Tunnelling

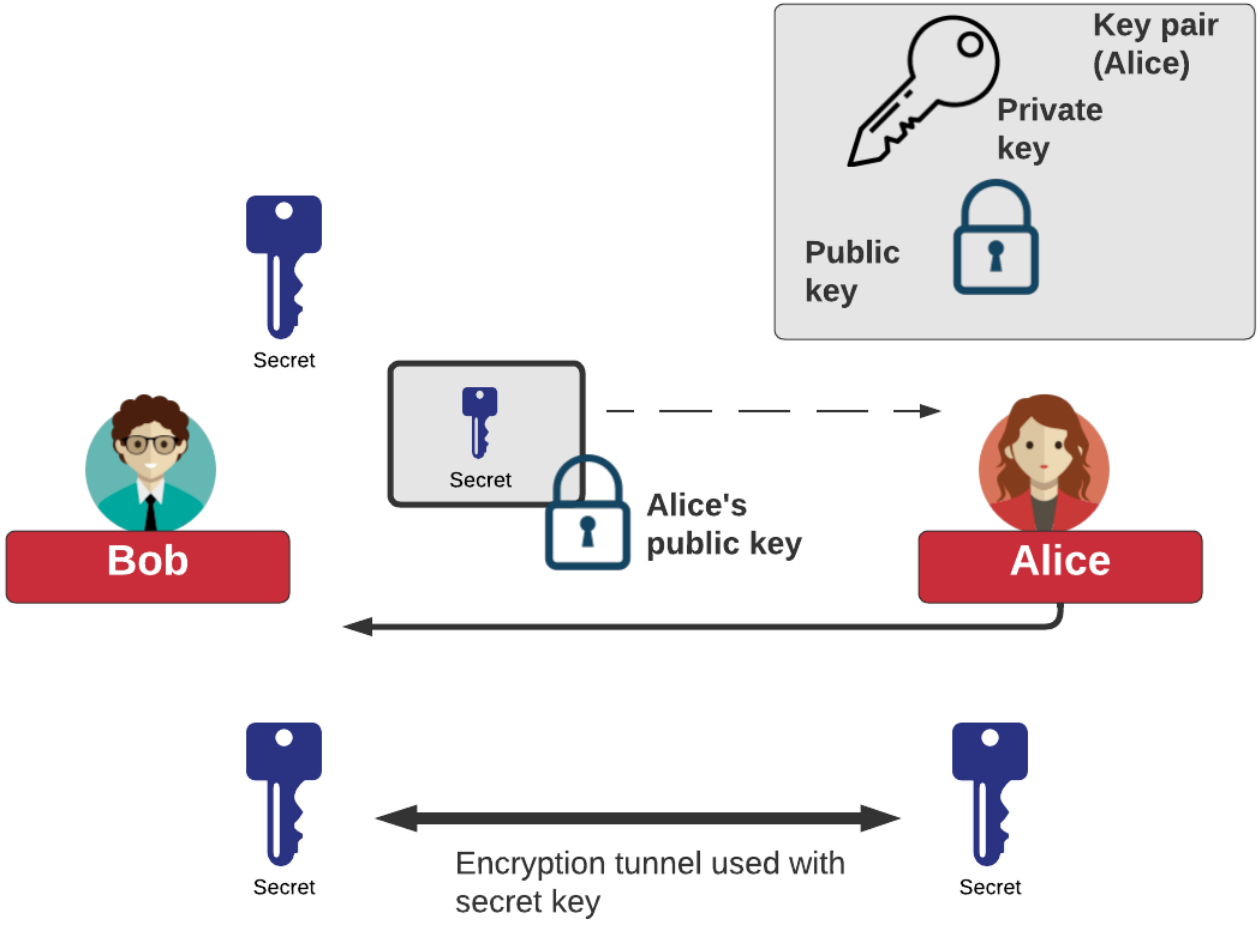
Basics.
SSL/TLS.
VPNs.

Tunnelling

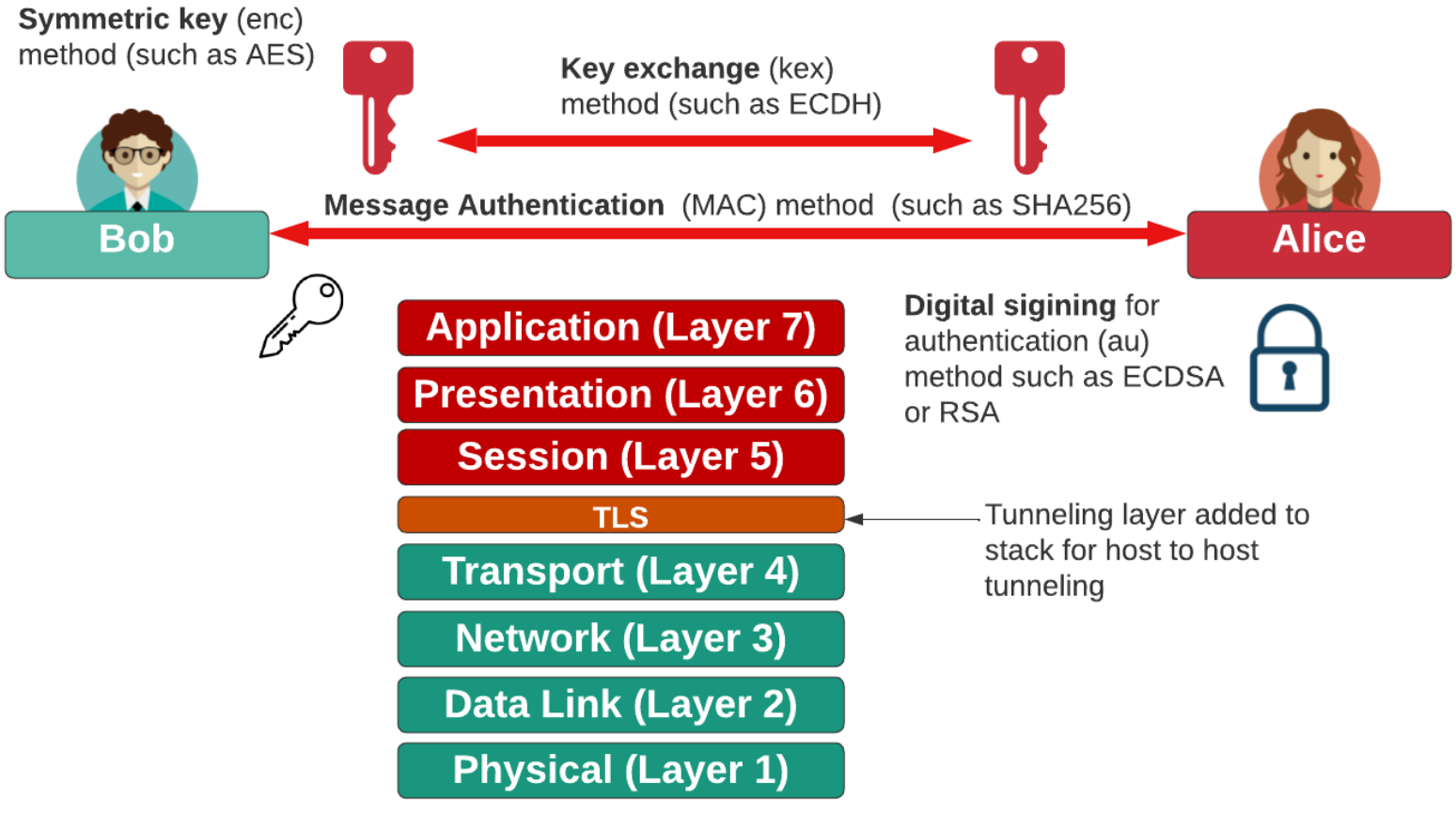
Basics.
SSL/TLS.
VPNs.

No	Date	Subject	Lab
2	13 Sept 2024	1. Introduction [Link] 2. Intrusion Detection Systems [Link]	Network Security Lab 1
3	26 Sept 2024	3. Network Security (Risks and Models) [Link]	Network Security Lab 2
4	3 Oct 2024	4. Ciphers and Fundamentals [Link]	AWS Security and Server Infrastructure Lab 3
5	10 Oct 2024	5. Secret Key 6. Hashing [Link]	Symmetric Key and Hashing Lab 4
6	17 Oct 2024	7. Public Key [Link] 8. Key Exchange [Link]	Public Key and Key Exchange Lab 5
7	24 Oct 2024	Reading week/Revision session	Reading week/Cipher Challenge
8	31 Oct 2024	9. Digital Certificates	Certificates Lab 6
9	7 Nov 2024	Test 1 here	
10	14 Nov 2024	10 Network Forensics here	Network Forensics Lab 7
11	21 Nov 2024	11. Splunk here	Splunk Lab Lab 8
12	28 Nov 2024	13. Tunnelling Here	Tunnelling Lab 9
13	5 Dec 2024	14. Blockchain and Cryptocurrencies here	Blockchain Lab.
14	12 Dec 2024		
15	19 Dec 2024	Hand-in: TBC [Here]	

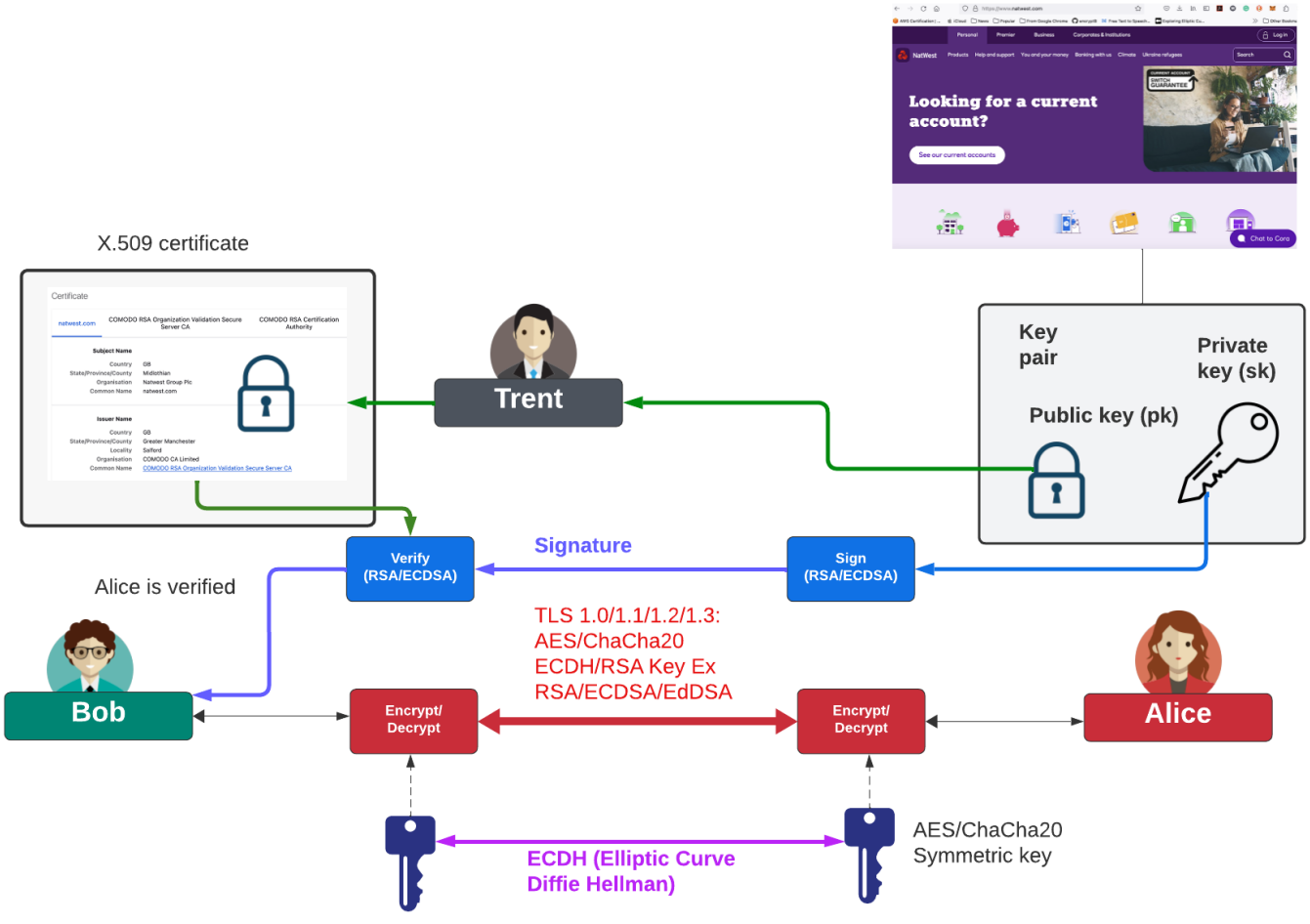
Tunnelling


Key pair
(Alice)
Private
key
Public
key
Secret
Secret
Alice's
public key
Bob
Alice
Secret
Encryption tunnel used with
secret key
Secret

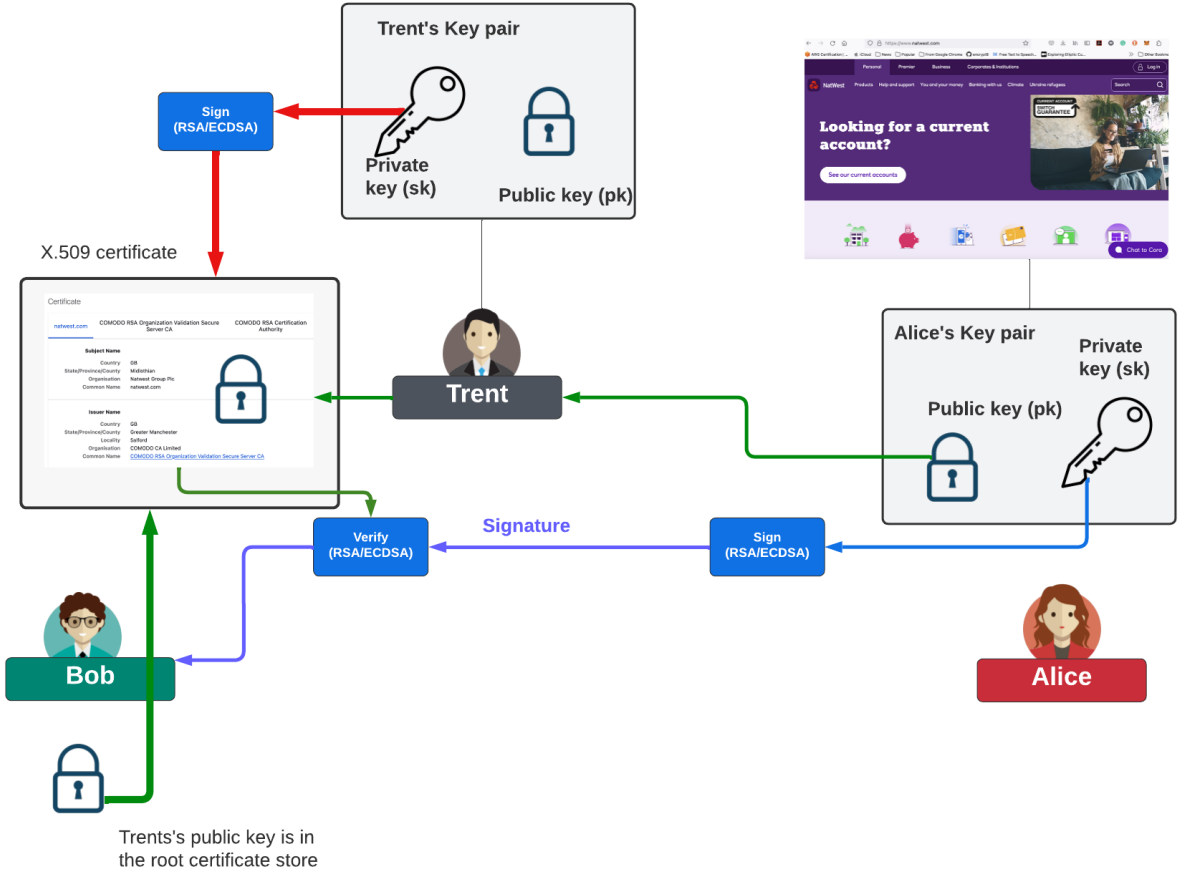
Tunnelling


Symmetric key (enc) method (such as AES)
Key exchange (kex) method (such as ECDH)
Bob
Message Authentication (MAC) method (such as SHA256)
Alice
Application (Layer 7)
Presentation (Layer 6)
Session (Layer 5)
TLS
Transport (Layer 4)
Network (Layer 3)
Data Link (Layer 2)
Physical (Layer 1)
Digital sigining for authentication (au) method such as ECDSA or RSA
Tunneling layer added to stack for host to host tunneling

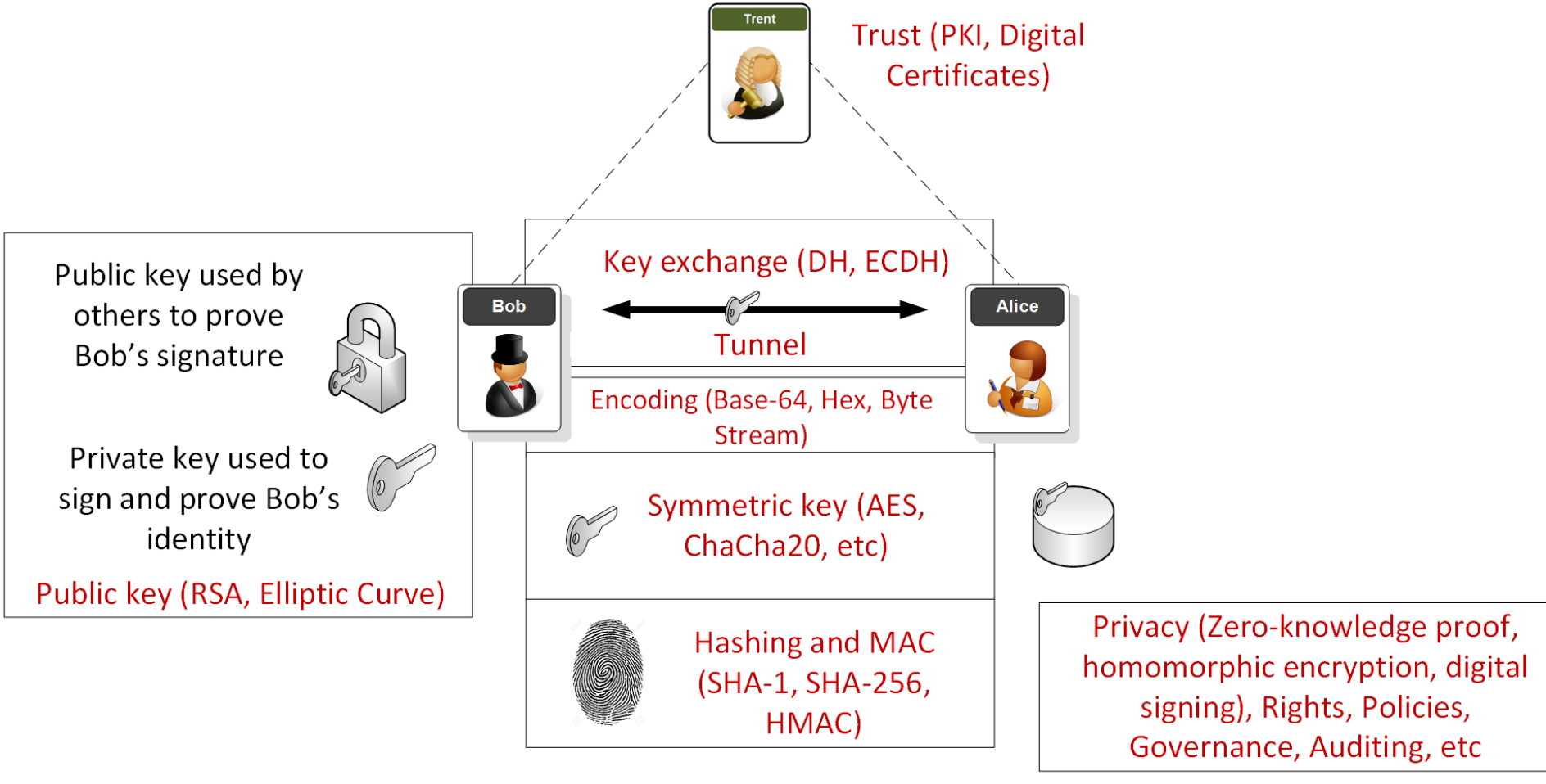
Tunnelling


X.509 certificate
Certificate
natwest.com
COMODO RSA Organization Validation Secure Server CA
COMODO RSA Certification Authority
Subject Name
Country GB
State/Province/County Midlothian
Organisation Natwest Group Plc
Common Name natwest.com
Issuer Name
Country GB
State/Province/County Greater Manchester
Locality Salford
Organisation COMODO CA Limited
Common Name COMODO RSA Organization Validation Secure Server CA
Looking for a current account?
See our current accounts
Chat to Cora
Trent
Key pair
Private key (sk)
Public key (pk)
Verify (RSA/ECDSA)
Signature
Sign (RSA/ECDSA)
Alice is verified
TLS 1.0/1.1/1.2/1.3:
AES/ChaCha20
ECDH/RSA Key Ex
RSA/ECDSA/EdDSA
Bob
Encrypt/ Decrypt
Encrypt/ Decrypt
Alice
ECDH (Elliptic Curve Diffie Hellman)
AES/ChaCha20 Symmetric key

Tunnelling


Trent's Key pair
Private key (sk)
Public key (pk)
Sign (RSA/ECDSA)
X.509 certificate
Trent
Alice's Key pair
Private key (sk)
Public key (pk)
Looking for a current account?
Verify (RSA/ECDSA)
Signature
Sign (RSA/ECDSA)
Bob
Alice
Trents's public key is in the root certificate store

Overview


Trent
Trust (PKI, Digital Certificates)
Public key used by others to prove Bob's signature
Private key used to sign and prove Bob's identity
Public key (RSA, Elliptic Curve)
Bob
Alice
Key exchange (DH, ECDH)
Tunnel
Encoding (Base-64, Hex, Byte Stream)
Symmetric key (AES, ChaCha20, etc)
Hashing and MAC (SHA-1, SHA-256, HMAC)
Privacy (Zero-knowledge proof, homomorphic encryption, digital signing), Rights, Policies, Governance, Auditing, etc

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: Submit

Do not show the results on the boards

Recently Seen	
www.yaklink.com	
billiardunderground.org	
ha.homenetwork.biz	
srv-web02.imageware.ch	
evisa.gov.ge	
www.theleveluppleague.com	Err
sportclinic.it	
edpnet.net	
bungholio.ch	
trade.eurocarparts.com	

Recent Best	
forachange.co.il	A+
auth.touchsurgery.com	A+
www.chegaga.de	A+
ps-metro-fsd-mm-10-0-fsd-mm- ...	A
callback.datinglab.net	A
www.rivanov.nl	A
www.ioffice.kz	B
afficheo.com	B
popuplabor-bw.de	B
mobile.imageware.ch	B

Recent Worst	
chepai.alltobid.com	F
mail.frende.no	F
mitpfa.dk	F
ow-analytics.com	F
mft.imageware.ch	T
selfservice.kvk.nl	F
www.migrosmagazin.ch	F
www.vkekk.lt	F
www.preiswerte-werbeartikel. ...	F
bbapp.toddmorton.net	T

Security Headers

Sponsored by netsparker

Home About

Scan your site now

enter address here

Scan

Hide results Follow redirects

Grand Totals

A+	657,797
A	4,792,956
B	1,573,217
C	789,919
D	2,710,689
E	1,788,375
F	11,569,900
R	2,313,267
Total	26,196,120

Recent Scans

twitter.com	A
lifar.ciotor.se	F
www.infodaymedia.c...	E
content-marketing-...	F
foxpd.bestwomepri....	F
deonath.com	F
www.ijamat.com	F
www.google.co.jp	D
activatemomentum.c...	F

Hall of Fame

www.le-systems.com	A
gltorsystem.com	A+
msdapps-dev.hamilt...	A+
twitter.com	A
fated.org	A+
www.fbhackpass.com	A+
dwpocrusapi-test.a...	A
dwpocranthemapi-te...	A
dev.hamiltonapps.r...	A+

Hall of Shame

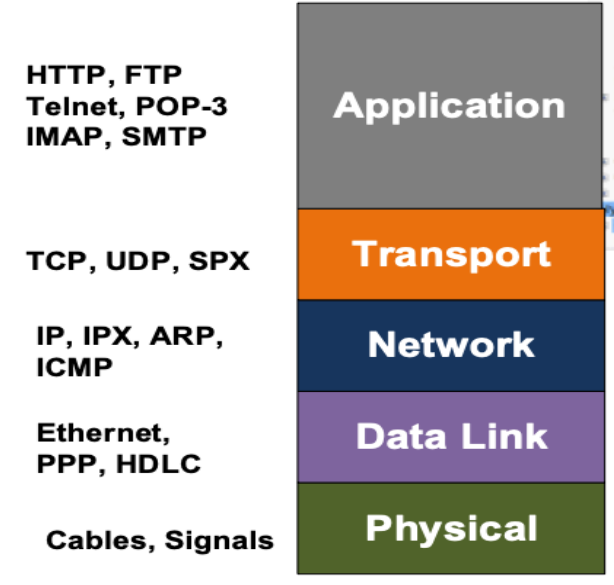
lifar.ciotor.se	F
content-marketing-...	F
foxpd.bestwomepri....	F
deonath.com	F
www.ijamat.com	F
activatemomentum.c...	F
www.janter.co.nz	F
guardiansafetybarr...	F
www.finderguru.com	F

Tunnelling

Basics.
TLS.
VPNs.

Tunnelling

Basics.
TLS.
VPNs.

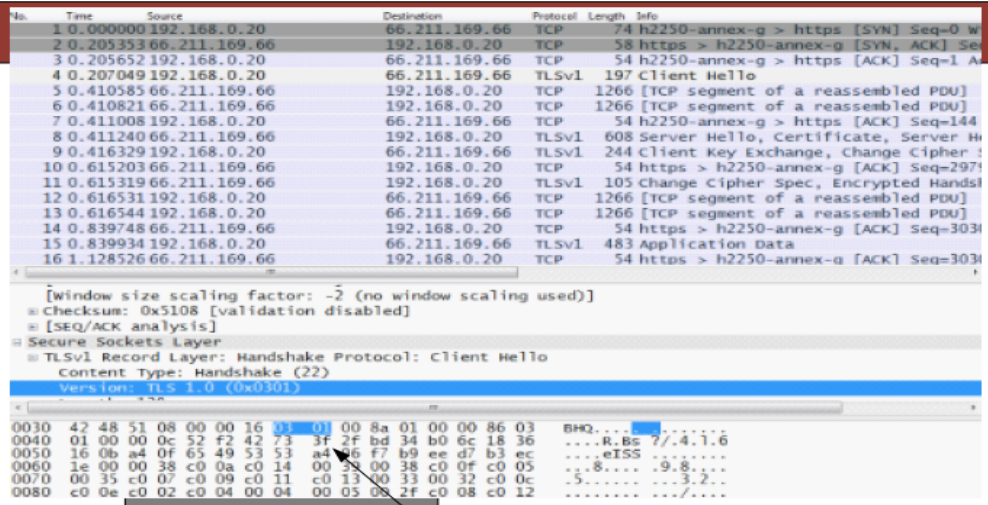


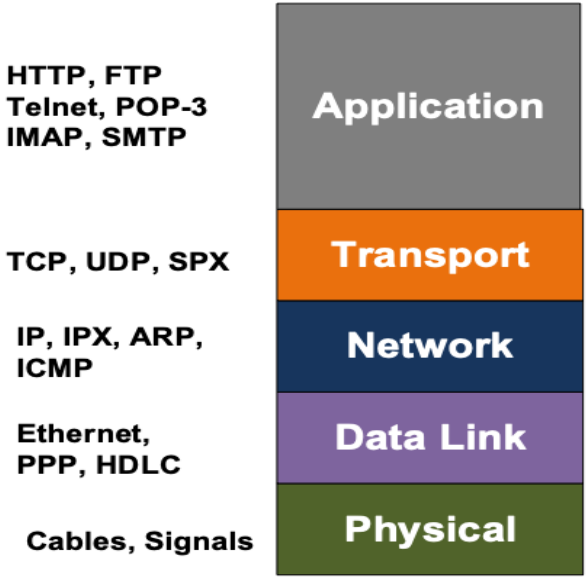

```
    4 0.000602 192.168.75.132      192.168.75.1    TCP      78 http > mgcp-gateway [SYN, ACK] Seq=0 Ack=1 W
    5 0.000681 192.168.75.1        192.168.75.132  TCP      66 mgcp-gateway > http [ACK] Seq=1 Ack=1 Win=66
    6 0.000835 192.168.75.1        192.168.75.132  HTTP    475 GET / HTTP/1.1
    7 0.055477 192.168.75.132      192.168.75.1    TCP    1514 [TCP segment of a reassembled PDU]
⊞ Destination: Vmware_0f:71:a3 (00:0c:29:0f:71:a3)
⊞ Source: Vmware_c0:00:08 (00:50:56:c0:00:08)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132 (192.168.75.132)
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 461
  Identification: 0x011e (286)
⊞ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
⊞ Header checksum: 0xe036 [validation disabled]
  Source: 192.168.75.1 (192.168.75.1)
  Destination: 192.168.75.132 (192.168.75.132)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: mgcp-gateway (2427), Dst Port: http (80), Seq: 1, Ack: 1, Len: 409
  Source port: mgcp-gateway (2427)
  Destination port: http (80)
  [Stream index: 0]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 410    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
⊞ Flags: 0x018 (PSH, ACK)
  Window size value: 16652
  [Calculated window size: 66608]
  [Window size scaling factor: 4]
⊞ Checksum: 0xf834 [validation disabled]
⊞ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
⊞ [SEQ/ACK analysis]
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  User-Agent: Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.15 Version/10.01\r\n
```

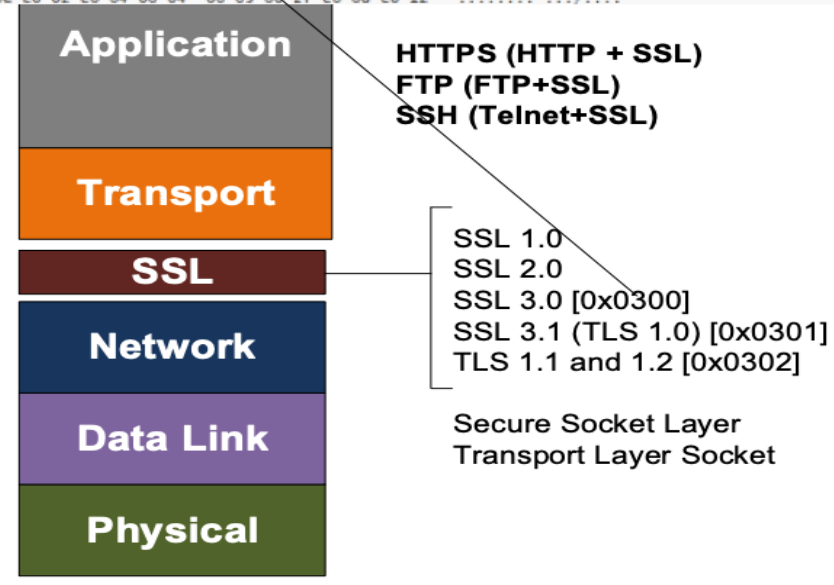
Author: Prof Bill Buchanan

Ports

HTTP	80	HTTPs	443
TELNET	23	SSH	22
SMTP	25	SMTPs	465
POP-3	110	POP-3s	995







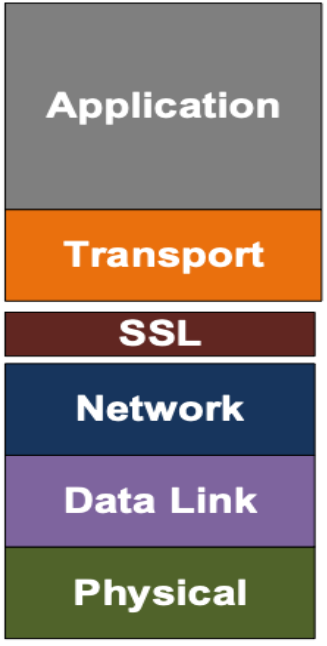
Author: Prof Bill Buchanan

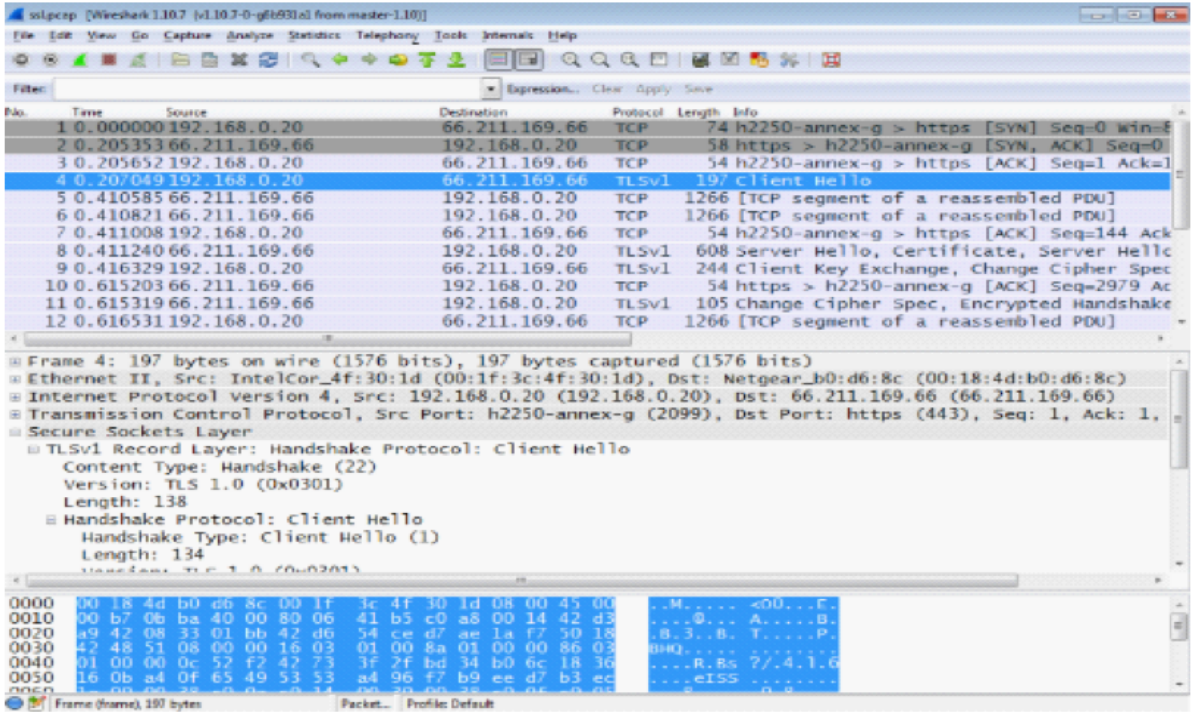
TCP [SYN] to Port 443

TCP [SYN,ACK] from Port 443

TCP [ACK] to Port 443

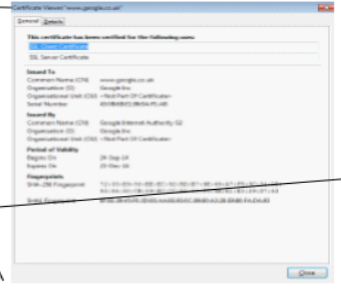
Client Hello (Start of Handshake)





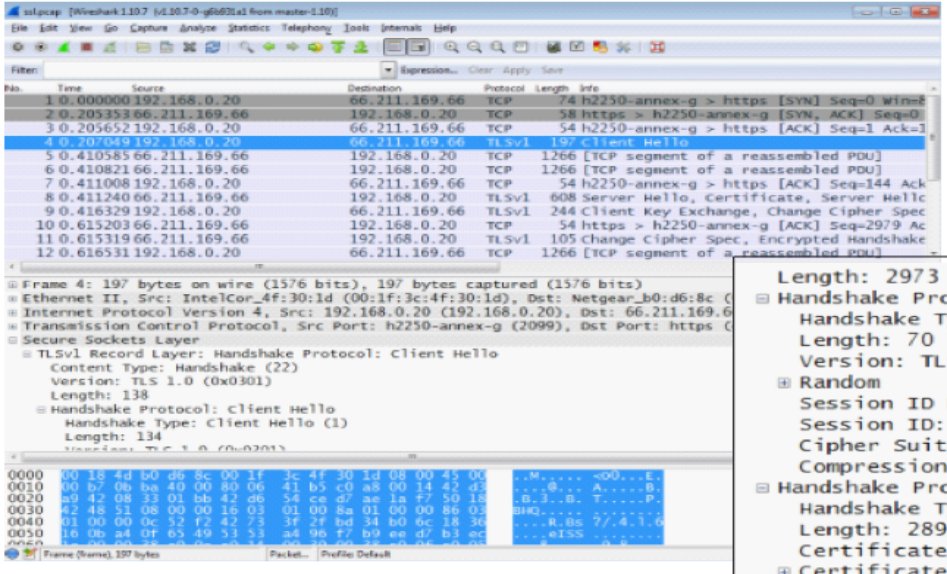
Author: Prof Bill Buchanan

Client Hello



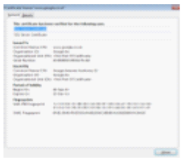
Server Hello

```
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 138
Handshake Protocol: Client Hello
  Handshake Type: Client Hello (1)
  Length: 134
  Version: TLS 1.0 (0x0301)
  Random
  Session ID Length: 0
  Cipher Suites Length: 56
  Cipher Suites (28 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
```




```
Length: 2973
Handshake Protocol: Server Hello
  Handshake Type: Server Hello (2)
  Length: 70
  Version: TLS 1.0 (0x0301)
  Random
  Session ID Length: 32
  Session ID: ed2175399c8f02d916e58afdbbd46317564a98a1d985632a...
  Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
  Compression Method: null (0)
Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 2891
  Certificates Length: 2888
  Certificates (2888 bytes)
```

Author: Prof Bill Buchanan



192.168.0.20

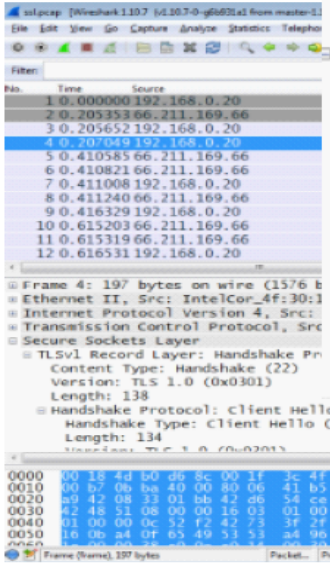
Client Hello

66.211.169.66

Public key

Server Hello

Client Key Exchange

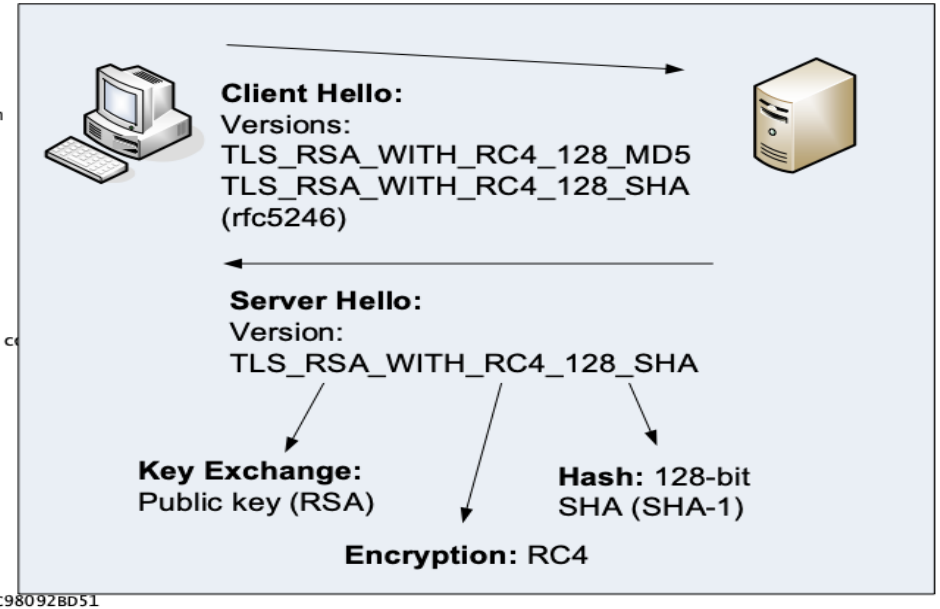


```
  [Window size scaling factor: -2 (no window scaling used)]
⊞ Checksum: 0x2a30 [validation disabled]
⊞ [SEQ/ACK analysis]
Secure Sockets Layer
⊟ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 134
  ⊟ Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 130
    ⊟ RSA Encrypted PreMaster Secret
        Encrypted PreMaster length: 128
        Encrypted PreMaster: 07d26b83aa8129bd8c48462627a1d3f67f34e2745959fce2...
⊟ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.0 (0x0301)
```

Author: Prof Bill Buchanan

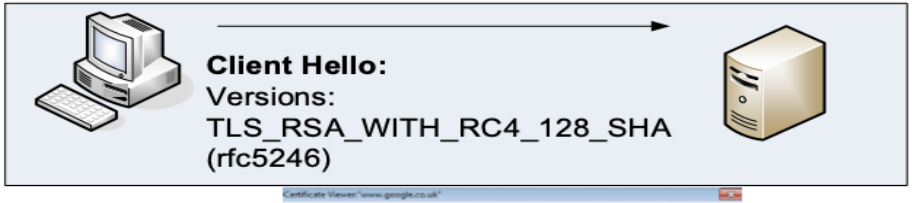
```
billbuchanan@Bills-MacBook-Pro:~$ openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEdjCCA16gAwIBAgIISVyALWN+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkGA1UE
---
SOx4I5L0D0jZYqKfJuImGcFwdIETqOEpCmkhJfGNHjVdzC/h/T61TmaY
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.c
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
---
SSL handshake has read 3719 bytes and written 446 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 9D92CEC32FA9F86C6D902081EE186C4FC68234FFF7B903D6621A86C98092BD51
    Session-ID-ctx:
    Master-Key:
B8A14DB1D3021E80B53F30EA94D2EEA155A995B926879B08E3D971EB16873D16F62929899E2FA368D374716DB14A412
B
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - fa 8d cb 50 53 3d 99 c8-b4 11 20 0c ca 53 e9 bd   ...PS=.... ..S..
    0010 - f8 8e 15 14 ec 82 c1 56-ab d9 9b 36 c2 56 b0 db   .......V...6.V..
    0020 - 2b d4 07 56 a5 02 ac 1f-34 fa 72 21 fd 7c ba 97   +..V....4.r!.|..
    0030 - 2a ae e9 20 04 ef 8a e5-a0 57 28 3a c7 67 04 ac   *.. .....W(:.g..
    0040 - 7d 14 bf b0 6d 96 9f cb-eb 0c 0a 40 07 5f a6 84   }...m......@._..
    0050 - e2 3b 98 0b e7 f4 b1 e1-04 be 15 6b 36 a5 57 b3   .;.........k6.W.
    0060 - 11 98 f2 f4 20 fe b5 7f-6b 10 4e 7a f9 b5 6d 02   .... ...k.Nz..m.
    0070 - 30 ec 07 e6 f0 c0 49 81-31 6b 30 f9 b0 d3 c4 25   0.....I.1k0....%
    0080 - 62 f3 92 33 e8 25 cc 22-32 84 54 e6 0e 76 b1 45   b..3.%."2.T..v.E
    0090 - 3a 60 83 cf 1b b0 97 7d-05 03 47 20 29 12 d9 8d   :`.....}..G )...
    00a0 - 6f 5a b4 f2                                       oZ..

    Start Time: 1413136351
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
```




```
TLS_RSA_WITH_AES_256_CBC_SHA256
Key: RSA Enc: AES_256_CBC  Hash: SHA256
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
Key ex: DH_DSS Enc: 3DES_EDE_CBC Hash: SHA
```

Author: Prof Bill Buchanan

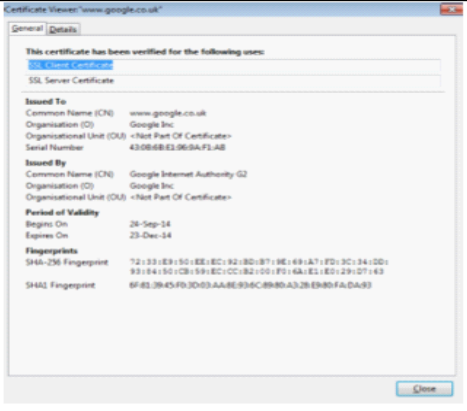


Server Hello:
Version:
TLS_RSA_WITH_RC4_128_SHA

Key Exchange:
Public key (RSA)

Encryption: RC4

Hash: 128-bit
SHA (SHA-1)



Session key

Public key

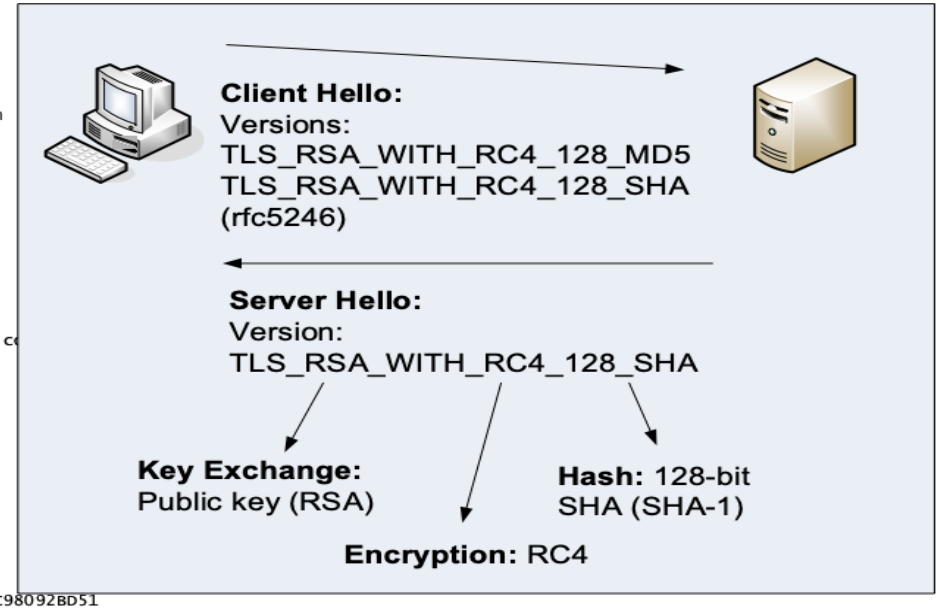
Private key

Tunnel created (RC4, Hash: SHA-1)

Author: Prof Bill Buchanan

```
billbuchanan@Bills-MacBook-Pro:~$ openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEdjCCA16gAwIBAgIISVyALWN+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkGA1UE
---
SOx4I5L0D0jZYqKfJuImGcFwdIETqOEpCmkhJfGNHjVdzC/h/T61TmaY
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.c
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
---
SSL handshake has read 3719 bytes and written 446 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 9D92CEC32FA9F86C6D902081EE186C4FC68234FFF7B903D6621A86C98092BD51
    Session-ID-ctx:
    Master-Key:
B8A14DB1D3021E80B53F30EA94D2EEA155A995B926879B08E3D971EB16873D16F62929899E2FA368D374716DB14A412
B
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - fa 8d cb 50 53 3d 99 c8-b4 11 20 0c ca 53 e9 bd   ...PS=.... ..S..
    0010 - f8 8e 15 14 ec 82 c1 56-ab d9 9b 36 c2 56 b0 db   .......V...6.V..
    0020 - 2b d4 07 56 a5 02 ac 1f-34 fa 72 21 fd 7c ba 97   +..V....4.r!.|..
    0030 - 2a ae e9 20 04 ef 8a e5-a0 57 28 3a c7 67 04 ac   *.. .....W(:.g..
    0040 - 7d 14 bf b0 6d 96 9f cb-eb 0c 0a 40 07 5f a6 84   }...m......@._..
    0050 - e2 3b 98 0b e7 f4 b1 e1-04 be 15 6b 36 a5 57 b3   .;.........k6.W.
    0060 - 11 98 f2 f4 20 fe b5 7f-6b 10 4e 7a f9 b5 6d 02   .... ...k.Nz..m.
    0070 - 30 ec 07 e6 f0 c0 49 81-31 6b 30 f9 b0 d3 c4 25   0.....I.1k0....%
    0080 - 62 f3 92 33 e8 25 cc 22-32 84 54 e6 0e 76 b1 45   b..3.%."2.T..v.E
    0090 - 3a 60 83 cf 1b b0 97 7d-05 03 47 20 29 12 d9 8d   :`.....}..G )...
    00a0 - 6f 5a b4 f2                                       oZ..

    Start Time: 1413136351
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
```




```
TLS_RSA_WITH_AES_256_CBC_SHA256
Key: RSA Enc: AES_256_CBC  Hash: SHA256
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
Key ex: DH_DSS Enc: 3DES_EDE_CBC Hash: SHA
```

Author: Prof Bill Buchanan

Internet Engineering Task Force (IETF)
Request for Comments: 8446
Obsoletes: 5077, 5246, 6961
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

E. Rescorla
Mozilla

August 2018

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8446.

Internet Engineering Task Force (IETF)
Request for Comments: 8446
Obsoletes: 5077, 5246, 6961
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

E. Rescorla
Mozilla
August 2018

The Transport Layer Security (TLS)

Abstract

This document specifies version 1.3 of t
(TLS) protocol. TLS allows client/serve
over the Internet in a way that is desig
tampering, and message forgery.

This document updates RFCs 5705 and 6066
5246, and 6961. This document also spec
TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track docu

This document is a product of the Interr
(IETF). It represents the consensus of
received public review and has been appr
Internet Engineering Steering Group (IES
Internet Standards is available in Secti

Information about the current status of
and how to provide feedback on it may be
https://www.rfc-editor.org/info/rfc8446.

Replay Attacks on Zero Round-Trip Time: The Case of the TLS 1.3 Handshake Candidates

Marc Fischlin Felix Günther

Cryptoplexity, Technische Universität Darmstadt, Germany
marc.fischlin@cryptoplexity.de, guenther@cs.tu-darmstadt.de

February 2, 2017

Abstract. We investigate security of key exchange protocols supporting so-called zero round-trip time (0-RTT), enabling a client to establish a fresh provisional key without interaction, based only on cryptographic material obtained in previous connections. This key can then be already used to protect early application data, transmitted to the server before both parties interact further to switch to fully secure keys. Two recent prominent examples supporting such 0-RTT modes are Google's QUIC protocol and the latest drafts for the upcoming TLS version 1.3.

We are especially interested in the question how replay attacks, enabled through the lack of contribution from the server, affect security in the 0-RTT case. Whereas the first proposal of QUIC uses state on the server side to thwart such attacks, the latest version of QUIC and TLS 1.3 rather accept them as inevitable. We analyze what this means for the key secrecy of both the preshared-key-based 0-RTT handshake in draft-14 of TLS 1.3 as well as the Diffie–Hellman-based 0-RTT handshake in TLS 1.3 draft-12. As part of this we extend previous security models to capture such cases, also shedding light on the limitations and options for 0-RTT security under replay attacks.

Replayable 0-RTT data presents a number of security threats to TLS-using applications, unless those applications are specifically engineered to be safe under replay (minimally, this means idempotent, but in many cases may also require other stronger conditions, such as constant-time response). Potential attacks include:

- Duplication of actions which cause side effects (e.g., purchasing an item or transferring money) to be duplicated, thus harming the site or the user.

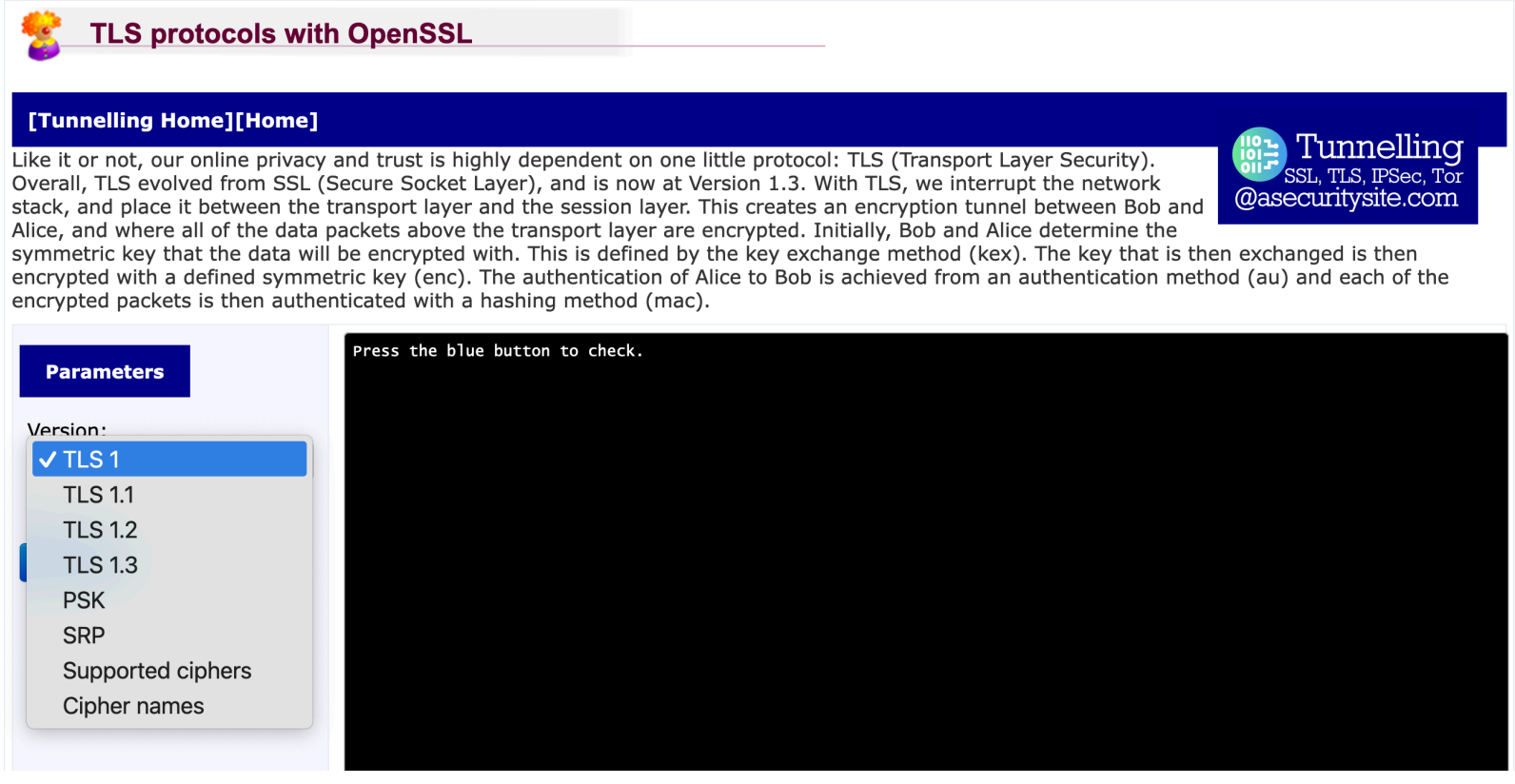
- Attackers can store and replay 0-RTT messages in order to re-order them with respect to other messages (e.g., moving a delete to after a create).

- Exploiting cache timing behavior to discover the content of 0-RTT messages by replaying a 0-RTT message to a different cache node and then using a separate connection to measure request latency, to see if the two requests address the same resource.

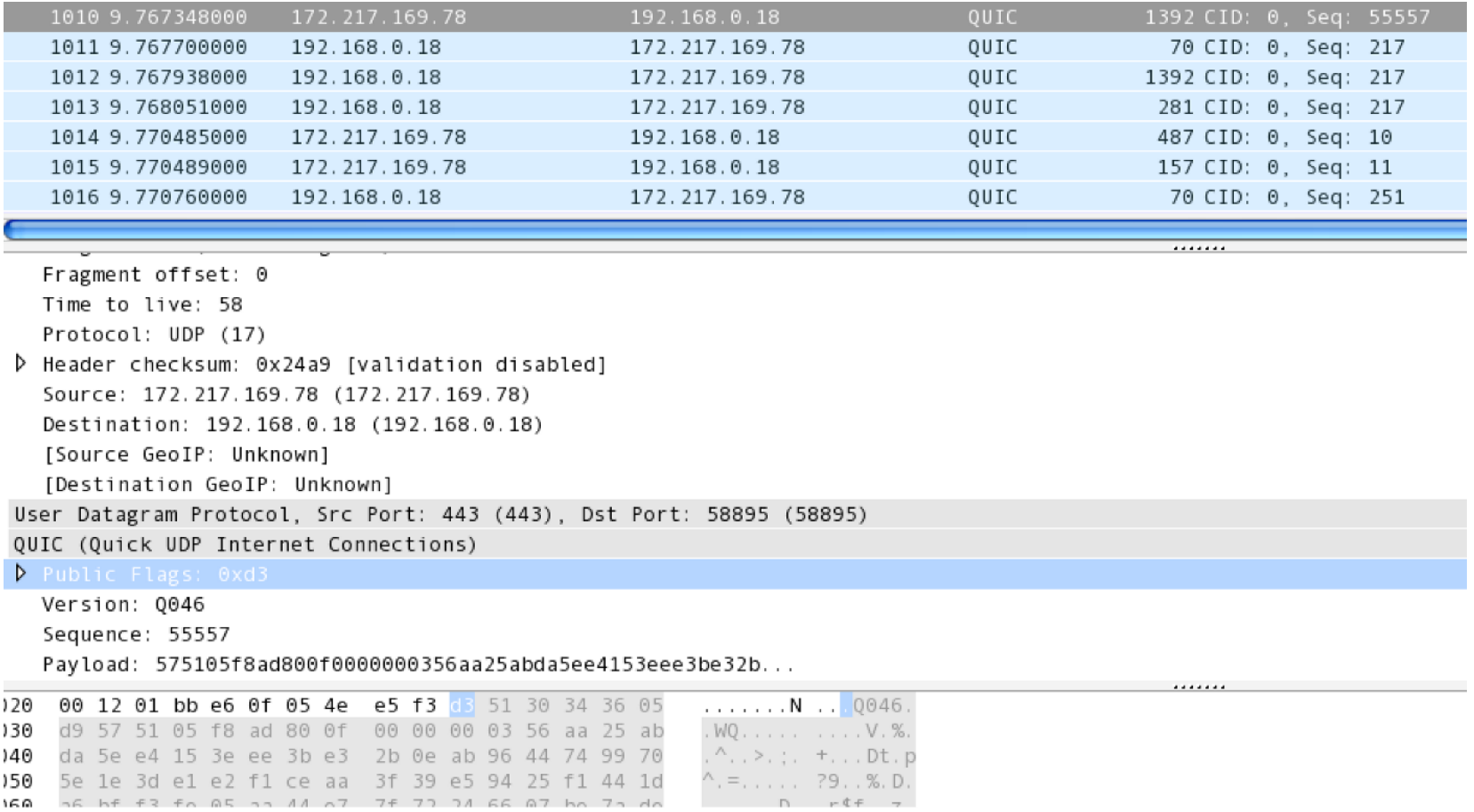
and how to provide feedback on it may be
https://www.rfc-editor.org/info/rfc8446.

inevitable. We analyze what this means for the key secrecy of both the preshared-key-based 0-RTT handshake in draft-14 of TLS 1.3 as well as the Diffie–Hellman-based 0-RTT handshake in TLS 1.3 draft-12. As part of this we extend previous security models to capture such cases, also shedding light on the limitations and options for 0-RTT security under replay attacks.

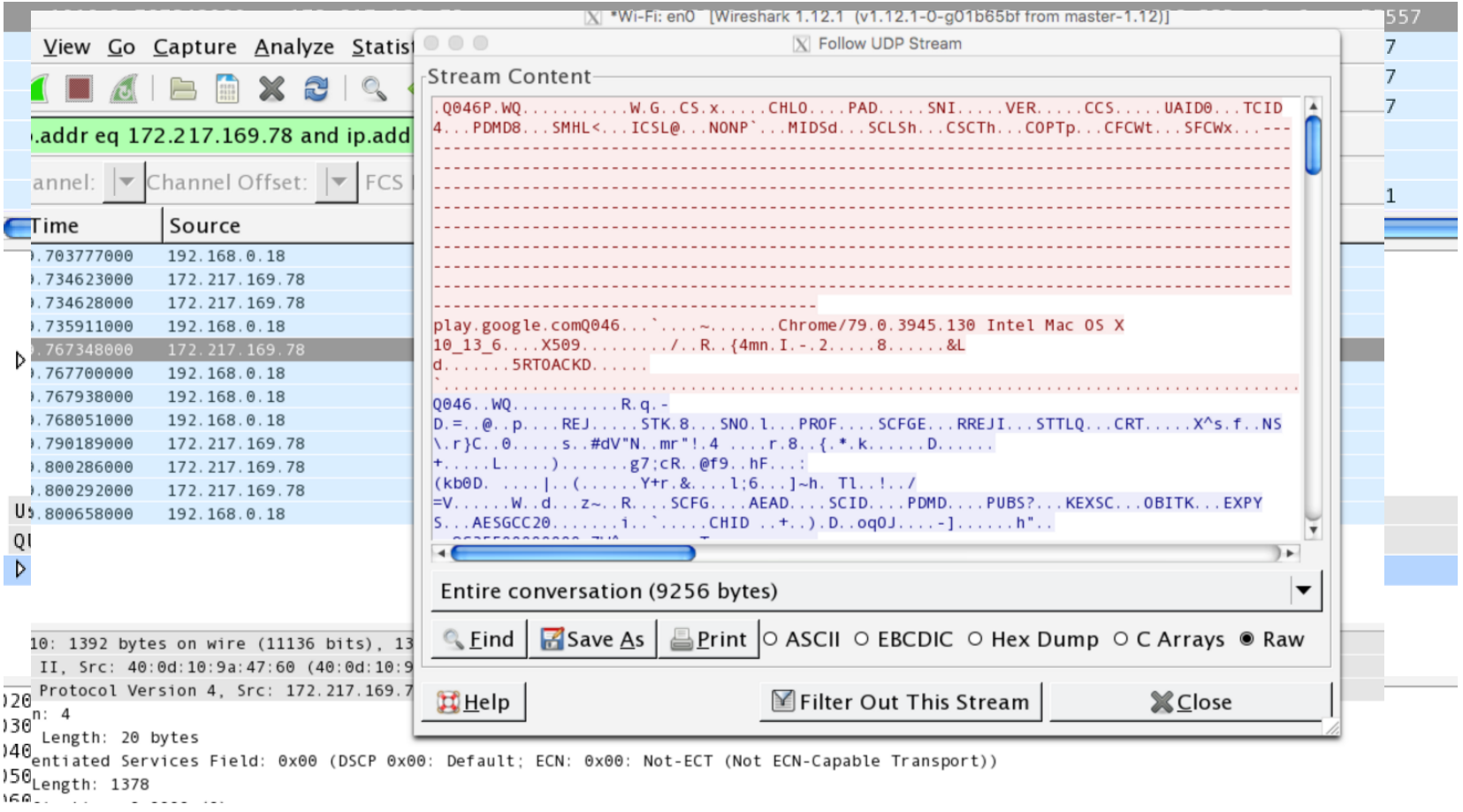
TLS Versions



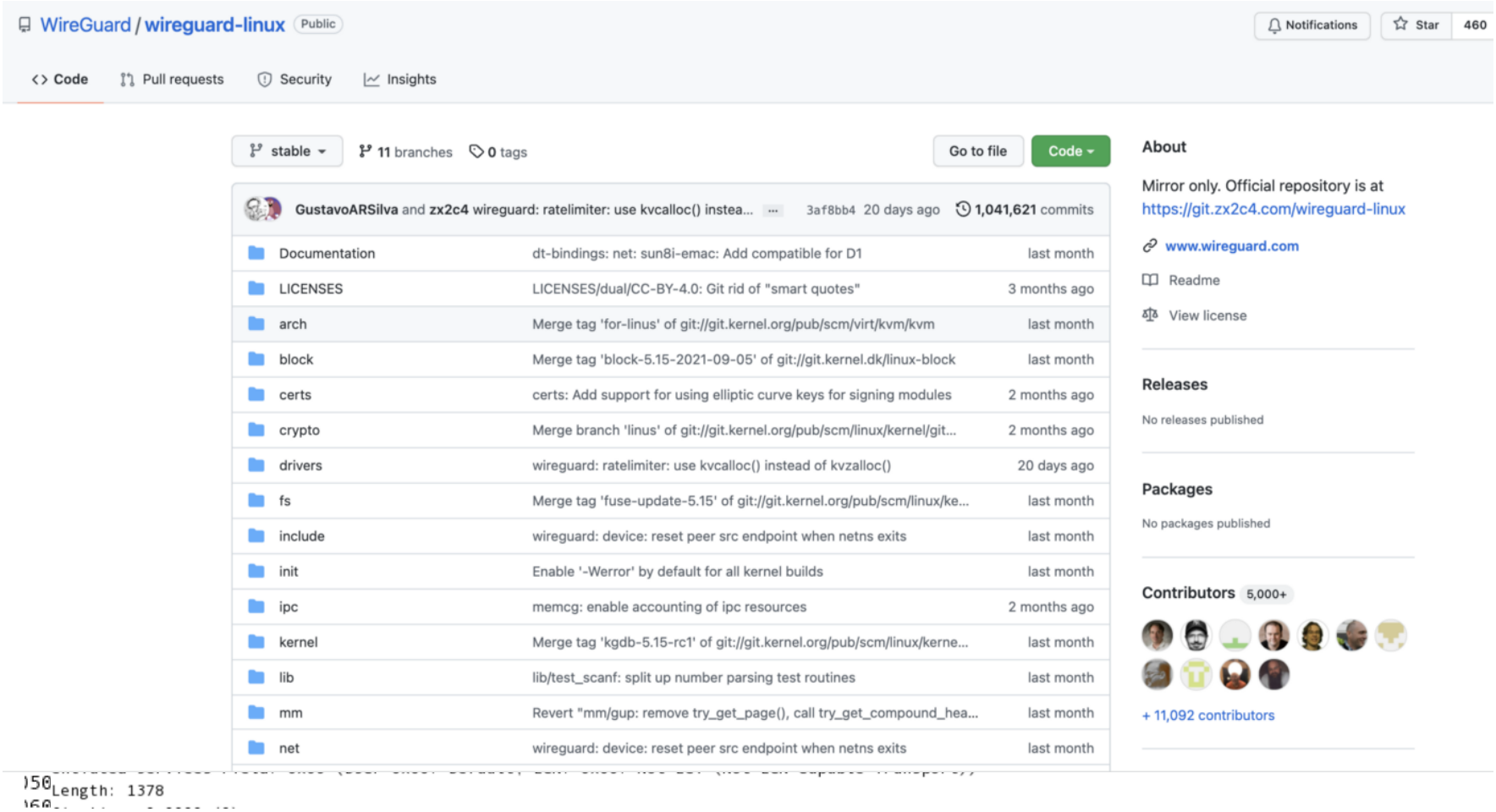
QUIC and WireGuard



QUIC and WireGuard



QUIC and WireGuard




```
050Length: 1378
```

Tunnelling

Basics.
TLS.
VPNs.

Tunnelling

Basics.
TLS.
VPNs.