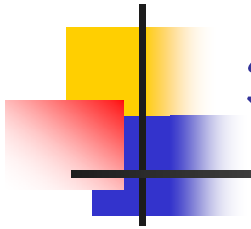
cshao@gdut.edu.cn

信息安全概论

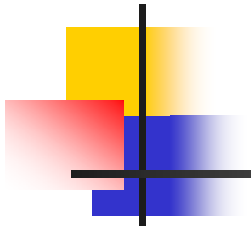


学习要求

第一章 概论

第一章 概论

- 1.1计算机与社会
- 1.2计算机中安全的重要性
- 1.3信息安全的定义
- 1.4信息安全的主要内容
- 1.5信息安全的模型
- 1.6信息安全的标准
- 1.7信息安全的发展趋势



1.1计算机与社会

- 1.1.1计算机逐步进入社会
- 1.1.2计算机的脆弱性

1.1.2计算机的脆弱性

- 计算机的脆弱性是计算机安全的缘由：
  - 电子产品对抗环境的能力弱
  - 数据密集，分布少
  - 计算机的存储以磁介质为主，容易剩磁和漏磁
  - 通讯网是不设防的开放大系统
  - 共享与封闭的矛盾
  - 任何新技术都产生新的安全隐患
  - 安全在系统设计中放在不重要的位置

第一章 概论

- 1.1计算机与社会
- 1.2计算机中安全的重要性
- 1.3信息安全的定义
- 1.4信息安全的主要内容
- 1.5信息安全的模型
- 1.6信息安全的标准
- 1.7信息安全的发展趋势

1.2计算机中安全的重要性

- 国家的安全数据、企业资料等数据不能被泄漏
- 计算机在广泛的学科中应用，社会对计算机依赖性越来越大
- 计算机面临形式极其严峻
  - 安全事件和系统漏洞数量剧增
  - 计算机病毒和垃圾邮件频发
  - 黑客活跃，计算机犯罪频发
  - 关键网站的安全防护仍然难以抵御攻击

1.2计算机中安全的重要性

- 世界各国纷纷开展安全技术研究
  - 2002年9月18日美国颁布了《保护网络空间的国家战略》草案
  - 2002年9月20日颁布了《美国国家安全战略》
  - 美国国家安全局(NSA)推出了《信息保障技术框架(IATF)》
  - 美国政府制定了《网络空间人才(Cybercorps)计划》
  - 在我们国内，已经成立了全国信息安全标准化委员会

第一章 概论

- 1.1计算机与社会
- 1.2计算机中安全的重要性
- 1.3信息安全的概念
- 1.4信息安全的主要内容
- 1.5信息安全的模型
- 1.6信息安全的标准
- 1.7信息安全的发展趋势

1.3信息安全的概念

1.3.1信息安全的定义

- 静态定义采用国际标准化组织ISO对“计算机安全”的定义：“为数据处理系统建立和采用的技术上和管理上的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露”。这个定义没有考虑网络的因素，偏重于静态信息保护。
- 动态定义则增加了对信息系统能连续正常工作的要求。
- 本课程所述的信息系统是指计算机网络信息系统，在不会发生歧义时，常将计算机网络信息系统安全简称为信息安全。

1.3信息安全的概念

- **1.3.2网络信息系统安全的目标**
  - 保密性**(Confidentiality)**
  - 完整性**(Integrity)**
  - 可用性**(Availability)**
  - 抗否认性（**Non-repudiation**）
  - 可控性（**Controllability**）

1.3信息安全的概念

- 保密性(Confidentiality)
  - 信息不泄露给非授权用户，不被非法利用，即使非授权用户得到信息也无法知晓信息的内容。
  - 通常通过访问控制阻止非授权用户获得机密信息
  - 通过加密技术阻止非授权用户获知信息内容。
  - 广州市涉密计算机信息系统分为A（国家绝密级）、B（国家机密级）、C（国家秘密级）、D（工作秘密级）四个级别。

1.3信息安全的概念

- 完整性(Integrity)
  - 一方面是指信息在生成、传输、存储和使用过程中不被篡改、丢失、缺损等
  - 另一方面是指信息处理的方法的正确性。
  - 一般通过访问控制阻止篡改行为
  - 通过消息摘要算法来检验信息是否被篡改。
  - 完整性是数据未经授权不能进行改变的特性，其目的是保证信息系统上的数据处于一种完整和未损的状态。

1.3信息安全的概念

- 可用性(Availability)
  - 指信息及相关的信息资源在授权人需要的时候，可以随时获得。
  - 例如通信线路中断故障会造成信息的在一段时间内不可用，影响正常的商业运作，这是信息可用性的破坏。
  - 网络环境下的拒绝服务攻击（DoS）、分布式拒绝服务（DDoS）都属于对可用性的攻击。
  - 可用性是信息资源服务功能和性能可靠性的度量，是对信息系统总体可靠性的要求。
  - 目前要保证系统和网络中能提供正常的服务，除了备份和冗余配置外，没有特别有效的方法。

1.3信息安全的概念

- 抗否认性（**Non-repudiation**）
  - 指能保障用户无法在事后否认曾对信息进行的生成、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。
  - 一般将使用数字签名和公证机制来保证不可否认性。

1.3信息安全的概念

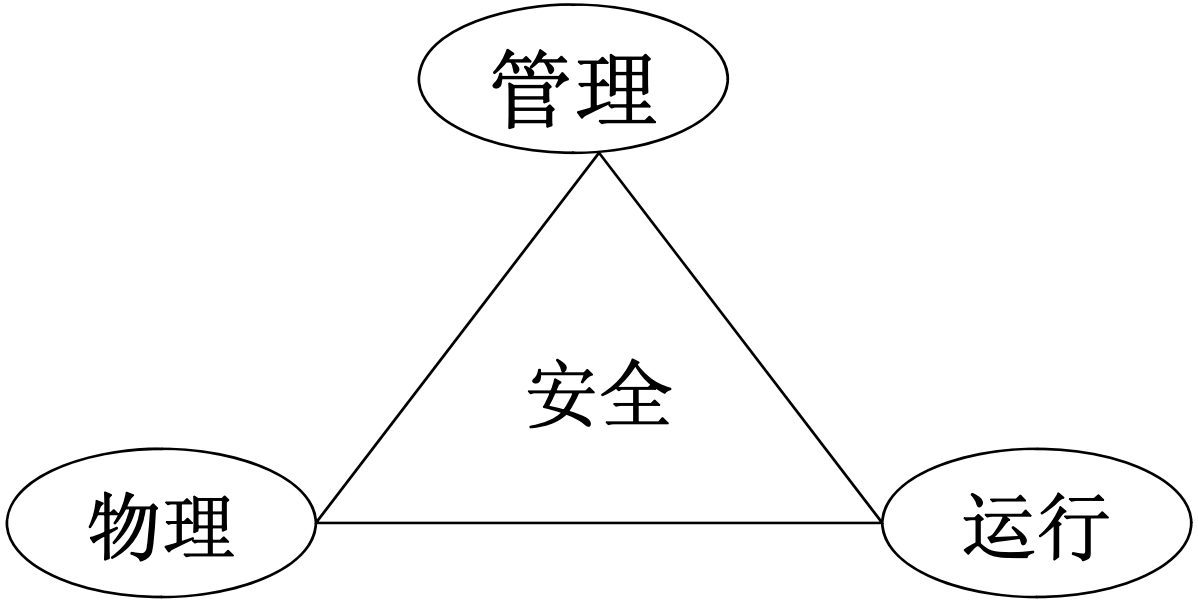
- 可控性（**Controllability**）
  - 指可以控制授权范围内的信息流向及行为方式，对信息的传播及内容具有开展能力。
  - 为保证可控性，通常通过握手协议和认证对用户进行身份鉴别，通过访问控制列表等方法来控制用户的访问方式，通过日志记录用户的所有活动以便于查询和审计。

1.3信息安全的概念

- **1.3.3面临的威胁**
- 泄密
- 欺骗
- 中断
- 篡夺
- 监听
- 篡改
- 抵赖
- 延时

1.4 信息安全的主要内容

- 网络信息系统安全包括物理安全、运行安全、管理和策略三个主要的领域。



1.4 信息安全的主要内容

- **1.4.1** 物理安全
- 物理安全是指保护计算机设备、网络以及其他设施免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施、过程。
- 它包括环境安全、设备安全和媒体安全三个方面。
- 环境安全指对计算机网络信息系统所在环境的安全保护
- 设备安全指对计算机网络信息系统设备的安全保护，包括设备的防盗、防毁，电源保护，防止电磁泄漏，防线路截获和抗电磁干扰等
- 媒体安全指对存储介质的安全管理

1.4 信息安全的主要内容

- **1.4.2** 运行安全：提供一套安全措施来保护信息处理过程的安全，其目的是保障系统功能的安全实现。
- 访问控制
- 加密、
- 鉴别、
- 病毒防护、
- 操作系统安全、数据库安全、网络安全
- 备份与恢复
- 应急
- 风险分析、
- 审计跟踪等各个方面。

1.4 信息安全的主要内容

- **1.4.3** 管理和策略
- 安全管理是保证计算机网络信息系统安全的特殊技术，它包含制度和教育两方面的内容。
- 安全立法;员工筛选;建立和完善安全管理制度;实施分级、分区的行政管理。

1.4 信息安全的主要内容

- 安全管理的三项原则是：
- （1）多人负责原则，即至少应有两人以上实施安全管理；
- （2）任期有限原则，即不定期循环任职；
- （3）职责分离原则，即编程与操作、信息传送与接收、操作介质与介质保密、系统管理与安全管理、应用程序编制与系统程序编制、访问证件管理与其他工作等实施分离。

1.4 信息安全的主要内容

- 安全策略是指在一个特定的环境中，为保证提供一定级别的安全保护所必须遵循的规则。
- 策略必须为组织机构的管理团队提供全面和坚决的安全支持；而管理则指示督导安全策略的实施以保证策略有效。信息安全专家可以推荐各种策略，同时也需要支持他们实施。如果没有管理的支持，那么策略也只能是“纸上谈兵”。

1.4 信息安全的主要内容

- 下面列出了一些需要考虑和制定相关计划的策略领域：
- 1. 系统管理策略
- 系统管理策略制定升级、监控、备份、审计等工作的指导方针和预期目标。
- 策略必须足够详细，以帮助系统管理人员能够明确地了解需要对系统和网络做哪些工作。
- 同时，策略也要有一定的灵活性，能应付一些紧急事件和无法预料的情况。

1.4 信息安全的主要内容

- **2** 资源需求分配策略
- 根据网络资源的责职确定哪些人允许使用某一设备，如用户如何授权访问，允许哪些用户使用、允许何时使用、允许何种操作；采用哪种登录方式（远程/本地），允许哪些用户访问哪些系统程序和应用程序，授权访问哪些数据，并制定授权方式和程序。

1.4 信息安全的主要内容

- **3** 使用策略
- 使用策略定义了信息和资源的使用方式，包括向用户解释如何使用系统资源和使用这些资源的目的是什么。
- 使用策略包括了隐私、所有权、不适当行为的后果等各方面的处理声明。如用户口令的设置规则，应多长时间内更改口令；如用户是自身提供备份还是网络服务者提供备份等。

1.4 信息安全的主要内容

- **4** 用户管理策略
- 用户管理策略需要确定职员日常必须发生的行为的各个方面。
- 这些策略必须能够解决新职员如何能安全地加入系统及员工离职后如何更新系统，以及解决职员的培训和定位问题。

1.4 信息安全的主要内容

- **5** 灾难恢复计划
- 灾难恢复计划（**Disaster Recovery Plan**，简称**DRP**）是指在紧急情况或安全事故发生导致系统崩毁时，如何保障计算机信息系统继续运行或紧急恢复。
- 绝大多数大企业都对灾难恢复计划投入很多资金，包括数据备份和双机热备份。
- 优秀的灾难恢复计划需要考虑到任何类型的紧急情况和可能的故障。简单来说，也许是单个系统瘫痪的恢复；复杂来说，可能是一个大型跨国公司的业务系统如何从自然灾害和灾难事件中的恢复。

1.5 信息安全的模型

- 1.5.1访问控制
- 1.5.2强制访问控制
- 1.5.3自主访问控制
- 1.5.4多级安全模型
- 1.5.5多边安全模型

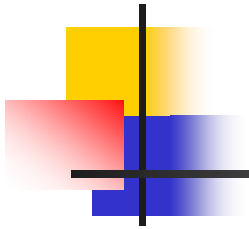
1.5.1访问控制

- 访问控制是计算机保护中极其重要的一环
- 它是在身份识别的基础上，根据身份对提出的资源请求加以控制。
- 访问控制机制决定用户及代表一定用户利益的程序能做什么，及做到什么程度。
- 访问控制中的三个元素
  - 访问的发起者称为主体，通常是进程，程序或用户
  - 包括各种资源称为客体如文件，设备，信号量，内存，用户
  - 保护规则，定义了主体与客体的可能的相互作用途径。

1.5.1访问控制

- 访问控制的两个重要过程：
  - **1**、通过"鉴别（**authentication**）"来检验主体的合法身份
  - **2**、通过"授权（**authorization**）"来限制用户对资源的访问级别

- 访问包括读取数据，更改数据，运行程序，发起连接等。



1.5.1访问控制

- 一般的保护机制：
  - 强制访问控制(mandatory access control)
    - 用户与资源都有一个固定的安全属性。系统用该安全属性来决定一个用户是否可以访问某个文件。安全属性是强制性的规定，由安全管理员，或是操作系统根据限定的规则确定的，用户或用户的程序不能加以修改
  - 自主访问控制（discretionary access control）
    - 用户可以按自己的意愿对系统的参数作适当的修改以决定哪些用户可以访问他们的资源，亦即一个用户可以有选择的与其他用户共享他的资源。用户有自主的决定权。

1.5.2强制访问控制

- 在强制访问控制系统中，所有主体（用户，进程）和客体（文件，数据）都被分配了安全标签，安全标签标识一个安全等级，访问控制执行时对主体和客体的安全级别进行比较。
- 用一个例子来说明强制访问控制规则的应用，如**WEB**服务以“秘密”的安全级别运行。假如**WEB**服务器被攻击，攻击者在目标系统中以“秘密”的安全级别进行操作，他将不能访问系统中安全级为“机密”及“高密”的数据。
- 强制访问控制进行了很强的等级划分，所以经常用于军事用途。

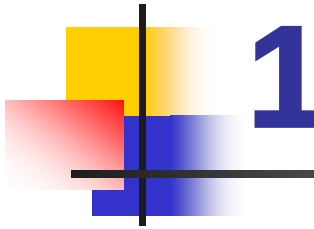
1.5.3自主访问控制

- 每个主体拥有一个用户名并属于一个组或具有一个角色；每个客体都拥有一个限定主体对其访问权限的访问控制列表（**ACL**）；每次访问发生时都会基于访问控制列表检查用户标志以实现对其访问权限的控制。

主体	访问权限
Interactive User	读
Administrator	完全控制
System	完全控制
Accounting	拒绝所有访问

1.5.4多级安全模型

- 将数据划分为多个安全级别与敏感度的系统称之为多级安全系统。
- **1. BLP保密性模型**
- **2. BIBA完整性模型**
- **3. Clark-Wilson完整性模型**



1. BLP保密性模型

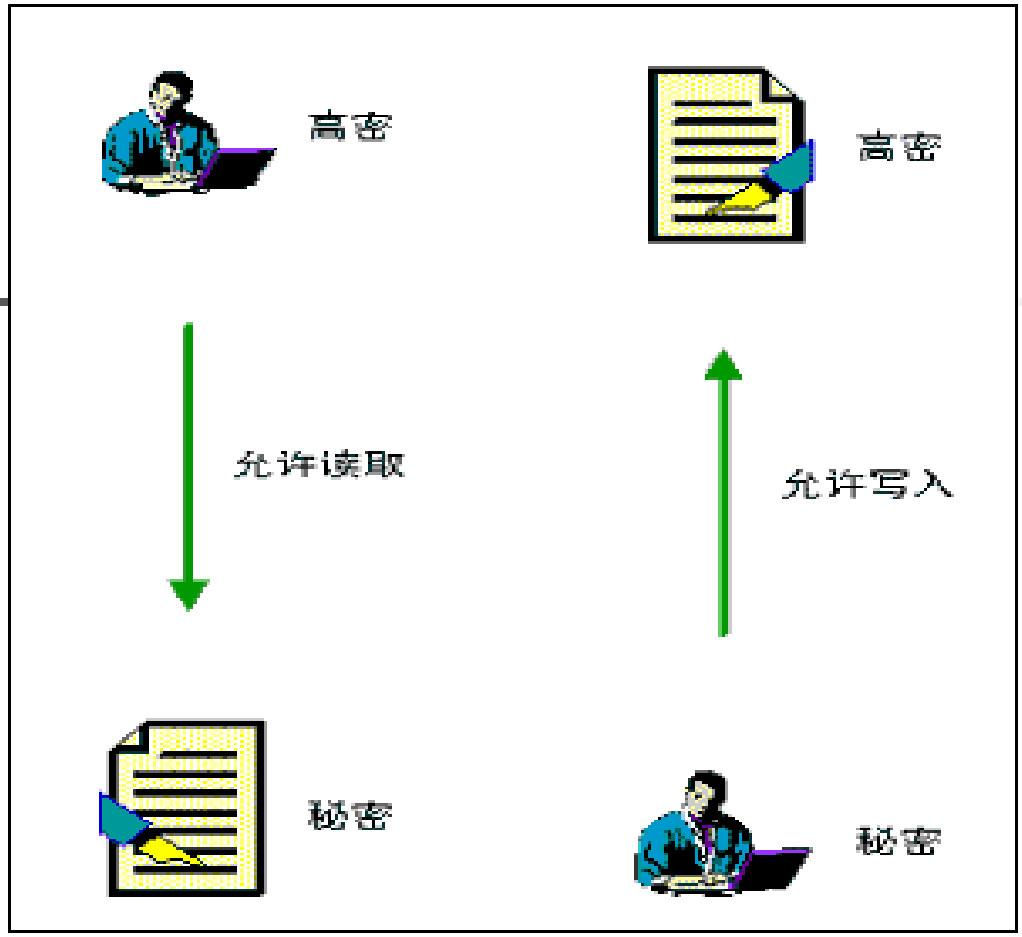
- **1973**年，**David Bell**和**Len LaPadula**提出
- 该模型基于强制访问控制系统，以敏感度来划分资源的安全级别，简称**Bell-LaPadula**保密性模型或**BLP**保密模型。
- 是第一个能够提供分级别数据机密性保障的多级安全策略模型。

1. BLP保密性模型

- **BLP**安全模型对主体和客体按照强制访问控制系统的策略进行分类，这种分类方法一般应用于军事用途。数据和用户被划分为以下五个安全等级：
- （1）公开（**Unclassified**）；
- （2）受限（**Restricted**）；
- （3）秘密（**Confidential**）；
- （4）机密（**Secret**）；
- （5）高密（**Top Secret**）。

1. BLP保密性模型

- 基于两种规则来保障数据的机密度与敏感度：
  - 规则1 (不)上读:主体不可读安全级别高于它的数据；
  - 规则2 (不)下写:主体不可写安全级别低于它的数据。
  - 例如，有一个安全级别为“高密”的用户，想要访问安全级别为“秘密”的文档，他将能够成功读取该文件，但不能写入；而安全级别为“秘密”的用户访问安全级别为“高密”的文档，则会读取失败，但他能够写入。这样，文档的保密性就得到了保障。



- 信息系统是一个由低到高的层次化结构。

1. BLP保密性模型

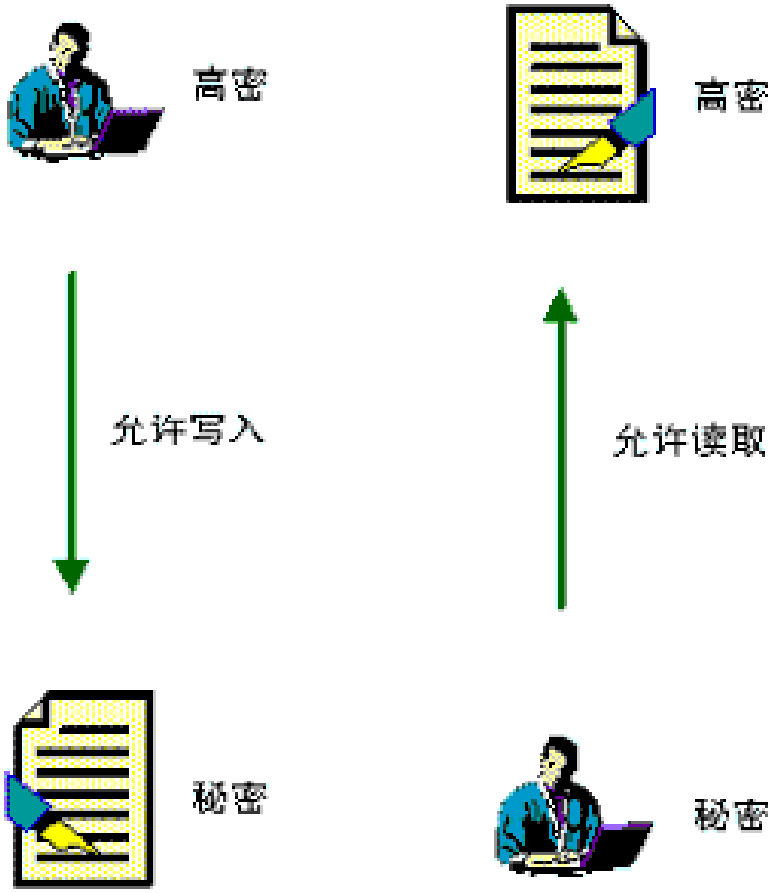
- 另一个例子是防火墙所实现的单向访问机制
- 所有内部数据被标志为“机密”或“高密”
- Internet（安全级别为“公开”）
- 防火墙提供“上读”功能来阻止Internet对内部网络的访问
- 提供“下写”功能来限制进入内部的数据流只能经由内向外发起的连接流入（例如，允许HTTP的“GET”操作而拒绝“POST”操作，或阻止任何外发的邮件）。

2. BIBA完整性模型

- 七十年代，**Ken Biba**提出了**BIBA**访问控制模型
- 该模型对数据提供了分级别的完整性保证，也使用强制访问控制系统。
- 数据和用户被划分为以下五个安全等级：
  - （1）公开（**Unclassified**）；
  - （2）受限（**Restricted**）；
  - （3）秘密（**Confidential**）；
  - （4）机密（**Secret**）；
  - （5）高密（**Top Secret**）。

2. BIBA完整性模型

- 基于两种规则来保障数据的完整性
  - 规则1　下读：主体不能读取安全级别低于它的数据；
  - 规则2　上写：主体不能写入安全级别高于它的数据。
- 一个安全级别为“机密”的用户要访问级别为“秘密”的文档，他将被允许写入该文档，而不能读取。如果他试图访问“高密”级的文档，那么读取操作将被允许，而写入操作将被拒绝。这样，就使资源的完整性得到了保障。



- 信息在系统中只能自上而下进行流动。

2. BIBA完整性模型

- BIBA模型在应用中的一个例子是对WEB服务器的访问过程。
- 定义Web服务器上发布的资源安全级别为“秘密”，Internet上用户的安全级别为“公开”，依照BIBA模型，Web服务器上数据的完整性将得到保障，Internet上的用户只能读取服务器上的数据而不能更改它，因此，任何“POST”操作将被拒绝。

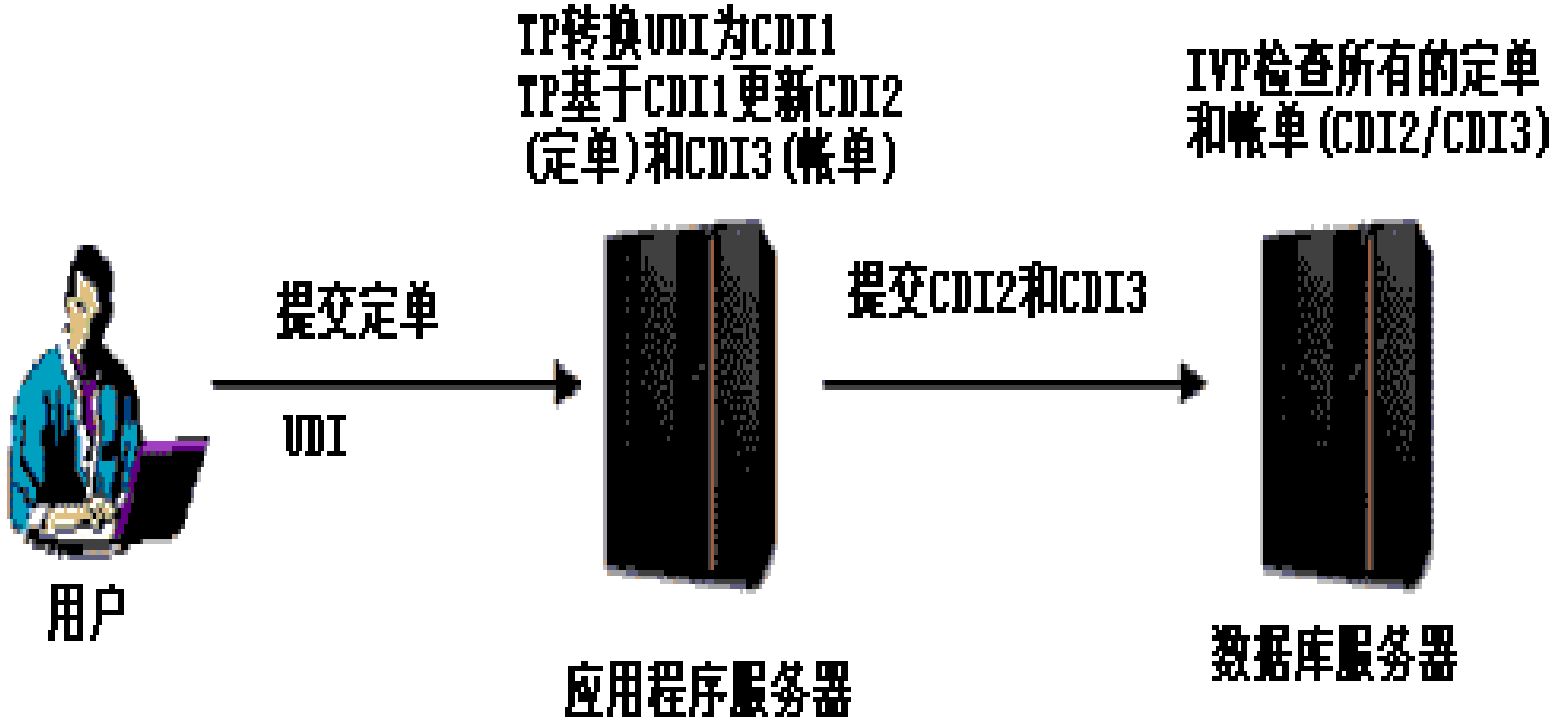
2. BIBA完整性模型

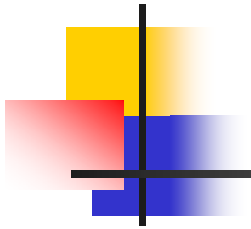
- 另一个例子是对系统状态信息的收集，网络设备作为对象，被分配的安全等级为“机密”，网管工作站的安全级别为“秘密”，那么网管工作站将只能使用**SNMP**的“**get**”命令来收集网络设备的状态信息，而不能使用“**set**”命令来更改该设备的设置。这样，网络设备的配置完整性就得到了保障。

3. Clark-Wilson完整性模型

- Clark-Wilson数据完整性安全模型是在1987年被提出的，通常被用在银行系统中来保证数据的完整性，是为现代数据存储技术量身定制的。
- 系统接受自由数据条目（UDI）并将其转换为受限数据条目（CDI）；
- 受限数据条目仅能被转换程序（TP）所改变；
- 转换程序保证受限数据条目的完整性；
- 每个受限数据条目拥有一个完整性检查程序（IVP）；
- 访问控制机制由三个元素组成（(主体，TP，CDI)。

3. Clark-Wilson完整性模型





1.5.5多边安全模型

- 1. Lattice安全模型
- 2. Chinese Wall模型

1. Lattice安全模型

- 多边意味着多个组织
- 多边安全系统即多个组织间的访问控制系统
- Lattice 模型通过划分安全边界对BLP模型进行了扩充，它将用户和资源进行分类，并允许它们之间交换信息。
- 多边安全的焦点是在不同的安全集束（部门，组织等）间控制信息的流动，而不仅是垂直检验其敏感级别。

1. Lattice安全模型

- 建立多边安全的基础
  - 为分属不同安全集束（组织，部门）的主体划分安全等级
  - 在不同安全集束中的客体也必须进行安全等级划分
  - 一个主体可同时从属于多个安全集束
  - 而一个客体仅能位于一个安全集束。

1. Lattice安全模型

- 在执行访问控制功能时
  - **lattice**模型本质上同**BLP**模型是相同的
  - 而**lattice**模型更注重形成“安全集束”
  - **BLP**模型中的“上读下写”原则在此仍然适用，但前提条件必须是各对象位于相同的安全集束中。
  - 主体和客体位于不同的安全集束时不具有可比性，因此在它们中没有信息可以流通。

2. Chinese Wall模型

- 安全策略的基础是客户访问的信息不会与目前他们可支配的信息产生冲突。
- 在投资银行中，一个银行会同时拥有多个互为竞争者的客户，一个银行家可能为一个客户工作，但他可以访问所有客户的信息。因此，应当制止该银行家访问其它客户的数据。

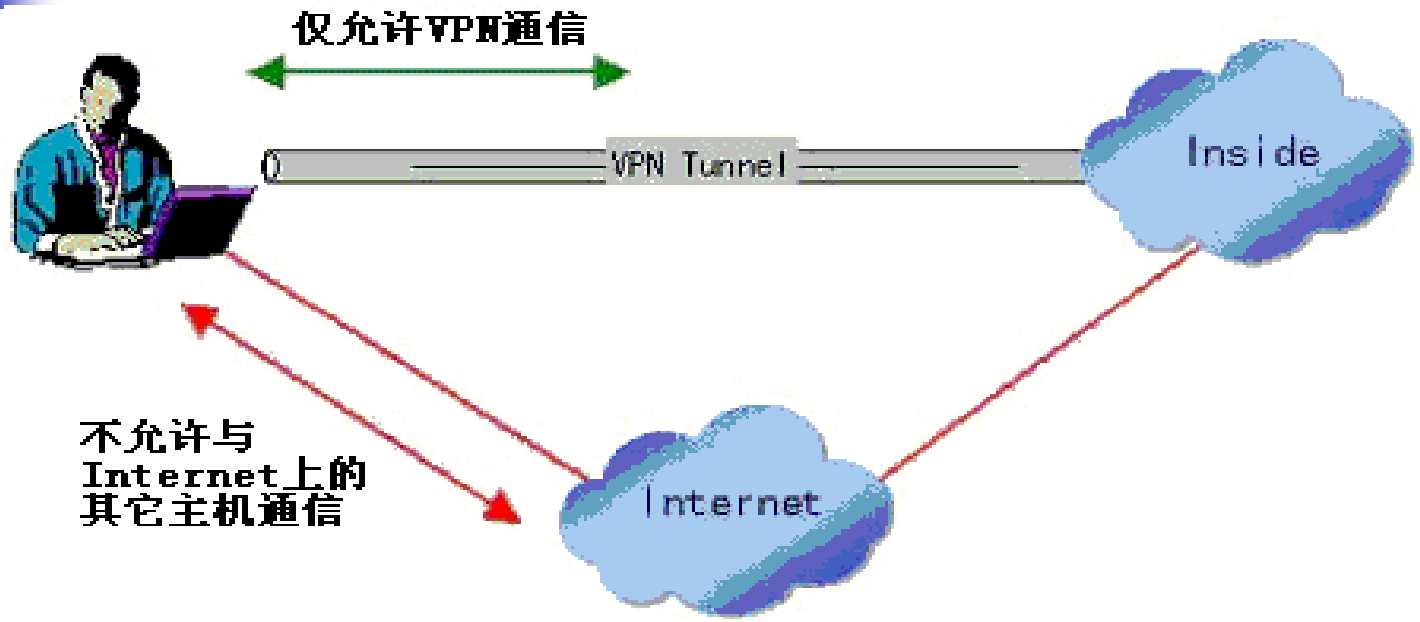
2. Chinese Wall模型

- **Chinese Wall**安全模型的两个主要属性：
- （1）用户必须选择一个他可以访问的区域；
- （2）用户必须自动拒绝来自其它与用户所选区域的利益冲突区域的访问。
- 银行家可以选择为谁工作，但是一旦选定，他就只能为该客户工作。

2. Chinese Wall模型—例子

- 位于防火墙内部的一台服务器，连接着内部与外部网络。假如策略禁止经由此服务器转发数据，该服务器将曝露于外部网络，也就是说，该服务器仅能与外部网络通讯，而不能与内部网络通讯。
- 另一个例子是远程访问**VPN**的情形。位于**Internet**上的用户与内部网络建立**VPN**会话之后，依照中国墙安全模型的建议，在任何时候，用户或与**Internet**通讯，或与公司网络进行通讯，二者只可选其一，也就是说，隧道不可分割。

2. Chinese Wall模型—例子



- 本安全模型的核心在于用户选择与其中一方进行通讯，则放弃了与另一方会话的权利。

1.6信息安全的标准

- **1.6.1** 信息安全标准的分类
- 1. 互操作标准
- 如对称加密标准DES、3DES、IDEA以及AES；非对称加密标准RSA；VPN标准IPSec；传输层加密标准SSL；安全电子邮件标准S-MIME；安全电子交易标准SET；通用脆弱性描述标准CVE。这些都是经过一个自发的选择过程后被普遍采用的算法和协议，是所谓的“事实标准”。

1.6信息安全的标准

- **2．技术与工程标准**
- **（1）信息产品通用测评准则（ISO 15408）**
- 通过信息安全产品的开发、评价和使用过程的各个环节的综合考虑来确保产品的安全性。
- （2）安全系统工程能力成熟度模型（SSE-CMM）
- 定义了一个安全工程过程应有的特征

1.6信息安全的标准

- （3）信息系统软件过程评估（ISO/IEC 15504）
- 该标准提供了一个软件过程评估的框架，它可以被任何组织用于软件的设计、管理、监督、控制以及提高获得、供应、开发、操作、升级和支持的能力。它提供了一种结构化的软件过程评估方法。

1.6信息安全的标准

- （4）信息和相关技术控制目标（COBIT）
- 它是安全与信息技术管理和控管的标准。COBIT归纳了世界上18项相关的来源，形成了一套专供企业经营者、使用者、IT专家、MIS稽核员和安控员来强化和评估IT管理和控制之规范。
- （5）系统与软件整合层次标准（ISO 15026）
-

1.6信息安全的标准

- （6）美国TCSEC（桔皮书）
- 1983年，美国发布“可信计算机系统评价标准TCSEC”（Trusted Computer Standard Evaluation Criteria orange book），该标准为计算机安全产品的评测提供了测试内容和方法，指导信息安全产品的制造和应用，是目前国际上影响最大的标准之一。它将安全分为7个安全级别（从低到高依次为D、C1、C2、B1、B2、B3和A级）和4个方面内容（安全政策、可说明性、安全保障和文档）。

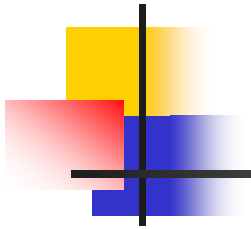
1.6信息安全的标准

- （7）欧洲ITSEC
- ITSEC是欧洲信息技术安全评估规则（Information Technology Security Evaluation Criteria）的简称，由英国、德国、法国、荷兰在二十世纪九十年代联合提出。ITSEC吸收了TCSEC的成功经验，并首次提出信息安全的保密性、完整性、可用性概念，把可信计算机的概念提高到可信信息技术的高度。ITSEC定义了从E0级（不满足品质级）到E6级（形式化验证级）的七个安全等级，对于每个信息系统，安全功能可以分别定义。

1.6信息安全的标准

- （8）加拿大CTCS
- **CTCS**是加拿大政府制定的可信任计算标准（**Canadian Trusted Computing Standard**），该标准由两部分组成：加拿大可信任计算机产品评估标准和普通标准，共划分为从**EAL1**到**EAL7**的七个保证级。

- 3．信息安全管理标准
- 常见的信息安全管理标准有：
- （1）信息安全管理体系标准（BS7799，其中第一部分成为ISO/IEC 17799）；
- （2）信息安全管理标准（ISO 13335）；



- （3）GB17895-1999《计算机信息系统安全保护等级划分准则》。
- 由我国公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准。该准则将信息系统安全分为五个等级：自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级，主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计跟踪等。

- **1.6.2** 安全管理标准**BS 7799**简介
- **BS 7799**是由英国标准协会（**BSI**）制定，主要提供了有效地实施**IT**安全管理的建议，介绍了安全管理的方法和程序。用户可以参照这个完整的标准制订出自己的安全管理计划和实施步骤，为有效的安全管理实践提供参考依据。

1.7 信息安全的发展趋势

- 1、信息安全技术的发展
  - 非对称计算技术、密码保护技术、信任计算技术
- 2、信息安全产品的发展
  - 被动防范、积极防范、可信计算
- 3、信息安全方案的发展
  - 外网安全方案、内网安全方案、应用安全方案
- 4、信息安全服务的发展
  - 产品售后服务、构架方案服务、风险管理服务