



- 1.实验报告如有雷同,雷同各方当次实验成绩均以0分计。
- 2. 当次小组成员成绩只计学号、姓名登录在下表中的。
- 3.在规定时间内未上交实验报告的,不得以其他方式补交,当次成绩按0分计。
- 4.实验报告文件以 PDF 格式提交。

本班序号	<u>60</u>	本班序号	29	组长姓名: 郑卓民
学生姓名	郑卓民_18342138	学生姓名	刘铭浩 18329042	
<u>实验分工</u>				
郑卓民	进行实验, 填写实验报告.			
刘铭浩	进行实验, 拍摄视频			

### SSL 协议分析

#### [目的]

- (1) 了解 SSL 工作原理。
- (2) 通过抓取数据包,了解客户端与 Web 服务端的实际工作流。

#### [环境]

本地主机 IP 地址: 192.168.88.104 (客户端)。

远程主机(百度服务器) IP 地址: 182.61.200.7 (访问: https://www.baidu.com)。

#### [实验]

实验时,启动协议分析器 Wireshark,打开浏览器,在地址栏输入 https://www.baidu.com,开始抓取数据包。在 Wireshark 过滤工具栏过滤掉其他无关数据包。

整个通信过程由客户端发起,由于 SSL 协议是基于传输层的 TCP 协议的,所以首先经过三次握手与服务器建立 TCP 连接。一旦连接建立成功,就进入 SSL 握手和数据传输阶段。下面结合 TCP 和 SSL 原理对数据交互流程进行分析,请根据实际捕获数据填写:

- (1)在  $1\sim3$  帧中,客户端与服务器先通过三次握手建立 TCP 连接,由于使用的是 https 协议,所以传输层的端口号为( ① )。
- (2) 第 4 帧开始,就进入 SSL 的握手阶段。客户端向服务器发送( ② )消息,其中包含了客户端所支持的各种算法。从解码中可以看出主要包括 RSA 和 DH 两大类算法,由它们产生多种组合。同时产生了一个随机数,这个随机数随后将应用于各种密钥的推导,并可以防止重放攻击。
  - (3) 第5帧为对方发过来 ACK 确认帧, 第6帧服务器发送(3) 消息,其中包含了服务器



选中的算法( ④ ),同时发来另一个随机数,这个随机数的功能与客户端发送的随机数功能相同。

- (4) 第7帧服务器返回(⑤) 消息,其中包含了服务器的证书,以便客户端认证服务器的身份,并从中获取其公钥。同时服务器告诉客户端(⑥),指明本阶段的消息已经发送完成。
- (5) 第 8 帧为本地客户端发送给服务器的 ACK 确认。第 9 帧开始客户端向服务器发送( ⑦ ) 消息,其中包含了客户端生成的预主密钥,并使用服务器的公钥进行加密处理。
- (6) 此时,客户端和服务器各自以预主密钥和随机数作为输入,在本地计算所需要的 4 个密钥参数 (其中包括 2 个加密密钥和 2 个 MAC 密钥),由于此过程并没有通过网络进行传输,所以也就没有在数据帧中体现出来。
  - (7) 在第9帧中客户端还向服务器发送(图)消息,以通告启用协商好的各项参数。
- (8) 第 10 帧服务器向客户端发送 ( ⑨ )消息,第 11 帧客户端发来确认消息,协商阶段结束。
- (9) 从第( ⑩ )帧到第( ① )帧,都为服务器和客户端之间交互应用数据信息。它们都使用协商好的参数进行安全处理。
- (10)由于TCP协议是面向连接的,最后的几帧为拆除TCP连接,由客户端发出FIN位为置位的TCP段,对方发来ACK确认帧以及FIN位为置位的TCP段,客户端再发出ACK帧进行确认,至此TCP连接释放,传输结束。

实验时,在执行连接之前,启动协议分析器 Wireshark,开始监控抓取数据包。在 Wireshark 过滤工具栏过滤掉其他无关数据包。按以下要求分析 SSL 工作过程。

	答案	截图	简要分析
1	443	▼ Transmission Control Protocol, Src Port: 14528, Dst Port: 443, \$     Source Port: 14528     Destination Port: 443     [Stream index: 8]     Try Segment Len: 0]	由于 <u>www.baidu.com 使用</u> https 协议,所以在 TCP
		[TO Segment Len: 0]	下端口 port 为 443
2	Client Hello	> Internet Protocol Version 4, Src: 192.168.88.104, Dst: 182.61.20 > Transmission Control Protocol, Src Port: 14529, Dst Port: 443, Si  > 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	SSI 握手阶段开始,客户 端发送 Client Hello 给服 务器



# 中山大學移动网络安全技术实验报告 SUN YAT-SEN UNIVERSITY

AND COL	SUN YAT-SEN UNIVERSITY		
3	Server Hello	✓ Iransport Layer Security  ✓ TLSv1.2 Record Layer: Handshake Protocol: Server Hello  Content Type: Handshake (22)  Version: TLS 1.2 (0x0303)  Length: 53	服务器发送完 ACK 确认
		➤ Handshake Protocol: Server Hello Handshake Type: Server Hello (2) Length: 49	帧给客户端后,发送
		Version: TLS 1.2 (0x0303) > Random: 5d944291191984682e5fbf3f57e0842cc9be11e0fd9991af Session ID Length: 0	Server Hello 信息给客户
		Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc0 Compression Method: null (0)	端
4	RSA	▼ Transport Layer Security ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Content Type: Handshake (22)	在发送的 Server Hello 信
		Version: TLS 1.2 (0x0303)  Length: 53  WHandshake Protocol: Server Hello  Handshake Type: Server Hello (2)	息里面可以找到服务器
		Length: 49 Version: TLS 1.2 (0x0303) > Random: 5d944291191984682e5fbf3f57e0842cc9be11e0fd9991af Session ID Length: 0	选用的加密算法,Cipher
		Cipher Suite: TLS_ECDHE_RSA_MITH_AES_128_GCM_SHA256 (0xc02f) Compression Method: null (0) Extensions Length: 9  * Extension: session_ticket (len=0) Type: session_ticket (35)	Suite 选用的是 TLS_RSA
(5)	Certificate	Length: 0  Transport Layer Security TLSV1.2 Record Layer: Handshake Protocol: Certificate Content Type: Handshake (22)	服务器发送证书给客户
		Version: TLS 1.2 (0x0303) Length: 3629 > Handshake Protocol: Certificate	端进行验证
		Handshake Type: Certificate (11) Length: 3625 Certificates Length: 3622 > Certificates (3622 bytes)	
6	Server Hello Done	<pre></pre>	服务器发送 Server Hello
			Done 表示本阶段传送信
		Length: 0	息完成
7	Client Key Exchange;	▼ Transport Layer Security ▼ T.Sv1.2 Record Layer: Handshake Protocol Client Key Exchange Content Type: Handshake (22) Version: TLS 1.2 (8xe)33)	客户端向服务器发送客
	Change Cipher Spec;	Length: 20  ✓ Handshake Protocol: Client Key Exchange  Handshake Type: Client Key Exchange (16)  Length: 66	户端生成的预主密钥,并
		> EC Diffie-Hellman Client Params  VT.LSV12. Record Layer: Change Cipher Spec Protocol:  Content Type: Change Cipher Spec (20)  Version: TLS 1.2 (0x00303)	使用服务器的公钥进行
		Length: 1 Change Cipher Spec Message  VILSV1.2 Record Layer: Handshake Protocol: Content Type: Handshake (22) Version: TLS 1.2 (80x0303)	加密处理
		Length: 40 Handshake Protocol: Encrypted Handshake Message	
8	Encrypted Handshake	▼ Transport Layer Security ▼ TLSV1.2 Record Layer: Handshake Protocol Content Type: Handshake (22) Version: TLS 1.2 (0x0303)	通告启用协商好的各项
	Message;	Length: 70 Handshake Protocol: Client Key Exchange Handshake Type: Client Key Exchange (16) Length: 66	参数
		> EC Diffie-Hellman Client Params  > TLSV1.2 Record Layer: Change Cipher Spec Protocol: Content Type: Change Cipher Spec (20) Version: TLS 1.2 (0x0303)	
		Length: 1 Change Cipher Spec Message  VILSV1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message Content Type: Handshake (22)	
		Version: TLS 1.2 (0x0303) Length: 40 Handshake Protocol: Encrypted Handshake Message	
9	Server Hello Done	<pre></pre>	服务器发送信息表示协
		Version: TLS 1.2 (0x0303) Length: 4  Handshake Protocol: Server Hello Done Handshake Type: Server Hello Done (14) Length: 0	商阶段结束
10	9	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 63 [TCP Spurious Retransmission] , Server Hello Done	第9帧启用协商好的参数
		66 [TCP Dup ACK 232#1] 1364 → 443 [ACK] Seq=644 Ack=4040 Win=66560 Len=6	后,即可使用协商好的参



## 中山大學移动网络安全技术实验报告

				数
(	11)	11	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 63 [TCP Spurious Retransmission] , Server Hello Done 66 [TCP Dup ACK 23Z#1] 1364 → 443 [ACK] Seq=644 Ack=4040 Win=66560 Len=1	同上
安全特点 机密性: SSL 协议使用密钥加密通信数据。				
	可靠性: 服务器和客户都会被认证,客户的认证是可选的。		<b>勺</b> 。	
	完整性: SSL 协议会对传送的数据进行完整性检查。			

(3)作为对比,接下来通过某网站的普通访问,分析连接和传输过程与 SSL 在安全性的差异。请根据抓取的数据包,分析登录过程:

	ip. addr == 47.52.27.250				
分析过程	No. Time	Source	Destination	Protocol	Length Info
力加过性	533 29.541089	192.168.88.104	47.52.27.250	TCP	66 6510 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1
	534 29.541894	192.168.88.104	47.52.27.250	TCP	66 6511 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1
	535 29.571159	47.52.27.250	192.168.88.104	TCP	66 80 → 6510 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK PERM=1 WS=128
	536 29.571235	192.168.88.104	47.52.27.250	TCP	54 6510 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
	537 29.571588	192.168.88.104	47.52.27.250	HTTP	466 GET / HTTP/1.1
	538 29.574698	47.52.27.250	192.168.88.104	TCP	66 80 → 6511 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK PERM=1 WS=128
	539 29.574772	192.168.88.104	47.52.27.250	TCP	54 6511 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
	540 29.604906	47.52.27.250	192.168.88.104	TCP	54 80 → 6510 [ACK] Seq=1 Ack=413 Win=30336 Len=0
	541 30.222939	47.52.27.250	192.168.88.104	HTTP	1514 [TCP Previous segment not captured] Continuation
	542 30.222940		192.168.88.104		1514 [TCP Out-Of-Order] 80 → 6510 [ACK] Seq=1 Ack=413 Win=30336 Len=1460
	543 30.222942	47.52.27.250	192.168.88.104	HTTP	1514 Continuation
	544 30.223036	192.168.88.104	47.52.27.250	TCP	66 [TCP Dup ACK 536#1] 6510 → 80 [ACK] Seq=413 Ack=1 Win=65536 Len=0 SLE=1461 SRE=2921
	545 30.223129	192.168.88.104	47.52.27.250	TCP	54 6510 → 80 [ACK] Seq=413 Ack=2921 Win=65536 Len=0
	546 30.228561	47.52.27.250	192.168.88.104	HTTP	1514 Continuation
	547 30.228562	47.52.27.250	192.168.88.104	HTTP	1514 Continuation
	548 30.228564	47.52.27.250	192.168.88.104	HTTP	1514 Continuation
		•		•	lab.com),经过三次握手成功访问之后,传输信息 ì,更加简单快速。
安全特点	安全性较低,无使用加密算法				

SSL 和普通访问对比分析的安全性结论:

SSL 比普通访问安全性更高,对传输信息进行加密处理,但对应地加重了服务器的负担, 降低了用户的访问速度

#### 【交实验报告】

上传实验报告: ftp://172.18.178.1/

截止日期(不迟于):2周之内完成

上传小组实验报告。上传文件名格式:组长序号组长名\_组员名\_实验名.pdf (由组长负责上传)视频文件名与小组文件名相同,扩展名是 mp4。

例如:文件名"6张三\_李四\_网络攻击分析实验.pdf"表示第6组的网络攻击分析实验报告