信息安全概论

Introduction to Information Security

主讲教师：赵 彦 锋

院　　系：信息工程学院 软件工程系

邮　　箱：c_zhaoyf@163.com

2021 年 03 月

第一周

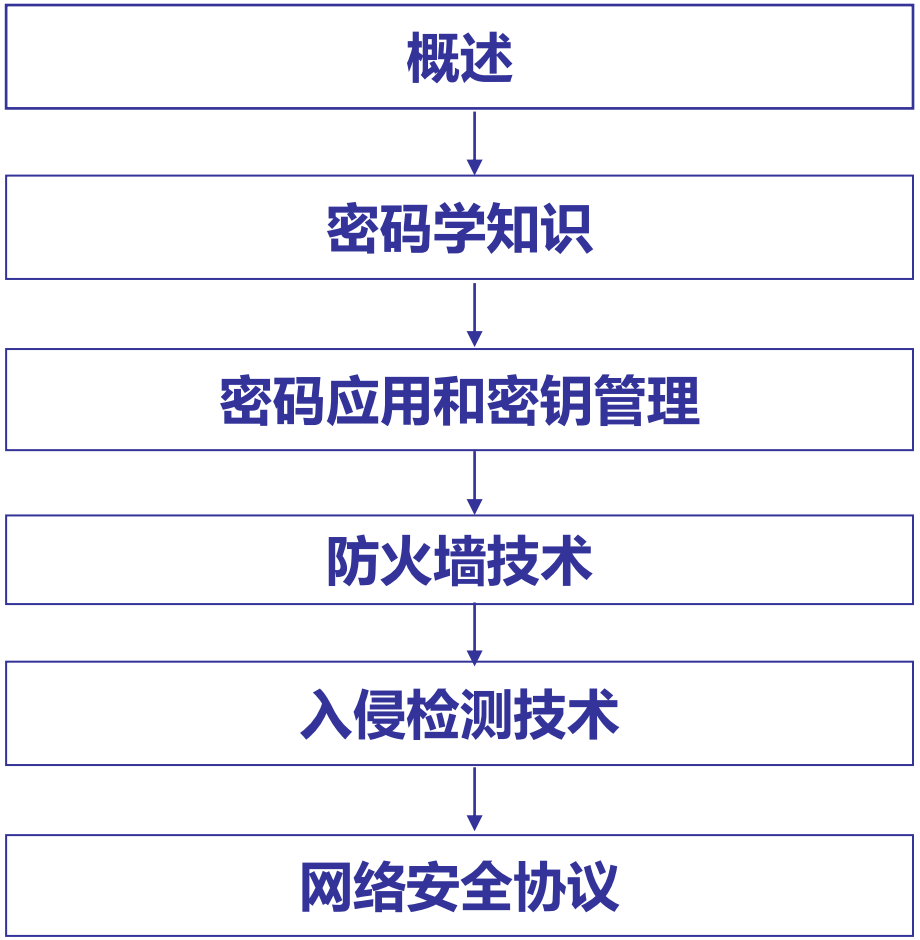
1.1 课程导学

一、信息安全概论---课程简介

信息安全概论课程是一门学科基础课（选修），课程在介绍信息安全的基本概念、研究内容及其发展的基础上，重点介绍了信息的保密性技术（密码理论）、信息的完整性技术（消息认证）、信息的抗否认性技术（数字签名）、防火墙技术和入侵检测技术等内容。课程内容由四大部分组成：

- 第一部分是概述，介绍了信息安全的概念、目标和发展；
- 第二部分介绍了密码学知识、对称密码体制和公钥密码体制；
- 第三部分介绍了密码应用和密钥管理；
- 第四部分介绍了网络安全技术和协议。

二、信息安全概论---知识图



三、信息安全概论---课程内容

一、概述：信息安全的目标、信息安全研究内容及发展。

二、密码学概论：基本概念、经典密码体制、密码分析。

三、对称密码体制：分组密码的原理、DES算法、分组密码的工作模式、流密码简介。

四、公钥密码体制：基本原理，RSA算法，ElGamal密码体制。

五、消息认证和数字签名：消息认证、HASH函数、数字签名体制。

六、密码应用和密钥管理：密码应用、密钥管理、公钥基础设施PKI。

七、防火墙技术：防火墙概述、防火墙技术及分类。

八、入侵检测技术：入侵检测原理、入侵检测技术。

九、网络安全协议：安全协议概述、IPSec协议、SSL协议及应用。

四、信息安全概论---教学基本要求

- 了解信息安全的重要性；
- 理解实现信息保密性、完整性和抗否认性的密码学原理；
- 掌握消息认证、数字签名的方法；
- 掌握基于机器学习的入侵检测系统和僵尸网络检测的实现原理和方法；
- 了解常用的网络安全协议及其应用现状。

五、信息安全概论---课程学习方法

- 建立网络信息安全观；
- 以实际需求（案例）学习相关安全技术；
- 充分利用优质的在线学习资源，建立“以学生为中心”的教与学模式；
- 注重理论与实践的结合，在大数据背景下充分利用开源在线开发平台完成课程实践任务。

六、信息安全概论---课时安排

- 总课时：32学时
- 讲　授：26学时（线上学习8学时，翻转2学时，线下学习16学时）
- 上　机：　6学时（基于机器学习的IDS实现、基于深度学习的BOTNET）

七、信息安全概论---学习要求

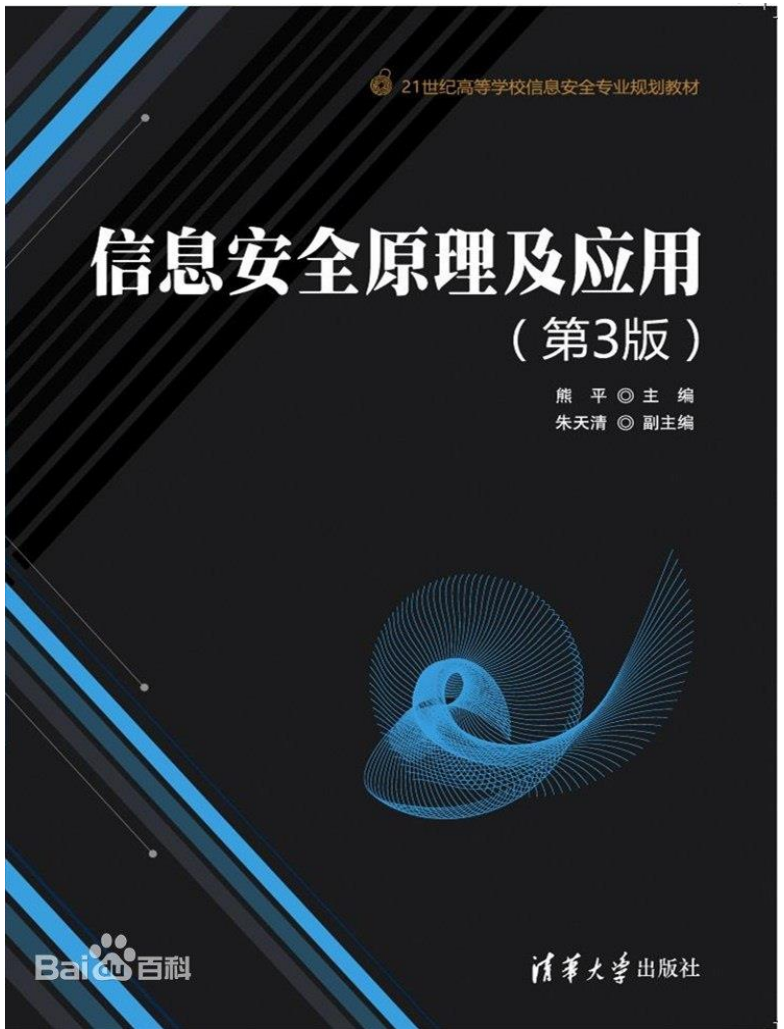
- 线上学习（平台数据）：及时观看视频、完成在线测试和积极参与线上讨论；
- 线下学习（教师数据）：实体课堂、翻转课堂和实践环节。

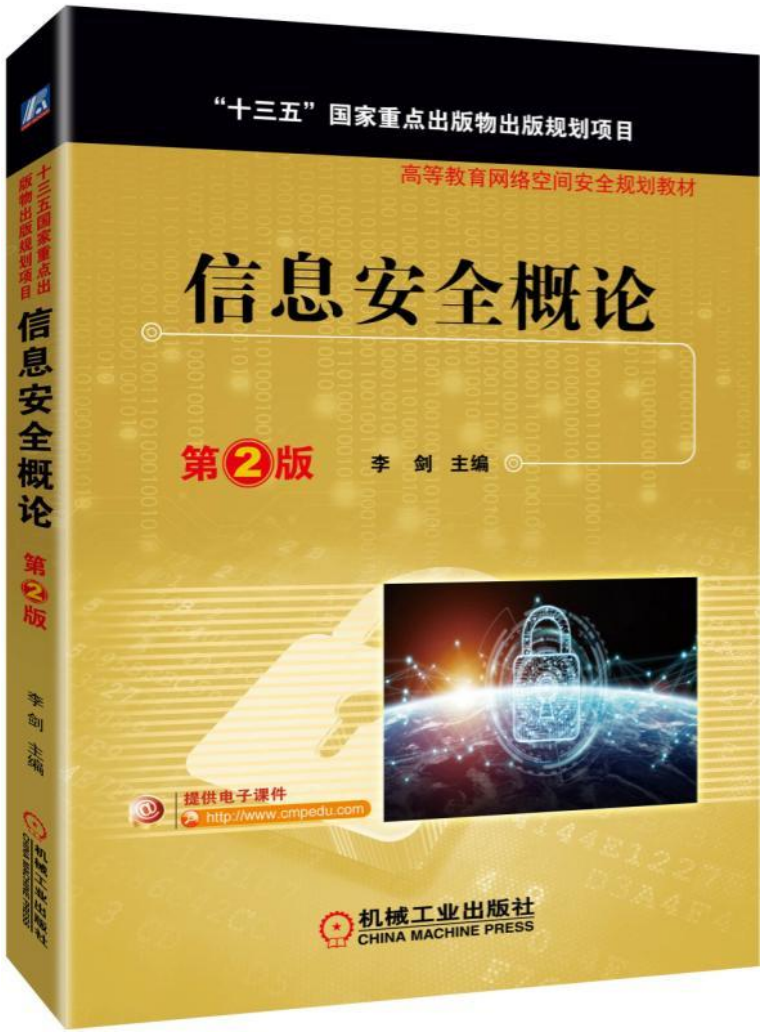
八、信息安全概论---考核

- 平时：50%（线上学习情况、课堂讨论、在线测试、作业、上机、考勤）
- 期末：50%（期末考试）

九、信息安全概论---教材和参考书

- 《信息安全原理及应用》第3版，熊平著，清华大学出版社。
- 《信息安全概论》第2版，李剑，机械工业出版社。





第一周

1.2 信息安全概述

1.2 信息安全概述---信息

- 目前,信息的定义还不统一；
- 在信息社会，信息成为社会发展的重要战略资源；
- 信息是经过加工（获取、推理、分析、计算、存储等）的特定形式数据，是物质运动规律的总和。信息的主要特点具有时效性、新知性和不确定性，信息是有价值的；
- 信息是主观世界和客观世界联系的桥梁，客观世界中不同事物都具有不同的特征，这些特征给人们带来不同的信息，而这些信息使人们能够认识客观事物；

- **信息安全的定义：**是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。
- **信息安全**是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、数学等多门学科的综合性学科。

1.2 信息安全概述---信息的安全威胁

物理因素

网络因素

系统因素

应用因素

管理因素

物理因素：

- 地震、水灾、火灾等环境事故造成设备损坏；
- 电源故障造成设备断电以至操作系统引导失败或数据库信息丢失；
- 设备被盗、被毁造成数据丢失或信息泄露；
- 电磁辐射可能造成数据信息被窃取或偷阅；
- 监控和报警系统的缺乏或者管理不善造成的事故。

网络因素：

- 数据在传输中，线路搭载、链路窃听可能造成数据被截获、窃听、篡改和破坏，数据的保密性、完整性无法保证；
- 网络边界若没有强有力控制，则外部攻击者可随意出入网络系统，从而获取各种数据和信息；
- 运行Web服务、数据库服务的平台，如不加防范，各种网络攻击可能对业务系统服务造成干扰、破坏，如DoS和DDoS。

系统因素：

- 操作系统在参数、服务配置中，缺省地开放一些端口，存在很大安全隐患和风险；
- 操作系统在设计和实现方面存在的漏洞；
- 数据库系统及相关商用产品的安全漏洞、病毒的威胁。

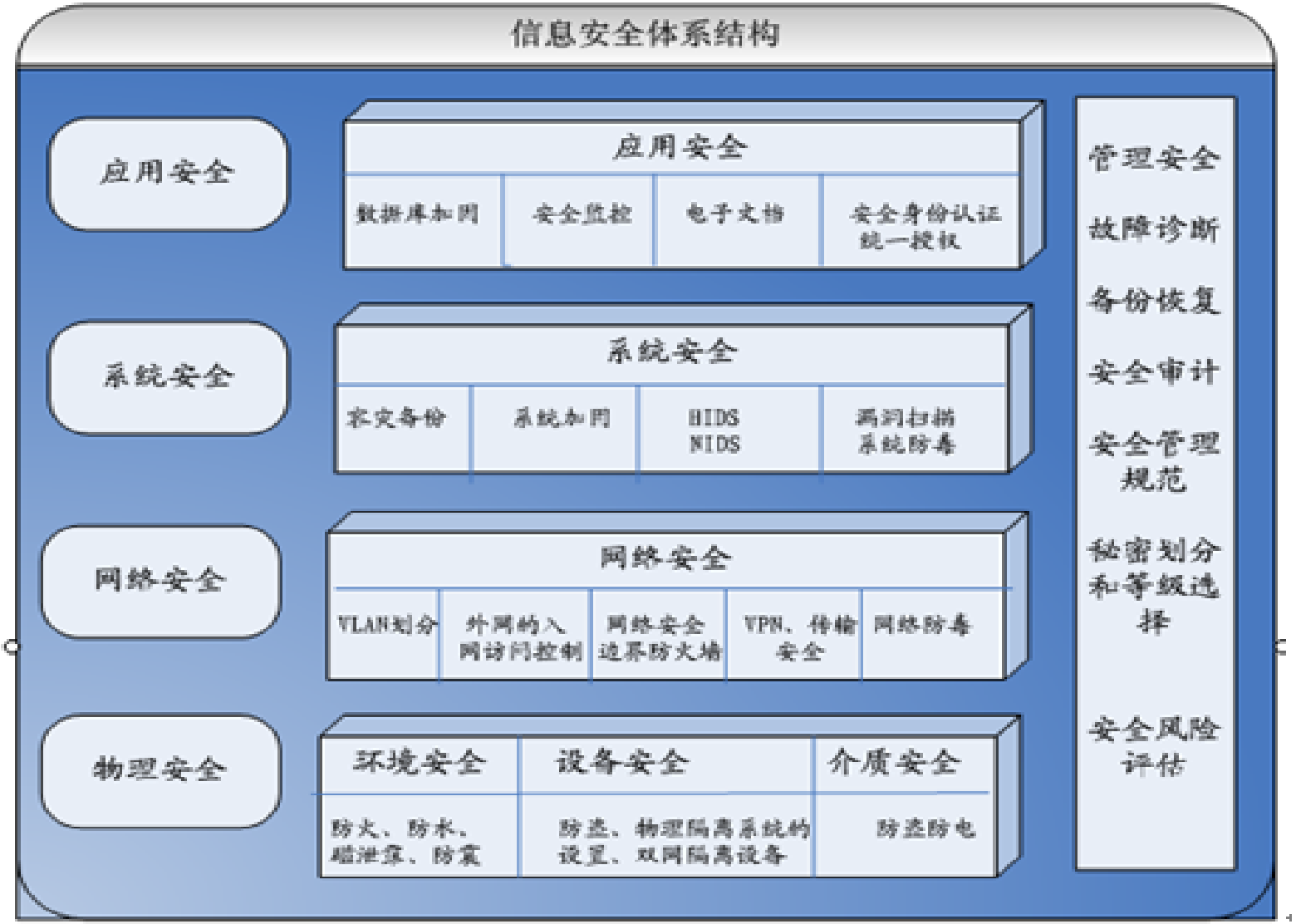
应用因素：

- 基于业务的数据交互和信息服务若不加以安全保护，会收到网络的入侵、威胁及数据泄密；
- 数据库服务器的非授权用户访问、自身的漏洞、数据丢失等；
- 信息系统访问控制风险，如非法用户非法访问和合法用户非授权访问。

管理因素：

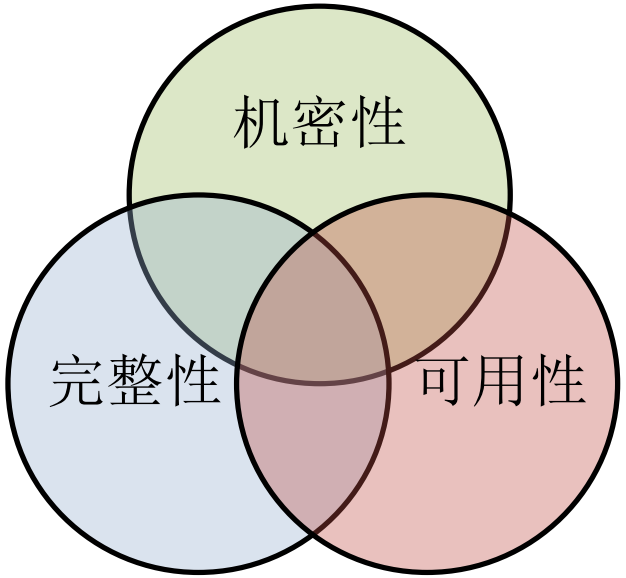
- 为防止来自内部网络的入侵，应加强网络安全管理，从制度、责任、权限、业务保障和维护规范性等方面加强安全管理能力。

1.2 信息安全概述---信息安全体系结构



➢信息安全究竟研究哪些方面？普遍的观点是：

信息安全的目标是保护信息的**机密性**（confidentiality）、**完整性**(integrity)、**可用性**(availability)；**CIA**



- **机密性**：保证信息不被非授权访问；即使非授权用户得到信息也无法知晓信息内容，因而不能使用。通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容。
- **完整性**：维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改。一般通过访问控制阻止篡改行为，同时通过消息摘要算法检验信息是否被篡改。
- **可用性**：指保障信息资源随时可提供服务的特性，即授权用户根据需要可以随时访问所需信息。是信息资源服务功能和性能可靠性的度量，

在不同的信息系统根据其业务类型可能还有更加细化的要求：

- **可靠性**：是指系统在规定条件下和规定时间内、完成规定功能的概率。
- **可审查性**：使用审计、监控、防抵赖等安全机制，使得使用者（包括合法用户、攻击者、破坏者、抵赖者）的行为有证可查，并能够对网络出现的安全问题提供调查依据和手段。
- **可控性**：是对信息及信息系统实施安全监控。管理机构对危害国家信息的来往、使用加密手段从事非法的通信活动等进行监视审计，对信息的传播及内容具有控制能力。

信息安全的目标是保护信息的**机密性**（confidentiality）、**完整性**(integrity)、**抗否认性**(non-repudiation)、**可用性**(availability)；

- **抗否认性**：指能保障用户无法在事后否认曾经对信息进行生成、签发、接收等行为，是针对通信各方信息真实同一性的安全要求。一般通过数字签名来实现。

常见攻击分类

- 口令破解：攻击者可通过获取口令文件，用破解工具获得口令。
- 连接盗用：在合法的通信连接建立后，攻击者可通过阻塞或摧毁通信的一方来接管已经通过认证的连接。
- 服务拒绝：攻击者可直接或通过控制其他主机发起攻击使目标瘫痪。

常见攻击分类

- 网络窃听：网络的开放性使攻击者可通过直接或间接窃听获取所需信息。
- 数据篡改：攻击者可通过截获并修改数据或重放数据等方式破坏数据的完整性。
- 地址欺骗：攻击者可通过伪装成被信任的IP地址等方式来骗取目标的信任。
- 社会工程：攻击者可通过各种社交渠道获得有关目标的结构、使用情况、安全防范措施等有用信息，从而提高攻击成功率。

常见攻击分类

- 恶意扫描：攻击者可编制或使用现有扫描工具发现目标的漏洞，进而发起攻击。
- 基础设施破坏：攻击者可通过破坏DNS、路由信息等基础设施使目标陷于孤立。
- 数据驱动攻击：攻击者可通过释放病毒、数据炸弹等方式破坏或遥控目标。

常见攻击分类

- 侦听(interception) – 中途窃听,攻击保密性
- 服务中断(interruption) – 攻击可用性
- 信息篡改（modification - of info） -攻击完整性
- 消息伪造（fabrication - of info）-攻击认证性

第一周

1.3 信息安全研究内容及发展

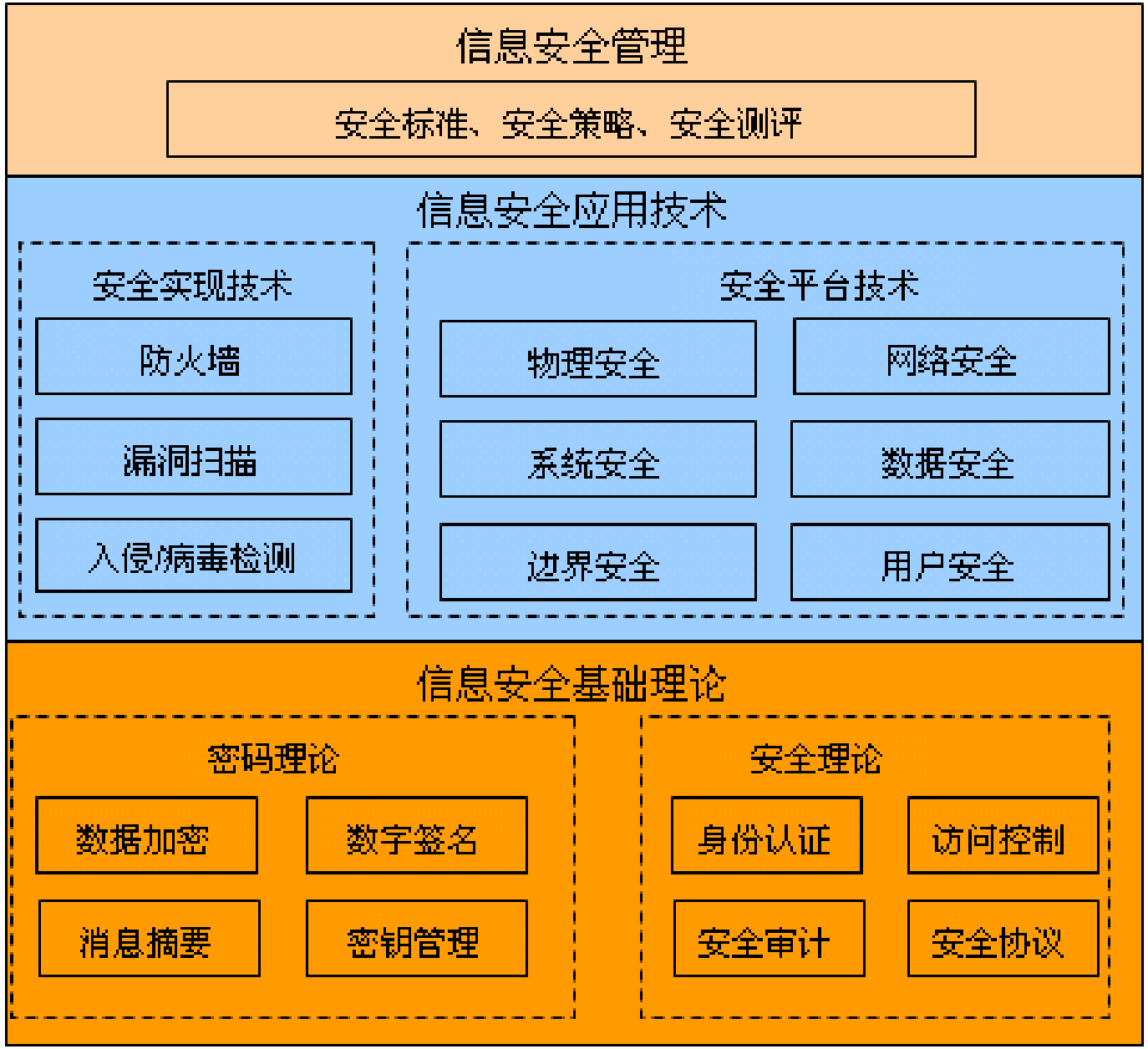
1.3 信息安全的研究内容

信息安全是一门交叉学科，涉及数学、通信、计算机等学科的知识。

大致可分为：

基础理论研究、应用技术研究、安全管理研究

1.3 信息安全的研究内容



1.基础研究

- 密码理论---是信息安全的基础，信息安全的保密性、完整性和抗否认性都依赖于密码算法。包括数据加密算法、数字签名算法、消息摘要算法及相应的密钥管理协议等。这些算法提供两方面的服务：一方面，直接对信息进行运算，保护信息的安全特征，即通过加密变换保护信息的机密性，通过消息摘要变换检测信息的完整性，通过数字签名保护信息的抗否认性；另一方面，提供对身份认证和安全协议等理论的支持。

1.3 信息安全的研究内容

1.基础研究---密码理论

数据加密算法-----DES,AES

数字签名算法

消息认证算法

密钥管理

1.基础研究---安全理论

身份认证（Authentication）

授权和访问控制（Authorization and Access Control）

审计追踪（Auditing and Tracing）

安全协议（Security Protocol）

2.应用研究---安全技术

防火墙技术（Firewall）

漏洞扫描技术（Venearbility Scanning）

入侵检测技术（Intrusion Detection）

防病毒技术（Anti-Virus）

2.应用研究---平台安全

Physical Security

Network Security

System Integrity

Application Confidentiality

User Security

Boundary Protection

3.管理研究

- 安全策略研究：包括安全风险评估、安全代价评估、安全机制的制定以及安全措施的实施和管理等；
- 安全标准研究：主要内容包括安全等级划分、安全技术操作标准、安全体系结构标准、安全产品测评标准和安全工程实施标准等；
- 安全评测研究：主要内容有评测的模型、方法、工具、规程等。

1.4 信息安全的发展

经典信息安全　　现代信息安全

1.经典信息安全

基本思想（技巧）：代换和置换

经典信息安全　　现代信息安全

2.现代信息安全

现代密码理论---A.Kerckhoffs---Shannon

第一阶段：1948年之前----密码技术是一种艺术

第二阶段：1949年---1975年---Communicaiton Theory of Security System

第三阶段：1976年---至今---New Direction in Cryptography

1.4 信息安全的发展

经典信息安全　　现代信息安全

1977年密码学发生了两件大事：DES和公钥密码体制

Thank you!

网络攻击是实现“不战而屈人之兵”最有效的武器之一

没有网络信息安全就没有国家安全