东南大学网络空间安全学院
密码学与安全协议

第一讲　绪论

黄　杰

- 联系方式：
  - 地址：无线谷 **A6栋 6206室**
  - 电话：**13675178016**
  - **Email：jhuang@seu.edu.cn**

上课的形式

- 课堂教学+大作业
- 期末考试采用闭卷
- 成绩计算方式：
  - 期末考试的卷面分数：60%
  - 平时成绩：40%，
    - 其中大作业：30%；
    - 考勤：10%
- 入群要求：姓名+学号

群聊：2023密码学与安全协议（南京）

教材资料

- 教材
  - **William Stallings**著，刘玉珍等译，密码编码学与网络安全——原理与实践。电子工业出版社。参考教材
  - 黄杰编著，信息系统安全，浙江大学出版社，**2020.1**。
  - 蒋睿、胡爱群等著，网络信息安全理论与技术。华中科技大学出版社，**2007.11**。
  - **Bruce Schneier**著，吴世忠等译，应用密码学—协议、算法与**C**源程序，机械工业出版社，**2000**。
  - 相关论文和网上刊登的资料。

本课程的主要内容

- 第一讲 绪论
- 第二讲 密码学的数学基础
- 第三讲 对称密码算法
- 第四讲 对称密钥的使用方法
- 第五讲 公钥密码算法
- 第六讲 消息认证和散列函数
- 第七讲 密钥管理技术
- 第八讲 数字签名和认证协议
- 第九讲 可信计算
- 第十讲 **PKI/CA**
- 总复习

第一讲　绪论

主要内容

- **1.1** 信息安全概述与密码学组成
- **1.2** 信息安全体系架构与密码学应用
- **1.3** 信息安全的相关标准

知识点

1、信息安全与密码学的关系？

2、安全风险的来源：脆弱性和外部威胁

3、信息安全体系结构分类及应用

4、安全需求或安全服务

1.1 信息安全概述与密码学组成

在我们日常生活中，听到的、看到的哪些内容与密码学有关？

引子：生活中的密码学

DNA

电报

口令

谜语

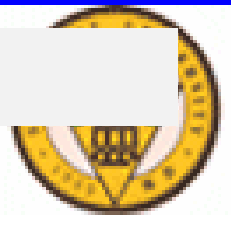
病毒

■什么是信息安全

为了防止未经授权就对知识、实事、数据或能力进行使用、滥用、修改、破坏、拒绝使用或使信息被非法系统辨识、控制而采取的措施。

信息安全是指信息在产生、传输、处理、存储、使用和销毁过程中的安全，即信息全生命周期的安全。

问题：信息安全解决的本质问题是什么？



信息安全的演化过程

用户独占单机系统
单用户单进程——物理安全
单用户多进程——进程保护

1940s
|
1960s

1960s
|
1970s

多用户主机共享系统
“单计算机系统”——安全主要由操作系统管理，即：由操作系统实现用户的身份认证和访问控制，以及事后的安全审计。

多用户联网信息系统
外部网络威胁为主，集中式管理，系统的边界清晰，安全管理相对容易，防火墙技术可以抵御大部分网络威胁。

1980s
|
1990s

1990s
|
至今

分布式信息系统
边界模糊，以防火墙技术为中心的传统安全防护手段不再适用，需要全新的信息安全理念和架构。

单计算机系统安全 → 网络安全 → 信息安全

- 信息安全目标的演化
  - 2000年之前，信息防护以边界防护为主。要求是严防死守，阻止入侵。
  - 2000年为分水岭。
  - 2000年后，信息防护的边界模糊。要求：信息保障，即防护和恢复；降低损失；保障业务的连续性。

通信保密 → 信息安全防护 → 信息保障

问　题

- 密码学是解决信息安全问题的唯一方法吗？
- 既然加密方法可以理解为将明文编码成任意无法识别的字符，那我们为什么还需要学习密码算法呢？

• 信息的安全风险来源：信息系统的脆弱性和安全威胁

信息系统的脆弱性

- **电磁泄漏**
  - 辐射泄漏、传导泄漏
- **芯片的脆弱性**
  - 硬件安全问题: 芯片存在设计缺陷; “后门”
- **数据库的安全漏洞**
  - 数据库自身存在安全缺陷、错误部署和配置、SQL注入、通信协议、存储介质
- **操作系统的安全漏洞**
  - 操作系统软件在设计上的缺陷或错误。
- **通信协议的安全漏洞**
  - 协议的开放性、协议的设计缺陷、代码实现的缺陷
- **移动存储介质的安全漏洞**
  - 移动存储介质在信息系统之间随意使用，造成病毒感染和传播;将内部介质非法带出使用，造成数据外泄。

安全威胁的来源

安全威胁的来源

自然 人为

物理攻击

通过物理接触信息系统及其周边设备的方式，对和数据产生破坏。

网络攻击

利用网络设备或协议存在的漏洞或安全缺陷对信息或数据进行攻击的行为。

恶意代码

指在用户不知情或未授权情况下潜入信息系统，在信息系统上安装运行，对信息安全产生威胁或潜在威胁的计算机代码。

安全管理

指通过信息安全需求，指导、规范和管理信息安全的一系列活动和过程。

问　题

- 风险分析的目的是什么？
- 为什么2G蜂窝网不考虑安全问题？

信息攻击模型

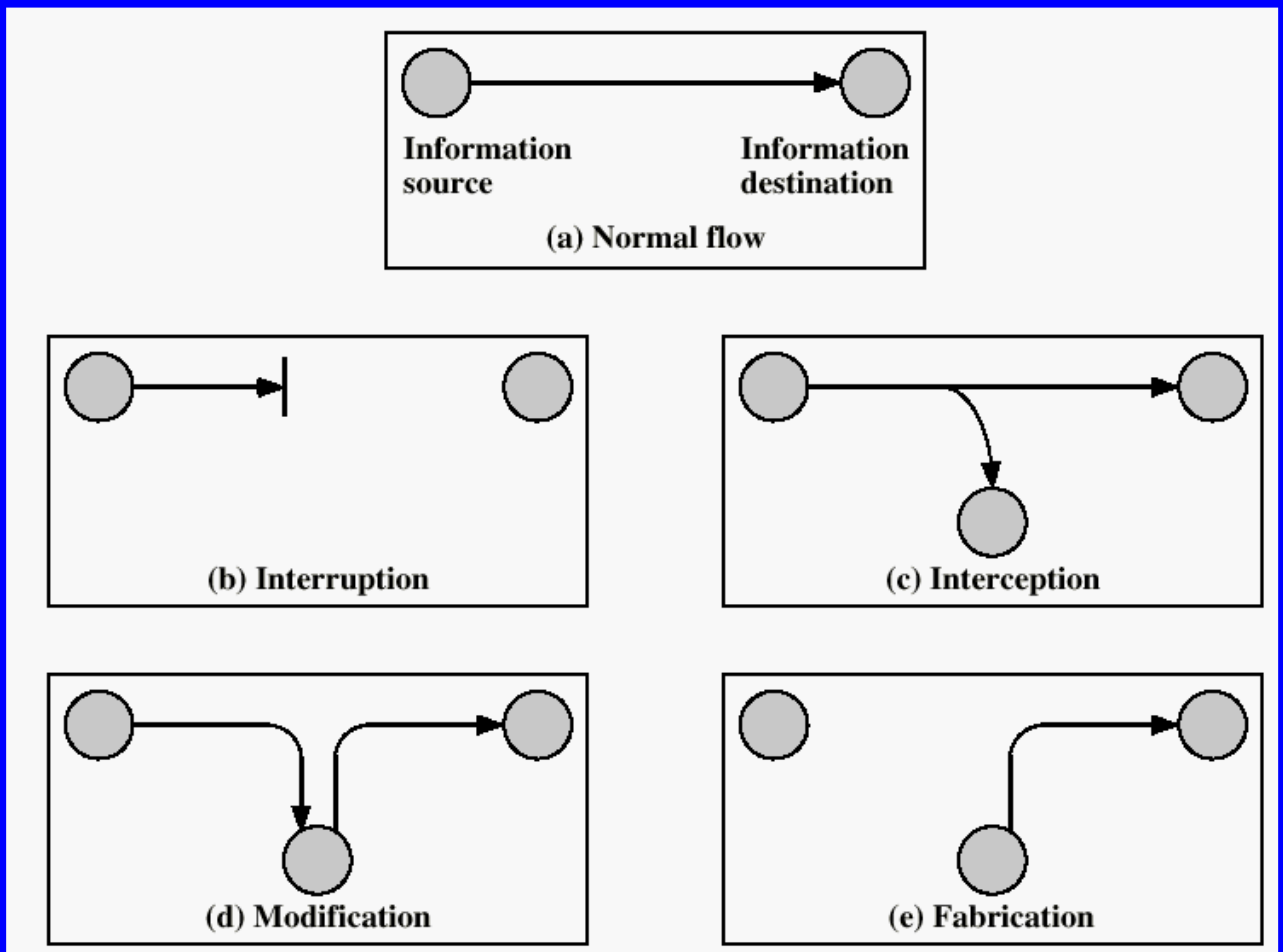
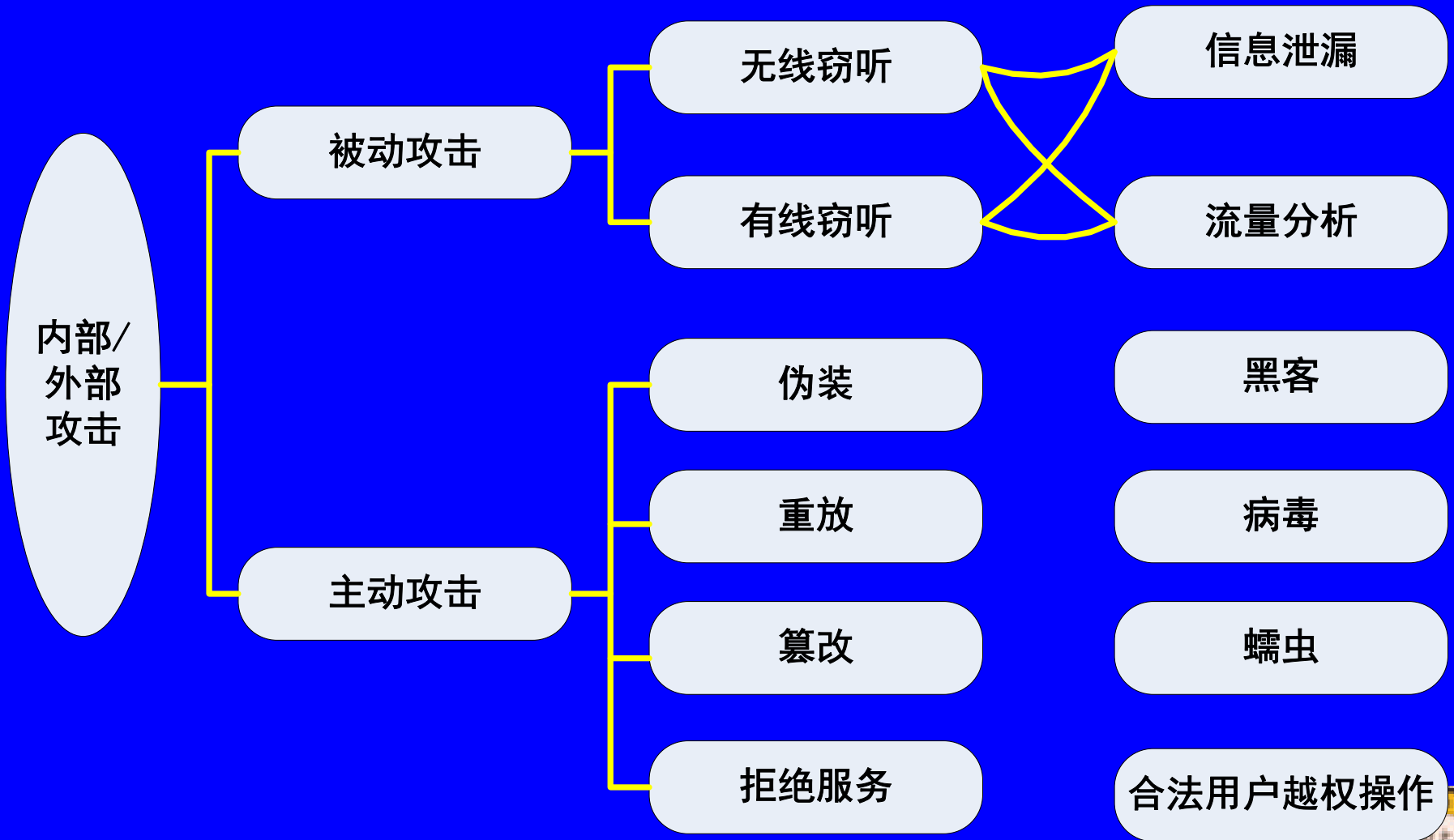


Figure 1.1 Security Threats


内部/外部攻击
被动攻击
主动攻击
无线窃听
有线窃听
伪装
重放
篡改
拒绝服务
信息泄漏
流量分析
黑客
病毒
蠕虫
合法用户越权操作

安全攻击的典型案例

沃尔辛厄姆

巴宾顿

玛丽女王

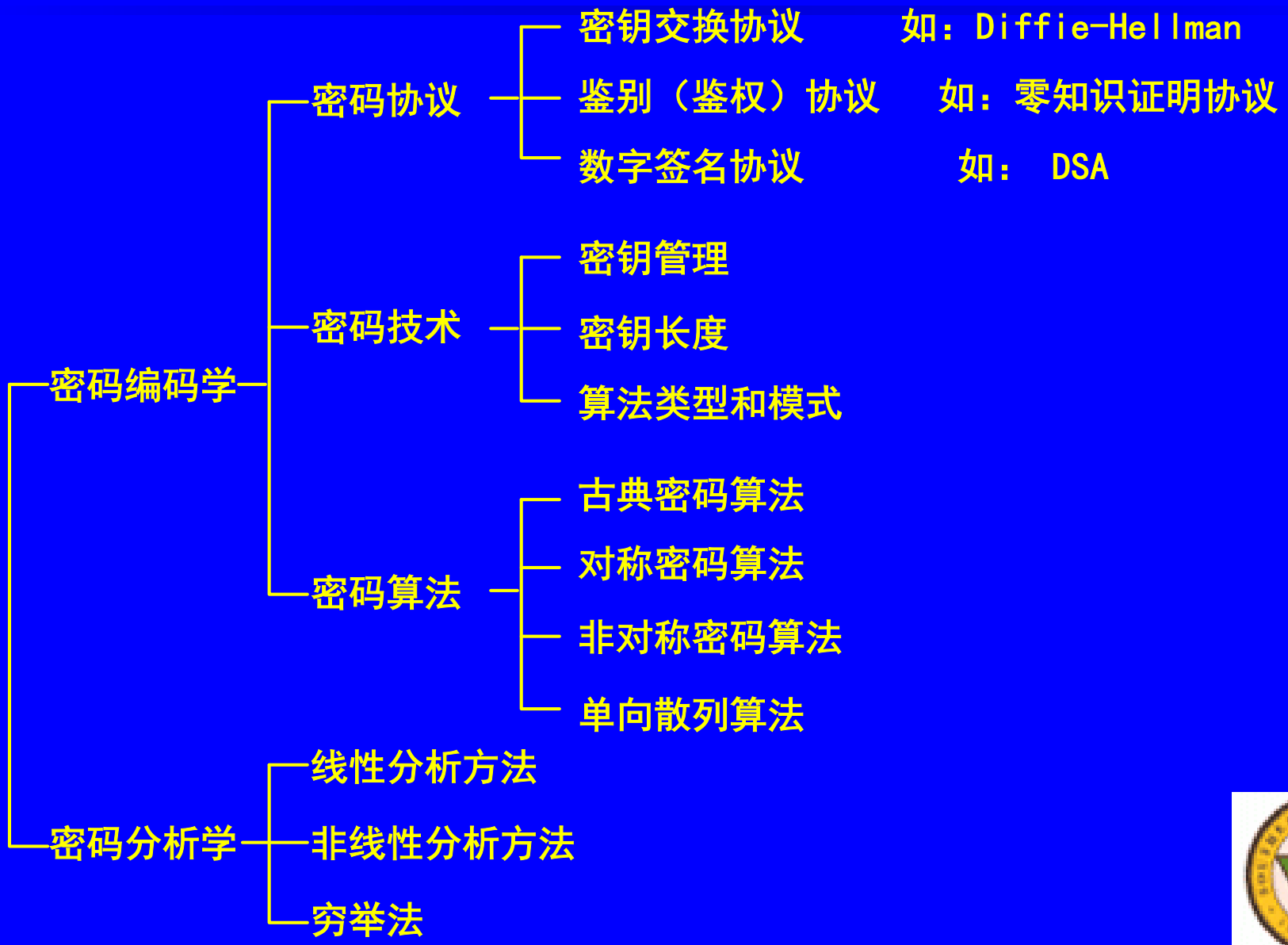
如何理解信息安全

- 没有绝对的标准
  - 安全的判别程度不同
  - 安全都是相对的
- 没有绝对的保证
  - 时间和空间的复杂性
  - 不是无懈可击：无条件的安全，计算安全
  - 任何系统都有漏洞和缺陷
  - 安全是有生存周期的

如何理解信息安全（续）

- 没有完美系统　　先有攻击还是先有防范
  - 对可用性的理解
  - 对可靠性的理解
  - 对可信性的理解
- 可用性
  - 在一定条件下的合理性
  - 开放性和安全性是一对矛盾，贯穿发展始终，长期对抗
  - 不可能存在一劳永逸、绝对安全的系统安全策略和安全机制

- **密码学组成：**


密码编码学
密码协议
密钥交换协议 如：Diffie-Hellman
鉴别（鉴权）协议 如：零知识证明协议
数字签名协议 如： DSA
密码技术
密钥管理
密钥长度
算法类型和模式
密码算法
古典密码算法
对称密码算法
非对称密码算法
单向散列算法
密码分析学
线性分析方法
非线性分析方法
穷举法

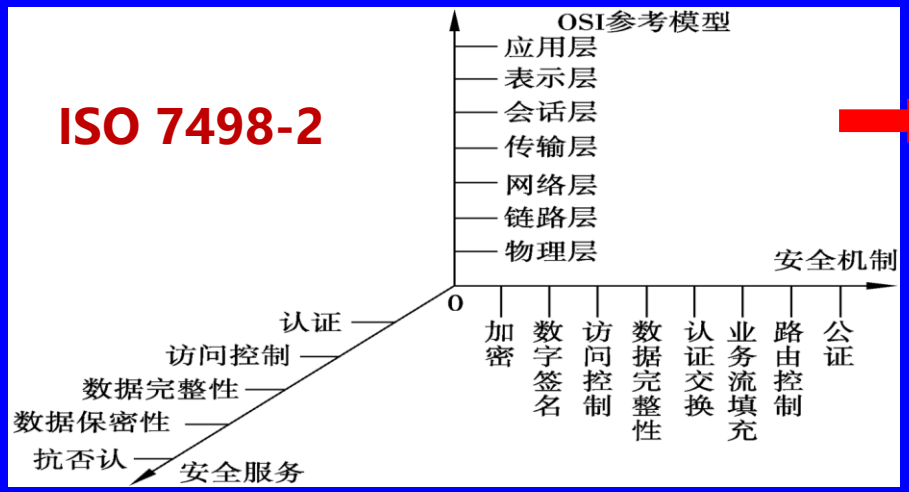
1.2 信息安全体系架构与密码学应用

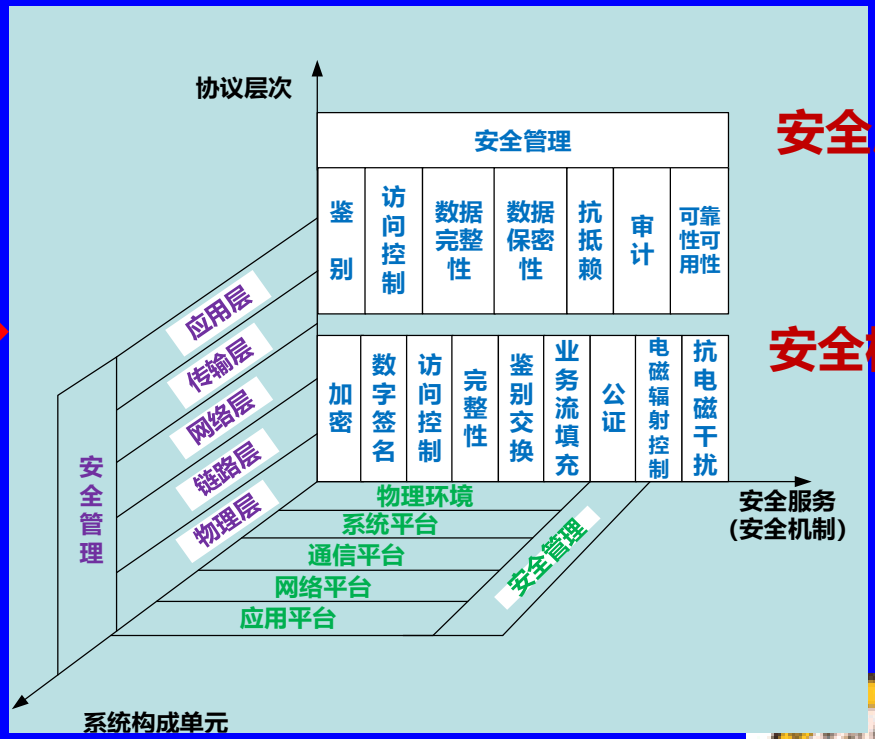
- 安全体系结构框架
- 安全体系结构的分类
- 安全服务
- 安全机制

1.2 信息安全体系结构

保障信息安全的体系结构，将协议层次、信息系统构成单元和安全服务（安全机制）作为三维坐标体系的三个维来表示，为信息系统安全提供全面的技术保障。

OSI体系结构





安全体系结构的类型

抽象体系

从描述需求开始，定义执行这些需求的功能函数。之后定义如何选用这些功能函数，以及如何把这些功能组织成一个整体的原理和相关的基本概念。

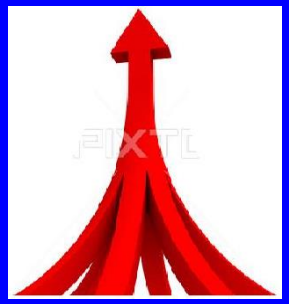
逻辑体系

逻辑体系就是满足某个假设需求集合的一个设计，它显示了把一个通用体系应用于具体环境时的基本情况。

安全体系结构类型

通用体系

通用安全体系是在已有的安全功能和相关安全服务配置的基础上，定义系统分量类型及实现这些安全功能的有关安全机制。

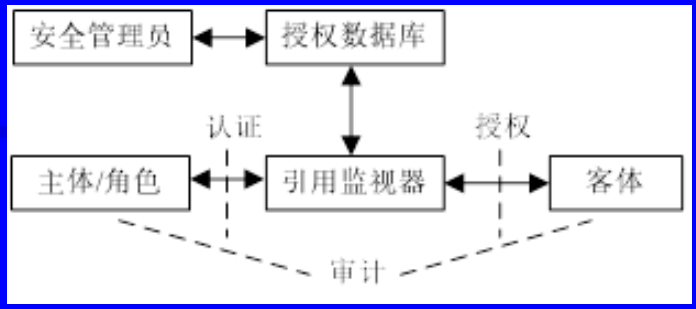


特殊体系

表达系统分量、接口、标准、性能和开销，表明如何把所有信息安全分量和机制结合起来以满足我们正在考虑的特殊系统的安全需求。

在美国国防部信息系统安全体系结构分类

安全体系包含的基本要素



安全需求

安全需求是指信息系统要达到的安全服务要求，是制定安全策略和建立安全模型的前提。

安全策略

安全策略指用于限定一个系统、实体或对象进行安全相关活动的规则集。

安全机制

安全机制是实现信息系统安全需求及安全策略的各种措施。

安全模型

安全模型用于准确描述系统在功能和结构上的安全特性，它反映了一定的安全策略。

问　题

- 4种安全体系结构如何使用？

安全服务

信息安全服务定义：

- **X.800**：通信开放系统协议层提供的一种服务，保证系统或传输数据的安全。

- **RFC2828**：一种系统提供的对系统资源进行特殊保护的处理或通信服务。

安全服务是一种安全需求。它通过安全机制实现安全策略。

安全服务

信息安全服务（信息安全的需求）：

- 认证（**Authentication**）
- 访问控制（**Access Control**）
- 保密性（**Confidentiality** ）
- 完整性**(Integrity)**
- 不可否认性**(Non-repudiation** ）

—ITU-T X.800 Security Architecture for OSI

认证（Authentication）

- 鉴别或认证，保证通信的合法性。用来验证系统实体和系统资源(如用户、进程、应用)的身份，例如鉴别想访问数据库的人的身份，确定是谁发送了报文，防止有人假冒。
- **同等实体认证和数据来源的认证**

访问控制（Access Control）

- 控制授权范围内的信息流向及行为方式。使用授权机制，控制信息传播范围、内容，实现对网络资源及信息的可控性。

保密性(Confidentiality)

- 指信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

- 连接保密性、非连接保密性、选择域保密性和流量保密性。

完整性(Integrity)

- 指网络信息未经授权不能进行改变的特性，既信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

不可否认性(Nonrepudiation)

- 指在信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。

- **源不可否认，宿不可否认。**

问　题

- 分析TCP/IP协议的安全需求?

- 信息安全的目标：
  - 假不了
  - 进不去
  - 看不懂
  - 改不得
  - 赖不掉

安全机制

- 加密
- 数字签名
- 访问控制
- 数据完整性

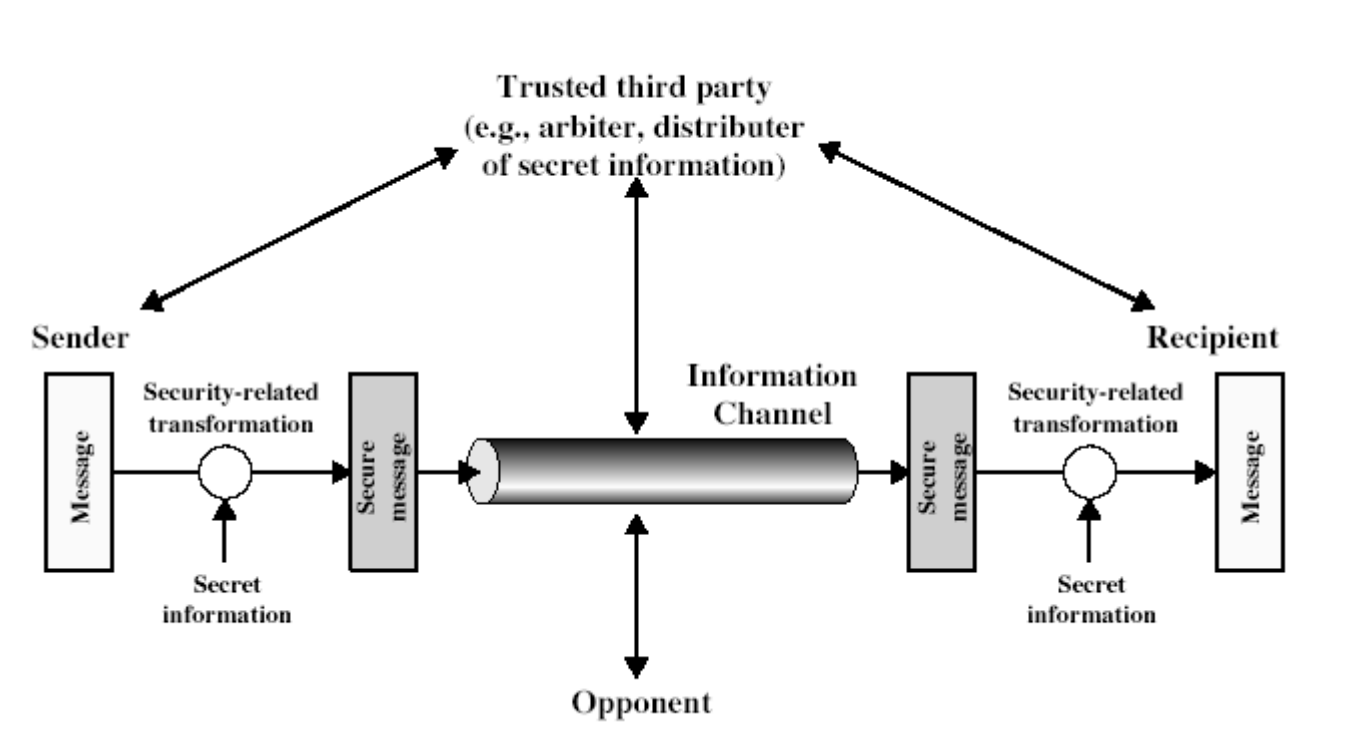
……

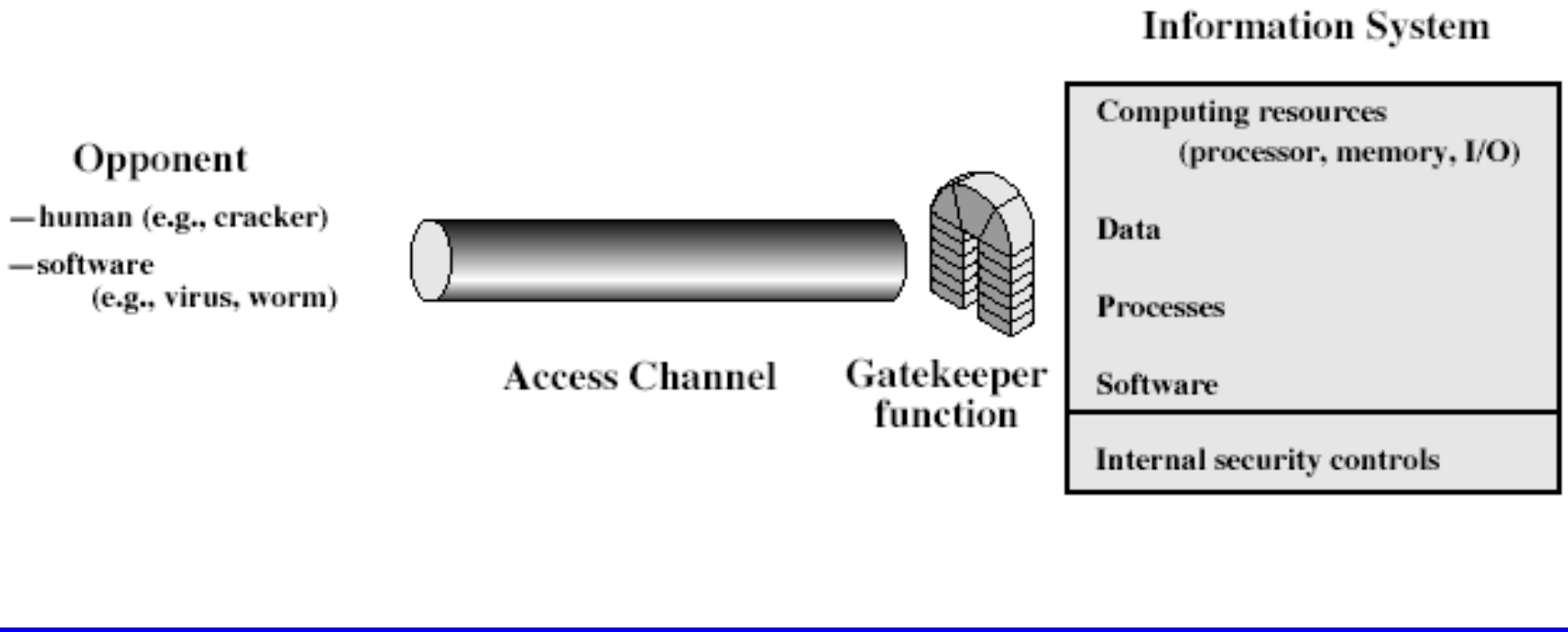
表1 安全攻击、安全机制、安全服务之间的关系

释放消息内容	流量分析	伪装	重放	更改消息	拒绝服务	安全攻击 / 安全机制 / 安全服务	加密	数字签名	访问控制	数据完整性	认证交换	流量填充	路由控制	公证
		✓				对等实体认证	✓	✓			✓			
		✓				数据源认证	✓	✓						
		✓				访问控制			✓					
✓						机密性	✓						✓	
	✓					流量机密性	✓					✓	✓	
			✓	✓		数据完整性	✓	✓		✓				
						非否认服务		✓		✓				✓
					✓	可用性				✓	✓			

安全模型

安全模型用于准确描述信息在生命周期某个环节的安全特性，它反映了一定的安全策略。




Information System
Opponent
—human (e.g., cracker)
—software
(e.g., virus, worm)
Computing resources
(processor, memory, I/O)
Data
Processes
Software
Internal security controls
Access Channel
Gatekeeper
function

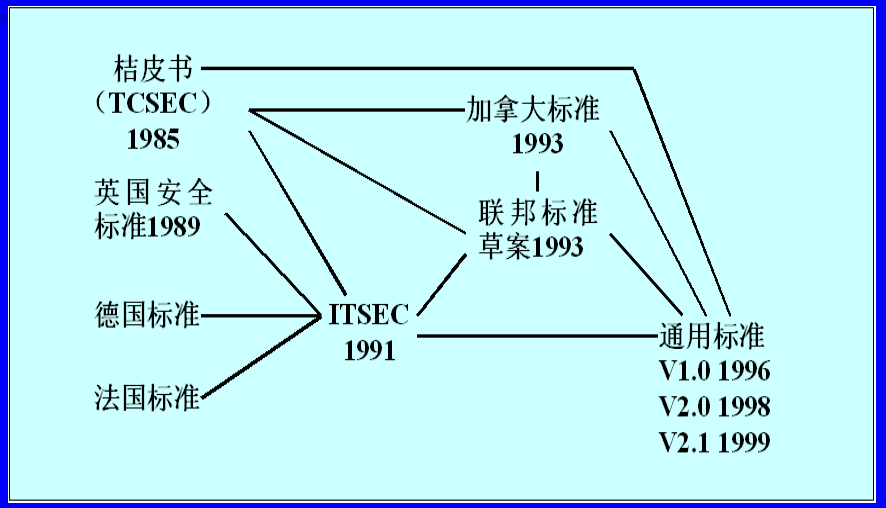
网络安全访问模型

1.3 信息安全的相关标准

1.3信息安全标准

- 国际上著名的标准化组织及其标准化工作
  - ISO，NIST，TCGA
- 密码标准
  - DES
  - AES
  - NESSIE(New European Schemes for Signature, Integrity, and Encryption)
- 可信计算机系统评价准则
  - TCSEC-ITSEC-CC
- 管理标准
  - ISO 17799

评估标准的演变



- 美国DoD
  - DoD85 TCSEC
  - TCSEC可信网络解释（TNI 1987）
  - TCSEC可信数据库管理系统解释（TDI 1991）
  - 彩虹系列Rainbow series
- 欧洲 – ITSEC
- 美国、加拿大、欧洲等共同发起Common Criteria（CC）

TCSEC可信计算机系统安全等级

类别	级别	名称	主要特征
A	A1	验证设计	形式化的最高级描述和验证，形式化的隐蔽通道分析，非形式化的代码对应证明
B	B3	安全区域	存取监控，高抗渗透能力
	B2	结构化保护	形式化模型/隐通道约束、面向安全的体系结构，较好的抗渗透能力
	B1	标识的安全保护	强制存取控制、安全标识
C	C2	受控制的存取控制	单独的可查性、广泛的审计跟踪
	C1	自主安全保护	自主存取控制
D	D	低级保护	相当于无安全功能的个人微机

ITSEC定义了七个安全级别

- E6：形式化验证；
- E5：形式化分析；
- E4：半形式化分析；
- E3：数字化测试分析；
- E2：数字化测试；
- E1：功能测试；
- E0：不能充分满足保证。

通用评价准则（CC）

- 美国为了保持他们在制定准则方面的优势，不甘心TCSEC的影响被ITSEC取代，他们采取联合其他国家共同提出新的评估准则的办法体现他们的领导作用。
- 91年1月宣布了制定通用安全评价准则（CC）的计划。它的全称是Common Criteria for IT security Evaluation 。
- 制定的国家涉及到六国七方，他们是美国的国家标准及技术研究所（NIST）和国家安全局（NSA），欧州的荷、法、德、英，北美的加拿大。

通用评价准则（CC）

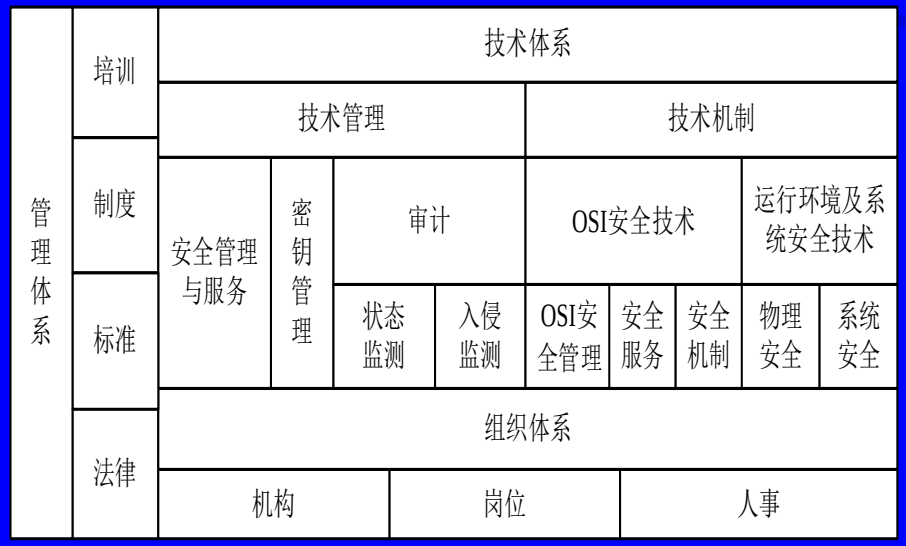
- 它的基础是欧州的ITSEC，美国的包括TCSEC 在内的新的联邦评价标准，加拿大的 CTCPEC，以及 国际标准化组织ISO :SC27 WG3 的安全评价标准
- 1995年颁布0.9版，1996年1月出版了1．0版。 1997年8月颁布2.0 Beata版， 2.0 版于1998年5月颁布。
- 1998-11-15 成为ISO/IEC 15408信息技术-安全技术-IT安全评价准则

CC标准评价的三个方面

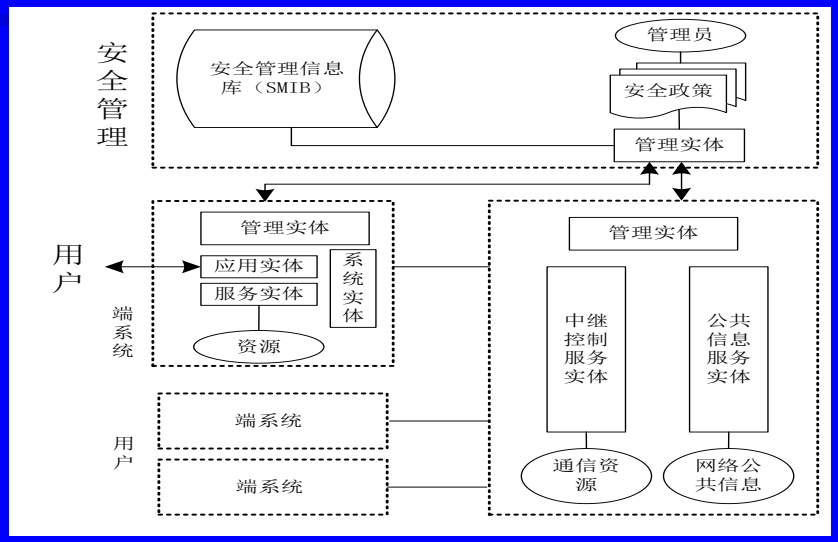
- CC标准评价的三个方面
  - 保密性（confidentiality）
  - 完整性（integrity）
  - 可用性（availability）
- CC标准中未包含的内容：
  - 行政管理安全的评价准则
  - 电磁泄露
  - 行政管理方法学和合法授权的结构
  - 产品和系统评价结果的使用授权
  - 密码算法质量的评价

谢谢

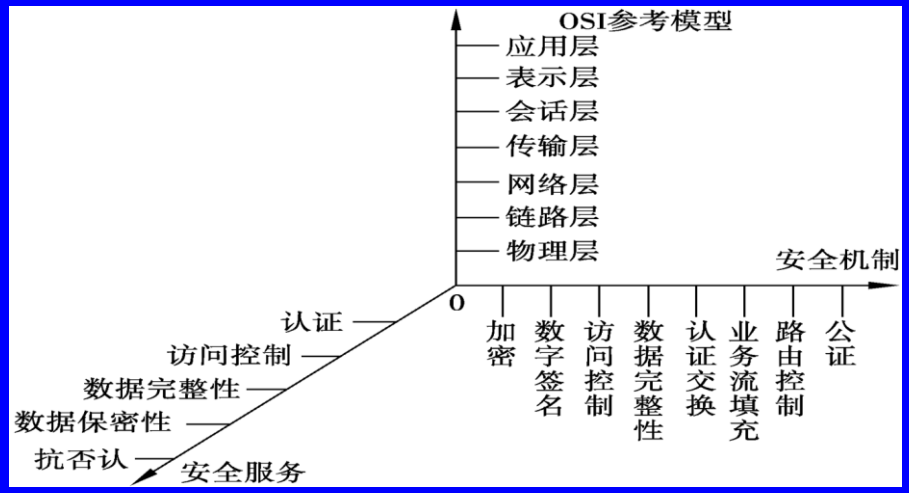
抽象体系



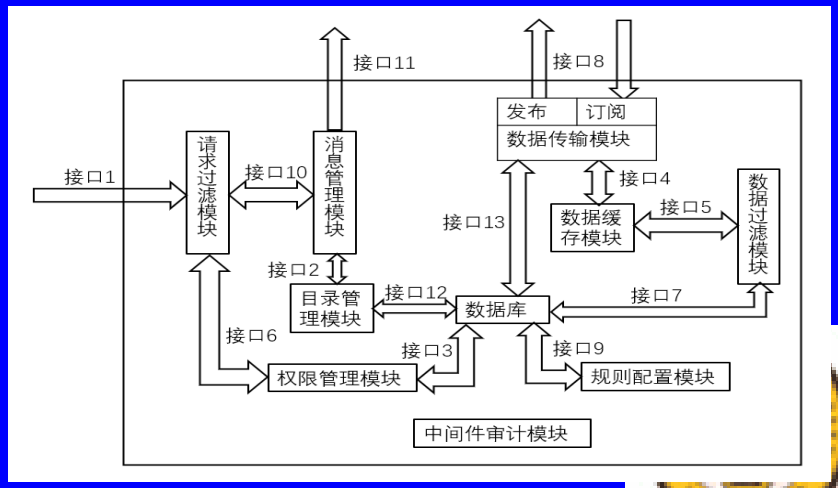
逻辑体系



通用体系



特殊体系



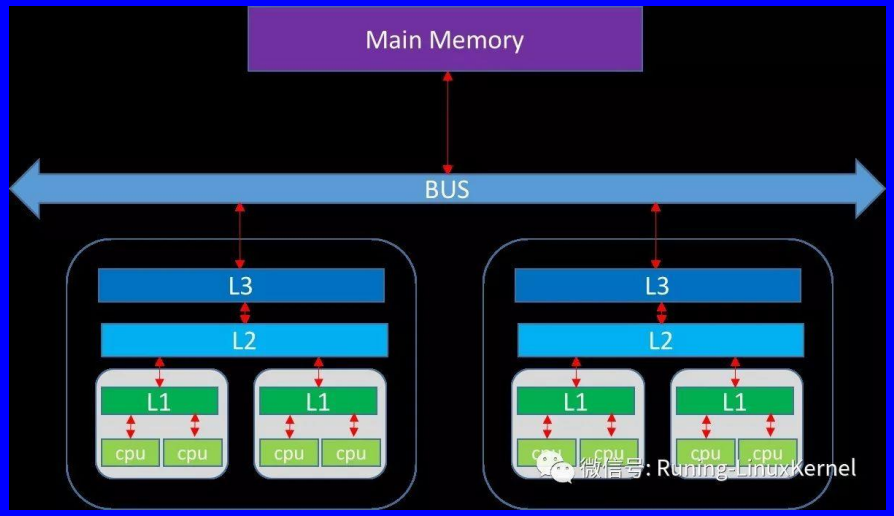
案例分析

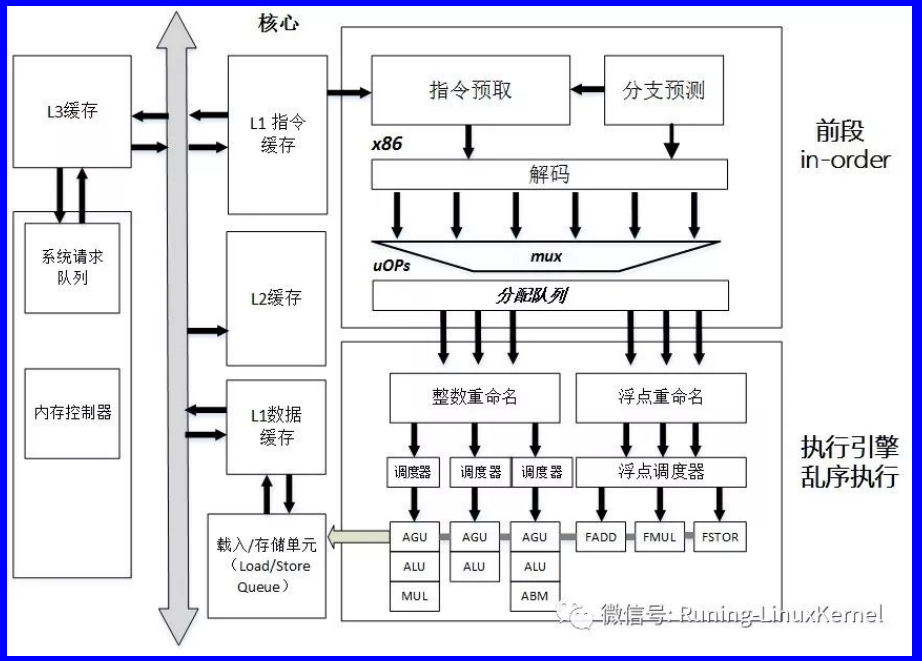
案例1　案例2

- 微处理器的两大安全漏洞——“Meltdown”（崩溃）和“Spectre”（幽灵），这两个漏洞能让黑客窃取计算机的全部内容，包括移动设备、个人计算机，以及云服务器。“Meltdown”漏洞破坏了用户和操作系统内核之间的基本隔离，允许低权限的用户“越界”访问核心内存。而“Spectre”（幽灵）破坏了不同应用程序之间的隔离，其问题的根源在于“推测执行（speculative execution）”这一优化技术，允许低权限的应用程序访问核心内存。

附件1：Meltdown漏洞分析

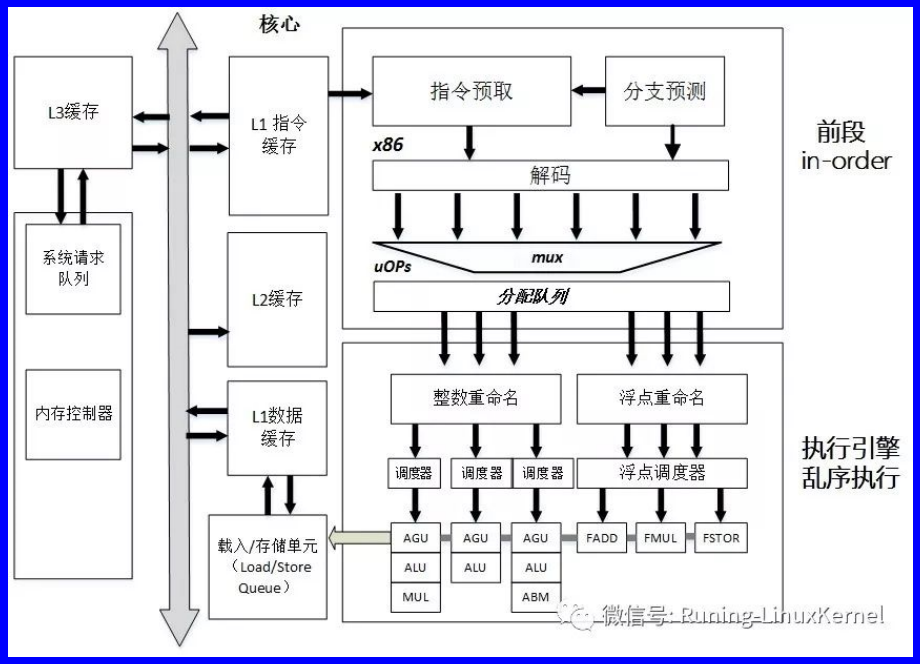
链接：
http://www.360doc.com/content/18/0108/08/32196507_720113856.shtml

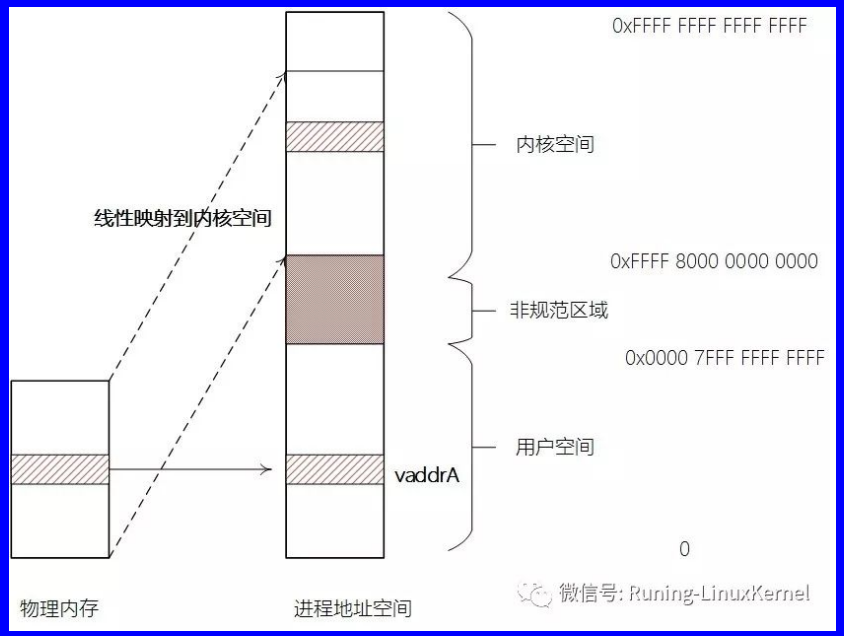




口根源：超标量体系结构（Superscalar Architecture）、乱序执行（Out-of-Order）技术和地址空间的管理

附件1：Meltdown漏洞分析





- **根源**：超标量体系结构（Superscalar Architecture）、乱序执行（Out-of-Order）技术和地址空间的管理

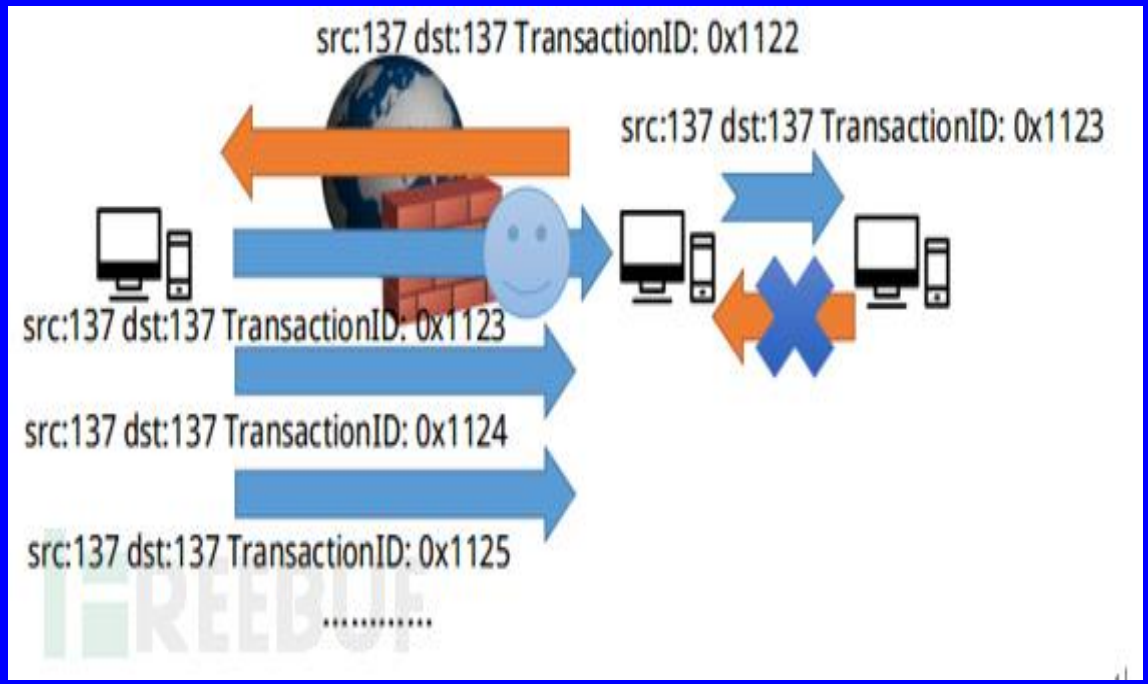
案例分析

案例1 | 案例2

- Windows操作系统的两个漏洞——Unicode漏洞和BadTunnel漏洞为例，Unicode漏洞是在IIS4.0/5.0中，Unicode字符解码时的一个漏洞，可以导致用户远程通过IIS错误地打开或执行Web根目录以外的文件，如：CMD.EXE，从而随意执行和更改目标计算机上的任意文件。BadTunnel漏洞是Windows历史上影响最广泛的漏洞，涵盖所有的Windows系统。该漏洞为原始设计问题，攻击者都可以利用该漏洞劫持整个目标网络，获取权限提升。

附件2：BadTunnel漏洞分析

链接：https://blog.csdn.net/zy_strive_2012/article/details/53127340



□ 根源：NetBIOS协议的安全漏洞

1. 受害主机向另一台主机发送SMB请求时，由于默认共享端口445（SMB）和139（NetBIOS会话）不可达，则向端口137发送NetBIOS NB STATE（NetBIOS名称服务）。
2. 一旦防火墙允许这个请求通过，则在两台主机之间建立隧道。这个隧道将保持一段时间。
3. 攻击主机可以发送大量的RESPONSE包，每个包的ID依次增加，直至蒙对为止

附件2：BadTunnel漏洞分析

BadTunnel攻击的实现依赖以下特性

- UDP协议，无连接会话；
- 广播请求可接受网段外回应。
- Windows默认开启WPAD。
- Windows文件处理API默认支持UNC path。
- Windows访问UNC path时，连接139和445端口失败后会发起NBNS NBSTAT query。
- NBNS无论作为服务端还是客户端，都使用同一个端口号。
- NBNS Transaction ID递增而不是随机。
- NBNS NBSTAT query和NBNS NB query共享同一个计数器。
- 系统在实现WPAD时也使用WEB缓存机制和NBNS缓存机制。