网络安全技术

北京邮电大学 计算机学院

张冬梅

第1部分 加密与认证

第1章 引言

第 1 章 引言

- 1.1 网络安全概念与安全需求
- 1.2 安全攻击
- 1.3 安全服务
- 1.4 安全机制
- 1.5 网络安全模型
- 1.6 安全标准

1.1 网络安全概念与安全需求

- 应用数据处理设备之前：物理和管理方法保障信息安全
- 信息安全的两次重大变革
  - 引入计算机之后：计算机安全[Computer Security]
  - 分布式系统、计算机网络的广泛使用：网络安全[Network Security]

网络中主要安全冲突范例

- 情况1：用户A发送文件给用户B（窃听[eavesdrop]）
- 情况2：管理员D发送指令给计算机E（篡改[tampering]）
- 情况3：用户F假冒管理员D发送指令给计算机E（伪造[forgery]）
- 情况4：被解雇的员工K截取并延长系统服务器的注销消息（延迟）
- 情况5：客户发送指示给股票经纪人，事后否认（否认[deny]）

网络安全需求

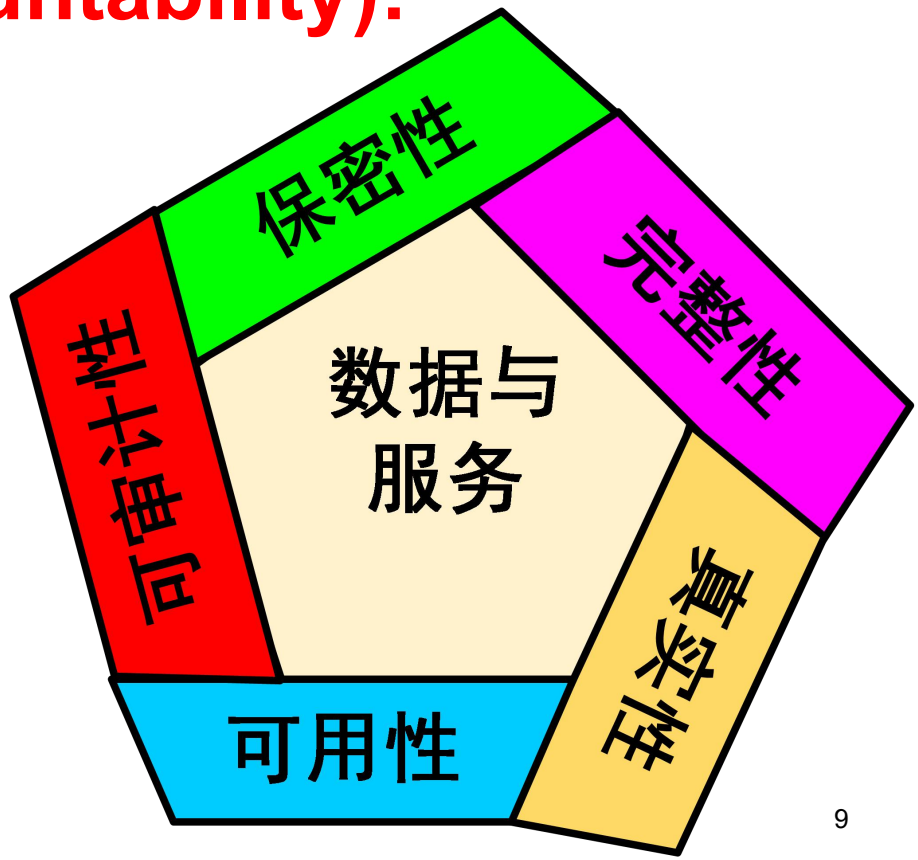
- **信息安全：**在既定的安全密级的条件下，信息系统抵御**意外事件**或**恶意行为**的能力，这些事件和行为将危及所存储、处理或传输的**数据**以及经由这些系统所提供的**服务**的**可用性**[Availability]、**机密性**[Confidentiality]、**完整性**[Integrity]、**非否认**[non-repudiation]和**真实性**[Authenticity]。
- 网络安全：除了要考虑**网络自身的安全因素**外，还必须考虑**操作系统、数据库、应用系统、人员管理**等因素。

计算机安全性质

- **机密性(Confidentiality):**
  - 数据机密性：保证信息不会被泄露给未经授权的实体。
  - 隐私性：保证个人可以控制和影响与之相关的信息，这些信息由可能被收集、存储和泄露。
- **完整性(Integrity):**
  - 数据完整性：确保信息和程序只能以特定和授权的方式进行改变；
  - 系统完整性：确保系统以一种正常的方式来执行预定的功能，免于有意或无意的非授权操作特定和授权的方式进行改变；
- **可用性(Availability):** 确保系统能工作迅速，对授权用户不能拒绝服务。

计算机安全性质（续）

- **真实性(authenticity):** 指保证实体(人、进程或系统)身份或信息、信息来源的真实性。
- **可审计性/可计量性(Accountability):** 指每个实体的行为可以被唯一地追溯到该实体。



CIA三元组

- 信息安全最基本的概念：CIA三元组
  - 这里的C，指的是Confidentiality机密性
  - 这里的I，指的是Integrity完整性
  - 这里的A，指的是Availability可用性
- NIST的FIPS199指出：机密性、完整性和可用性是信息和信息系统的三个安全目标。

	安全需求	安全缺失
保密性	对信息的访问和公开进行授权限制，包括保护个人隐私和秘密信息	信息的非授权泄露
完整性	防止对信息的非授权修改或破坏，包括确保信息的不可否认性和真实性	信息的非授权修改和损坏
可用性	确保对信息的及时和可靠的访问和使用	对信息和信息系统访问和使用的中断。

举例：典型应用环境的安全需求

应用环境	安全需求
所有网络	(1)阻止外部的入侵
银行	(1)避免欺诈或交易的意外修改; (2)识别零售的交易顾客 (3)保护个人识别号(PIN)以免泄露; (4)确保顾客的秘密
电子交易	(1)确保交易的起源和完整性; (2)保护共同的秘密 (3)为交易提供合法的电子签名
政府	(1)避免无密级而敏感的信息的未授权泄露或修改 (2)为政府文件提供电子签名
公共电信载体	(1)对授权的个人限制访问管理功能; (2)避免服务中断 (3)保护用户的秘密
互联/专用网络	(1)保护团体/个人的秘密; (2)确保消息的真实性

计算机安全挑战

- 安全问题非常复杂，需要缜密充分的论证推理
- 设计安全机制和算法，需要考虑其潜在攻击
- 安全机制需要慎重考虑使用场合
- 需要复杂的机制产生、分配和保护机密信息
- 攻击与防御是智力对抗，攻击者只需发现利用一个弱点即可，防御者需要防御所有弱点。
- 安全投入不直接产生经济效益
- 安全需要定时经常性监控和持续改进
- 安全性与易用性是矛盾的

1.2 安全体系结构

- **安全威胁**：破坏安全的**潜在可能，**是脆弱性被利用而可能带来的危险
- **安全攻击**：任何可能会**危及信息安全**的**行为**

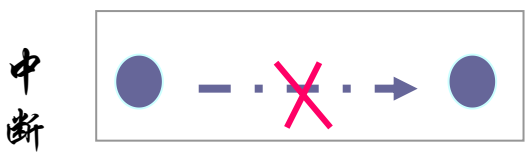
安全攻击	产生的后果
窃听	破坏机密性
篡改与伪造	破坏完整性
拒绝服务	破坏可用性
欺骗（或假冒）	破坏(身份)真实性
否认	破坏可计量性

CIA

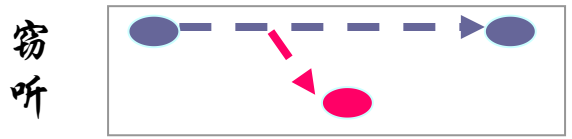
- **安全机制**：用来**检测、防范安全攻击**并从中**恢复系统**的机制
- **安全服务**：增强数据处理系统安全性和信息传递安全性的服务,用来**防范安全攻击,利用一种或多种安全机制来提供服务**。

1.3 安全攻击

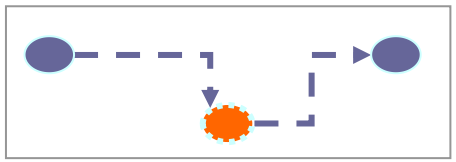
- 网络通信面临的潜在威胁
  - 中断Interruption
  - 窃听Interception
  - 篡改Modification
  - 假冒Fabrication



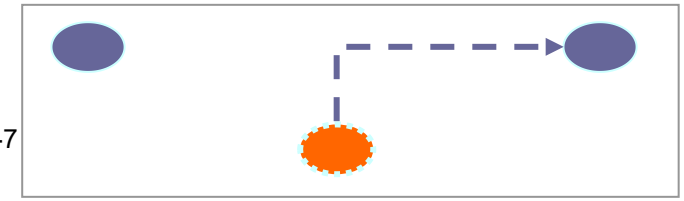
可用性



机密性



完整性



真实性

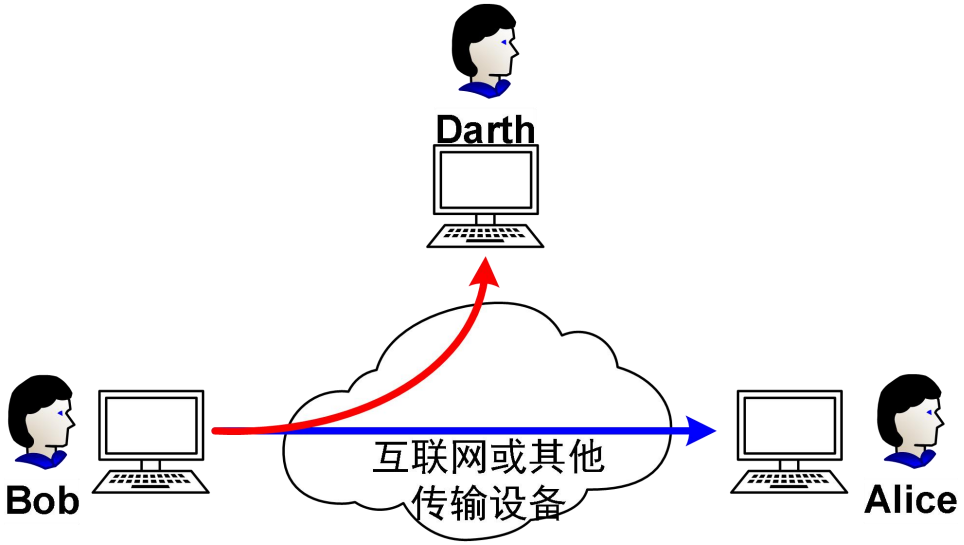
1.3 安全攻击

- 安全攻击的分类（X.800和RFC2828）
  - 被动攻击[Passive Attacks]：企图了解或利用系统信息但是不影响系统资源(只监听信息，不对其进行修改)。
  - 主动攻击[Active Attacks]：试图改变系统资源或影响操作系统(监听而且修改信息)

1.3.1 被动攻击

- 目标：获取传输的信息
- 两种形式
  - 窃听：消息内容泄露攻击
  - 监测：通信量(流量)分析

    [traffic analysis]攻击

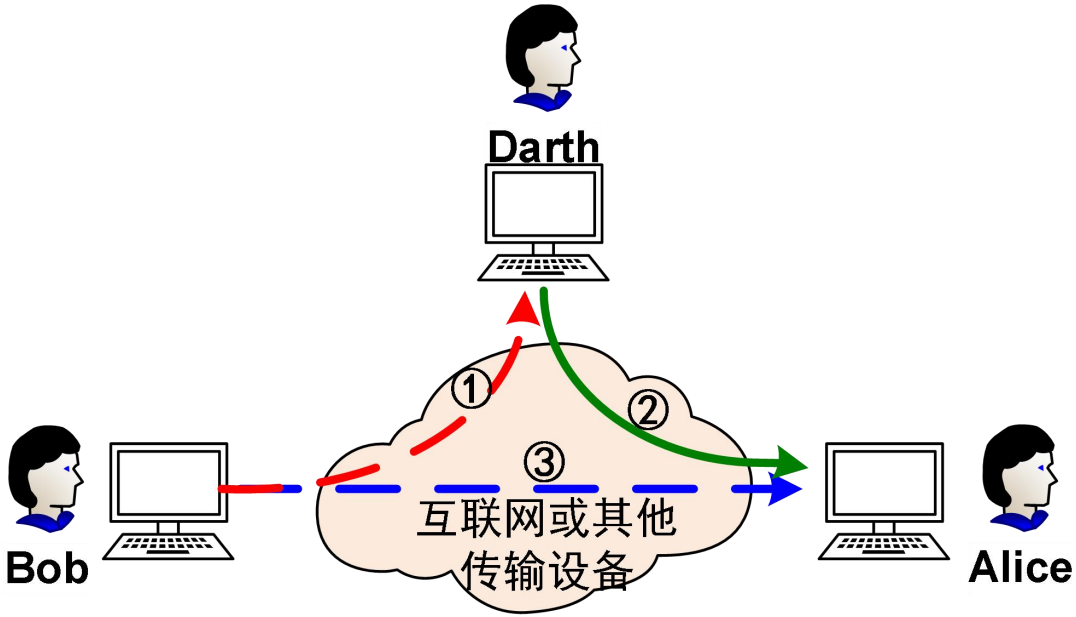


- 特点：不改变数据，难以检测
- 防范攻击的方法：加密技术

对付被动攻击的重点是防范而非检测

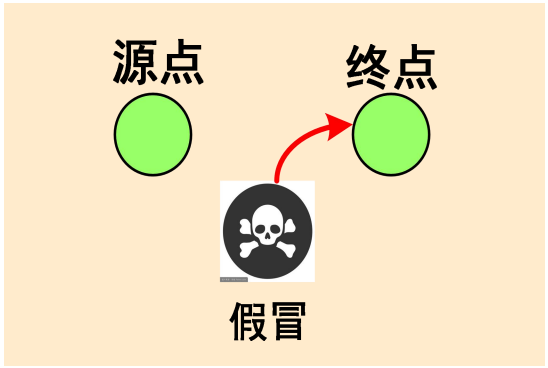
1.3.2 主动攻击

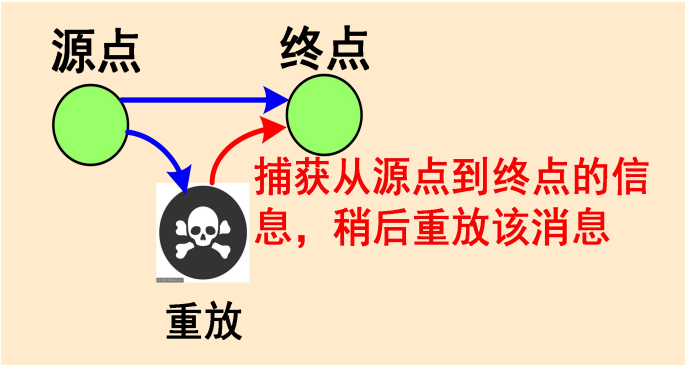
- 目标：修改或添加数据的内容
- 能够检测，但是防范困难



1.3.2 主动攻击

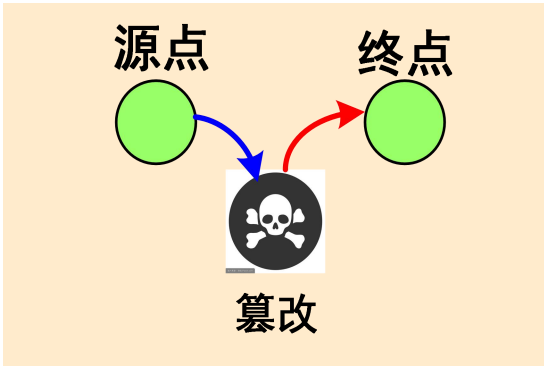
- 典型方法
  - 假冒[masquerade]：一个实体假冒成另一个不同的实体
  - 重放[replay]：指攻击者未经授权地将截获的信息再次发送(re-use of observed data to produce an unauthorised effect)

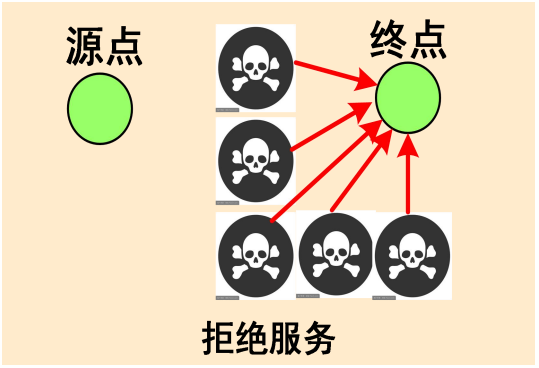




1.3.2 主动攻击

- 篡改[modification]：修改、延迟或者重排消息
- 拒绝服务[denial of service]：阻止或禁止对通信设备的正常使用或管理。





1.4 安全服务

- **背景：**为了有效评估某个机构的安全需求，并选择各种安全策略与产品，安全管理员需要系统性方法来定义安全需求以及满足这些需求的服务。
- **X.800的定义：**由通信开放系统的协议层提供的，并能确保系统或数据传输足够安全的服务。
- **RFC4949的定义：**由系统提供的对系统资源进行特定保护的处理或通信服务。
- **安全服务实现了安全策略，安全服务由安全机制来实现**

Security services implement security policies, and are implemented by security mechanisms.

安全服务(X.800)

- X.800将安全服务分为**5类14种**特定的服务

问题：RFC4949定义的安全服务包括哪些？各类服务的含义是什么

认证	对等实体认证
	数据源认证
访问控制	访问控制
数据机密性	连接机密性
	无连接机密性
	选择域机密性
	流量机密性
数据完整性	带有恢复的连接完整性
	无恢复的连接完整性
	选择域连接完整性
	无连接的完整性
	选择域无连接的完整性
不可抵赖性	源的不可抵赖性
	目的地的不可抵赖性

安全服务(X.800)—认证

- 第一类：认证[Authentication]
- 认证服务：提供某个实体(人或系统)的身份的保证
- 是最重要的安全服务，是抗假冒攻击的方法
- 包括两种认证：对等实体认证和数据源认证。
  - 1. 对等实体认证[Peer Entity Authentication]

    同逻辑连接一起使用，用以提供对连接双方实体的机密性保证
  - 2. 数据源认证[Data-Origin Authentication]

    在非连接传输中，确保数据来源与所声称的一致

安全服务(X.800)—访问控制

- 第二类：访问控制[Access Control]
- 目标：防止对资源(如计算资源、通信资源或信息资源)的非授权访问。
- 非授权访问：包括未经授权的使用、泄露、修改、销毁以及颁发指令等。
  - 3. 访问控制[Access Control]

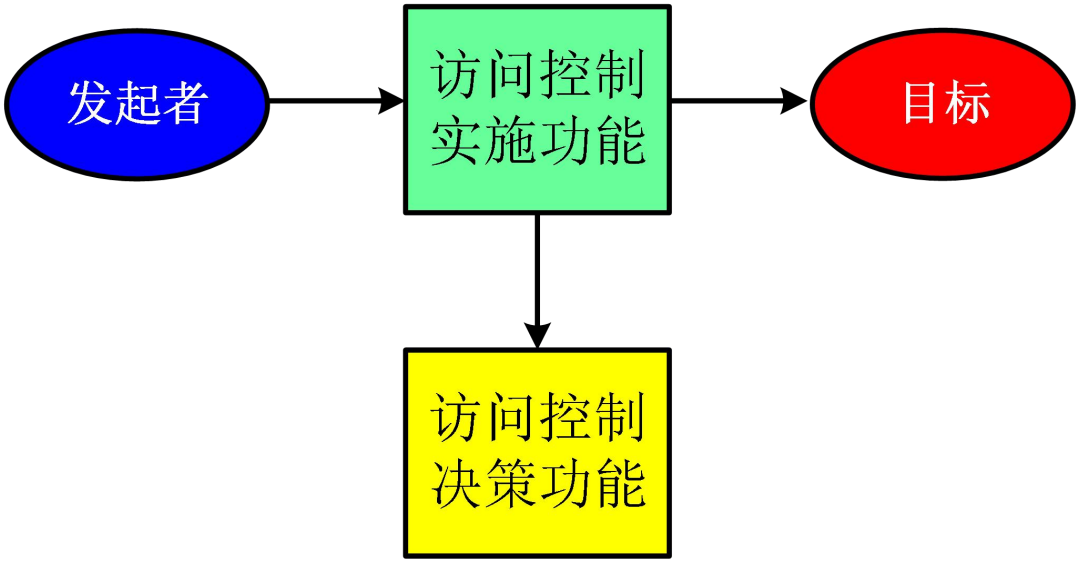
    控制谁能访问资源，在什么条件下可以进行访问以及访问资源允许做什么等

安全服务(X.800))—访问控制

- 访问控制支持机密性、完整性、可用性以及可控性等基本安全目标
- 访问控制是实施授权的一种方法，既是通信安全的问题，计算机（操作系统）安全的问题。
- 访问控制的另一个作用：保护敏感信息不经过有风险的环境传送。

安全服务(X.800))—访问控制

- 访问控制模型
  - 两部分：访问控制实施组件和访问控制决策组件。
  - 发起者做出对目标执行特定访问的请求；
  - 访问控制实施组件通知访问控制决策组件
  - 访问控制决策组件做出决定，允许或禁止该访问请求。



安全服务(X.800))—数据机密性

- 第三类：数据机密性[Data Confidentiality]
  - 防止非授权的数据泄露
  - 4. 连接机密性[Connection Confidentiality]：对连接中所有用户数据的保护
  - 5. 无连接机密性[Connectionless Confidentiality]：对单一数据块中所有用户数据的保护
  - 6. 选择域机密性[Selective-Field Confidentiality]：对连接或单一数据块的用户数据的选择域的保护
  - 7. 流量机密性[Traffic-Flow Confidentiality]：对可能从流量中获取的信息的保护

安全服务(X.800)) —数据完整性

- **第四类：数据完整性[Data Integrity]**
  - 确保被认证实体发送的数据与接收到的数据完全相同（无篡改、插入、删除或重放）
  - **8. 带有恢复的连接完整性：**确保连接中所有用户数据的完整性，检测实体数据序列中任意的篡改、插入、删除或重放，并且尝试恢复数据
  - **9.无恢复的连接完整性：**确保连接中所有用户数据的完整性，检测实体数据序列中任意的篡改、插入、删除或重放，不尝试恢复数据

安全服务(X.800) —数据完整性

- **10. 选择域连接完整性：**在一个连接中，提供对传输数据块中用户数据选择域的完整性，检测选择域中的数据是否被篡改、插入、删除或重放
- **11. 无连接的完整性：**对单一无连接数据块提供完整性保护并且对数据篡改进行检测。此外，也可以提供有限的重放数据检测
- **12. 选择域无连接的完整性：**对单一无连接数据块中选择域提供完整性保护并且对数据篡改进行检测。

安全服务(X.800) —不可抵赖性

- 第五类：不可抵赖性认证[Nonrepudiation]
  - 目的：保护通信用户免遭来自系统中其他合法用户的威胁（指参与某次通信交换的一方事后不诚实地否认曾发生过本次交换），而不是来自未知攻击者的威胁。
  - 概念：提供对被全程参与或部分参与通信的实体拒绝的防范
  - 13. 源的不可抵赖性[Nonrepudiation, Origin]

证明消息由特定一方发出

  - 14. 目的地不可抵赖性[Nonrepudiation, Destination]

证明消息由特定一方接收

安全服务(X.800) —可用性

- **第六类：可用性[Availability]**
  - 定义为：系统的性质
  - 或者定义为：在接收到授权实体的命令时，系统资源根据系统性能规范所表现出来的可访问性和可用性。
  - 多种攻击可导致可用性缺失或者下降
  - 该服务主要致力于解决拒绝服务攻击引起的安全问题，与适当的管理和控制系统资源有关，因此与访问控制服务和其他安全服务有关

1.5 安全机制

- 安全机制是用来实现安全服务的方法或过程
- X.800将安全机制划分为：在特定协议层上执行的机制和没有指定特定协议层或安全服务的机制。

特定的安全机制

- 为提供OSI安全服务，可能合并到适当的协议层中
- 1. 加密[Encipherment]：使用数学算法将数据转换为不能轻易理解的形式
- 2. 数字签名[Digital Signature]：为了允许接收方证明数据源和数据单元的完整性并防止数据伪造而将数据附加到数据单元或者对数据单元进行密码变换。
- 3. 访问控制：强制执行对资源的访问权限的各种机制
- 4. 数据完整性：确保数据单元或者数据单元流完整性的各种机制

特定的安全机制

- **5. 认证交换[Authentication Exchange]：**通过信息交换以确保一个实体身份的一种机制
- **6. 流量填充[Traffic Padding]：**通过填充数据流空余位的方式来干扰
- **7. 路由控制[Routing Control]：**支持对某些数据的特定物理安全通道的选择，并且允许路由改变，特别是当安全性受到威胁时
- **8. 公证[Notarization]：**使用可信第三方以确保某种数据交换的属性

普适的安全机制

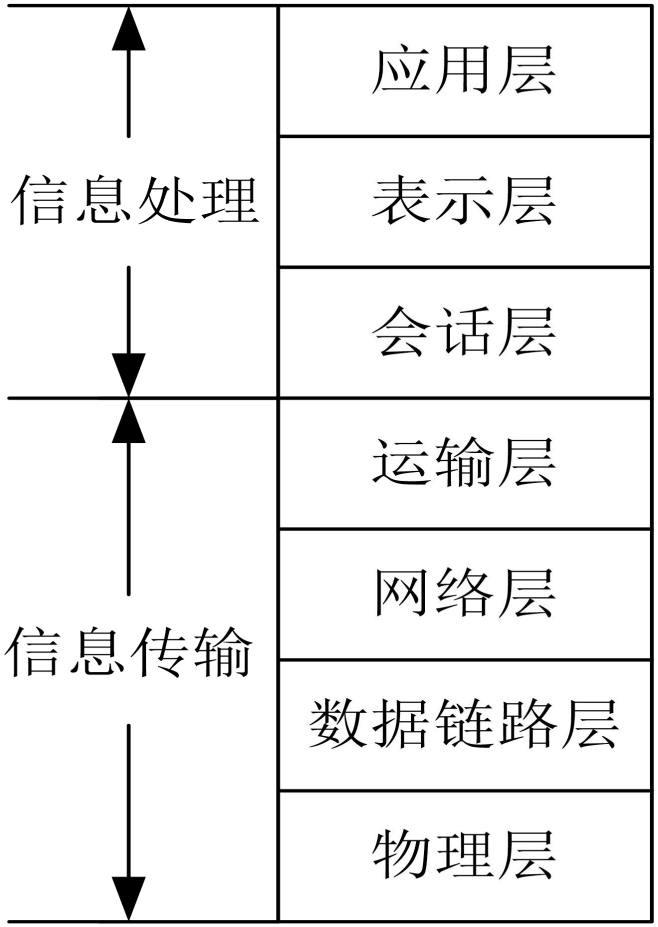
- 没有指定特定OSI安全服务或者协议层的机制
- 1. 可信功能：相对于某个标准而言正确的功能（例如，由安全策略建立的标准）
- 2. 安全标签：绑定在资源（可能是数据单元）上的记号，用来命名或者指定该资源的安全属性
- 3. 事件检测[Event Detection]：与安全相关事件的检测
- 4. 安全审计跟踪[Security Audit Trail]：收集可能对安全审计有用的数据，它对系统记录和活动进行单独的检查和分析
- 5. 安全恢复：处理来自机制的请求，例如事件处理和管理功能，并且采取恢复措施。

安全服务与安全机制之间的关系

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	Y	Y			Y			
数据源认证	Y	Y						
访问控制			Y					
机密性	Y						Y	
流量机密性	Y					Y	Y	
数据完整性	Y	Y		Y				
不可抵赖性		Y		Y				Y
可用性				Y	Y			

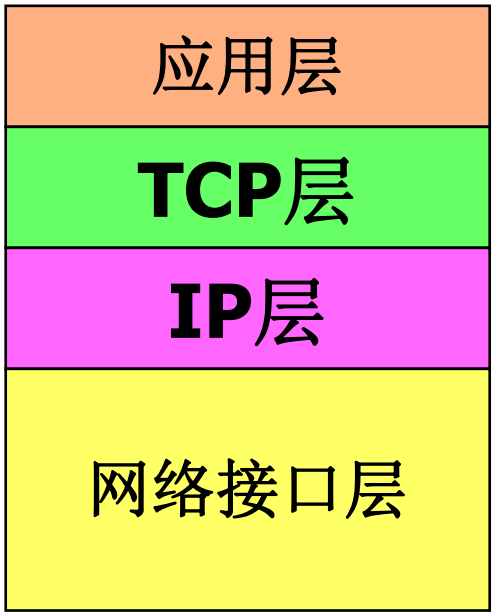
1.6 网络安全模型

- OSI参考模型
  - 应用层
  - 表示层
  - 会话层
  - 运输层
  - 网络层
  - 数据链路层
  - 物理层



TCP/IP参考模型

- 应用层：直接为网络应用提供服务
- TCP层（传输层）：提供不依赖于具体网络的端对端的数据传输服务
- IP层（网络层）：负责对数据包进行路由选择，即决定数据包的具体传输路径。
- 网络接口层：将IP分组在物理网络上传输。



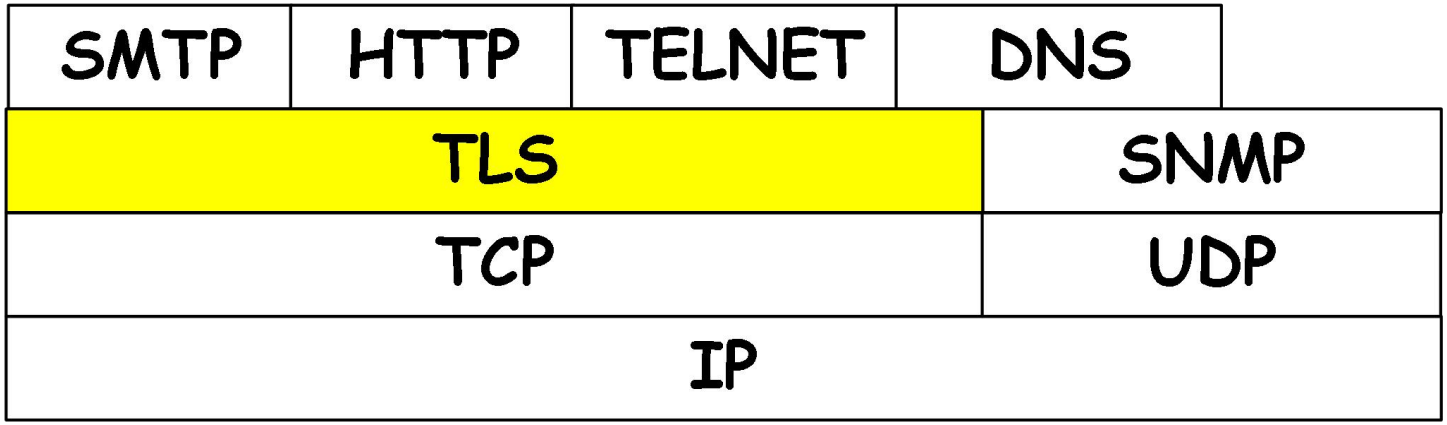
安全服务的分层配置

- 应用层安全
  - 应用层是实施数据加密、访问控制的理想位置。
  - 安全防护面向用户的应用程序，可以实施细粒度、灵活的安全控制，缺点是需要对每个应用单独设计安全机制

<table>
<tr><td>PGP</td><td>PEM</td><td>S/MIME</td><td>HTTPS</td><td>SSH</td><td>DNSSEC</td><td>SNMPv3</td><td></td></tr>
<tr><td colspan="3">SMTP</td><td>HTTP</td><td>TELNET</td><td>DNS</td><td>SNMP</td><td>Kerberos</td></tr>
<tr><td colspan="5">TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="8">IP</td></tr>
</table>

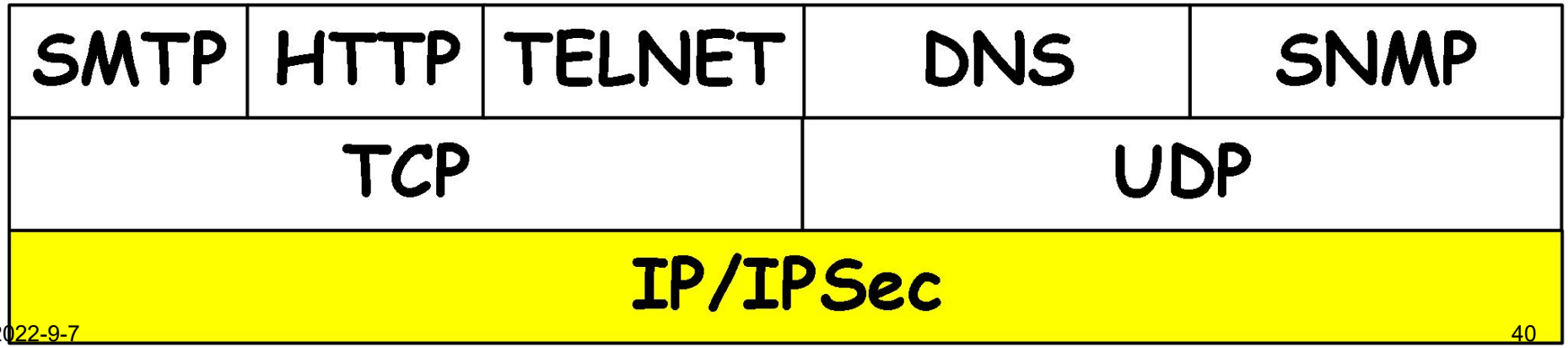
安全服务的分层配置(续)

- 传输层安全
  - 不强制每个应用都在安全方面进行改进
  - 传输层处理的安全需求
    - 端系统是可信的，基础的通信网络是不可信的
    - 由端系统颁布的安全需求
    - 与网络连接有关的安全需求，不与任何特定的应用关联



安全服务的分层配置(续)

- 网络层安全
  - 网络层实现安全服务的优点
    - 消减密钥协商的开销
    - 不需要针对每个应用设计安全机制
    - 为传输层协议“无缝”提供安全服务
    - 能够构建虚拟专用网VPN

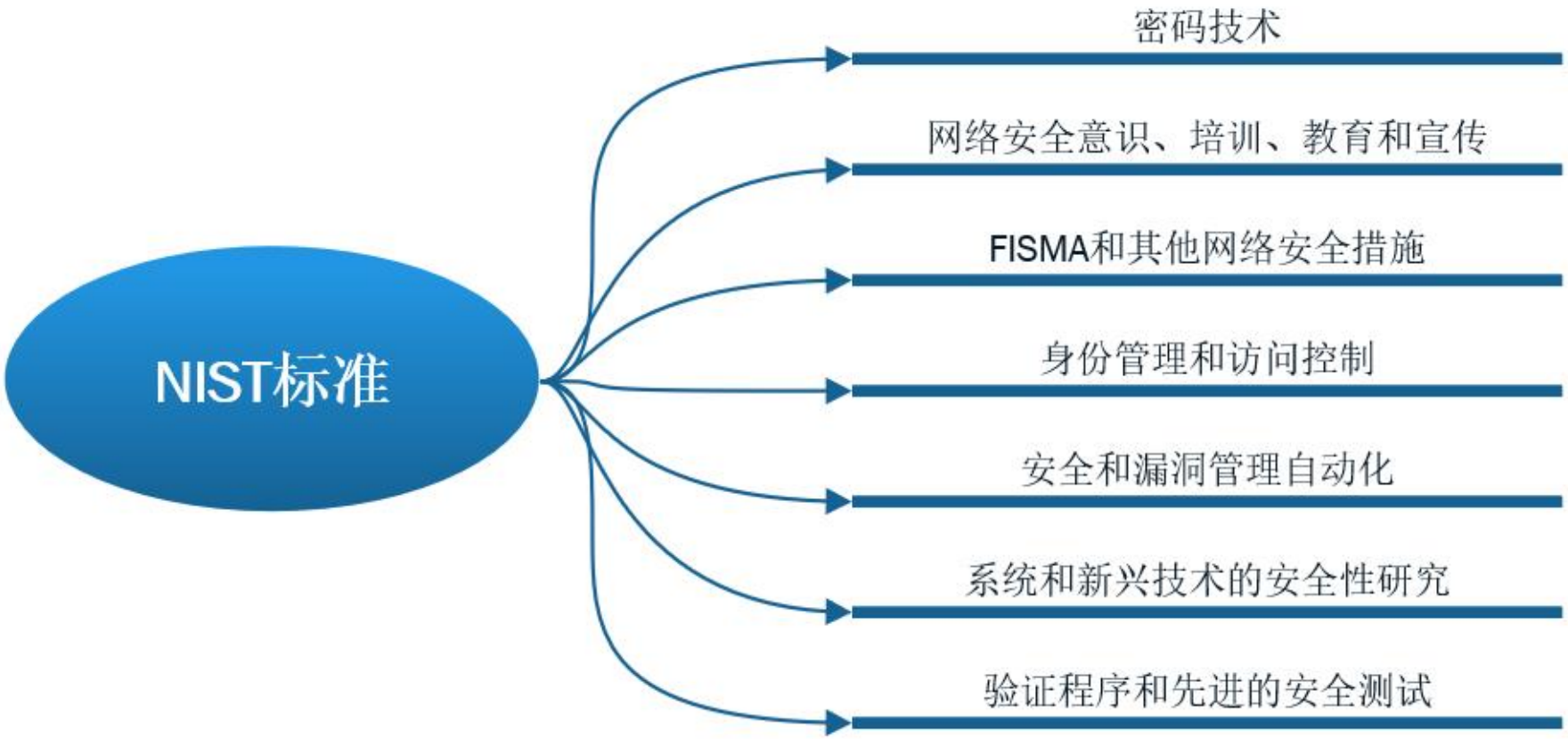


安全服务的分层配置(续)

- 数据链路层安全
  - 主要通过链路加密设备对数据进行保护
  - 该层安全保护对高层透明
  - 不能保护子网络节点内部的弱点

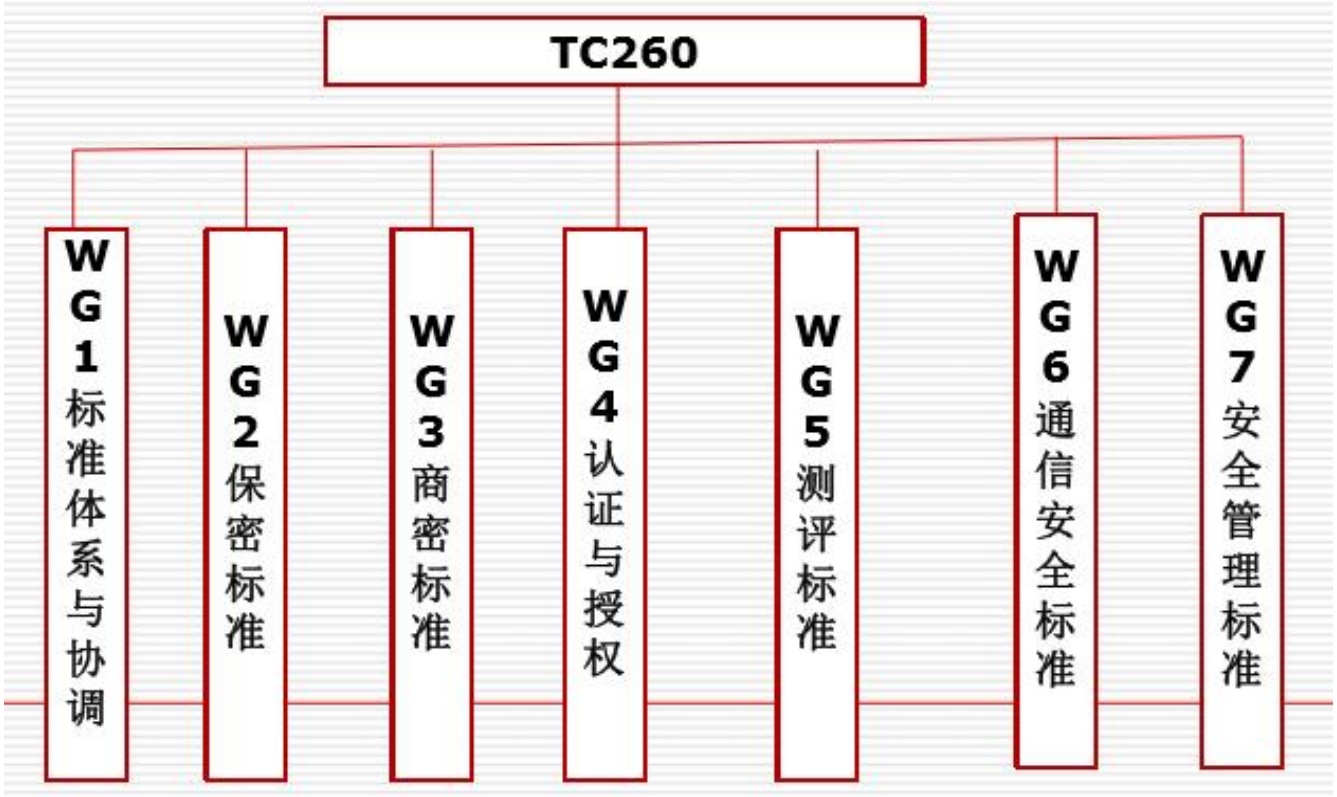
1.7 标准

- **国家标准与技术研究所（NIST）：是美国联邦政府的一个机构，负责处理计量科学、标准以及政府部门使用的技术。**



1.7 标准

- **TC260全国信息安全标准化委员会：2002年4月15日在北京正式成立，是信息安全技术专业领域内从事信息安全标准化工作的技术工作组织，负责组织开展国内信息安全有关的标准化技术工作。**



1.7 标准

- **互联网工程任务组（IETF）** 是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定。

Internet Engineering Task Force

Abbreviation	IETF
Formation	January 16, 1986
	Standards Organization
Purpose/focus	Creating standards applying to the internet to improve the usability of internet
Region served	Worldwide

- **IETF是松散的、自律的、志愿的民间学术组织**

- **IETF标准**
  - 互联网草案(Internet Draft)---任何人都可以提交，无特殊限制
  - RFC文档---正式文件，历史存档，批准后内容不做改变不允许随意标准；第二个它是一种试验性的，RFC无非是说我们在一起想做这样一件事情，尝试一下；还一个就是文献历史性的

作业

- RFC4949定义的安全服务包括哪些？请描述各类安全服务的含义。