



wireshark抓包分析HTTPS



白帽青年
不以物喜，不以己悲

关注他

8 人赞同了该文章

一、名词解释

TLS

安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成： TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。

记录协议主要负责使用对称密码对消息进行加密；握手协议分为握手协议，密码规格变更协议、警告协议和应用数据协议4个部分



RTT

RTT(Round Trip Time)：一个tcp连接的往返时间，即数据发送时刻到接收到确认的时刻的差值；

密码套件

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

TLS：指使用的协议是TLS

ECDHE：密钥交换算法

ECDSA：签名或验证算法

AES_128_GCM：对称加密算法。对称密钥加密算法是AES，强度即密钥长度为128位，GCM是工作模式，AES是块密码，也就是对输入的纯文本用固定长度的块来进行加密，加密后的每个块按再顺序发送，最后按类似的方式来

SHA256: 签名哈希算法



Diffie Hellman 密钥协商算法

使用Diffie Hellman算法进行TLS密钥交换具有优势。客户端和服务端都为每个新会话生成一个新密钥对。一旦计算出预主密钥，将立即删除客户端和服务器的私钥。这意味着私钥永远不会被窃取，确保完美的前向保密。

如果使用RSA，则客户端将如上所述通过其自己计算预主密钥，使用服务器的公钥（RSA公钥）对其进行加密，并通过客户端密钥交换消息将其发送回服务器。然后，服务器可以使用其私钥解密它。

二、TLS 握手原理：

Client Hello

1.1、Client Hello 报文：客户端对加密算法的支持度不同，因此需要向服务端发送客户端支持的加密套件（Cipher Suite），同时还要生成一个随机数同时保存在客户端和发送给服务

Server Hello

2.1、Server Hello 报文：服务端收到 Client Hello 之后，生成一个随机数同时保存在服务端和发送给客户端

2.2、Server Certificate 报文：向客户端发送 CA 认证的数字证书，用来鉴别服务端身份信息

2.3、Server Hello Done 报文：表示服务端宣告第一阶段的客户端服务端握手协商结束

2.4、可选：Certificate Request 报文：必要情况下，要求客户端发送证书验证身份

2.5、可选：Server Key Exchange 报文：仅当服务器提供的证书不足以允许客户端交换预主密钥时，才会发送此消息

Client Finish

3.1、Client Key Exchange 报文：客户端收到 CA 数字证书并通过验证，获取服务端公钥。Client Key Exchange 报文包括有一个随机数，这个随机数被称为 Pre-master key/secret；一个表示随后的信息使用双方协商好的加密方法和密钥发送的通知

3.2、Client Cipher Spec 报文：该报文通知服务端，此后的通信都将使用协商好的加密算法计算对称密钥进行加密通信（也就是使用两个随机数以及第三个 Pre-master key/secret 随机数一起算出一个对称密钥 session key/secret）

3.3、Finished 报文：该报文包括连接至此的所有报文的校验值，使用服务端公钥进行加密

3.4、可选：Client Certificate 报文：如果服务端请求，客户端需要发送 CA 数字证书

3.5、可选：Certificate Verify 报文：服务端如果要求 CA 数字证书，那么需要通过 HASH 算法计算一个服务端发送来的信息摘要

Server Finish

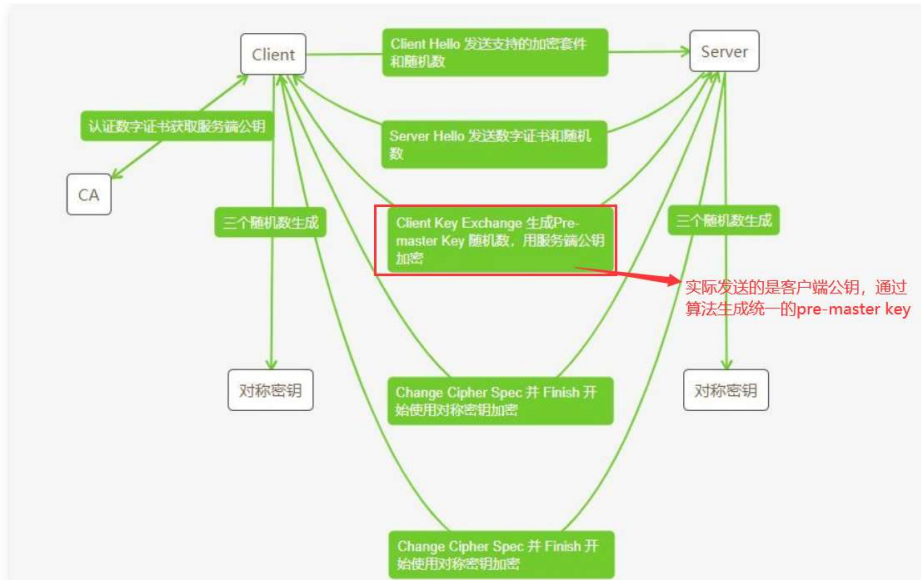
4.1、服务端最后对客户端发送过来的 Finished 报文使用服务端私钥进行解密校验

4.2、Client Cipher Spec 报文：报文通知服务端，此后的通信都将使用协商好的加密算法计算对称密钥 session key/secret 进行加密通信

4.3、Finished 报文：标志 TLS 连接建立成功

TLS 握手成功，此后通过对称密

大致图解：



三、TLS 1.2 握手过程抓包：

No.	Time	Source	Destination	Protocol	Length	Info
1024	2020-12-06 17:53:16.000	172.19.68.69	172.18.132.150	TCP	66	4919 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1025	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TCP	66	443 → 4919 [SYN, ACK] Seq=0 Ack=1 Win=16066 Len=0 MSS=1460 SACK_PERM=1 WS=2
1027	2020-12-06 17:53:16.000	172.19.68.69	172.18.132.150	TCP	54	4919 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1028	2020-12-06 17:53:16.000	172.19.68.69	172.18.132.150	TLSv1.2	571	Client Hello
1031	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TCP	60	443 → 4919 [ACK] Seq=1 Ack=518 Win=15544 Len=0
1032	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TLSv1.2	1514	Server Hello
1033	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TCP	1514	443 → 4919 [PSH, ACK] Seq=1461 Ack=518 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
1034	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TCP	1230	443 → 4919 [PSH, ACK] Seq=2921 Ack=518 Win=15544 Len=1176 [TCP segment of a reassembled PDU]
1035	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TCP	54	4919 → 443 [ACK] Seq=518 Ack=2921 Win=26266 Len=0
1036	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TCP	1514	443 → 4919 [ACK] Seq=4097 Ack=518 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
1037	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TLSv1.2	1004	Certificate, Server Key Exchange, Server Hello Done
1038	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TCP	54	4919 → 443 [ACK] Seq=518 Ack=5557 Win=26266 Len=0
1040	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TLSv1.2	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1041	2020-12-06 17:53:16.000	172.18.132.150	172.19.68.69	TCP	528	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1044	2020-12-06 17:53:16.000	172.19.68.69	172.18.132.150	TCP	54	4919 → 443 [ACK] Seq=644 Ack=6781 Win=261376 Len=0
1067	2020-12-06 17:53:18.000	172.19.68.69	172.18.132.150	TLSv1.2	617	Application Data
1068	2020-12-06 17:53:18.000	172.18.132.150	172.19.68.69	TCP	60	443 → 4919 [ACK] Seq=6781 Ack=1207 Win=14924 Len=0
1069	2020-12-06 17:53:18.000	172.18.132.150	172.19.68.69	TCP	1514	443 → 4919 [ACK] Seq=6781 Ack=1207 Win=14924 Len=1460 [TCP segment of a reassembled PDU]
1070	2020-12-06 17:53:18.000	172.18.132.150	172.19.68.69	TLSv1.2	83	Application Data

Client Hello:

客户端发送32位随机数、所支持的加密套件、session id（用于协商会话关闭后，重新打开时需不需要再次握手）、extension（添加一些拓展功能，tls1.3使用）；compress（支持的压缩方法）

Frame 571: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{4FE48297-00C4-4203-A9BF-EE183CB8AAC}, id 0	
Ethernet II, Src: HuaweiE_65:43:1b (54:ee:75:65:43:1b), Dst: HuaweiE_33:ae:24 (f8:9b:ef:33:ae:24)	
Internet Protocol Version 4, Src: 172.19.68.69, Dst: 172.18.132.150	
Transmission Control Protocol, Src Port: 4919, Dst Port: 443, Seq: 1, Ack: 1, Len: 517	
Transport Layer Security	
TLSv1.2 Record Layer: Handshake Protocol: Client Hello	
Content Type: Handshake (22)	
Version: TLS 1.0 (0x0301)	
Length: 512	
Handshake Protocol: Client Hello (1)	
Length: 508	
Version: TLS 1.2 (0x0303)	
Random: 6f38b242c0da2509aade1226f276f642f886da39680073...	
Session ID Length: 32	
Session ID: c901b3f5b58f4b4f59634153796b6157999117215ac2cd40...	
Cipher Suites Length: 36	
Cipher Suites (18 suites)	
Cipher Suite: TLS_AES_128_GCM_SHA256 (0xc1301)	
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0xc1303)	
Cipher Suite: TLS_AES_256_GCM_SHA384 (0xc1302)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03a9)	
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03ab)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc03c)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc03d)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00aa)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0xc001)	

Server Hello:

服务端给客户端发送一个32位随机数，以及选中的 Cipher Suite 加密算法，和tls版本

Frame 1032: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{4FE48297-00C4-4203-A9BF-EE183CB8AAC}, id 0	
Ethernet II, Src: HuaweiE_33:ae:24 (f8:9b:ef:33:ae:24), Dst: Wistron_65:43:1b (54:ee:75:65:43:1b)	
Internet Protocol Version 4, Src: 172.18.132.150, Dst: 172.19.68.69	
Transmission Control Protocol, Src Port: 443, Dst Port: 4919, Seq: 1, Ack: 518, Len: 1460	
Transport Layer Security	
TLSv1.2 Record Layer: Handshake Protocol: Server Hello	
Content Type: Handshake (22)	
Version: TLS 1.2 (0x0303)	
Length: 84	
Handshake Protocol: Server Hello (2)	
Length: 80	
Version: TLS 1.2 (0x0303)	
Random: fccaab01f109c3785c7705c4254672a5994204bf0b0e28...	
Session ID Length: 0	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	
Compression Method: null (0)	
Extensions Length: 40	
Extension: renegotiation_info (len=1)	
Extension: server_name (len=0)	
Extension: ec_point_formats (len=4)	
Extension: session_ticket (len=0)	
Extension: application_layer_protocol_negotiation (len=0)	
Extension: extended_master_secret (len=0)	

Certificate、Server Key Exchange、Server Hello Done:

certificate: 该过程中服务器用私钥签名证书, 发送给客户端以认证身份

server key exchange: 由于服务端选择了Elliptic Curve Diffie Hellman算法交换密钥, 在此过程服务端将生成一对DH公钥和私钥, 私钥保留(用于服务器端生成预主密钥(Pre-master key)), 并将公钥发送给客户端(用于客户端生成预主密钥), 同时将前一阶段所有的会话内容利用私钥进行签名发给客户端, 用于验证服务端身份, 防止中间人攻击。有没有这一过程都是却决于密钥交换算法自身。在这个数据包中, 还给出了服务端生成公私钥所用的算法 sec256r1

server hello done: 表示server hello结束, 这是个空消息

```
Frame 1037: 1004 bytes on wire (8032 bits), 1004 bytes captured (8032 bits) on interface \Device\NPF_{4FE48297-00C4-4203-A0BF-EE183C8BAACC}, id 0
Ethernet II, Src: HuaweiE_33:ae:24 (f8:98:ef:33:ae:24), Dst: Mistront_65:43:1b (54:ee:75:65:43:1b)
Internet Protocol Version 4, Src: 172.18.132.150, Dst: 172.19.68.69
Transmission Control Protocol, Src Port: 443, Dst Port: 4919, Seq: 5557, Ack: 518, Len: 950
[5 Reassembled TCP Segments (6070 bytes): #1032(1371), #1033(1460), #1034(1176), #1036(1460), #1037(603)]
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 680
    Handshake Protocol: Certificate
  Transport Layer Security
    TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
      Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 329
        EC Diffie-Hellman Server Params
          Curve Type: named_curve (0x03)
          Named Curve: secp256r1 (0x0017)
          Pubkey Length: 65
          Pubkey: 042951b08af6a7af97ef4f6c5d92bf2a28525dc908aebf
          Signature Algorithm: sha256_rsa_sha256 (0x0804)
          Signature Length: 256
          Signature: 013e4bdcdcb387bf569f3d1c58b74d7e6d4c1a5350c
    TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
      Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

知乎 @白帽青年

Client Key Exchange、Change Cipher Spec、Encrypted Handshake Message:

```
Frame 1040: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF_{4FE48297-00C4-4203-A0BF-EE183C8BAACC}, id 0
Ethernet II, Src: Mistront_65:43:1b (54:ee:75:65:43:1b), Dst: HuaweiE_33:ae:24 (f8:98:ef:33:ae:24)
Internet Protocol Version 4, Src: 172.19.68.69, Dst: 172.18.132.150
Transmission Control Protocol, Src Port: 4919, Dst Port: 443, Seq: 518, Ack: 6507, Len: 126
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 70
    Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 66
      EC Diffie-Hellman Client Params
        Pubkey Length: 65
        Pubkey: 041af733a00393d3b097d52d3f6f396134e72baff9ef
    TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
    TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

知乎 @白帽青年

client key exchange: 客户端也生成一对DH公钥和私钥, 私钥保留(用于客户端生成预主密钥), 公钥发给服务端(用于服务端生成预主密钥(Pre-master key))

此时客户端在本地计算出预主密钥Pre-master key, 由于算法特性, 客户端和服务端根据各自的DH密钥计算的结果是相等的, 并通过Pre-master key计算出主密钥

change cipher spec: 客户端根据交互过程中获得的信息, 以及应用服务端规定的密码套件, 已经生成了相应的密钥。通过这条消息, 客户端告诉服务器端: 从现在起, 我将使用双方约定的密码规范进行通信

encrypted handshake message: 客户端利用生成的密钥加密一段finishde数据传送给服务端, 此数据是为了在正式传输应用之前对刚刚握手建立起来的加解密通道进行验证

New Session Ticket、Change Cipher Spec、Encrypted Handshake Message:

```
Frame 1041: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits) on interface \Device\NPF_{4FE48297-00C4-4203-A0BF-EE183C8BAACC}, id 0
Ethernet II, Src: HuaweiE_33:ae:24 (f8:98:ef:33:ae:24), Dst: Mistront_65:43:1b (54:ee:75:65:43:1b)
Internet Protocol Version 4, Src: 172.18.132.150, Dst: 172.19.68.69
Transmission Control Protocol, Src Port: 443, Dst Port: 4919, Seq: 6507, Ack: 644, Len: 274
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 218
    Handshake Protocol: New Session Ticket
      Handshake Type: New Session Ticket (4)
      Length: 214
      TLS Session Ticket
        Session Ticket Lifetime Hint: 7200 seconds (2 hours)
        Session Ticket Length: 208
        Session Ticket: 792708209c41a38c7dc88eca903109125d607acc3eeff68
    TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: change cipher spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
    TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

知乎 @白帽青年

服务端在本地计算出预主密钥Pre-master key，由于算法特性，客户端和服务端根据各自的DH密钥计算的结果是相等的，并通过Pre-master key计算出**主密钥**

new session ticket: 服务端告知客户端将生成新的session ticket用于保持会话（session ticket与前面提到的session id作用类似，但两者实现方式不同）

change cipher spec: 通过这条消息，服务端告诉客户端：从现在起，我将使用双方约定的密码规范进行通信

encrypted handshake message: 作用与客户端一致，至此，握手协议结束，双方开始建立加密通道。

可观察到后续的报文都是经过加密，表明已使用**对称密钥**进行加密传输

No.	Time	Source	Destination	Protocol	Length	Info
1036	2020-12-06 17:53:16.000000	172.18.132.150	172.19.68.69	TCP	54	1514 → 4919 [ACK] Seq=4097 Ack=518 Win=15544 Len=0 [TCP segment of a reassembled PDU]
1037	2020-12-06 17:53:16.000000	172.18.132.150	172.19.68.69	TLSv1.2	1084	Certificate, Server Key Exchange, Server Hello Done
1038	2020-12-06 17:53:16.000000	172.19.68.69	172.18.132.150	TCP	54	4919 → 1514 [ACK] Seq=518 Ack=5557 Win=262656 Len=0
1040	2020-12-06 17:53:16.000000	172.19.68.69	172.18.132.150	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1041	2020-12-06 17:53:16.000000	172.18.132.150	172.19.68.69	TLSv1.2	120	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1044	2020-12-06 17:53:16.000000	172.19.68.69	172.18.132.150	TCP	54	4919 → 1514 [ACK] Seq=644 Ack=6781 Win=261376 Len=0
1047	2020-12-06 17:53:18.000000	172.19.68.69	172.18.132.150	TLSv1.2	617	Application Data
1068	2020-12-06 17:53:18.000000	172.18.132.150	172.19.68.69	TCP	60	443 → 4919 [ACK] Seq=6781 Ack=1207 Win=14924 Len=0
1069	2020-12-06 17:53:18.000000	172.18.132.150	172.19.68.69	TCP	54	443 → 4919 [ACK] Seq=6781 Ack=1207 Win=14924 Len=0
1070	2020-12-06 17:53:18.000000	172.18.132.150	172.19.68.69	TLSv1.2	83	Application Data
1071	2020-12-06 17:53:18.000000	172.18.132.150	172.19.68.69	TCP	54	4919 → 443 [ACK] Seq=1207 Ack=8270 Win=262656 Len=0
1072	2020-12-06 17:53:18.000000	172.18.132.150	172.19.68.69	TCP	54	443 → 4919 [ACK] Seq=8270 Ack=1207 Win=14924 Len=0

四、TLS 1.3握手过程抓包

125	2020-12-06 18:51:01.000000	172.19.68.69	172.18.132.150	TCP	66	1429 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
126	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TCP	66	443 → 1429 [SYN, ACK] Seq=0 Ack=1 Win=16060 Len=0 MSS=1460 SACK_PERM=1 WS=2
128	2020-12-06 18:51:01.000000	172.19.68.69	172.18.132.150	TCP	54	1429 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
129	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TLSv1.3	571	Client Hello
130	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TCP	60	443 → 1429 [ACK] Seq=1 Ack=518 Win=15544 Len=0
131	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
132	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TCP	1230	443 → 1429 [PSH, ACK] Seq=20921 Ack=518 Win=15544 Len=1176 [TCP segment of a reassembled PDU]
133	2020-12-06 18:51:01.000000	172.19.68.69	172.18.132.150	TCP	54	1429 → 443 [ACK] Seq=518 Ack=2921 Win=262656 Len=0
135	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TCP	1514	443 → 1429 [ACK] Seq=4097 Ack=518 Win=15544 Len=1460 [TCP segment of a reassembled PDU]
136	2020-12-06 18:51:01.000000	172.19.68.69	172.18.132.150	TCP	54	1429 → 443 [ACK] Seq=518 Ack=5557 Win=262656 Len=0
137	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TLSv1.3	1169	Application Data, Application Data, Application Data
142	2020-12-06 18:51:01.000000	172.19.68.69	172.18.132.150	TCP	54	1429 → 443 [ACK] Seq=518 Ack=6672 Win=261632 Len=0
152	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TLSv1.3	134	Change Cipher Spec, Application Data
153	2020-12-06 18:51:01.000000	172.19.68.69	172.18.132.150	TCP	465	Application Data
154	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TLSv1.3	341	Application Data
155	2020-12-06 18:51:01.000000	172.18.132.150	172.19.68.69	TLSv1.3	341	Application Data
156	2020-12-06 18:51:01.000000	172.19.68.69	172.18.132.150	TCP	54	1429 → 443 [ACK] Seq=1009 Ack=7246 Win=262656 Len=0

Client Hello:

客户端发送32位随机数、所支持的加密套件、session id、compress（支持的压缩方法）、并预先使用一些安全套件，生成客户端公、私钥，将公钥放在key_share中发送给服务端。

Frame 128: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface vDevice\NPF_{AFE48297-00C4-4203-A0B6-EE183C8BAACC}, Id 0	
Ethernet II, Src: Mitront_65:43:1b (54:ee:75:65:43:1b), Dst: Huaweiife_33:ae:24 (f8:9b:ef:33:ae:24)	
Internet Protocol Version 4, Src: 172.19.68.69, Dst: 172.18.132.150	
Transmission Control Protocol, Src Port: 1429, Dst Port: 443, Seq: 1, Ack: 1, Len: 517	
Transport Layer Security	
TLSv1.3 Record Layer: Handshake Protocol: Client Hello	
Content Type: Handshake (22)	
Version: TLS 1.0 (0x0301)	
Length: 512	
Handshake Protocol: Client Hello (1)	
Handshake Type: Client Hello (1)	
Length: 508	
Version: TLS 1.2 (0x0303)	
Random: 4b4e90404be1eccc498af353dbb81cc0c02de25aa2d0d.	
Session ID Length: 32	
Session ID: a5f383c30af311dfa33beaf522de50180fded123ce61320.	
Cipher Suites Length: 36	
Cipher Suites (18 suites)	
Cipher Suite: TLS_AES_128_GCM_SHA256 (0xc1301)	
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0xc1303)	
Cipher Suite: TLS_AES_256_GCM_SHA384 (0xc1302)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc002b)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc002c)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0301)	
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0302)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc002d)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc002e)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc002f)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc0030)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc0013)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc0014)	
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc0015)	
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc0016)	
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x0301c)	
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x0301d)	
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x00013)	
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x00014)	
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00016)	
Length: 508	
Version: TLS 1.2 (0x0303)	
Random: 4b4e90404be1eccc498af353dbb81cc0c02de25aa2d0d.	
Session ID Length: 32	
Session ID: a5f383c30af311dfa33beaf522de50180fded123ce61320.	
Cipher suites length: 36	
Cipher suites (18 suites)	
Compression Methods Length: 1	
Compression Methods (1 method)	
Extensions Length: 399	
Extension: server_name (len=24)	
Extension: extended_master_secret (len=0)	
Extension: renegotiation_info (len=1)	
Extension: supported_groups (len=14)	
Extension: ec_point_formats (len=2)	
Extension: session_ticket (len=0)	
Extension: application_layer_protocol_negotiation (len=14)	
Extension: status_request (len=5)	
Extension: key_share (len=107)	
Type: key_share (51)	
Length: 107	
Key Share Extension	
Client Key Share Length: 105	
Key Share Entry: Group: X25519, Key Exchange length: 32	
Group: X25519 (29)	
Key Exchange Length: 32	
Key Exchange: cc2905aeecc8dd3f2aac09ad192d47091018b26227e579.	
Key Share Entry: Group: secp256r1, Key Exchange length: 65	
Group: secp256r1 (23)	
Key Exchange Length: 65	
Key Exchange: 0c1d1f53555e2429faef379283d336791f3922e98bc95.	
Extension: supported_versions (len=5)	
Extension: signature_algorithms (len=24)	
Extension: psk_key_exchange_modes (len=2)	
Extension: record_size_limit (len=2)	
Extension: padding (len=143)	

Server Hello 、 Change Cipher Spec、 Application Data

此时服务端已具备足够信息生成预主密钥，进而生成主密钥，因此会发送 Change Cipher Spec 告知客户端，之后的消息将会加密传输；此后所有的报文都将被加密成Application Data（由上述握手过程可见）

Frame 130: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{4FE48297-00C4-4203-A0BF-EE183CB8AAC}, Id 0

Ethernet II, Src: HuaweiE12, 08:00:27:14:00:24 (88:98:f4:32:ae:24), Dst: WiStronT_05:43:1b (54:ee:75:65:43:1b)

Internet Protocol Version 4, Src: 172.18.132.150, Dst: 172.19.68.69

Transmission Control Protocol, Src Port: 443, Dst Port: 1429, Seq: 1, Ack: 518, Len: 1460

Transport Layer Security

↳ TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 155

↳ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 151

Version: TLS 1.2 (0x0303)

Random: 5fcb795a95aa4399965ee5a3b52590d899ea37ee16b82

Session ID Length: 32

Session ID: a6538c30eef11ffca3b0a1522de5010bfed123ce6132b

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Compression Method: null (0)

Extensions Length: 79

↳ Extension: supported_versions (len=2)

Type: supported_versions (43)

Length: 2

Supported Version: TLS 1.3 (0x0304)

↳ Extension: key_share (len=69)

Type: key_share (51)

Length: 69

↳ Key Share extension

↳ Key Share Entry: Group: secp256r1, Key Exchange length: 65

Group: secp256r1 (23)

Key Exchange length: 65

Key Exchange: 0a530315595f87f4dd4afe790b6ca142954813f9187df30b2

↳ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

↳ TLSv1.3 Record Layer: Application Data Protocol: Http-over-Tls

知乎 @白帽青年

使用wireshark解密后的数据包

No.

Time

Source

Destination

Protocol

Length

Info

372 2020-12-07 17:56:15.172.18.132.150172.19.68.77TCP662320 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

373 2020-12-07 17:56:15.172.18.132.150172.19.68.77TCP66443 → 2329 [SYN, ACK] Seq=0 Ack=1 Win=1040 Len=0 MSS=1460 SACK_PERM=1 WS=2

378 2020-12-07 17:56:15.172.19.68.77172.18.132.150TCP542329 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0

379 2020-12-07 17:56:15.172.19.68.77172.18.132.150TLSv1.3571Client Hello

380 2020-12-07 17:56:15.172.18.132.150172.19.68.77TCP60443 → 2329 [ACK] Seq=1 Ack=518 Win=15544 Len=0

381 2020-12-07 17:56:15.172.18.132.150172.19.68.77TLSv1.3153Hello Retry Request, Change Cipher Spec

382 2020-12-07 17:56:15.172.19.68.77172.18.132.150TLSv1.3377Change Cipher Spec, Client Hello

383 2020-12-07 17:56:15.172.18.132.150172.19.68.77TLSv1.31514Server Hello, Encrypted Extensions

386 2020-12-07 17:56:15.172.18.132.150172.19.68.77TCP1514443 → 2329 [ACK] Seq=1560 Ack=1041 Win=15022 Len=1460 [TCP segment of a reassembled PDU]

387 2020-12-07 17:56:15.172.19.68.77172.18.132.150TCP542329 → 443 [ACK] Seq=1041 Ack=3020 Win=131328 Len=0

389 2020-12-07 17:56:15.172.18.132.150172.19.68.77TCP1230443 → 2329 [PSH, ACK] Seq=3020 Ack=1041 Win=15022 Len=1176 [TCP segment of a reassembled PDU]

390 2020-12-07 17:56:15.172.19.68.77172.19.68.77TCP1514443 → 2329 [ACK] Seq=4190 Ack=1041 Win=15022 Len=1460 [TCP segment of a reassembled PDU]

391 2020-12-07 17:56:15.172.19.68.77172.18.132.150TCP542329 → 443 [ACK] Seq=1041 Ack=5656 Win=131328 Len=0

392 2020-12-07 17:56:15.172.18.132.150172.19.68.77TLSv1.31163Certificate, Certificate Verify, Finished

398 2020-12-07 17:56:15.172.18.132.150172.19.68.77TLSv1.3128Finished

399 2020-12-07 17:56:15.172.18.132.150172.19.68.77TLSv1.3341New Session Ticket

400 2020-12-07 17:56:15.172.18.132.150172.19.68.77TLSv1.3341New Session Ticket

401 2020-12-07 17:56:15.172.19.68.77492400 → 443 [40B] Seq=5155 Ack=7339 Win=231320 Len=0

知乎 @白帽青年

此后客户端接收到服务端创建的公钥和随机数后，根据对应算法计算出预主密钥和主密钥，进行加密消息验证和加密传输。

五、 TLS 1.3握手过程优化

使用 TLS 1.2 需要两次往返（ 2-RTT ）才能完成握手，然后才能发送请求。

TLS 1.3 协议只需要一次往返（ 1-RTT ）就可以完成握手，发送加密请求，更加安全。

发布于 2020-12-08 11:09

抓包 HTTPS Wireshark

发布一条带图评论吧

2 条评论

默认 最新

Hapy

请问博主，客户端和服务器的私钥都自己保留，那么请问这个私钥在哪里能查看？

05-19

回复 喜欢

pony

请教下，client hello的时候，是怎么决定tls的版本的？我看你这里实例有tls1.2和1.3的

2021-09-30

回复 喜欢

文章被以下专栏收录

网络协议

https://zhuanlan.zhihu.com/p/324456506

6/7

推荐阅读

Wireshark抓包(网络分析)

前言贴一张wireshark抓包的总图，便于理解分析 网络分层 为了让大家更容易「看得见」 TCP，我搭建不少测试环境，并且数据包抓很多次，花费了不少时间，才抓到比较容易分析的数据包。 接下来...

你瞅啥



WireShark 抓包及常用协议分析

你瞅啥



WireShark 抓包及常用协议分析

like you



如何

叶焱