计算机网络安全

第1章 网络安全概述

大纲

- 计算机安全的概念（1.1）
- OSI的安全体系（1.2）
  - 安全威胁与攻击（1.3、1.4）
  - 安全机制（1.5）
  - 安全服务（1.6）
- 安全模型（1.7）
- 安全标准（1.8）

1.1 计算机安全概述

1.1.1 计算机安全的定义

- NIST计算机安全手册给出如下定义：

  （NIST是美国国家标准及技术研究所）

- 计算机安全（computer security）-为自动化信息系统提供保护，以达到保持信息系统资源（包括硬件、软件、固件、信息/数据、通信）的完整性、可用性和机密性的目标。

- 用于保护数据安全和防御黑客的工具集合的通用名称就是计算机安全。

1.1.1 计算机安全的定义（续）

- CIA（中央情报局(Central Intelligence Agency)）三元组（三个关键目标）：
- 机密性（confidentiality）

- 保密性（secrecy）：保证私有的或机密的信息不会被泄露给未授权的个体。

- 隐私性(privacy)：确保相关资源被合法用户访问（读、浏览、打印、了解资源是否存在等）

1.1.1 计算机安全的定义（续）

- **完整性（integrity）**

-数据完整性：确保信息或程序只能在指定的或以授权的方式下才能够被改变（写、替换、删除、创建）。

-系统完整性：确保系统在未受损的方式下执行预期的功能，避免对系统进行有意或无意的非授权操作。

1.1.1 计算机安全的定义（续）

- **可用性（availability）**

  所有资源在适当时候可以由授权方访问。

  - 拒绝服务（denial of service）

  -机密性的强保护会严重限制可用性平衡

  -数据项或服务是可用的：对请求的及时响应；

  -对用户公平分配资源：服务和系统有容错性，当发生故障时，服务以可接受的方式终止，而非数据丢失；便于使用；可控制并发；支持同时访问、死锁管理和独占式访问。

1.1.1 计算机安全的定义（续）

额外增加的两个概念（目标）：

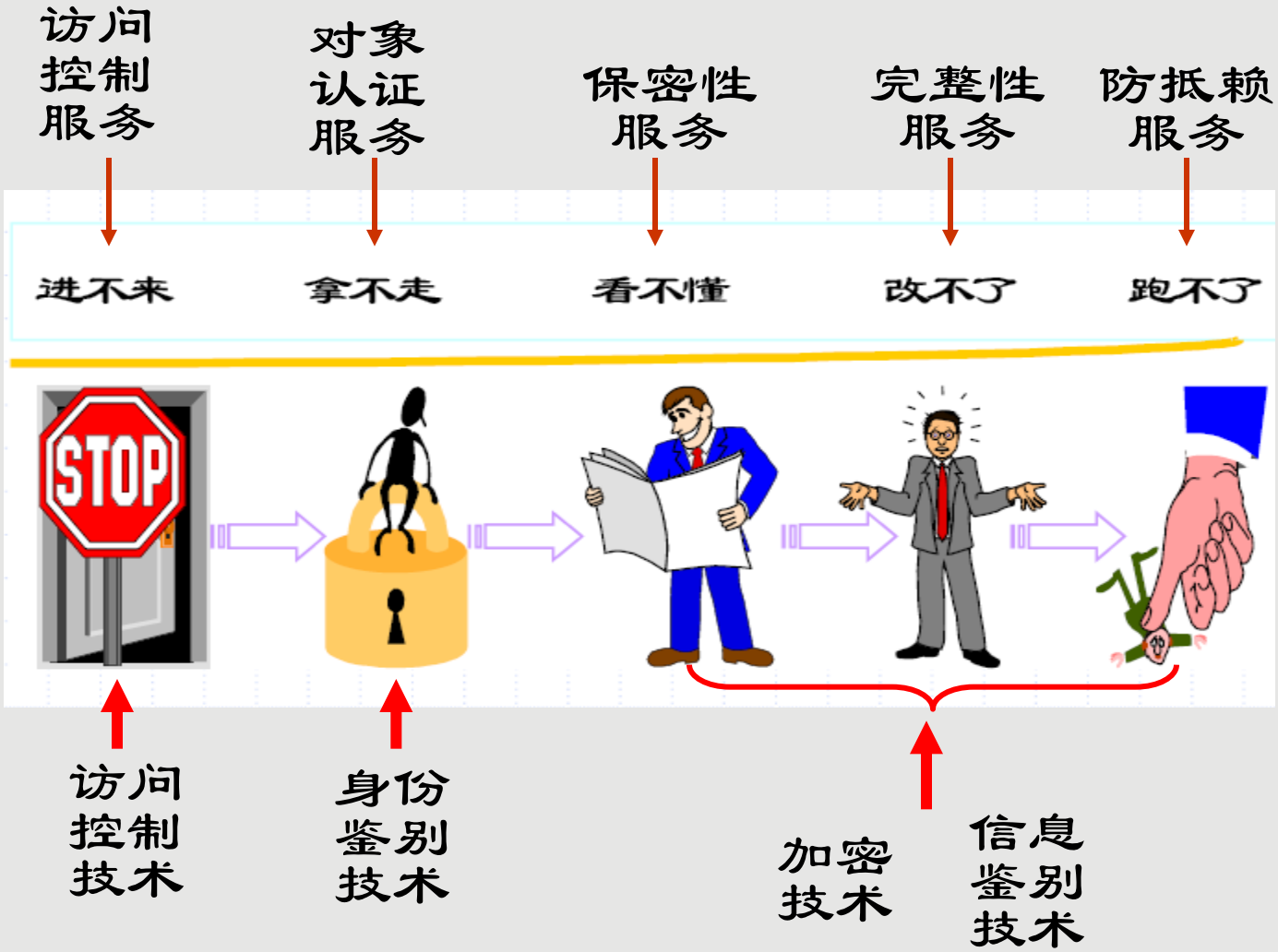
- 真实性（authenticity）

  验证用户的身份与其声称的是否一致。

- 责任性(accountability)（不可抵赖性或不可否认性）

要求实体的动作可以被唯一地追踪，需要支持抗抵赖、故障隔离、入侵检测和防护、事后恢复与诉讼

计算机安全的含义--安全目标



1.1.2 计算机安全挑战

保护信息和保护钱财的差异

	信息	钱财
规模和可移动性	设备小，可移动性强	庞大、笨重、不可移动
避免物理接触的能力	简单	困难
资源价值	高低不同	高

1.1.2 计算机安全挑战（续）

- **与保护有价物品的系统进行对比**
  - **预防：警卫、警报系统；**
  - **事后: 犯罪侦查技术DNA\指纹\视网膜\声音\弹道学证据， 警力的迅速反映；**
  - **存储:大量现金和货币依靠系统本身多层保护\复杂的锁\访问的多方系统**
- **安全的相对性**

1.1.2 计算机安全挑战（续）

- **信息不安全的原因**
  - 信息窃取更加难以防范
  - 安全防范意识淡漠、措施简陋
    - 相当一部分组织缺乏安全认识
    - 对盗版软件危害毫无意识
  - 事后处理消极
    - 调查取证障碍

1.1.2 计算机安全挑战（续）

1.安全问题与安全机制可能非常复杂，甚至是相当深奥的论证推理。

2.在设计与开发一种特定安全机制或算法时，必须考虑对这些安全特性的潜在的攻击。成功的攻击往往是利用了机制中不可预见的弱点。

3.只有考虑过各种威胁后，所设计安全机制才有意义。

4.安全机制通常不止一种特定算法或协议，要求参与者拥有机密信息，如何产生、分配和保护这些机密信息。

1.1.2 计算机安全挑战（续）

5.安全本质—企图发现漏洞的作恶者和设计者或管理者之间的一场智力较量。攻击者只要发现一个弱点，设计者需发现和堵塞所有的弱点使其安全。

6.用户和管理者自然倾向—直到灾难发生前总觉得在安全方面的投入是没什么利益可图的。

7.安全仍然很普遍地是一种事后的考虑，在设计结束之后被引入。

8.很多用户甚至是管理员都认为，强的安全对于一个信息系统或者信息的使用而言在有效性和易操作方面是一种障碍。

1.1.3 针对数据的威胁和控制方法

◆**机密性**

- **目标：保证信息不能被非授权访问，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。**

- **威胁：分接线路、安置漏洞、垃圾箱、监视电磁波、贿赂员工、推断数据点、请求数据**

- **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。**

1.1.3 针对数据的威胁和控制方法

◆**完整性**

- 目标：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。

- 威胁 数据传输、存储和数据格式 重放攻击（replay）

- 通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。

1.1.3 针对数据的威胁和控制方法

◆**抗抵赖性**

- 目标：能保障用户无法在事后否认曾经对信息进行的生成、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。

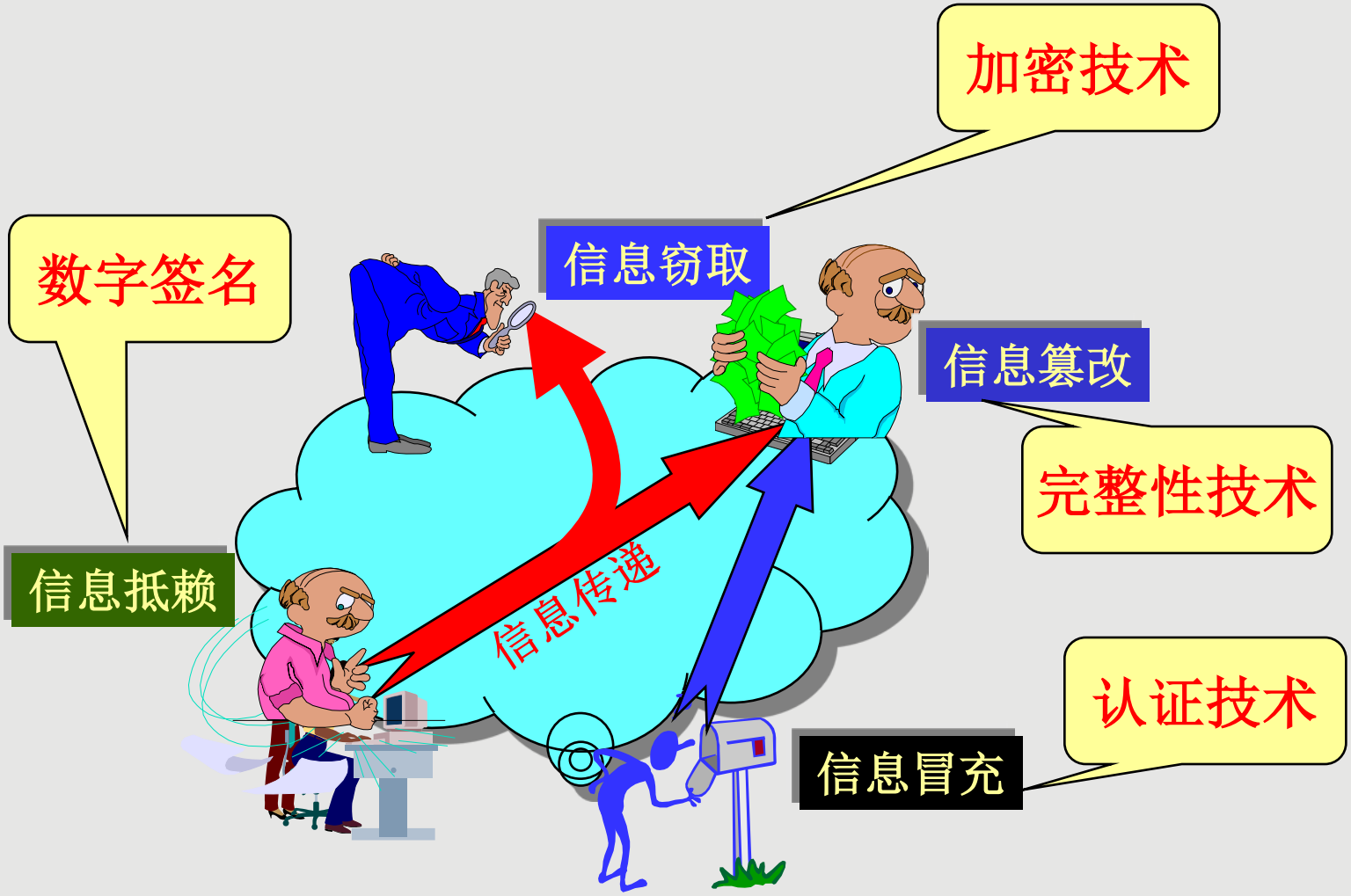
- 通过数字签名来提供抗否认。

◆ 可用性

– 目标：保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时访问所需信息。

- 抵抗拒绝服务攻击

1.1.3 针对数据的威胁和控制方法



1.2 OSI安全体系结构

- **OSI安全体系结构**是一个提供系统方法的框架，定义安全要求和表征方法，定义了安全攻击，机制和服务，以及这些类别之间的关系。
- ITU-T 推荐标准X.800（OSI安全体系结构 ）
- **安全攻击**：任何可能会危及机构的信息安全的行为
- **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**：用来增强机构的数据处理系统安全性和信息传递安全性的服务，利用了一种或多种安全机制提供服务。

1.2 OSI安全体系结构

威胁和攻击（RFC 2828)

- **威胁**

当出现可能会妨害安全并造成损害的环境、能力、行为或事件时，存在的一种潜在的安全威胁。

- **攻击**

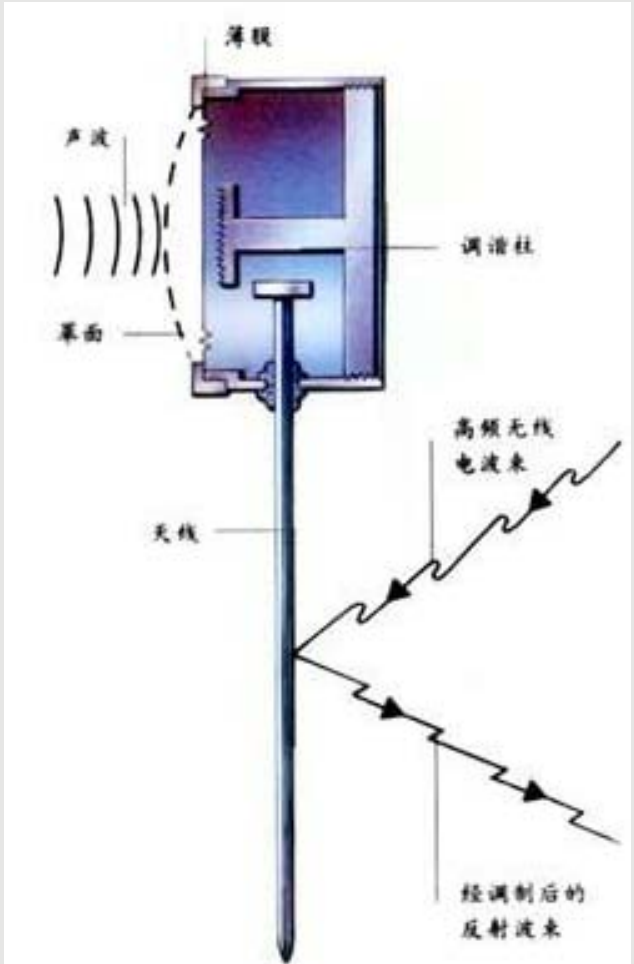
从智能的威胁中衍生的对系统安全的袭击。是一种故意逃避安全服务并且破坏系统安全策略的智能行为。

1.3 安全威胁

- **安全威胁**
  - 故意的(如系统入侵)
  - 偶然的(如将信息发到错误地址)
- **故意威胁**
  - 被动威胁
  - 主动威胁

1.3.1 被动威胁

- 只对信息进行监听，而不对其修改和破坏。



1.3.2 主动威胁

- **对信息进行故意篡改和破坏，使合法用户得不到可用信息**
  - **物理威胁**
  - **系统漏洞造成的威胁**
  - **身份鉴别威胁**
  - **线缆连接威胁**
  - **恶意代码**

主动威胁-物理威胁

- 偷窃
- 废物搜寻
- 间谍行为
- 身份识别错误

主动威胁-系统漏洞造成的威胁

- 乘虚而入
- 不安全服务
  - 蠕虫
- 配置和初始化错误
  - 木马

主动威胁-身份鉴别威胁

- 口令圈套
- 口令破解
- 算法考虑不周
- 编辑口令

主动威胁-线缆连接威胁

- 窃听
- 拨号进入
- 冒名顶替

主动威胁-恶意代码

- 病毒
- 蠕虫
- 代码炸弹
- 特洛伊木马

1.4 安全攻击

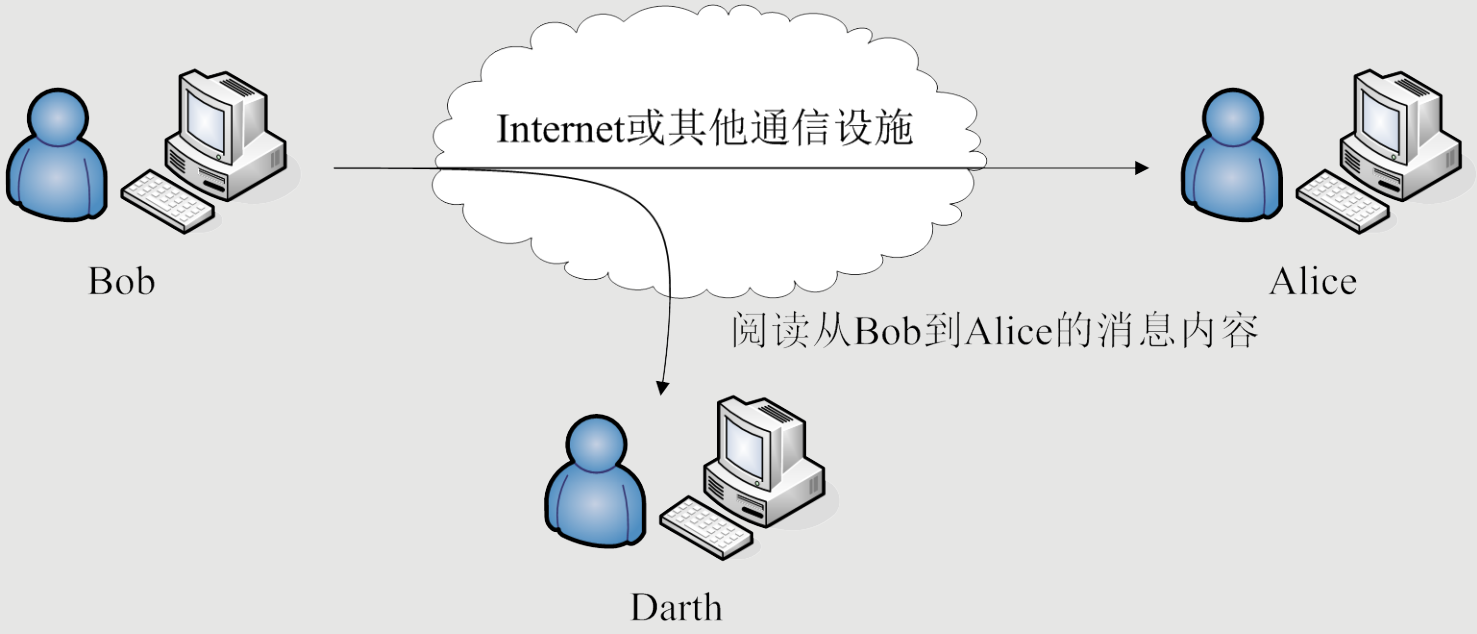
网络攻击是指降级、瓦解、拒绝、摧毁计算机或计算机网络中的信息资源，或者降级、瓦解、拒绝、摧毁计算机或计算机网络本身的行为。

在最高层次上，ISO 7498-2将安全攻击分成两类，即被动攻击和主动攻击。

1.4.1 被动攻击（passive attack）

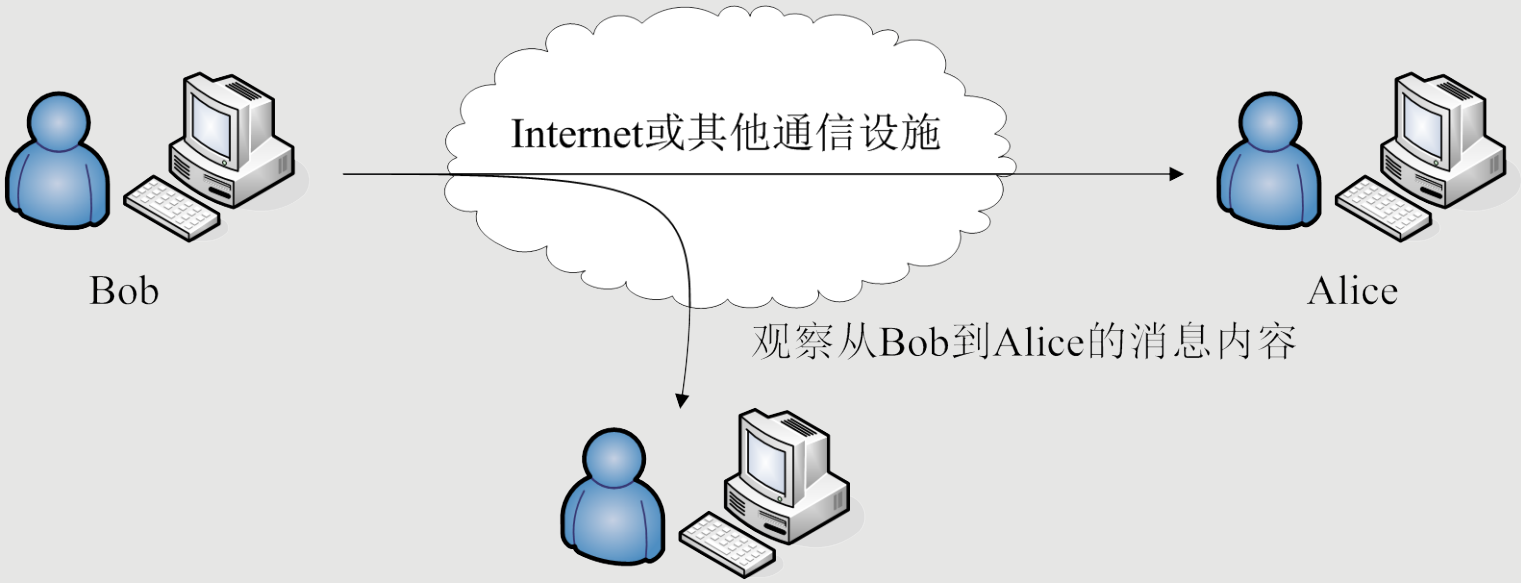
- **被动攻击试图收集、利用系统的信息**但不影响系统的正常访问，数据的合法用户对这种活动一般不会觉察到。
- **被动攻击采取的方法**是对传输中的信息进行**窃听和监测**，主要目标是获得传输的信息。
- **有两种主要的被动攻击方式**：**信息收集**和**流量分析**。

被动攻击 - 信息收集



(a)消息内容的泄漏

被动攻击 -流量分析



(b)流量分析

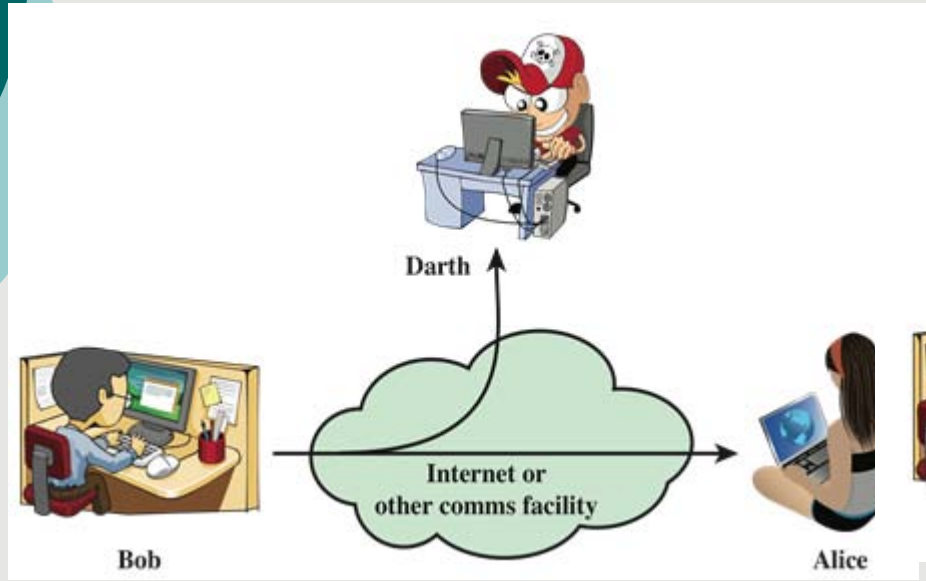
1.4.2 主动攻击（active attack）

- **主动攻击**则是攻击者访问他所需信息的故意行为，**一般会改变系统资源或影响系统运作。**
- **主动攻击**包括对数据流进行篡改或伪造数据流，可分为四类：
  - 假冒（masquerade）
  - 重放（replay）
  - 改写（modification）
  - 拒绝服务（denial of service）

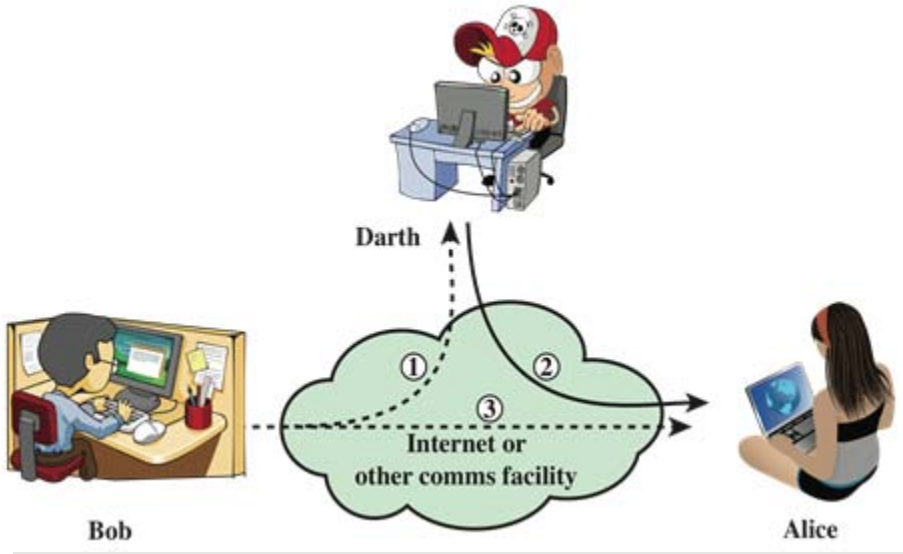
→主动攻击的方式

- **伪装**是指某实体假装成别的实体。典型的比如：攻击者捕获认证信息，并在其后利用认证信息进行重放，这样它就可能获得其他实体所拥有的权限。
- **重放**是指攻击者将获得的信息再次发送，从而导致非授权效应。
- **消息修改**是指攻击者修改合法消息的部分或全部，或者延迟消息的传输以获得非授权作用。
- **拒绝服务**指攻击者设法让目标系统停止提供服务或资源访问，从而阻止授权实体对系统的正常使用或管理。典型的形式有查禁所有发向某目的地的消息，以及破坏整个网络，即或者使网络失效，或者是使其过载以降低其性能。

安全攻击



(a) 被动攻击



(b) 主动攻击

图1.1 安全攻击

1.5 安全服务

X.800对安全服务的定义为：

由通信开放系统的协议层提供的，并能确保为系统或者数据传输提供足够的安全的服务。

在RFC 2828中定义：

由系统提供的对系统资源实施某种特定的保护的处理或通信服务。安全服务实现安全策略，而安全机制实现安全服务。

1.5 安全服务（续）

认证

保证通信的实体是它所声称的实体。

同等实体认证

用于逻辑连接时为连接的实体的身份提供可信性

数据源认证

在无连接传输时保证收到的信息来源是声称的来源

访问控制

阻止对资源的非授权使用（即这项服务控制谁能存取资源，在什么条件下可以存取，这些存取的资源可用做什么)

数据机密性

保护数据免于非授权泄漏

连接机密性

保护一次连接中所有的用户数据

无连接机密性

保护单个数据块里的所有用户数据。

选择域机密性

对一次连接或单个数据块里选定的数据部分提供保密性

流量机密性

保护那些可以通过观察流量而获得的信息

数据完整性

保证收到的数据确是授权实体所发出的数据(即没有修改、插入、删除或重放)

具有恢复功能的连接完整性

提供一次连接中所有用户数据的完整性、检测整个数据序列内存在的修改、插人、删除或重放，且试图恢复之。

无恢复的连接完整性

同上，但仅提供检测，无恢复

选择域连接完整性

提供一次连接中传输的单个数据块用户数据中选定部分的数据完整性，并判断选定域是否有修改插入、删除或重放

无连接完整性

为单个无连接数据块提供完整性保护，并检测是否有数据修改。另外，提供有限的重放检测

迭择域无连接完整性

为单个无连接数据块内选定域提供完整性保护；判断选定域是否被修改

不可抵赖性

防止整个或部分通信过程中，任一通信实体进行否认的行为

源不可抵赖性

证明消息是由特定方发出的

目的地不可抵赖性

证明消息被特定方收到

1.5.1 认证

确保通信实体就是他所声称的实体。

标准中定义了两种：

◆对等实体认证：

在一次联系中确认对等实体的身份。确保实体不是伪装的，也不是未经授权的。

◆数据源认证：

在无连接传输中，确认数据单元的源。这种支持类似电子邮件等应用。

1.5.2 访问控制

- **用于防治未授权用户非法使用系统资源。**
- **该服务可应用于对资源的各种访问类型(如通信资源的使用，信息资源的读、写和删除，进程资源的执行)或对资源的所有访问。**

1.5.3 数据机密性

保护传输的数据免受被动攻击。可以保护所有的数据，也可以保护单个消息或某个特定的字段。另一方面保护数据流免于分析。

分为四种情况：

- **连接机密性：保护在连接上的所有用户数据。**
- **无连接机密性：保护所有单一数据块中的用户数据。**
- **选择字段：在连接上的或者单个数据块中的所有用户数据的被选字段的机密性。**
- **流量机密性：保护可能从流量的观察中获得的信息。**

1.5.4 数据完整性

与机密性服务一样。使用范围同。能确保所接受的消息与发送的消息是一样的，没有受到复制、插入、更改、重新排序或者重放。

- **具有恢复能力的连接完整性**：对在连接上的所有用户数据提供完整性服务，并且按照完全的数据顺序检测任何对数据的更改、插入、删除或者重放，具有恢复的功能。
- **不具有恢复能力的连接完整性**：与上面相同，但只是提供检测，不具有恢复的能力。
- **选择字段的连接完整性**：对在连接上的传输的数据块中的用户数据的被选字段的提供完整性。
- **无连接的完整性**：对于单个无连接的数据块提供完整性服务。

1.5.5 不可抵赖性

- **用于防止发送方在发送数据后否认发送和接收方在收到数据后否认收到或伪造数据的行为。**
  - **具有源点证明的不能否认：为数据接收者提供数据源证明，防止发送者以后任何企图否认发送数据或它的内容。**
  - **具有交付证明的不能否认：为数据发送者提供数据交付证明， 防止接收者以后任何企图否认接收数据或它的内容。**

1.5.6 可用性服务

X.800和RFC 2828 将**可用性**定义为系统的性质。**无论用户何时需要，系统总能提供服务，那么这个系统就是可用的。**

多种攻击能够导致**可用性**的丢失或者降低。可以采用自动的对策对多种攻击进行修正，例如**认证和加密**，而其他的攻击则需要某种物理行为来预防或者丢失的分布式系统元素的可用性。

1.6 安全机制

表1.3 列出了X.800定义的安全机制，从中可以看出安全机制被划分为在特定协议层上执行的机制以及没有指定特定协议层或安全服务的机制。

表1.3 安全机制（X.800）

特定安全机制	普遍的安全机制
可以并入适当的协议层以提供一些OSI安全服务 **加密** 运用数学算法将数据转换成不可知的形式。数据的变换和复原依赖于算法和零个或多个加密密钥 **数字签名** 附加于数据元之后的数据，是对数据元的密码变换，以使得(如接收方)可证明数据源和完整性，并纺止伪造 **访问控制** 对资源行使存取控制的各种机制 **数据完整性** 用于保证数据元或数据单元流的完整性的各种机制 **认证交换** 通过信息交换来保证实体身份的各种机制 **流量填充** 在数据流空隙中插人若干位以阻止流量分析 **路由控制** 能够为某些数据选择特殊的物理上安全的路线并允许路由变化(尤其是在怀疑有侵犯安全的行为时) **公证** 利用可信的第三方来保证数据交换的某些性质。	不局限于任何OSI安全服务或协议层的机制 **可信功能** 据某些标准被认为是正确的(例如，根据安全策略所建立的标准) **安全标签** 资源(可能是数据元)的标志，指明该资源的安全属性 **事件检侧** 检测与安全相关的事件 **安全审计跟踪** 收集可用于安全审计的数据，它是对系统记录和行为的独立回顾和检查 **安全恢复** 处理来自安全机制的请求，如事件处理、管理功能和采取恢复行为

表1.4 安全服务和安全机制的关系

安全服务 \ 安全机制	加密	数字签名	访问控制	教据完整性	认证交换	流量填充	路由控制	公证
同等实体认证	Y	Y			Y			
数据源认证	Y	Y						
访问控制			Y					
保密性	Y						Y	
流量保密性	Y					Y	Y	
数据完整性	Y	Y		Y				
不可否认性		Y		Y				Y
可用性				Y	Y			

1.7 网络安全模型

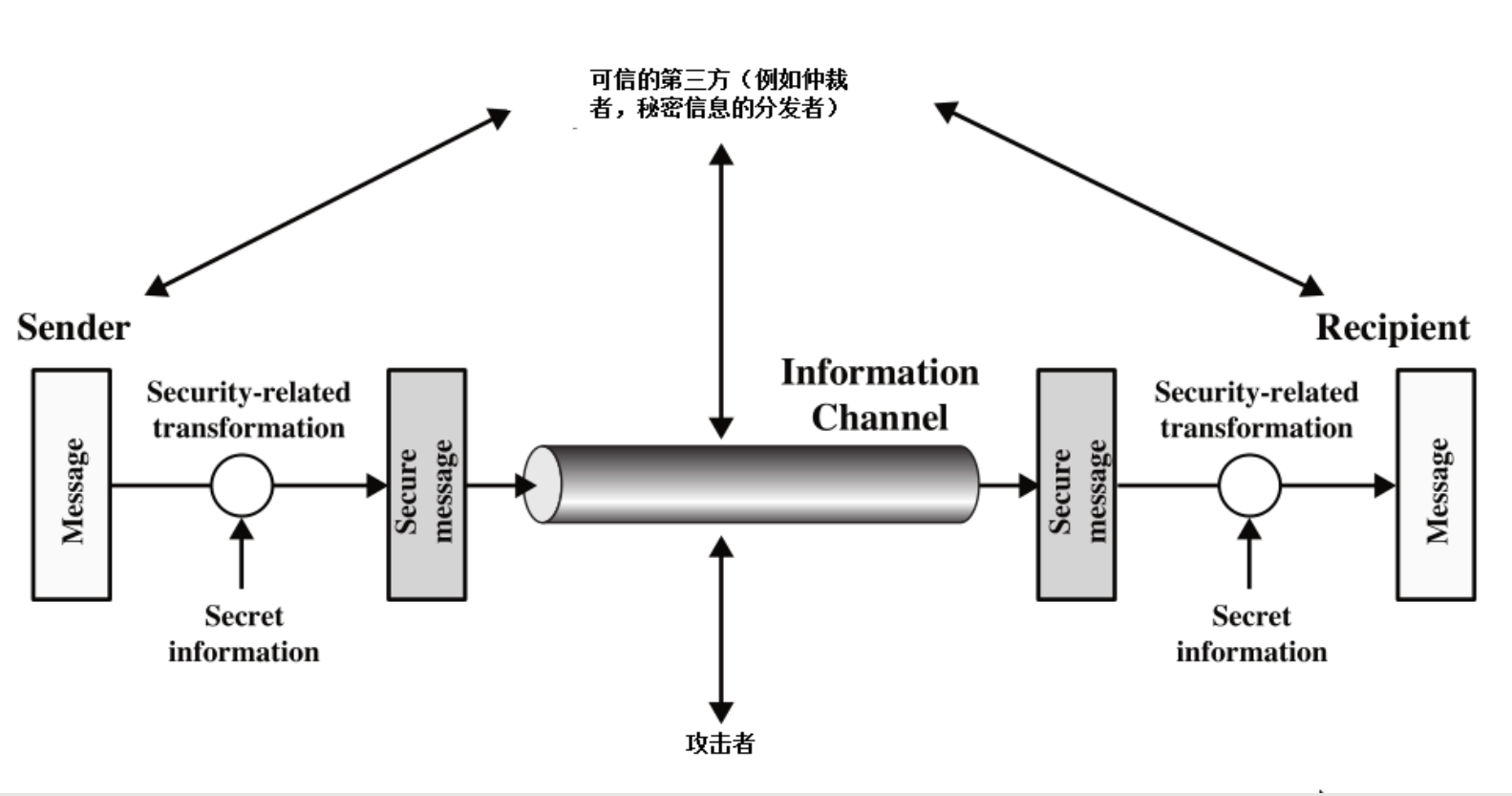


图1.2 网络安全模型

1.7 网络安全模型（续）

- 所有用于提供安全性的技术都包含以下两个主要部分：
  - 对待发送信息进行与安全相关的转换。包括消息加密，使得对于攻击者而言该信息不可读；以及建立在消息内容上面的附加码，它可以用来验证发送者的身份。
  - 两个主体共享一些不希望被攻击者所知的秘密信息。包括在消息变换中使用的加密密钥，它在传输之前用于打乱消息而在接收之后用于恢复消息。

1.7 网络安全模型（续）

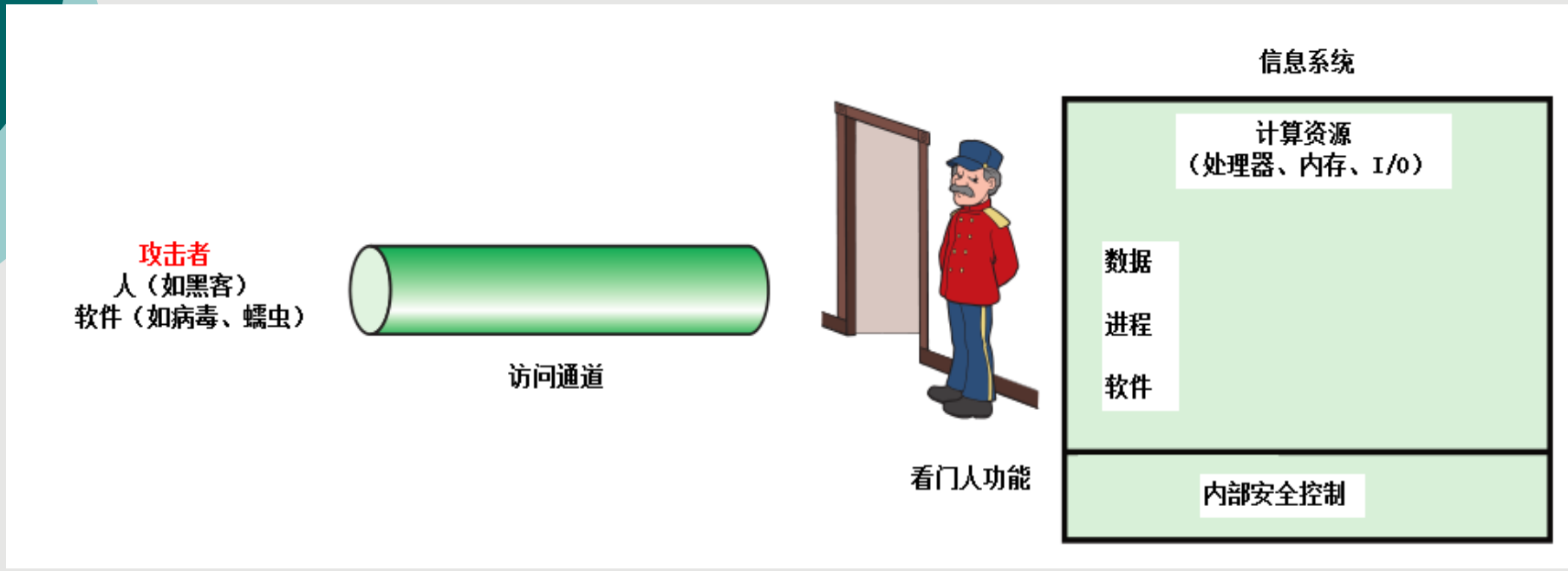


图1.3 网络访问安全模型

1.8 标准

- 国际标准化组织（ISO）

  - ISO 17799

包含了133个安全控制措施来帮助组织识别在运行过程中对信息安全有影响的元素。成为组织实施信息安全管理的实用指南（风险评估、策略、信息安全组织、资产管理、人力资源安全、物理安全、通信安全、访问控制，IS获取、开发与维护、安全事故管理、业务持续性管理、一致性）

  - ISO27001：2005

根据ISO17799：2005制定的一个ISMS（信息安全管理系统）体系实施规范，并可使用该规范对组织的信息安全管理体系进行审核与认证。

1.8 标准（续）

- **美国国家标准和技术研究所（NIST）**
  - FIPS PUB 200（美国联邦信息与信息系统最低安全需求）
  - NIST SP 800-100(信息安全手册：管理者指南)
  - NIST SP 800-55（信息技术系统安全度量指导）
  - NIST SP 800-27（信息技术安全工程原理）
  - NIST SP 800-53（美国联邦信息系统的推荐安全控制措施）

1.8 标准（续）

- 国际电信联盟电信标准化部门（ITU-T）
  - X.800系列推荐标准（20个）
  - X.800，X.802和X.803标准描述了在开放系统的安全；
  - X.805标准提供了端到端通讯安全框架；
  - X.810，X.811，X.812，X.813，X.814，X.815和X.816涵盖全面安全框架（如认证、访问控制、抗抵赖、加密、完整性、安全审计和安全警报）
  - X.830，X.831，X.832，X.833。X.834和X.835标准提供了通用的上层安全。

有关安全信息和可信第三方服务的标准已经在X.841，X.842和X.843已经提出

1.8 标准（续）

- **信息技术安全评估通用准则（CC）**

  定义了一组已知有效性的IT需求，用来对未来产品和系统建立安全需求

- **Internet标准和Internet协会（Request for common，RFC）**

  RFC2196(网站安全手册)在网站上开发计算机安全策略和程序的指南

  RFC3552（撰写安全方面的RFC文本指南）

小结

- 计算机安全的概念
- OSI的安全体系
  - 安全威胁与攻击
  - 安全机制
  - 安全服务
- 安全模型
- 安全标准