The Security Impact of HTTPS Interception

NDSS ‘17

Z. Durumeric, Z. Ma, D. Springall, R. Barnes, N. Sullivan, E. Bursztein, M. Bailey, J. Alex Halderman, V. Paxson

Presented by: Sanjeev Reddy

go NSRG!

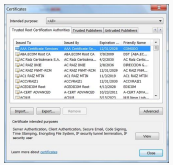
Some Background

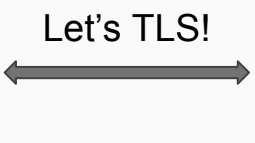
How to TLS

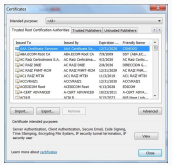
1.  Hi, I'm Chrome! 

2.  Hi, I'm Domain! Here's my cert  

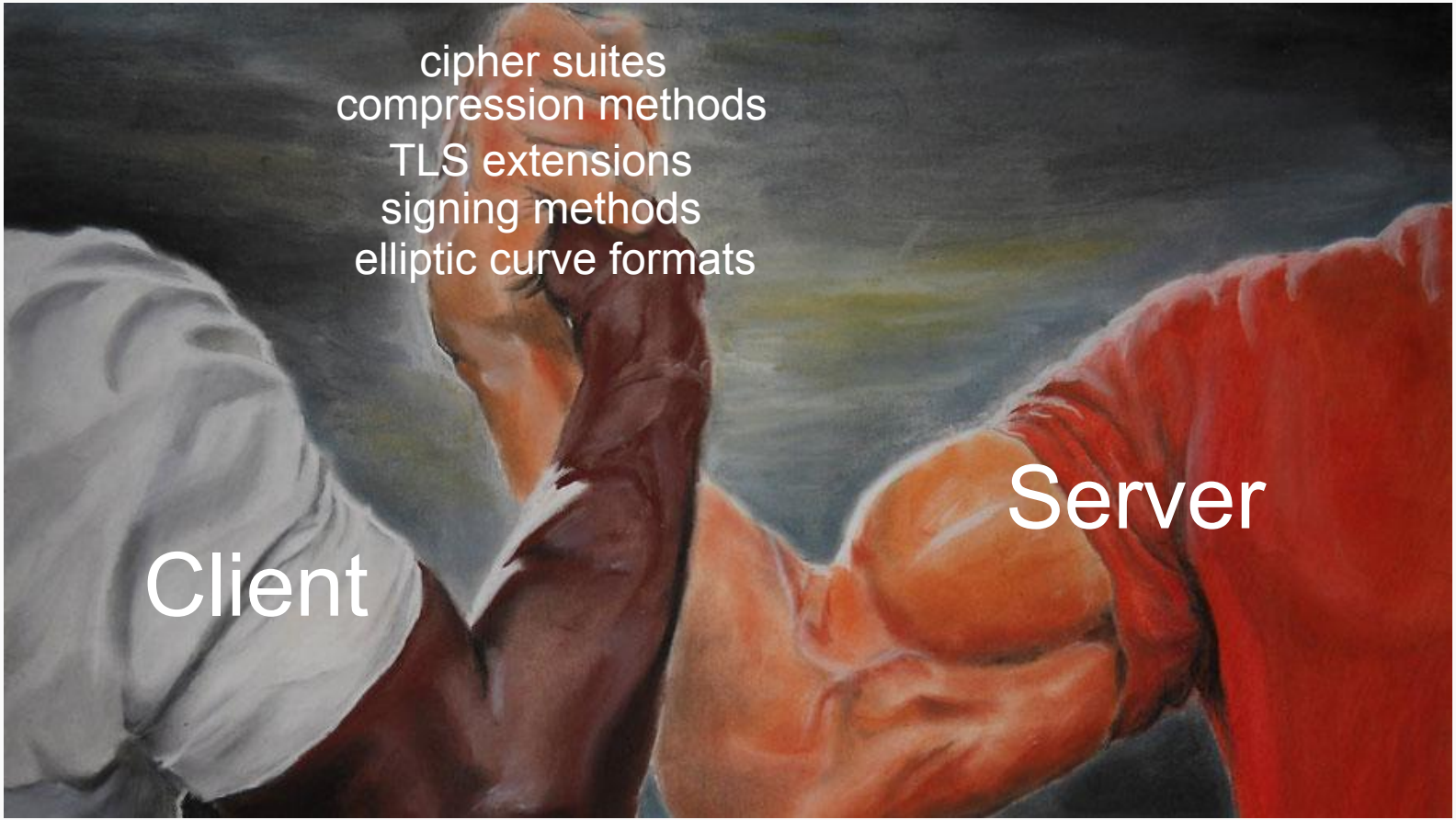
3.  ?  Was this signed by someone I trust?



4.  ✓  Let's TLS! 



How to TLS


cipher suites
compression methods
TLS extensions
signing methods
elliptic curve formats
Client
Server

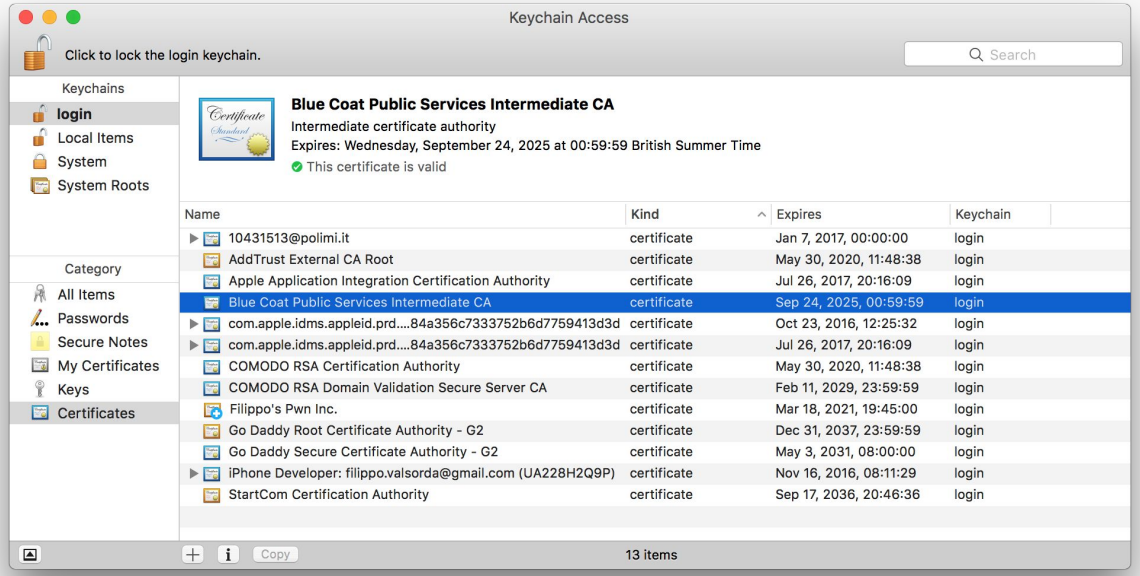
How to TLS (now with interception!)

But doesn't TLS protect
against man-in-the-middling?

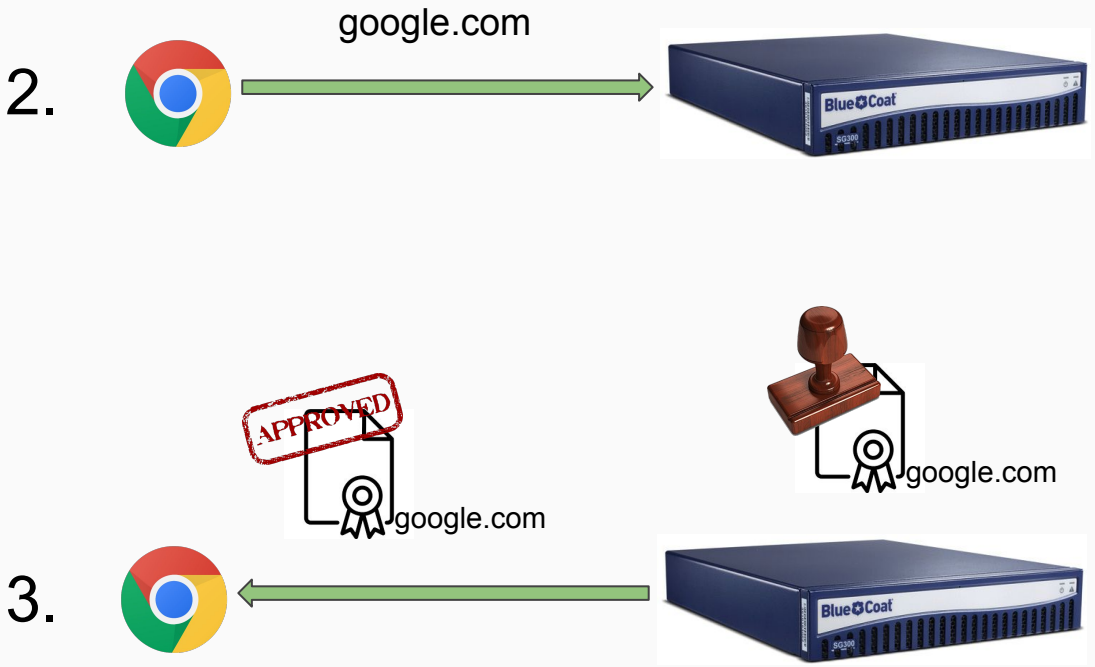
Answer: kind of...

How to TLS (now with interception!)

1.



How to TLS (now with interception!)

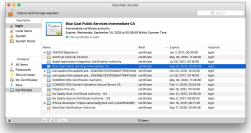


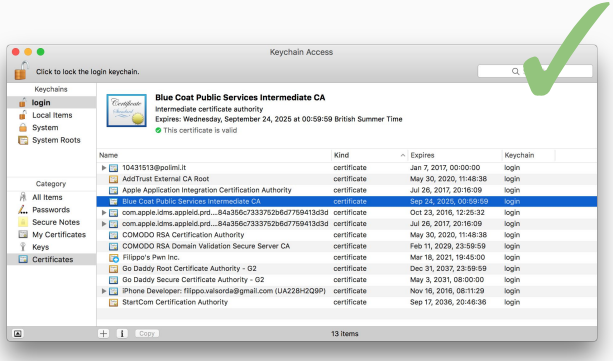
How to TLS (now with interception!)

4. 

?

Was this signed by someone I trust?



5. 

6. 

Google

Who’s intercepting? Why?

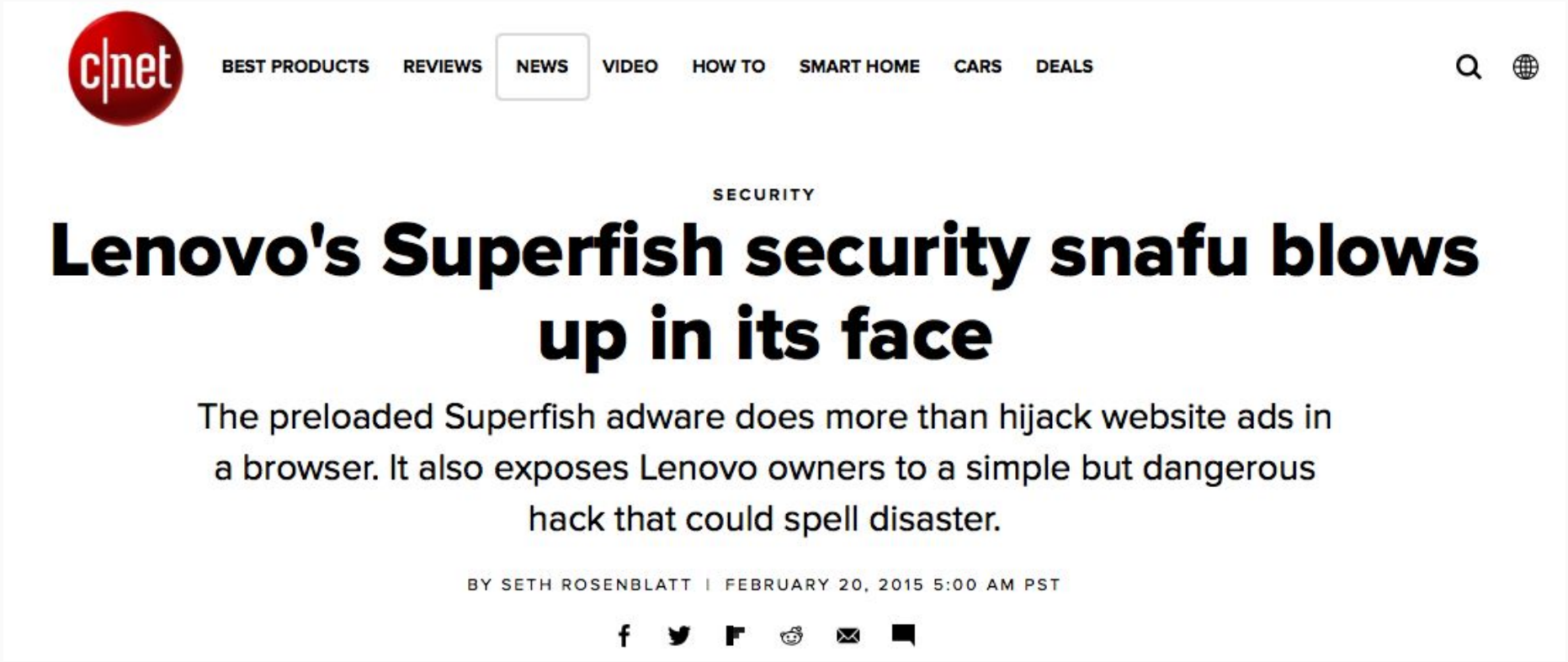
- Corporate middleboxes
  - content filtering
  - malware detection
  - traffic analysis
- Antivirus software
  - content filtering
  - malware detection
- Bloatware and malware
  - content injection
  - traffic analysis

avast

privdog

Superfish™
Search Visually

Superfish



c|net BEST PRODUCTS REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS

SECURITY

Lenovo's Superfish security snafu blows up in its face

The preloaded Superfish adware does more than hijack website ads in a browser. It also exposes Lenovo owners to a simple but dangerous hack that could spell disaster.

BY SETH ROSENBLATT | FEBRUARY 20, 2015 5:00 AM PST

Goals of this Paper

- Detect interception and identify the interceptors
- Evaluate the security impact of interception

Part 1:
Detecting Interception

Detection Strategy

Identify a mismatch in connection details between HTTP User-Agent Header and TLS Client Hello

HTTP User-Agent Header

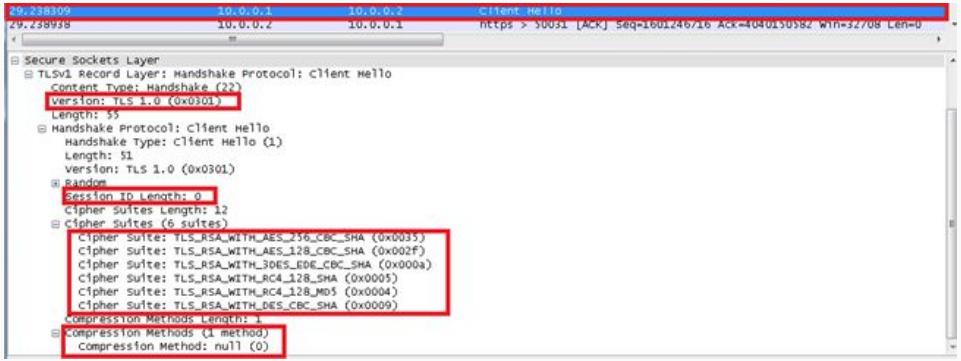
A standard HTTP header that includes:

- Client browser
- Client OS

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

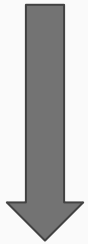
TLS Client Hello

- First message in establishing a TLS connection between a client and server
- Specifies details for the connection as chosen by the client
  - Cipher suites
  - Compression methods
  - TLS extensions

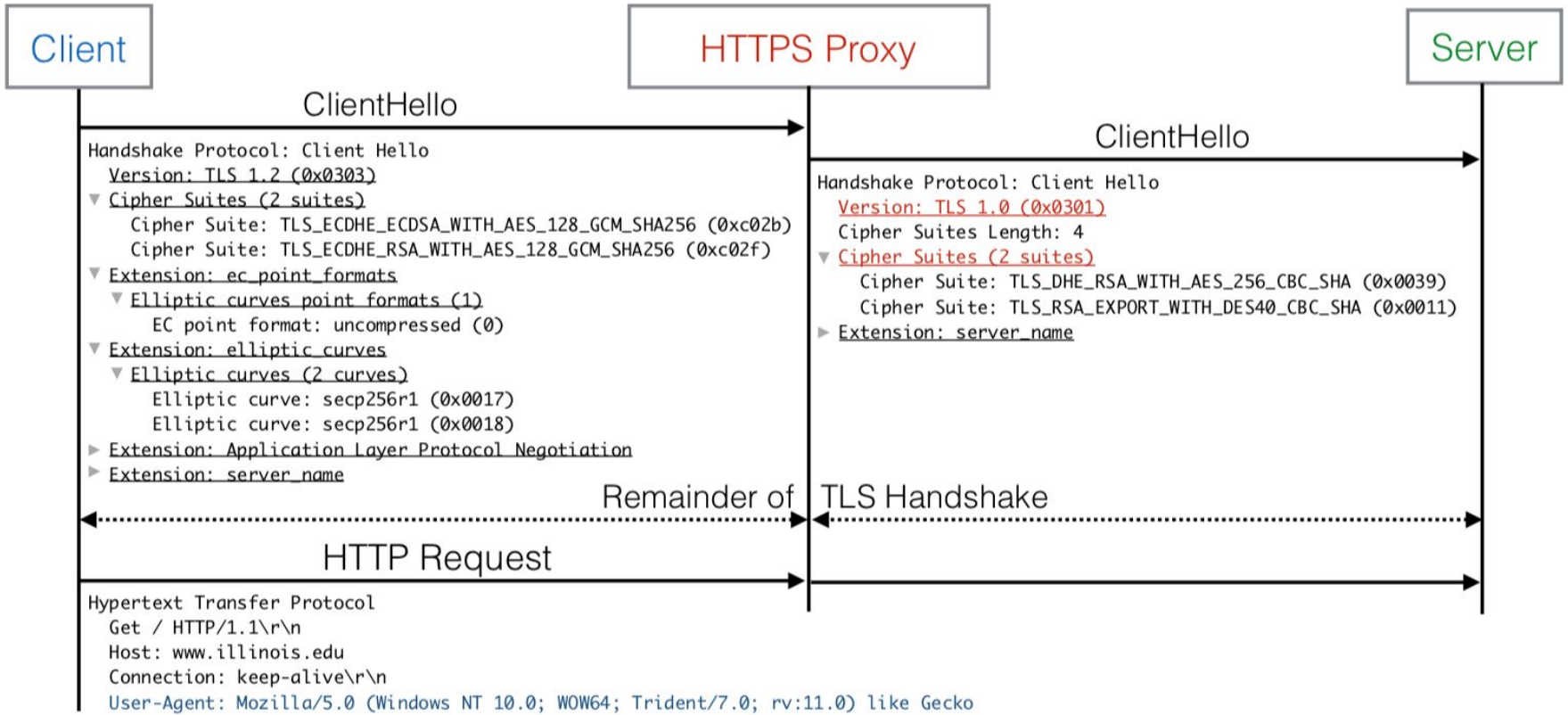


Key Insight

Identify a mismatch in connection details between HTTP User-Agent Header and TLS Client Hello



See if the Client Hello message of the advertised browser matches the Client Hello received by the server


Client
HTTPS Proxy
Server
ClientHello
Handshake Protocol: Client Hello
Version: TLS 1.2 (0x0303)
Cipher Suites (2 suites)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Extension: ec_point_formats
Elliptic curves point formats (1)
EC point format: uncompressed (0)
Extension: elliptic_curves
Elliptic curves (2 curves)
Elliptic curve: secp256r1 (0x0017)
Elliptic curve: secp256r1 (0x0018)
Extension: Application Layer Protocol Negotiation
Extension: server_name
ClientHello
Handshake Protocol: Client Hello
Version: TLS 1.0 (0x0301)
Cipher Suites Length: 4
Cipher Suites (2 suites)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Cipher Suite: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0011)
Extension: server_name
Remainder of TLS Handshake
HTTP Request
Hypertext Transfer Protocol
Get / HTTP/1.1\r\n
Host: www.illinois.edu
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Analyzing Browser Client Hellos




Goal:

- Develop a set of heuristics that will allow us to associate a Client Hello with a specific browser

Analyzing Browser Client Hellos: Firefox

- Most consistent across versions and OSes
- TLS parameters are pre-determined
- Uses its own TLS implementation (NSS)

Analyzing Browser Client Hellos: Chrome

- Alters behavior depending on platform
- Supports multiple ciphers/extensions per version
- Users can disable cipher suites
- Supports fewer extensions/ciphers than OpenSSL

Analyzing Browser Client Hellos: IE/Edge

- Allows arbitrary reordering, activation, and deactivation of cipher suites
- Uses Microsoft SChannel library

Analyzing Browser Client Hellos: Safari

- Uses Apple Secure Transport
- Enforces strict presence and ordering of cipher suites and extensions

Analyzing Interceptor Client Hellos

Goal:

- Develop a set of heuristics that will allow us to associate a Client Hello with a specific interception agent

avast

privdog

Superfish™
Search Visually

Measuring TLS Interception

Deploy heuristics at 3 vantage points and attempt to recognize intercepted traffic

- Firefox update servers
- E-commerce sites
- Cloudflare CDN

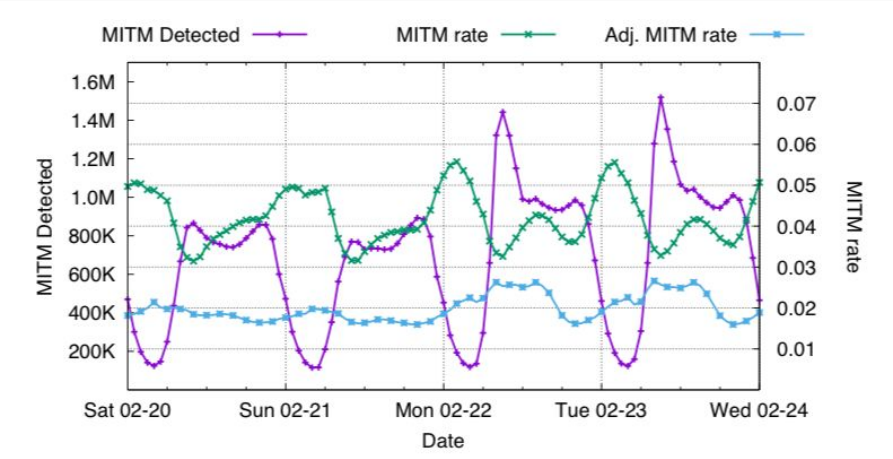
Results

Interception happens more than expected!

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%

Results: Firefox Update Server - **4% Interception**

- Lower interception rate likely due to Firefox's inbuilt certificate store
- Most common interception fingerprints belong to Bouncy Castle on Android 4.x and 5.x
  - Responsible for 47% of Firefox interceptions
  - Traffic originates from ASes belonging to mobile providers
- Peak interception rates are inversely proportional to peak traffic



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%

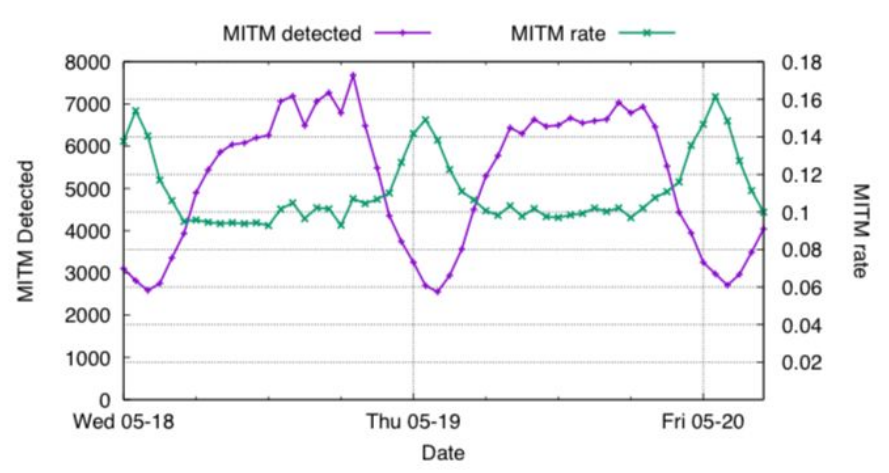
Results: E-commerce Sites - **6.2% Interception**

- Of the observed intercepted traffic
  - 58% attributed to antivirus, 35% to middleboxes, 1% to malware, 6% to misc.
  - 1.6% was identified due to HTTP proxy headers
- Exclude measurements from BlueCoat proxies that mask client User-Agent with generic string

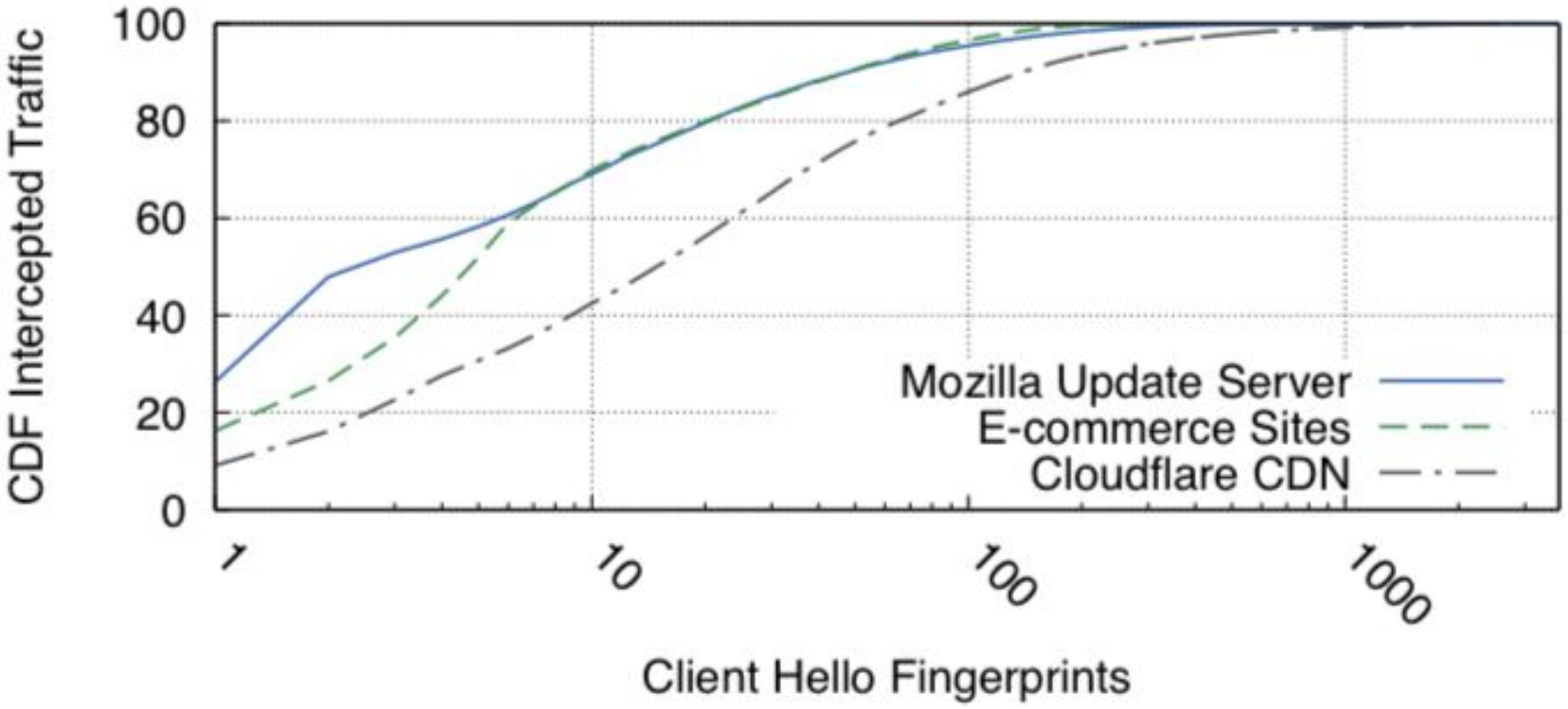
E-commerce Sites			
Browser	All Traffic	Intercepted	Of Intercepted
Chrome	40.3%	8.6%	56.2%
Explorer	16.8%	7.4%	19.6%
Firefox	13.5%	8.4%	18.2%
Safari	10.2%	2.1%	3.4%
Chromium	7.6%	0.1%	0.1%
Mobile Safari	7.6%	0.9%	1.1%
Other	4.0%	4.0%	2.4%
OS	All Traffic	Intercepted	Of Intercepted
Windows 7	23.3%	9.6%	56.6%
Windows 10	22.5%	9.3%	14.3%
iOS	17.3%	0.1%	1.1%
Mac OS	15.8%	2.1%	6.5%
Android	9.4%	1.0%	0.5%
Windows 8.1	6.9%	8.3%	15.8%
Other	4.8%	21.4%	15.2%

Results: Cloudflare - **10.9% Interception**

- Required a lot of scrubbing to remove false-positives
  - Focus on top 50 non-hosting ASes in the United States
- 4 of top 5 intercepted fingerprints belong to antivirus software
- Similar interception rate patterns to Firefox update servers



Cloudflare			
Browser	All Traffic	Intercepted	Of Intercepted
Chrome	36.2%	14.7%	48.8%
Mobile Safari	17.5%	1.9%	3.3%
Explorer	14.9%	15.6%	21.2%
Safari	8.9%	6.5%	5.3%
Firefox	8.5%	18.2%	14.2%
Mobile Chrome	8.4%	4.7%	3.6%
Other	5.6%	7.0%	3.6%
OS	All Traffic	Intercepted	Of Intercepted
Windows 7	23.9%	13.4%	29.2%
Windows 10	22.9%	13.1%	27.4%
iOS	17.5%	2.0%	3.2%
Mac OS	16.0%	6.6%	9.6%
Android	9.5%	4.8%	4.2%
Windows 8.1	4.9%	24.4%	11.0%
Other	5.3%	31.7%	15.4%


CDF Intercepted Traffic
100
80
60
40
20
0
1
10
100
1000
Client Hello Fingerprints
Mozilla Update Server
E-commerce Sites
Cloudflare CDN

Part 2:
Evaluating Security Impact

Establishing a Scale

Goal: Quantify how interception affects original connection security

- **A (Optimal)**
  - TLS connection is as secure as a modern web browser's
- **B (Suboptimal)**
  - Uses non-ideal settings but is not vulnerable to known attacks
- **C (Known attack)**
  - Connection is vulnerable to known TLS attacks or uses weak ciphers
- **F (Severely broken)**
  - Presents attack surface for a MITM attack or uses broken ciphers

Security Evaluations: Middleboxes

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

Security Evaluations: Client-side Interception

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

Impact of Interception

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: 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: 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%

Thoughts for the Future

- Is interception the way to go?
- Think about where TLS and HTTPS validation occurs
- Crypto libraries need to be secure by default
- Does antivirus need to intercept?
- Have security products that are actually secure
- Do not assume a client is behaving safely
- Network admins need to test for security

Industry Response

- Some took action
- Some ignored
- Some played difficult
- Some didn’t care

Takeaways

- Interception is more frequent than previously expected
- Connection security is often reduced
- We need to be more careful