西安交通大学

计算机网络原理与应用课程作业

姓名：　　屈彬
学号：　　2140505062
次数：　　第 1 次
日期：　2018 年 3 月 14 日

利用 Wireshark 软件获取并分析 TLS 协议

目录

第 1 章 实验背景

1.1 TLS 简介

TLS 全称“Transport Layer Security（安全传输层）”，用于在两个通信应用程序之间提供保密性和数据完整性，常用于 Web 应用中客户端与服务器的加密通信。虽然 TLS 协议被定义为传输层的安全协议，但实际在抓包结果中可以看到 TLS 协议部分是被封装在 TCP 等传输层协议内的，而应用层的内容则封装在 TLS 内。在登录西安交通大学学生版统一认证网关的过程中，客户端页面也采用 TLS 加密方式向服务器提交表单，因此通过本实验也能对西安交通大学统一认证网关的安全机制有更好的了解。

通过查阅国内相关文献[1] 以及国外的一些文献[3] ，可以了解到 TLS 协议由记录协议、更改密码协议以及警告协议三个高层协议构成，其中，记录协议还包括握手子协议。记录协议从高层 ssL 子协议收到数据后，对它们进行数据分段、压缩、认证和加密形成 ssL 记录；更改密码规格协议将密文状态由挂起状态复制到当前状态；警告协议用来传递 ssL 的相关警告。由于握手过程是可以被 Wireshark 软件轻易捕获的，在抓包时，我们主要关心的是 TLS 协议中的握手过程。TLS 的握手过程如图 1.1 所示。

在图 1.1 中，左侧代表客户端，右侧代表服务端。当客户端向服务端发起握手时，客户端首先向服务端发送“ClientHello”字段，包含会话 ID（Session ID）等信息；服务端收到“ClientHello”字段后，返回一个“ServerHello”字段，同样包含会话 ID 等信息；之后服务端和客户端之间会进行密钥交换，在结束握手前，服务器还向客户端发送更改密钥的信息。

但在实际的网络应用中，TLS 协议的握手过程是否真的如图 1.1 所示。本实验将通过 Wireshark 软件对西安交通大学学生版统一身份认证网关的登录过程进行抓包分析，以探究竟。

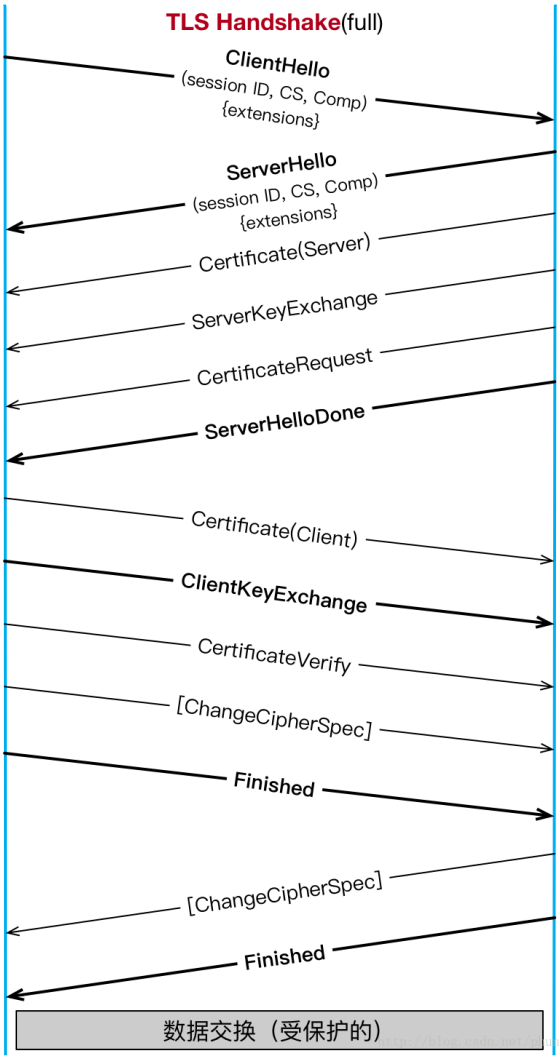

图 1.1: TLS 协议握手过程[2]

1.2 实验目标

1. 利用 Wireshark 软件对西安交通大学学生版统一认证网关的登录过程进行抓包。
2. 根据抓包结果，分析 TLS 协议握手过程。
3. 解密客户端向服务端提交的表单。

第 2 章 实验工具

1. Wireshark 软件：用于获取网络通信过程经过本地的数据包。本实验所使用的版本为 2.4.5。
2. 支持 IE6 以上内核的浏览器：用于访问西安交通大学学生版统一身份认证网关。
3. CTeX + TeXstudio：用于报告写作。

第 3 章 实验过程

第 4 章 实验结论

参考文献

[1] 李天目. Ssl/tls 协议的安全分析与改进. 信息网络安全, 1:51–54, 2005.

[2] CSDN. TLS 握手协商流程解析. http://blog.csdn.net/phunxm/article/details/72853552, 2017. [Online; accessed 14-Mar-2018].

[3] S Turner. Transport layer security. *IEEE Internet Computing*, 18(6):60–63, 2014.