网络安全——

网络安全概述

北京邮电大学

郑康锋

zkfbupt@163.com

目录

- 资产保护
- 网络安全保障模型
- 网络攻击类型及分类
- 网络安全服务
- 网络安全评估
- 网络安全标准

网络安全概述——

资产保护

资产保护

资产的类型：任何有效的风险分析始于需要保护的资产和资源的鉴别。一般可分成以下4类：

- 物理资源：**物理资源是具有物理形态的资产。**包括工作站、服务器、终端、网络设备、外围设备等，基本上，凡是具有物理形态的计算资源都是物理资源。

- 知识资源：和物理资源相比，知识资源更难鉴别，因为它只以电子的形式存在。**知识资源可以是任何信息的形式，并直在组织的事务处理中起一定的作用。**它包括软件、财务信息、数据 库记录以及计划图表等。例如，公司通过电子邮件交换、信息，这些电子报文的存储应看成 知识资产。

资产保护

- **时间资源**：时间也是一个重要的资源，甚至是一个组织最有价值的资源。当评估时间损失对一个组织的影响时，应考虑、由于时间损失引起的全部后果。

- **信誉资源**：在2000年2月，大部分网络公司诸如Yahoo、Amazon、eBay和Buy. com等在受到拒 绝服务攻击以后，他们的股票价狂跌。虽然这是暂时的，但足以说明消费者和股票持有者对他们的可信度确实存在影响，且可测量。又如，2000年10月围绕Microsoft系统的问 题公开暴露，公众不仅对公司，也对其产品的可信度产生了一定的影响。

资产保护

资产的有效保护。资产一旦受到威胁和破坏，就会带来两类损失：

- **一类是即时的损失**，如由于系统被破坏，员工无法使用，因而降低了劳动生产率；又如，ISP的在线服务中断带来经济上的损失；

- **另一类是长期的恢复所需花费**，也就是从攻击或失效到恢复正常需要的花费，例如，受到拒绝服务攻击，在一定期间内资源无法访问带来的损失；又如，为了修复受破坏的关键文件所需的花费等。

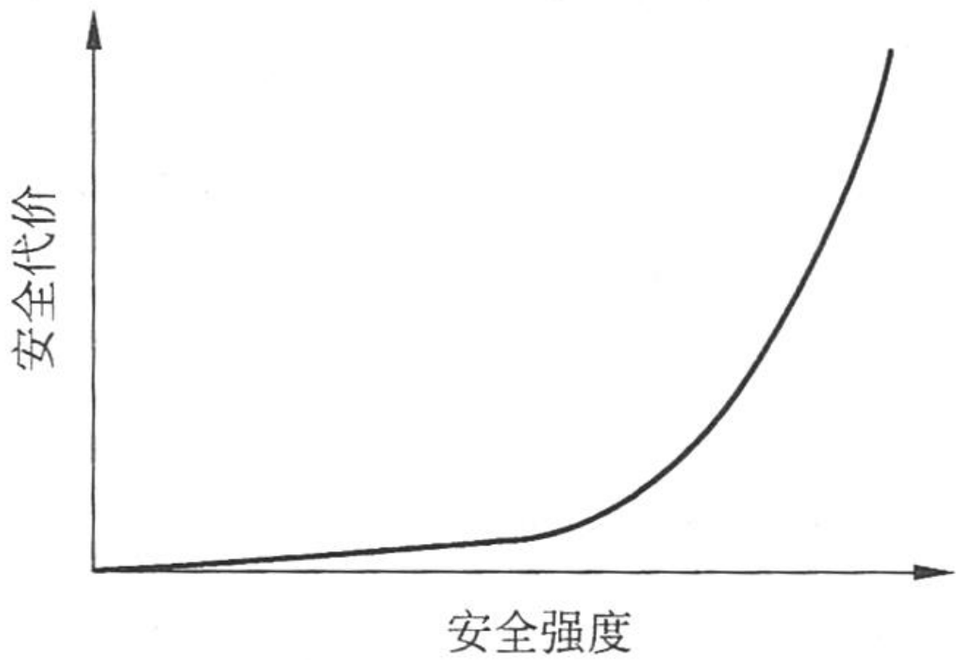
资产保护

要获得安全强度和安全代价的折中，需要考虑以下因素：

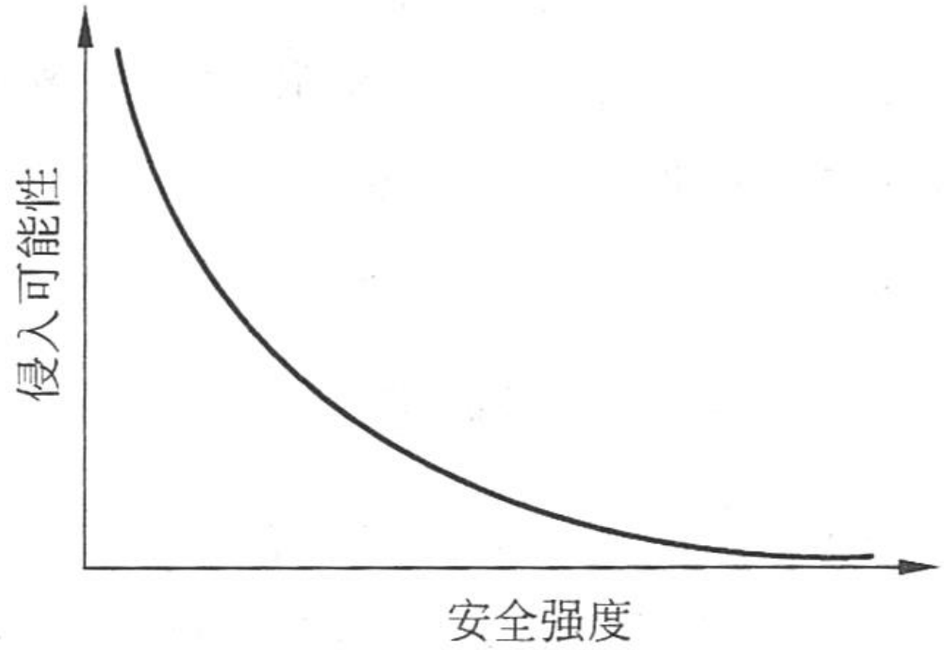
- **用户的方便程度**。不应由于增加安全强度给用户带来很多麻烦。
- **管理的复杂性**。对增加安全强度的网络系统要易于配置、管理。
- **对现有系统的影响**。包括对增加的性能开销以及对原有环境的改变等。
- **对不同平台的支持**。网络安全系统应能适应不同平台的异构环境的使用。

资产保护

安全强度、安全代价和侵入可能性的关系



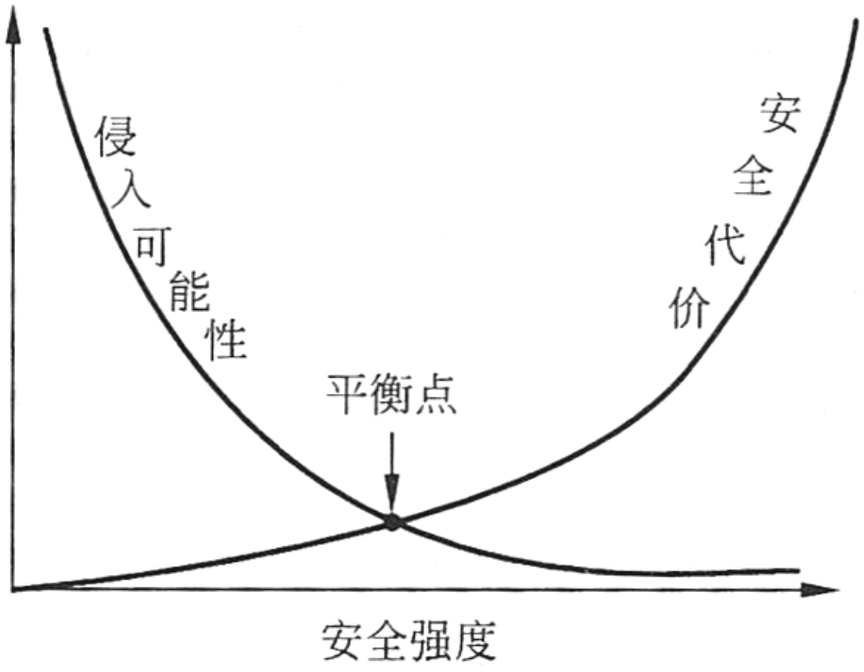
(a) 安全强度和安全代价的关系



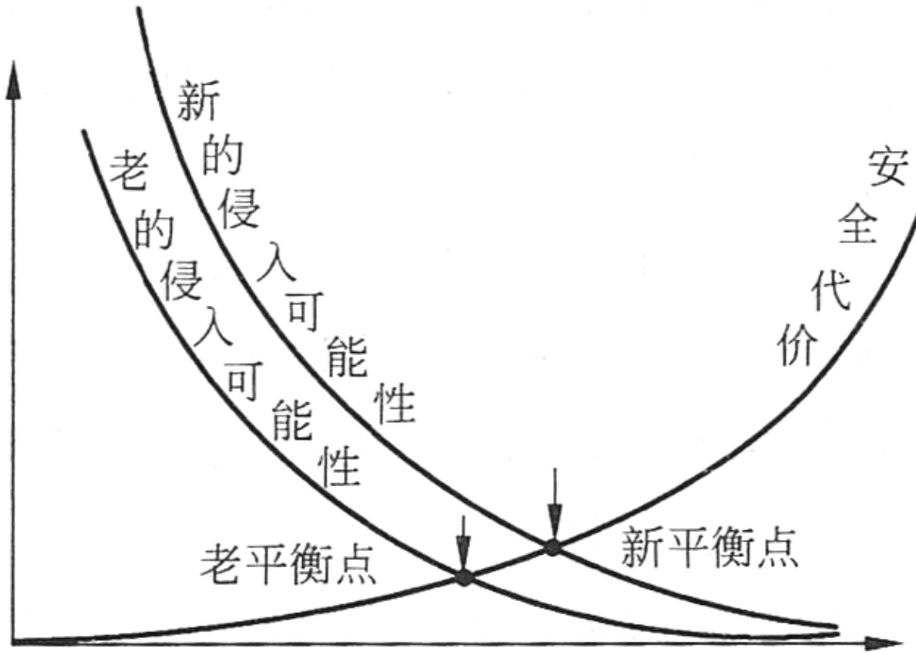
(b) 安全强度和侵入可能性的关系

资产保护

安全强度、安全代价和侵入可能性的关系



(c) 安全代价和侵入可能性的折中



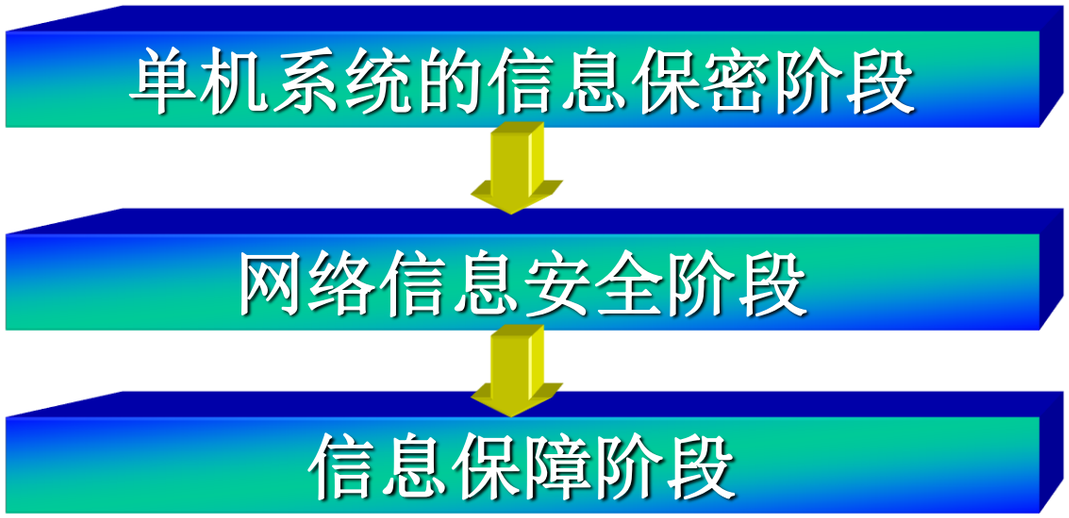
(d) 平衡点的变化

网络安全概述——

信息安全模型

信息安全概念与技术的发展

信息安全的概念与技术是随着人们的需求，随着计算机、通信与网络等信息技术的发展而不断发展的。



单机系统的信息保密阶段

信息保密技术的研究成果：

① **发展各种密码算法及其应用**：

DES（数据加密标准）、RSA（公开密钥体制）、ECC（椭圆曲线离散对数密码体制）等。

② **计算机信息系统安全模型和安全评价准则**：

访问监视器模型、多级安全模型等；TCSEC（可信计算机系统评价准则）、ITSEC（信息技术安全评价准则）等。

信息保障阶段

信息保障（IA）概念与思想的提出：20世纪90年代由美国国防部长办公室提出。

定义：通过确保信息和信息系统的可用性、完整性、可控性、保密性和不可否认性来保护信息系统的信息作战行动，包括综合利用保护、探测和反应能力以恢复系统的功能。

信息保障阶段

- 信息保障技术框架IATF：由美国国家安全局制定，提出“纵深防御策略”DiD（Defense-in-Depth Strategy）。

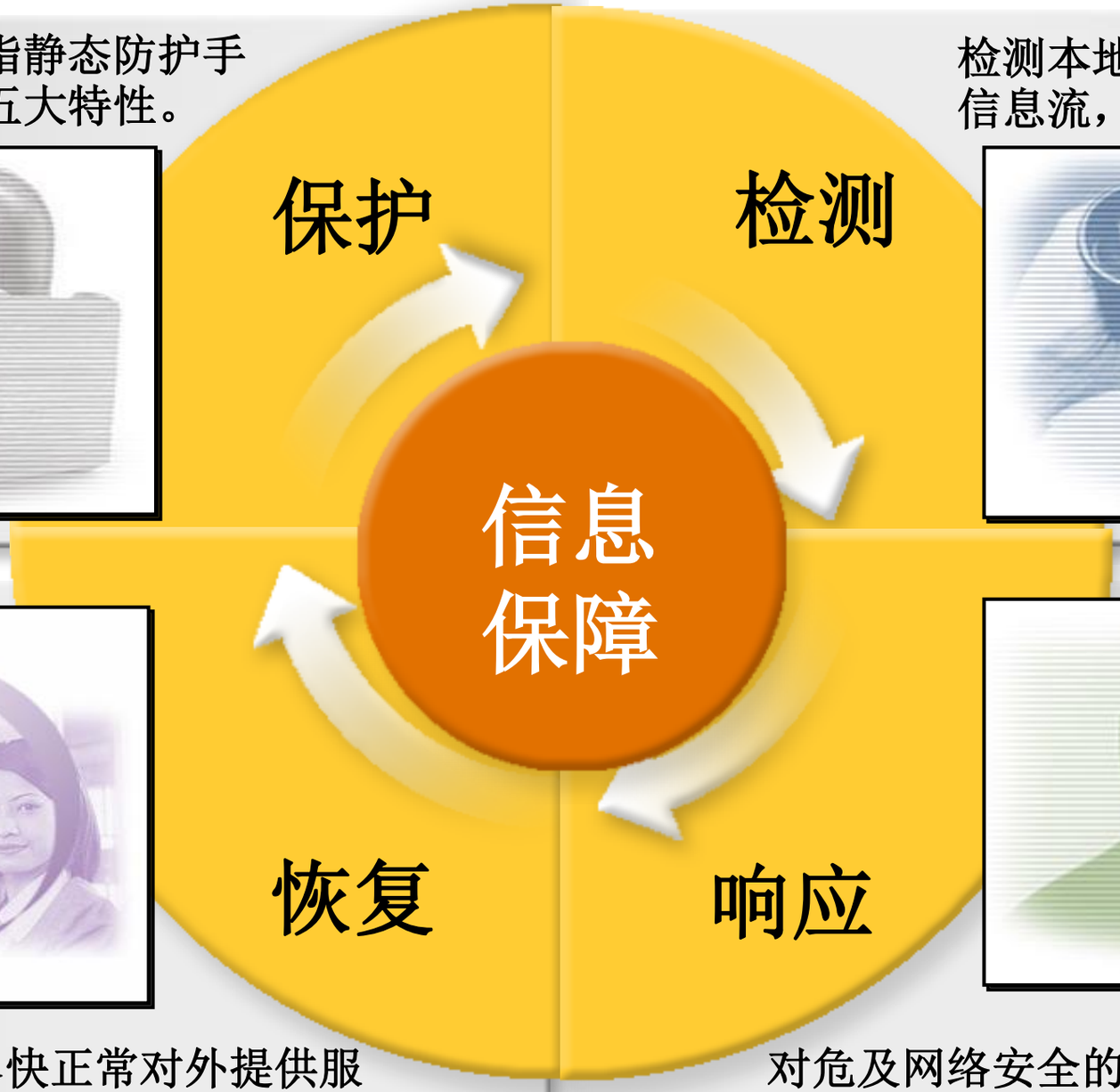
- 在信息保障的概念下，信息安全保障的PDRR模型的内涵已经超出了传统的信息安全保密，而是保护（Protection）、检测（Detection）、响应（Reaction）和恢复（Restore）的有机结合。

- 信息保障阶段不仅包含安全防护的概念，更重要的是增加了主动和积极的防御观念。

PDRR安全模型

采用一切手段（主要指静态防护手段）保护信息系统的五大特性。

检测本地网络的安全漏洞和存在的非法信息流，从而有效阻止网络攻击



及时恢复系统，使其尽快正常对外提供服务，是降低网络攻击造成损失的有效途径

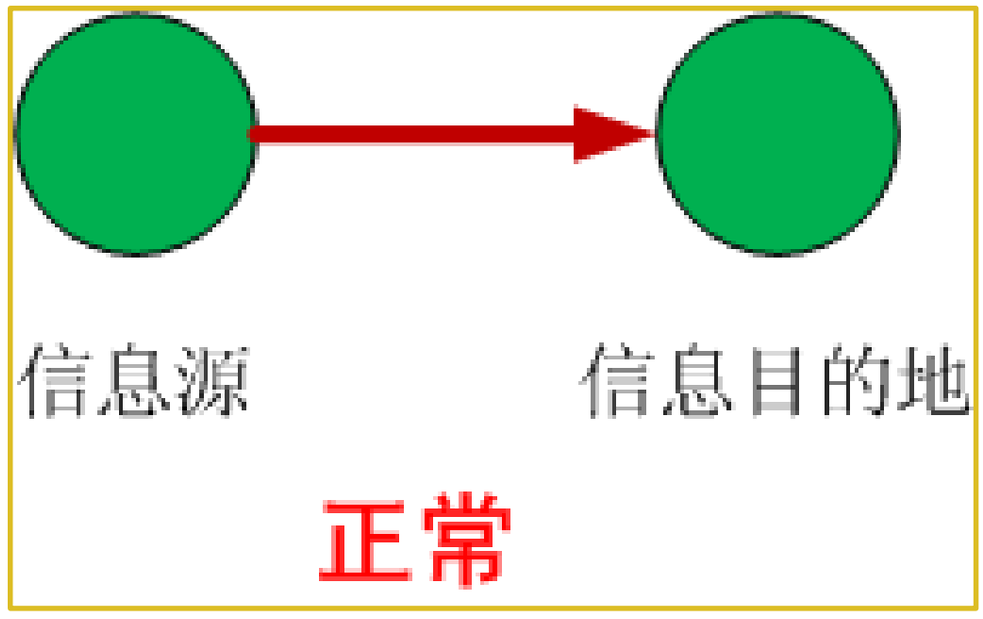
对危及网络安全的事件和行为做出反应，阻止对信息系统的进一步破坏并使损失降到最低

网络安全概述——

网络攻击类型及分类

攻击类型

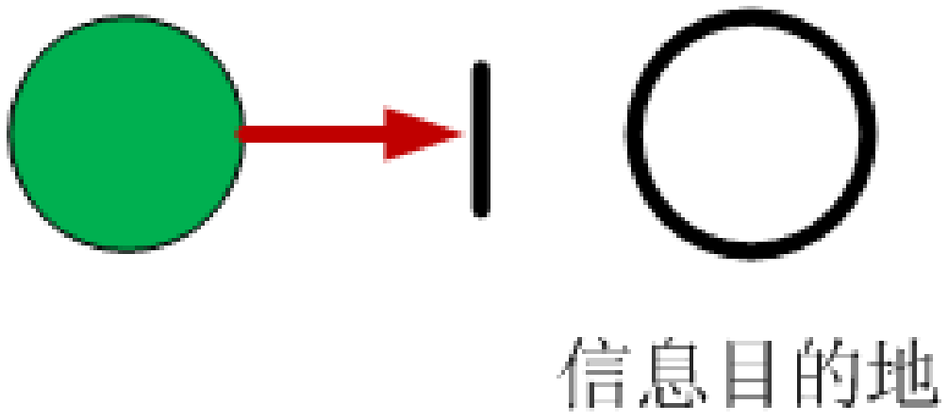
攻击的类型。从安全属性来看，攻击类型可分为4类：阻断攻击、截取攻击、篡改攻击、伪造攻击；



上图是从源站到目的站的正常信息流。

攻击类型

- (1)阻断攻击
- 阻断攻击使系统的资产被破坏，无法提供用户使用，这是一种针对可用性的攻击。例如，破坏硬盘之类的硬件，切断通信线路，使文件管理系统失效等。

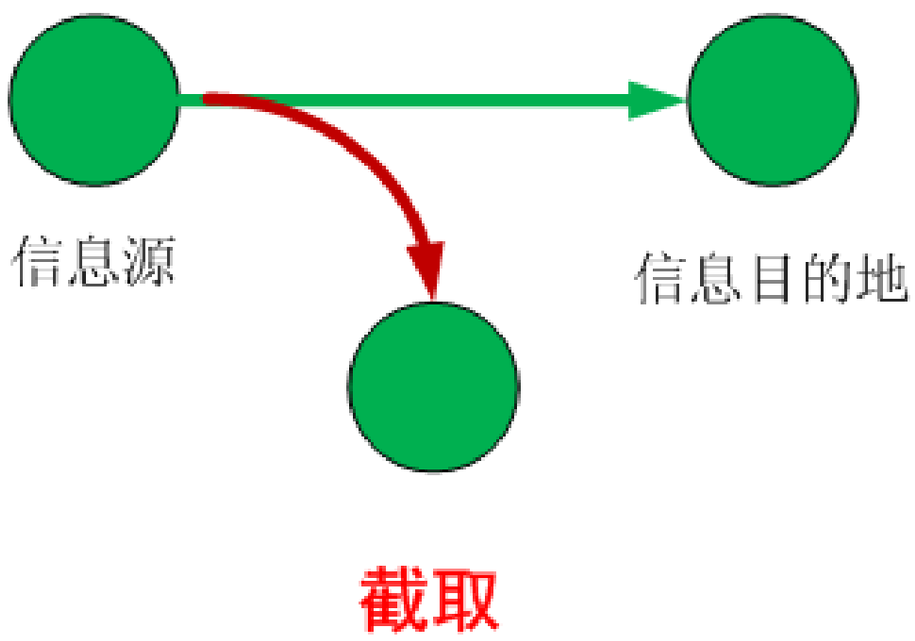


阻断

攻击类型

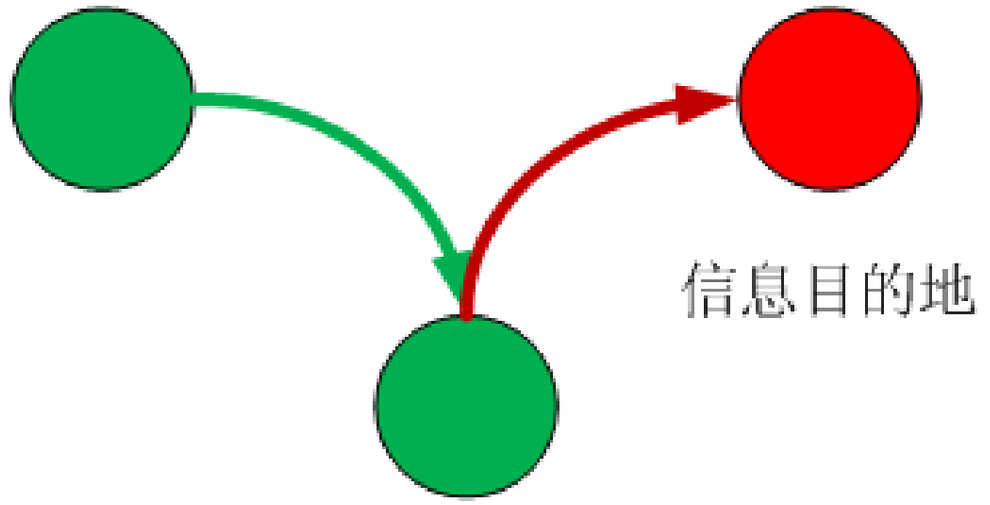
➔(2)**截取攻击**

➔截取攻击可使非授权者得到资产的访问，这是一种针对机密性的攻击。非授权者可以是一个人、一个程序或一台计算机，例如，通过窃听获取网上数据以及非授权的复制文件和程序。



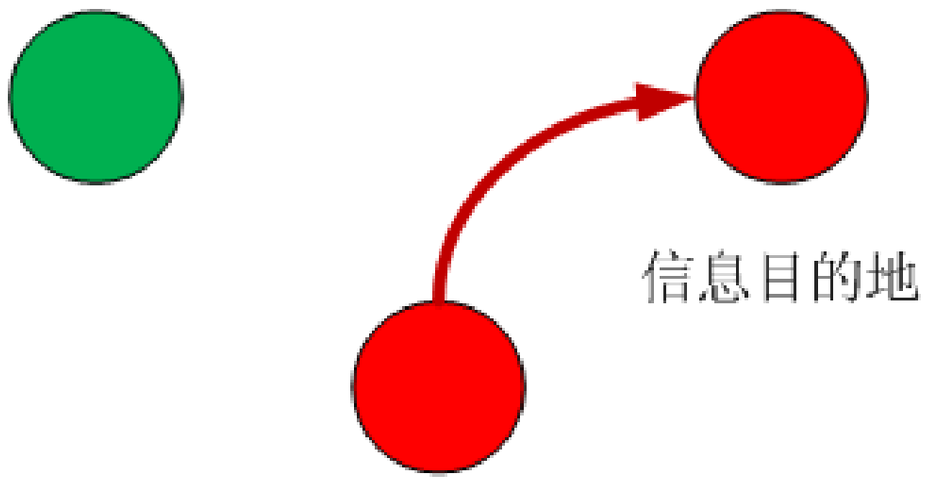
攻击类型

- (3)篡改攻击
- 篡改攻击是非授权者不仅访问资产，而且能修改信息，这是一种针对完整性的攻击。例如，改变数据文件的值，修改程序以及在网上正在传送的报文内容。



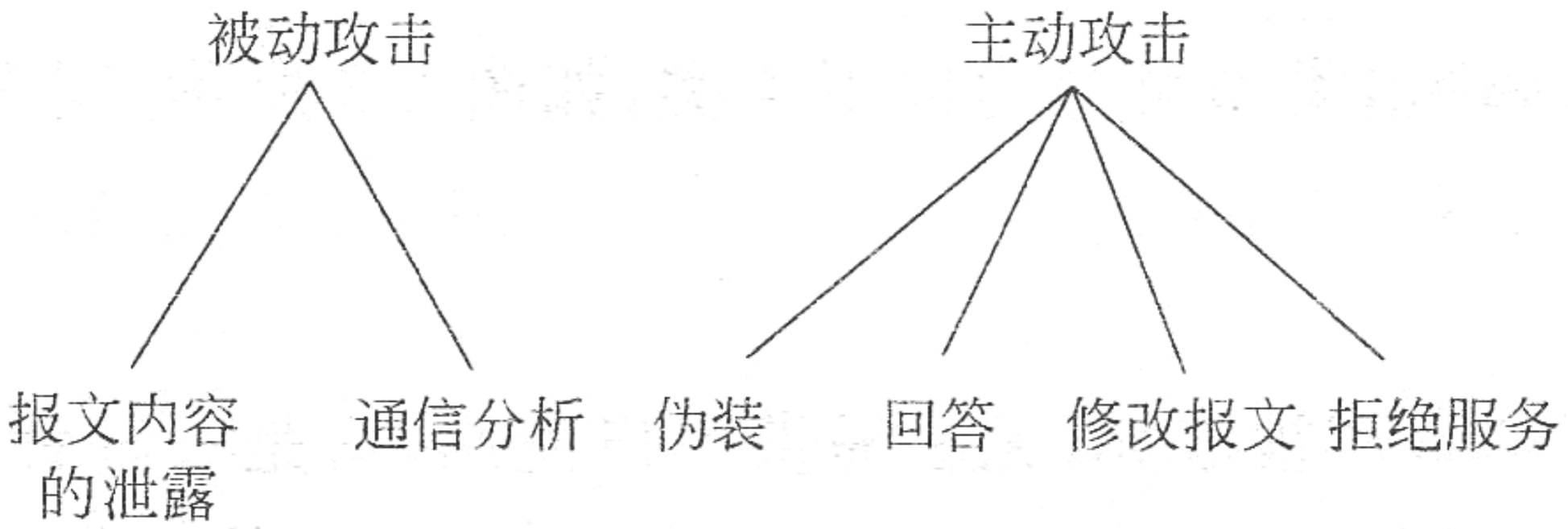
攻击类型

- (4)**伪造攻击**
- 伪造攻击是非授权者在系统中插入伪造的信息，这是一种针对真实性的攻击。例如：在网上插入伪造的报文，或在文件中加入一些记录。



攻击类型

- **主动攻击和被动攻击**
  - ➔从攻击方式来看，攻击类型可分为被动攻击和主动攻击



攻击类型

- **被动攻击**
  - 目的是获取正在传输的信息。**被动攻击包括传输报文内容的泄露和通信流量分析**。报文内容的泄露易于理解，一次电话通信、一份电子邮件报文、正在传送的文件都可能包含敏感信息或秘密信息。
  - **对被动攻击的检测十分困难，因为攻击并不涉及数据的任何改变。然而阻止这些攻击的成功是可行的，因此，对被动攻击强调的是阻止而不是检测。**

攻击类型

- **主动攻击**：包含对数据流的某些修改，或者生成一个假的数据流。它可分成4类:

  - (1)**伪装**

    - 伪装是一个实体假装成另一个实体。伪装攻击往往连同另-类主动攻击一起进行。
    - 例如，身份鉴别的序列被捕获，并在有效的身份鉴别发生时作出回答，有可能使具有很少 特权的实体得到额外的特权，这样不具有这些特权的人获得了这些特权。

  - (2)**回答**

    - 回答攻击包含数据单元的被动捕获，随之再重传这些数据，从而产生一个非授权的 效果。

攻击类型

- (3)修改报文
  - 修改报文攻击意味着合法报文的某些部分已被修改，或者报文的延迟和重新排序，从 而产生非授权的效果。
- (4)拒绝服务
  - 拒绝服务攻击是阻止或禁止通信设施的正常使用和管理。这种攻击可能针对专门的 目标(如安全审计服务)，抑制所有报文直接送到目的站;也可能破坏整个网络，使网络不可用或网络超负荷，从而降低网络性能。
- **主动攻击和被动攻击具有相反的特性。被动攻击难以检测出来，然而有阻止其成功的方法。而主动攻击难以绝对地阻止，因为要做到这些，就要对所有通信设施、通路在任 何时间进行完全的保护。因此对主动攻击采取检测的方法，并从破坏中恢复。**

攻击类型

- **访问攻击**
  - 攻击者企图获得非授权信息，这种攻击可能发生在信息驻留在计算机系统中或在网络上传输的情况下。是针对信息机密性的攻击。
  - 常见的访问攻击有3种:
    - (1)**窥探(snooping)**：是查信息文件，发现某些攻击者感兴趣的信息。攻击者试图打开计算机系统的文件，直到找到所需信息；
    - (2)**窃听(eavesdropping)**：是偷听他人的对话，为了得到非授权的信息访问，攻击者必须将自己放在一个信息通过的地方，一般采用电子的窃听方式；
    - (3)**截获(interception)**：不同于窃听，它是一种主动攻击方式。攻击者截获信息是通过将自己插入信息通过的通路，且在信息到达目的地前能事先捕获这些信息。

攻击类型

- **篡改攻击**
  - 篡改攻击是攻击者企图修改信息，而他们本来是无权修改的。这种攻击可能发生在信息驻留在计算机系统中或在网络上传输的情况下，是针对信息完整性的攻击。
  - 常见的篡改攻击有3种:
    - (1)**改变**：改变已有的信息。例如，攻击者改变已存在的员工工资，改变以后的信息虽然仍存在于该组织，但已经是不正确的信息。这种改变攻击的目标通常是敏感信息或公共信息。
    - (2)**插入** ：插入信息可以改变历史的信息。例如，攻击者在银行系统中加一个事务处理，从而将 客户账户的资金转到自己账户上。
    - (3)**删除** ：删除攻击是将已有的信息去除，可能是将历史记录的信息删除。例如，攻击者将一个事务处理记录从银行结账单中删除，从而造成银行资金的损失。

攻击类型

- **拒绝服务攻击**
  - 拒绝服务攻击(Denial-of-Service， DoS)是拒绝合法用户使用系统、信息、能力等各种资源。可分成以下4种:
    - (1)**拒绝访问信息**：使信息不可用，信息被破坏或者将信息改变成不可使用状态，也可能信息仍存在，但已经被移到不可访问的位置。
    - (2)**拒绝访问应用**：目标是操纵或显示信息的应用。通常对正在运行应用程序的计算机系统进行攻击，使应用程序不可用而不能完成任务。
    - (3)**拒绝访问系统**：通常是使系统宕机，使运行在该计算机系统上的所有应用无法运行，使 存储在该计算机系统上的所有信息不可用。
    - (4)**拒绝访问通信**：是针对通信的一种攻击，已有很多年历史。这类攻击可能用切断通信电缆、干扰无线电通信以及用过量的通信负载来淹没网络。

攻击类型

- **否认攻击**
  - 否认攻击是针对信息的可审性进行的。否认攻击企图给出假的信息或者否认已经发生的现实事件或事务处理。
  - 否认攻击包括两类:
    - (1)**假冒**：假冒是攻击者企图装扮或假冒别人和别的系统。这种攻击可能发生在个人通信、事务处理或系统对系统的通信中。
    - (2)**否认**：否认一个事件是简单地抵赖曾经登录和处理的事件。例如，一个人用信用卡在商店 里购物，然而当账单送到时，告诉信用卡公司，他从未到该商店购物。

攻击分类

- **网络攻击分类原则**
  - 可接受性：分类方法符合逻辑和惯例，易于被大多数人接受；
  - 确定性（也称无二义性）：对每一分类的特点描述准确；
  - 完备性（也称无遗漏性）：分类体系能够包含所有的攻击；
  - 互斥性：各类别之间没有交叉和覆盖现象；
  - 可重现性：不同人根据同一原则重复分类的过程，得出的分类结果是一致的；
  - 可用性：分类对不同领域的应用具有实用价值；
  - 适应性：可适应于多个不同的应用要求；
  - 原子性：每个分类无法再进一步细分。

攻击分类

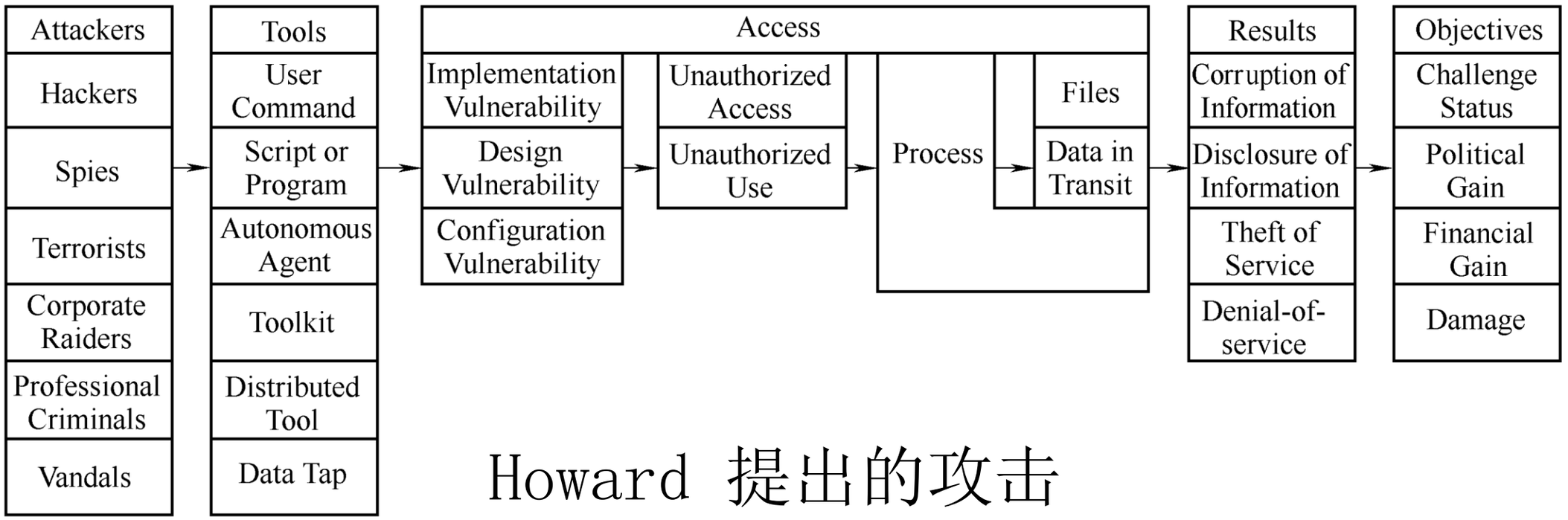
- **按照经验术语分类**
  - Icove按经验将攻击分成病毒和蠕虫、资料欺骗、拒绝服务、非授权资料拷贝、侵扰、软件盗版、特洛伊木马、隐蔽信道、搭线窃听、会话截持、IP 欺骗、口令窃听、越权访问、扫描、逻辑炸弹、陷门攻击、隧道、伪装、电磁泄露、服务干扰等20 余类；
  - Cohen将攻击分为特洛伊木马、伪造网络资料、冒充他人、网络探测、电子邮件溢出、时间炸弹、获取工作资格、刺探保护措施、干扰网络、社会活动、贿赂、潜入、煽动等。

攻击分类

- **基于单一属性的分类方法**
  - Neumann 和Parker通过分析3000 余种攻击实例，从系统滥用的角度将攻击分为9类，即外部滥用、硬件滥用、伪造、有害代码、绕过认证或授权、主动滥用、被动滥用、恶意滥用、间接滥用，并进一步将其细化为26 种具体的滥用攻击。
  - Stallings依据实施方法对网络攻击进行了分类，将攻击实施的手段归纳为5 种，分别是中断、拦截、窃听、篡改、伪造。
  - Jayaram从攻击的实施方法将网络攻击分成物理攻击、系统弱点攻击、恶意程序攻击、权限攻击和面向通信过程的攻击5类。
  - Cheswick和Bellovin依据攻击后果将针对防火墙的攻击分成窃取口令、错误和后门、信息泄漏、协议失效、认证失效、拒绝服务等类别。

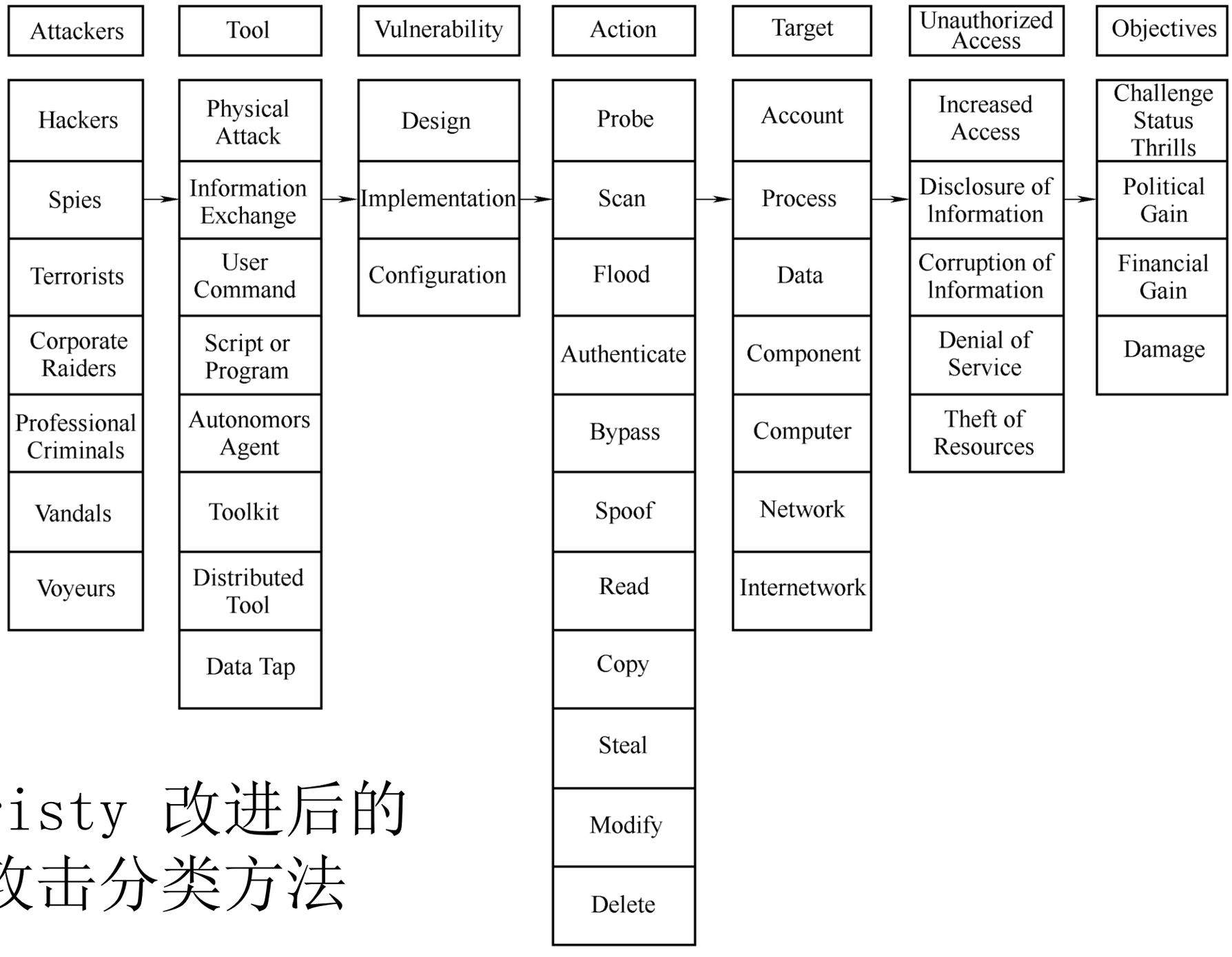
攻击分类

- **基于多属性的分类方法**
  - 基于多属性的分类方法指同时抽取攻击的多个属性，并利用这些属性组成的序列来表示一个攻击过程，或由多个属性组成的结构来表示攻击，并对过程或结构进行分类的方法。



Howard 提出的攻击分类方法

攻击分类



Christy 改进后的攻击分类方法

攻击分类

- 基于应用的分类方法：基于应用的分类方法是对特定类型应用、特定系统而发起的攻击的属性进行分类描述的方法。
  - Alvarez和Petrovie在分析对Web应用而发起的攻击时，重点从攻击入口、漏洞、行为、长度、HTTP 头及动作、影响范围、权限等方面对攻击进行描述，并用不同长度的比特位所代表的数字来表示每一个属性，从而形成一个攻击编码向量；
  - Weaver等人从目标发现、选择策略、触发方式等角度对计算机蠕虫进行了描述，对于攻击者也按其动机不同进行了划分；
  - Mirkovic等人在对DDOS 类攻击进行描述时，对其自动化程度、扫描策略、传播机制、攻击的漏洞、攻击速度的动态性、影响等属性进行了划分；

网络安全概述——

网络信息安全服务

网络信息安全服务

- 针对不同攻击需要的安全服务

安全服务 / 攻击	机密性	完整性	可用性	可审性
访问攻击	×			×
篡改攻击		×		×
拒绝服务			×	
否　　认		×		×

网络信息安全服务

- **机密性服务**：提供信息的保密。
- **完整性服务**：提供信息的正确性。
- **可用性服务**：提供的信息是可用的。
- **可审性服务**：本身不针对攻击提供保护，需与其它服务结合。

机密性防护

- **文件机密性**
  - 对纸面文件，主要是存放这类文件的物理位置必须是可控的，通过物理位置的访问控 来保护文件的机密性。
  - 对电子文件，有几种情况：
    - 文件可能同时存放在不同位置，如后备磁带、多个计真机系统、软盘或CD等。因此，也需要物理位置的访问控制；
    - 存放在计算机系统中的电子文件，可以使用访问控制及加密。
  - 为实现文件机密性服务，所需提供的机制包括物理安全机制、计算机文件访问控制以及文件加密。
  - 文件机密性的要求包括身份标识和身份鉴别、正确的计算机系统配置，如使用加密则还需合适的密钥管理。

机密性防护

- **信息传输机密性**

  - 仅仅保护存储在文件中的信息是远远不够的。信息有可能在传输过程中受到攻击， 主此必须同时保护在传输中的信息机密性。

  - 可基于每个报文信息进行加密保护，也可以对链路上的所有通信进行加密。

  - 加密能阻止窃听，但不能完全阻止信息的截获。为了保护被截获的信息，需要合适的身份标识和身份鉴别，它可决定远程端点的身份。

机密性防护

- **通信流机密性**
  - 主要关心两个端点之间所发生的通信形式。
  - 这些信息形式通过通信分析可识别组织之间的通信情况。例如，很多新闻机构发现某一时刻有大量的快餐送至政府某重要规关，则可推测某些紧急事件甚至是危机可能发生。
  - 在大量通信流的两个端点之间加入模糊(遮掩)信息流可提供通信流机密性服务。

完整性防护

- **文件完整性**

  - 纸面文件：为防止修改纸面文件，可采用多种方法，包括在每一页上签名、装订成册、分发多个文件复制本等。另一种方法是使用与机密性服务相同的机制，完全阻止非授权者访问文件。

  - 电子文件：对电子文件进行修改比较容易，使用字处理工具进行。保护电子信息完整性的最基本的方法是采用与保护信息机密性一样的方法，即计算机文件访问控制。如同机密性服务，十分重要的是必须正确识别那些企图修改文件的访问者。这只有通过身份标识和身份鉴别来实现。

  - 因此完整性服务也必须和身份标识、身份鉴别功能结合在一起。

完整性防护

- **信息传输完整性**

  - 信息在传输中也可能被修改，然而如果不实施截获攻击就很难对传输中的信息进行修改。通常用加密方法可阻止大部分的篡改攻击。当加密和强身份标识、身份鉴别功能结合在一起时，截获攻击便难以实现。

  - 因此，完整性服务可成功地阻止篡改攻击和否认攻击。任何篡改攻击都可能改变文件或传输中的信息，当完整性服务能检测到非授权者的访问，篡改攻击就不能成功进行。当完整性服务和身份标识、身份鉴别服务很好地结合，即使组织以外的文件被 改变也能被检测出来。

可用性防护

- **可用性**是用来对拒绝服务攻击的系统恢复。可用性并不能阻止DoS，但可用性服务可用来减少这类攻击的影响。

  - 后备：后备是最简单的可用性服务，是指对重要信息复制一份拷贝，并将其存储在安全的地方。

  - 在线恢复：在线恢复提供信息和能力的重构。不同于后备，带有在线恢复配置的系统能检测出故障，并重建诸如处理、信息访问、通信等能力。它是通过使用冗余硬件自动处理的。

  - 灾难恢复 ：灾难恢复是针对大的灾难来保护系统、信息和能力。灾难恢复是当整个系统或重要 兰主备不可用时采取的重构一个组织的进程。

可审性防护

- **身份标识与身份鉴别**
  - 有两个目的：其一是对试图执行一个功能的每个人的身份进行标识；其二是验证这些人声称的身份。
  - 身份鉴别可使用以下任何一种或其组合的方法 实现:
    - (1)知识因子——你知道什么，如口令或PIN(个人身份标识号)。
    - (2)拥有因子——你有什么，如智能卡或标记。
    - (3)生物因子——你是什么，如指印、视网膜。

可审性防护

- **身份认证技术**
  - 口令技术：是常用的一种身份认证技术，使用口令存在的最大问题是口令的泄露。譬如：被他人看见、被猜出、放在文件中被读取；
  - 采用物理形式的身份认证标记进行身份认证的鉴别技术：常用的身份认证标记是磁卡和智能卡；
  - 生物特征：指纹、虹膜、脸型等

可审性防护

- **身份认证协议**
  - 基于密码学原理的密码身份认证协议比基于口令或者地址的认证更加安全，而且能 运提供更多的安全服务。
  - 身份认证协议一般有两个通信方，可能还会有一个双方都信任的第三方参与进行。 其中一个通信方按照协议的规定向另一方或者第三方发出认证请求，对方按照协议的规定作出响应或者其他规定的动作，当协议顺利执行完毕时双方应该确信对方的身份。

可审性防护

- **审计功能**

  - 在物理世界，审计的方法有入门的日志、签名本、录像仪等二这些物理记录的目的是 提供执行各种行动的记录。应该特别指出的是，必须采用完整性服务以保证这些审计记 录没有被修改过。否则，这些审计记录是值得怀疑的。

  - 在电子世界，计算机系统提供日志，以记录用户ID的行动。假如身份标识与身份鉴别功能的作用合适，这些事件就能跟踪用户的行为。同样，必须保护好计算机系统上的审 计记录，防止非授权者对其进行修改，事实上，审计记录要防止任何人的修改。

数字签名

- 在完整性服务与可审性服务中都提到数字签名。
- **数字签名**是通信双方在网上交换信息用公钥密码防止伪造和欺骗的一种身份认证。
- 在传统密码中，通信双方用的密钥是一样的，既然如此，收信方可以伪造、修改密文，发信方也可以抵赖他发过该密文，若产生纠 卦，将无法裁决谁是谁非。

数字签名

若 A 要向 B 送去信息 m，A 可用 A 的保密的解密算法 D_A 对 m 进行加密得 $D_A(m)$，再用 B 的公开算法 E_B 对 $D_A(m)$ 进行加密得

$$C=E_B(D_A(m))$$

B 收到密文 C 后先用他自己掌握的解密算法 D_B 对 C 进行解密得

$$D_B(C)=D_B(E_B(D_A(m)))=D_A(m)$$

再用 A 的公开算法 E_A 对 $D_A(m)$ 进行解密得

$$E_A(D_A(m))=m$$

从而得到了明文 m。

由于 C 只有 A 才能产生，B 无法伪造或修改 C，所以 A 也不能抵赖，这样就能达到签名的目的。不是所有公钥系统都具有数字签名的能力，RSA 第一个提出这样的功能。

Kerberos鉴别

- Kerberos鉴别是一种使用对称密钥加密算法来实现通过可信第三方密钥分发中心（KDC)的身份认证系统。

- 是美国麻省理工学院(MIT)为了保护Athena项目中的网络服务和资源而开发的， Kerberos版本5的协议已被Internet工程部IEIF正式接受为 RFC 1510。

Kerberos鉴别

- Kerberos使用对称密钥加密算法来实现通过可信第三方密钥分发中心的认证服务，它提供了网络通信方之间相互的身份认证手段，而且并不依赖于主机操作系统和地址。

- Kerberos设计的目标是在开放网络上运行，不要求网络上所有主机的物理安全，同时还 假设通过网络传输的包可以被任意截获、修改和插入。Kerberos系统非常适合在一个物理网络并不安全的环境下使用，它的安全性经过了实践的考验。

公钥基础设施

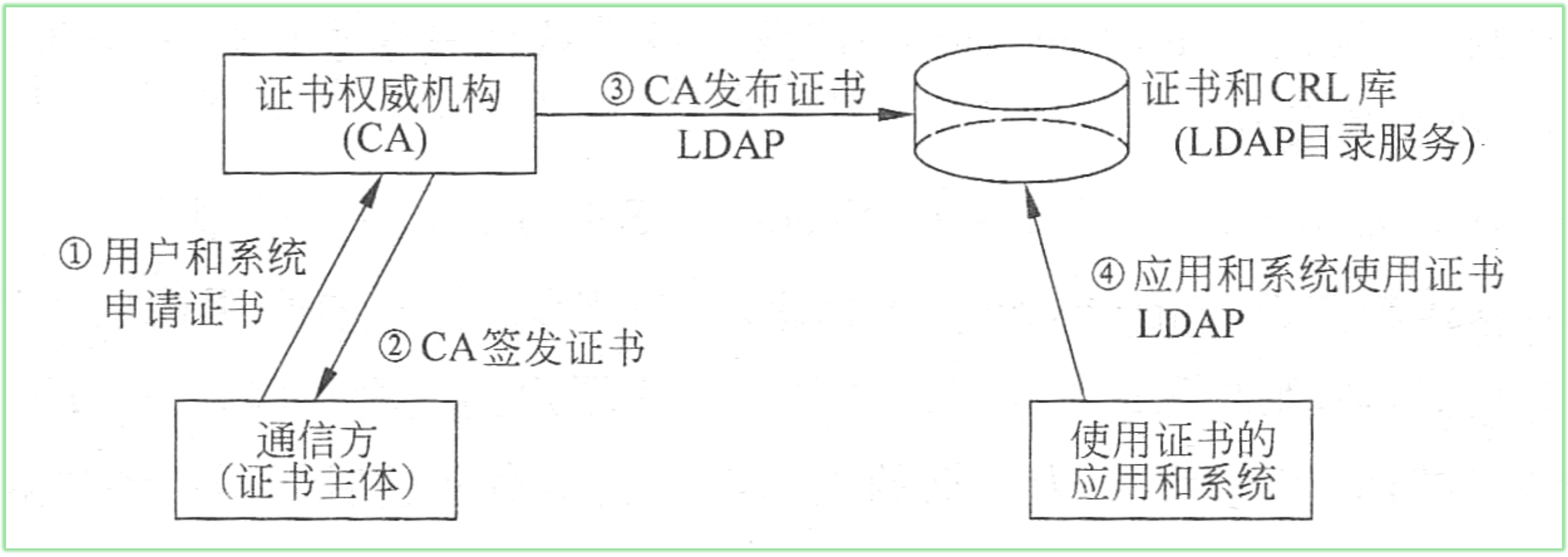
- 公钥基础设施(PKI)是在分布式计算系统中提供的使用公钥密码系统和X.509证书安全服务的基础设施。

- PKI产品和服务允许使用者在网络上建立一个安全领域，在该领或中可以签发密钥和证书。

- PKI支持使用者在建立的安全领域中进行加密密钥和证书的使用和管理，提供密钥管理(包括密钥更新、恢复和托管）、证书管理(包括产生和撤销），以及互安全政策管理等。

- PKI还提供通过证书层次结构(Certificate Hierarchy)或者通过直接专叉证书(Cross Certificate)的方法在本地安全领域与其他安全领域之间建立相互信任的关系。

公钥基础设施


证书权威机构
(CA)
③ CA发布证书
LDAP
证书和CRL 库
(LDAP目录服务)
① 用户和系统
申请证书
② CA签发证书
④ 应用和系统使用证书
LDAP
通信方
(证书主体)
使用证书的
应用和系统

访问控制

- **访问控制概念**

  - 机密性服务和完整性服务都需要实施访问控制。
  - 访问控制是确定来访实体有否访问权以及实施访问权限的过程。
  - 被访问的数据，如文件、数据报文、分组数据包、数据帧等，统称客体。能访问或使用客体的活动实体称做主体，如用户以及作为用户代理的进程、作业或任务等。
  - 访问控制一般都是基于安全政策和安全模型的。Lampson提出的访问矩阵(Access Matrix)是表示安全政策的最常用的访问控制安全模型。为节省存储空间，实际系统通常并不直接采用矩阵，而是采用访问控制表或者权利表进行表示，也称访问控制表(Access Control List， ACL)。

访问控制

- **访问控制分类**
  - 根据能够控制的访问对象粒度可以将访问控制分为粗粒度(Coarse Grained)访问控制、中粒度(Medium Grained)访问控制和细粒度(Fine Grained)访问控制。
  - 这里并没有严格定义的区分标准，但是人们通常认为能够控制到文件甚至记录对象的访问控制可以称为细粒度访问控制，而只能控制到主机对象的访问控制称为粗粒度访问控制。

网络安全概述——

网络安全评估

安全评估准则

1. 可信计算机系统评估准则（TCSEC）
2. 信息技术安全评估准则（ITSEC）
3. 信息安全技术通用评估准则（CC）
4. 我国信息安全评估准则

安全评估准则

- 可信计算机系统评估准则（TCSEC）

  - TCSEC(Trusted Computer System Evaluation Criteria)是由美国国家计算机安全中心(NCSC)于1983年制定的计算机系统安全等级划分的基本准则，又称橘皮书。

  - 提供一种标准，使用户可以对其计算机系统内敏感信息安全操作的可信程度做评估。给计算机行业的制造商提供一种可循的指导规则；使其产品能够更好地满足敏感应用的安全需求。

  - TCSEC共分为4类7级：D、C1、C2、B1、B2、B3、A1。

安全评估准则

- 可信计算机系统评估准则（TCSEC）
  - D级，无保护级
  - C1级，自主安全保护级
  - C2级，受控存取保护级
  - B1级，标记安全保护级
  - B2级，结构化保护级
  - B3级，安全域级
  - A级，验证设计级

安全评估准则

- 信息技术安全评估准则（ITSEC）

  - ITSEC（Information Technology Security Evaluation Criteria）由英、法、德、荷等四国于1989年联合提出，俗称白皮书。

  - 针对TCSEC准则的局限性，首次提出了信息安全的保密性、完整性、可用性等概念，把可信计算机的概念提高到可信信息技术的概念。

  - ITSEC定义了从E0级（没有任何保证）到E6级（形式化验证）的七个安全等级。

  - 目前，ITSEC已大部分被CC替代。

安全评估准则

- 信息安全技术通用评估准则（CC）
  - CC（Common Criteria for Information Technology Security Evaluation）由美国国家标准技术研究所（NIST）、国家安全局（NSA），欧洲的荷、法、德、英以及加拿大等6国7方于1995年联合正式提出。
  - 可提供结果的可重复性和客观性，用来评估信息系统或产品的安全性，主要用户包括消费者、开发者和评估者。

安全评估准则

- 信息安全技术通用评估准则（CC）

CC包括三个部分:

- 简介和一般模型：正文介绍了CC中的有关术语、基本概念和一般模型以及与评估有关的一些框架，附录部分主要介绍保护轮廓（PP）和安全目标（ST）的基本内容。
- 安全功能要求：按“类-族-组件”的方式提出安全功能要求，提供了表示评估对象TOE安全功能要求的标准方法。
- 安全保证要求：定义了评估保证级别，建立了一系列安全保证组建作为表示TOE保证要求的标准方法。
- CC的三个部分相互依存，缺一不可。

安全评估准则

- 信息安全技术通用评估准则（CC）

在CC中定义了7个递增的评估保证级（Evaluation Assurance Levels：EALs）：

  - EAL1：功能测试
  - EAL2：结构测试
  - EAL3：系统测试和检查
  - EAL4：系统设计、测试和复查
  - EAL5：半形式化设计和测试
  - EAL6：半形式化验证的设计和测试
  - EAL7：形式化验证的设计和测试

安全评估准则

- 我国信息安全评估准则

  - 公安部提出并组织制定了强制性国家标准GB-17859：1999《计算机信息安全保护等级划分准则》，该准则于1999年9月13日经国家质量技术监督局发布，并于2001年1月1日起实施。

  - 《准则》是计算机信息系统安全等级保护系列标准的核心，制定《准则》是实行计算机信息系统安全等级保护制度建设的重要基础。

  - 《准则》规定了计算机信息系统安全保护能力的5个等级。

安全评估准则

- 我国信息安全评估准则
  - 第一级：用户自主保护级
  - 第二级：系统审计保护级
  - 第三级：安全标记保护级
  - 第四级：结构化保护级
  - 第五级：访问验证保护级

网络安全评估方式

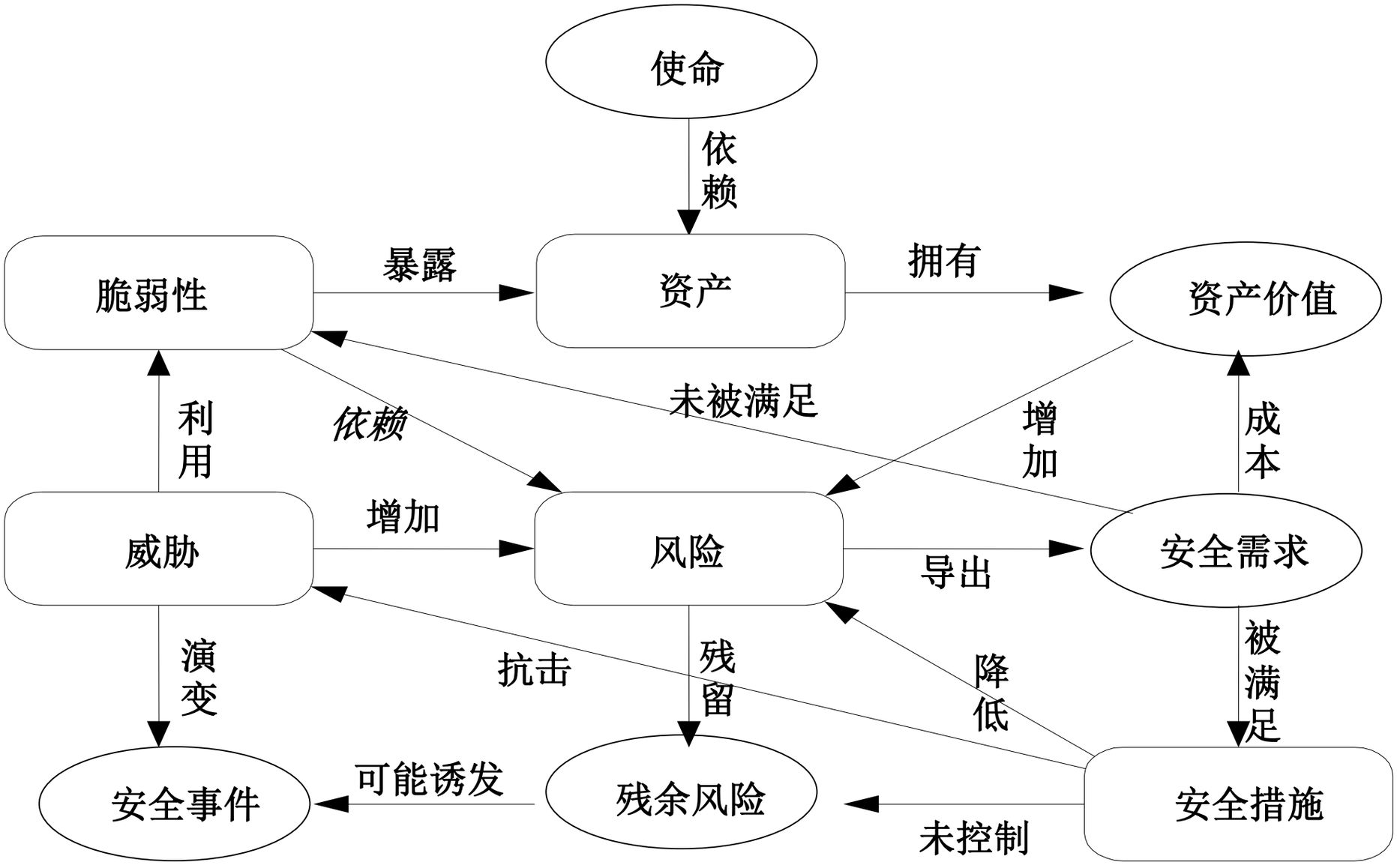
1. 风险评估
2. 生存性评估
3. 网络安全态势评估
4. 网络攻击效果评估
5. 安全测评
6. 信息安全工程能力 评估
7. 信息系统审计

风险评估

风险评估(Risk Assessment)，就是从风险管理的角度，运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的防御威胁的防护对策和整改措施，以防范和化解信息安全风险，或者将风险控制在可接受的水平，从而最大限度地保障网络和信息安全。

风险评估

- 风险各要素及其相互间关系



风险评估常用方法

- （1）基于知识的分析方法

  - 基于知识的分析方法又称作经验方法，它牵涉到对来自类似组织（包括规模、商务目标和市场等）的“最佳惯例”的重用，适合一般性的信息安全社团。

  - 采用基于知识的分析方法，只要通过多种途径采集相关信息，识别组织的风险所在和当前的安全措施，与特定的标准或最佳惯例进行比较，从中找出不符合的地方，并按照标准或最佳惯例的推荐选择安全措施，最终达到消减和控制风险的目的。

  - 可以采用一些辅助性的自动化工具，市场上可选的此类工具有多种，Cobra 就是典型的一种。

风险评估常用方法

- （2）基于模型的分析方法

  - 2001 年1 月，由希腊、德国、英国、挪威等国的多家商业公司和研究机构共同组织开发了一个名为CORAS 的项目，即Platform for Risk Analysis of Security Critical Systems。该项目的目的是开发一个基于面向对象建模特别是UML 技术的风险评估框架，它的评估对象是对安全要求很高的一般性的系统，特别是IT 系统的安全。

  - CORAS 考虑到技术、人员以及所有与组织安全相关的方面，通过CORAS 风险评估，组织可以定义、获取并维护IT 系统的保密性、完整性、可用性、抗抵赖性、可追溯性、真实性和可靠性。

风险评估常用方法

- （3）定量分析

  - 定量分析方法的思想很明确：对构成风险的各个要素和潜在损失的水平赋予数值或货币金额，当度量风险的所有要素（资产价值、威胁频率、弱点利用程度、安全措施的效率和成本等）都被赋值，风险评估的整个过程和结果就都可以被量化了。

  - 对定量分析来说，有两个指标是最为关键：

    - 事件发生的可能性；
    - 威胁事件可能引起的损失。

风险评估常用方法

- （4）定性分析
  - 定性分析方法是目前采用最为广泛的一种方法，它带有很强的主观性，往往需要凭借分析者的经验和直觉，或者业界的标准和惯例，为风险管理诸要素（资产价值，威胁的可能性，弱点被利用的容易度，现有控制措施的效力等）的大小或高低程度定性分级，例如“高”、“中”、“低”三级。
  - 定性分析操作起来相对容易，但也可能因为操作者经验和直觉的偏差而使分析结果失准。

风险评估常用方法

- 定性分析与定量分析方法比较：
  - 定性分析的准确性稍好但精确性不够，定量分析则相反；
  - 定性分析没有定量分析那样繁多的计算负担，但却要求分析者具备一定的经验和能力；
  - 定量分析依赖大量的统计数据，而定性分析没有这方面的要求；
  - 定性分析较为主观，定量分析基于客观；
  - 定量分析的结果很直观，容易理解，而定性分析的结果则很难有统一的解释。

风险评估工具

- （1）调查问卷
  - 风险评估者通过问卷形式对组织信息安全的各个方面进行调查， 问卷解答可以进行手工分析，也可以输入自动化评估工具进行分析。
  - 从问卷调查中，评估者能够了解到组织的关键业务、关键资产、主要威胁、管理上的缺陷、采用的控制措施和安全策略的执行情况

风险评估工具

- （2）检查列表
  - 检查列表通常是基于特定标准或基线建立的， 对特定系统进行审查的项目条款，通过检查列表，操作者可以快速定位系统目前的安全状况与基线要求之间的差距。
- （3）人员访谈
  - 风险评估者通过与组织内关键人员的访谈， 可以了解到组织的安全意识、业务操作、管理程序等重要信息。

风险评估工具

- （4）漏洞扫描器
  - 漏洞扫描器（包括基于网络探测和基于主机审计）可以对信息系统中存在的技术性漏洞（弱点）进行评估。许多扫描器都会列出已发现漏洞的严重性和被利用的容易程度。典型工具有 Nessus、ISS、CyberCop Scanner等。
- （5）渗透测试
  - 一种模拟黑客行为的漏洞探测活动， 它不但要扫描目标系统的漏洞，还会通过漏洞利用来验证此种威胁场景。

风险评估工具

- （6）目前常见的自动化风险评估工具

  - COBRA（Consultative, Objective and Bi-functional Risk Analysis）：英国的 C&A系统安全公司推出的一套风险分析工具软件，它通过问卷的方式来采集和分析数据，并对组织的风险进行定性分析，最终的评估报告中包含已识别风险的水平和推荐措施。

  - CRAMM（CCTA Risk Analysis and Management Method）：英国政府的中央计算机与电信局于1985年开发的一种定量风险分析工具，同时支持定性分析。可以评估信息系统风险并确定恰当对策，适用于各种类型的信息系统和网络，也可以在信息系统生命周期的各个阶段使用。

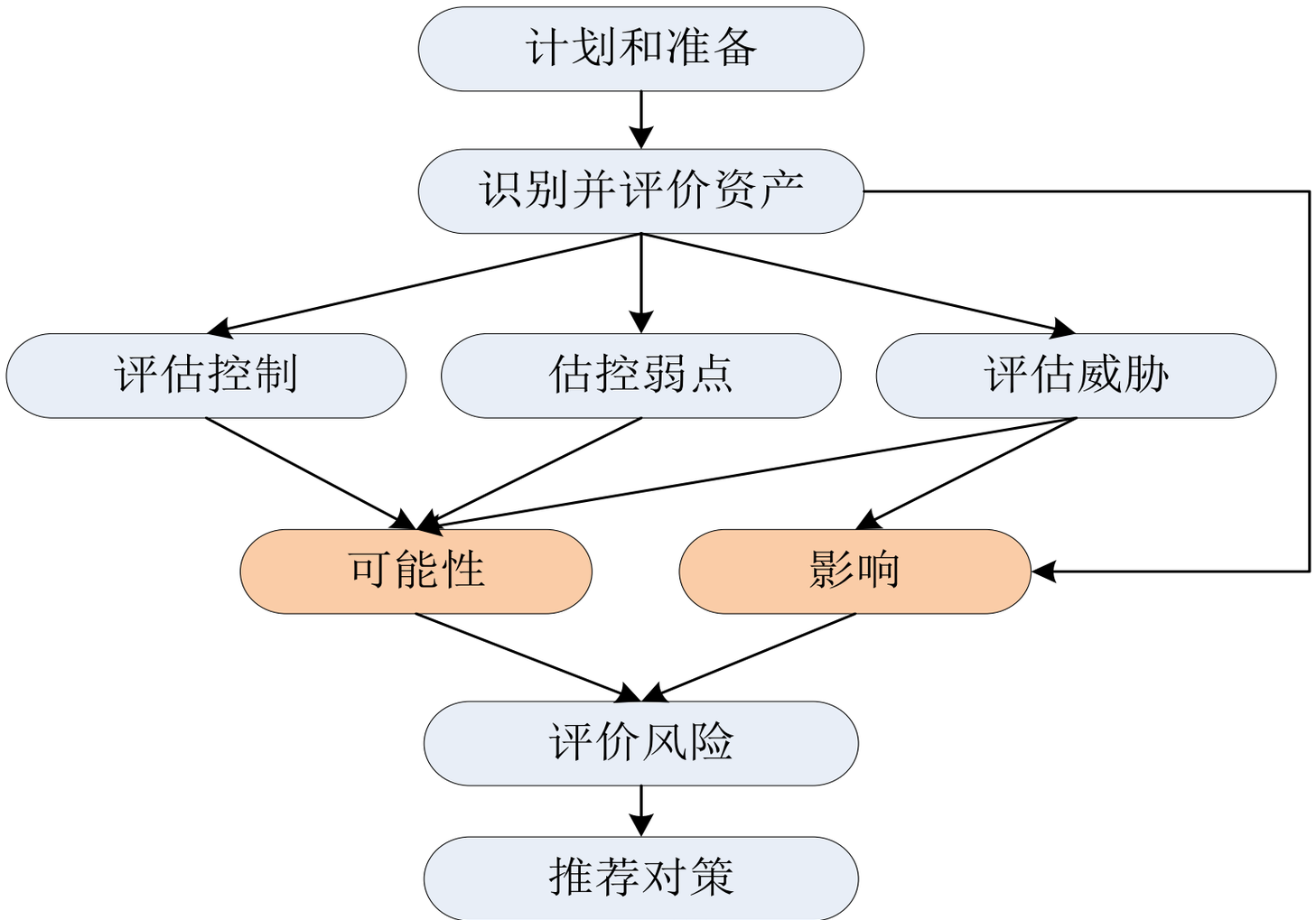
风险评估工具

- ASSET（Automated Security Self-Evaluation Tool）：美国国家标准技术协会发布的一个可用来进行安全风险自我评估的自动化工具，它采用典型的基于知识的分析方法，利用问卷方式来评估系统安全现状与 NIST SP 800-26 指南之间的差距。

- CORA（Cost-of-Risk Analysis）：国际安全技术公司开发的一种风险管理决策支持系统，它采用典型的定量分析方法，可以方便地采集、组织、分析并存储风险数据，为组织的风险管理决策支持提供准确的依据。

风险评估基本过程

- 风险评估是组织确定信息安全需求的过程，包括资产识别与评价、威胁和弱点评估、控制措施评估、风险认定在内的一系列活动。



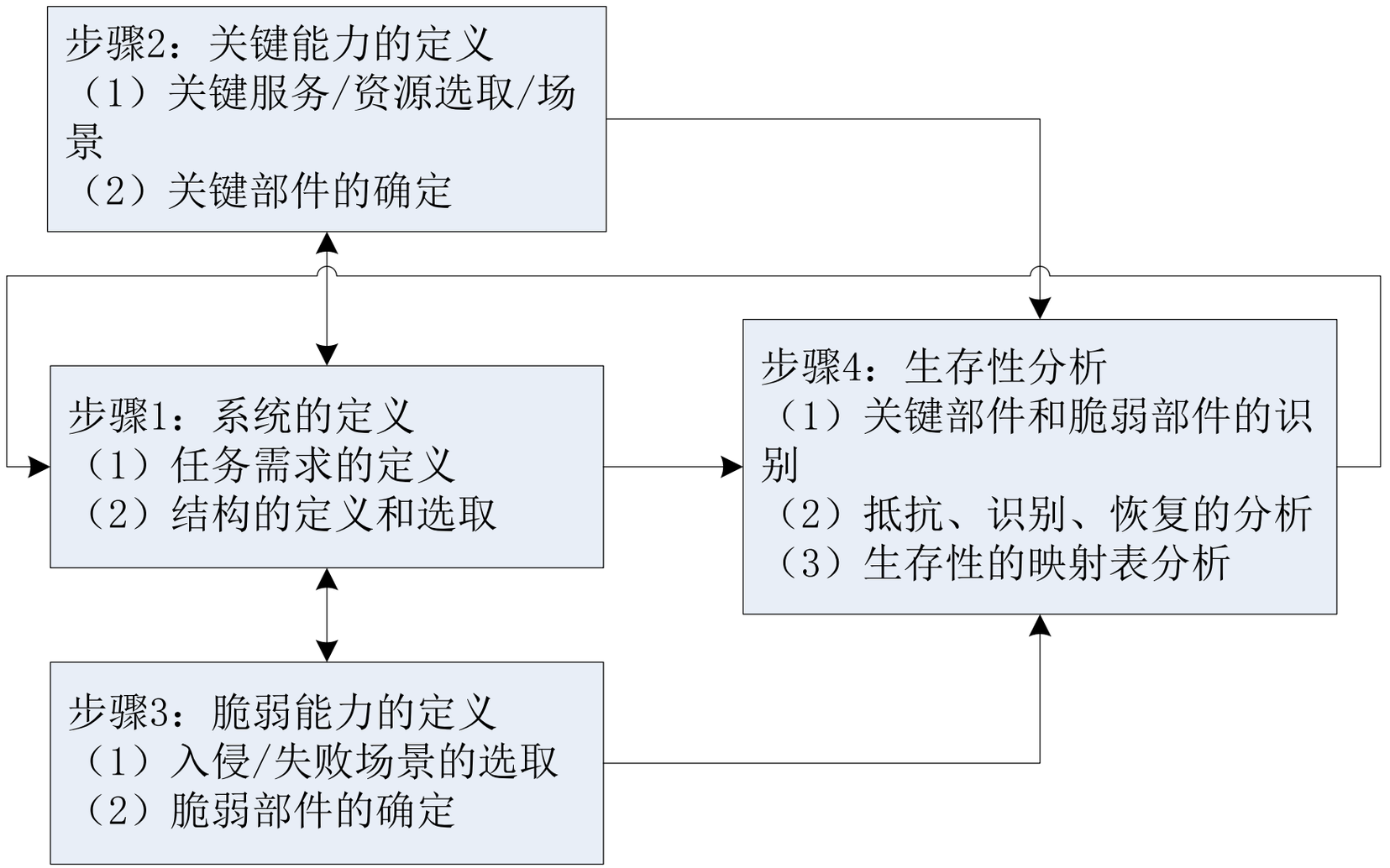
生存性评估

生存性评估(Survivability Assessment)，是从生存能力角度评价信息系统的安全性。所谓生存性，是指系统在遭受攻击、发生故障或出现意外事故的情况下仍然能及时完成任务的能力。

生存性评估，主要衡量网络或信息系统的抗攻击性(Resistance)、可识别性(Recognition)和可恢复性(Recovery)。

生存性评估典型方法

- 卡耐基梅隆大学SEI研究中心提出的SNA(Survivable Network Analysis)分析方法是一种主要的定性分析方法。

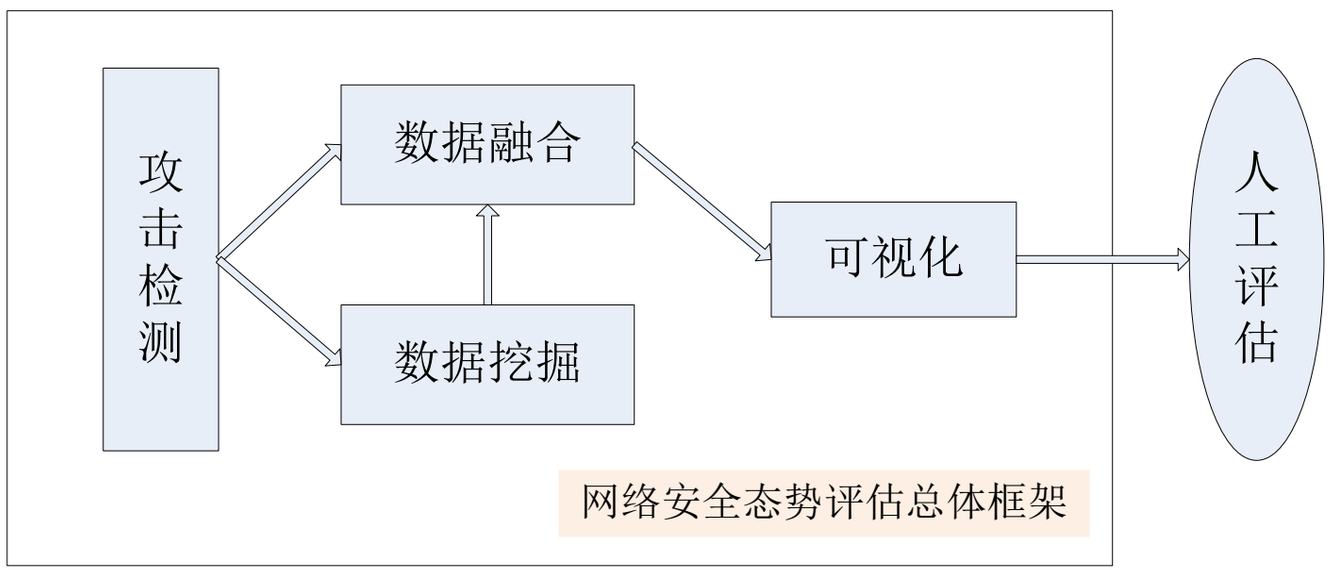


网络安全态势评估

安全态势评估(Security Situation Assessment)，是从检测数据的角度评估当前网络信息系统面临的安全威胁状况。

态势评估的数据源，多是入侵检测等动态检测系统的报警信息，以及系统或网络运行时的性能数据，通过将这些数据进行融合，分析当前系统或网络面临的安全威胁状况和发展趋势。

网络安全态势评估总体框架



- 攻击检测，是指传统入侵检测，也包括漏洞扫描和系统、应用系统日志审计等，它们向上级模块提供攻击数据。
- 数据融合，是指利用入侵检测得到的攻击信息来进行数据融合进而获得安全态势知识的过程。
- 数据挖掘，是指在数据融合所得到的安全态势知识中发现新的未知模式的过程。
- 可视化，是指使用可视化工具将态势信息从抽象的数字形式转换为人们易于接受和理解的图表形式。

网络攻击效果评估

网络攻击效果评估(Network Attack Effect Assessment)，主要从攻击效果角度评估信息系统的安全性和网络攻击的能力，是信息安全评估领域一个年轻而有挑战的分支。

该技术通过对典型网络攻击样式的原理剖析，深入分析网络攻击的典型效果，建立攻击效果评估模型和实现系统，对计算机网络攻击的效果进行定性和定量的评估。

安全测评

安全测评，是从安全技术、功能和机制角度来进行信息系统的安全评估，通过选择公认的信息技术产品或信息系统的安全认证标准，如美国的TCSEC、ISO/IEC 15408(CC)、我国的GB17859-1999等，给出信息系统的安全性认证等级。

系统安全工程能力评估

系统安全工程能力成熟度模型 (System Security Engineering Capability Maturity Model，简称SSE-CMM)，将信息安全看成一项系统工程，通过系统生命周期内一系列过程来保证安全，并从低到高定义了6个能力成熟级别，来评价组织机构的系统安全工程能力。

信息系统审计

信息系统审计，又称IT审计(IT Audit)，通常根据公认的标准或指导规范实施与否及其实施程度，来评估信息系统和相关资源的安全性、有效性、效率、完整性等。例如CobiT标准中提供了许多IT过程的审计模块和方法，也可利用ISO/IEC 17799审计信息安全管理体系，通过ITIL对IT服务管理进行审计。

评估方式比较

安全评估方式	评估对象	衡量指标	主要评估方法
风险评估	信息系统的安全性	风险（发生的可能性发生后可能产生的影响）	按照“资产/威胁/弱点”模型，对风险进行定性或定量分析
生存性评估	信息系统的生存性	抗攻击性、可识别性可恢复性	区分系统的必要服务和次要服务，结合入侵情景，分析信息系统的生存性
安全态势评估	运行中的信息系统的安全性	安全威胁状况和发展趋势	利用报警信息和性能数据，进行数据融合，分析当前的威胁状况和发展趋势
网络攻击效果评估	遭受攻击的信息系统的安全损失	攻击效果	通过采集攻击前后目标网络环境和攻击机器的数据，对攻击效果进行评估
安全测评	信息产品的安全性认证等级	安全技术、功能和机制等	在信息技术产品或系统的标准指标下，得出信息系统的安全性认证级别
系统安全工程能力成熟度模型	组织的系统安全工程能力	系统工程	采用能力成熟度模型CMM来评价一个组织整体上的系统安全工程能力成熟性
信息系统审计	信息系统的安全性、有效性、效率等	审计	根据公认的标准或最佳惯例实施与否及其程度，对信息系统进行评估

网络安全概述——

网络安全标准

网络安全标准化组织

- (1) ISO:国际标准化组织(International Organization for Standardization)
  - 国际标准化组织始建于1946年，是世界上最大的非政府性标准化专门机构，它在国际标准化中占主导地位。ISO的主要活动是制定国际标准，协调世界范围内的标准化工作，组织各成员国和技术委员会进行交流，以及与其他国际性组织进行合作，共同研究有 关标准问题。
  - ISO的目的和宗旨是:在世界范围内促进标准化工作的发展，以利于国际物资交流和 互助，并扩大在知识、科学、技术和经济方面的合作。

网络安全标准化组织

- (2) IEC:国际电工委员会(International Electro-technical Commission)

  - IEC是世界上成立最早的非政府性国际电工标准化机构，是联合国经社理事会 (ECOSOC)的甲级咨询组织。目前，IEC成员国包括了大多数工业发达国家及一部分发 展中国家。这些国家的人口占世界人口的80%，其生产和消耗的电能占全世界的95%， 制造和使用电气、电子产品占全世界产量的90%。

  - 1EC的宗旨:促进电工标准的国际统一，促进电气、电子工程领域中标准化及有关方 面的国际合作，增进国际间的相互了解。

网络安全标准化组织

- (3) ITU:国际电信联盟(International Telecommunication Union)
  - 国际电信联盟于1865年5月在巴黎成立，1947年成为联合国的专门机构。ITU是世界各国政府的电信主管部门之间协调电信事务的一个国际组织，它研究制定有关电信 业务的规章制度，通过决议提出推荐标准，收集有关情报。
  - ITU的目的和任务:维持和发展国际合作，以改进和合理利用电信，促进技术设施的 发展及其有效运用，以提高电信业务的效率，扩大技术设施的用途，并尽可能使之得到广 泛应用，协调各国的活动。

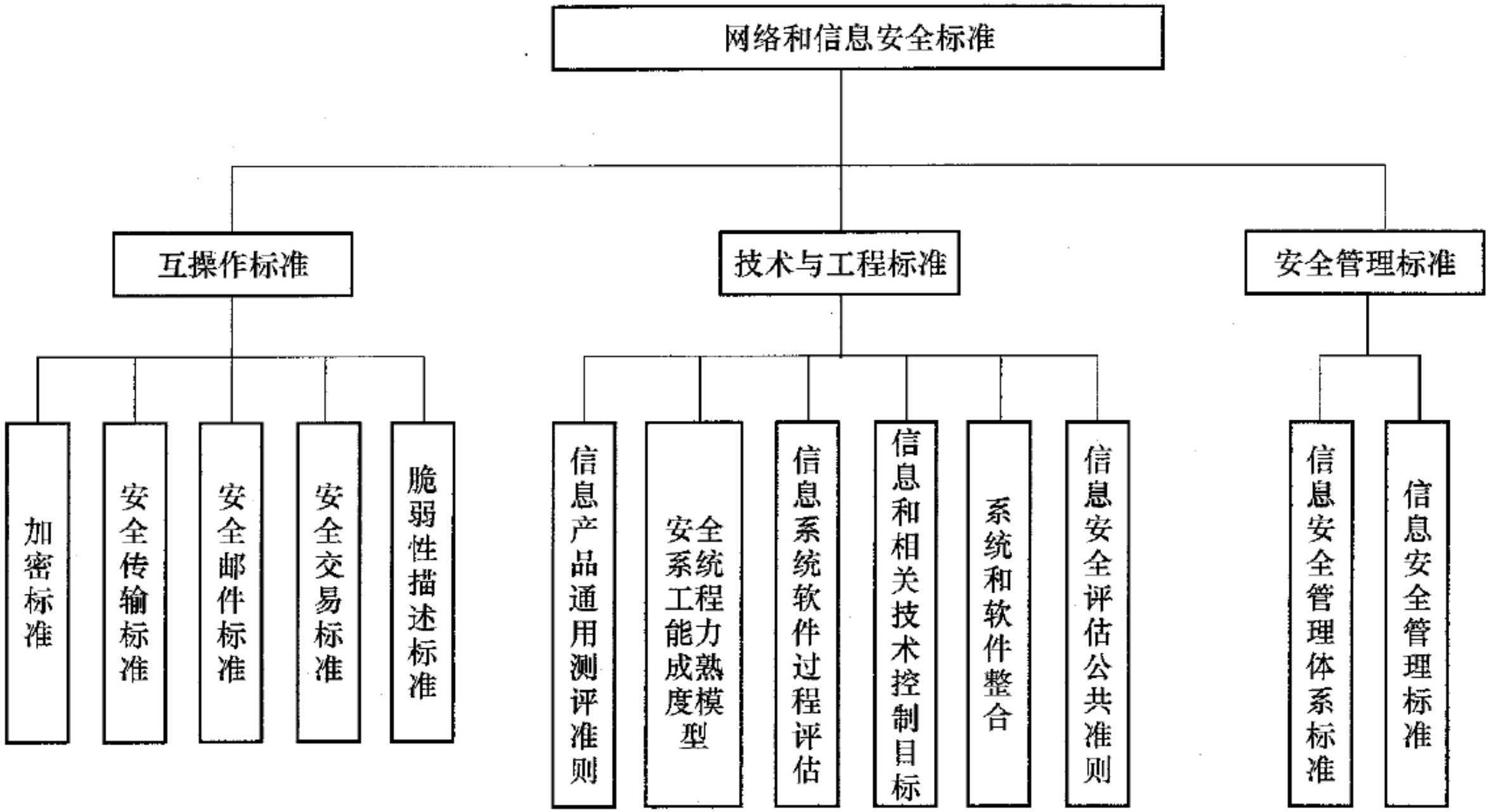
网络安全标准化组织

- (4) IETF

  - 互联网工程任务组(IETF， The Internet Engineering Task Force)，成立于1985年 底，其主要任务是负责互联网相关技术规范的研发和制定。

  - 目前，IETF已成为全球互联网界最具权威的大型技术研究组织。IETF的自身定位是一个互联网技术研发的跨国民间组织。虽然已有很多互联网技术规范通过在IETF讨论成为了公认标准，但它仍有别于像国际电联这样传统意义上的标准制定组织。

网络安全标准分类


网络和信息安全标准
互操作标准
技术与工程标准
安全管理标准
加密标准
安全传输标准
安全邮件标准
安全交易标准
脆弱性描述标准
信息产品通用测评准则
全统程力熟模
安系工能成度型
信息系统软件过程评估
信息和相关技术控制目标
系统和软件整合
信息安全评估公共准则
信息安全管理体系标准
信息安全管理标准

网络安全标准分类

- 1.互操作标准
  - 互操作标准包括：加密标准，如对称加密标准DES，3DES、IDEA以及被普遍看好的AES;非对称加密标准(RSA）;安全传输标准，如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)等。
  - 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"。

网络安全标准分类

- 2.技术与工程标准

  - 信息产品通用测评准则(ISO 15408)：支持产品中IT安全特征的技术性评估、描述用户对安全性的技术需求

  - 安全系统工程能力成熟度模型(SSE-CMM)：定义安全工程过程应有特征

  - 信息系统软件过程评估(ISO/IEC 15504)：提供软件过程评估的框架

  - 信息和相关技术控制目标(COBIT)：是安全与信息技术管理和控管的标准

  - 系统与软件整合层次(ISO 15026)：定义一个基于风险分析的软件整合层次流程，同时也定义整合层次必须将软件的风险值限制在一定范围内

  - 信息安全评估公共准则(ISO/IEC 15408-1999)：CC的目的是允许用户指定他们的安全需求，允许开发者指定他们产品的安全属性，并且允许评估者决定是否产品确实符合他们的要求

网络安全标准分类

- 3.网络与信息安全管理标准

  - (1)信息安全管理体系标准(BS 7799，其中第一部分成为ISO/IEC 17799) :BS 7799 提供一个开发组织安全标准、有效安全管理实施的公共基础，还提供了组织间交易的可信 度。

  - (2)信息安全管理标准(ISO 13335) : 《IT安全管理方针》系列(第一至第五部分)，已经在国际社会中开发了很多年。5个部分组成分别如下:

    - ISO/IECI3335-1: 1996《IT安全的概念与模型》
    - ISO/IECI3335-2: 1997《IT安全管理和计划制定》
    - ISO/IECI3335-3: 1998《IT安全管理技术》
    - ISO/IECI3335-4: 2000《安全措施的选择》
    - ISO/IEC13335-5《网络安全管理方针》

问题和讨论