

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: SPO1 – T09

HTTPS – Is Privacy Making Us LESS Secure?

Hal Lonas, CTO

Webroot
@hlonas

David Dufour, VP Engineering

Webroot
@DavidMDufour

5 March 2019

#RSAC

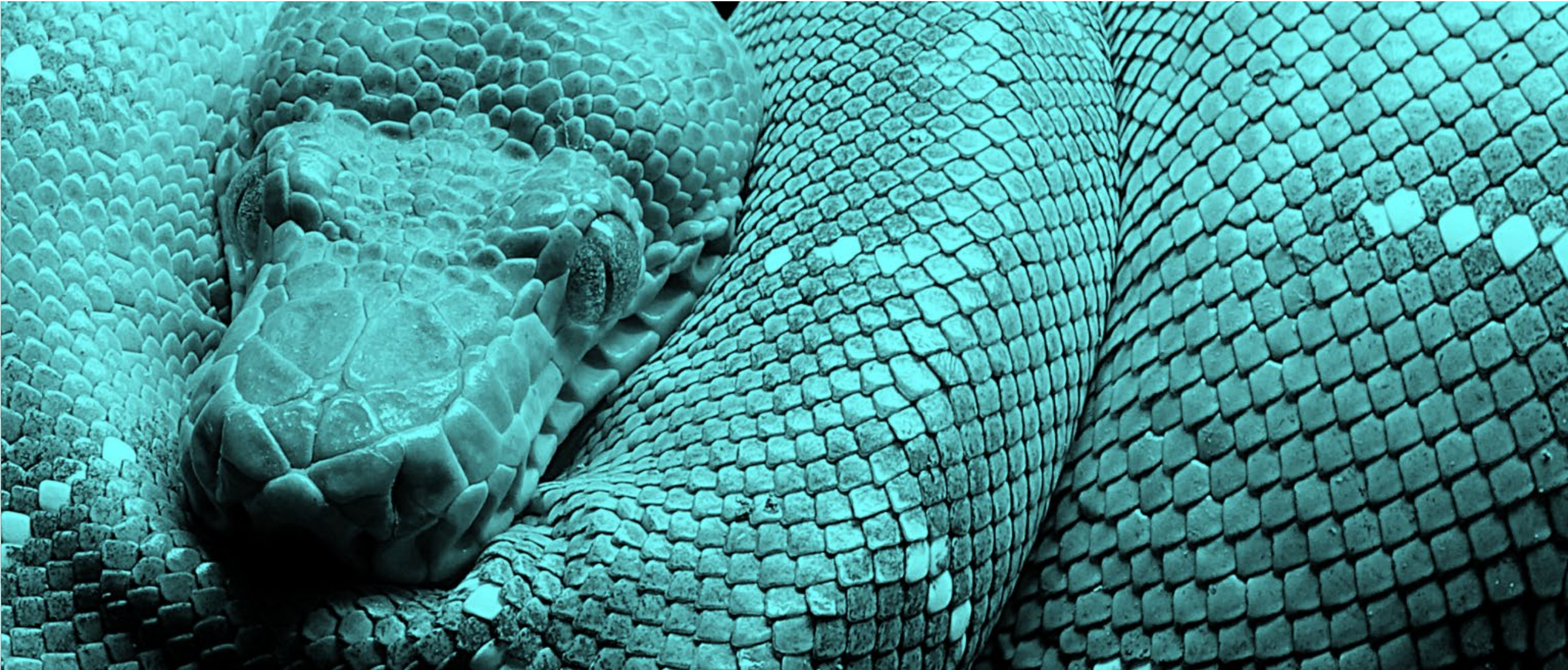
Introduction

PRIVACY vs. SECURITY

What's the Catch?



HTTP vs. HTTPS



Anatomy of a URL

scheme://subdomain.domain.com/file?argstring

microsoft.newdomain.ru/**whatcouldpossiblygowrong**/logintomyaccount

bankofa**r**nerica.com



Deceptive site ahead

Attackers on **www.bankofarnerica.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

[Learn more](#)

☐ Help improve Safe Browsing by sending some [system information and page content](#) to Google. [Privacy policy](#)

Details

Back to safety

HTTP vs. HTTPS

SSL Certificate




<https://www.ssl>

Free Website SSL Certificates



Free SSL Certificates & Free Wildcard SSL Certificates in Minutes

 Secure | <https://> enter your website to secure

Create Free SSL Certificate



100% Free Forever

Never pay for SSL again. Thanks to [Letsencrypt](#) the first non-profit CA.



Widely Trusted

Our free SSL certificates are trusted in 99.9% of all major browsers.



Enjoy SSL Benefits

- Protect user data & gain trust
- Improve Search Engine Ranking
- Prevent forms of website hacking

Over 2,000,000+ Free SSL Certificates Created

FBI Warning



TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

19 February 2019

PIN Number

20190219-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:

www.fbi.gov/contact-us/field

E-mail:

cywatch@fbi.gov

Phone:

1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP: GREEN**. The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

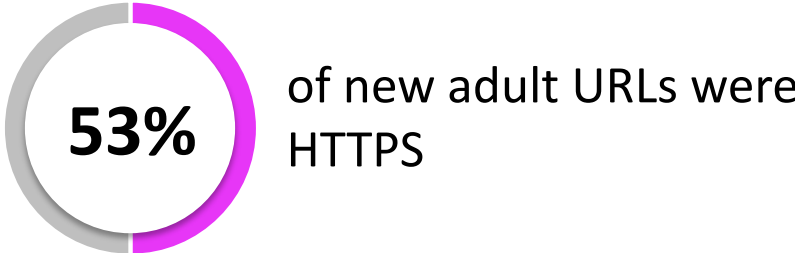
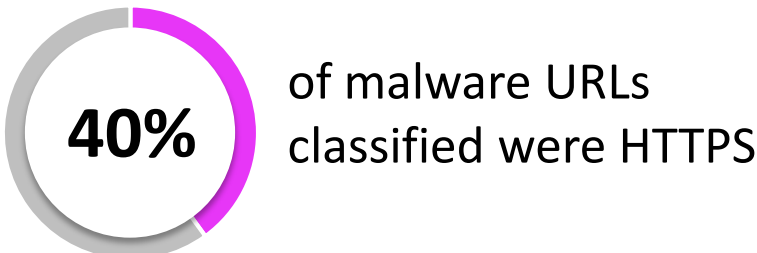
Cyber Actors Exploit Website Secure Certificates in Phishing Campaigns

Summary

The FBI assesses cyber threat actors are exploiting HTTPS in phishing campaigns, incorporating website certificates in their phishing, impacting potential victims, and increasing the chance of a successful compromise. The increase of HTTPS use in phishing campaigns is consistent with the global adoption of the website secure certificates protocol, which was primarily introduced to provide privacy, data integrity, and trusted web traffic while data is in transit. Cyber criminals have been observed abusing HTTPS in phishing campaigns by using mass emails masquerading as trustworthy entities in an attempt to acquire sensitive information for malicious purposes or to trick online users into opening a malicious file.

Bad URLs Using HTTPS

Over 11 months in 2018:



In September 2018:



Top HTTPS phishing sites:

- Wells Fargo
- DocuSign
- Microsoft
- Netflix
- Chase
- Apple
- PayPal
- Bank of America
- Dropbox
- Yahoo

*Targets with at least 500 phishing sites.

Exploiting HTTPS



HTTP vs. HTTPS

HTTP from maps.google.com

- Session starts in HTTP
- Note it's somewhat human (OK, nerd) readable

Capturing from Ethernet 2 (port 80)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|-----------------------|
| 1 | 0.000000 | 10.17.17.18 | 216.58.199.78 | TCP | 66 | 51907 → 80 [SYN] Seq= |
| 2 | 0.000477 | 10.17.17.18 | 216.58.199.78 | TCP | 66 | 51908 → 80 [SYN] Seq= |
| 3 | 0.147632 | 216.58.199.78 | 10.17.17.18 | TCP | 66 | 80 → 51907 [SYN, ACK] |
| 4 | 0.147713 | 10.17.17.18 | 216.58.199.78 | TCP | 54 | 51907 → 80 [ACK] Seq= |
| 5 | 0.148681 | 10.17.17.18 | 216.58.199.78 | HTTP | 1101 | GET / HTTP/1.1 |
| 6 | 0.148868 | 216.58.199.78 | 10.17.17.18 | TCP | 66 | 80 → 51908 [SYN, ACK] |
| 7 | 0.149014 | 10.17.17.18 | 216.58.199.78 | TCP | 54 | 51908 → 80 [ACK] Seq= |
| 8 | 0.297682 | 216.58.199.78 | 10.17.17.18 | TCP | 60 | 80 → 51907 [ACK] Seq= |
| 9 | 0.447068 | 216.58.199.78 | 10.17.17.18 | HTTP | 637 | HTTP/1.1 302 Found (1 |

> Frame 5: 1101 bytes on wire (8808 bits), 1101 bytes captured (8808 bits) on interface 0

> Ethernet II, Src: Dell_e0:c7:9b (e4:b9:7a:e0:c7:9b), Dst: 02:e0:52:7f:36:11 (02:e0:52:7f:36:11)

> Internet Protocol Version 4, Src: 10.17.17.18, Dst: 216.58.199.78

> Transmission Control Protocol, Src Port: 51907, Dst Port: 80, Seq: 1, Ack: 1, Len: 1047

> Hypertext Transfer Protocol

```

0000  02 e0 52 7f 36 11 e4 b9 7a e0 c7 9b 08 00 45 00  ..R.6...z....E.
0010  04 3f 39 81 40 00 80 06 02 8c 0a 11 11 12 d8 3a  ..9.@... ..:
0020  c7 4e ca c3 00 50 28 d4 9d 31 46 bb db f4 50 18  .N...P(. .1F...P.
0030  01 02 b1 82 00 00 47 45 54 20 2f 20 48 54 54 50  ....GET / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 70 73  /1.1..Host: maps
0050  2e 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 43 6f 6e  .google.com..Con
0060  6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c  nection: keep-al
0070  69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73  ive..Upgrade: Ins
0080  65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20  ecure-Requests:
0090  31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d  1..User-Agent: M
00a0  6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64  ozilla/5 .0 (Wind
00b0  6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e  ows NT 1 0.0; Win
00c0  36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65  64; x64) AppleWe
00d0  62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54  bKit/537 .36 (KHT
00e0  4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20  ML, like Gecko)
00f0  43 68 72 6f 6d 65 2f 37 32 2e 30 2e 33 36 32 36  Chrome/7 2.0.3626
0100  2e 31 30 39 20 53 61 66 61 72 69 2f 35 33 37 2e  .109 Safari/537.
0110  33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74  36..Accept: text
0120  2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f  /html,application
0130  6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c  n/xhtml+xml,appl
0140  69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e  ication/xml;q=0.
0150  39 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61  9,image/webp,ima
  
```

HTTP vs. HTTPS

HTTPS (TLS) from maps.google.com

- Search switches to HTTPS
- Note it's NOT readable

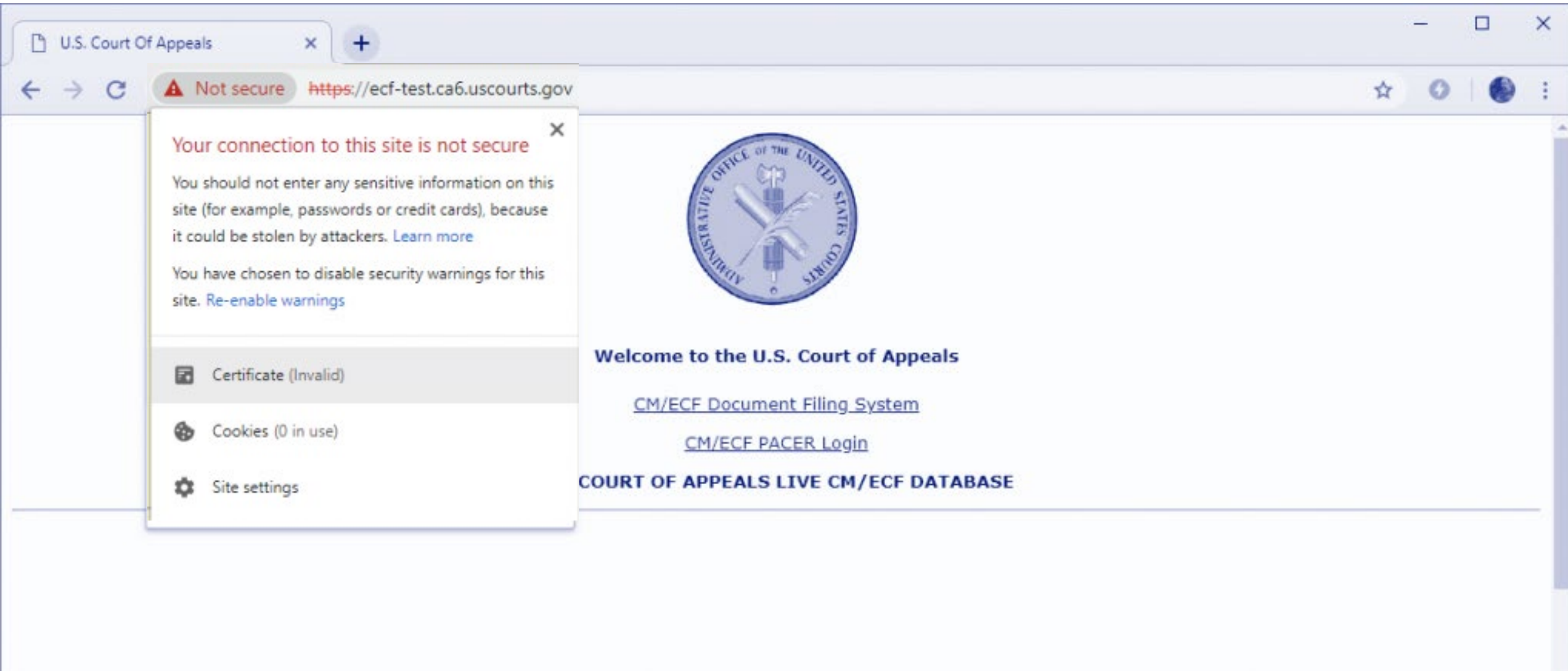
Wireshark packet capture showing an HTTPS (TLS) connection. The interface is *Ethernet 2 (port 443). The packet list shows the following details:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------|----------------|----------|--------|---|
| 16 | 1.181810 | 10.17.17.18 | 162.125.34.129 | TCP | 54 | 51473 → 443 [ACK] Seq=6863 Ack=601 Win=256 Len=0 |
| 17 | 1.194193 | 162.125.2.3 | 10.17.17.18 | TCP | 66 | 443 → 51962 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MS |
| 18 | 1.194251 | 10.17.17.18 | 162.125.2.3 | TCP | 54 | 51962 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0 |
| 19 | 1.194762 | 10.17.17.18 | 162.125.2.3 | TLSv1.2 | 237 | Client Hello |
| 20 | 1.210438 | 162.125.2.3 | 10.17.17.18 | TCP | 60 | 443 → 51962 [ACK] Seq=1 Ack=184 Win=30208 Len=0 |
| 21 | 1.212452 | 162.125.2.3 | 10.17.17.18 | TLSv1.2 | 1514 | Server Hello |
| 22 | 1.212453 | 162.125.2.3 | 10.17.17.18 | TCP | 1514 | 443 → 51962 [ACK] Seq=1461 Ack=184 Win=30208 Len=1460 |
| 23 | 1.212456 | 162.125.2.3 | 10.17.17.18 | TLSv1.2 | 553 | Certificate, Server Key Exchange, Server Hello Done |
| 24 | 1.212533 | 10.17.17.18 | 162.125.2.3 | TCP | 54 | 51962 → 443 [ACK] Seq=184 Ack=3420 Win=66048 Len=0 |
| 25 | 1.214557 | 10.17.17.18 | 162.125.2.3 | TLSv1.2 | 180 | Client Key Exchange, Change Cipher Spec, Encrypted Ha |
| 26 | 1.230075 | 162.125.2.3 | 10.17.17.18 | TLSv1.2 | 296 | New Session Ticket, Change Cipher Spec, Encrypted Han |
| 27 | 1.231153 | 10.17.17.18 | 162.125.2.3 | TLSv1.2 | 574 | Application Data |
| 28 | 1.231342 | 10.17.17.18 | 162.125.2.3 | TCP | 1494 | 51962 → 443 [ACK] Seq=830 Ack=3662 Win=65792 Len=1440 |

Frame 27: 574 bytes on wire (4592 bits), 574 bytes captured (4592 bits) on interface 0
 Ethernet II, Src: Dell_e0:c7:9b (e4:b9:7a:e0:c7:9b), Dst: 02:e0:52:7f:36:11 (02:e0:52:7f:36:11)
 Internet Protocol Version 4, Src: 10.17.17.18, Dst: 162.125.2.3
 Transmission Control Protocol, Src Port: 51962, Dst Port: 443, Seq: 310, Ack: 3662, Len: 520
 Secure Sockets Layer

The packet details show the TLSv1.2 handshake and the first data frame (Application Data) which is encrypted and not readable.

Bypassing Browser Warnings



HTTPS: Then and Now



RSA®Conference2019

Analogies from Other Tech / Industry



Export Controls, Encrypted Communications



RSA®Conference2019

Making HTTPS as Safe as Possible



APPLY: What to Do



APPLY: Privacy vs. Security



RSA[®]Conference2019

Questions?

Hal Lonas @hlonas

David Dufour @DavidMDufour