《安全协议模型与设计》课程概述

汪　定

南开大学 网络空间安全学院

2021年11月6日

教育工作经历

教育经历

2004-2008	南开大学	信息安全	本科
2010-2013	哈尔滨工程大学	信息安全	硕士
2013-2017	北京大学	信息安全	博士

工作经历

2017-2018	中国移动	信息安全中心项目经理
2018-2019	北京大学	讲师，“博雅”博士后
2019-至今	南开大学	教授，博士生导师，青年学科带头人
	网络与数据安全技术天津市重点实验室	副主任

提 纲

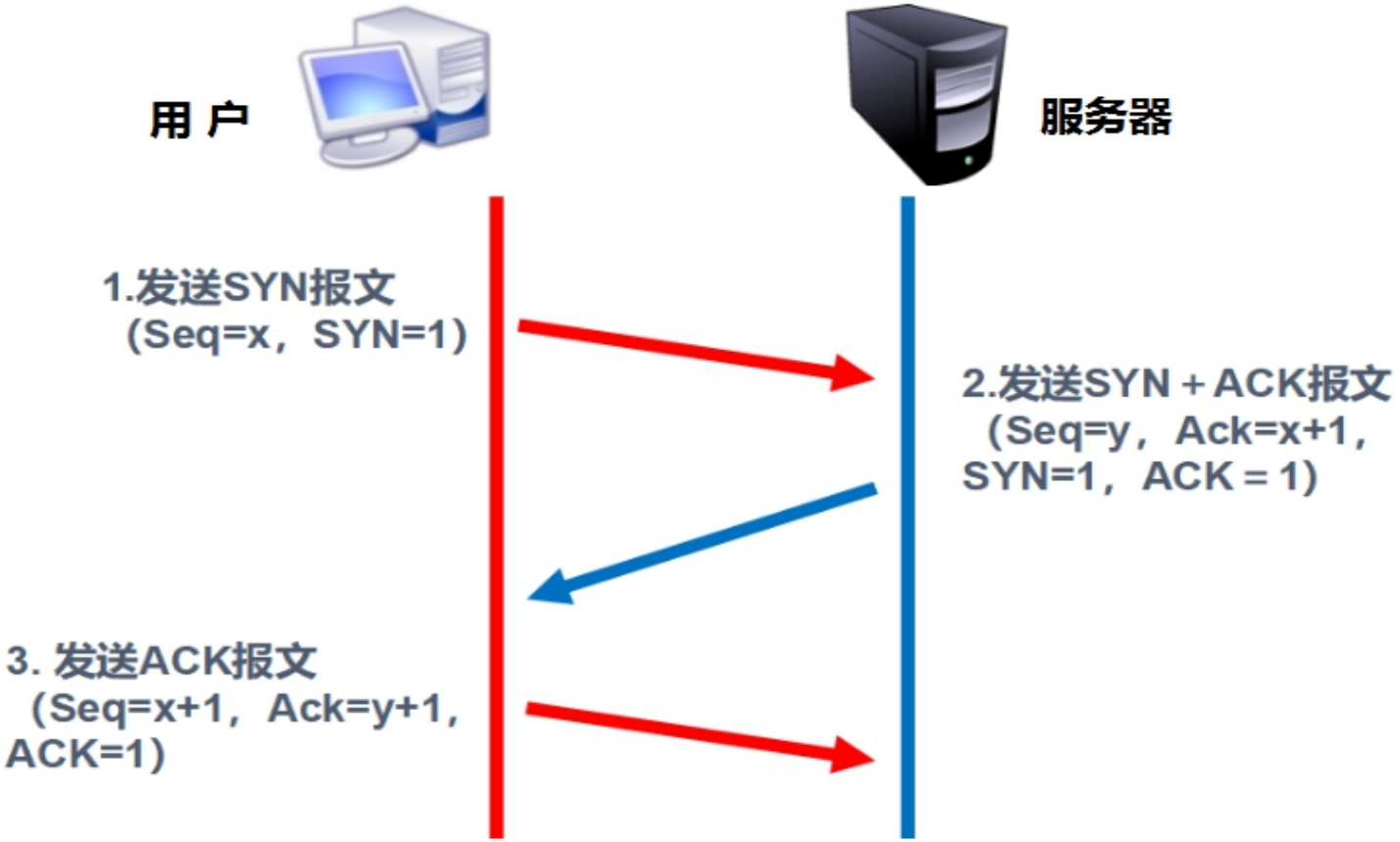
CONTENTS

1. 课程认识
2. 课程大纲
3. 重点内容
4. 教学目的

什么是协议？

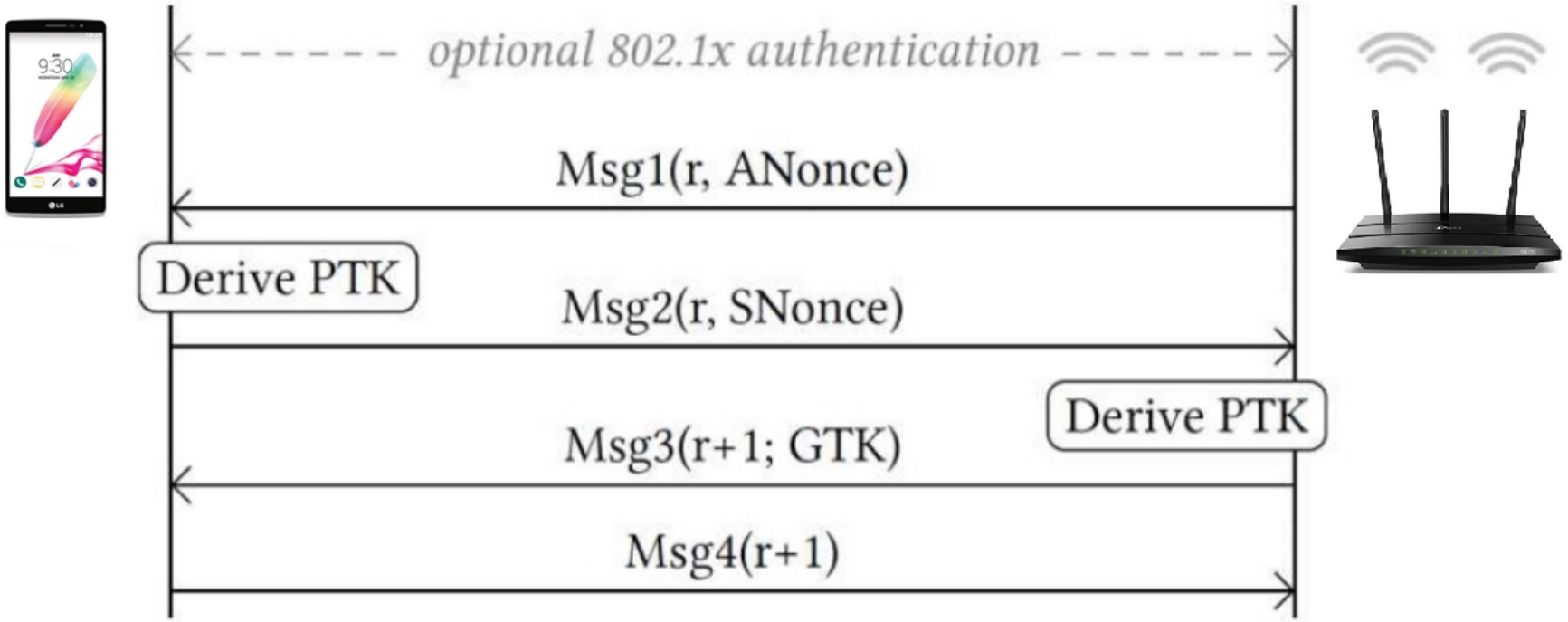
- Protocol, 协议

两个或两个以上的参与者为完成某项特定任务而采取的一系列步骤。



什么是安全协议？

WiFi 认证四步握手协议



- Security Protocol, 安全协议

  具有安全功能的协议。

安全协议 = 密码协议

- 安全协议的别名
  - 具有安全功能的协议——安全协议
  - 安全协议的设计一般采用密码技术——也称密码协议
  - 具体意义：密码协议是建立在密码体制基础上的一种交互通信的协议，它运行在计算机通信网或分布式系统中，借助于密码算法来达到安全功能。

- **密码技术：** 随机数生成、加密/解密算法、Hash运算、数字签名等 。
- **安全协议功能：** 身份认证、消息认证、密钥建立、隐私保护等。
- **应用系统：** 电子货币、电子选举、电子拍卖、电子银行等。

安全协议 vs. 网络协议

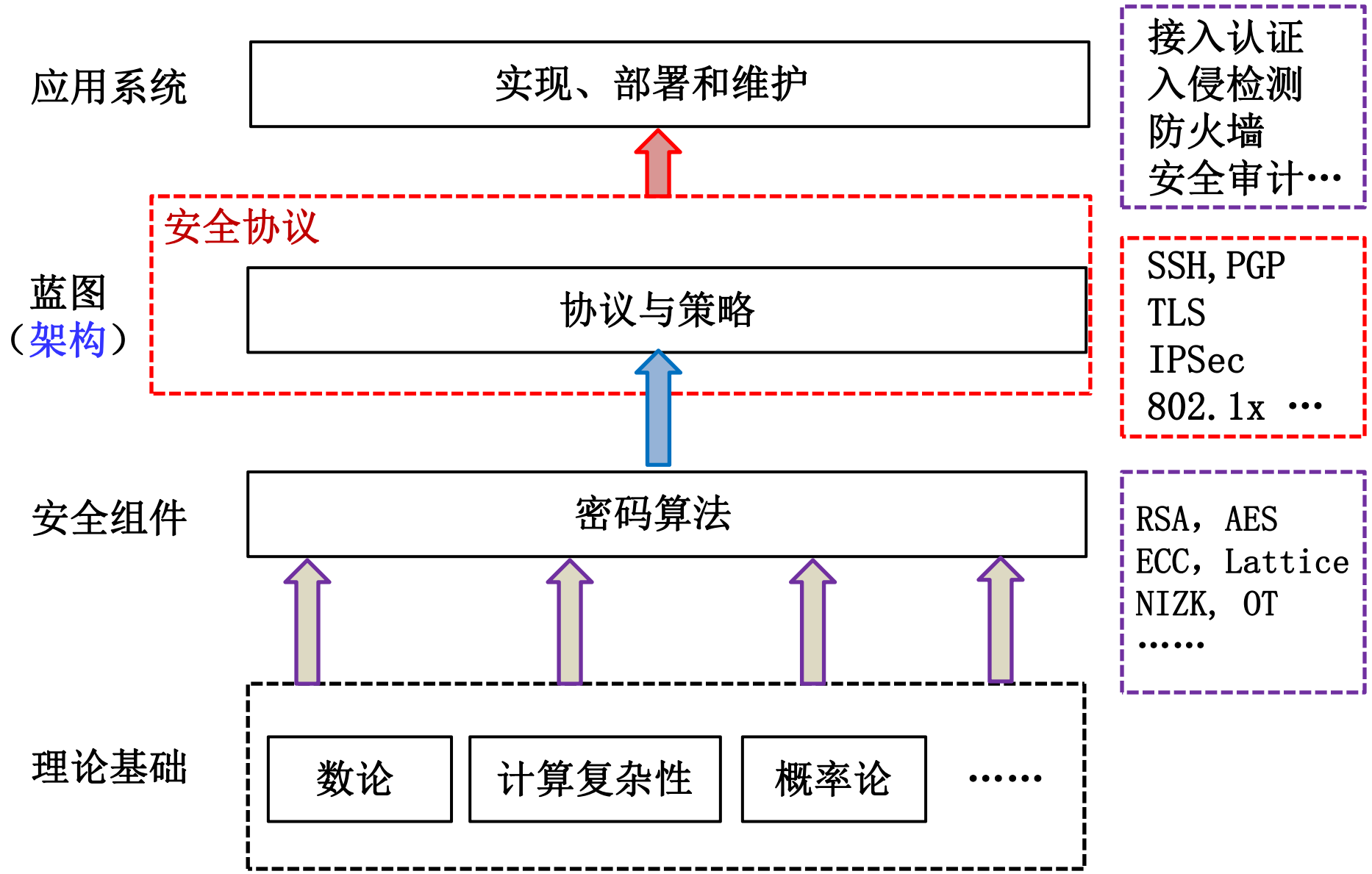
- 网络协议——实现网络通信功能的协议

OSI七层网络模型	TCP/IP四层概念模型	对应网络协议
应用层(Application)	应用层	HTTP、FTP、TFTP、DHCP、NTP、POP3、IMAP4、SNMP、SMTP、DNS、
表示层(Presentation)		
会话层(Session)		
传输层(Transport)	传输层	TCP、UDP
网络层(Network)	网络层	IP、ICMP、ARP、RARP、OSPF、VRRP、IGMP、BGP
数据链路层(Data Link)	网络接口层	PPP、PPTP
物理层 (Physical)		

- 安全协议——实现安全功能的协议

OSI七层网络模型	TCP/IP四层概念模型	对应的安全传输协议
应用层(Application)	应用层	SSH, PGP, 微信的安全传输协议, ……
表示层(Presentation)		
会话层(Session)		
传输层(Transport)	传输层	TLS, SSL
网络层(Network)	网络层	IPSec
数据链路层(Data Link)	网络接口层	L2TP、802.1x(WiFi)
物理层 (Physical)		

在网络空间安全知识体系中的位置



课程大纲

课程基本情况

- 课程名称：安全协议模型与设计
- 英文名称：Model and Design of Security Protocols
- 课程编码：CSSE0014
- 课程属性：专业选修课
- 共8个章节，每章4学时，共32学时
- 考试形式：期末笔试 50% + 平时成绩20% + 课程实践 30%

课程内容设置

- 第一部分：概论和基础，即第1、2章
- 第二部分：四类重要协议，即第3~6章
- 第三部分：两个实际应用，即第7、8章

重点内容

第一章 安全协议概论

1.1 密码学基础

1.2 安全协议基本概念和工具

第二章 基础安全协议

2.1 不经意传输

2.2 隐私信息提取

2.3 承诺

2.4 零知识证明

重点内容（2）

第三章 认证

3.1 基本概念

3.2 身份认证

3.3 密钥建立

第四章 隐私保护

4.1 匿名协议

4.2 位置隐私保护

第五章 数据审计

5.1 数据审计

5.2 静态数据审计

第六章 安全多方计算

6.1 安全性定义与模型

6.2 泄露容忍安全性

6.3 通用可组合安全性

第七章 安全传输层协议国际标准

7.1 标准协议解读

7.2 攻击和分析

7.3 最新进展

第八章 比特币与区块链

8.1 比特币中的密码学协议

8.2 区块链技术

8.3 区块链技术进阶

教学目的和要求

- 目的

  使学生理解安全协议模型的基本思想，系统地掌握安全协议的设计与分析方法，为进一步学习、研究和工作奠定基础。

- 要求
  - 理解身份认证、隐私保护、数据审计和安全多方计算等领域的经典协议
  - 掌握协议的攻击方法和改进措施
  - 熟悉这些安全协议的设计原则和方法
  - 知悉安全协议领域最新重要进展
  - 深刻理解安全协议在解决现实安全问题中的重要作用

请各位同学交流指正！

邮箱：wangding@nankai.edu.cn
房间：计算机楼602