



网络空间安全实验基础

Hands-on Cybersecurity - Fundamentals

|  |
| --- |
| 传输层安全协议（TLS） |

主讲人：张玉健

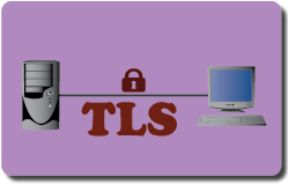


课程提纲

• TLS协议概览

• TLS握手

• TLS数据传输

• TLS客户端编程

• TLS服务端编程

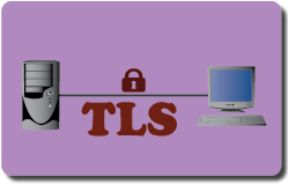
• TLS代理编程

课程提纲

• TLS协议概览

• TLS握手

• TLS数据传输

• TLS客户端编程

• TLS服务端编程

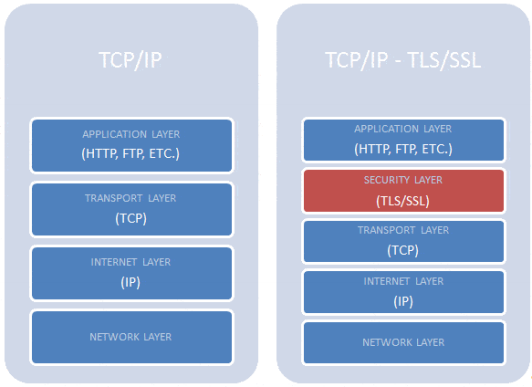
• TLS代理编程

引入TLS目的

 **TLS（Transport** **Layer** **Security）的目的**

• TCP/IP协议栈的问题：payload明文，极易被窃听、篡改、仿冒等

• TLS的作用：为网络通信提供机密性（Confidentiality）、认证性（Authentication）及数据 完整性（Integrity）保障



3

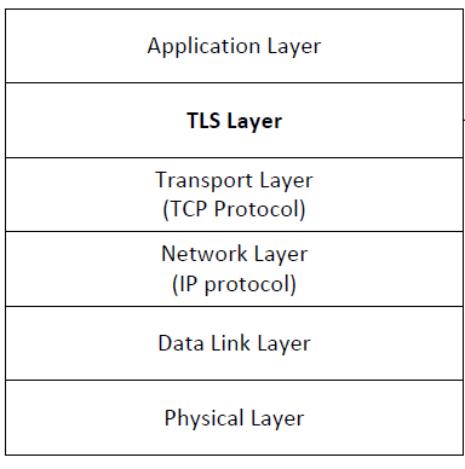
TLS层的工作

 **TLS介于传输层和应用层之间**

• 从应用层看：向/从TLS层发送/收取数据明文

• 从TLS层看：处理数据加密/解密、完整性验证等

• 从传输层看：向/从TLS层发送/收取数据密文





TLS的发展历程

 **TLS的发展时间线**

• 1994年，网景（NetScape）公司设计了 SSL 1.0

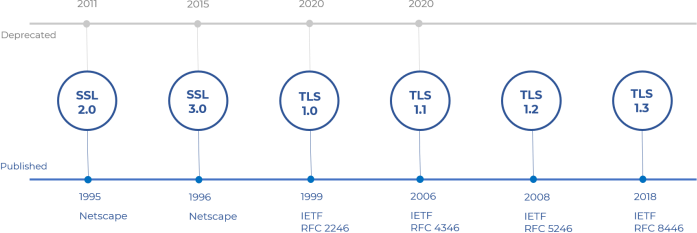
• 1995年，SSL 2.0，存在严重漏洞

• 1996年，SSL 3.0，得到大规模应用

• 1999年，IETF 对 SSL 进行标准化，发布了 TLS 1.0

• 2006年和2008年，TLS 进行了两次升级，分别为 TLS 1.1 和 TLS 1.2

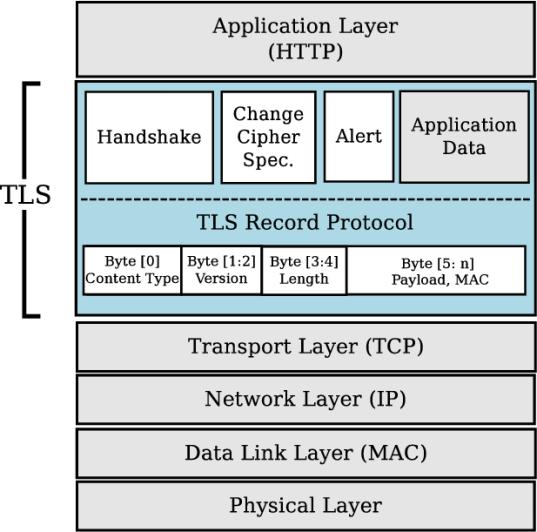
• 2018年，TLS 1.3作为建议标准发布于RFC 8446





5

TLS协议框架

 **TLS的子协议**

• Handshake

• Change Cipher Spec. (deprecated in TLS 1.3)

|  |
| --- |
| Application Data |

|  |
| --- |
| Handshake |

|  |
| --- |
| Heartbeat |

|  |
| --- |
| Change  Cipher  Spec. |

|  |
| --- |
| Alert |

• Alert

• Heartbeat (extended by RFC6520)

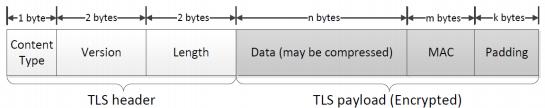
• Application Data

 **TLS记录层（Record）**

• 作用：提供数据封装、压缩、加/解密等功能

• 格式：type、version、 length、payload

• payload长度：最大214



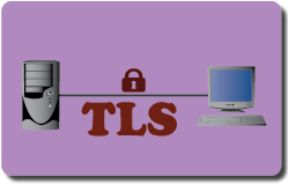
6

课程提纲

• TLS协议概览

• TLS握手

• TLS数据传输

• TLS客户端编程

• TLS服务端编程

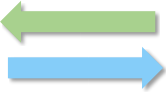
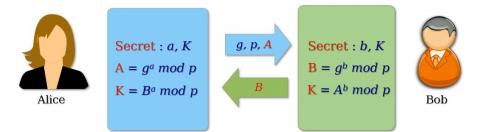
• TLS代理编程

TLS握手的目的和选择

 **密钥协商**

|  |
| --- |
| 基于RSA的密钥协商 |
|  |

• 基于RSA



*PK*

Enc*PK*(*K*)

Secret : *K*

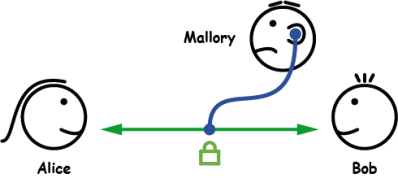


*PK, SK*

• 基于Diffie-Hellman（DH）

 **认证**

• RSA已提供认证功能，直接使用？

• DH未提供（基于DH的证书几乎没有）

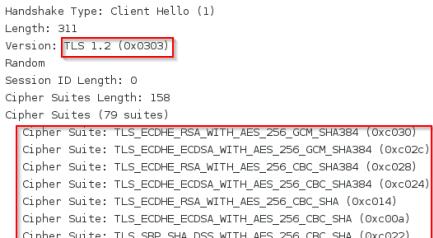
Once got the  ,

is historical communication safe?

|  |
| --- |
| 基于Diffie-Hellman的密钥协商 |
|  |

完美前向保密（Perfect Forward Secrecy）问题

TLS的加密套件

 **加密套件（Cipher** **Suite）**

• Key Exchange：密钥协商算法

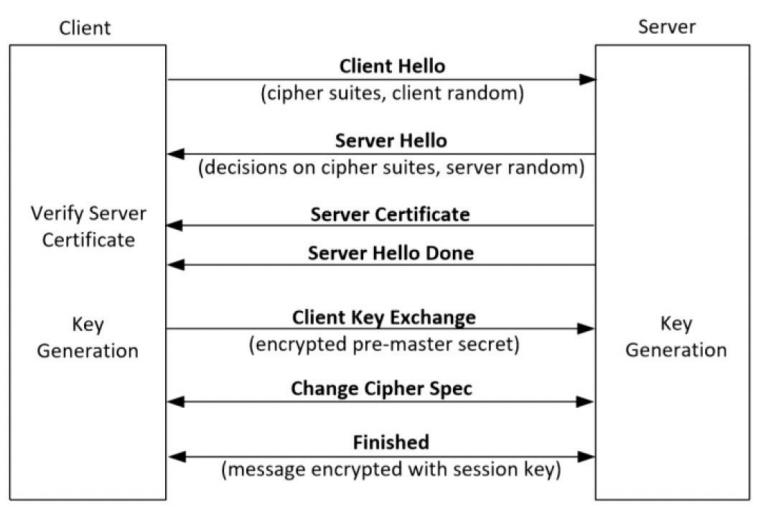
• Authentication：身份认证算法

• Encryption：对称加密算法

• MAC(Message Authentication Code)：消息认证码算法



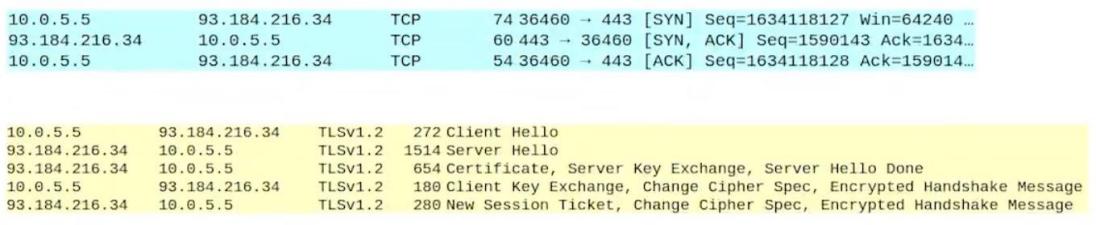
TLS握手协议（v1.2）



TLS握手协议（v1.2）报文

TCP握手







TLS握手

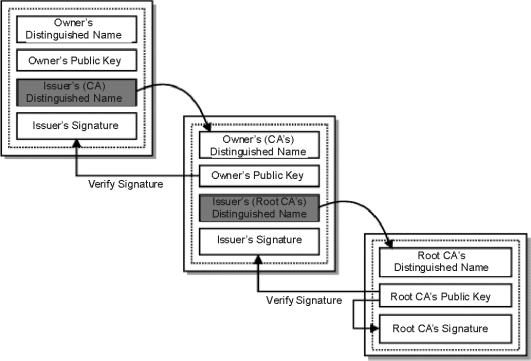
TLS握手中的证书验证

 **客户端验证服务端的证书**

• 验证证书的有效期、签名等

• 验证访问的域名与证书中的名称是否一致

• 客户端需要预安装根证书（参见PKI）



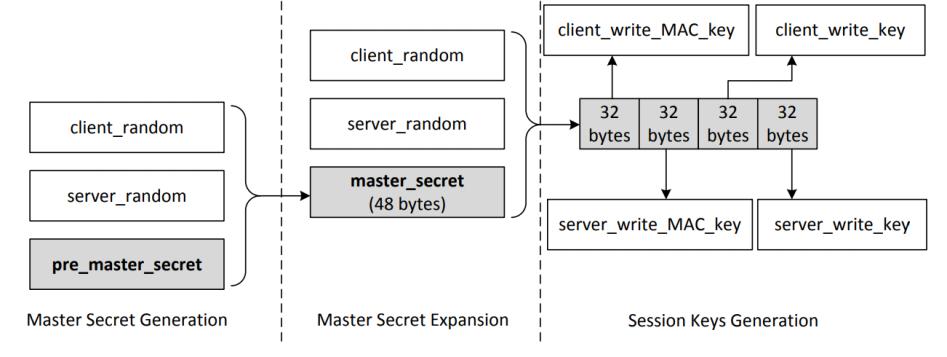
12

TLS握手中的密钥生成

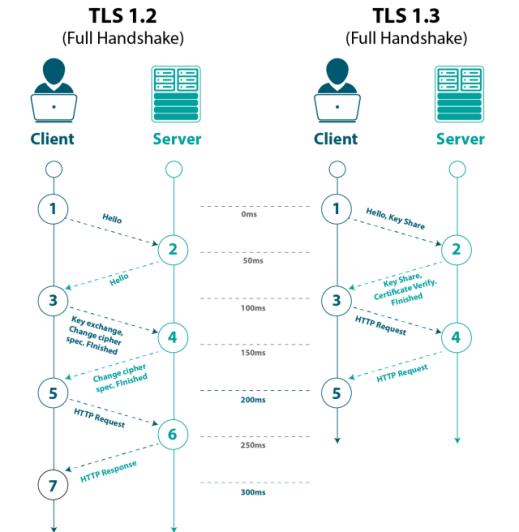
 **会话密钥的生成**

• 用途：后续通信过程的对称加密

• 来源：三个随机数（client\_random、server\_random、pre\_master\_secret）



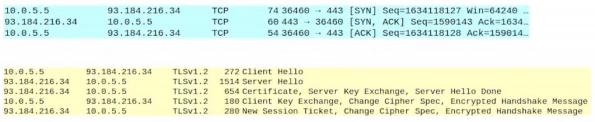
TLS握手协议（v1.3）的变化



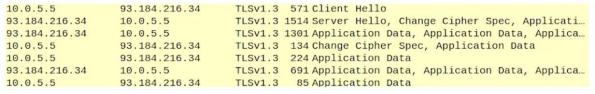
• 密钥交换：取消基于RSA的方法，使用ECDHE

• 减少步骤：客户端提前预测并使用Cipher Suite

TLS 1.2报文



TLS 1.3报文



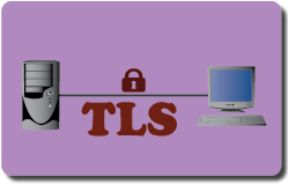
14

课程提纲

• TLS协议概览

• TLS握手

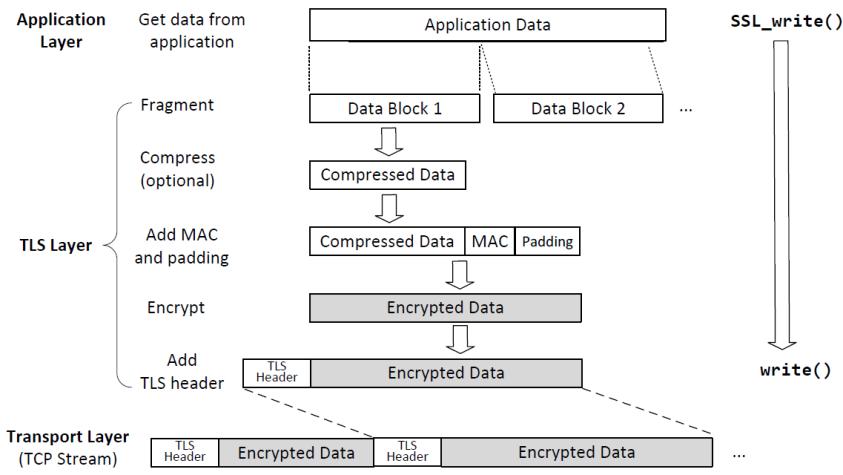
• TLS数据传输

• TLS客户端编程

• TLS服务端编程

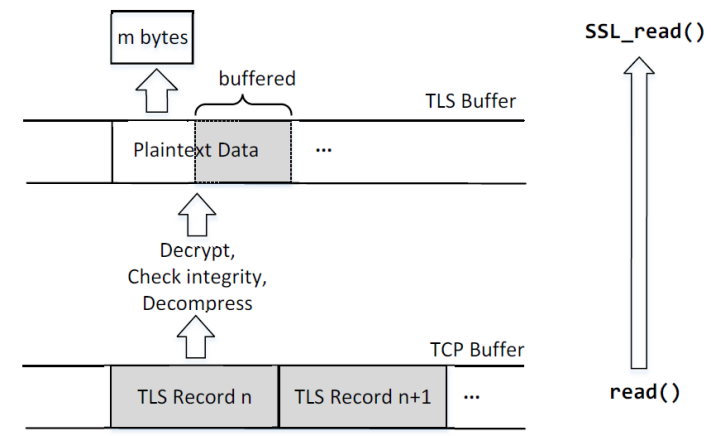
• TLS代理编程

通过TLS发送数据



• 封装 • 压缩 • 加密

通过TLS接收数据



• 解密

• 解压缩

• 完整性校验

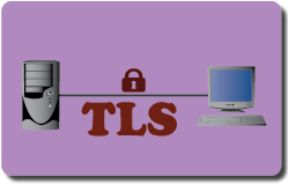
• 用户态缓存

课程提纲

• TLS协议概览

• TLS握手

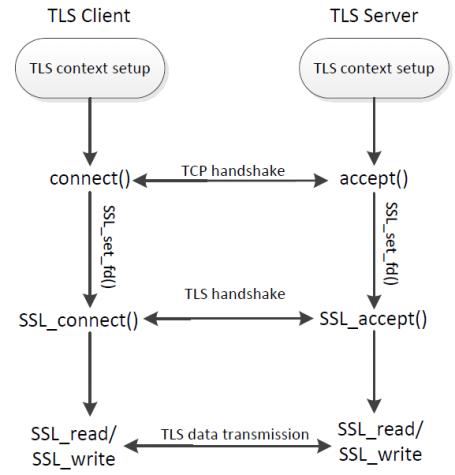
• TLS数据传输

• TLS客户端编程

• TLS服务端编程

• TLS代理编程

TLS编程总览

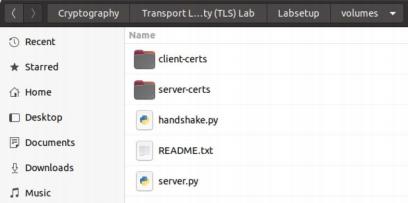


启动容器



|  |
| --- |
|  |

为降低实验难度，大部分代码已给出



|  |
| --- |
|  |

与真实网站TLS握手（实验任务一.a） 



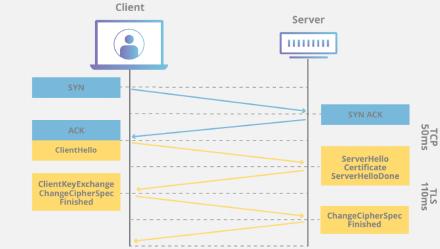
 **与真实网站（任选HTTPS）建立TLS握手连接**

• 实验步骤

① 在虚拟机VM的当前实验目录下运行hankshake.py

|  |
| --- |
| ./handshake.py www.alipay.com |

• 要求：记录程序、操作命令和输出结果，写入实验 报告，对实验现象进行解释。



20

与真实网站TLS握手（实验任务一.b） 

 **更换根证书目录**

• 实验步骤

① 修改hankshake.py的证书目录



注意：此时该目录为空

② 将此前访问网站验证时需要的根证书复制到./client-certs中，并生成哈希索引



③ 再次运行hankshake.py观察结果

• 要求：记录程序、操作命令和输出结果，写入实验报告，对实验现象进行解释。

与真实网站TLS握手（实验任务一.c） 

 **体会检查主机名称的重要性**

• 实验步骤

① 获取目标网站的IP地址



② 通过修改/etc/hosts新建一个域名指向该IP地址（也可通过DNS劫持）



③ 修改handshake.py中的check\_hostname选项



④ 运行hankshake.py观察结果

思考：如果www.example.com是钓鱼网站将会怎样？

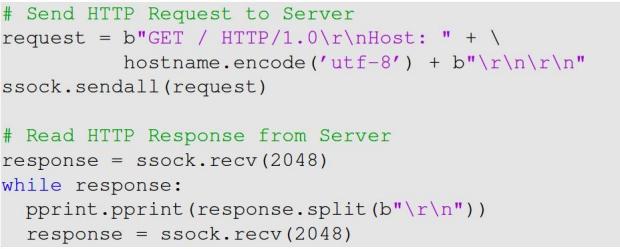
• 要求：记录程序、操作命令和输出结果，写入实验报告，对实验现象进行解释。

与真实网站TLS握手（实验任务一.d） 

 **与网站进行数据传输**

• 实验步骤

① 修改handshake.py，在TLS握手后增加收发数据代码



② 运行hankshake.py观察结果

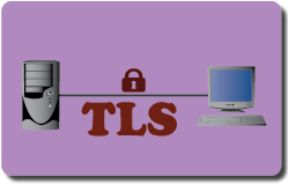
• 要求：记录程序、操作命令和输出结果，写入实验报告，对实验现象进行解释。

课程提纲

• TLS协议概览

• TLS握手

• TLS数据传输

• TLS客户端编程

• TLS服务端编程

• TLS代理编程

搭建一个TLS服务端（实验任务二.a） 

 **搭建一个TLS服务端**

• 实验步骤

① 为服务端生成证书，放置./server-certs/目录

会用到PKI实验中的内容

② 在server容器中运行server.py



③ 在虚拟机上修改/etc/hosts

④ 利用实验任务一中client与服务端对话

注意：需将根证书导入到./client-certs中

• 要求：记录程序、操作命令和输出结果，写入实验 报告，对实验现象进行解释。

搭建一个TLS服务端（实验任务二.b） 

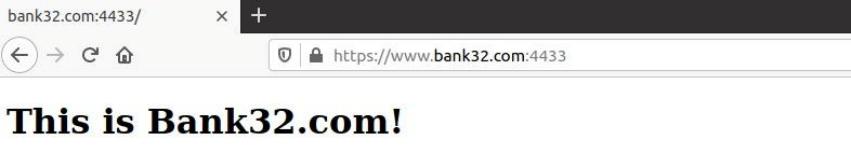
 **用浏览器打开测试**

• 实验步骤

① 在虚拟机上打开浏览器，输入地址（注意端口号是4433）



② 检查出现的问题，尝试进一步修复（PKI实验中的内容）



|  |
| --- |
|  |

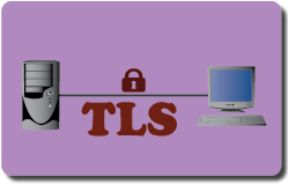
• 要求：记录程序、操作命令和输出结果，写入实验报告，对实验现象进行解释。

课程提纲

• TLS协议概览

• TLS握手

• TLS数据传输

• TLS客户端编程

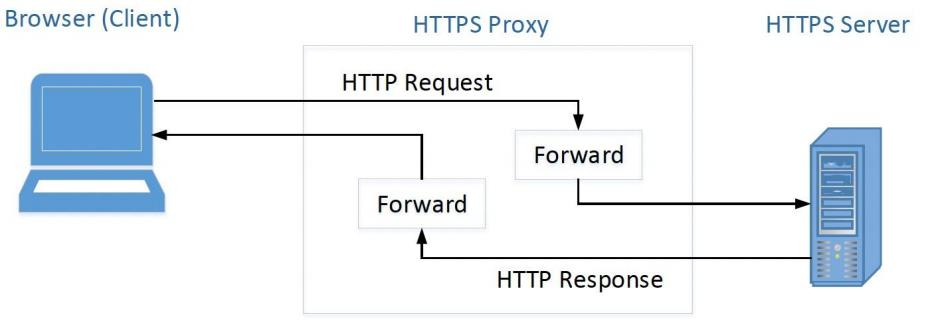
• TLS服务端编程

• TLS代理编程

TLS代理（MITM代理）





Proxy’s Root CA

搭建一个TLS代理（实验任务三） 



 **搭建一个TLS代理**

• 实验步骤

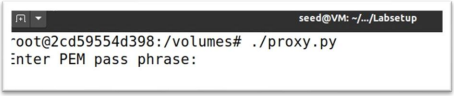
① 为目标网站（如www.example.com）颁发一个证书

② 修改客户端（可直接用虚拟机）的DNS配置文件/etc/hosts



|  |
| --- |
|  |

③ 在mitm-proxy容器内运行TLS代理程序



④ 通过浏览器访问目标网站（注意：需导入步骤 1中签发者的根证书）

• 要求：记录程序、操作命令和输出结果，写入实验报告，对实验现象进行解释。

小结

• TLS握手（v1.2 v.s. v1.3)

• 密钥协商和服务器认证

• TLS数据传输

• TLS客户端和服务端编程（Python)

• MITM代理

注意：为避免影响后续实验，请清除本实验用过的VM相关配置（恢复/etc/hosts，删除ModelCA根证书） 30