山东大学 计算机 学院

计算机网络 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：202000130143 | 姓名： 郑凯饶 | | 班级： 2020级1班 |
| 实验题目：SSL | | | |
| 实验学时：2 | | 实验日期： 2022-6-7 | |
| 实验目的：  研究安全套接字协议，关注通过TCP传送的SSL记录。 | | | |
| 硬件环境：  Dell Latitude 5411  Intel(R) Core(TM) i5-10400H CPU @ 2.60GHz(8GPUs),~2.6GHz | | | |
| 软件环境：  Windows 10 家庭中文版64位（10.0，版本18363）  Wireshark-win64-3.6.2 | | | |
| 实验步骤与内容：   1. 问题： 2. 对于前八个以太网帧，指出每一帧的来源，确定每帧包含的SSL记录数量，并且列出记录类型，绘制时序图。 3. 列出SSL记录所有字段及长度。 4. 展开ClientHello记录，回答内容类型的值。 5. ClientHello是否包含不重数，十六进制值是多少？ 6. ClientHello通知了它所支持的加密套件(cyber suites)对第一个密码套件，指出非对称、对称、哈希算法分别是什么？ 7. 找到ServerHello SSL记录。此记录是否指定了之前的密码套件，选择的密码套件中有哪些算法？ 8. 是否包含不重数，它的用途？ 9. 会话ID。 10. 是否包含证书，证书是否适合用单一的以太网帧传输？ 11. 找到客户端密钥交换记录，是否包含前主密钥，它的用途，是否加密，加密后的长度？ 12. Chipher Spec record的作用？字节数？ 13. Handshake record中什么被加密了，为什么？ 14. 服务器是否向客户端发送Chipher Spec record和Handshake record，与客户端发送的有什么不同？ 15. 应用程序数据如何加密？记录是否包含消息认证码MAC？Wireshark是否区分数据和MAC？ 16. 指出并解释你的其他发现？ 17. 阐述基本方法   TSL的四次握手过程：               1. 实验结果展示与分析   （1）筛选得      103-113帧为前八帧。SSL记录来源及类型如下：    时序图如下：    （2）依次占2Byte，1B，2B    （3） 0x01  （4）    （5） 非对称：RSA 对称：RC4 哈希：MD5    （6）    （7） 有如上图，防止“重放攻击”  （8） 如图  （9）是，在单独的记录中。证书较长需要分片传输。    （10）如图，通过RSA加密（使用服务器公钥），长度为128B，和不重数一起用于生成主密钥。    （11）指示之后发送信息是经过加密的。长度为1B    （12）Encrypted Handshake Message被加密    （13） 是，部分不同，Handshake Message的明文是所有握手报文的MAC，但由于双方MAC密钥不同，摘要后的密文不同。  （14）使用之前协商的方法进行加密，而相应的密钥通过主密钥切片而得。包含用于报文完整性鉴别，Wireshark不区分。 | | | |
| 结论分析与体会：  理论上如果我们是信息交流的一方，我们可以解密所有会话（好像这是显然的），只不过对于普通用户来说加解密是透明的。假期我希望尝试一下通过Wireshark进行SSL报文的解密，或者自己尝试编程解密算法。TLS四次握手进行了身份认证、会话密钥交换，保证之后会话的完整性、保密性、权威性，是网络通信的重要组分。希望以后还有机会学习网络安全、密码学相关的知识。 | | | |