks.

| Country     | MITM % | Country     | MITM % |
|-------------|--------|-------------|--------|
| Guatemala   | 15.0%  | Kiribati    | 8.2%   |
| Greenland   | 9.9%   | Iran        | 8.1%   |
| South Korea | 8.8%   | Tanzania    | 7.3%   |
| Kuwait      | 8.5%   | Bahrain     | 7.3%   |
| Qatar       | 8.4%   | Afghanistan | 6.7%   |

Fig. 10: **Countries with Highest Firefox Interception**—We show the ten countries with the highest interception rates when connecting to the Mozilla update server. Countries with above average interception rates generally have a large amount of traffic intercepted by a single, dominant mobile provider.

Why do you think these are reported so differently?

- Cloudflare: resident vs cell; Firefox: country; Google: nothing

If you had IP address data, what questions would you want to ask?

- For validation
- To better understand forces driving interception

# Measuring “insecurity” due to proxying

How should we think about security impact of proxies?

- There is built-in added insecurity (new point of compromise, etc) but that is already “baked-in” in security/business decision
- But if we assume proxy *itself* is secure, what is impact on security of **connection**?

How to measure that?

- Are options being offered “worse” than what the browser had
- Does proxy do a worse job than browser



# Categorical data

Individual features, map back to qualitative grading scheme

- A: equivalent to modern browser
- B: non-ideal settings, but no known attack
- C: vulnerable to known attacks (but may be non-trivial attacks)
- D: Severely broken (straightforward for active PiTM)

What are tradeoffs in this kind of quantization?

| Product                        | Grade | Validates Certificates | Modern Ciphers | Advertises RC4 | TLS Version | Grading Notes                 |
|--------------------------------|-------|------------------------|----------------|----------------|-------------|-------------------------------|
| A10 vThunder SSL Insight       | F     | ✓                      | ✓              | Yes            | 1.2         | Advertises export ciphers     |
| Blue Coat ProxySG 6642         | A*    | ✓                      | ✓              | No             | 1.2         | Mirrors client ciphers        |
| Barracuda 610Vx Web Filter     | C     | ✓                      | ✗              | Yes            | 1.0         | Vulnerable to Logjam attack   |
| Checkpoint Threat Prevention   | F     | ✓                      | ✗              | Yes            | 1.0         | Allows expired certificates   |
| Cisco IronPort Web Security    | F     | ✓                      | ✓              | Yes            | 1.2         | Advertises export ciphers     |
| Forcepoint TRITON AP-WEB Cloud | C     | ✓                      | ✓              | No             | 1.2         | Accepts RC4 ciphers           |
| Fortinet FortiGate 5.4.0       | C     | ✓                      | ✓              | No             | 1.2         | Vulnerable to Logjam attack   |
| Juniper SRX Forward SSL Proxy  | C     | ✓                      | ✗              | Yes            | 1.2         | Advertises RC4 ciphers        |
| Microsoft Threat Mgmt. Gateway | F     | ✗                      | ✗              | Yes            | SSLv2       | No certificate validation     |
| Sophos SSL Inspection          | C     | ✓                      | ✓              | Yes            | 1.2         | Advertises RC4 ciphers        |
| Untangle NG Firewall           | C     | ✓                      | ✓              | Yes            | 1.2         | Advertises RC4 ciphers        |
| WebTitan Gateway               | F     | ✗                      | ✓              | Yes            | 1.2         | Broken certificate validation |

Fig. 3: **Security of TLS Interception Middleboxes**—We evaluate popular network middleboxes that act as TLS interception proxies. We find that nearly all reduce connection security and five introduce severe vulnerabilities. \*Mirrors browser ciphers.

| Product                  | - Grade | Validates Certificates | Modern Ciphers | TLS Version | Grading Notes             |
|--------------------------|---------|------------------------|----------------|-------------|---------------------------|
| Avast ...                |         |                        |                |             |                           |
| AV 11                    | A*      | ✓                      | ✓              | 1.2         | Mirrors client ciphers    |
| AV 11.7                  | F       | ✓                      | ✓              | 1.2         | Advertises DES            |
| AVG ...                  |         |                        |                |             |                           |
| Internet Security 2015–6 | C       | ✓                      | ✓              | 1.2         | Advertises RC4            |
| Bitdefender ...          |         |                        |                |             |                           |
| Internet Security 2016   | C       | ✓                      | ○              | 1.2         | RC4, 768-bit D-H          |
| Total Security Plus 2016 | C       | ✓                      | ○              | 1.2         | RC4, 768-bit D-H          |
| AV Plus 2015–16          | C       | ✓                      | ○              | 1.2         | RC4, 768-bit D-H          |
| Bullguard ...            |         |                        |                |             |                           |
| Internet Security 16     | A*      | ✓                      | ✓              | 1.2         | Mirrors client ciphers    |
| Internet Security 15     | F       | ✓                      | ✗              | 1.0         | Advertises DES            |
| CYBERSitter ...          |         |                        |                |             |                           |
| CYBERSitter 11           | F       | ✗                      | ✗              | 1.2         | No cert. validation, DES  |
| Dr. Web ...              |         |                        |                |             |                           |
| Security Space 11        | C       | ✓                      | ○              | 1.2         | RC4, FREAK                |
| Dr. Web 11 for OS X      | F       | ✓                      | ✗              | 1.0         | Export ciphers, DES, RC2  |
| ESET ...                 |         |                        |                |             |                           |
| NOD32 AV 9               | F       | ○                      | ○              | 1.2         | Broken cert. validation   |
| Kaspersky ...            |         |                        |                |             |                           |
| Internet Security 16     | C       | ✓                      | ✓              | 1.2         | CRIME vulnerability       |
| Total Security 16        | C       | ✓                      | ✓              | 1.2         | CRIME vulnerability       |
| Internet Security 16     | C       | ✓                      | ✓              | 1.2         | 768-bit D-H               |
| KinderGate ...           |         |                        |                |             |                           |
| Parental Control 3       | F       | ○                      | ✗              | 1.0         | Broken cert. validation   |
| Net Nanny ...            |         |                        |                |             |                           |
| Net Nanny 7              | F       | ✓                      | ✓              | 1.2         | Anonymous ciphers         |
| Net Nanny 7              | F       | ✓                      | ✓              | 1.2         | Anonymous ciphers         |
| PC Pandora ...           |         |                        |                |             |                           |
| PC Pandora 7             | F       | ✗                      | ✗              | 1.0         | No certificate validation |
| Qustodio ...             |         |                        |                |             |                           |
| Parental Control 2015    | F       | ✓                      | ✓              | 1.2         | Advertises DES            |

## Interception:

- No Interception (conn. allowed)
- Connections Blocked
- Connections Intercepted

## Certificate Validation:

- ✗ No Validation
- Broken Validation
- ✓ Correct Validation

## Modern Ciphers:

- ✗ No Support
- Non-preferred Support
- ✓ Preferred Support

| Network                  | Increased Security | Decreased Security | Severely Broken |
|--------------------------|--------------------|--------------------|-----------------|
| E-commerce (All Traffic) | 4.1%               | 26.5%              | 17.7%           |
| E-commerce (Middleboxes) | 0.9%               | 62.3%              | 58.1%           |
| Cloudflare               | 14.0%              | 45.3%              | 16.0%           |
| Firefox Updates          | 0.0%               | 65.7%              | 36.8%           |

| Dataset                          | Original Security | New Security |       |       |       |
|----------------------------------|-------------------|--------------|-------|-------|-------|
|                                  |                   | →A           | →B    | →C    | →F    |
| Firefox                          | A→                | 34.3%        | 16.8% | 12.2% | 36.8% |
| E-commerce Sites:<br>All Traffic | A→                | 57.1%        | 2.9%  | 5.6%  | 8.1%  |
|                                  | B→                | 2.7%         | 10.2% | 1.2%  | 8.3%  |
|                                  | C→                | 0.6%         | 0.4%  | 1.0%  | 0.3%  |
|                                  | F→                | 0.0%         | 0.2%  | 0.1%  | 1.0%  |
| E-commerce Sites:<br>Middleboxes | A→                | 13.5%        | 3.0%  | 0.8%  | 18.0% |
|                                  | B→                | 0.7%         | 23.3% | 0.6%  | 37.8% |
|                                  | C→                | 0.1%         | 0.1%  | 0.0%  | 2.2%  |
|                                  | F→                | 0.0%         | 0.0%  | 0.0%  | 0.0%  |
| Cloudflare                       | A→                | 17.3%        | 1.1%  | 29.7% | 10.0% |
|                                  | B→                | 0.0%         | 0.0%  | 0.0%  | 0.0%  |
|                                  | C→                | 9.4%         | 3.3%  | 22.0% | 4.5%  |
|                                  | F→                | 0.8%         | 0.1%  | 0.4%  | 1.5%  |

Fig. 15: **Change in Security**—We calculate the change in connection security based on the parameters advertised in the Client Hello message and the security of the browser in the HTTP User-Agent header.

## Note undercurrent of advocacy in paper

Does not affect methodology or analysis

But does emerge in recommendations;  
also note focus on middleboxes

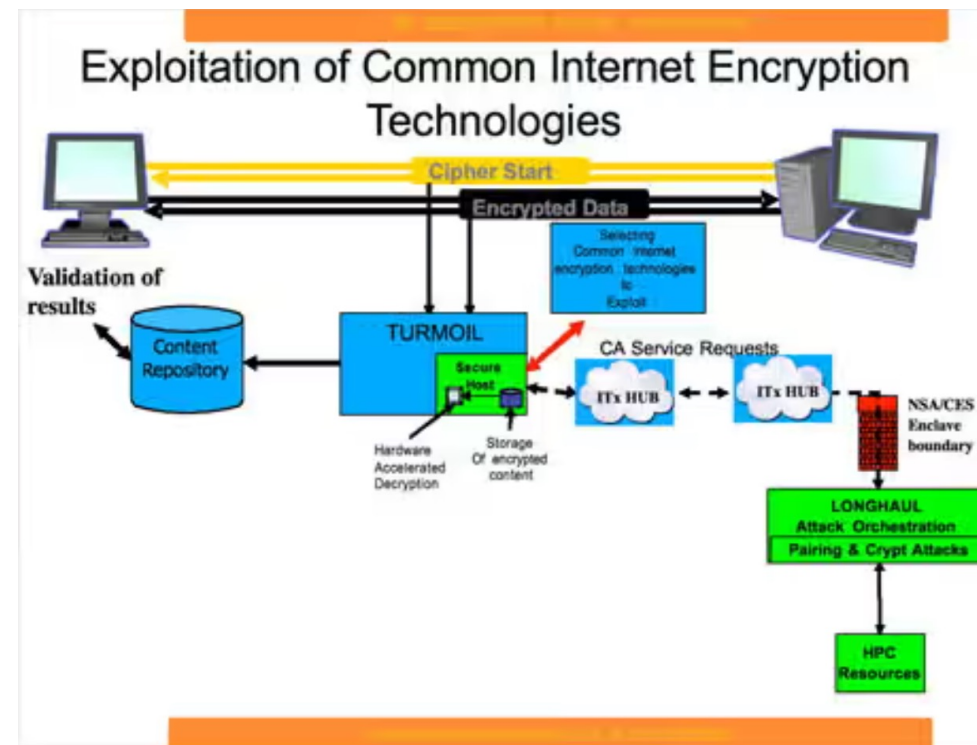
Not an accident that this paper is written at this time

- Any guesses about what might have been going on at the time that would have made this whole topic so interesting?

Aside: would this help in detecting state actors using passive interception/decryption?

Intercept TLS sessions (TURMOIL)  
and break crypto where possible  
(LONGHAUL)

No – invisible to client and server  
both (also no timing impact)



## Next class

“Re: CAPTCHAs – Understanding CAPTCHAs from an Economic Context”