



本学期实验总体安排



- 实验指导书链接: <https://network-security.p.cs-lab.top/>
- SEED实验室的链接:
 - <https://seedsecuritylabs.org/>
 - <https://seedsecuritylabs.org/chinese/>
- 实验提交地址 (校内网/VPN) : <http://grader.tery.top:8000/#/login>



只有敲代码才能
感受到温暖



哈爾濱工業大學(深圳)
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

网络安全实验

Lab5 TLS

CONTENTS

目录

「01」

实验目的

「02」

实验任务

「03」

实验原理

「04」

作业提交



实验目的



- 了解TLS的工作原理；
- 通过抓包分析，理解TLS握手过程中的各字段的含义；
- 掌握TLS协议的工作过程。



只有敲代码才能
感受到温暖



实验任务



- 任务1：完成TLS客户端的握手抓包分析过程和TLS的证书验证过程，并理解分析TLS的客户端编程；
- 任务2：利用多种方式完成TLS的服务器端响应客户端的过程，并理解分析TLS的服务器端编程。



只有敲代码才能
感受到温暖



1 TLS协议

数据在互联网中传输时如果未受到保护，很容易被其他人读取甚至修改。应用程序为了保证通信的安全性，需要加密数据并且检测数据的完整性。这可以用密码算法来实现，但是密码算法众多，就算同一种密码算法也可有不同的参数。

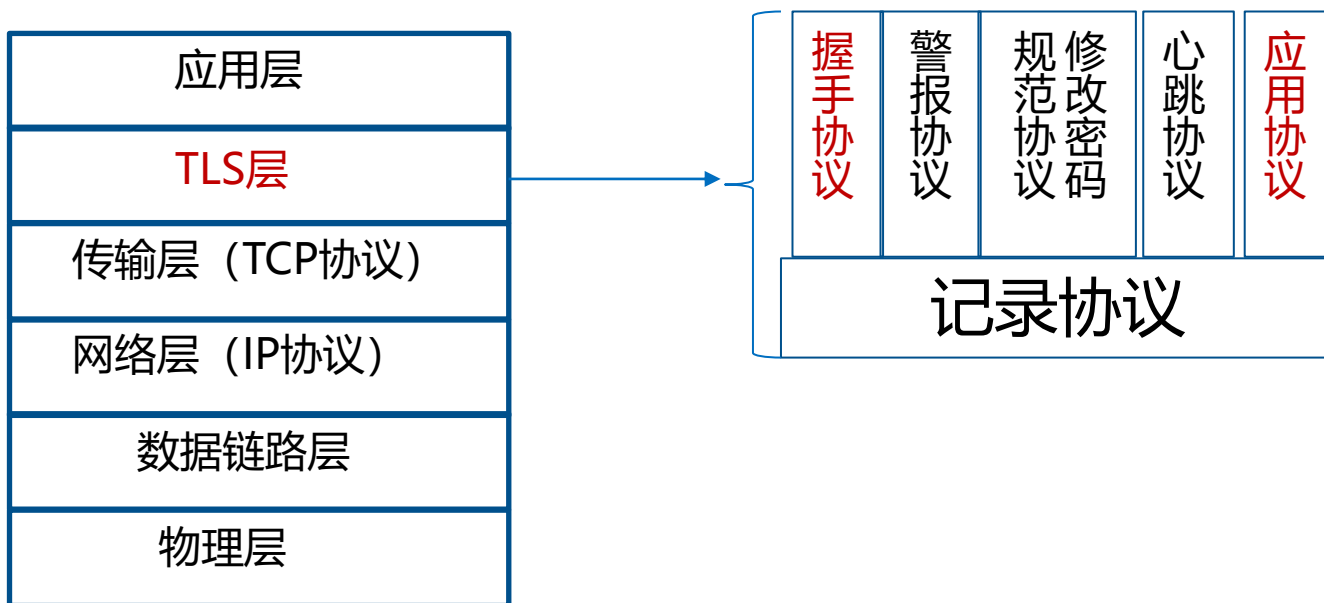
为了方便不同的应用程序之间彼此通信，它们需要遵循一个共同的标准。传输层协议（Transport Layer Security, TLS）就是这样一个标准。





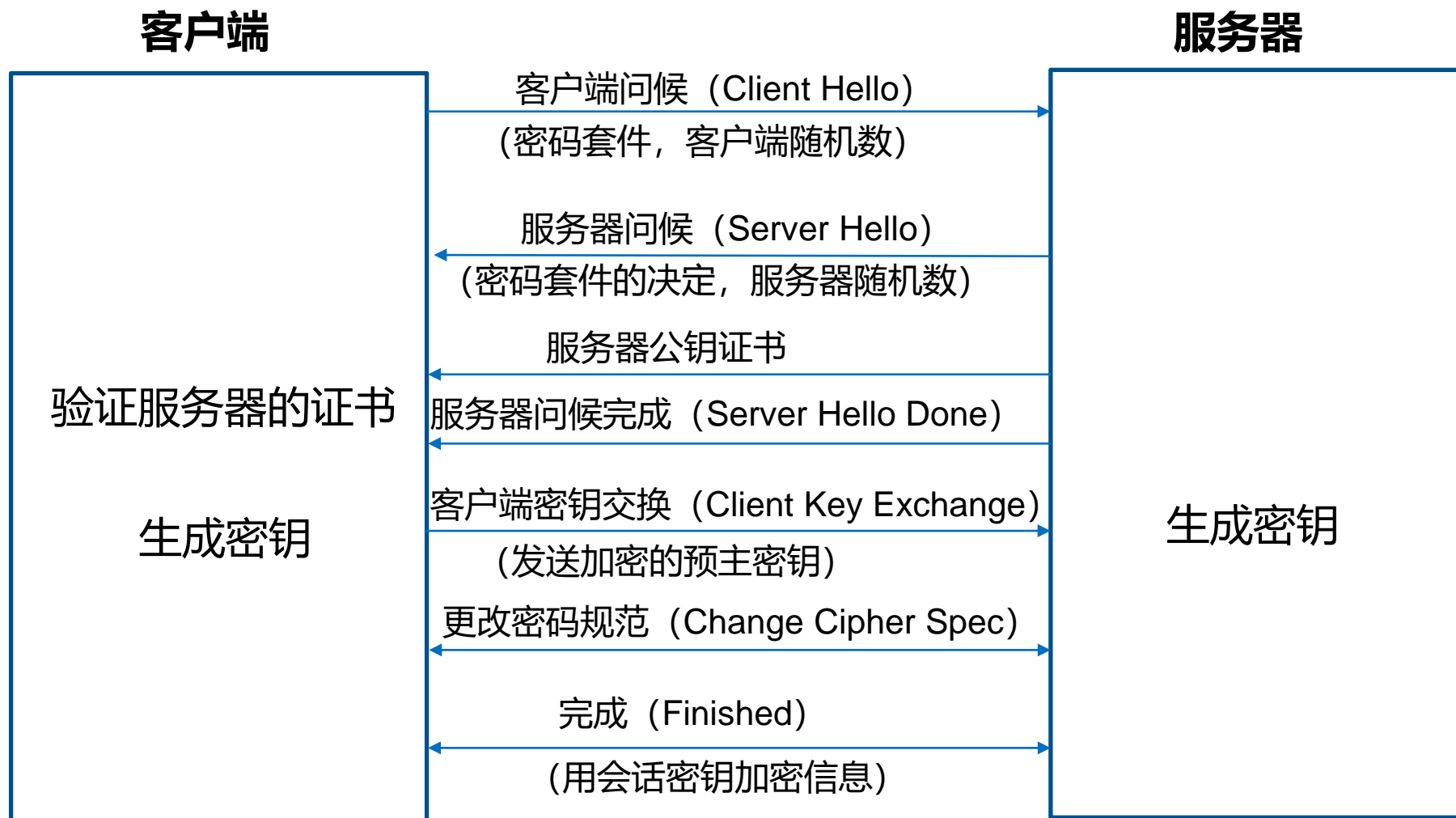
1 TLS协议

TLS位于应用层和传输层之间，应用程序将未受保护的数据传递给TLS层，TLS层负责**加密、解密和完整性检查**，然后将受保护的数据提供给传输层进行传输。





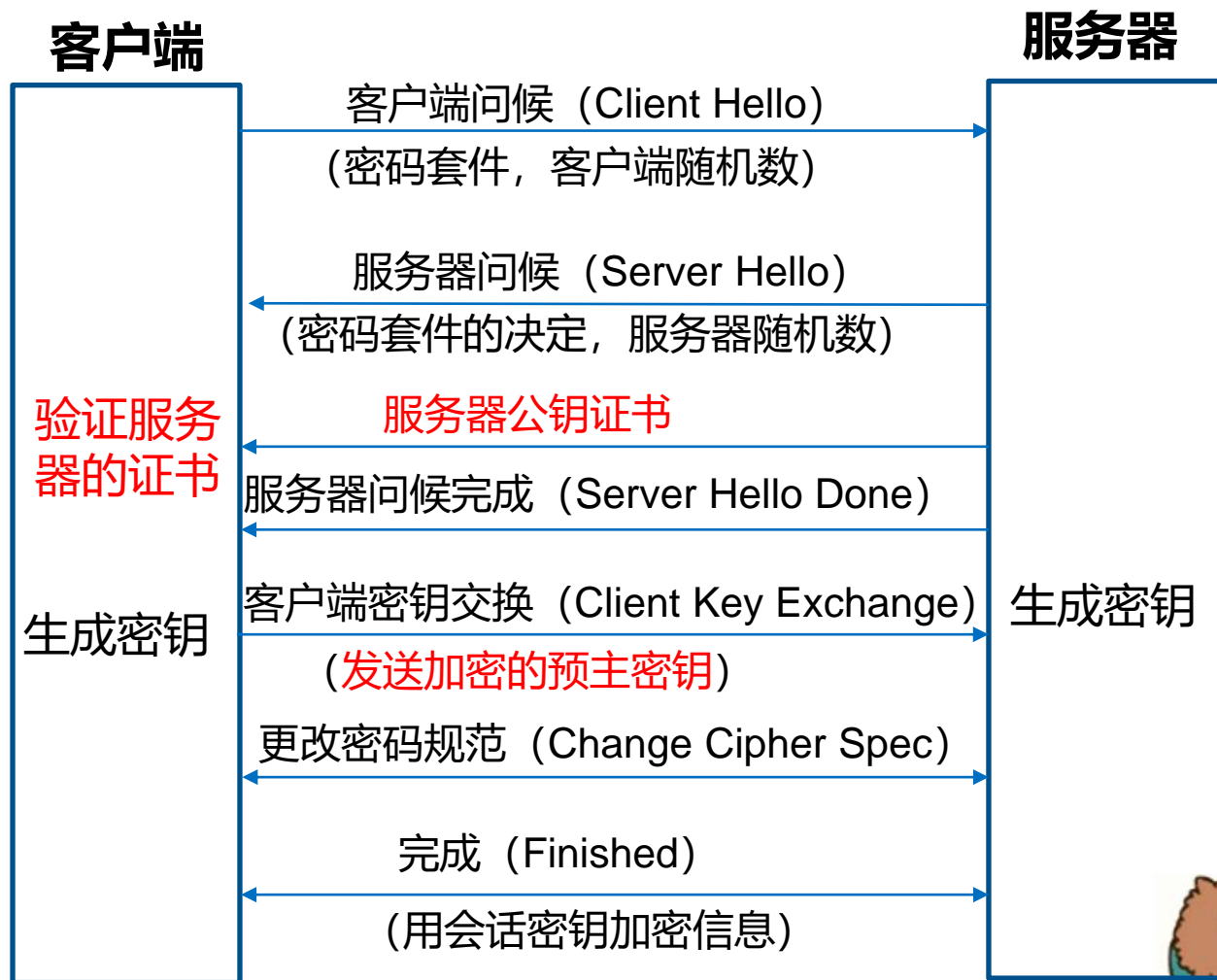
2 ➤ TLS握手：目的是让客户端和服务端共同商定加密参数并生成会话密钥



2 ➤ TLS握手 ---- 证书验证

为什么服务器要发送公钥证书？

- 在第五步，预主密钥在发送给服务器时用服务器的公钥进行加密。
- 如果直接发送公钥可能会受到中间人攻击，因此服务器应该发送其公钥证书。

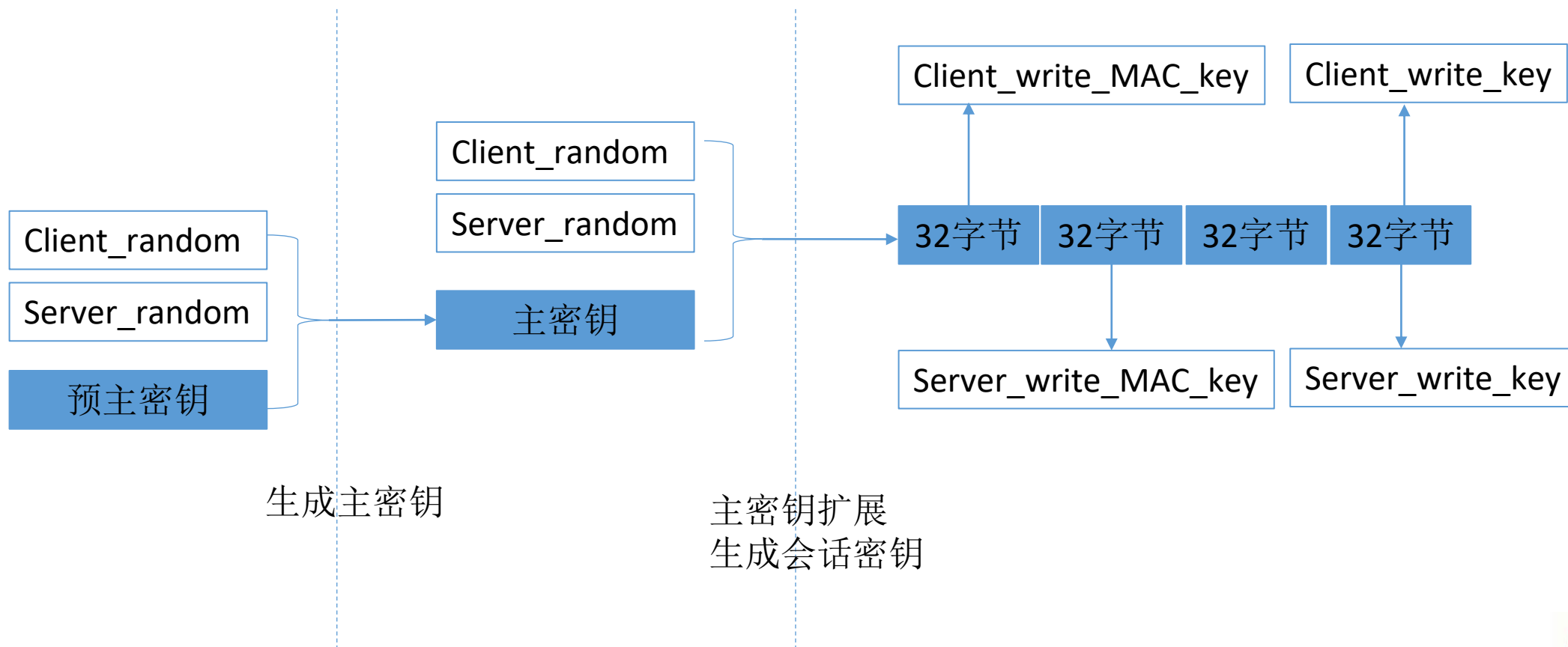


安全隐患： 只检查证书是否有效，但是并不检查证书中身份信息。





2 ➤ TLS握手 ---- 密钥生成和交换





实验原理

3

➤ TLS数据传输

应用层

提供数据

TLS层

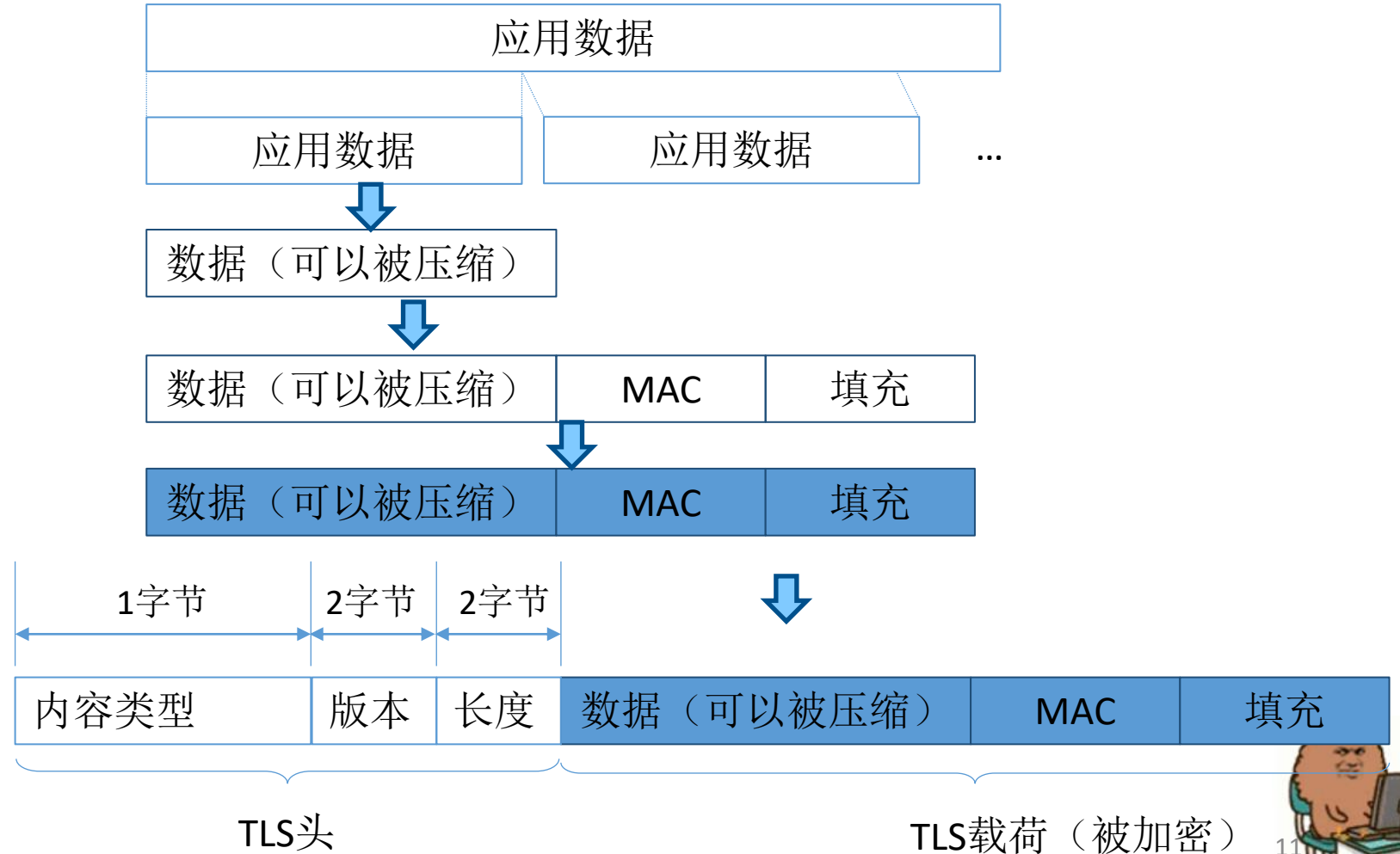
数据分块

数据压缩
(可选)

添加MAC
和填充

加密

添加TLS头



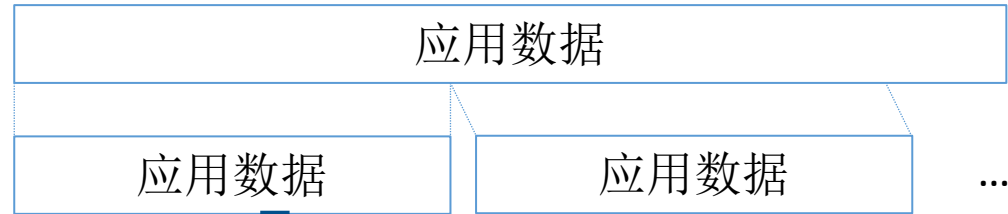
只有敲代码才能
感受到温暖



实验原理

3 ➤ TLS数据传输

应用层 提供数据



TLS层

数据分块

数据压缩
(可选)

添加MAC
和填充

加密

添加TLS头

数据 (可以被压缩)

数据 (可以被压缩) MAC 填充

数据 (可以被压缩) MAC 填充

TLS头 加密的数据

传输层



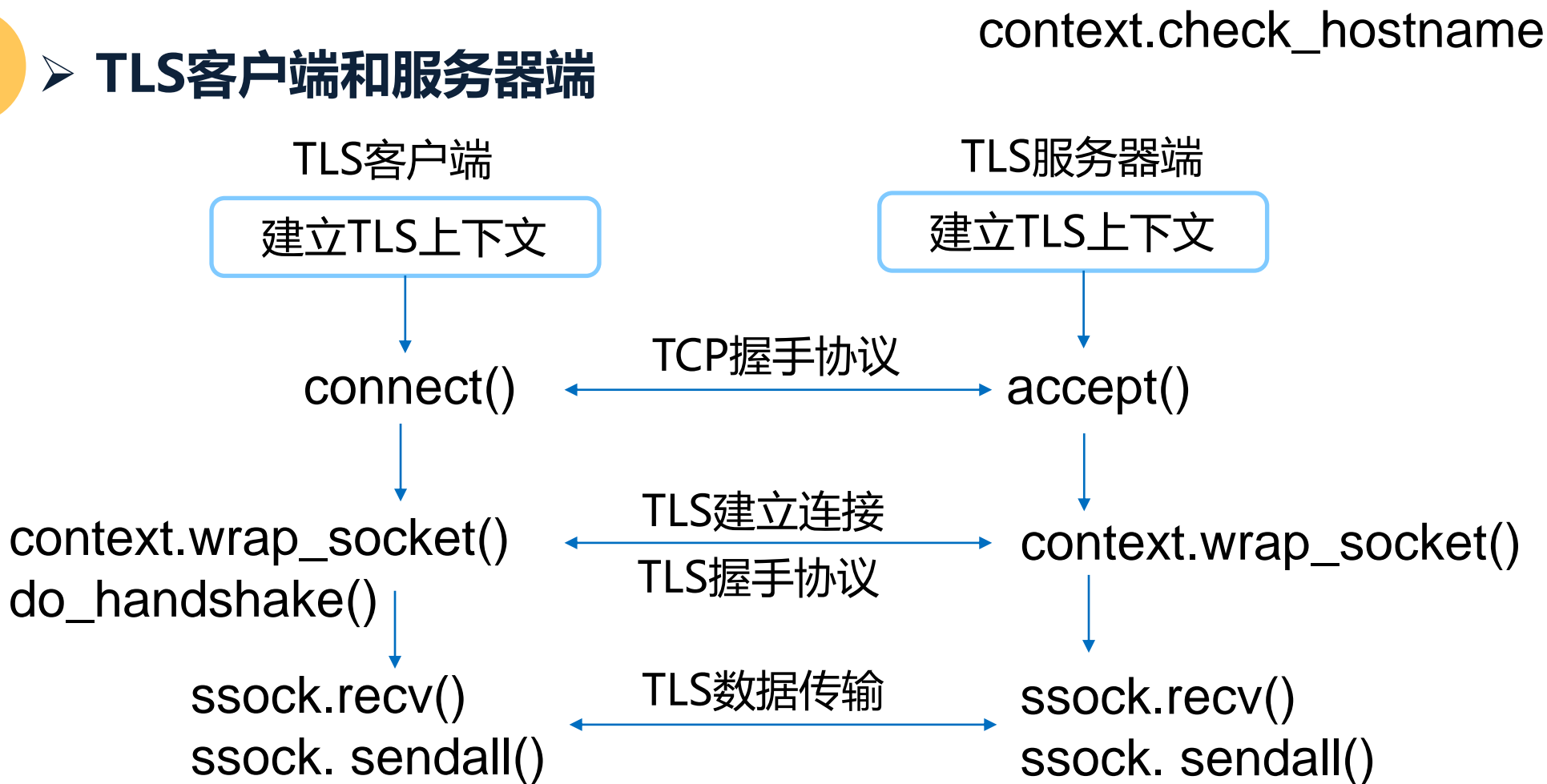
12

只有敲代码才能
感受到温暖



4

➤ TLS客户端和服务端端





Task1 TLS 客户端

Task1.1 TLS握手

Task1.2 TLS协议中的CA认证

Task1.3 TLS认证中的校验服务器的主机名

Task1.4 利用TLS协议传输应用数据

Task2 TLS 服务器端

Task2.1 实现一个简单的TLS服务器

Task2.2 利用主机浏览器测试实现的TLS服务器

Task2.3 测试服务器有别名的情况





作业要求



提交内容：实验报告（有模板）

截止时间：

实验课后一周内提交至HITsz Grader 作业提交平台，具体截止日期参考平台发布。

- 登录网址：： <http://grader.tery.top:8000/#/login>
- 推荐浏览器： Chrome
- 初始用户名、密码均为学号，登录后请修改

注意

上传后可自行下载以确认是否正确提交



只有敲代码才能
感受到温暖



**同学们
请开始实验吧！**