

第1讲 信息安全概述



目 录



- 1.1 前言
- 1.2 信息安全的概念
- 1.3 信息安全的内容
- 1.4 信息安全的目标



前言

- u 随着互联网的飞速发展，信息作为一种无形的资源，被广泛应用于政治、军事、经济、科研等各行各业，其重要性与日俱增
- u 随之而来的安全性问题也越来越多
- u 据联邦调查局统计，美国每年因网络安全造成的损失高达75亿美元
- u 据美国金融时报报道，每20秒就发生一次计算机安全事件，1/3的防火墙被突破
- u 美国联邦调查局计算机犯罪组负责人称：给我精选10名“黑客”，90天内，我将使美国趴下



前言

- U 1988年11月2日，美国康奈尔大学的学生罗伯特·莫里斯释放多个蠕虫病毒，造成因特网上近6 000台主机瘫痪，据称损失高达几千万美元
- U 1989年3月2日凌晨，3名德国黑客因涉嫌向前苏联出售机密情报被捕，他们在两年多的时间内，闯入了许多北约和美国的计算机系统，窃取了许多高度机密的信息。
- U 1996年9月，美国中央情报局的主页被一群远在瑞典的少年黑客改为中央笨蛋局（Central Stupidity Agency）



前言

- u 2000年10月，黑客入侵微软公司并获取微软新开发产品的机密源代码，震动了微软公司高层。有的媒体冠以“黑客太黑，微软太软”的大标题，讽刺微软这样的著名公司都无法挡住黑客凶猛的攻击
- u 在海湾战争中，美国特工将伊拉克从德国进口的一批计算机打印设备中换上含有可控“计算机病毒”的芯片，导致伊拉克的计算机系统在战争初期就陷入全面瘫痪
- u 美国已生产出第一代采用“病毒固化”技术的芯片，并开始嵌入出口的计算机产品中。一旦需要，便可遥控激活



信息安全事件

Ø 各类银行卡已经为越来越多的人所接受。可银行卡的安全漏洞却是一个极大的隐患，美国这样金融系统高度发达的国家，动辄几千万人的卡资料外泄，让消费者心惊胆战。

Ø 2007年，美国有史以来最大客户资料劫案

ü 美国零售业巨头TJX公司4570万张信用卡和借记卡资料遭黑客窃取，成为美国迄今最严重的一次金融信息安全事件。



TJX公司事件

u 2006年12月，TJX公司向执法机关举报说，4500多万名客户的个人资料被黑客盗走

u 公司及调查人员没有公布事件细节。据已透露的细节得知黑客可能的手段：

Ø 店内电脑看管不严

ü 很多TJX零售店内的电脑没有防火墙的保护，可以直接连上公司网络。黑客用USB盘把黑客软件装到电脑上，TJX公司承认在电脑系统中发现了“可疑软件”。盗贼们可以控制这些电脑，把它们变成连接到TJX公司网络的远程终端



TJX公司事件

u 黑客可能的手段:

Ø 无线接入

ü 黑客们开着车在店铺林立的商业区逡巡，车里有一台笔记本电脑、一个望远镜天线和一个802.11的无线网卡。TJX公司也许并不是他们的头号目标，但他们发现居然可以连接上TJX公司的内部网，而且还能利用得到的信息进一步深入TJX公司的IT系统

Ø 密码输入器

ü 盗贼们进入一家商店，其中一个人吸引收银员的注意力，其他人乘机偷偷将收银台上的密码输入器换成事先改装好的同样设备，这个动作只需要12秒就能完成。几天后，盗贼们回到商店，将原来的密码输入器换回去，就能获得改装设备上存储的账户信息了



TJX公司事件

- u 2007年3月，一些被盗数据出现在佛罗里达州。盗贼们用被盗的TJX公司的客户信息伪造信用卡，然后在佛罗里达州50个县的沃尔玛超市疯狂消费，诈骗了大约800万美元的购物卡。
- u 2007年7月，美国特勤局宣布，另一起南佛罗里达州的诈骗团伙案也使用了被盗的TJX公司的客户信息。



TJX公司事件

- U 黑客直接攻破了TJX的加密软件，“等于拿到了大门钥匙进去偷东西”。
- U 发生如此严重的信息安全事故，说明很多保管有消费者数据的公司，尤其是那些客户群庞大的零售巨头，信息安全系统漏洞百出。
- U 公司老总们总结出**最重要的教训**是：“找到你的公司或机构中的薄弱环节，如果你自己不发现的话，别人会找到它们的”



信息安全事件

U 2006年下半年，信息安全公司赛门铁克（Symantec）发现大约有600万台电脑被“可疑软件”感染。赛门铁克说，现在俨然已经形成地下的“网络经济”，黑客们已经从单兵作战变为有组织的犯罪团体，窃取来的数据资料通过一条“地下网络链”进行交易。

Ø 比如：获取一个Skype帐号，大约12美元，就可以花别人的钱打免费的网络电话；获取一个里面仍存有余额的支付账号，要价10美元到500美元不等，可以用他人账号进行网络购物……

U 赛门铁克报告说：仅2006年下半年，他们就“监测”到有4943张信用卡资料被非法交易，由此导致的欺诈消费等损失可达数百万美元。

对经济、社会、政治
等影响日益加深



信息化与国家安全——经济

- u 一个国家信息化程度越高，整个国民经济和社会运行对信息资源和信息基础设施的依赖程度也越高。
- u 我国计算机犯罪的增长速度超过了传统的犯罪
 - Ø 97年20几起，98年142起，99年908起，2000年上半年1420起。
- u 利用计算机实施金融犯罪已经渗透到了我国金融行业的各项业务。
 - Ø 近几年已经破获和掌握100多起。涉及的金额几个亿。



黑客攻击事件造成经济损失



1999年4月26日，台湾人编制的CIH病毒的大爆发，有统计说我国大陆受其影响的PC机总量达36万台之多。有人估计在这次事件中，经济损失高达近12亿元。



信息化与国家安全——社会稳定

- U 互连网上散布一些虚假信息、有害信息对社会管理秩序造成的危害，要比现实社会中一个造谣要大的多。
- U 99年4月，河南商都热线一个BBS，一张说交通银行郑州支行行长协巨款外逃的帖子，造成了社会的动荡，三天十万人上街排队，挤提了十个亿。
- U 网上治安问题，民事问题，进行人身侮辱。



对社会的影响

u 针对社会公共信息基础设施的攻击严重扰乱了社会管理秩序

Ø 2001年2月8日正是春节，新浪网遭受攻击，电子邮件服务器瘫痪了18个小时。造成了几百万的用户无法正常的联络。

u 网上不良信息腐蚀人们灵魂



信息化与国家安全——信息战

U“谁掌握了信息，控制了网络，谁将拥有整个世界。”

（美国著名未来学家阿尔温 托尔勒）

U“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”

（美国前总统克林顿）

U“信息时代的出现，将从根本上改变战争的进行方式。”

（美国前陆军参谋长沙利文上将）



前言



事实说明，在信息时代，信息系统的安全性已经成为非常重要的研究课题。





1.2 信息安全的概念



1.2 信息安全的概念

- p “安全”一词的基本含义为：“远离危险的状态或特性”。
- p 信息安全——信息的存储、处理和传递过程中涉及的安全问题。
 - p 保护信息系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。
 - p 在商业和经济领域，信息安全主要强调的是消减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降低到最低程度。

§信息安全：在信息风险和控制之间保持平衡。 — Jim Anderson, Inovant (2002)





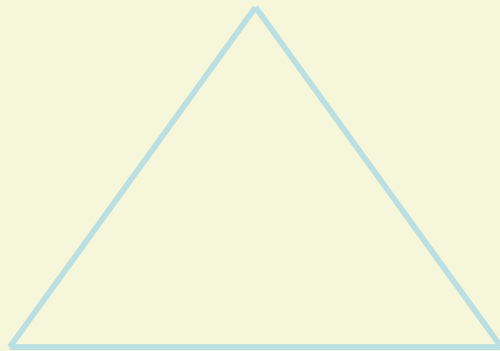
1.3 信息安全的内容



1.3 信息安全的内容

u 关于信息安全的两种主要论点

机密性
(Confidentiality)



完整性 (Integrity) 可用性 (Availability)

国外：信息安全金三角
面向属性的信息安全框架

信息安全的保护目标

内容安全

数据安全

运行安全

物理安全

国内：信息安全分层结构
面向应用的信息安全框架

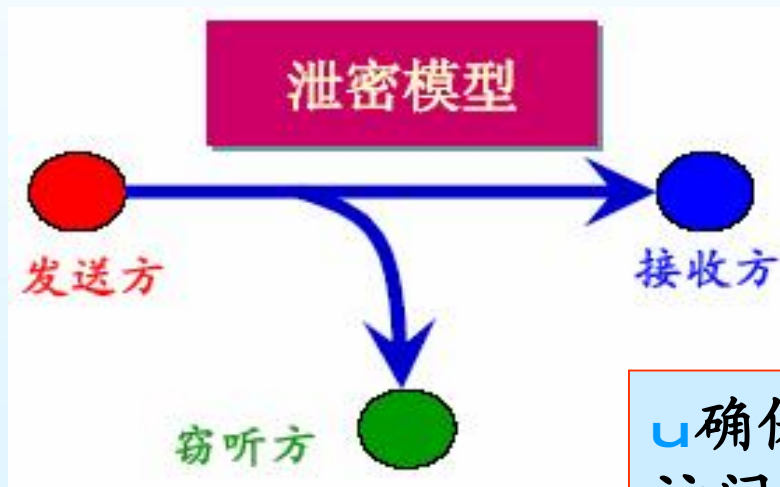


1.3 信息安全的内容

一、信息安全的重要属性:

——安全的信息交换应满足的性质:

1. 机密性 (Confidentiality)

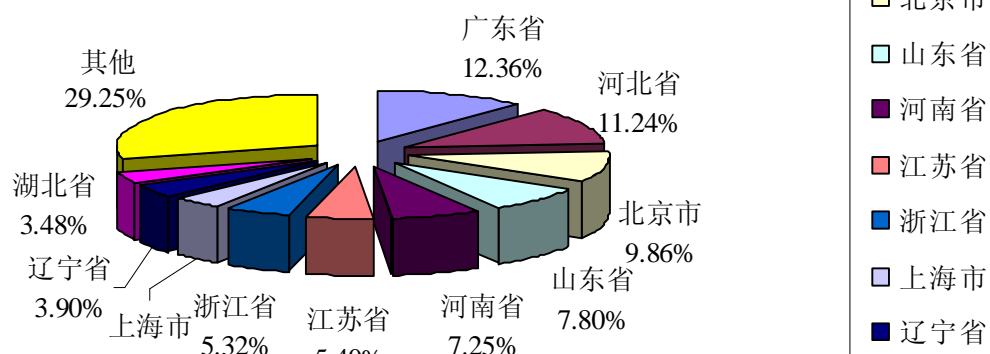


u 确保信息只能被授权访问方所接收的属性。

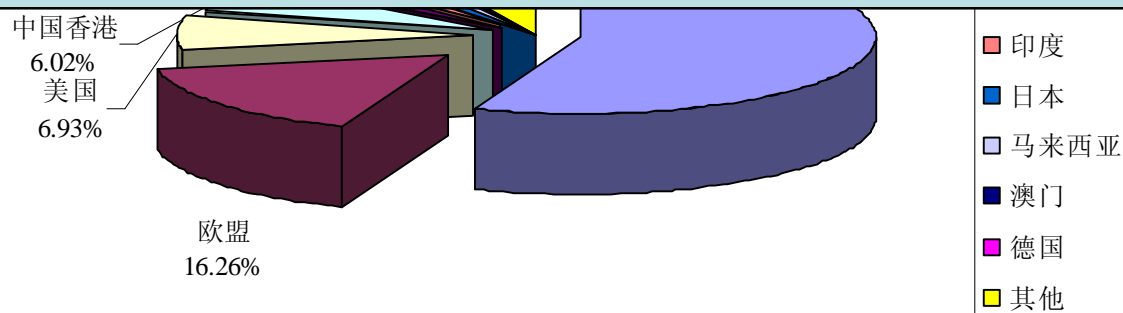
“加密”



被境外通过木马程序控制的中国大陆主机对应IP按地区分布
2008年7月



频繁发生的失窃密事件 严重危及国家安全



2006年02月27日0

日本海上自卫队出了最大泄密的新闻。共同社、《东京新闻》均在事件。

据日本媒体报道，负责机要通信的通信兵在用。但这名通信兵的个软件散布到了因特网上，被“解密”或“机密”字样的日本海上自卫队秘密文件。

专题推荐

美国2006年版《四年防务评估报告》对中国的关注有了明显的提升。

边海防，乃国家安危的第一道屏障；戍边人，是共和国大厦的第一道岗哨

新闻搜索

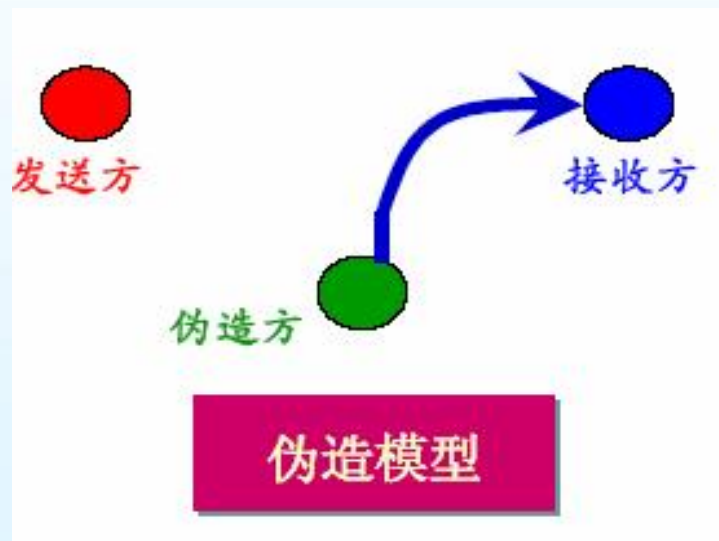
1.3 信息安全的内容

一、信息安全的重要属性:

——安全的信息交换应满足的性质:

2. 真实性 (Authenticity)

真实且能够被验证及信任的属性。

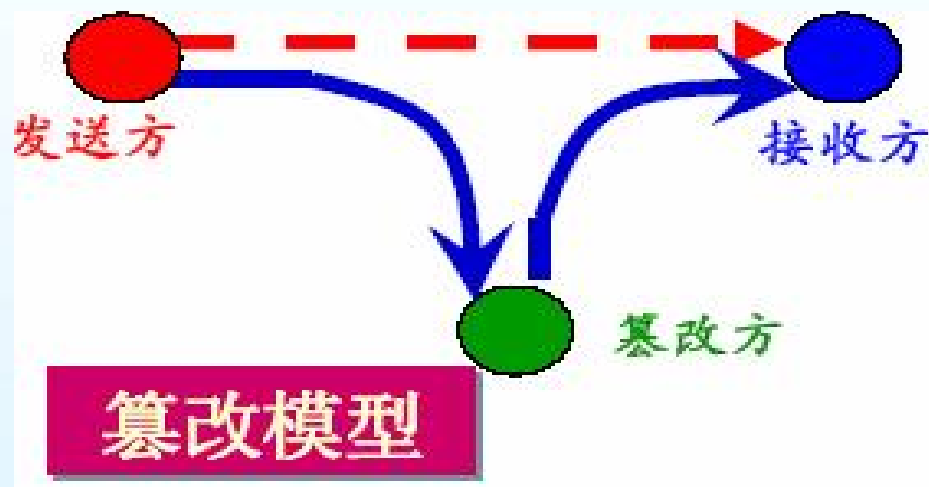


u “数字签名”

u “认证”



3. 完整性 (Integrity)



数据不被以非授权或意外的方式进行修改、破坏或丢失的属性。

“完整性检验”



完整性映射要点：HASH函数



HASH函数也称消息摘要（Message Digest）

☐ 其输入为一个可变长 x ，返回一固定长度串，该串 h 称为输入 x 的HASH值（消息摘要）。

☐ 特点：

☐ 输入 x 可以为任意长度，输出数据串长度固定。

☐ 给定任何 x ，能够计算出 $H(x)$ 。

☐ 单向函数，即给出一个HASH值 h ，很难反向计算出一个一特定输入 x ，使 $h=H(x)$ 。就是说，不可能从HASH值来获取原始消息，即使是原始消息的很少一部分信息都不可能获得。

☐ 任意两条消息 x 、 y ，使 $H(x)=H(y)$ 是计算不可行的，即符合唯一性原理。





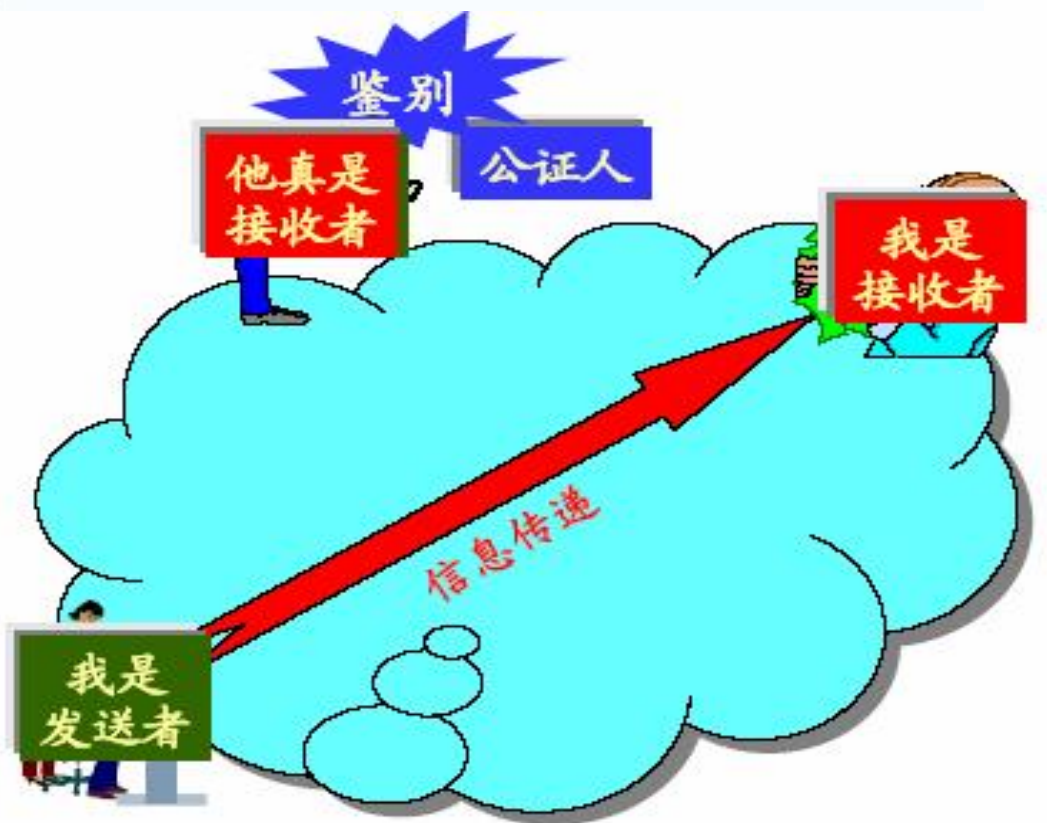
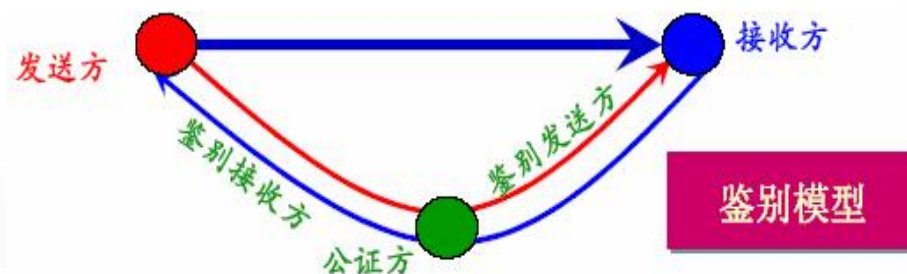
- u 山东大学王小云教授先后在国际上宣布她对摘要算法MD5、SHA-1等算法的攻击报告，引起了国际密码界的热烈反响。
- u MD5创始人，RSA算法的发明人之一罗纳德（Ronald L.Rivest）对她的评价是“高水平的世界级研究”，“当然，我并不希望看到MD5就这样倒下，但人必须尊重真理”。



1.3 信息安全的内容

信息安全的重要属性:

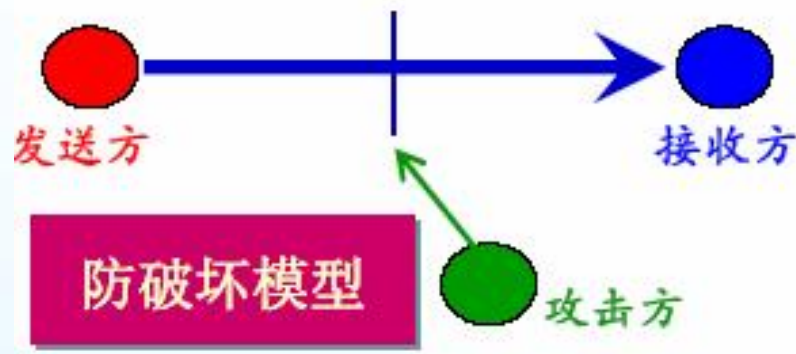
4. 可鉴别性 (authentication)



能够检验一个系统实体所声称的身份或为一个系统实体进行检验身份的属性。

” CA签发数字证书”

5.可用性 (Availability)



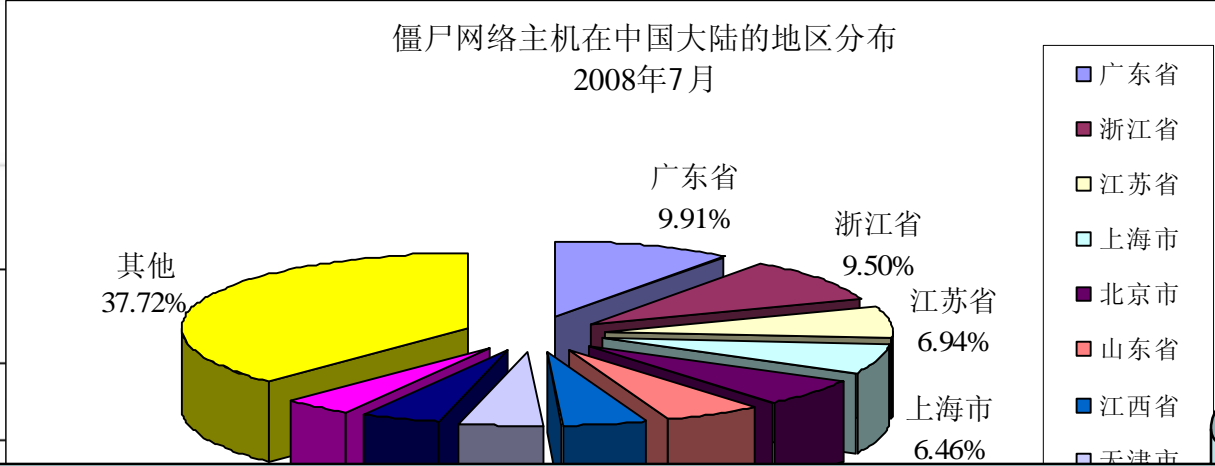
确保授权用户需要时能够访问信息及相关资源的属性。

“冗余系统——保障系统的可靠性”

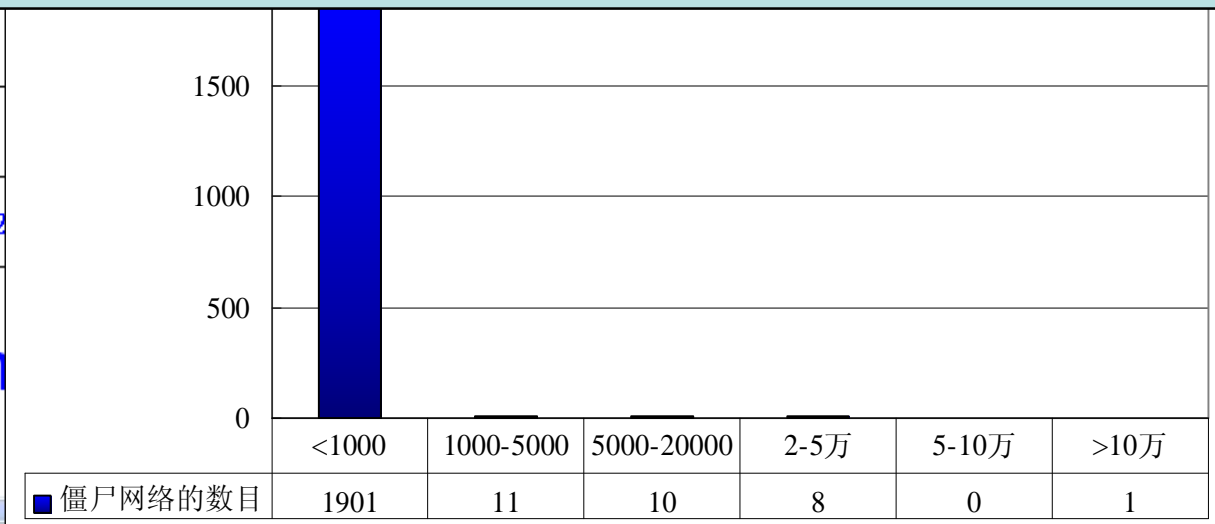
“灾备系统——保障系统的生存性”



- CIH (1998.6)
- 梅丽莎(Melissa)
- 我爱你(ILove)
- 红色代码(RedCode)
- SQL Slammer
- 冲击波(Blast)
- 霸王虫(Sobit)
- MyDoom(2004.1)
- Bagle (2004.1)
- 震荡波(Sasser) (2004.4)



层出不穷的大规模网络攻击事件 造成严重的经济损失

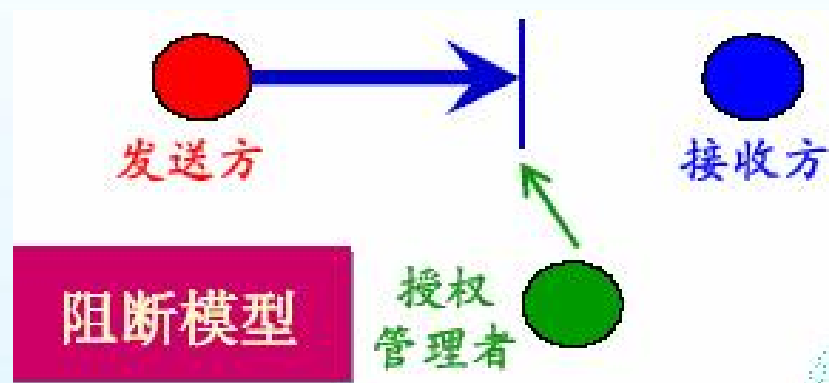
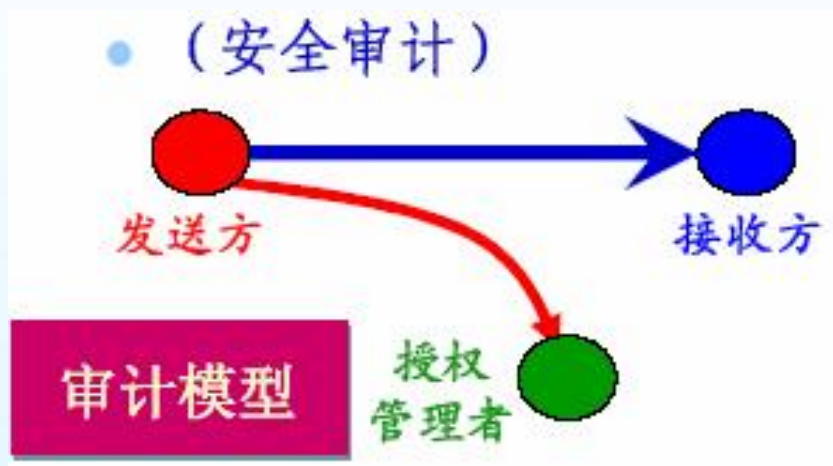


摘自《Inform

恶意代码

信息安全的重要属性:

6.可控性 (Controllability)



确保系统状态可被授权方所控制的属性。



安全审计：保证系统是可控的、可信的

u 建立系统日志、应用日志和安全日志，以记录用户的所有操作行为。

ü 网络环境下比较重要的日志：

(1) 连接时间日志

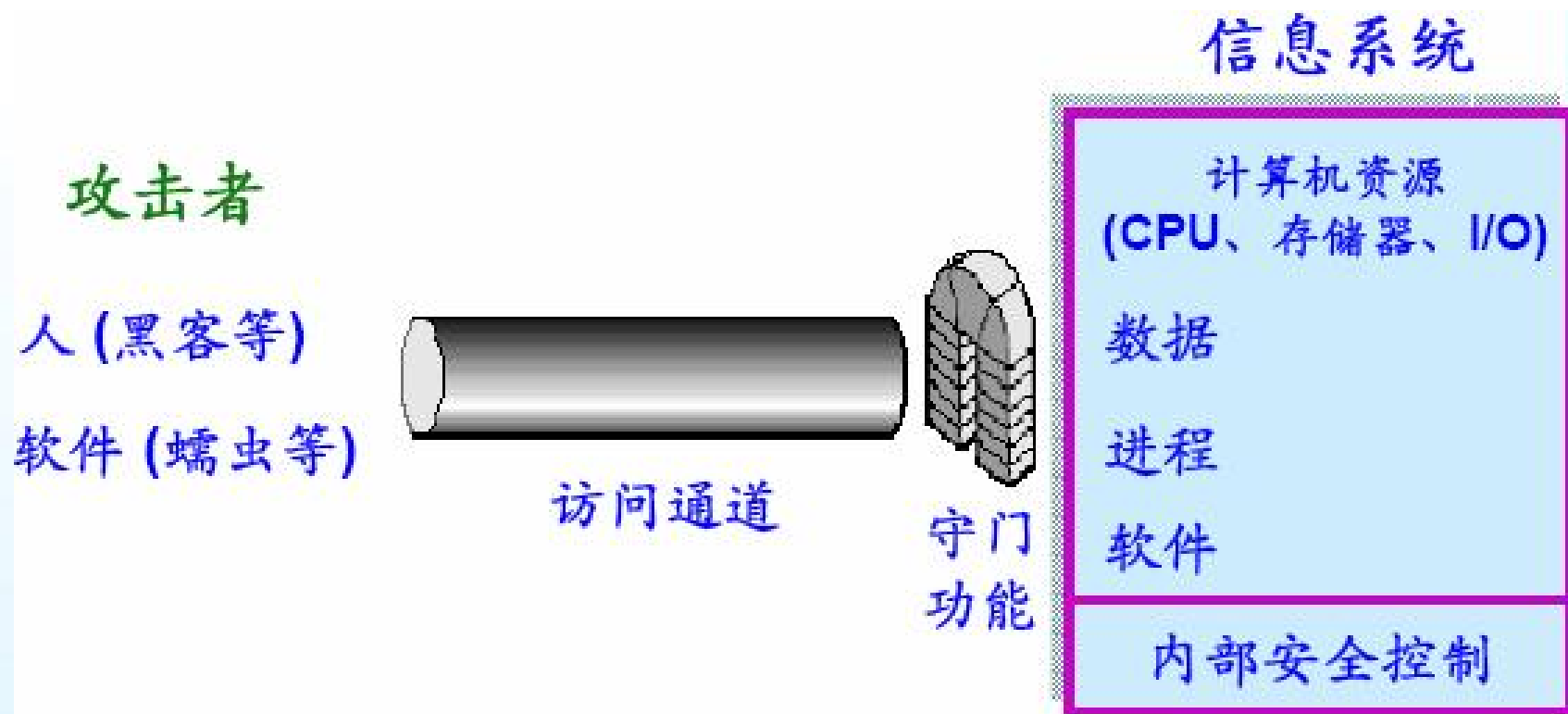
(2) 进程统计日志

(3) 错误日志



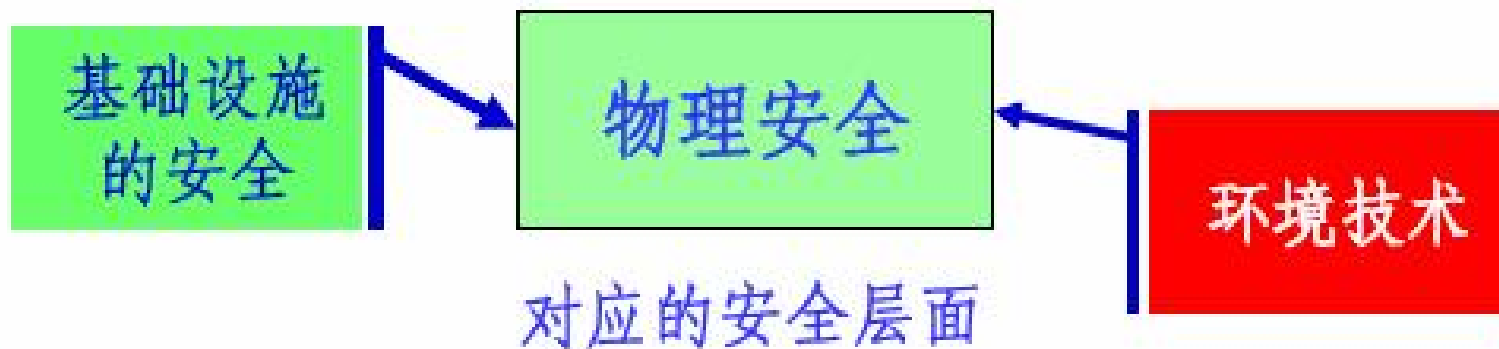
```
ModemLog_Vt100 V1808 (D) - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
11-30-2006 07:58:13.703 - 读取: 总数: 558, 每秒: 17, 写入的: 总数: 779, 每秒: 24
11-30-2006 08:00:13.703 - 读取: 总数: 5166, 每秒: 38, 写入的: 总数: 5758, 每秒: 41
11-30-2006 08:02:13.703 - 读取: 总数: 5727, 每秒: 4, 写入的: 总数: 6221, 每秒: 3
11-30-2006 08:04:13.703 - 读取: 总数: 12882, 每秒: 59, 写入的: 总数: 7719, 每秒: 12
11-30-2006 08:06:13.703 - 读取: 总数: 509958, 每秒: 4892, 写入的: 总数: 23086, 每秒: 128
11-30-2006 08:08:13.703 - 读取: 总数: 600649, 每秒: 5, 写入的: 总数: 23380, 每秒: 1
11-30-2006 08:10:13.703 - 读取: 总数: 601453, 每秒: 6, 写入的: 总数: 23669, 每秒: 3
11-30-2006 08:12:13.703 - 读取: 总数: 601956, 每秒: 4, 写入的: 总数: 24003, 每秒: 2
11-30-2006 08:14:13.703 - 读取: 总数: 602382, 每秒: 3, 写入的: 总数: 24189, 每秒: 1
11-30-2006 08:16:13.703 - 读取: 总数: 611730, 每秒: 77, 写入的: 总数: 25676, 每秒: 12
11-30-2006 08:18:13.703 - 读取: 总数: 622440, 每秒: 89, 写入的: 总数: 27336, 每秒: 13
11-30-2006 08:20:13.703 - 读取: 总数: 623015, 每秒: 4, 写入的: 总数: 27545, 每秒: 1
11-30-2006 08:22:13.703 - 读取: 总数: 623976, 每秒: 8, 写入的: 总数: 27866, 每秒: 2
11-30-2006 08:24:13.703 - 读取: 总数: 624525, 每秒: 4, 写入的: 总数: 28187, 每秒: 2
11-30-2006 08:26:13.703 - 读取: 总数: 625116, 每秒: 4, 写入的: 总数: 28368, 每秒: 1
11-30-2006 08:28:13.703 - 读取: 总数: 625814, 每秒: 5, 写入的: 总数: 28651, 每秒: 2
```


网络访问安全模型



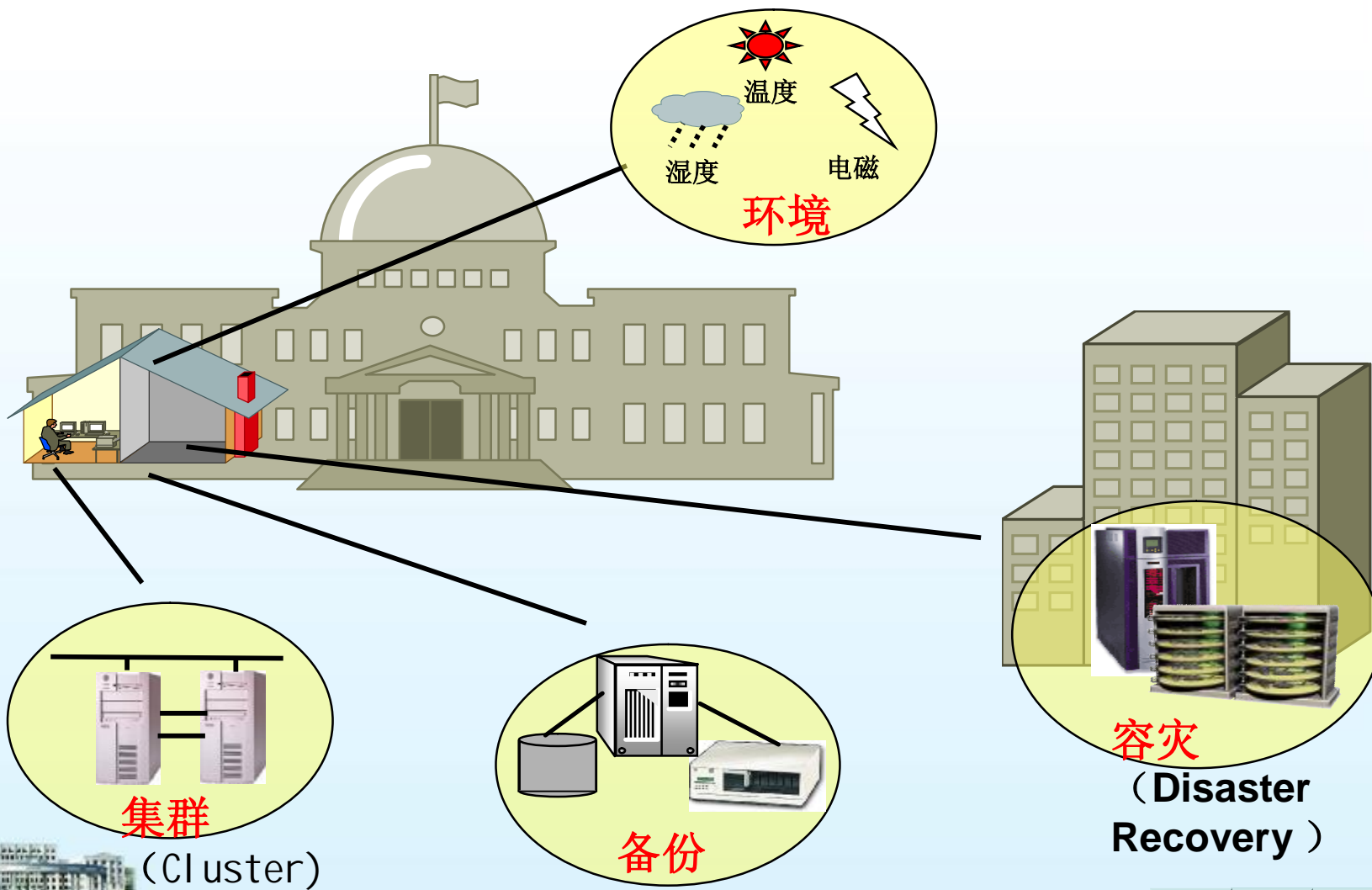
二、信息安全的分层结构

一、从作用层次的角度看信息安全



物理安全

系统可靠性——保障物理安全





- 集群和容灾技术的目的，是为了保证系统的可用性，也就是说，当意外发生时，系统所提供的服务和功能不会因此而间断。
- 对数据而言，集群和容灾技术是保护系统的在线状态，保证数据可以随时被访问。
- 这种方式不仅可以挽回硬件设备损坏带来的损失，也可以挽回逻辑错误和人为恶意破坏的损失。



为什么需要灾备?



■ 911事件发生后，世贸中心1200家企业的信息化系统（其中不乏摩根士丹利这样的巨型跨国公司的信息中心）全部损毁，本地数据全部丢失



为什么需要灾备?



■ 2002年7月23日，北京首都国际机场离港系统出现故障停机1小时，60个航班和约6000名旅客被延迟



为什么需要灾备?



■ 上海市轨道交通4号线2003年7月1日凌晨发生险情，临江花苑大厦内的劳动保障局和市财税局的重要信息系统被迫中断和搬迁



为什么需要灾备?

北京·热线

副责编 王 瑞 副责编 刘幸炎 副责编 赵 阳

京华时报

2008年11月9日 星期日 邮E-mail:abc@jrhua.cn

07

全市铁路售票系统瘫痪5小时

南站一度滞留上千旅客 北京铁路局紧急启动备用售票系统

本报讯 (记者夏伟明 周宇)昨天早上8点,北京各大火车站陆续出现售票系统瘫痪,系统死机故障,铁路售票系统一度瘫痪。受此影响,北京南站、北京西站等售票大厅大批旅客滞留,北京铁路局紧急启动备用售票系统,统一出售“无座票”。5小时后,各站售票系统恢复正常。

早上8点半,市民李女士来到北京南站,准备买票去上海。在售票厅李女士却发现,8台自动售票机只有一台可以出票,其余7台都已“暂停服务”。而在该台售票机前,已排起近10米的长队,还有不少人在周围试图排队。

此时的人工售票窗口前也排满了旅客。“正常只需半分钟就可买到票,现在要4分钟,甚至更长。”旅客张先生说,8点半以后,南站的售票系统基本瘫痪,滞留售票大厅的旅客越来越多,一度达到上千人。与此同时,北京西站、北京站均有旅客反映火车站售票系统瘫痪、购票队伍积压等情况,市内一些火车站代售点也无法正常售票。



昨天上午,在南站售票厅内,自动售票机已暂停服务,但仍有许多旅客在排队等候。

上午9点半,记者来到北京南站,发现许多旅客已买到车票,但车票均显示为“无座”。北京南站值班站长王先生说,故障发生后,车站查看了故障前当天各趟列车的售票情况,将可售票平均分配到各个窗口,按列车的开车时间以“无座票”的形式售卖。“但由于自动售票机偶尔也能出一次票,所以这种售票方式可能会有误差。”王先生说,出现购票人数多于剩余座位数,但这个误差不会超过10人,乘客持“无座票”上车基本可找到座位。

北京铁路局表示,昨天上午开始,由于售票系统计算机部分配件故障,北京地区各站售票速度缓慢。接到消息后,北京铁路局已启动售票系统应急预案,并迅速组织工程技术人员抓紧处理故障配件。经全力抢修,北京地区各站售票系统于12点50分全部恢复正常。

■各站应对方案

南站:启用500张手写代用票

由于南站每隔10多分钟就有列车发出,加上前往南站候车的人大多是即买即走的京津城际旅客,所以北京南站在本次售票系统故障中受影响最大。

为避免过多旅客滞留,故障发生后不久,南站工作人员就开始用手

写车票代替磁卡车票使用。据悉,在北京铁路局启动备用售票系统前,该站已经发放了500张手写代用票。

“这种票和纸质票差不多,有南站的特殊标记,只在特殊情况下使用。”北京南站相关负责人表示,

人表示,在车站售票系统出现瘫痪,而北京铁路局还未启动备用售票系统前,这种手写票方式虽然原始,但即管用。

9点左右,北京铁路局启动备用售票系统后,北京南站停止了手写代用票,统一发售“无座票”。

西站:引导短途客候车室补票

故障发生后,北京西站采取了多项措施来缓解这一情况。西站党委书记魏鸿仁介绍,首先,西站启动了代用票系统,让前往石家庄、邯郸、张家口等地的短途旅客到候车室补票,让这些旅客尽量

即来即走,减少积压。其次是稳定车站秩序,从上午10点开始,车站派出站内工作人员清理闲杂人等,对旅客分流放行。与此同时,西站还临时抽调20多名休班的售票员上岗售票,开通了所

有窗口,压缩了职工吃饭时间,并通过广播向旅客进行解释和宣传。

“我一直在现场,没有发现旅客有过激举动。”魏鸿仁说,经过系统维护,北京西站的售票系统于12点40分恢复正常。

北京站:循环广播告知故障情况

据了解,此次故障对北京站的影响比较小,因为该站有将近一半的售票窗口设置在广场前廊,不

易导致旅客滞留。另外,当前正值旅客出行淡季,车站旅客并不多。不过,该站依旧采取

措施,通过循环广播告知旅客售票故障,请求旅客谅解,并且提醒旅客注意车站公告。

2008年11月8日,北京火车站售票系统死机瘫痪,不得已采用手写无座票的售票方式进行应急处理,直到5小时后系统才修复



u 从这些案例我们可以看出，信息系统灾难距离我们是多么的近、多么的直接、多么的频繁！远非我们想象的是遥不可及的事情！

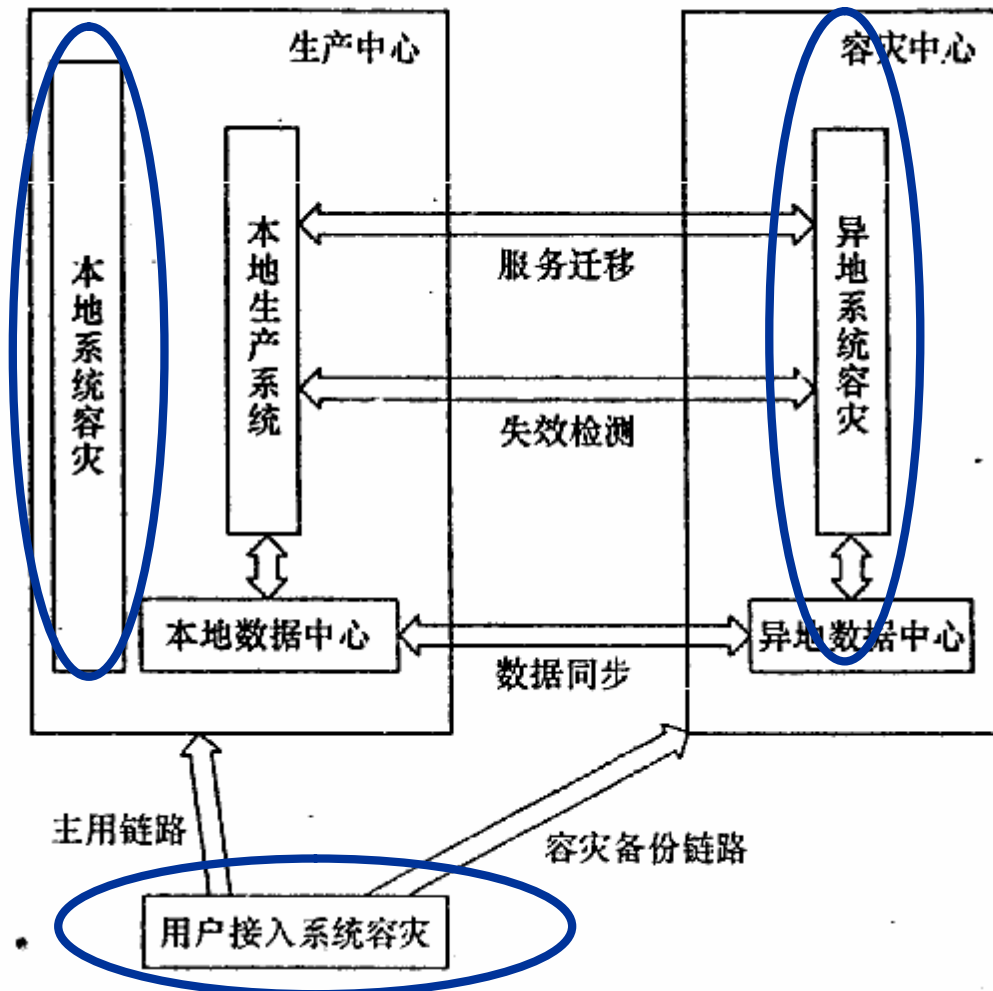


容灾系统

- u 容灾的目的：防止信息系统在遭受灾难时造成系统服务停止和数据丢失
- u 容灾的实现：主要通过在地建立和维护一个容灾中心，利用地理上的分散性来保证对灾难性事件的抵御能力
- u 容灾系统应包含
 - Ø 数据容灾、网络容灾、服务容灾、容灾规划



容灾系统的体系结构



灾备成功典型案例

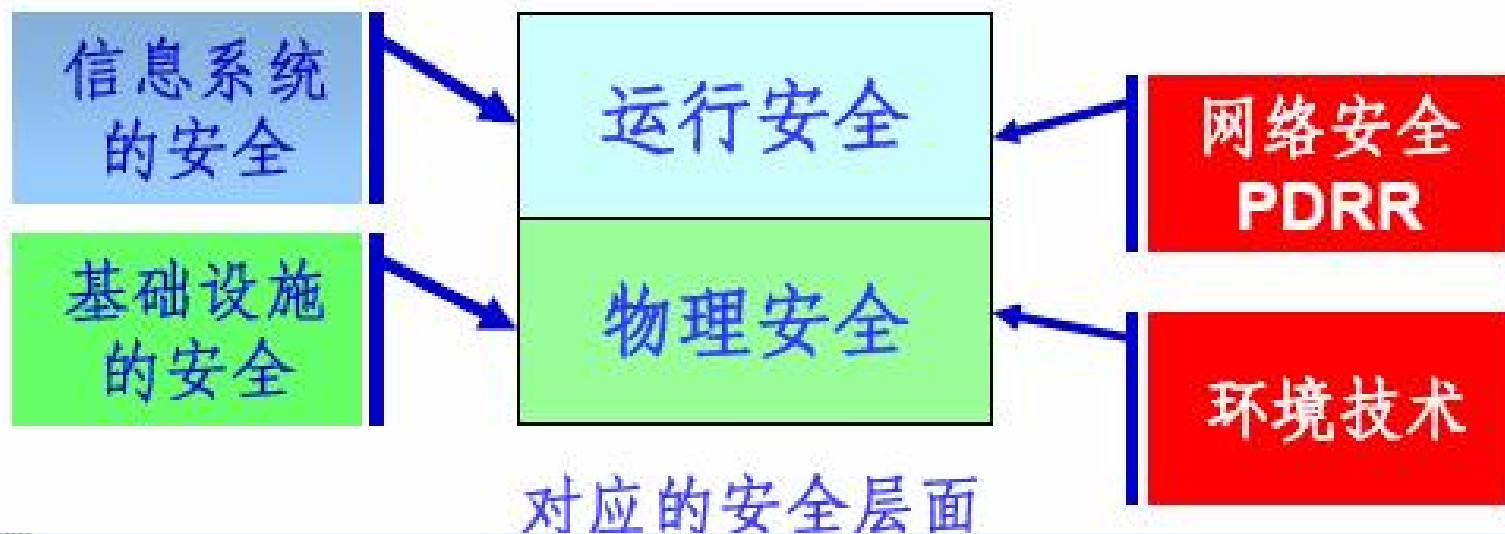
u“911”事件后发生后，因国贸大厦的轰然倒塌，位于其中的德意志银行和纽约银行两个银行走向了
两条截然不同的道路。

Ø 因为在异地建立了数据灾备中心，德意志银行很快就恢复了业务；

Ø 而后者却在数月后因数据的丢失被迫破产清盘，从而引发了以金融保险业为主的客户对数据灾难备份建设的庞大需求



运行安全



关于运行安全

- u 指对网络与信息系统的运行过程和运行状态的保护。主要涉及网络与信息系统的**真实性、可控性、可用性**等。
- u 主要涉及的技术：
 1. 风险评估体系、安全测评体系
 2. 漏洞扫描、安全协议
 3. 防火墙、物理隔离系统、访问控制技术、防恶意代码技术
 4. 入侵检测及预警系统、安全审计技术：
 5. 容侵技术、审计与追踪技术、取证技术、动态隔离技术
 6. 网络攻击技术，Phishing、Botnet、DDoS、木马等技术



威胁来自何方？


系统固有的问题、人的安全意识都可以引起系统的安全问题。

n 防护设施不完备。


n 开放了某种不必要的服务端口。

n 口令比较简单，容易被猜测出来。

n 系统存在**BUG**。




保护不足
(手段不完备)



一扇门没关
(有后门)



非法入侵
(强度不够)



存在死穴
(有致命缺陷)



引发网络安全的主要因素

1. 攻击可控性——控制信息系统
2. 攻击可用性——阻塞信息系统

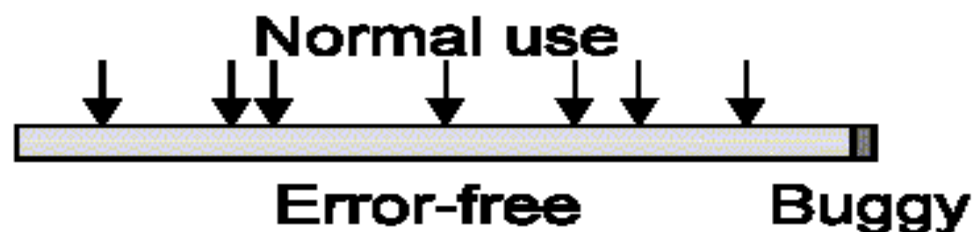
u 安全漏洞：系统的客观存在

u 风险 = （安全漏洞+ 脆弱性）x 威胁



安全漏洞是导致系统不安全的核心要素

- 所有软件都是有错的,通常情况下99.99%无错的程序很少会出问题

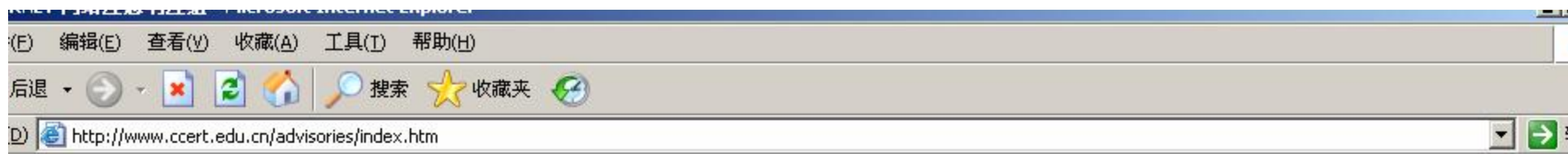


- 同安全相关的99.99%无错的程序可以确信会被人利用那0.01%的错误



- 0.01%安全问题等于100%的失败





CCERT 中国教育和科研计算机网紧急响应组

关于我们 | 系统补丁 | 安全漏洞 | 常用工具 | 相关文档 | 安全论坛 | 教育培训 | 安全公告 | 垃圾邮件 | 安全资源 | 相关链接

[-首页](#)

[|-安全漏洞](#)

漏洞检索

[English](#)

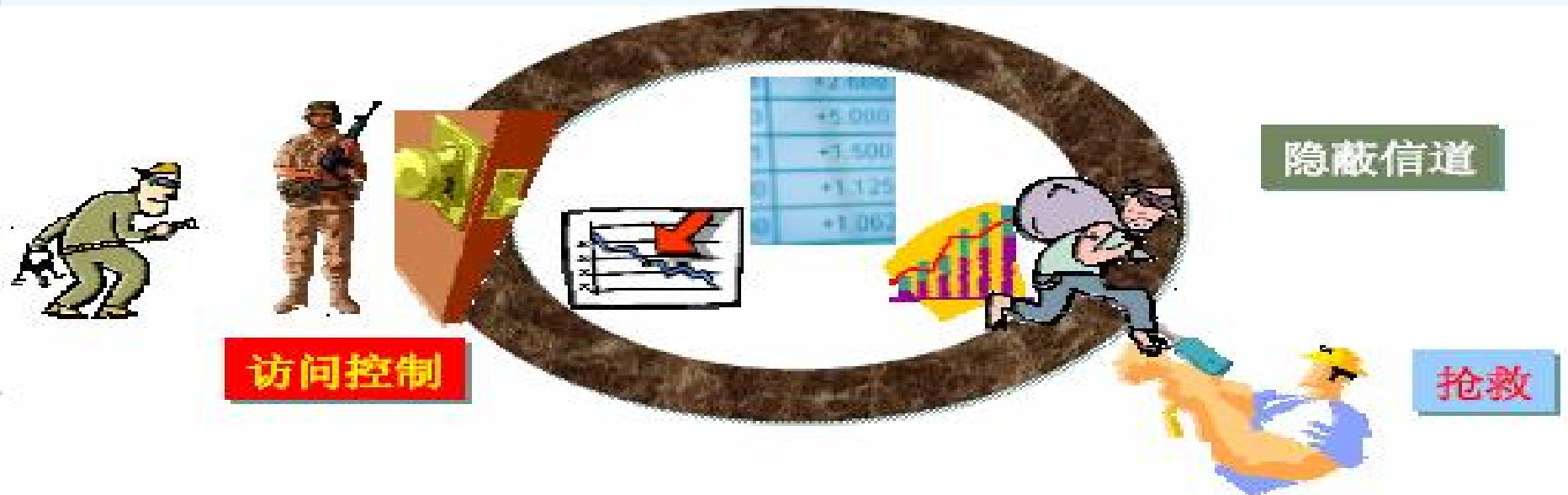
共4页 第 1 2 3 4 页 [下一页](#) [尾页](#)

CCERT编号	标题	作者	来源
CCERT-90	Microsoft Office XP中的漏洞可能允许远程执行代码	starry	微软安全公告 (MS05-005)
CCERT-89	WinAMP in_cdda.dll CDA设备名缓冲区溢出漏洞	starry	绿盟科技安全小组 (NSFOCUS Security Team)
CCERT-88	索引服务中可能允许远程执行代码漏洞 (871250)	starry	微软安全公告 (MS05-003)
CCERT-87	光标和图标格式处理中的漏洞可能允许远程执行代码漏洞 (891711)	starry	微软安全公告 (MS05-002)
CCERT-86	HTML帮助中可能允许代码执行漏洞 (890175)	starry	微软安全公告 (MS05-001)
CCERT-85	WINS中可能允许远程执行代码漏洞 (870763)	starry	微软安全公告 (MS04-045)
CCERT-84	Windows 内核和 LSASS 中允许权限提升的漏洞 (885835)	starry	微软安全公告 (MS04-044)
CCERT-83	超级终端可能允许执行代码漏洞 (873339)	starry	微软安全公告 (MS04-043)
CCERT-82	DHCP 中可能允许远程执行代码和拒绝服务攻击漏洞 (885249)	starry	微软安全公告 (MS04-042)
CCERT-81	WordPad 中可能允许执行代码漏洞 (885836)	starry	微软安全公告 (MS04-041)
CCERT-80	Internet Explorer浏览器HTML元素漏洞 (889293)	starry	微软安全公告 (MS04-040)
CCERT-79	Internet Explorer 的累积性安全更新 (834707)	starry	Microsoft 安全公告 MS04-038
CCERT-78	Windows Shell 中的漏洞可能允许执行远程代码 (841356)	starry	Microsoft 安全公告 MS04-037

安全漏洞是导致系统不安全的核心要素

系统安全漏洞的存在原因：

1. 调试后门：调试软件残留的结果
2. 隐蔽信道：功能之间的相互影响（功能污染）
 - 系统救援所带来的后门：救援时不需要认证身份



安全漏洞是导致系统不安全的核心要素

系统安全漏洞的存在原因：

3. 恶意设置：人为因素

逻辑炸弹：以条件毁坏为目的



安全漏洞是导致系统不安全的核心要素

系统安全漏洞的存在原因：

3. 恶意设置：人为因素

- | 逻辑炸弹：以条件毁坏为目的
- | 木马：以获取信息为目的



木马具有远程管理（控制）系统的能力

阅览、拷贝、修改、
注入信息...



系统安全漏洞的存在原因：



1. 调试后门：调试软件残留的结果
2. 功能污染：一个功能影响了另一个功能
 - ü 系统救援所带来的后门：救援时不需要认证身份
3. 恶意设置：人为因素
 - ü 逻辑炸弹：以条件毁坏为目的
 - ü 木马：以获取信息为目的
4. 软件正确性不可证明：软件漏洞的客观存在
 - ü 程序攻击，黑客攻击



第一例电脑黑客事件

- u 1998年6月16日，上海某信息网的工作人员在例行检查时，发现网络遭到不速之客的袭击。7月13日，犯罪嫌疑人杨某被逮捕。这是我国第一例电脑黑客事件。
- u 经调查，此黑客先后侵入网络中的8台服务器，破译了网络大部分工作人员和500多个合法用户的帐号和密码，其中包括两台服务器上超级用户的帐号和密码。
- u 今年22岁的杨某是国内一著名高校数学研究所计算数学专业的直升研究生，具有国家计算机软件高级程序员资格证书，具有相当高的计算机技术技能。据说，他进行电脑犯罪的历史可追溯到1996年。当时，杨某借助某高校校园网攻击了某科技网并获得成功。此后，杨某又利用为一电脑公司工作的机会，进入上海某信息网络，其间仅非法使用时间就达2000多小时，造成这一网络直接经济损失高达1.6万元人民币。
- u 据悉，杨某是以“破坏计算机信息系统”的罪名被逮捕的。据有关人士考证，这是修订后的刑法实施以来，我国第一起以该罪名侦查批捕的刑事犯罪案件。



安全漏洞是导致不安全的核心要素



系统安全漏洞的存在原因：

1. 调试后门：调试软件残留的结果
2. 功能污染：一个功能影响了另一个功能
 - ü 系统救援所带来的后门：救援时不需要认证身份
3. 恶意设置：人为因素
 - ü 逻辑炸弹：以条件毁坏为目的
 - ü 木马：以获取信息为目的
4. 软件正确性不可证明：软件漏洞的客观存在
 - ü 程序攻击，黑客攻击
 - ü 蠕虫攻击



蠕虫攻击

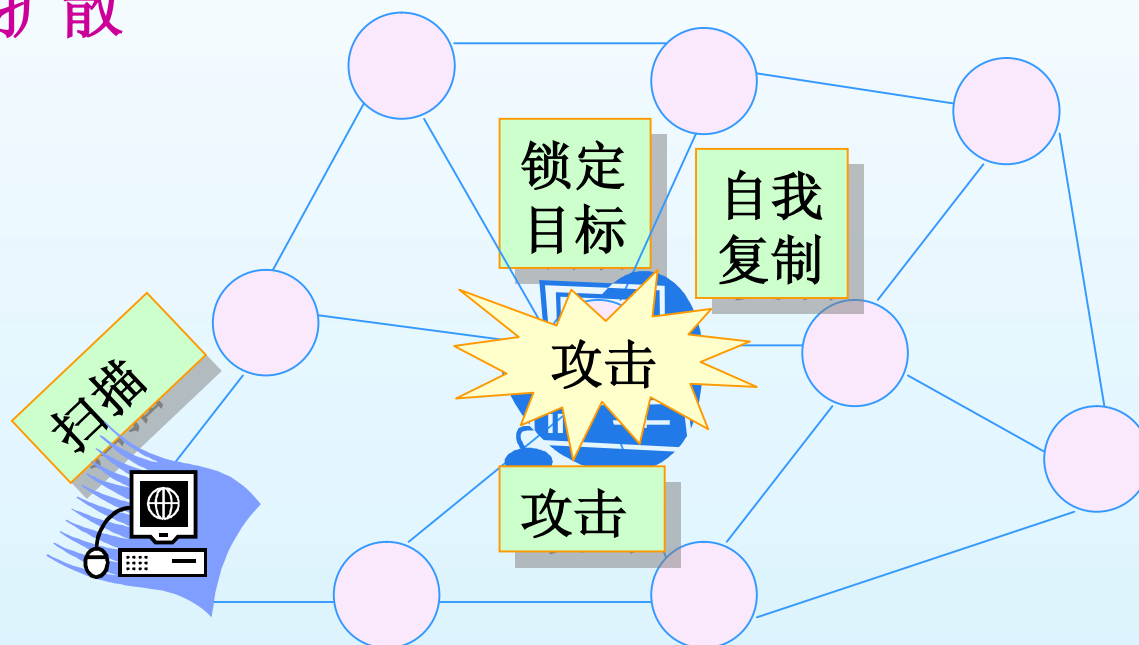
- u 1988年11月3日，第一个“蠕虫”被放到Internet上。
- u 在几小时之内，数千台机器被传染，Internet陷入瘫痪。
- u “蠕虫”的作者Robert Morris J.r被判有罪，接受三年监护并被罚款。
- u “Morris蠕虫”的出现改变了许多人对Internet安全性的看法。一个单纯的程序有效地摧毁了数百台（或数千台）机器，那一天标志着Internet安全性研究的开始。



蠕虫的工作机理

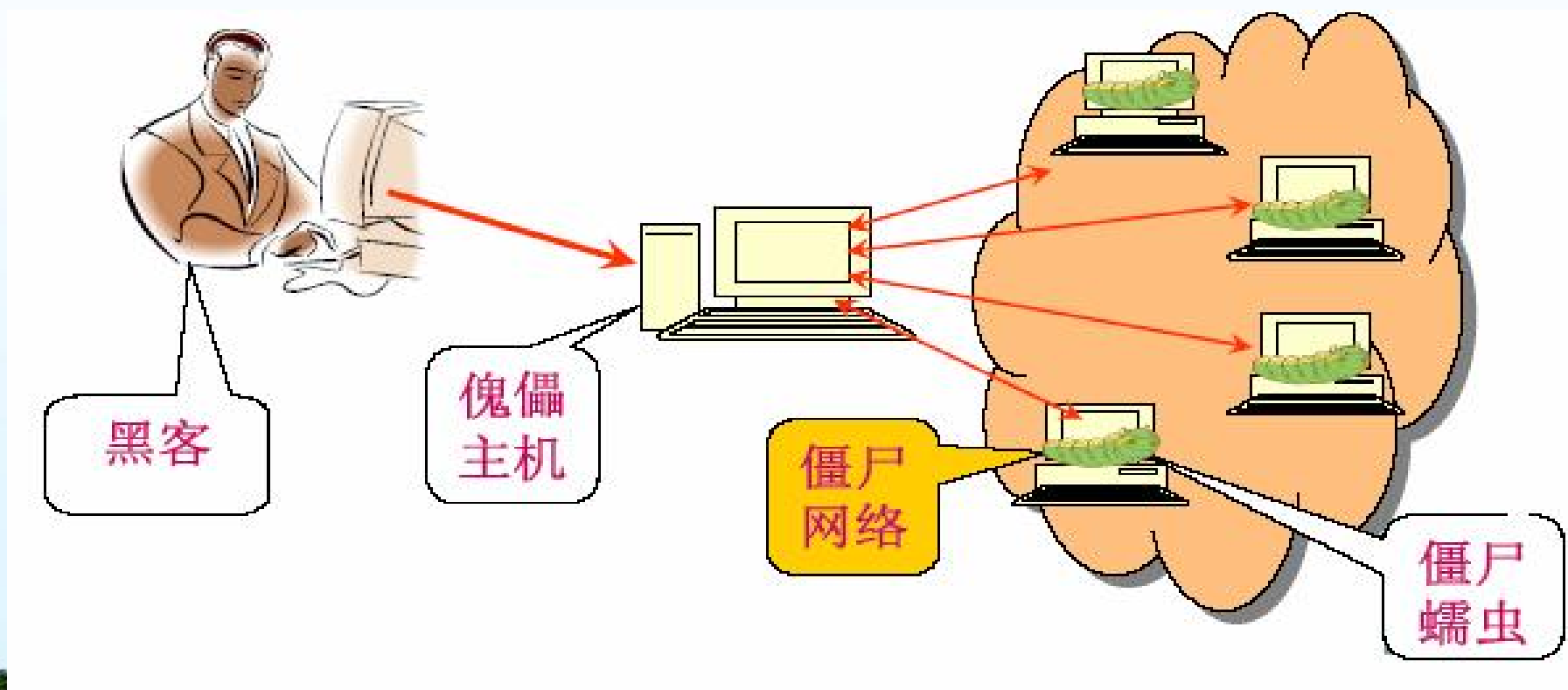
蠕虫扩散步骤:

- 扫描，寻找合适目标
- 锁定目标，探察漏洞
- 攻击：传染，驻留
- 自我复制，扩散



僵尸网络：拥有了木马武器的蠕虫

- U 黑客利用蠕虫等手段在互联网中数百到数十万台计算机上植入僵尸程序以便到达暗中操控的目的，这些被操控的计算机构成的网络被称作僵尸网络。



系统安全漏洞的客观存在:

- ü 调试后门: 调试软件残留的结果
 - ü 功能污染: 一个功能影响了另一个功能
 - ü 恶意设置: 人为因素
 - ü 软件正确性不可证明: 软件漏洞的客观存在
- u 协议漏洞: 缺少认证机制, 可以被协议攻击者所利用
- Ø 协议的参与主体是谁? 如何认定?
- ü DNS欺骗 —— 对通信主体身份的攻击
 - ü 垃圾邮件

TCP/IP协议簇
通常不强制性
确定交互双方
的身份.....



脆弱性：系统的薄弱环节

风险 = （安全漏洞 + 脆弱性） × 威胁

u 信息系统的脆弱性

Ø 互联网访问认证过程中处于不对称状态：缺乏信任保障机制，导致信息系统信任危机：

ü 在商家充分质疑、防范用户的时候，有谁提供让用户防范商家的手段？

！ 谁来保证我所上的网站就是我想要上的那个？

！ 谁来保证我所登录的帐号是我要登录的？



脆弱性：系统的薄弱环节

风险 = （安全漏洞 + 脆弱性） × 威胁

U 互联网访问认证过程中处于不对称状态：缺乏信任保障机制，导致信息系统信任危机：

ü 在商家充分质疑、防范用户的时候，有谁提供让用户防范商家的手段？

l 网络钓鱼（Phishing）：

Phishing = Phreak + Fishing ;

Phreak=Phone+freak

ü Phi shi ng 攻击使用欺诈邮件和虚假网页设计来诱骗收件人访问，网页上设置恶意代码，或有时访问者提供其具有经济价值的信息。



Phishing

- u 欺诈式垃圾邮件，70%的人会如约访问。
- u 虚假冒充网页，与真实网页基本相同。弹出假的登录窗口，访问者中15%会上当。

网络仿冒事件报告者 (前十个报告数量最多的组织机构)	数量
eBay (电子港湾)	207
MarkMornitor (美国安全公司)	43
Brandimension (加拿大安全公司)	22
BFKCERT (德国CERT)	17
VeriSign (互联网域名管理公司)	17
AusCERT (澳大利亚CERT)	15
Inter Identitiy (美国安全公司)	14
MasterCard (万事达卡)	13
HSBC (汇丰银行)	10
Royal Bank of Scotland (苏格兰皇家银行)	10



脆弱性：系统的薄弱环节



风险 = （安全漏洞 + 脆弱性） × 威胁

u 互联网访问认证过程中处于不对称状态：缺乏信任保障机制，导致信息系统信任危机：

Ø 在商家充分质疑、防范用户的时候，有谁提供让用户防范商家的手段？

ü 网络钓鱼（Phishing）

u 信息系统资源的局限所带来的脆弱性

Ø 导致形成DDoS的可能性



协议脆弱性：资源消耗形成的DoS攻击



这类攻击通常都设置假 **IP**地址

- 在TCP包中通过将同步位设为1的方式来请求连接，如果得到连接确认后不予理会，而是继续发出申请，将有可能耗尽服务器端的有限的响应连接的资源。



举例：DDoS—Smurf反射式拒绝服务攻击

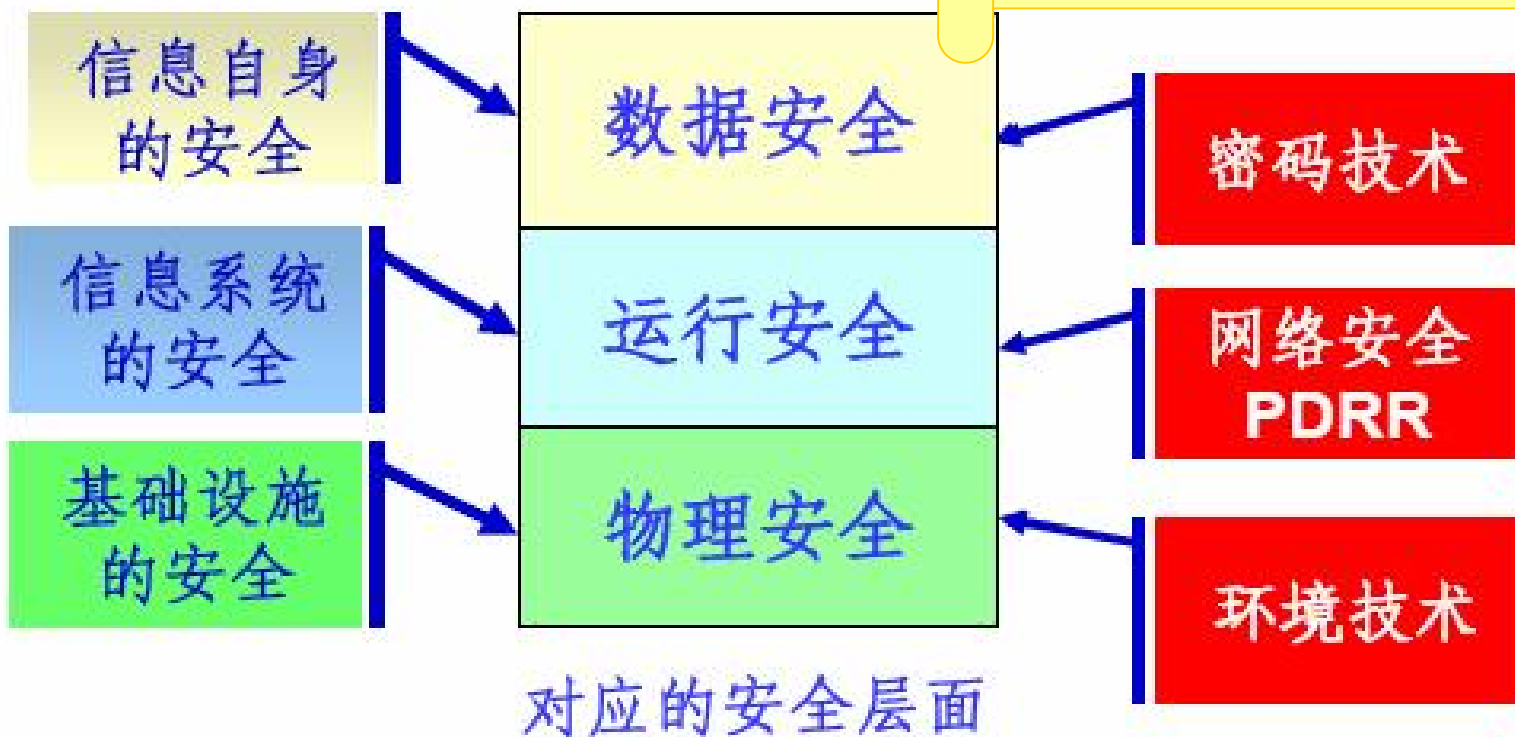


1. 攻击者A冒充被攻击对象B向受害网络C发送ICMP请求报文，要求受害网络回复。
2. 受害网络C中的所有机器同时向被攻击对象B发送回复报文。
3. 被攻击对象B被大量回复报文所阻塞。

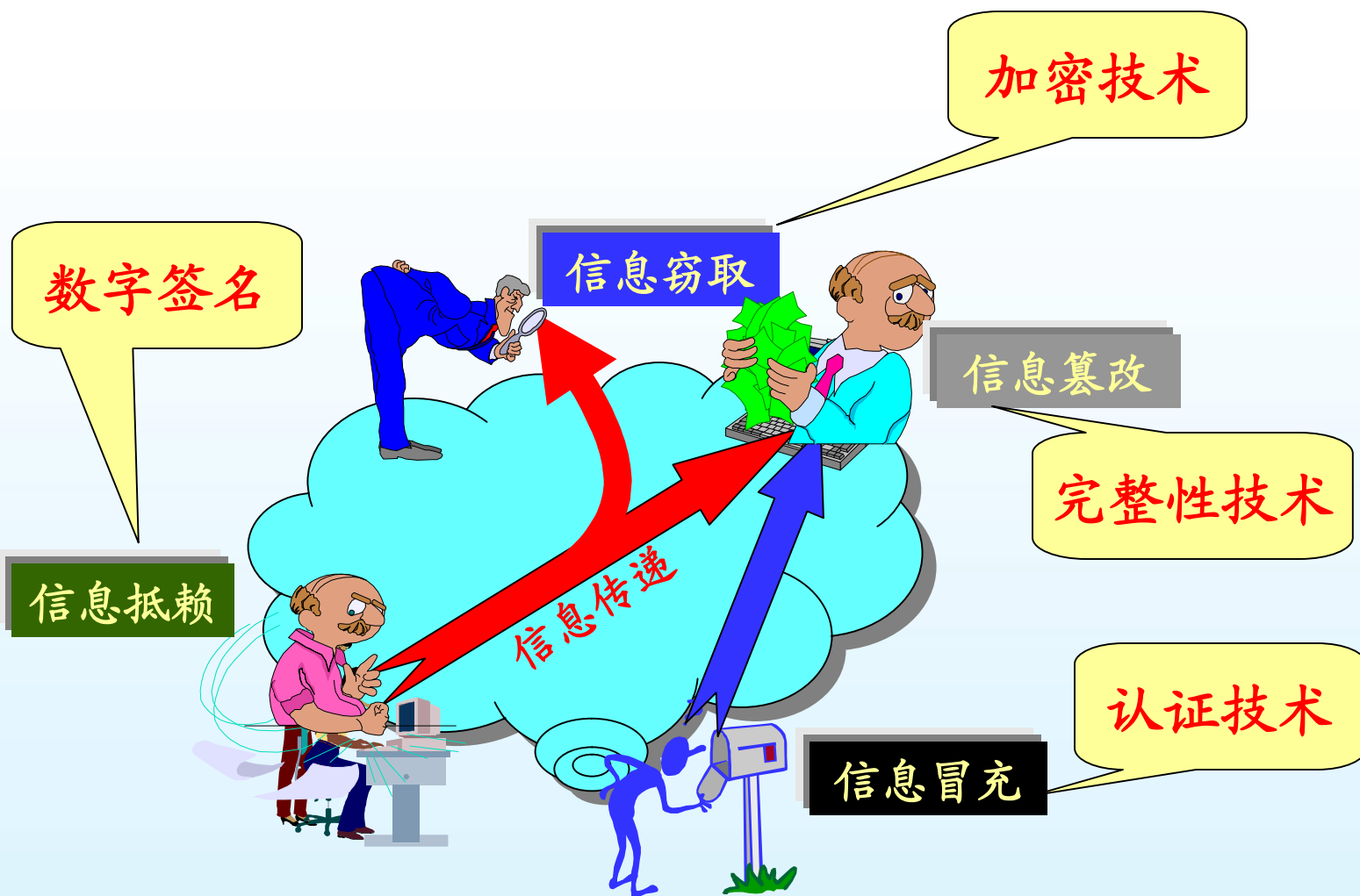


数据安全

1. 防泄露
2. 仿冒充
3. 防篡改
4. 防抵赖



关于数据安全——四个主要威胁



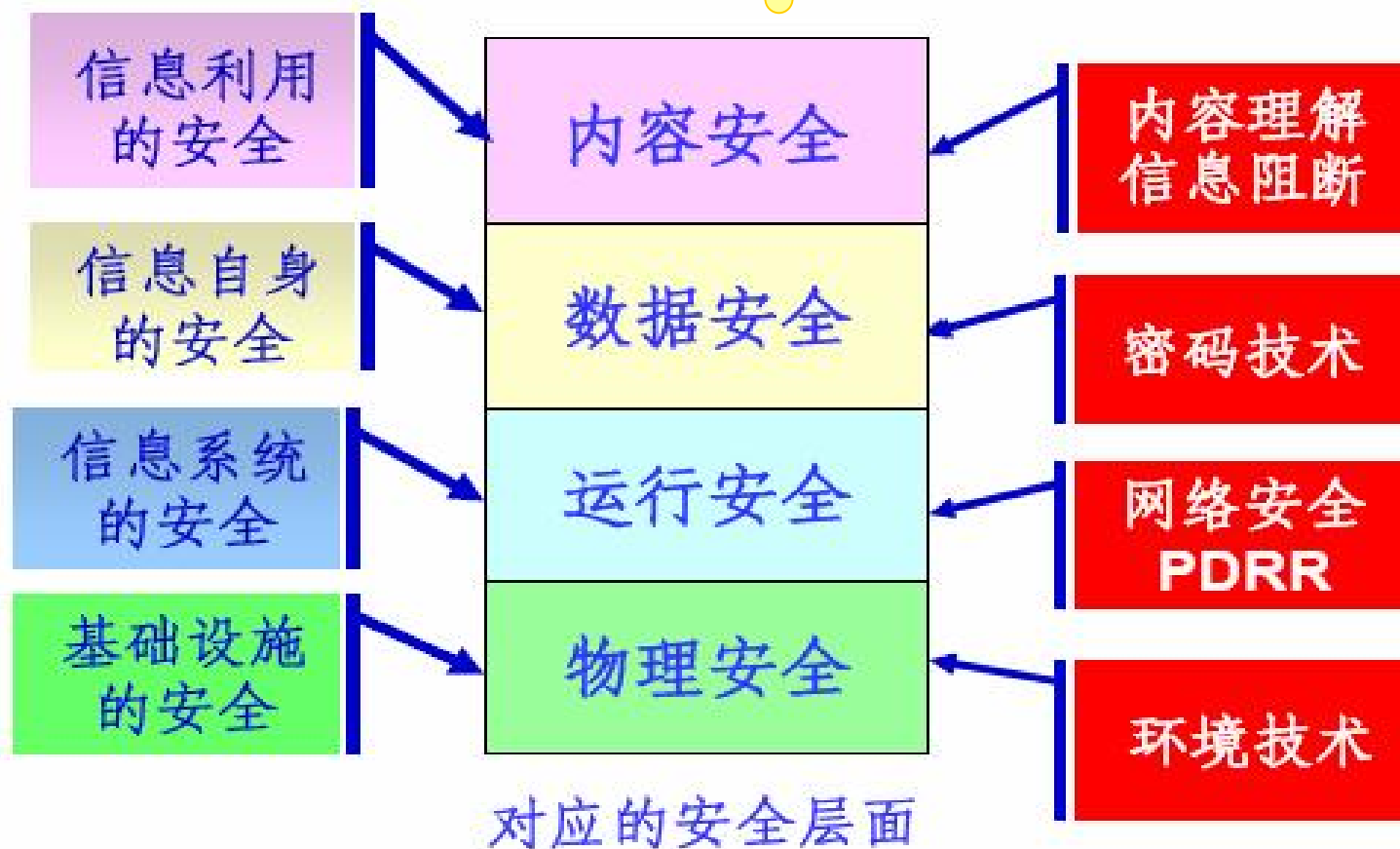
关于数据安全

- u 指对信息在数据收集、处理、存储、检索、传输、交换、显示、扩散等过程中的保护，使得在数据处理层面保障信息依据授权使用，不被非法冒充、窃取、篡改、抵赖。主要涉及信息的机密性、真实性、完整性、不可否认性等。
- u 主要涉及的技术
 - ü 对称与非对称密码技术及其硬化技术、VPN等技术：防范信息泄密
 - ü 认证、鉴别、PKI等技术：防范信息伪造
 - ü 完整性验证技术：防范信息篡改
 - ü 数字签名技术：防范信息抵赖
 - ü 秘密共享技术：防范信息破坏



从作用层次的角度看信息安全

有害信息的过滤



关于内容安全

U 指对信息在网络内流动中的选择性阻断，以保证信息流动的可控能力。主要涉及信息的机密性、真实性、可控性、可用性等。

U 主要涉及的技术：

Ø 文本识别、图像识别、流媒体识别、群发邮件识别等：用于对信息的理解与分析；

Ø 面向内容的过滤技术（CVP）、面向URL的过滤技术（UFP）、面向DNS的过滤技术等。

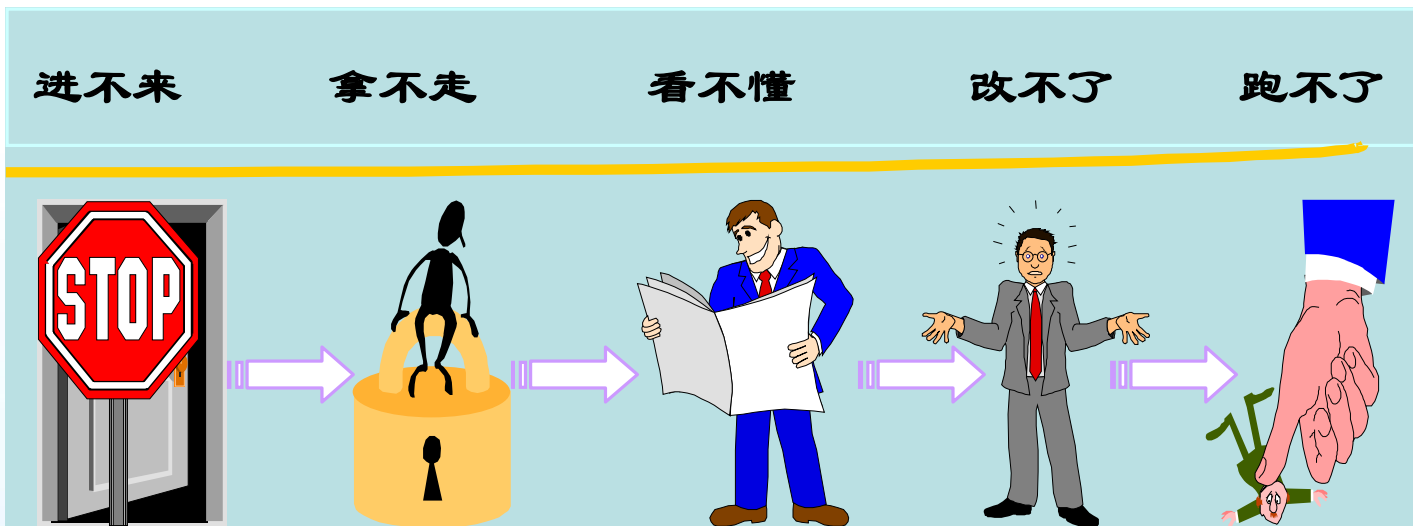




1.4 信息安全的目标



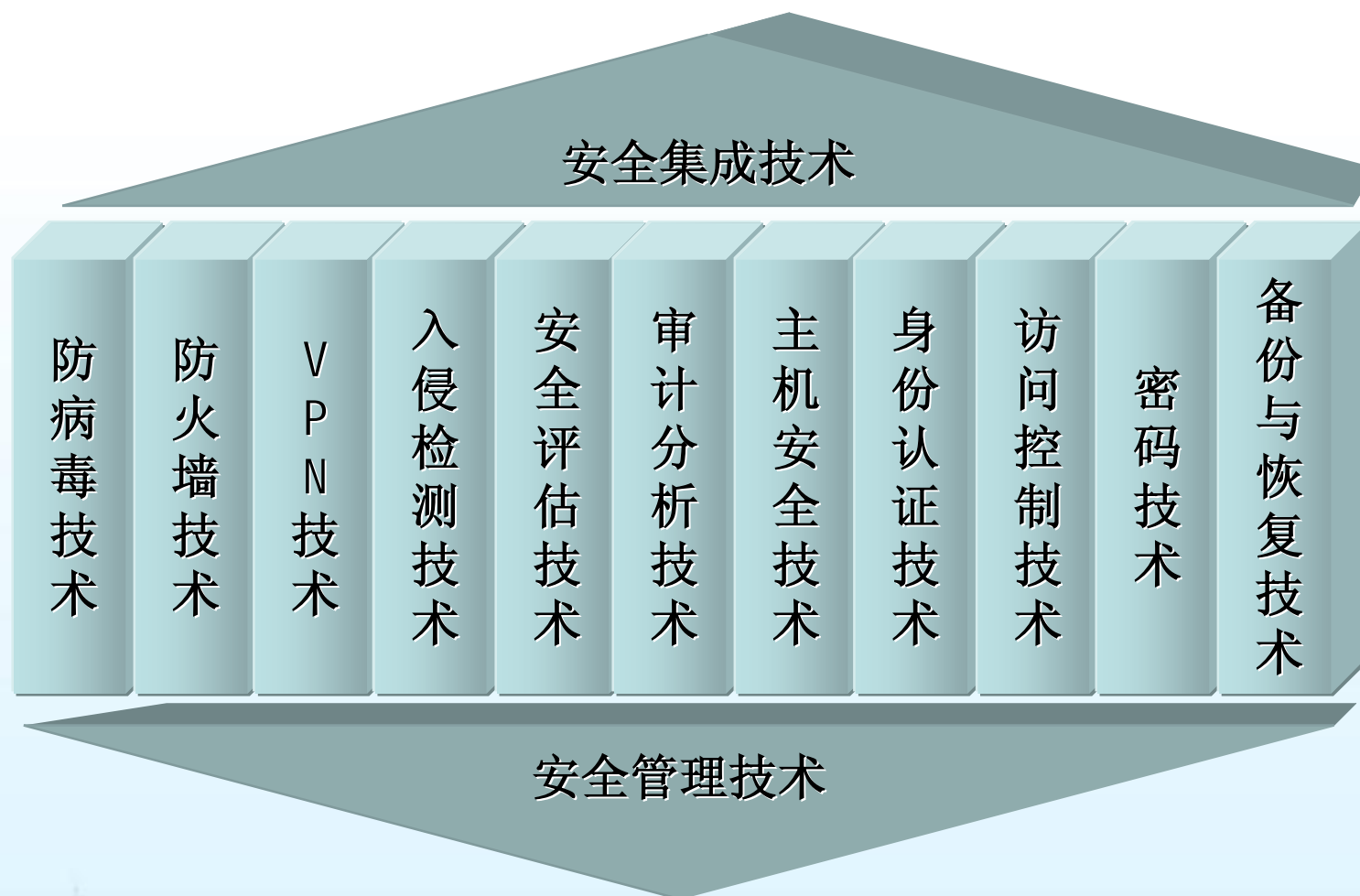
1.4 信息安全的目标



- 1、“进不来”——访问控制机制
- 2、“拿不走”——授权机制
- 3、“看不懂”——加密机制
- 4、“改不了”——数据完整性机制
- 5、“跑不了”——审计/监控/签名机制



信息安全的关键技术



END!



R&Q?

