



警示

- 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	60	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	
实验分工				
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 1~3 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，所以也就没有数据帧中体现出来。

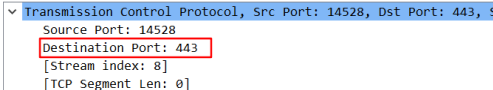
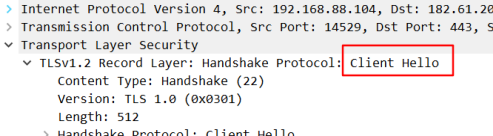
（7）在第 9 帧中客户端还向服务器发送（ ⑧ ）消息，以通告启用协商好的各项参数。

（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（ ⑪ ）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		由于 www.baidu.com 使用 https 协议，所以在 TCP 下端口 port 为 443
②	Client Hello		SSL 握手阶段开始，客户端发送 Client Hello 给服务器



③	Server Hello	<ul style="list-style-type: none">Transport Layer Security<ul style="list-style-type: none">TLSv1.2 Record Layer: Handshake Protocol: Server Hello<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 53Handshake Protocol: Server Hello<ul style="list-style-type: none">Handshake Type: Server Hello (2)Length: 49Version: TLS 1.2 (0x0303)Random: 5d944291191984682e5fbf3f57e0842cc9be11e0fd9991af...Session ID Length: 0Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)Compression Method: null (0)	服务器发送完 ACK 确认 帧给客户端后，发送 Server Hello 信息给客户 端
④	RSA	<ul style="list-style-type: none">Transport Layer Security<ul style="list-style-type: none">TLSv1.2 Record Layer: Handshake Protocol: Server Hello<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 53Handshake Protocol: Server Hello<ul style="list-style-type: none">Handshake Type: Server Hello (2)Length: 49Version: TLS 1.2 (0x0303)Random: 5d944291191984682e5fbf3f57e0842cc9be11e0fd9991af...Session ID Length: 0Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)Compression Method: null (0)Extensions Length: 9Extension: session_ticket (len=0)<ul style="list-style-type: none">Type: session_ticket (35)Length: 0	在发送的 Server Hello 信 息里面可以找到服务器 选用的加密算法，Cipher Suite 选用的是 TLS_RSA
⑤	Certificate	<ul style="list-style-type: none">Transport Layer Security<ul style="list-style-type: none">TLSv1.2 Record Layer: Handshake Protocol: Certificate<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 3629Handshake Protocol: Certificate<ul style="list-style-type: none">Handshake Type: Certificate (11)Length: 3625Certificates Length: 3622Certificates (3622 bytes)	服务器发送证书给客户 端进行验证
⑥	Server Hello Done	<ul style="list-style-type: none">Transport Layer Security<ul style="list-style-type: none">TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 4Handshake Protocol: Server Hello Done<ul style="list-style-type: none">Handshake Type: Server Hello Done (14)Length: 0	服务器发送 Server Hello Done 表示本阶段传送信 息完成
⑦	Client Key Exchange; Change Cipher Spec;	<ul style="list-style-type: none">Transport Layer Security<ul style="list-style-type: none">TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 70Handshake Protocol: Client Key Exchange<ul style="list-style-type: none">Handshake Type: Client Key Exchange (16)Length: 66EC Diffie-Hellman Client ParamsTLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec<ul style="list-style-type: none">Content Type: Change Cipher Spec (20)Version: TLS 1.2 (0x0303)Length: 1Change Cipher Spec MessageTLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 40Handshake Protocol: Encrypted Handshake Message	客户端向服务器发送客 户端生成的预主密钥，并 使用服务器的公钥进行 加密处理
⑧	Encrypted Handshake Message;	<ul style="list-style-type: none">Transport Layer Security<ul style="list-style-type: none">TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 70Handshake Protocol: Client Key Exchange<ul style="list-style-type: none">Handshake Type: Client Key Exchange (16)Length: 66EC Diffie-Hellman Client ParamsTLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec<ul style="list-style-type: none">Content Type: Change Cipher Spec (20)Version: TLS 1.2 (0x0303)Length: 1Change Cipher Spec MessageTLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 40Handshake Protocol: Encrypted Handshake Message	通告启用协商好的各项 参数
⑨	Server Hello Done	<ul style="list-style-type: none">Transport Layer Security<ul style="list-style-type: none">TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done<ul style="list-style-type: none">Content Type: Handshake (22)Version: TLS 1.2 (0x0303)Length: 4Handshake Protocol: Server Hello Done<ul style="list-style-type: none">Handshake Type: Server Hello Done (14)Length: 0	服务器发送信息表示协 商阶段结束
⑩	9	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 63 [TCP Spurious Retransmission], Server Hello Done 66 [TCP Dup ACK 232#1] 1364 → 443 [ACK] Seq=644 Ack=4040 Win=66560 Len=0	第 9 帧启用协商好的参数 后，即可使用协商好的参



			数
⑪	11	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 63 [TCP Spurious Retransmission], Server Hello Done 66 [TCP Dup ACK 232#1] 1364 → 443 [ACK] Seq=644 Ack=4040 Win=66560 Len=0	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。 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:

分析过程	
	访问普通 http 协议的网站(http://inpluslab.com), 经过三次握手成功访问之后, 传输信息无需使用 SSL 进行加密, 都是明文传输, 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