



声 明

- 本PPT是电子工业出版社出版的教材《计算机网络安全原理》配套教学PPT（部分内容的深度和广度在教材的基础上有所扩展），作者：吴礼发
 - 本PPT可能直接或间接采用了网上资源、公开学术报告中的部分PPT页面、图片、文字，引用时我们力求在该PPT的备注栏或标题栏中注明出处，如果有疏漏之处，敬请谅解。同时对被引用资源或报告的作者表示诚挚的谢意！
 - 本PPT可免费使用、修改，使用时请保留此页。
-

第一章 绪论





内容提纲

1

计算机网络及其脆弱性

2

计算机网络安全

3

计算机网络安全威胁

4

网络安全模型

5

网络安全机制与服务

6

网络安全内容与组织





计算机网络

- 计算机网络：由通信信道连接的主机和网络设备的集合，以方便用户共享资源和相互通信
 - 主机：计算机和非计算机设备
 - 信道：有线与无线
 - 网络设备：集线器、交换机、路由器等





计算机网络

- 计算机网络：由**通信信道**连接的**主机**和**网络设备**的集合，以方便用户共享资源和相互通信
 - 互联网（internet或internetwork）
 - 因特网（Internet）

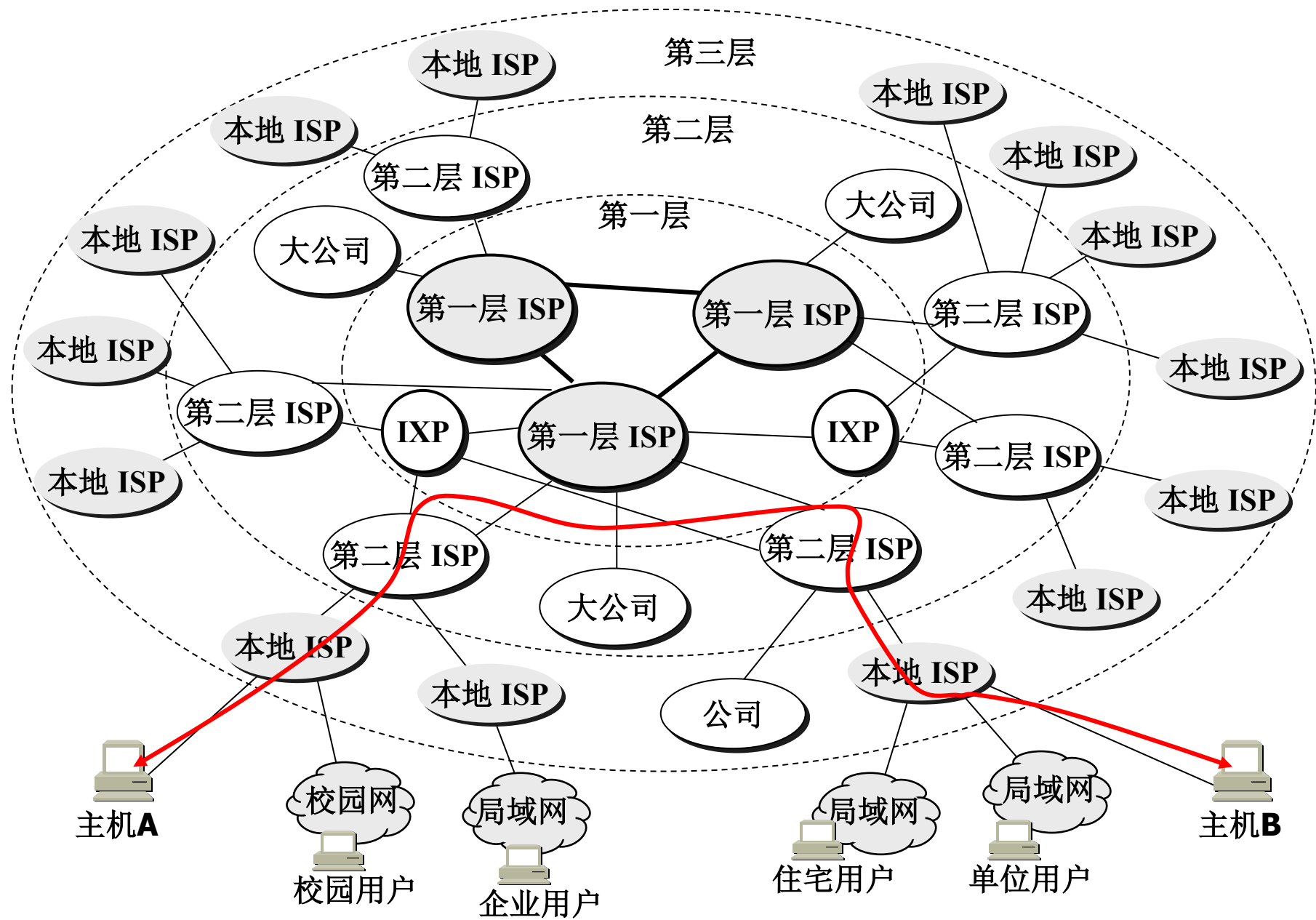




计算机网络结构和组成

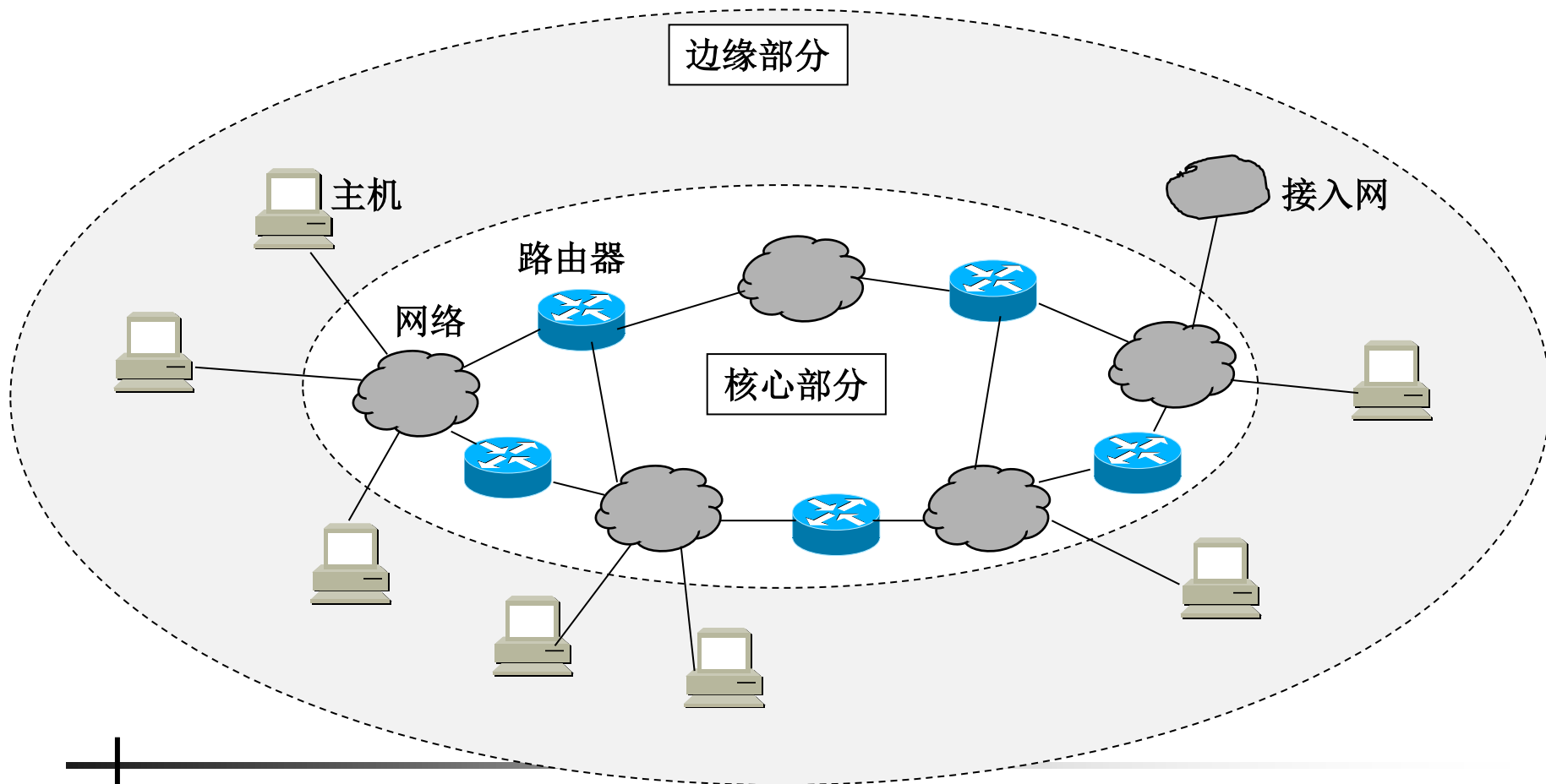
- 因特网：多层次ISP结构的网络





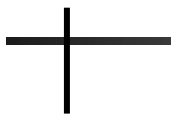
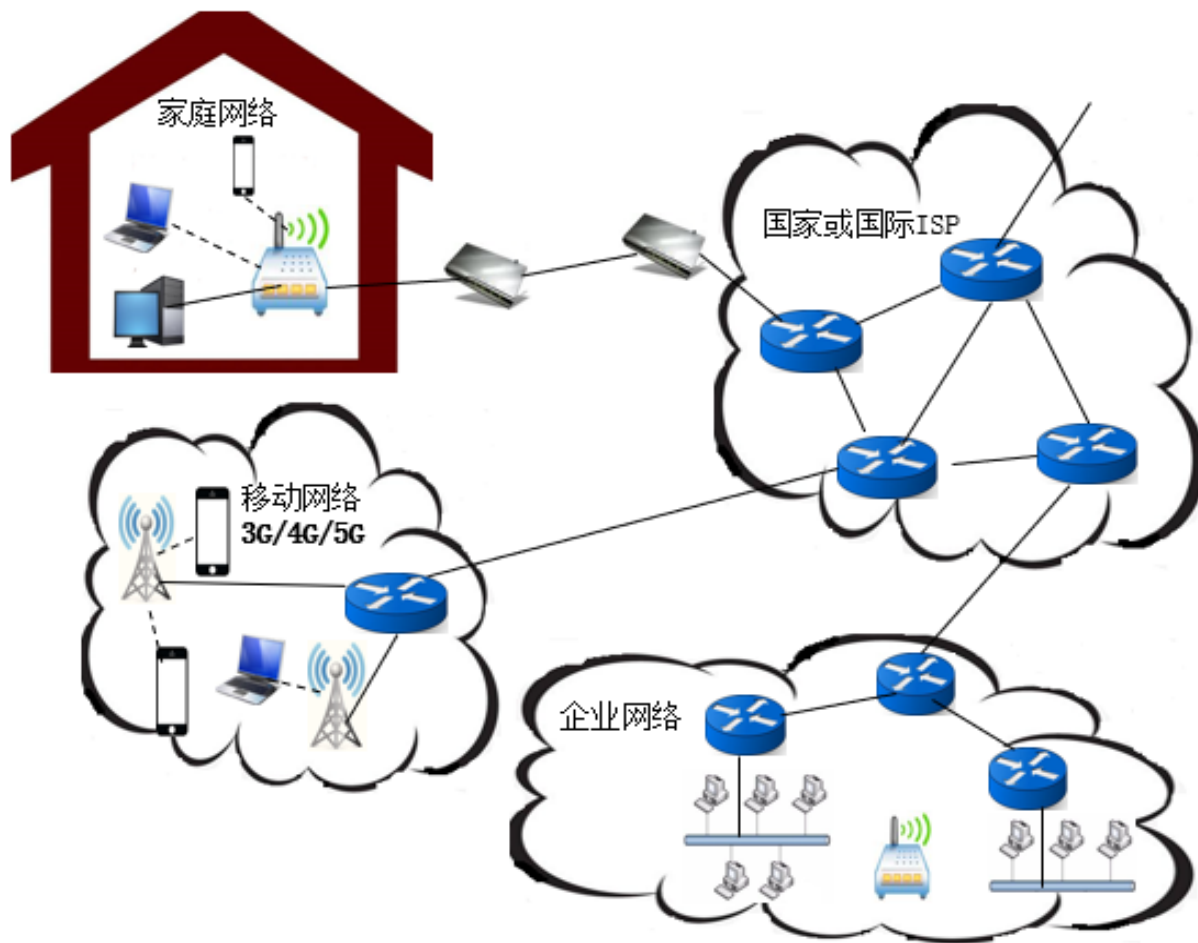
计算机网络结构和组成

■ 因特网：边缘部分 + 核心部分



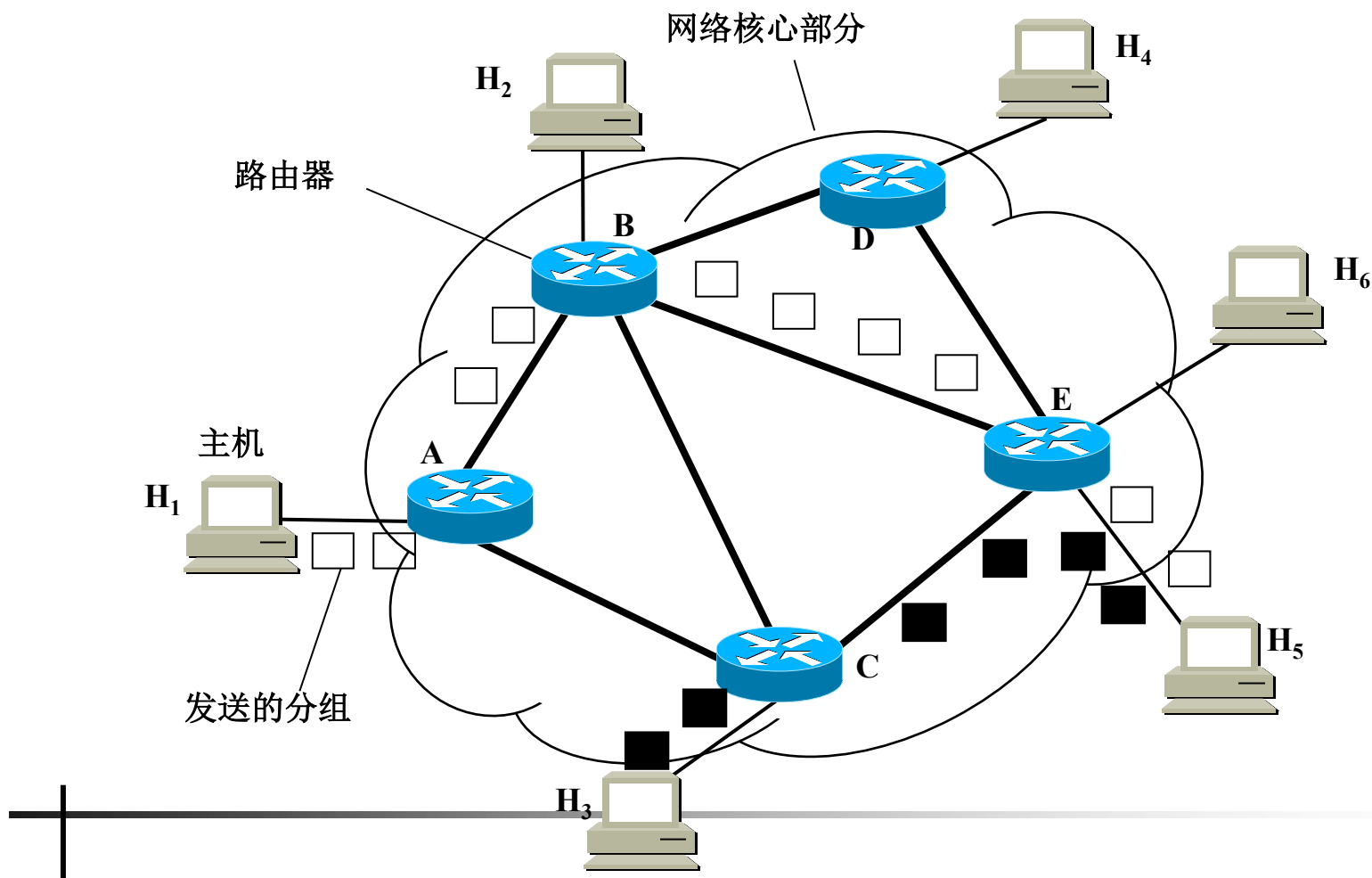
计算机网络结构和组成

- 边缘部分：主机 + 接入网



计算机网络结构和组成

- 核心部分：大量网络 + 路由器



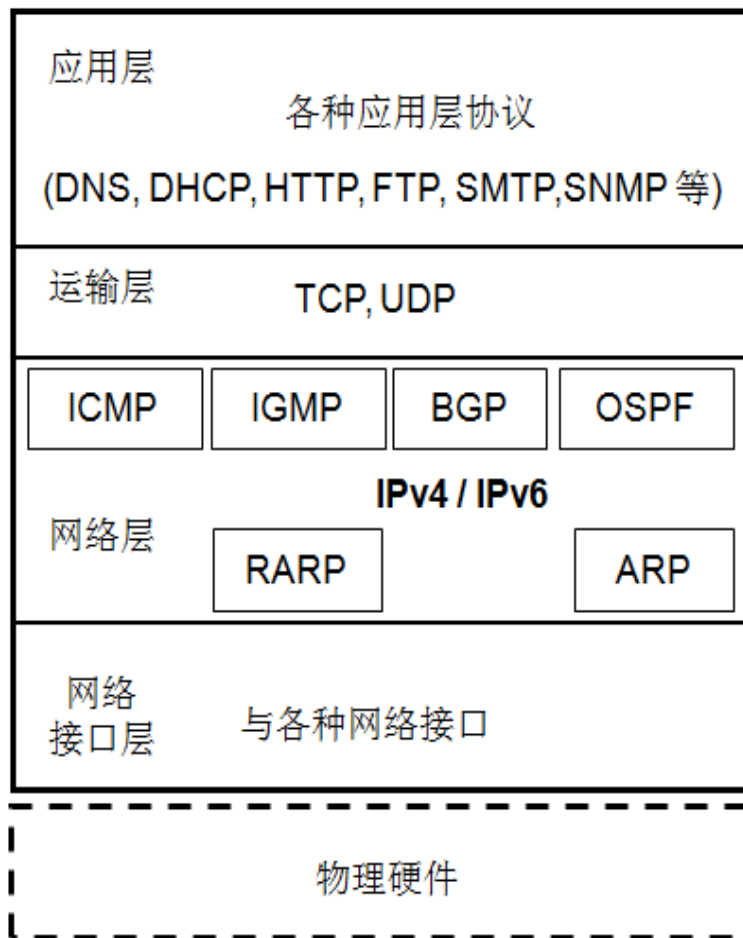


网络体系结构

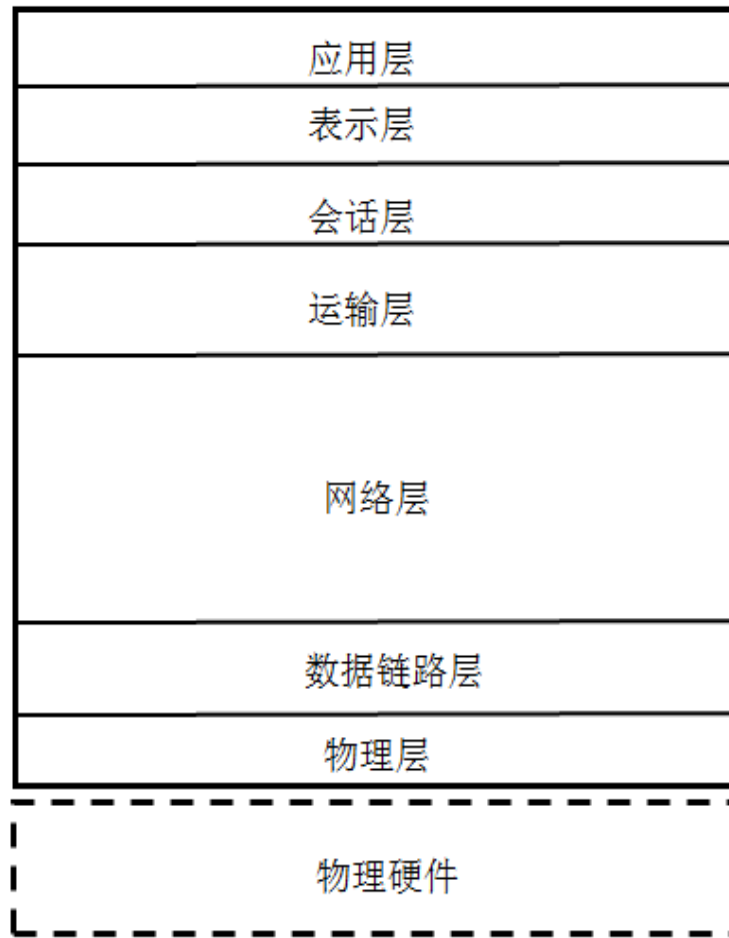
- 网络的体系结构(architecture): 计算机网络的各层及其协议的集合
 - 协议 (protocol) : 为网络中互相通信的对等实体间进行数据交换而建立的规则、标准或约定, 三要素: 语法、语义、同步



网络体系结构



(a) TCP/IP体系结构



(b) OSI/RM



计算机网络的脆弱性

- 从网络体系结构上分析
 - 分组交换、认证与可追踪性、尽力而为的服务策略、匿名与隐私、无尺度网络、级联结构、互联网的级联特性、中间盒子





计算机网络的脆弱性

- 问题一：分组交换

- Internet是基于分组交换的，这使得它比电信网（采用电路交换）更容易受攻击：
 - 所有用户共享所有资源，给予一个用户的服务会受到其它用户的影响；
 - 攻击数据包在被判断为是否恶意之前都会被转发到受害者！（很容易被DoS攻击）；
 - 路由分散决策，流量无序。





计算机网络的脆弱性

- 问题二：认证与可追踪性

- Internet 没有认证机制，任何一个终端接入即可访问全网（而电信网则不是，有UNI、NNI接口之分），这导致一个严重的问题就是IP欺骗：攻击者可以伪造数据包中的任何区域的内容然后发送数据包到Internet中。
- 通常情况下，路由器不具备数据追踪功能（Why？），因此没有现实的方法验证一个数据包是否来自于其所声称的地方。攻击者通过IP欺骗隐藏来源。





计算机网络的脆弱性

- 问题三： 尽力而为(best-effort)

- 因特网采取的是尽力而为策略：把网络资源的分配和公平性完全寄托在终端的自律上是不现实的（DDoS利用的就是这一点）





计算机网络的脆弱性

■ 问题四：匿名与隐私

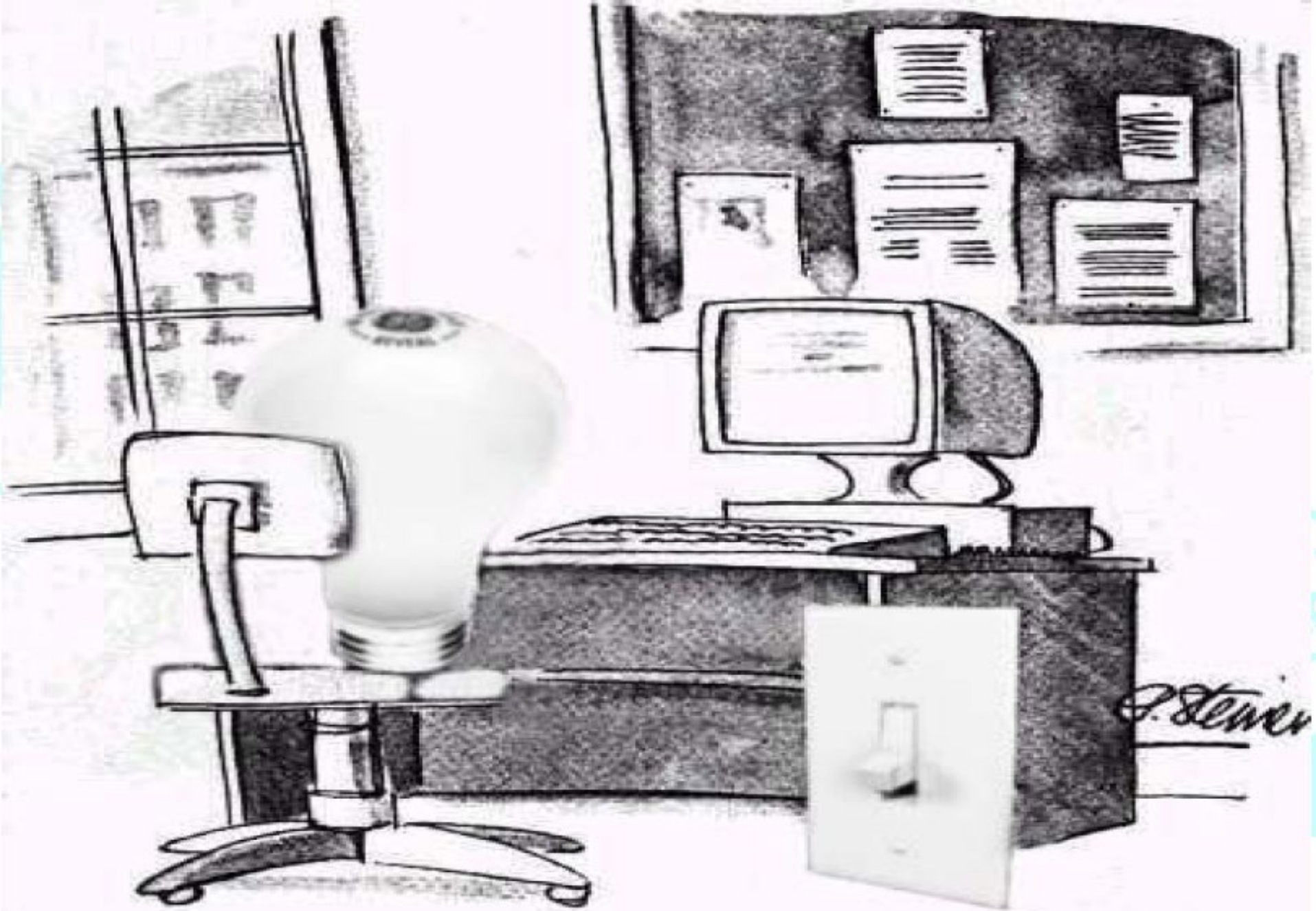
- 普通用户无法知道对方的真实身份，也无法拒绝来路不明的信息（如邮件）
- 有人提出新的体系：终端名字与地址分离

**On the Internet, nobody knows you are a dog;
On the Internet, all knows you are not a dog!**





"On the Internet, nobody knows you're a dog."



"On the Internet, nobody knows you're a light bulb."



计算机网络的脆弱性

- 问题五：对全球网络基础实施的依赖
 - 全球网络基础设施不提供可靠性、安全性保证，这使得攻击者可以放大其攻击效力：
 - 一些不恰当的协议设计导致一些（尤其是畸形的）数据包比其它数据包耗费更多的资源（如TCP SYN包比其它的TCP包占用的目标资源更多）；
 - Internet是一个大“集体”，其中有很多的不安全的系统



计算机网络的脆弱性

■ 问题六：无尺度网络

- 无尺度网络的典型特征是网络中的大部分结点只和很少结点连接，而有极少数结点与非常多的结点连接。这种关键结点（称为“枢纽”或“集散结点”）的存在使得无尺度网络对意外故障有强大的承受能力（删除大部分网络结点而不会引发网络分裂），但面对针对枢纽结点的协同性攻击时则显得脆弱（删除少量枢纽结点就能让无尺度网络分裂成微小的孤立碎片）。**CDN Loop攻击**





计算机网络的脆弱性

■ 问题七：互联网的级联特性

- 互联网是一个由路由器将众多小的网络级联而成的大网络。当网络中的一条通讯线路发生变化时，附近的路由器会通过“边界网关协议(BGP)”向其邻近的路由器发出通知。这些路由器接着又向其他邻近路由器发出通知，最后将新路径的情况发布到整个互联网。也就是说，一个路由器消息可以逐级影响到网络中的其它路由器，形成“蝴蝶效应”。“网络数字大炮”





计算机网络的脆弱性

- 问题八：中间盒子（Middle Box）
 - 违背了“端到端原则”，从源端到目的端的数据分组的完整性无法被保证，互联网透明性逐渐丧失



中间盒子

端到端的原则

- End to End principle (1984)
 - Smart hosts; simple networks
 - Packets flow from src to dst unaltered
- Functionalities should be implemented in end hosts, rather than in networks
 - Encryption, reliable transmission,...



David Clark
MIT



中间盒子

中间盒子 (Middle-Box)

- Internet evolves, ignoring any principles



- MiddleBox, Lixia Zhang(RFC3234):
 - Performance
 - DNS resolvers, Proxy, Cache, CDN
 - Protocol Translation, NAT, IPv4-IPv6
 - Security protection
 - Firewall, IDS/IPS
- Other purpose of MiddleBox
 - Monetization, Phishing,...



Prof. Lixia Zhang

中间盒子

端到端原则



- 端到端的原则出现在以下权威的文献中

- Saltzer, J. H., Reed, D. P., & Clark, D. D. 系统设计中的端到端观点, ACM TOCS, 1981
- Clark, D. D. DARPA互联网协议设计原则, CCR, 1995
- Carpenter, B., 互联网体系结构原则, RFC 1958, 1996
- Carpenter, B., 互联网透明性, RFC 2775, 2000

- 端到端原则的批评和反思

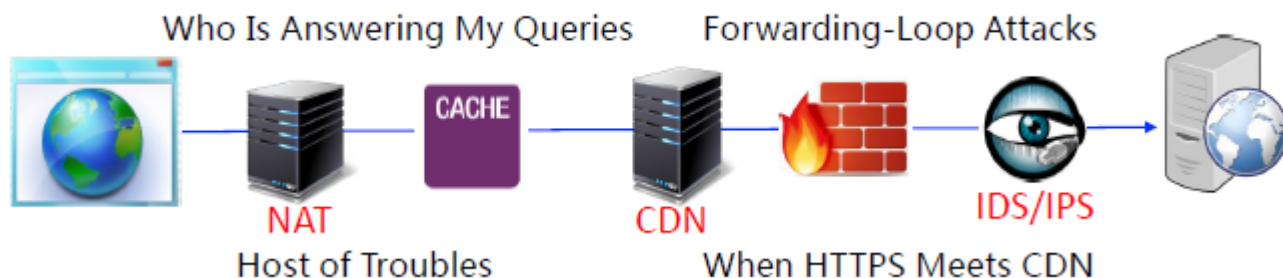
- Blumenthal, S. & Clark, D., 重新考虑互联网体系结构的设计, ACM TOIT, 2001
- Moors, T., 关于“系统设计端到端观点”的批评. ICC, 2002
- Clark, D. and etc. 扭斗的网络空间: 定义明天的互联网, SIGCOMM, 2002
- J. Kempf, 中间盒子的兴起与端到端的未来, RFC 3724, 2004

中间盒子

中间盒子所带来的安全威胁



- 增加了网络和应用的复杂性，NAT
- 增加了攻击面，通过攻击网络而影响端系统
- 协议理解和实现的不一致性
- 没有一个集中的协调机构验证协议的部署和事实



中间盒子

NAT的野蛮生长



360
企业安全

安全第一

- 在NAT蓬勃发展的初期，IETF对NAT的部署有很大争议
- IAB Network Layer workshop(RFC 2956, 1999)

```
2.2 NAT, Application Level Gateways & Firewalls

The previous section indicated that the deployment of NAT (Network
Address Translation), Application Level Gateways and firewalls causes
loss of network transparency. Each of them is incompatible with
certain applications because they interfere with the assumption of
end to end transparency. NAT especially complicates setting up
servers, peer to peer communications and "always-on" hosts as the
endpoint identifiers, i.e. IP addresses, used to set up connections
are globally ambiguous and not stable (see [2]).

NAT, application level gateways and firewalls however are being
increasingly widely deployed as there are also advantages to each,
either real or perceived. Increased deployment causes a further
decline of network transparency and this inhibits the deployment of
new applications. Many new applications will require specialized
Application Level Gateways (ALGs) to be added to NAT devices, before
those applications will work correctly when running through a NAT
device. However, some applications cannot operate effectively with
NAT even with an ALG.
```

- 张丽霞：NAT技术的教训
 - “今天大多数人认同IETF最初没有标准化NAT是错误的。为什么错过了机会？简单来说是由于当时一切都不明朗。”
 - IETF对部署一个新的协议——IPv6过于乐观
 - IETF当时对工程上的妥协（trade-off）缺乏足够的理解

中间盒子

Security&Privacy 酒店无线网络

Wifi

网络插入的内容



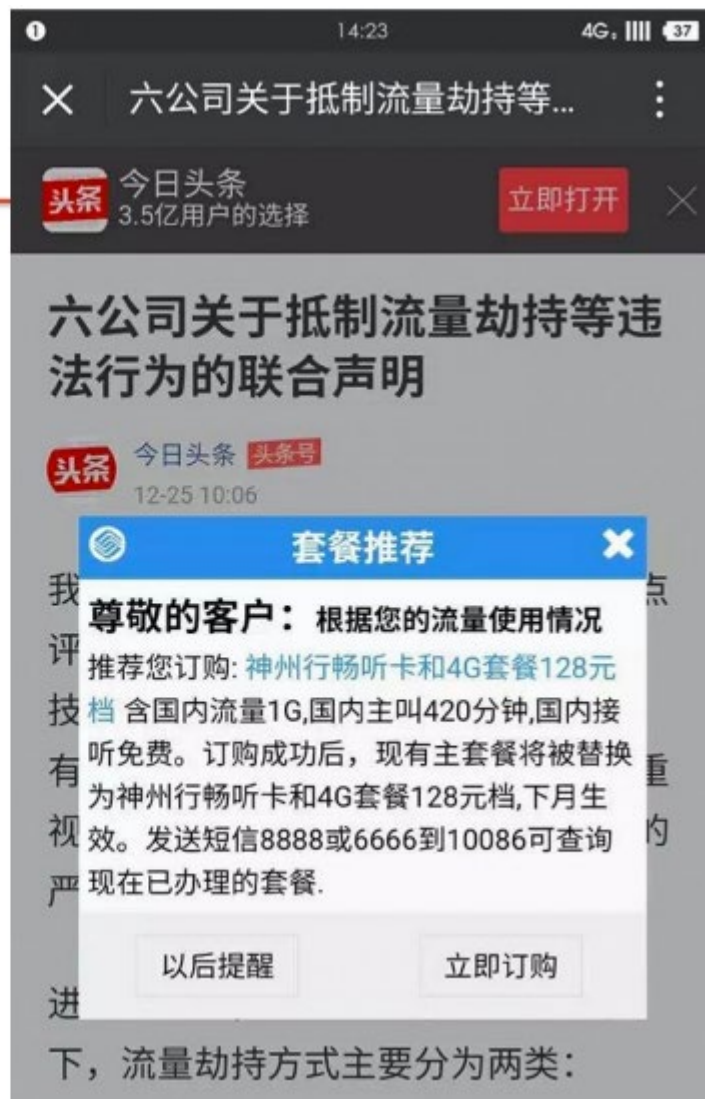
中间盒子

用户手机上被插入的广告



中间盒子

抵制流量劫持的声明，
也被劫持了





中间盒子

- 清华大学段海新教授团队关于中间盒子主要研究成果

- HTTPS in CDN, S&P 2014
- Cookies lack integrity, USENIX Security 15
- Forwarding loop, NDSS 2016
- Host of troubles, CCS 2016
- DNS interception, USENIX Sec 2018





中间盒子

■ 清华大学段海新教授：

- 中间盒子提高了性能、可靠性甚至安全性，但是也带来了许多安全问题：
 - 增加了复杂性、增加了攻击面
- 然而，回到最初的端到端和简单结构已不可能
- 互联网标准并非那么“标准”
 - 很多标准都是现有厂商实现，然后达成共识（标准）
 - 即使现有标准，歧义或不同的理解导致实现不一致
 - 不同的厂商的实现缺乏协调
- 互联网的创新和魅力
 - 没有一个集中的控制着、协调人
 - 并非严丝合缝的战车，每个个体都是自由舒展的灵魂



计算机网络的脆弱性

- 从具体的网络协议上分析
 - TCP/IP体系中的很多协议，如ARP、IP、ICMP、TCP、UDP、HTTP、DNS等，也存在可被攻击者利用的缺陷





内容提纲

1

计算机网络及其脆弱性

2

计算机网络安全

3

计算机网络安全威胁

4

网络安全模型

5

网络安全机制与服务

6

网络安全内容与组织



计算机网络安全

- 定义：是指计算机网络中的硬件资源和信息资源的安全性，它通过网络信息的产生、存储、传输和使用过程来体现，包括：**网络设备**（包括设备上运行的网络软件）的安全性，使其能够正常地提供网络服务；网络中**信息**的安全性，即网络系统的信息安全。其目的是保护网络设备、软件、数据，使其能够被合法用户正常使用或访问，同时要免受非授权的使用或访问

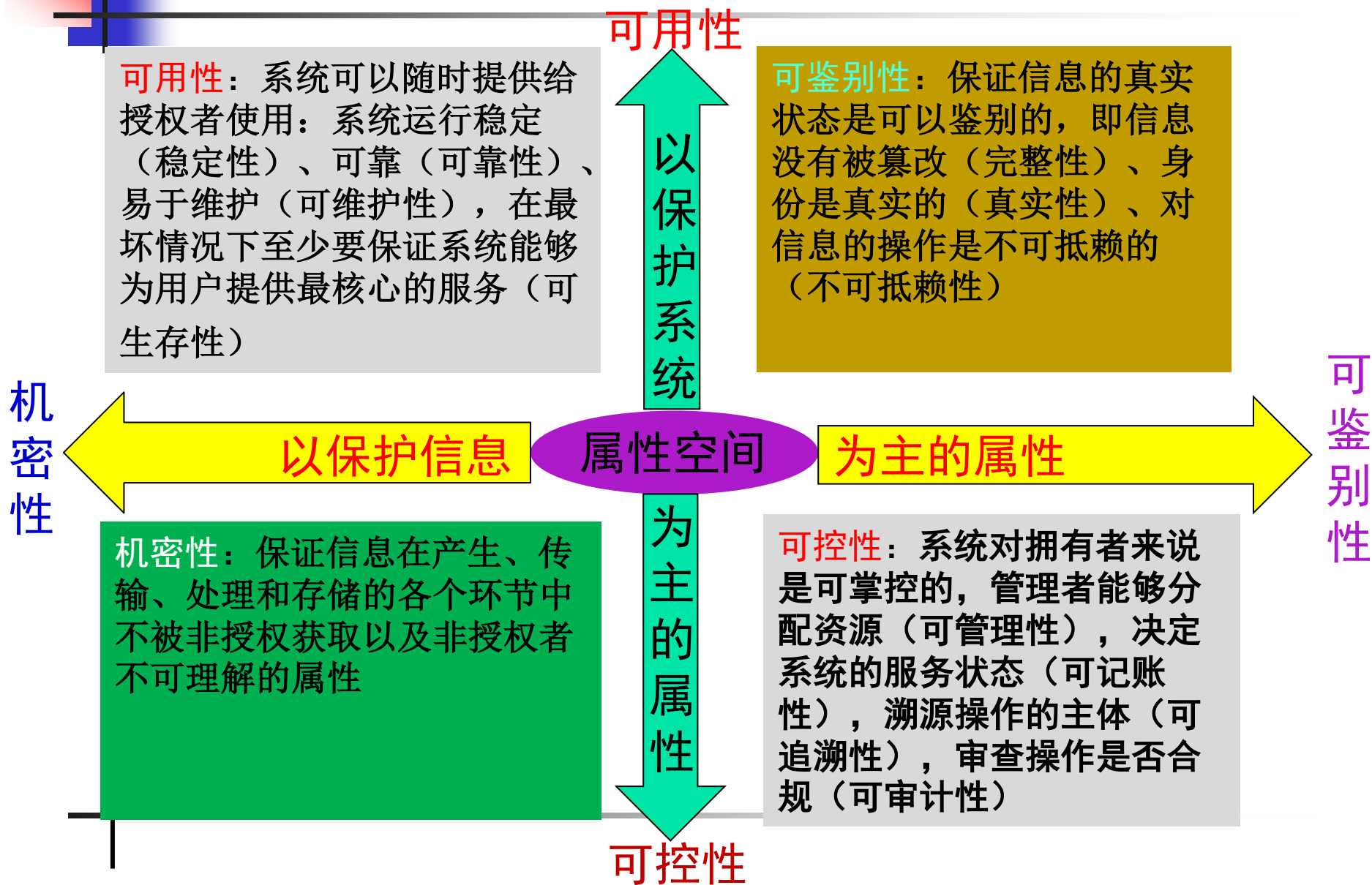




计算机网络安全

- 网络是否安全主要通过“安全属性”来评估
 - 机密性（Confidentiality或Security）
 - 完整性（Integrity），包括：系统完整性和数据完整性
 - 可用性（Availability）
 - 不可否认性（Non-repudiation）或不可抵赖性
 - 可靠性（Reliability）、可信性（Dependability or Trusty）
- 

计算机网络安全





信息安全

- 定义：信息系统安全、信息自身安全和信息行为安全的总称，目的是保护信息和信息系统免遭偶发的或有意的非授权泄露、修改、破坏或失去处理信息的能力，实质是保护信息的安全属性，如机密性、完整性、可用性和不可否认性等





计算机安全

- 定义：指计算机**硬件**、**软件**以及其中的**数据**的安全性（机密性、完整性、可用性、可控性等）不受自然和人为有害因素的威胁和危害





网络空间安全

■ 网络空间（Cyberspace）

只包含
信息与
通信技
术设施

网络空间是指相互依赖的**信息技术基础设施网络**，其中包括互联网、电信网、计算机系统和关键行业的嵌入式处理器和控制器。

--美国《第54号国家安全总统令/第23号国土安全总统令》P3

Cyberspace means the interdependent network of **information technology infrastructures**, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

--America, National Security Presidential Directive/NSPD-54. P3





网络空间安全

- 网络空间（Cyberspace）
 - 俄罗斯：信息空间中的一个活动范围，其构成要素包括互联网和其它电信网络的通信信道，还有确保其正常运转以及确保在其上所发生的任何形式的人类（个人、组织、国家）活动的技术基础设施。按此定义，网络空间包含设施、承载的数据、人以及操作





网络空间安全

■ 网络空间（Cyberspace）

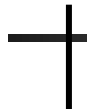
包含设
施、所
承载的
数据、
以及人

网络空间是由下述部分或全部组件构成的物理和非物理域：包括机械化和自动化系统、**计算机和通信网络**、程序、自动化信息、**计算机所表达的内容、交易和监管数据**以及那些使用这些数据的人。

--以色列的《3611号决议：推进国家网络空间能力》P.1

Cyberspace is the physical and non-physical domain that is created or composed of part or all of the following components: mechanized and computerized systems, **computer and communications networks**, programs, computerized information, **content conveyed by computer, traffic and supervisory data** and **those who** use such data.

--Israel, *Resolution No. 3611: Advancing National Cyberspace Capabilitie*. P.1



网络空间安全

■ 网络空间（Cyberspace）

信息安全专业规范（第二版）
学科论述的主要修订

四、主要修订内容

- 网络空间**
2008年，美国第54号总统令对Cyberspace进行了定义：Cyberspace是信息环境中
的一个整体域，它由独立且互相依存的信息基础设施和网络组成。包括互联网、电信网、
计算机系统、嵌入式处理器和控制器系统。
- 我们的定义**
网络空间是信息时代人们赖以生存的信息环境，是所有信息系统的集合。
- 比较**
 - 美国的定义总体是合理的，但列出许多具体系统和网络，比较繁琐。而且，随着信息
技术的发展还会出现新的系统和网络，需要进行修改和调整。
 - 我们的定义抓住了信息环境和信息系统两大核心内涵，而且表述简洁，不因技术发展
而调整。

网络空间安全

■ 网络空间（Cyberspace）

网络空间四要素：网络空间载体（设施）；网络空间资源（数据）
网络活动主体（用户）；网络活动形式（操作）

网络空间载体：设施，信息通信技术系统的集合

网络操作对象：数据，表达人类所能理解的意图的信号状态

网络活动主体：用户，网络活动的主体要素，属于人的代理

网络活动形式：操作，对数据的加工、存储、传输、展示等服务形式

网络空间的一般性定义：网络空间是一种人造的电磁空间，其以互联网、各种通信系统与电信网、各种传播系统与广电网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器等信息通信技术基础设施为**载体**，**用户**通过在其上对**数据**进行创造、存储、改变、传输、使用、展示等**操作**，以实现特定的信息通信技术活动。

在这个定义中，“载体”、“数据”是在技术层面反映出“Cyber”的属性；“用户”、“操作”是在社会层面反映出“Space”的属性。2

网络空间安全

■ 网络空间安全（Cyberspace Security）

定义网络空间安全（424要素）

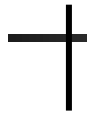


网络空间安全涉及到在网络空间中**电磁设备、信息通信系统、运行数据、系统应用**中所存在的安全问题，**既要防止、保护**包括互联网、各种电信网与通信系统、各种传播系统与广电网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器等在内的信息通信技术系统及其所承载的数据免受攻击；**也要防止、应对**运用或滥用这些信息通信技术系统而波及到**政治安全、经济安全、文化安全、社会安全、国防安全**等情况的发生。针对上述风险，需要采取**法律、管理、技术、自律**等综合手段来进行应对，确保信息通信技术系统及其所承载数据的**机密性、可鉴别性**（包括完整性、真实性、不可抵赖性）、**可用性、可控性**得到保障。



网络空间安全

■ 网络空间安全（Cyberspace Security）

- 方滨兴：在信息通信技术的硬件、代码、数据、应用**4个层面**，围绕着信息的获取、传输、处理、利用**4个核心功能**，针对网络空间的设施、数据、用户、操作**4个核心要素**来采取安全措施，以确保网络空间的机密性、可鉴别性、可用性、可控性**4个核心安全属性得到保障**，让信息通信技术系统能够提供安全、可信、可靠、可控的服务，面对网络空间攻防对抗的态势，通过信息、软件、系统、服务方面的确保手段、事先预防、事前发现、事中响应、事后恢复的应用措施，以及国家**网络空间主权**的行使，既要应对信息通信技术系统及其所受到的攻击，也要应对信息通信技术相关活动的衍生出政治安全、经济安全、文化安全、社会安全与国防安全的问题
- 

网络空间安全

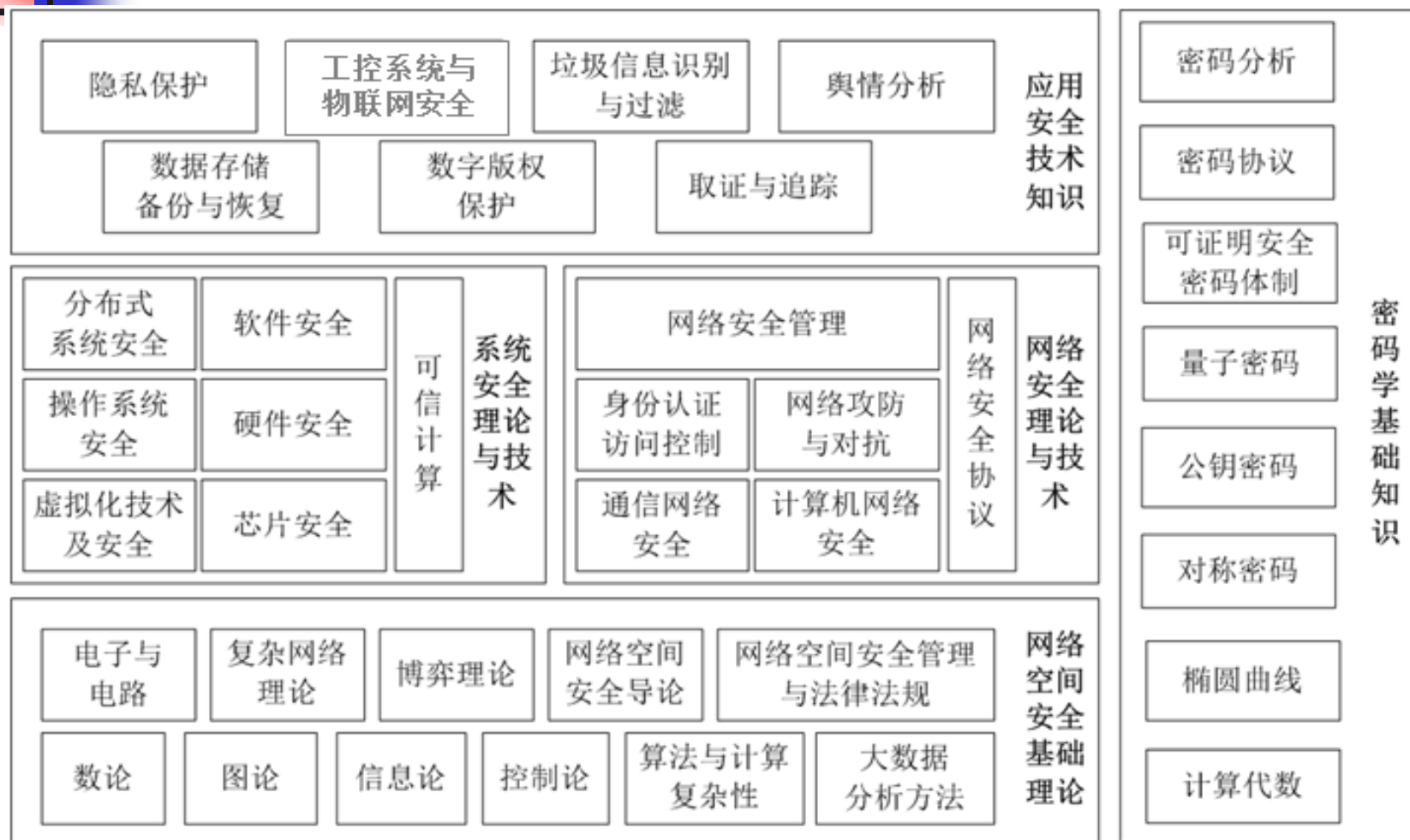
■ 网络空间安全（Cyberspace Security）

信息安全专业规范（第二版）
学科论述的主要修订

四、主要修订内容

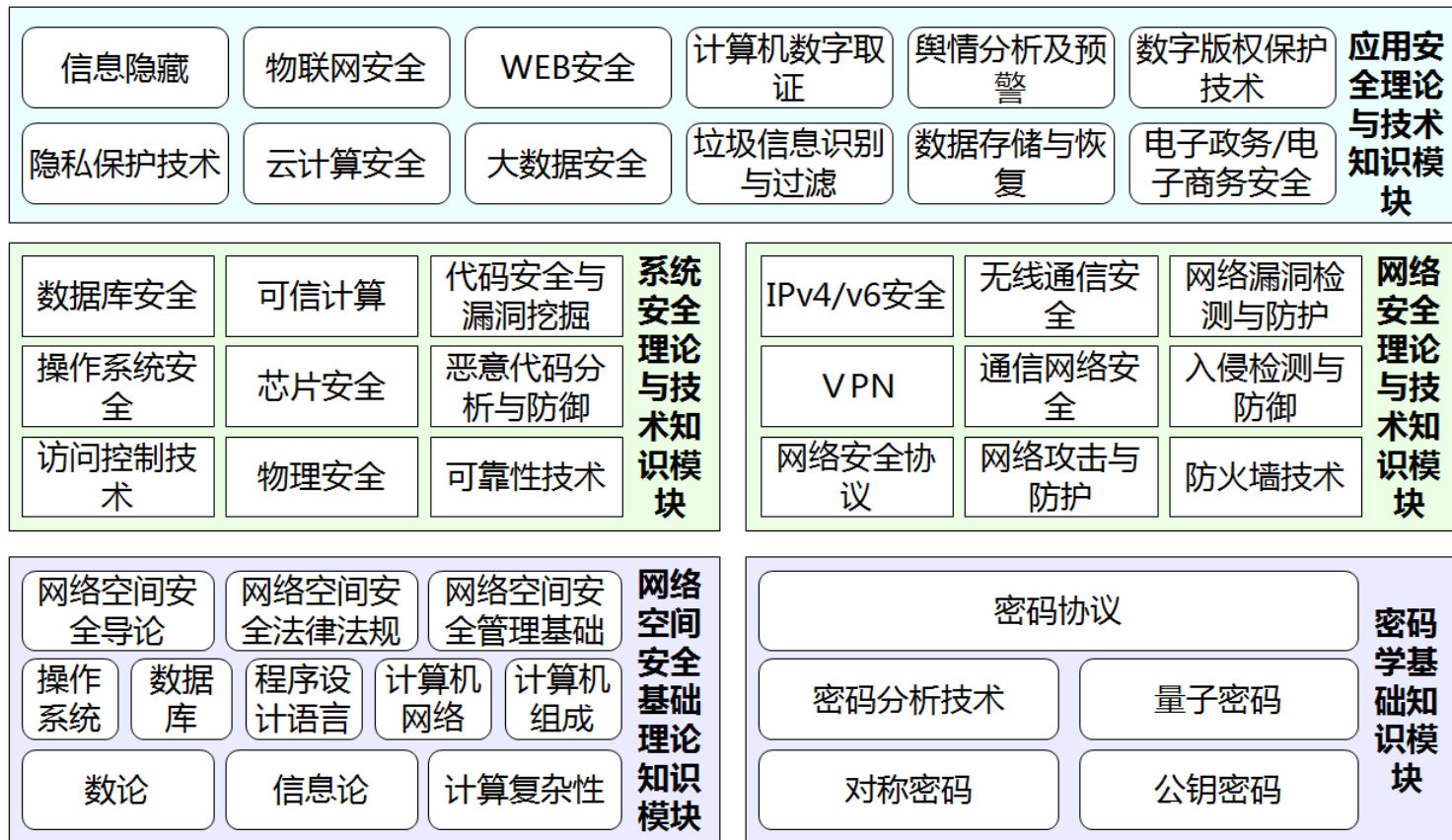
- **网络空间安全**
网络空间既是人的生存环境，也是信息的生存环境，因此网络空间安全是人和信息对网络空间的基本要求。同时，网络空间是所有信息系统的集合，是复杂的巨系统。人在其中与信息相互作用、相互影响。因此，网络空间存在更加突出的信息安全问题。
- **网络空间安全的核心内涵**
 - 信息论的基本观点指出：系统是载体，信息是内涵。
 - 因此，网络空间安全的核心内涵仍是信息安全（信息及其所在系统的安全），没有信息安全就没有网络空间安全。

网络空间安全



网络空间安全一级学科论证报告给出的网络空间安全知识体系

网络空间安全



美国NICE列出的网络空间安全知识体系



内容提纲

1

计算机网络及其脆弱性

2

计算机网络安全

3

计算机网络安全威胁

4

网络安全模型

5

网络安全机制与服务

6

网络安全内容与组织



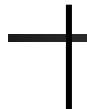


网络安全威胁因素

- 环境和灾害因素

- 温度、湿度、供电、火灾、水灾、地震、静电、灰尘、雷电、强电磁场、电磁脉冲等，均会破坏数据和影响信息系统的正常工作

- 人为因素：多数安全事件是由于人员的疏忽、恶意程序、黑客的主动攻击造成的

- 有意：人为的恶意攻击、违纪、违法和犯罪
 - 无意：工作疏忽造成失误（配置不当等），会对系统造成严重的不良后果
- 



网络安全威胁因素

- 系统自身因素

- 计算机系统硬件系统的故障
- 软件组件：操作平台软件、应用平台软件和应用软件
- 网络和通信协议

- 系统自身的脆弱和不足是造成信息系统安全问题的内部根源，攻击者正是利用系统的脆弱性使各种威胁变成现实



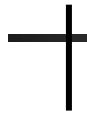
网络安全威胁因素

- 在系统的设计、开发过程中有如下因素会导致系统、软件漏洞：
 - 系统基础设计错误导致漏洞
 - 编码错误导致漏洞
 - 安全策略实施错误导致漏洞
 - 实施安全策略对象歧义导致漏洞
 - 系统设计 / 实施时相关人员刻意留下后门



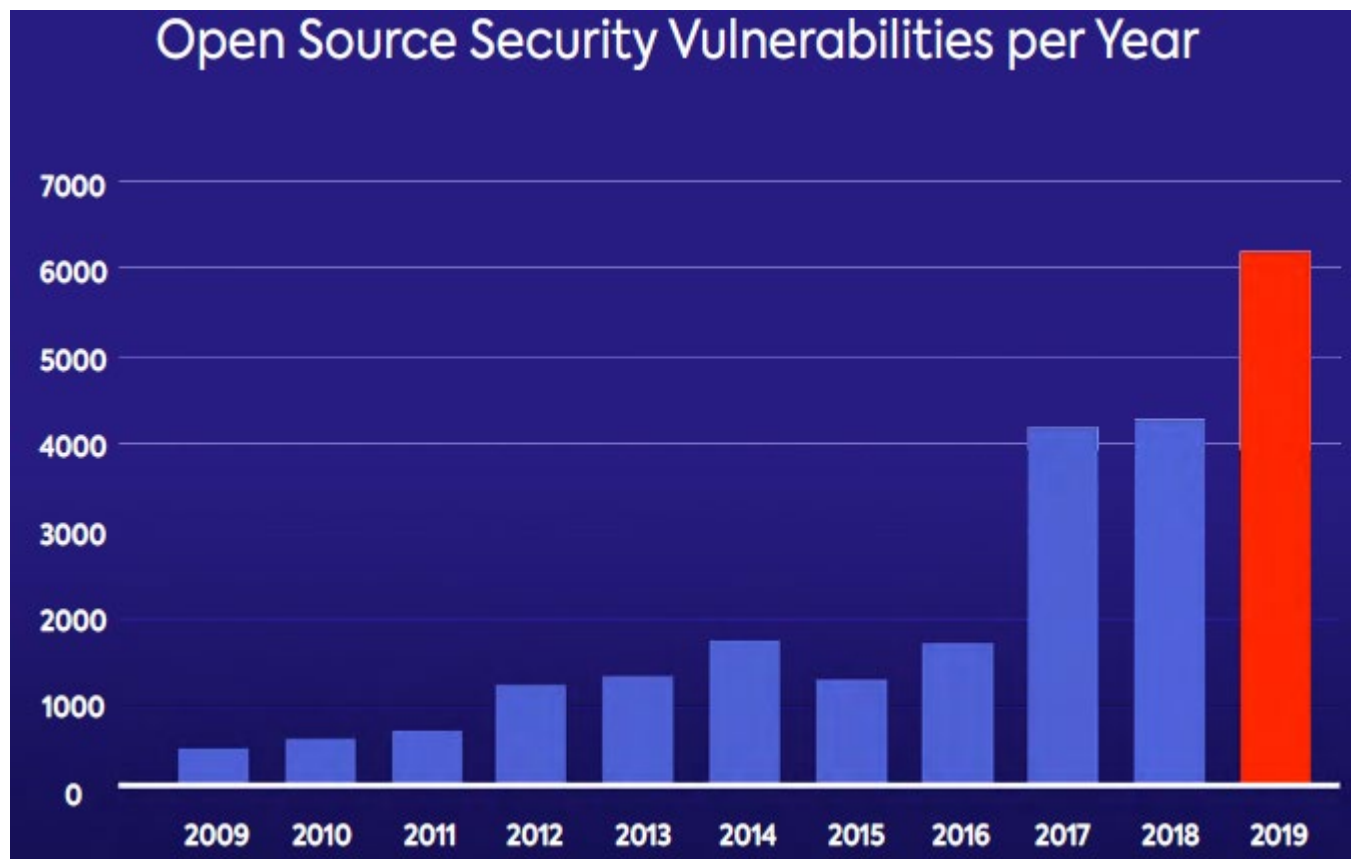


网络安全威胁因素

- 漏洞不仅存在，而且层出不穷， Why?
 - 方案的设计可能存在缺陷
 - 从理论上证明一个程序的正确性是非常困难的
 - 一些产品测试不足，匆匆投入市场
 - 为了缩短研制时间，厂商常常将安全性置于次要地位
 - 系统中运行的应用程序越来越多，相应的漏洞也就不可避免地越来越多
- 

网络安全威胁因素

- 漏洞不仅存在，而且层出不穷， Why?

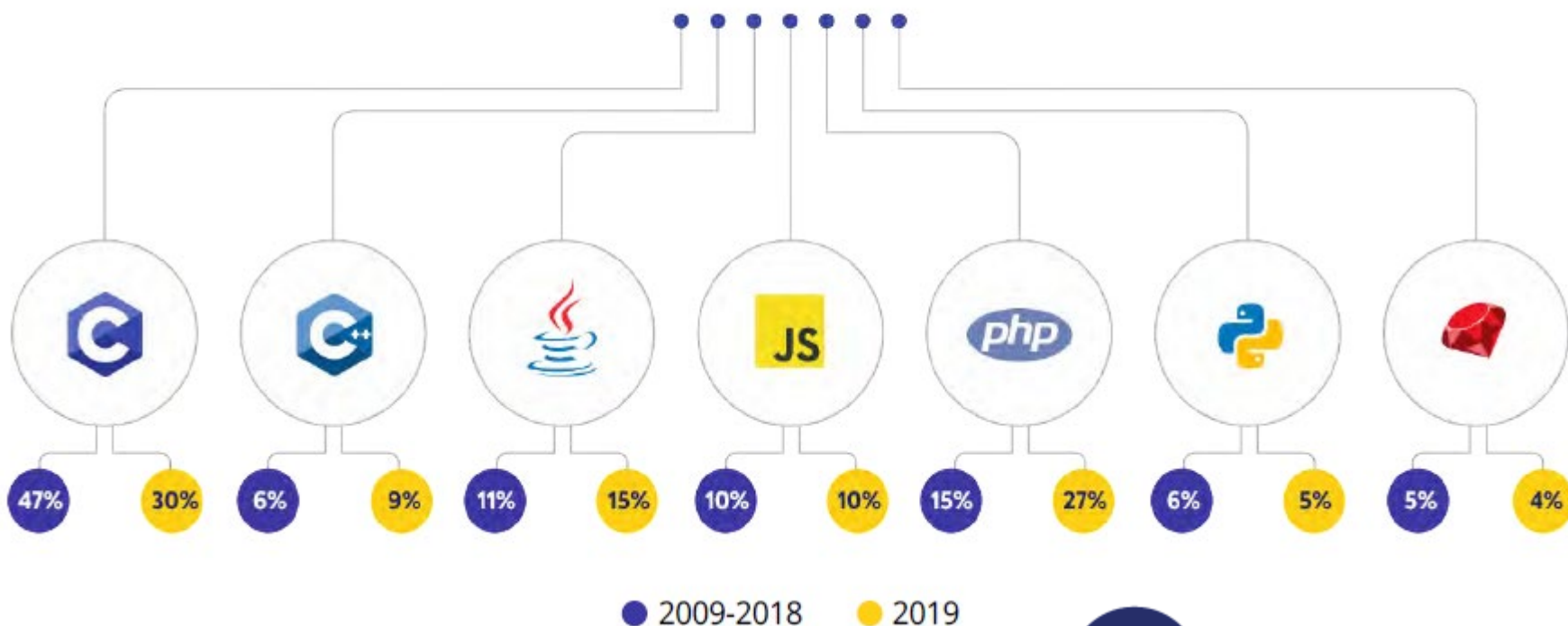


WhiteSource

网络安全威胁因素

- 漏洞不仅存在，而且层出不穷， Why?

Open Source Vulnerabilities per Language, 2019 vs. 2009-2018



WhiteSource



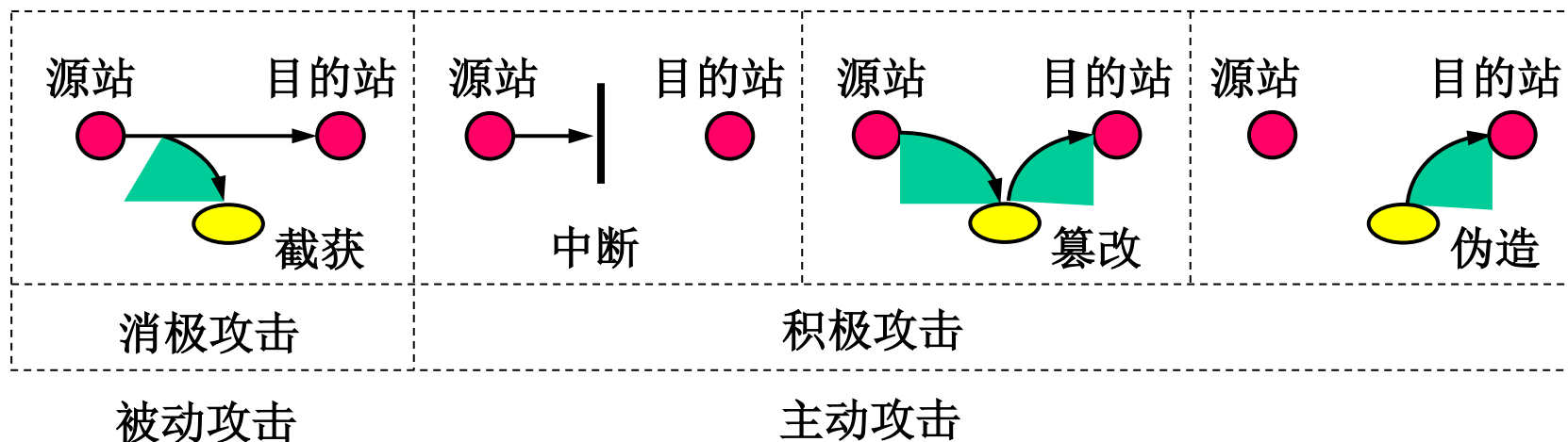
网络攻击

- 从发起攻击的来源来分，可将攻击分为三类：**外部攻击**、**内部攻击**和**行为滥用**
- 从攻击对被攻击对象的影响来分，可分为**被动攻击**和**主动攻击**
 - 主动攻击：**伪装、重放、修改报文、拒绝服务**
 - 被动攻击：**监听传输的报文内容、通信流量分析**



网络攻击

■ Stallings : 基于攻击实施手段的网络攻击分类





网络攻击

■ Icove分类：基于经验术语分类方法

- | | |
|-----------|----------------|
| ◆ 病毒和蠕虫 | ◆ IP 欺骗 |
| ◆ 资料欺骗 | ◆ 口令窃听 |
| ◆ 拒绝服务 | ◆ 越权访问 |
| ◆ 非授权资料拷贝 | ◆ 扫描 |
| ◆ 侵扰 | ◆ 逻辑炸弹 |
| ◆ 软件盗版 | ◆ 陷门攻击 |
| ◆ 特洛伊木马 | ◆ 隧道 |
| ◆ 隐蔽信道 | ◆ 伪装 |
| ◆ 搭线窃听 | ◆ 电磁泄露 |
| ◆ 会话截持 | ◆ 服务干扰 |





一般攻击过程

足迹追踪: **Target Footprinting**

远端扫描: **Remote Scanning**

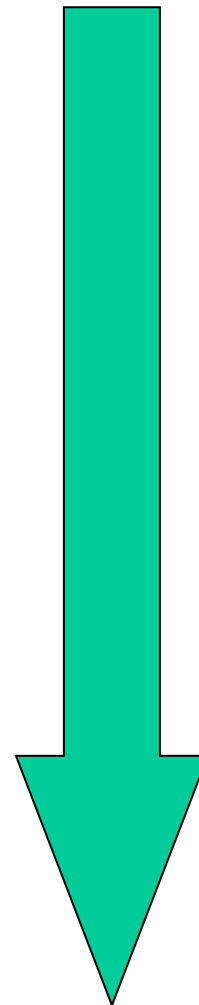
资源列举: **Resource Enumerating**

权限获取: **Access Gaining**

权限提升: **Privilege Escalating**

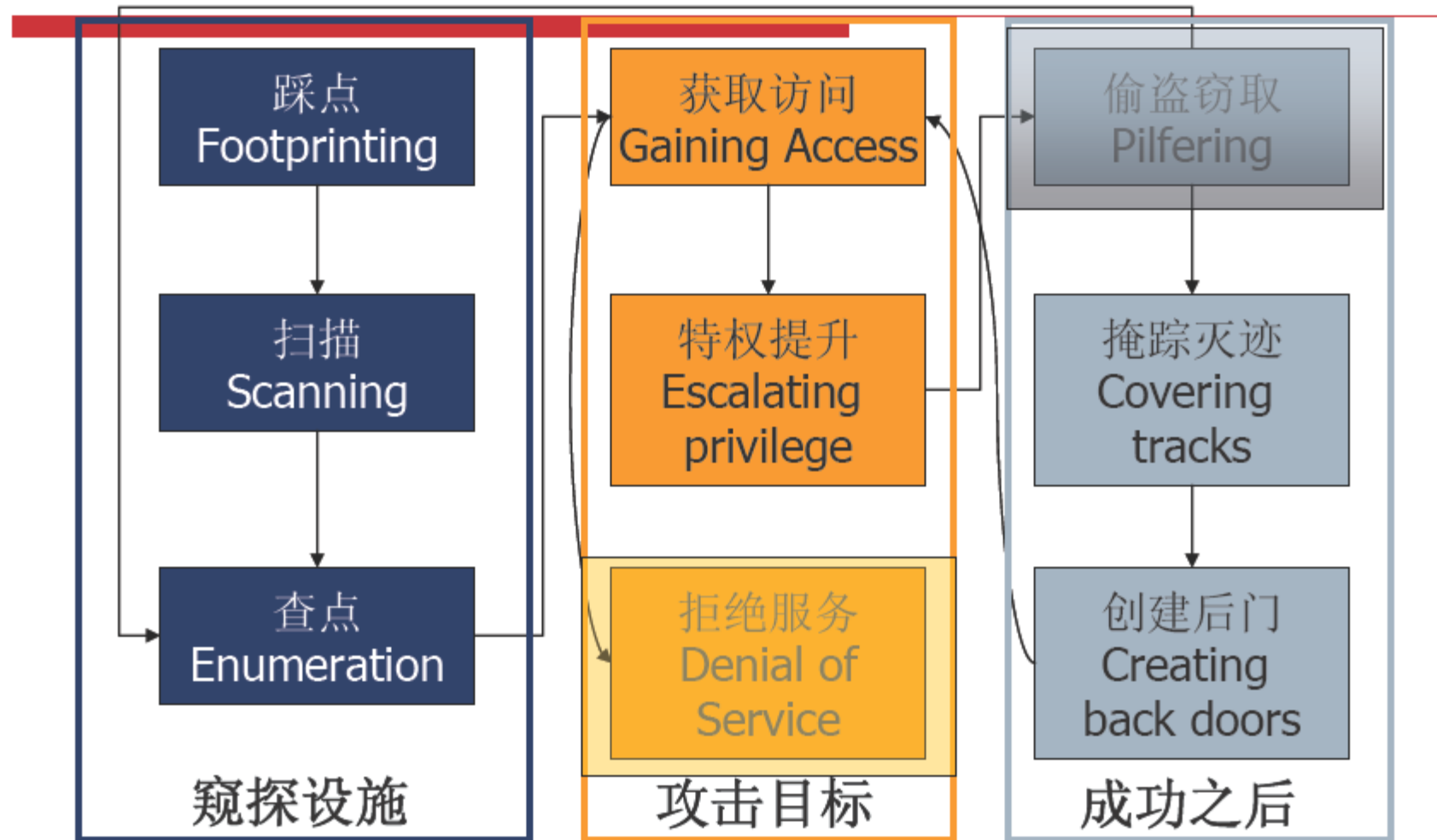
设置后门: **Backdoors Creating**

毁踪灭迹: **Tracks Covering**



一般攻击过程

《黑客大曝光》——黑客剖析图





APT攻击

保持
隐蔽

确定目标

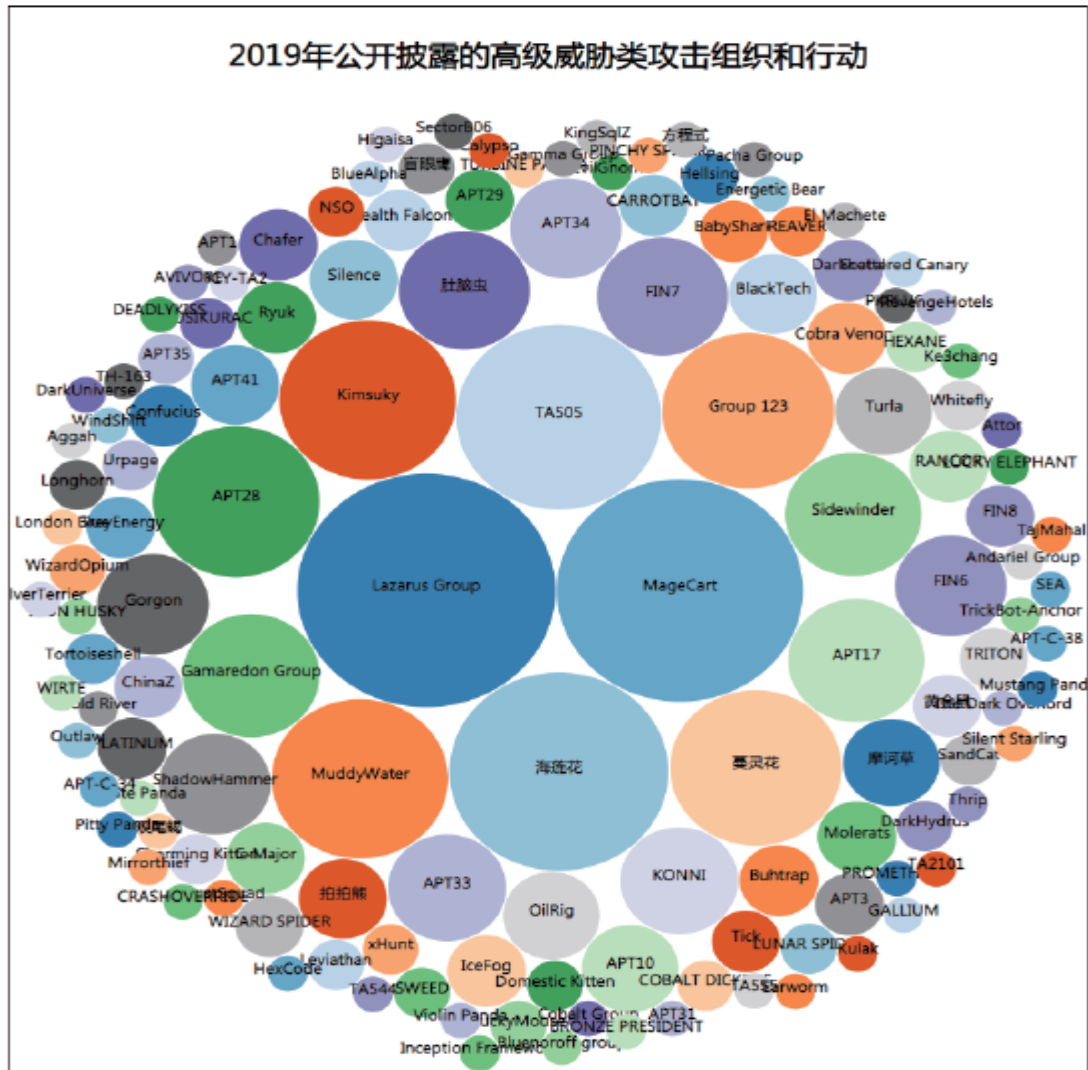
搜集信息

长期渗透

开展攻击

- 恶意代码
- 系统和软件漏洞
- 社会工程学
-

APT攻击





内容提纲

1

计算机网络及其脆弱性

2

计算机网络安全

3

计算机网络安全威胁

4

网络安全模型

5

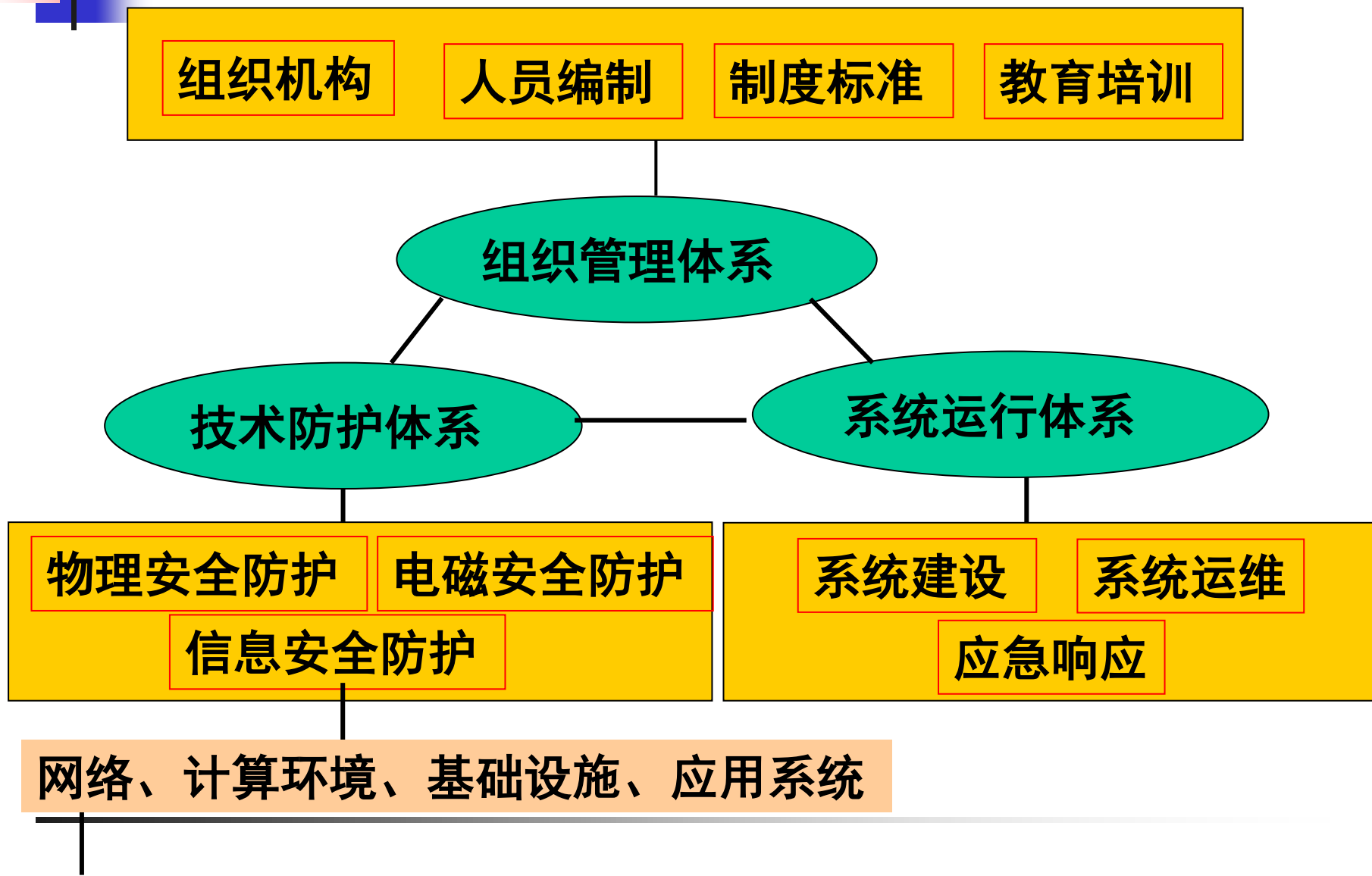
网络安全机制与服务

6

网络安全内容与组织



网络安全保障体系





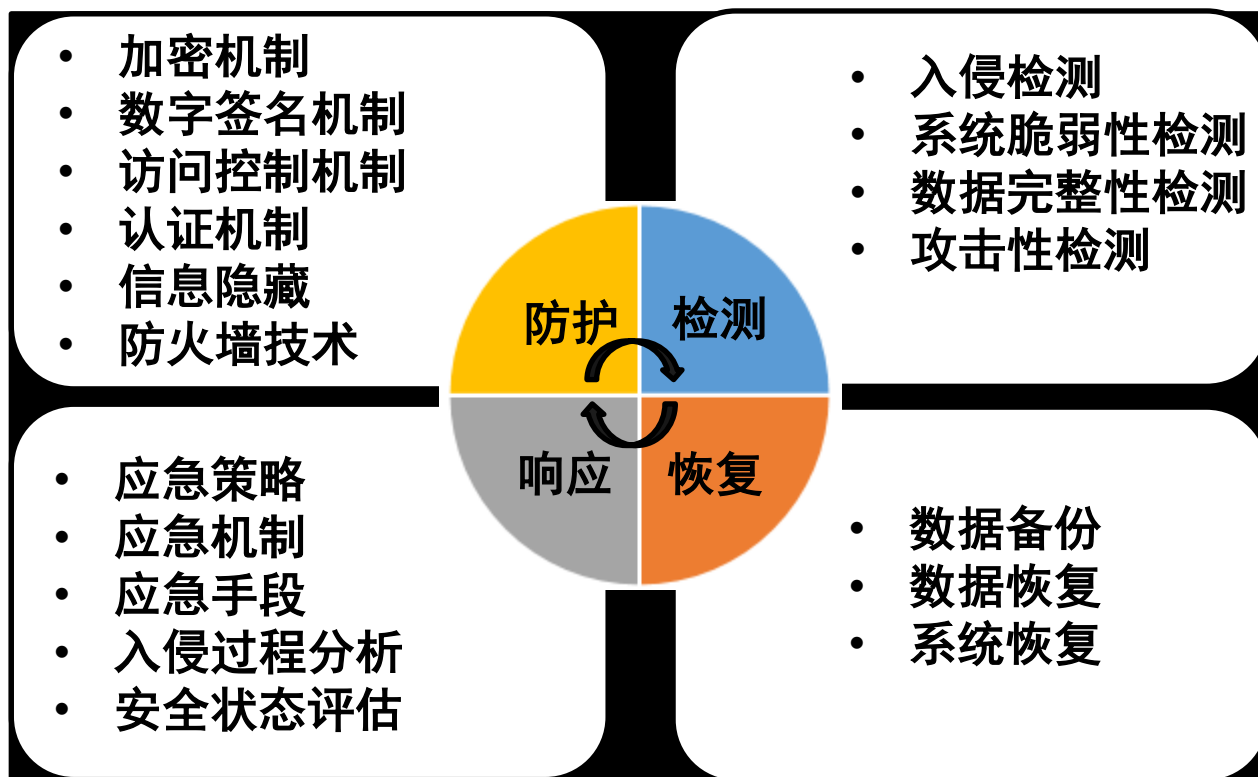
网络安全模型

- 网络安全模型以建模的方式给出**解决安全问题的过程和方法**，主要包括：
 - 准确描述构成安全保障机制的要素以及要素之间的相互关系；
 - 准确描述信息系统的行为和运行过程；
 - 准确描述信息系统行为与安全保障机制之间的相互关系



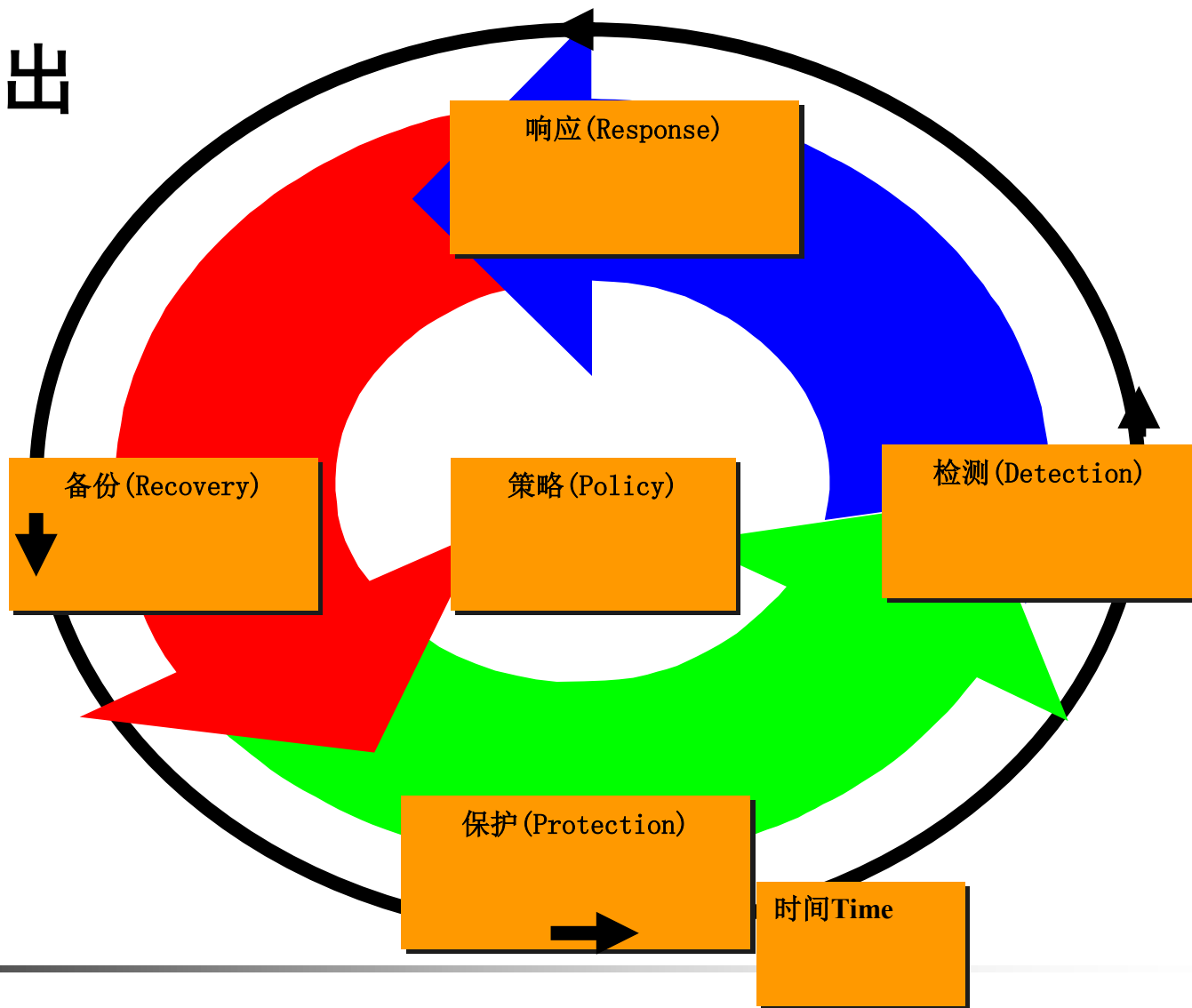
PDRR模型

- DoD提出：防护（Protection）、检测（Detection）、恢复（Recovery）、响应（Response）



P2DR模型

■ ISC提出





IATF框架

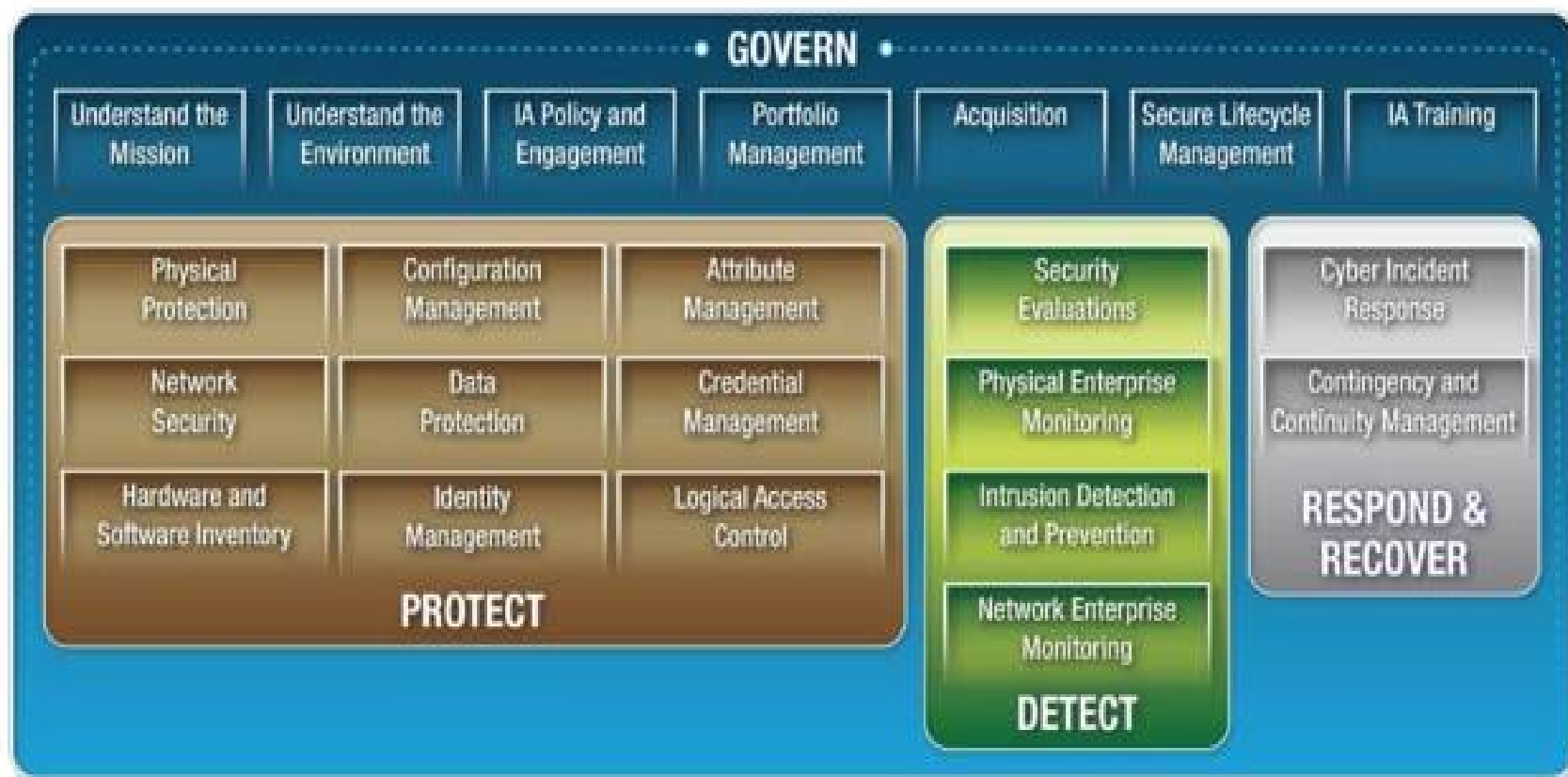
- IATF从整体、过程的角度看待信息安全问题，认为稳健的信息保障状态意味着信息保障的策略、过程、技术和机制在整个组织的信息基础设施的所有层面上都能得以实施，其代表理论为“深度防护战略”。IATF强调人、技术、操作三个核心要素，关注四个信息安全保障领域：保护网络和基础设施、保护边界、保护计算环境、支撑基础设施，为建设信息保障系统及其软硬件组件定义了一个过程，依据纵深防御策略，提供一个多层次的、纵深的安全措施来保障用户信息及信息系统的安全

IATF框架

- IATF定义的要三要素中，人是信息体系的主体，是信息系统的拥有者、管理者和使用着，是信息保障体系的核心，同时也是**最脆弱的**。
 - 人是第一位的要素：**安全管理的重要性**
 - 针对人的攻击：社会工程学攻击



CGS框架





内容提纲

1

计算机网络及其脆弱性

2

计算机网络安全

3

计算机网络安全威胁

4

网络安全模型

5

网络安全机制与服务

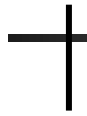
6

网络安全内容与组织





网络安全体系结构

- ISO于1988年发布了ISO 7498-2标准，即开放系统互联(OSI, Open System Interconnection)安全体系结构标准，该标准等同于国家标准的GB/T 9387.2-1995。1990年，ITU决定采用ISO 7498-2作为其X.800推荐标准。因此，X.800和ISO 7498-2标准基本相同。1998年，RFC 2401给出了Internet协议的安全结构，定义了IPsec适应系统的基本结构，这一结构的目的是为IP层传输提供多种安全服务
- 



安全体系结构

- 提供了安全服务和安全机制的一般性描述（这些安全服务和安全机制都是网络系统为保证安全所配置的哪些部分、哪些位置必须配备哪些安全服务和安全机制），指明在网络系统中，并规定如何进行安全管理





安全机制

- 定义：用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程（或实现该过程的设备、系统、措施或技术）



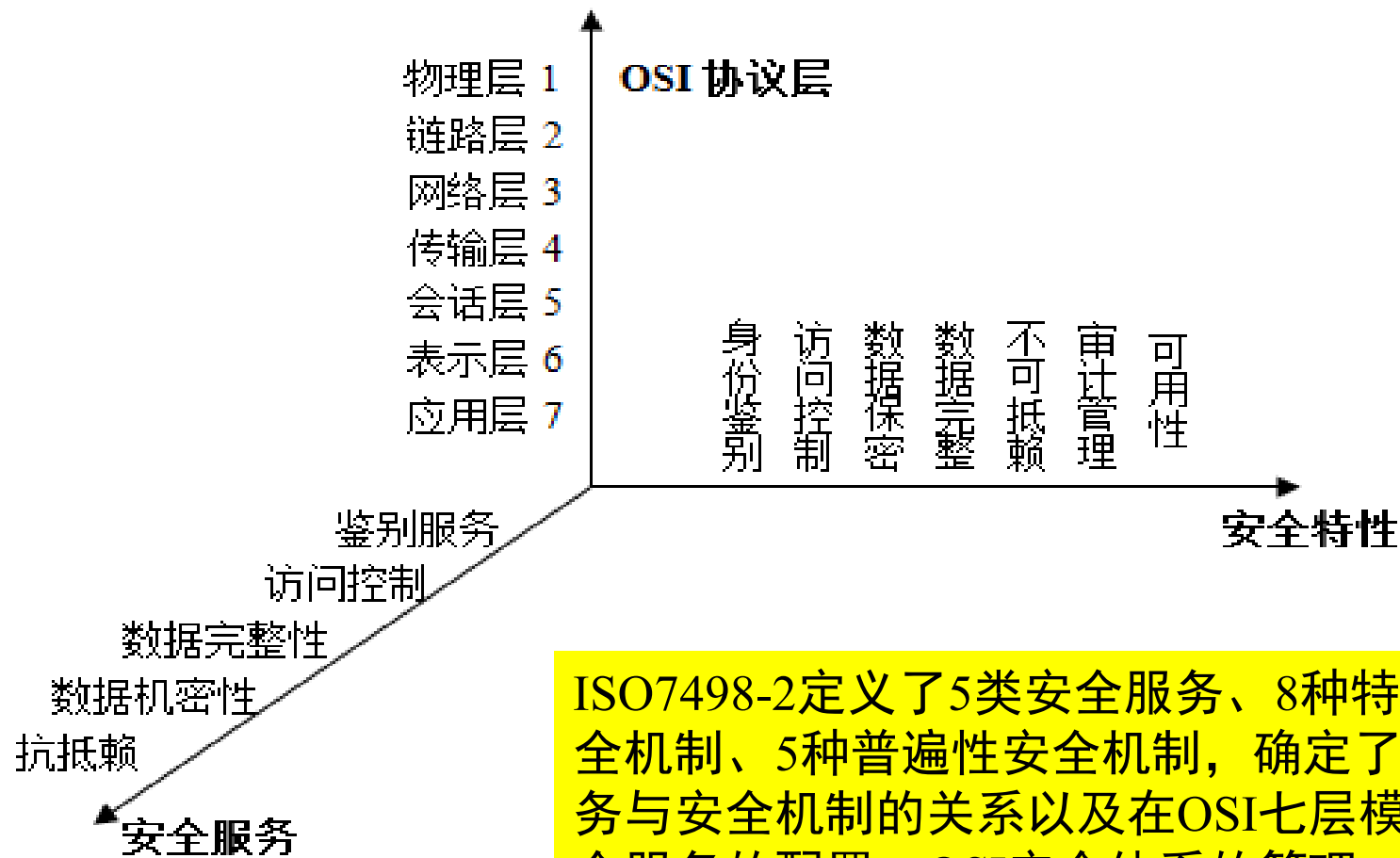


安全服务

- 定义：指加强数据处理系统和信息传输的安全性的处理过程或通信服务，主要利用一种或多种安全机制对攻击进行反制来实现



ISO安全机制与安全服务



ISO7498-2定义了5类安全服务、8种特定的安全机制、5种普遍性安全机制，确定了安全服务与安全机制的关系以及在OSI七层模型中安全服务的配置、OSI安全体系的管理。

ISO安全机制与安全服务

表 1-1 安全服务与安全机制的关系

服务 \ 机制	加密机制	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	公证机制
对等实体认证	√	√			√			
数据源认证	√	√						
访问控制服务			√					
连接机密性	√						√	
无连接机密性	√						√	
选择字段机密性	√							
通信业务流机密性	√					√	√	
带恢复的连接完整性	√			√				
不带恢复的连接完整性	√			√				
选择字段连接完整性	√			√				
无连接完整性	√	√		√				
选择字段无连接完整性	√	√		√				
不可抵赖，带交付证据		√		√				√

ISO安全机制与安全服务

表 1-2 安全服务与基于 TCP/IP 体系结构服务层关系

安全服务	TCP/IP 协议层			
	网络接口层	网络层	运输层	应用层
对等实体鉴别		✓	✓	✓
数据原发鉴别		✓	✓	✓
访问控制		✓	✓	✓
连接机密性	✓	✓	✓	✓
无连接机密性	✓	✓	✓	✓
选择字段机密性				✓
通信业务流机密性	✓	✓		✓
带恢复的连接完整性			✓	✓
不带恢复的连接完整性		✓	✓	✓
选择字段的连接完整性				✓
无连接完整性		✓	✓	✓
选择字段无连接完整性				✓
不可抵赖				✓



内容提纲

1

计算机网络及其脆弱性

2

计算机网络安全

3

计算机网络安全威胁

4

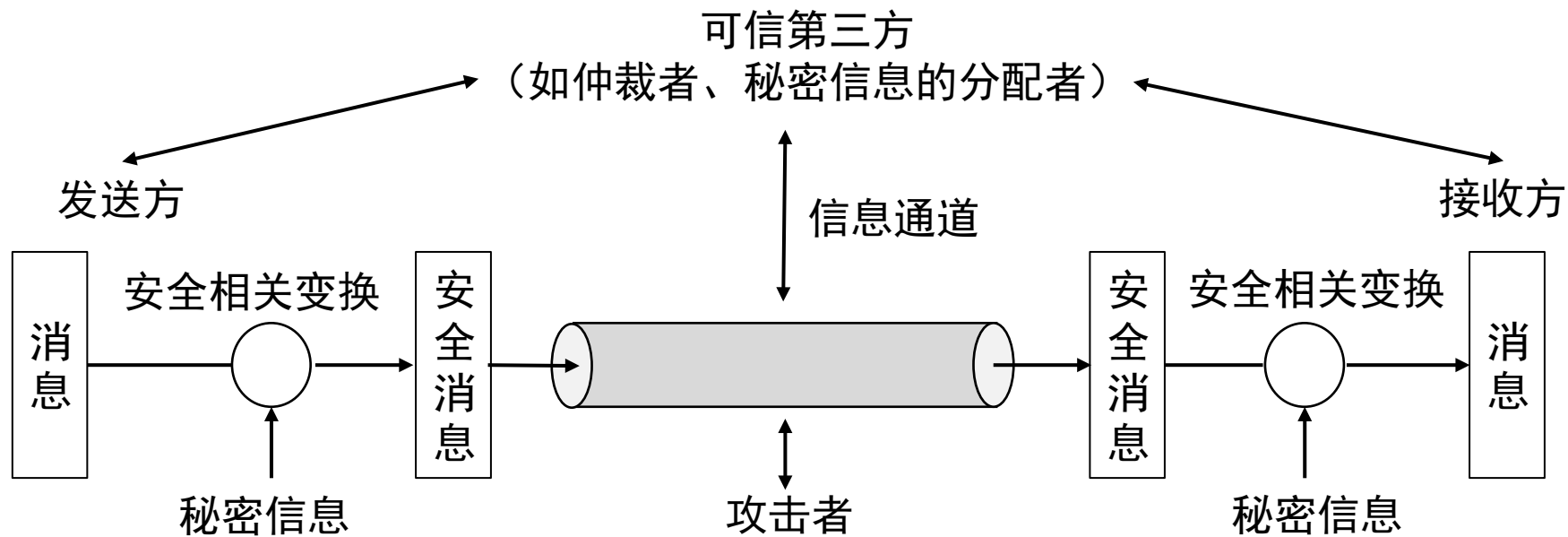
网络安全模型

5

网络安全机制与服务

6

网络安全内容与组织



网络通信安全模型

消息认证（源认证、目的认证、完整性、真实性）、不可否认（数字签名）

第4章 PKI与数字证书

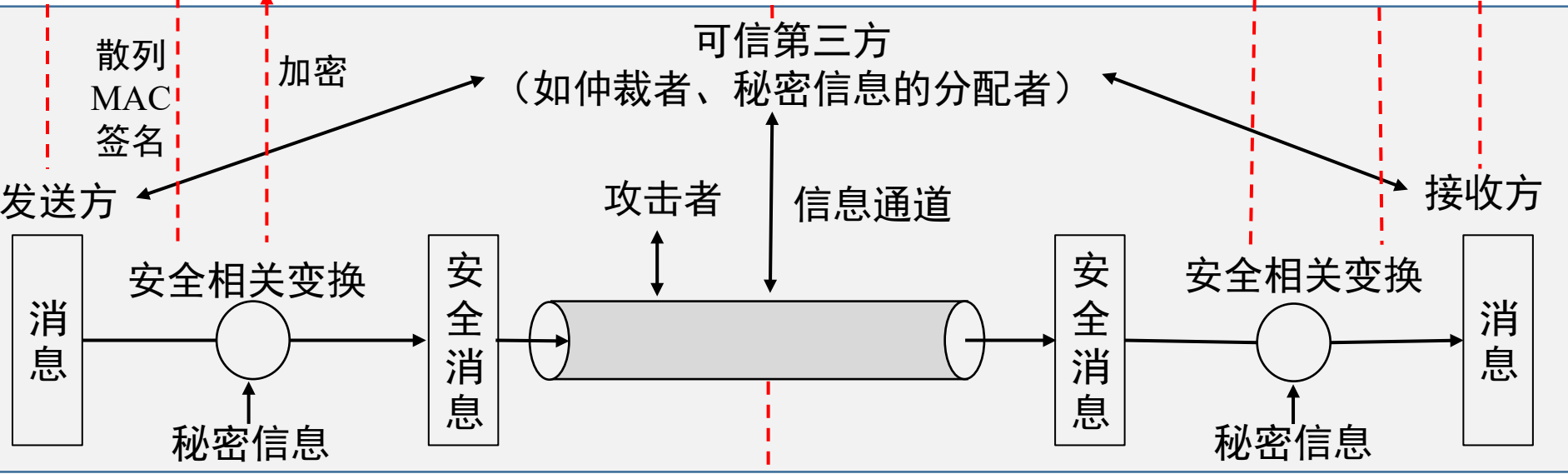
验证（散列，MAC，签名）

第3章 认证与数字签名

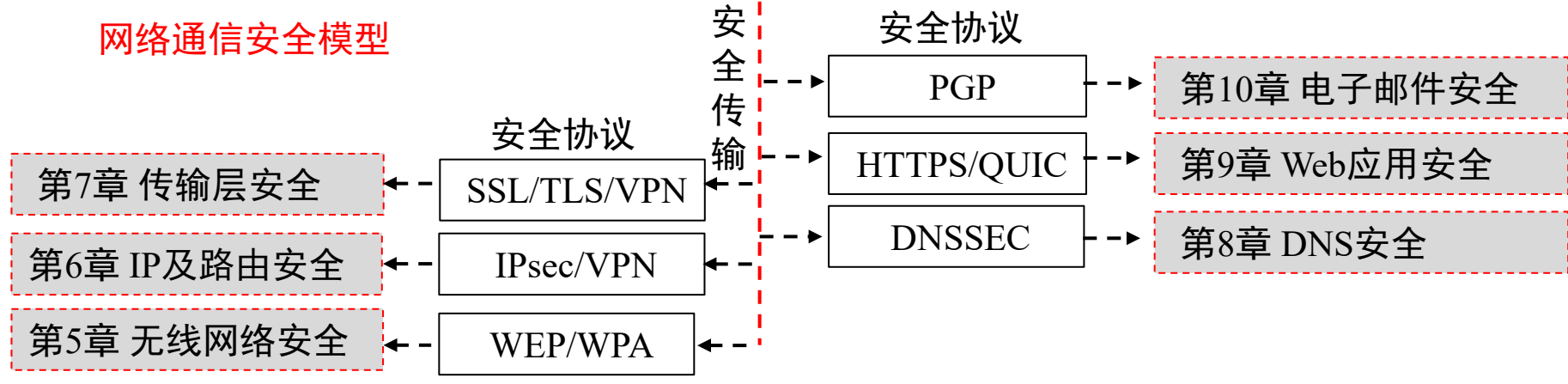
第2章 密码学基础知识

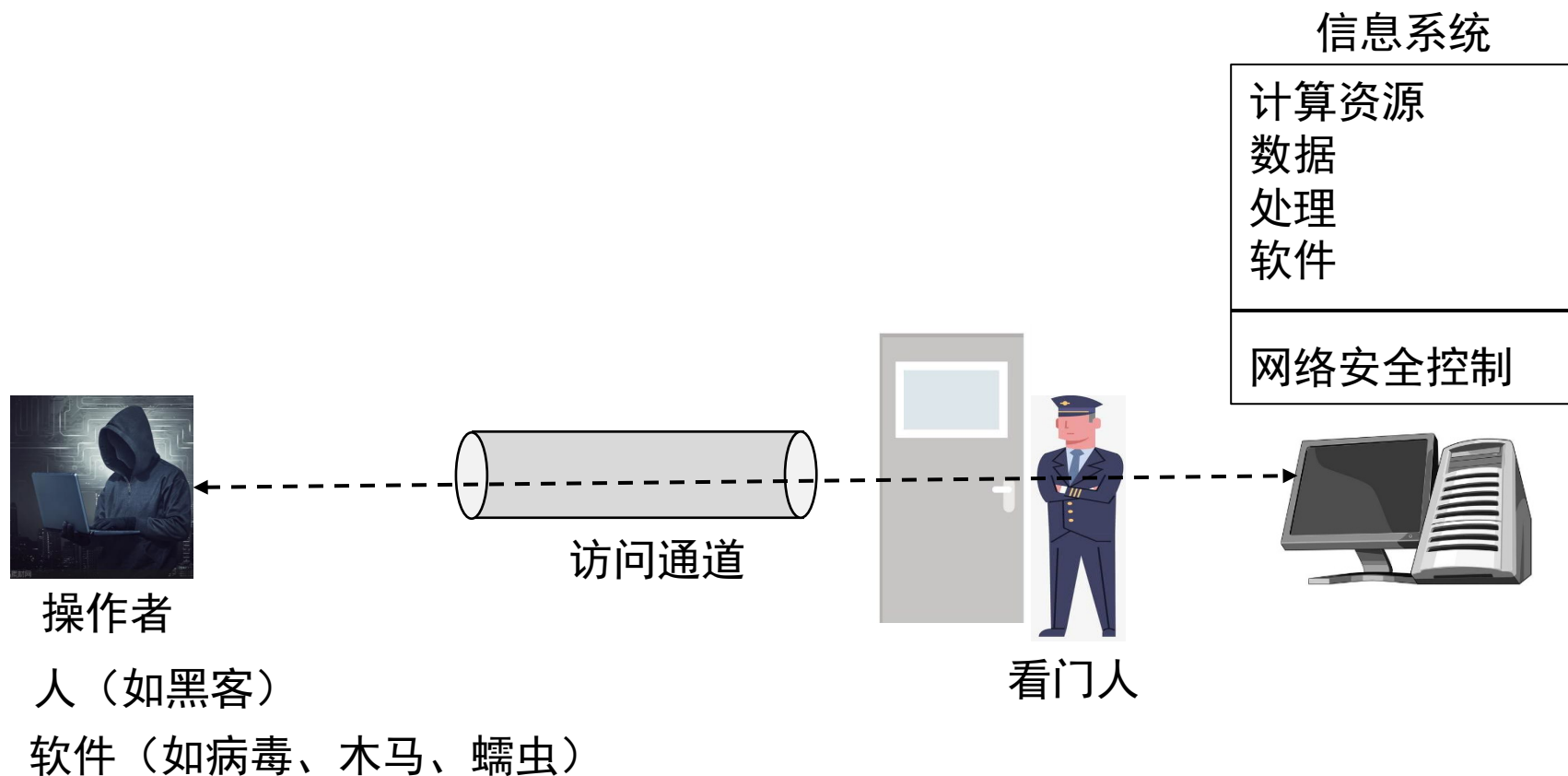
KDC, CA

解密

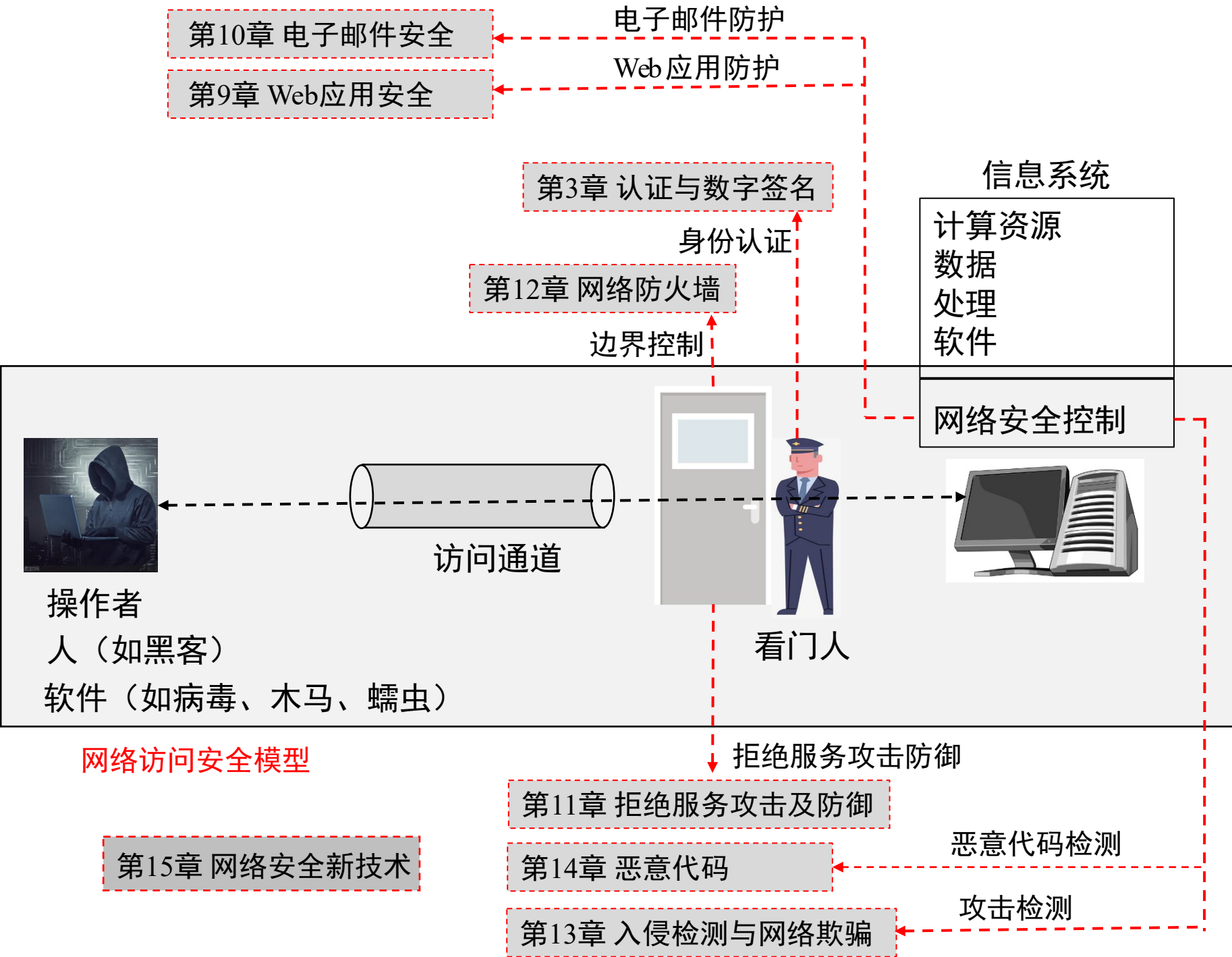


网络通信安全模型





网络访问安全模型





网络安全新技术

- 移动目标防御(Moving Targeting Defense, MTD)
- 网络空间拟态防御(Cyber Mimic Defense, CMD)
- 零信任安全(Zero Trust, ZT)
- 软件定义网络安全 (Software-Defined Network, SDN)

第15章 网络安全新技术



网络安全防护技术

第11章 拒绝服务攻击及防御

第15章 网络安全新技术

第13章 入侵检测与网络欺骗

第12章 网络防火墙

第9章

第10章

第14章 恶意代码

应用层

电子邮件(SMTP/POP3/IMAP)

Web应用(HTTP)

域名解析系统(DNS)

传输层

UDP

TCP

ICMP

IGMP

BGP

OSPF

IPv4 / IPv6

网络层

RARP

RIP

ARP

网络接口层

与各种网络接口

无线接入网

物理硬件

TCP/IP协议栈

第10章 电子邮件安全

第9章 Web应用安全

第8章 DNS安全

第7章 传输层安全

第6章 IP及路由安全

第5章 无线网络安全

第4章 PKI与数字证书

第3章 认证与数字签名

第2章 密码学基础知识

第1章 概述

网络安全协议

PGP

HTTPS/QUIC

DNSSEC

SSL/TLS/VPN

IPsec/VPN

WEP/WPA/移动

身份认证

消息认证

数字签名

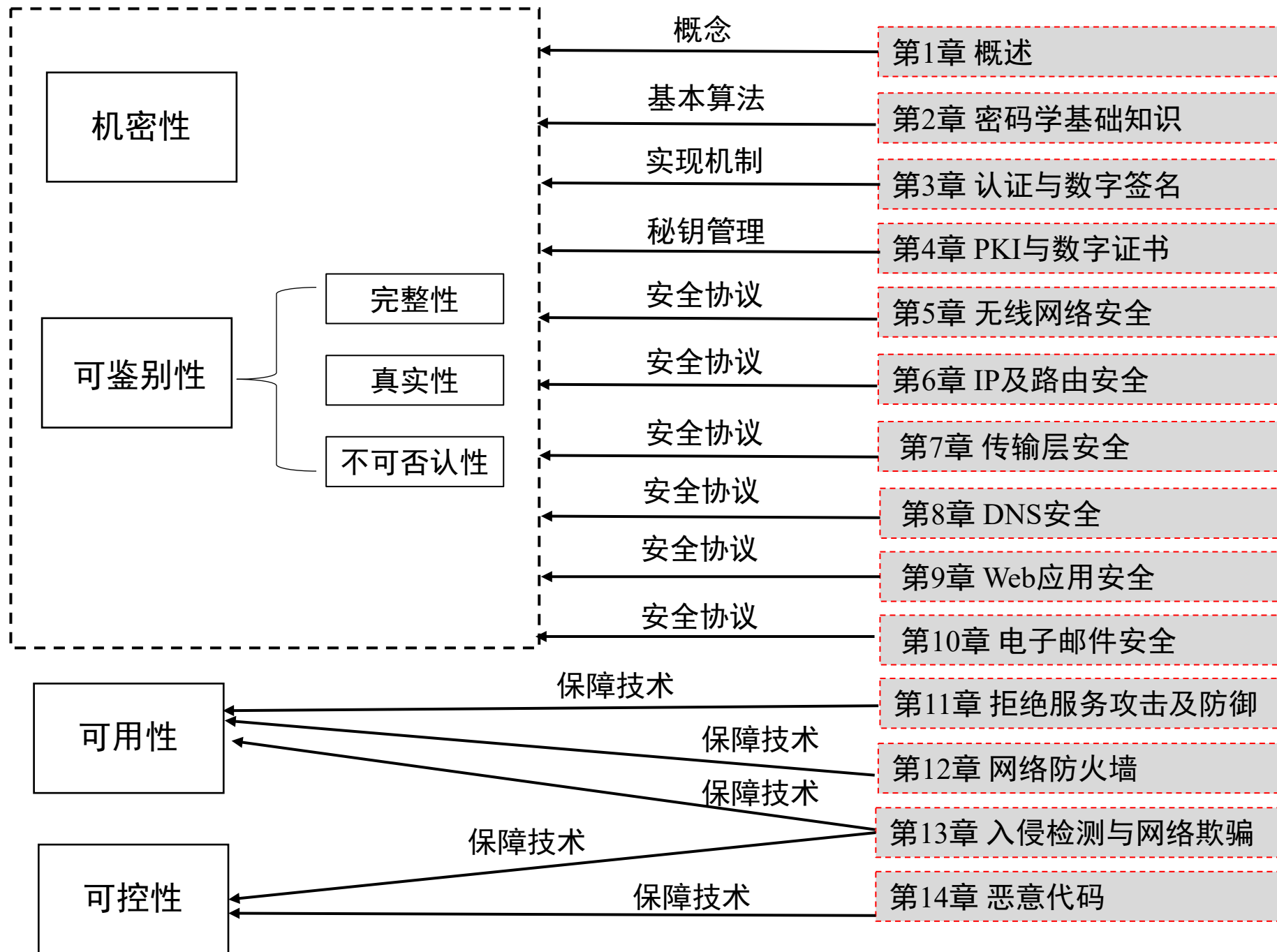
对称密码

公开密码

公钥基础设施

公钥分发

网络安全基础





本章小结





作业

