数字化资源

SHU ZI HUA ZI YUAN

环境安全建构研究

HUAN JING AN QUAN GOU JIAN YAN JIU

主编 张怀涛 崔 波 刘二灿

◎ 吉林文史出版社

数字化资源环境安全建构研究

主　编　张怀涛　崔　波　刘二灿
撰著者　（以姓氏笔画为序）
万　瑛　王冬晓　王春西
李予红　杨灵芝　杨莉萍
苌群策　赵慧君　胡　炜
陶　钢　崔文媛　崔　萌
董明霞

吉林文史出版社

图书在版编目(CIP)数据

数字化资源环境安全建构研究/张怀涛，崔波，刘二灿主编. —长春：吉林文史出版社，2009.5
ISBN 978-7-80626-600-7

Ⅰ.数… Ⅱ.①张…②崔…③刘… Ⅲ.计算机网络—信息资源—环境—安全—研究 Ⅳ.G203

中国版本图书馆 CIP 数据核字(2009)第 073787 号

书　　名： 数字化资源环境安全建构研究
主　　编： 张怀涛　崔　波　刘二灿
责任编辑： 杨晓天
装帧设计： 圣明文化
出版发行： 吉林文史出版社
地　　址： 长春市人民大街 4646 号　　邮编：130021
印　　刷： 阜新工大印刷有限责任公司
开　　本： 787mm×1092mm　1/16
印　　张： 29.5
字　　数： 790 千字
出版时间： 2009 年 5 月第 1 版
印刷时间： 2009 年 8 月第 1 次印刷
书　　号： ISBN 978-7-80626-600-7
定　　价： 48.50 元

前　言

祸兮福所依，福兮祸所伏。在这个科学技术突飞猛进的信息时代里，黑客、噪音、污染、垃圾、入侵等等虽然不断改头换面，却一样没少。从经济的角度思维，它占用了人们的有效经济运行时间，大大缩短了人们的工作效率，构成了物质和精神的双重污染。

在信息化建设中，关于“路、车、货”的争论由来已久，所谓“路、车、货”是一种形象的说法，其实质是指信息技术（包括基础设施、硬件、软件）与信息资源的关系问题。在相当长的一段时间内，我们的注意力主要集中于信息技术的推广和基础设施的建设上，而对于信息资源的开发利用则注意不够。恰恰是数字化资源建设，才是处理、协调好“路（网络）”、“车（设备）”、“货（资源）”之间关系的重中之重。当人们讲“有路没车、有车没货”或者“有车没好货”的时候，反映了人们在实际工作中痛切地意识到了技术与资源脱节的严重问题。

“实现信息化需要三分技术、七分管理、十二分数据（信息）”，而今，“有路有车，有车有货”了。但是，如何保障“货”的安全，又成为一个关键问题了。

国民经济和社会对信息和信息系统的依赖也越来越大，所以，数字化资源环境安全成为国家安全战略的重要组成部分，他也是国家信息化、信息安全保障高层决策的基本依据。

当一个社会从经济到文化、从工作到生活、从军事到政务都已离不开信息技术，而信息技术又隐藏着巨大且不可能根除的风险。面临的最大问题莫过于如何加强信息环境安全的保护研究，这就是我们撰写《数字化资源环境安全建构研究》的初衷。

今人面临的风险并不弱于古人，人类智力的进步并不意味着风险的化解，因为这种进步会鼓励人们不断把触角伸向新的、风险莫测的领域。在新的安全环境下，病毒木马会变得更加隐蔽，不像过去那样会让用户电脑鸡飞狗跳或完全瘫痪，更多的是驻留在用户电脑后台，秘密窃取信息，比如银行帐号信息、游戏卡、游戏币以及个人信息。

黑客产业对用户生活的影响在逐渐变大，有人测算，全球每10个网站就有1个有挂马病毒。据国内瑞星“云安全”系统监测，仅2009年7月1日，互联网上就有25万个网页带有木马活动，118万人次网民遭受攻击。

病毒的发展速度可谓是日新月异，从世界上第一个电脑病毒C－BRAIN开始，2008年上半年电脑病毒数量超过去五年病毒总和。2005年，一天只有大约

50 种特征码被添加到数据库中，而 2008 年，该数字增加到了 5000。2009 年 6 月，全球病毒总数已超过 1100 万个。

人们懂得，计算机的智能无论是多么强大，毕竟是来源于作为始发因素的人的智力，机器的思维是第二性的模拟思维，它是由初始的人的思维所赋予的，再聪明的机器人，也仅仅体现了"始作俑者"人的聪明。自从有网络开始，病毒和反病毒之间的战争就从来没有停止过，技术上与病毒的对抗可谓永无止境。

面对网络安全的脆弱性，除了在网络设计上增加安全服务功能、完善系统的安全保密措施外，还必须花大力气加强网络的安全管理。因为诸多的不安全因素恰恰反映在组织管理和人员录用等方面，而这又是计算机网络安全所必须考虑的基本问题，应引起各计算机网络应用部门领导和相关人员的重视。也许最危险的黑客是"内鬼"，2009 年 7 月爆出的"力拓间谍门"事件可见一斑，在 6 年里，力拓的商业间谍"迫使中国钢企在近乎讹诈的进口铁矿石价格上多付出 7，000 多亿元人民币的沉重代价"，相当于"澳洲 10% 的 GDP"。

人必须对互联网的工具价值要有正确的认识，融合于网络社会，主体人是处在社会信息化技术目标与社会目标矛盾、虚拟与现实的矛盾之中，充分发挥"人"在信息环境安全保护方面的主体作用至关重要。

"鹰"毕竟是"鹰"。科学技术的进步，推动着哲学世界观的发展。恩格斯说过："随着自然科学领域中的每一个划时代的发现，唯物主义也必然要改变自己的形式。"科技是一把双刃剑，它既可以造福于人类，也会给人类造成某种危害。人类总是依靠科技的正面效应不断克服它的负面效应，从而形成一种制衡状态，推动科技上一个新水平，在新水平上又会产生新的负效应，再促使人们去克服，由此周而复始。人类的历史就是一个从必然王国向自由王国发展的历史，"发展是硬道理"，创新是一个永恒的主题。

"道高一尺，魔高一丈"，事物的负面效应总像影子一样跟随着正面效应出现，这大概是一个长久性课题，好像也带有规律性。人们如果处理得好，善于去利用这种矛盾制衡机制，就会让其成为社会、科技、经济发展的强大动力。

目　录

第一章　数字化资源环境安全基础

Internet 的出现，带来了信息技术的一次革命，它为整个世界提供了开放的学习、生活和工作环境。在这种开放的环境下，信息被自由地广泛传播和快速利用，资源得到了最大程度的共，为整个世界和时代带来了数不清的新机遇。但是，机会与挑战一路同行。在 Internet 环境下，数据从源端传递到目的端可能面临多种威胁，其中有四种典型的安全威胁，即篡改、截获、中断和伪造。这些威胁破坏了信息的完整性、保密性、可用性和真实性。对于不太敏感或者价值不高的信息来说，这些威胁的危害并不大；但对于像政府决策和军事部署等高度机密的信息而言，就不能等闲视之了。因此，必须构建一个可靠的、可信赖的安全信息系统来保证这些信息的安全性。

第一节　数字化信息系统的安全

信息系统包括信息存储系统（如数据库）、信息处理系统（如计算机）和信息传播系统（如通信网络）等，它的安全是一个错综复杂的问题，涉及面非常广。在这个信息社会里，由于计算机系统中的安全漏洞而引发的各类入侵事件所造成的已远远不止是经济上的损失，它甚至会影响到社会的稳定和国家的安全。信息系统的安全形势已经非常严峻。

一、信息资源安全环境现状

信息技术的不断发展，使得网络资源的双刃剑效应日渐凸显。日益严重的来自网络的安全威胁，如网络数据窃贼、黑客侵袭、病毒发布，甚至系统内部泄密，已经使信息安全成为各行业信息化建设中的首要问题。

据国家安全部门负责人透露，有 63.6%的企业用户处于“高度风险”级别，我国每年因网络泄密导致的经济损失高达上百亿。因此，网络安全技术作为一个独特的领域越来越受到各个行业的关注。

1. 全球病毒监控

近几年，网络病毒和攻击数量成倍增长，病毒也由单一型向综合型超级发展，变种数量庞大、隐藏深、危害严重；日益丰富的网络应用使病毒的传播途径大大增加。

2009 年 4 月江民全球病毒监控系统统计显示，2009 年第一季度，江民全球病毒监控系统共监测发现病毒发作 2400 多万次，数千万台计算机受到病毒的感染。这些木马病毒绝大部分是以窃取用户私密信息牟利为终极目标，用户电脑一旦被病毒入侵，网游玩家的虚拟财产、网银用户的个人资金都将面临巨大的经济损失。

值得注意的是，随着国内注册用户数达到 1300 万，Skype 网络电话也成为了木马病毒的攻击目标。据江民反病毒专家介绍，相关病毒入侵电脑后会将自身图标伪装成“Skype”的程序图标，以此来诱骗用户点击，一旦用户点击图标，木马病毒就会被激活，随后会打开一个高仿真的“Skype”登录窗口，如果用户在这个仿冒的登录窗口中输入自己的网络电话账号和密码并点击“登录”按钮，病毒就会将用户的账号信息秘密发送到黑客指定的远程服务器站

点上，致使用户的账号密码丢失，盗用账号上的资金。此外，病毒在盗号后还会显示出“文件丢失，请重新下载安装”的虚假信息蒙蔽用户。

2. 瑞星报告

安全软件厂商瑞星发布的《中国大陆地区 2009 年第一季度挂马网站安全威胁报告》显示，2009 年 1 月至 3 月，互联网上出现的挂马网页累计达 1 亿 9 千多万个，平均每天有 889 万余人次网民访问这些网页，累计有 8 亿人次网民遭木马攻击。大型网站、浏览器和流行软件成为黑客窥测的对象，一季度有 24202 个大型网站和流行软件被植入木马，这已经成为威胁国内互联网安全的最主要因素之一。浏览器已经成为木马侵入用户电脑的主要渠道。

据统计，2009 年第一季度排行前两位的木马网站为 gg6781. cn 和 sb3589. cn，这两个网站分别攻击了超过 86 万的网民。从木马网站域名类型的统计来看，CN 域名是黑客挂马最热门的类型。第一季度，有 85. 5%的木马网站使用 CN 域名。

包括某些名为“安全浏览器”的产品，只要是基于 IE 内核即会被黑客所利用，从技术上来说，所谓的“安全浏览器”根本不存在，网民应安装具有“反挂马”功能的主流安全软件，以免被木马侵入。

《瑞星安全报告》指出，由于目前流行的各种热门网站、客户端软件和浏览器，都存在着众多漏洞和安全薄弱点，使得用户遭到攻击的渠道暴增；随着黑客——病毒产业链臻于完善，支撑互联网发展的多种商业模式都遭到了盗号木马、木马点击器的侵袭，使得用户对于网络购物、网络支付、网游产业的安全信心遭到打击。

2009 年 3 月份，中国互联网新增病毒 417 万个，同比增加了 17. 2%；病毒感染机器数达 2336 万台次。其中，排名前十的病毒均系木马，并全部与盗号相关。金山毒霸云安全中心在 3 月份共截获有效挂马网址 27 万个，同比增加了近 3 倍。政府、学校网站仍然是被挂马的重灾区。除了频繁攻击各类门户、平台类网站进行挂马外，反病毒工程师发现，黑客已开始利用百度竞价、百度快照、谷歌图片来提高挂马攻击的效率。以下是几期典型的挂马事件。

(1)“票务中国”网站被挂马

2009 年 1 月 21 日，流行票务网站“票务中国”被黑客恶意挂马，网页中被植入恶意代码，代码位于域名为 http://＃＃＃＃. 706sese. cn 的服务器上。

(2)“猎杀者外挂”被挂马

2009 年 3 月 2 日，网游玩家中流行的“猎杀者外挂”程序被黑客挂马，带毒网页为猎杀者外挂内嵌的网页，玩家在使用猎杀者外挂之后，会自动打开那个被挂马的网页，导致中毒。

(3)“极品时刻表”被挂马

2009 年 3 月 9 日，网民中流行的“极品时刻表”软件被黑客挂马，技术分析标明，“极品时刻表”内嵌的网页被黑客植入木马，当用户使用该软件查询列车车次时，就会遭到攻击。

(4)“酷狗”软件被挂马

2009 年 2 月 25 日和 3 月 14 日，“酷狗”软件被两次挂马。由于黑客植入的木马没有典型特征，中毒用户丝毫察觉不到自己的电脑已遭到攻击，给用户安全带来极大风险。

3. 病毒敛财

2009 年 4 月 13 日北京晚报报道：电脑病毒盗窃用户的账号密码等行为已经为电脑用户熟知，但是，南京警方破获的一个案件仍然让很多人大吃一惊：一个名为“大小姐集团”的木马病毒制造传播团伙，案犯自己交代生意最好的三个月赚了 3000 万元。

(1)电脑遭入侵后惨变“肉鸡”

电脑运行越来越慢、上网时网站主页被锁定、电脑不断弹出广告，这是许多电脑用户遇到的现象。这些用户的电脑很可能感染电脑病毒，变成了“肉鸡”。

浏览网页、下载软件、游戏辅助工具，通过 QQ、MSN 等传输文件、使用 U 盘、移动硬盘

等，均有可能感染电脑病毒，变成随时可能挨宰的“肉鸡”。与以往不同的是，电脑病毒已经越来越带有经济的特点：盗窃用户电脑内的网上银行账号及密码、游戏账号及密码，甚至包括其中带有经济价值的文件、相册等。据了解，“大小姐”木马曾经全国泛滥，南京警方确认该案案值超过1500万元，案犯自己交代生意最好的三个月赚了3000万元。曾受“大小姐”攻击的网络游戏，包括“武林外传”、“梦幻西游”等40多款，受害玩家不计其数。

(2)六大集团控制产业链

电脑病毒作者不再是单枪匹马作战，而是联合起来呈集团作战模式，并且形成了分工明晰的产业链，有的负责制作木马病毒，有的负责将木马病毒传输到用户电脑，有的负责将用户电脑上有价值的信息分类打包，然后销售。

国内有六大挂马集团：色情五月天集团、王晓峰集团、李宝玉集团、螃蟹集团、成龙集团、CCTV－Just等，它们发起的攻击次数超过了网民遭遇的总攻击量的90%。从用户电脑中盗窃的有价值信息卖掉后才能变成真金白金。在百度网站上用“游戏信封”作为关键词进行搜索，能找到很多销售游戏账号及密码的网站，有关方面专家称，一封游戏信封就是一个包含了某位用户账号、密码的电子邮件。那些盗窃来的信息中价值比较高的账号及密码，会作为一手信出售，卖价也高，有的能卖到上万元。挑选后的信息会作为二手信，价格相对低廉，甚至开价2元钱甩卖。

(3)电脑病毒与股市相关联

网络病毒与股市大盘指数呈现深度的负相关关系。即股市上涨，网络病毒数量下降；股市下跌，网络病毒数量上升，且病毒数量的增减幅度与股市的下降和上升幅度密切相关。

2008年7月至9月，金山毒霸安全中心检测到的每日上报病毒次数呈现大幅增长态势，而在此期间，国内A股市场上证综指呈现急速下降态势。国外的一份报告显示，9月份以来，随着美国证券市场指数的急速下跌，网络病毒也呈现激增的态势。

这些数据表明，证券与网络病毒的高度负相关并不是巧合。病毒团伙有可能会密切关注资本市场表现，并实时调整以保证最大利益，以弥补因经济颓势带来的损失。另外，经济颓势会带来大量失业和待业青年，这使网络游戏用户数量呈现增长态势，吸引网游盗号木马团伙制作出更多木马病毒盗取网游虚拟财产。

由于电脑病毒形成了完整的产业链条，技术人员在其中收获颇丰。受此刺激，一些原本从事杀毒行业的技术人员，已经转移到木马病毒产业链中，这尤其值得相关部门警惕。

4. 最恶毒的10个病毒

美国旧金山的专栏作家伊恩·汤姆森和肖恩·尼古拉斯发表了他们认为迄今为止最恶毒的10个计算机病毒排行榜。

Creeper。Creeper可能是第一个计算机病毒，尽管这种说法还有争议。这个病毒是在1971年由Bob Thomas使用Tenex操作系统制作的。

Brain。Brain是在1986年年中出现的第一个用微软DOS操作系统制作的病毒。这个病毒是巴基斯坦的两兄弟Basit和Amjad Farooq Alvi编写的，原来是用于阻止拷贝一个医药软件的。

MyDoom。MyDoom是感染主机，然后重新发送整个地址簿的攻击方式。这种病毒使用经过检验而可靠的方法通过电子邮件和地址簿传播。

Nimda。尼姆达(Nimda)是历史上传播速度最快的病毒之一，在上线之后的22分钟之后就成为传播最广的病毒。

Melissa。这是一个浪漫的爱情故事。一个男孩遇到了一个女该。女孩靠跳舞赚钱，男孩回家为那个女孩编写计算机病毒。这个计算机病毒后来流传了出去，造成了数百万美元的损失。这是我们这个时代的罗密欧与朱丽叶。

Storm。Storm 是一个大型的恶意僵尸网络病毒，是在 2007 年年初以欧洲发洪水的假新闻的形式首先出现的。这个病毒给用户造成的威胁有一年多的时间。

ExploreZip。ExploreZip 病毒是在 10 年前编写的，但是，这种病毒目前仍在传播。这是病毒如此顽强的一个很好的例子。

Conficker。Conficker. C 病毒原来要在 2009 年 3 月进行大量传播，然后在 4 月 1 日实施全球性攻击，引起全球性灾难。不过，这种病毒实际上没有造成什么破坏。

Klez。Klez 也是一种非常顽强的病毒。在首次出现 7 年之后，这种病毒目前仍在传播。

Elk Cloner。Elk Cloner 病毒是一个 15 岁的高中学生 Rich Skrenta 为了开玩笑而编写的。遗憾的是他的玩笑很快就变成了坏事。Elk Cloner 病毒通过启动扇区传播，成为了后来病毒传播的标准方式。

5. 中国互联网十大病毒

金山互联网安全公司 2009 年 4 月 9 日，正式发布的《2009 年 3 月中国互联网安全报告》报告显示：3 月份，中国互联网十大病毒均系木马，并全部与盗号相关。

表 1－1 中国互联网十大病毒

排名	病毒名	金山毒霸中文病毒名	感染量
1	win32. vbt. hl. 84701	无公害感染源	2279580
2	win32. troj. small. ag. 7680	迷你下载器 AG	1652350
3	win32. troj. sysjunkt. hh	NS 窥视器	1559380
4	win32. troj. encodeie. ao. 524288	传奇盗号下载器 AO	1496680
5	win32. troj. onlinegamet. fd. 295241	网游盗号木马 295241	1446300
6	win32. troj. onlinegames. dc. 36864	cfg 寻仙盗号器变种	1359340
7	win32. troj. dropper. jg. 210338	盗号木马下载器 JG	1349380
8	win32. binder. agent. ar. 110592	地下城盗贼	1311540
9	win32. troj. sysjunk2. ak. 32768	木马驱动器 32768	1217900
10	win32. troj. qqpswt. bs. 116858	QQ 小偷	1196430

数据还显示：2009 年 3 月份，金山毒霸云安全中心共截获有效挂马网址 272，221 个，与 2 月份相比，增加了近 3 倍。其中，政府、学校网站仍然是被挂马的重灾区。目前，网页挂马已经成为病毒传播的主要渠道。挂马集团的触角已经延伸到公安局网站、人民法院以及一些其他一些政府机关的网站，猖獗程度可想而知。

6. 力拓间谍门

据《中国青年报》2009 年 7 月 24 日报道：7 月 5 日，胡士泰等四名力拓雇员因涉嫌窃取中国国家机密被上海市国家安全局刑拘。胡士泰等人通过贿赂获得的机密信息，应该包括国内各大钢企的原料库存周转天数、进口矿需求、吨钢单位毛利、生铁的单位消耗等财务数据。

机密遭窃，让力拓摸清了中国钢铁业的谈判底线，中方被动不言而喻。自 2002 年以来，铁矿石价格飙升，除 2007 年的谈判中方居于主动外，其余年份均处于被动。测算显示，中方为此累计多支付 7000 亿元，而这相当于“澳洲 10％的 GDP”。

媒体和舆论强烈谴责“潜伏者”和“内鬼”。中国社科院全国日本经济学会理事白益民表示：“国人的反思不能仅仅停留在对‘内鬼’的道德谴责层面，也不能只是拾遗补阙似的小修小补，而应全面检讨国家经济安全状况，从更为宏观的层面检视我国的国家经济安全体系以及经济发展模式，以应对全球化格局下的全新经济竞争。”

工业间谍、商业间谍国际上早已有之，屡见不鲜，几乎一直伴随着工业社会以来的进程。中国加入 WTO 以后，融入全球经济越来越深，对资源和市场的争夺也越来越激烈。随之而来的是巨大的信息流竞争。信息流的竞争，中间就有相应的谍战。全球化格局下，国际商业

社会更是无时无刻不在发生类似案例。近十年来，跨国公司在华行贿案件一直呈上升趋势，在中国遭调查的50万件腐败案件，六成以上与国际贸易和外商有关。目前已进入经济谍战高发期。

中国现代国际关系研究院经济安全研究中心主任江涌说："与西方发达国家比起来，我国的经济安全体系非常脆弱，几乎就是一片空白。力拓'间谍门'只是暴露了这一现状而已。"在中国，无论是立法还是组织体系都极为缺乏，中国还没有一部经济安全法。

进入改革开放新时期后，《保密法》明确将"国民经济和社会发展中的秘密事项"列入国家秘密的保护范围，但遗憾的是"经济保密始终没有得到应有的重视"，从而成为中国保密体系的"短板"。

德国情报部门的最新研究报告表明，几个主要发达国家，国家安全开支中用于维护经济安全的开支比例就超过了一半，凸显经济安全在国家安全当中的重要地位。

为保护本国安全，100年来美国出台了一系列法律。1917年就有《反间谍法》，1947年出台《国家安全法》，其后又不断修正，弥补漏洞与不足。进入全球化时代，为应对全新的竞争格局，1996年出台了《反商业间谍法》。"9·11事件"后，又出台了《爱国者法案》。随后由于主权财富基金崛起，新兴国家到美国并购频繁发生，《外国投资与国家安全法》应运而生。

相比之下，中国现行的《保密法》、《国家安全法》均针对的是传统安全，已不适应形势发展需要。应以此次力拓"间谍门"为契机，全面评估反思我国的经济安全体系，将其提升至战略高度加以重建。

不以我们的意志为转移，我国已进入商贸谍战的高发期，对重要经济情报和国家经济运行安全的威胁与日俱增。窃密就在眼前，面对力拓案件折射出的制度缺陷、主体缺位、监管缺失的严峻现实，我们应感到振聋发聩，是应该警醒起来了。

二、信息环境安全基础

不同的安全环境存在着不同的安全威胁，也就有着不同的安全目标。理想的安全目标就是使信息系统完全按照系统所有者的和运营者所设想的方式来工作，并尽可能地帮助管理员和用户避免错误。信息系统的安全可以分为系统内部安全和系统外部安全两部分。

1. 内部安全环境

一般而言，信息系统由计算机硬件、软件、管理员及用户组成，因此信息系统的内部安全也由硬件安全、人员安全、软件安全组成。

(1)硬件安全

重在保证系统自身的可靠性，为系统提供基本的存储保护和运行保护机制。存储保护是指对存储在不同的存储设备(如寄存器、内存、磁盘)中的数据的保护。运行保护是指计算机硬件能够提供不同的运行状态，使得某些指令只能在特定的运行状态下执行，从而为软件的安全奠定基础。

(2)人员安全

指对系统的管理员和用户进行安全教育和培训，增强安全防范意识。人员是信息系统中最积极的因素，可以通过很多信息系统以外的手段进行信息的传播，人员安全问题可以在管理领域得到解决。

(3)软件安全

随着通讯技术和网络技术的迅速发展，物理隔离对于信息系统的保护作用显得越来越小了，因此通常情况下我们涉及最多的是软件的安全。我们可以把软件安全进一步分解为以下目标：

●保密性。保护信息不被非法泄漏给非授权的用户、实体或过程，同时也不能为它们所

利用；

●完整性。保护系统中的各类数据，使之避免受到非授权的改动或删除，这种改动或删除可能是非法的恶意行为，也可能是由于疏忽导致的错误操作；

●可用性。保证在任何时候都可以向合法用户提供保证质量的服务，其中包括准确的数据和及时的响应速度；

●可控性。指对信息的传播及内容具有控制能力，使得每个人只能访问和！控制自己职能范围内的数据；

●可追踪性。系统中发生的各种事件都可以找到相应的用户对该事件负责，可以依此确定是否存在非法入侵或者偶然的误操作及其对系统造成的破坏程度，使得用户为其行为负责，从而最终减少对系统的潜在的攻击行为。

不同的应用场合对以上所述各个方面的安全性的侧重点也不同。例如，对于军队和情报部门，它们对于信息的保密性要求最高，而大型网站对于保密性的要求则要低得多，它们对系统的完事性和可用性的要求较高。某些商业机构，如银行，则对于数据完整性和用户行为可追踪性的要求超过了对于保密性的要求。

2. 信息系统安全标准

国际上较早和较为系统地研究信息系统安全问题的是国际信息处理联合会(IFIP)。IFIP 下属的国际计算机安全技术委员会是研究计算机及网络技术安全的世界性学术组织，全球主要发达国家及部分发展中国家的计算机安全问题专家都是其成员。该委员会专家们重点讨论的问题之一就是数据库及网络系统安全技术，并一直致力于研究制定计算机信息系统安全评级准则的工作。

最早提出计算机安全标准的是美国国防部所属的计算机安全中心，该中心于 1983 年公布了适用于多用户操作系统的《可信计算机系统评估标准》，1989 年和 1991 年该中心又制定了《可信网络指南》和《可信数据库指南》。1992 年，基于美国国防部国家安全中心的 CZ 级要求，美国国家标准与技术研究所和国家安全局联合制定了《多用户操作系统最低限度安全要求》，其中安全特性包括 8 个方面：身份识别和验证、访问控制、可查性、审计、客体再用、精确性、服务的可靠性、数据交换和验证。安全保障要求则由 4 个方面来决定：开发环境、开发过程、操作文件、操作环境。1990 年，美、法、德、荷兰联合制定《信息技术安全保密评估准则》，于 1993 年修订后正式用于欧洲计算机信息系统安全评估工作。

历史上影响较大的两个安全评价标准 TCSEC 和 CC 都对审计提出了明确的功能要求我国的国标《计算机信息系统安全保护等级划分准则》也有相应的规定。

(1)可信计算机系统评估标准(TCSEC)

20 世纪 70 年代初期，欧美等发达国家就开始重视计算机系统的安全性问题。美国国防部 DOD 于 1983 年公布了世界上第一个计算机系统安全性评估标准—可信计算机系统评估标准(TCSEC)，随后 DOD 又颁布了可信计算机系统评估标准对数据库管理系统的解释(TDI)，它将 TCSEC 扩展到数据库管理系统。

我国在 1994 年 2 月发布了“中华人民共和国计算机系统信息安全保护条例”，标志着我国计算机信息处理工作对安全性的需求进入了一个新的阶段。

由于美国在计算机科技方面的领先地位，安全标准以美国的标准最为驰名。下面介绍 TCSEC 和 TDI 标准的基本情况。

TCSEC 中对安全系统的评估分成四大类、七个安全级别，即 D，C1、C2、B1、B2、B3、A1，其中以 A1 为最高安全级别，D 为最低安全级别。各个级别定义的基本内容如表 1—2 所示。

表 1－2　TCSEC/TDI 安全等级

级　别	定　义
A1	设计的形式化验证(Verified Design)
B3	安全域(Security Domains)
B2	结构化保护(Structural Protection)
C2	带标记的安全保护(Labeled Security Protection)
C1	受控制的存取保护(Controlled Security Protection)
D	自主安全保护(Discretionary Security Protection)
	最小保护(Minimal Protection)

TCSEC 从 C2 级开始要求具有审计功能，到 B3 级已经提出了关于审计的全部功能要求，A1 和 A1＋两个级别较 B3 级没有增加任何安全审计特征。因此，TCSEC 共定义了四个级别的审计要求：C2、B1、B2、B3。

●C2 级要求审计以下事件。用户的身份标识和鉴别、用户地址空间中客体的引入和删除、计算机操作员/系统管理员/安全管理员的行为、其它与安全有关的事件。对于每一个审计事件，审计记录应包含以下信息：事件发生的日期和时间、事件的主体(即用户)、事件的类型、事件成功与否；对于用户鉴别这类事件，还要记录请求的来源(如终端号)；对于在用户地址空间中引入或删除客体，则要记录客体的名称；系统管理员对于系统内的用户和系统安全数据库的修改也要在审计记录中得到体现。C2 级要求审计管理员应能够根据每个用户的身份进行审计。

●B1 级相对于 C2 级增加了以下需要审计的事件。TCSEC 对 B1 级安全定义了如下事件：客户登录；向客户空间中引入新的对象(创建，复制等)；从客户空间中删除对象；计算机操作员，管理员，安全员的行为；所有的安全相关事件，包括所有试图改变系统安全状态的事件，如：改变客体安全等级，修改客户口令，频繁登录等；打印输出等。对于可以输出到硬拷贝设备上的人工可读标志的修改(包括敏感标记的覆写和标记功能的关闭)、对任何具有单一安全标记的通讯通道或 I/O 设备的标记指定、对具有多个安全标记的通讯通道或 I/O 设备的安全标记范围的修改。因为增加了强制访问控制机制，B1 级要求在审计数据中也要记录客体的安全标记，同时审计管理员也可以根据客体的安全标记制定审计原则。

●B2 级的安全功能要求。B2 级较之 B1 级增加了可信路径和隐蔽通道分析等，因此，除了 B1 级的审计要求外，对于可能被用于存储型隐蔽通道的活动，在 B2 级也要求被审计。

●B3 级。B3 级在 B2 级的功能基础上，增加了对可能将要违背系统安全政策这类事件的审计，比如对于时间型隐蔽通道的利用。审计子系统能够监视这类事件的发生或积聚，并在这种积聚达到某个阈值时立即向安全管理员发出通告，如果随后这类危险事件仍然持续下去，系统应在做出最小牺牲的条件下主动终止这些事件。这种及时通告意味着 B3 级的审计子系统不象其它较低的安全级别那样只要求安全管理员在危险事件发生之后检查审计记录，而是能够更快地识别出这些违背系统安全政策的活动，并产生报告和进行主动响应。响应的方式包括锁闭发生此类事件的用户终端或者终止可疑的用户进程。一般地，“最小的牺牲”是与具体应用有关的，任何终止这类危险事件的行为都是可以接受的。

TDI 是 TCSEC 在数据库管理系统方面的扩充和解释。TDI 不能独立成为一个标准，需要联合 TCSEC 作为参照，TCSEC 中各个安全级别的安全性是积聚性的，即较高安全级具有所有较低安全级的安全性能。TDI 沿用了 TCSEC 的做法，从四个方面来描述安全等级的划分标准，即安全策略、责任、保证和文档。每大项又分为若干子项。

在上述等级中，D 级的计算机系统除了物理上的安全设施外没有任何安全措施，C1 级只提供了非常初级的安全机制，现有的商业系统往往稍作改造或根本不用改动即可满足其要

求。C2 级安全实际上是安全产品的最低档次，有很多商业产品已得到该级别的认证。Bl 级别包括了强制存取控制以及审计等安全机制，它能够比较好地满足大型企业或一般政府部门对于数据的安全需求，这一级别通常认为是真正意义上的安全产品。

在 TCSEC 的评价准则中，Bl 级开始就要求具有强制访问控制和形式化模型技术的应用，Al 级更是对形式化的最高级描述和验证及形式化的隐秘通道分析等进行了要求。可见，数据模型、形式化描述和验证技术在高安全级别的计算机系统的设计和实现中是不可缺少的。

TCSEC/TDI 中的一个主要概念是可信计算基(TCB)，它是计算机系统中保护机制的全部。计算机系统的安全完全依赖于实施安全策略可信的软件、硬件和负责系统安全管理的人员，这些就构成了可信计算基。TCB 由一个或多个成分组成，它们一起对产品或系统实行统一的安全策略。简单地说，TCB 是数据库系统或产品中的所有安全相关部门之和。由此可见，安全数据库系统开发的核心问题是 TCB 的设计与实现。

我国自 2001 年 1 月 1 日起开始实施强制性国家标准 GB17859 — 1999。它将安全系统划分为一级至五级共五个级别。

(2)CC 标准

CC 标准是美国、加拿大、英国、法国、德国、荷兰等国家联合提出的信息安全评价标准，在 1999 年通过国际标准化组织认可，成为信息安全评价国际标准。

CC 标准采用了保护轮廓定义书(PP)和安全对象定义书(ST)的思想，把安全需求分为安全功能需求和安全保证措施两个相互独立的方面。CC 标准在组织上分为三部分，第一部分描述标准的概貌和基本概念，第二部分定义了一系列公认的安全功能，第三部分定义了一系列用于取得一定可信度的安全保证措施。

CC 标准的安全需求用类、族和组件的形式进行定义。

首先，把安全功能的全集根据侧重点的不同划分为若干类，每个类又根据不同的安全目标化分为若干小组，称为族。对于一个族内的安全需求，又根据其强度和能力的不同划分为更小的组，称为组件。组件是最小的安全需求单位，是安全需求和具体表现形式，可以根据一定的安全策略和安全目标从预先定义的组件中进行选择以构成保护保护轮廓定义书(PP)或安全对象定义书(ST)。CC 标准所定义的类和族都具有正式的名称，而组件是用其所属的类和族名后加上编号表示的。CC 标准也给出了组件间的信赖关系。把多个安全需求组件组合在一起所得到的结果就叫做一个安全组件包。安全组件包可用于构造更大的安全组件包或用于构造保护轮廓定义书(PP)和安全对象定义书(ST)。安全组件包可以表示一组安全功能需求或安全保障需求，这些需求可以满足预定的安全目标中的某个子目标的需要。

CC 标准定义了 11 个公认的安全功能需求类，它们是安全审计类、通信类、加密支持类、用户数据保护类、身份识别与鉴别类、安全管理类、隐私类、安全功能件保护类资源使用类、安全产品访问类和可信路径/通道类。安全审计类涉及与安全有关的操作信息的识别、记录、存储和分析等方面的需求。通信类涉及数据交换双方的身份确定等方面的需求，包括收、发双方的防抵赖性等。加密支持类涉及密钥管理和加密操作等方面的需求。用户数据保护类涉及对用户数据进行保护的安全功能和安全政策等方面的需求。身份识别与鉴别类涉及证实用户身份和确立安全属性等方面的需求。身份识别与鉴别类涉及证实用户身份和确立安全属性等方面的需求。安全管理类涉及对产品的发全功能件中的属性、数据和功能等进行管理方面的需求。隐私类涉及确保用户身份的隐蔽性和防止用户身份被盗用等方面的需求。安全功能件保护类涉及确保安全功能件中的有关机制和数据的完事性等方面的需求。资源使用类涉及对需要访问的资源的可用性给予支持等方面的需求。安全产品访问类涉及对人(用户)、机(安全产品)会话过程的建立进行控制等方面的需求。可信路径/通信类

涉及在用户与安全功能之间建立可信通信路径、在安全功能件与其它可信 IT 产品之间建立可信通信通道等方面的需求。

CC 标准预定义一套评价保障等级(EAL),作为刻画产品的安全确信度的尺度。EAL 是由 CC 标准中定义的安全保障需求组件构成的一个特定的组件包,由此可见,CC 标准对产品安全确信度的衡量是与产品的安全功能相对独立的。EAL 在产品的安全确信度与建立相应确信度的可行性以及所需付出的代价之间给出了不同等级的权衡。按安全确信度由低到高依次递增的顺序,CC 标准定义了 EAL1、EAL2、EAL3、EAL4、EAL5、EAL6 和 EAL7 等 7 个安全确信度等级,每个 EAL 只包含某个保证需求族的一个组件以及它们的所有保证信赖关系,这种保证等级的递增是通过将低等级 EAL 中的某些组件替换为同族中更高级别的组件或添加其它的保证组件来实现的。EAL 的各个等级都涉及到了 CC 标准中定义的安全保障需求的各个类的内容,例外的是,EAL1 和 EAL2 不涉及生命周期支持类,同时 EAL1 不涉及脆弱性评估类。

为了适应我国的信息化建设,我国对于计算机系统安全的评价也制定了相应的标准。中国国家标准 GB17859 — 1999 是 1999 年由中国国家质量技术监督局发布的《计算机信息系统安全保护等级划分准则》。这个标准是参照 TCSEC 标准制定的。与 TCSEC 基本一致,但去掉了 TCSEC 标准中的 D 和 A1 两个安全等级,其它安全等级从低到高依次称为第一至第五级(分别为用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级),同时,舍去了 TCSEC 标准中有关保障要求方面的内容。

而针一对数据库管理系统技术要求中,也专门列出了数据库管理系统安全相关的要求。

3. 信息环境安全基础

在 Internet 上传递的数据,可能面临窃听,中断,篡改和伪造等威胁,因而,这些数据在本质上是不安全的。通过加密来保证数据在源端和目的端之间的安全传递是必要的。而身份验证,访问控制和安全审计是保证信息环境安全的基础、也是最基本的三种手段。访问控制和安全审计总是以客体身份为基础的。访问控制根据客体身份安全等级,来决定是否授权其访问信息系统。审计则是安全的必要补充,它跟踪客户的敏感操作并将其记录在文件中,以保证责任明确。

(1)身份验证

一个安全的应用系统应将非法客户拒之门外,并能够审计合法客户的行为,因此身份验证是必要的。通常,身份验证主要基于三种知识:客户知道什么(如口令等);客户拥有什么(如智能卡等);客户是什么(如生物特征等)。当然,结合这些方法是可行的。一个可信的身份验证方法应该达到如下目标:

- 客户只能注册一次,不管他使用多少个系统执行他们的业务;
- 注册必须快速而有效;
- 要访问系统,客户必须登录,一次会话只有一个身份;
- 身份验证必须有效;
- 身份验证必须高效率;
- 身份验证必须适应客户环境。

客户登录到系统通常需要输入某种形式的身份标志(如 ID,磁卡等)以便进行身份认证。显然,客户登录是一种审计事件,客户身份信息也是审计信息,但是认证信息(如口令)建议不要当作审计信息。审计客户身份信息有明显的优点:入侵者,犯罪者都易于检测。

当前的身份验证机制主要有口令,Token 字,智能卡,数字签名和生物技术等技术。

(2)访问控制

访问控制就是主体请求对客体进行访问时,系统根据主体(进程)的用户和组的标识符、