中国信息安全年鉴
CHINA INFORMATION SECURITY YEARBOOK

中国信息协会信息安全专业委员会

2002-2003

中国信息安全年鉴

中国信息协会信息安全专业委员会

二〇〇三年

《2002-2003 中国信息安全年鉴》编辑委员会

编 者 说 明

《中国信息安全年鉴》是中国信息协会信息安全专业委员会主持编辑的年刊，旨在多方位记述我国信息安全动态和信息安全建设进程。

《2002－2003 中国信息安全年鉴》的涵盖时间是 2002 年初至 2003 年 3 月。这段时间，无论在全球还是在我国，对于信息安全界来说都是极不平凡的一年，是世界各国政府重新审视信息安全的一年。

《中国信息安全年鉴》自 1998 年首版以来，得到了国家信息安全各主管部门及各行业部门领导、业内专家及企事业单位的大力支持和好评。《2002-2003 中国信息安全年鉴》继承以往的工作经验，除保留原有的综合篇、政策法规篇、标准篇、部委省市篇、机构篇、认证评测篇、专题论述篇以及企业篇等栏目外，还新增了“国际篇”，为读者了解和研究国际信息安全动态提供参考；同时，基于我国电子政务的建设进程及信息安全界由此面临的机遇与挑战，本卷还增加了“电子政务篇”，“附录”收录了有关信息安全业的一些参考资料。

需要说明的是，由于今年部分地区的“非典”疫情，使本卷的“企业篇”征稿受到影响，特向各企业和读者致歉。

感谢主管部门对本刊支持。由于水平所限，《2002-2003 中国信息安全年鉴》不足之处，希望业界同仁提出批评、建议。

编者

2003 年 7 月 10 日

定价：180 元/本

目　录

综合篇

2002年国内外信息安全年度报告

吴世忠

一、2002年国内信息安全状况

2002年是中国加入WTO的第一年，刚刚融入国际社会经济贸易体系的中国正在经历着信息化的变革，与全球IT萧条形成鲜明对比，2002年是中国信息化发展十分重要的年头。国民经济和社会发展日益依赖于信息技术的发展以及对信息资源的开发和利用。在党的十五届五中全会上，国家领导人在谈到国家的工业化与信息化时明确指出："信息化已经成为当今世界经济和社会发展的大趋势，也是我国产业优化升级和实现工业化、现代化的关键环节。"党的十六大更是将"以信息化带动工业化，以工业化促进信息化"作为中国长期发展的战略。2001年下半年重新成立的国家信息化领导小组是中国信息化历史上最具权威的领导机构。2002年初国务院信息化工作办公室便以"电子政务"为龙头，启动新一轮信息化浪潮。到2002年底，中国通信网络规模容量已跃居世界第一位。中国通信网络传输全部实现了数字化，交换实现了程控化，网络技术层次进入世界先进行列。截至2002年10月，全国光缆总长度达到209万公里，其中长途光缆44.4万公里；互联网骨干网间带宽达到100兆以上，国际出入口带宽超过1万兆。SDH光通信系统、密集波分复用技术大量应用于干线网络，ATM宽带交换骨干网已经建立，IP和多媒体网初具规模，城域网逐步投入商用，宽带接入网大面积推开。电信网络正在加速向新一代宽带高速网演进，信息产业成为中国国民经济的第一支柱产业，为中国的信息化建设奠定了坚实的基础。中国互联网信息中心（CNNIC）第十一次统计结果数据显示，截至2002年12月31日，我国上网用户已达5910万人，与第十次调查相比，我国上网用户总人数半年增加了1330万人，增长率为29%，和去年同期相比增长75.4%，网民总量居世界第二。

国家信息化发展的良好开局预示着我国面对的将是一个更加开放的数字化、网络化和信息化的发展环境，经济全球化以及信息技术与网络技术的高度融合发展将给我国带来历史上难得的发展机遇。信息化水平的提高给我们带来巨大机遇的同时，也将严峻的挑战摆在我们面前。由于信息系统本身的脆弱性和日益复杂性，加之社会发展的不稳定因素，我国面临的信息安全问题逐渐凸现，2002年先后出现了多起与网络和信息安全相关的重大事件，直接影响到国民经济正常运行和社会的稳定，从而使2002年成为中国的"信息安全年"。

1. 2002年中国信息安全年的出现及特点

1.1 2002年国内信息安全主要问题

（1）“电子政务年”的安全隐患

2002年3月，国家信息化领导小组作出决定，把电子政务建设作为今后一个时期我国信息化工作的重点，并将2002年定为中国的“电子政务年”。各地、各部门贯彻中央指示，电子政务建设在全国迅速推进。据报道，到2002年7月我国已有五千多个政府网站。由于电子政务信息的特殊性和敏感性，电子政务的发展必然要面对信息安全的严峻考验。从目前政府信息化建设的实际看，安全问题和隐患仍然很突出。首先是安全保密措施不力。对我国政府上网工程的数百个网站进行的测试表明，大部分网站安全保障措施不足，难以抵御常见的黑客攻击。其次是内部管理控制不严，致使涉密材料直接上网，近年来已发生过多起绝密文件或重要会议文件在网上泄露的恶性事件。第三是安全制度不健全，且监督不够。政府部门在信息化建设中，对信息安全管理制度的重视还不够，加之内部工作人员在使用网络的过程中缺乏安全保密意识，致使涉及我国科研秘密、军事机密和工作机密的信息在网上暴露，给我国带来严重损失。第四是对承建政府信息化工程的公司、企业缺乏管理和规范，致使某些国外公司直接参与了包括信息安全在内的政府信息化工程系统集成，而且很多国内公司欠缺安全保密的制度和观念，将参与的涉密信息化系统工程的有关技术内容用作商业宣传和发表文章，甚至有些不法之徒还将这些敏感和涉密材料通过网络向境外兜售，给我国的安全保密工作带来巨大的现实威胁。第五是对信息技术产品的安全性没有把握。由于我国信息基础设施中核心技术的自主性不强，CPU、BIOS、操作系统以及高端网络设备多数靠国外引进，而对这些设备和软件缺乏有效的监控管理。虽然我国已在几年前就按WTO的规则，针对信息安全技术和信息安全产品的安全性测评认证成立了专门机构，但由于投入有限，加之缺乏相应的配套政策，使得我国的信息安全测评认证尚不能满足目前信息化发展的要求。一旦国家重要政府机构的信息网络受到合力攻击，将会产生无法预料的灾难性后果。

（2）重大信息安全事件连连发生

2002年中国发生的网络和信息安全事件与以往任何一年相比，不仅数量多，而且性质严重。见诸媒体的信息安全重大事件就有以下多起：1）从2002年1月1日起，国内先后发生数十起“法轮功”顽固分子破坏广播电视传播网络和利用广播电视设施传播反动信息的恶行。2） IP电话通信技术被恶意滥用，数据走私和电话骚扰行为猖獗，直接影响了政府的日常工作和居民的正常生活，造成极坏的影响。3）2002年最受人关注的信息安全事件是：“法轮功” 邪教组织公然践踏国际法和民用通信基本准则，分别于6月23日、9月8日至11日非法攻击我“鑫诺”卫星通信，严重干扰了中国农村电视节目和远程电视教育节目。攻击卫星事件不仅引起国内各阶层的愤慨和唾弃，也遭到国际社会的广泛谴责。4）6月29日晚，由于卫星通信故障，交通银行武汉分行外汇交易厅电子屏幕报价出现异常，美元对港元汇价变成1：124，致使13名汇民在几分钟内净赚30万美元，银行事后对此不予认可，引出国内首例网络炒汇纠纷案。5）7月5日深圳证券交易所因卫星通信故障（对外公开的原因是系统崩溃）而被迫停市半天，造成

直接经济损失和社会影响。6）北京首都国际机场 7 月 23 日 11 时 15 分至 12 时 30 分信息系统出现故障（民航总局调查后公开的结论是离港系统前端的电脑软件发生内部文件冲突），出港旅客无法办理登机手续，由于故障发生时正是航班密集时段，造成 100 多个航班延误，1 万多名旅客滞留机场。

（3）电脑病毒泛滥、黑客攻击频繁

我国在“9.11”事件发生之后，也受到了全球信息安全领域大气候的影响和感染。2002 年我国的政府及商业网络与信息系统遭受了来自国内外电脑病毒（如“尼姆达”、“蓝色代码”、“红色代码”、“将死者”、“求职信”等）的侵袭；信息安全意识不足和保护措施强度不够的普遍现象使黑客攻击事件比去年略有增多。据专业部门统计，我国与互联网相连的网络管理中心 95%都遭到过境内外黑客的攻击或入侵，攻击和入侵从原来只光顾大型网站转为也捎带攻击毫无防备的普通个人用户，信息安全问题波及的范围由原来专业计算机用户扩大到整个国家和普通大众，网络与信息安全已成为现实问题。

（4）网络安全现状难以令人满意

信息安全意识不足和保护措施强度不够以及缺乏内部有效管理机制是信息安全问题频出的主要原因。由于信息安全意识淡薄、信息安全技术和管理机制欠缺等种种原因，国内相当部分的行业和网民对信息安全问题缺乏足够重视，或因安全需要花费代价而干脆不采取任何防范措施，或只限于安装防火墙或防病毒软件。2002 年 1 月 CNNIC 调查结果显示：在网上用户主要采取的安全措施中防病毒软件 78%，防火墙 64.6%，密码加密 27.3%，电子签名 4.1%。另外，31%的用户认为目前网上交易存在的最大问题是网络和信息的安全性得不到保障；在过去一年内 63.3%的国内互联网用户被黑客入侵过；用户对目前网络的安全状况感到非常满意的仅占 0.9%。信息安全专家人士普遍认为：尽管这些年来网络等信息安全问题得到了越来越多的重视，但我国重要网络应用系统普遍不设防的状况并未见根本改变。

1.2 2002 年国内信息安全问题的新特点

2002 年国内发生的网络与信息安全事件彻底改变了我国的信息安全状况，综合分析 2002 年的这些事件，可以初步归纳出以下特点：

（1）信息安全事件从互联网扩大到基础网络

自 1995 年互联网进入中国以来，围绕病毒传染、黑客攻击和内容管理的网络与信息安全工作绝大部分是针对互联网环境的，今年发生的现实安全事件却更多的是针对通信卫星、有线电视网、电话网和行业基础网络（如机场业务系统和证交所信息系统）等基础设施的恶意干扰和破坏，这对我国的网络与信息安全而言是一个十分严酷的挑战。经过近十年的飞速发展，我国的基础网络已非常庞大（通信网络的规模容量已跃居世界第一位），过去通信基础设施（如发射器、天线、光缆等）有专人巡查和看守的安全措施已经难以维持，基础网络的安全运行和确保畅通将是日益重要的现实问题。

（2）从个别人的好奇发展到有组织犯罪

以前，无论是破坏力极大的恶意代码制造者，还是轰动一时的网络黑客，大多都是

怀有强烈好奇心和表现欲的技术高手，这类人员数量非常有限。过去发生的网络安全事件大多是出于对网络技术的好奇心和对某些敏感问题表达正义感而制造的麻烦。今年多起事件的性质都是严重的刑事案件，是经过精心策划的、有组织有预谋的网络犯罪。现在年轻一代对信息技术的掌握程度普遍加深，而且黑客自动工具在网上随便下载，使得普通人甚至不必掌握高深的黑客技术，就可以发动攻击和入侵。同时，信息系统用户麻痹大意、水平有限，信息系统漏洞频出，留下各种可乘之机。加上社会问题增多，网络社团力量壮大，邪教势力和恐怖组织日益狡猾，敌对势力越来越意识到信息技术的“两用特征”，使得有组织的网络犯罪日益增长，给国家管理和社会稳定带来隐患。

（3）从间接的损害发展到直接的破坏

2002 年前网络与信息安全事件的损害方式主要以“黑网页”、“改内容”等为主，由于破坏者的力量和关注的范围均有限，加上我国信息化水平不高，近年来绝大多数信息安全问题造成的只是间接影响。2002 年的安全事件有一半多是直接的人为破坏，而且是直接对网络设施的物理性破坏，如切断线路、干扰转发器等。这些破坏行为与过去的网络黑客相比已有了本质的变化。

（4）从局部影响发展到广泛的影响

过去发生的网络与信息安全事件以黑网页和死机为主要表现形式，其结果往往只能影响到一个部门或一个局部网络。2002 年的安全事件不仅影响到了国民经济的正常运行，而且干扰了国家管理和社会稳定，尤其是鑫诺卫星受攻击事件和重大业务系统出现技术故障影响到了社会的方方面面，造成了极其广泛的负面影响，从而使网络与信息安全问题真正成为一项国家大事，引起党和国家的高度关注。

（5）从少量损失发展到高额的代价

无论是病毒感染、还是网页被黑、抑或是系统死机，传统的网络与信息安全事件所造成的直接经济损失均比人们想象的要低，要防范和对抗这些安全攻击的成本也相对较低。这也是网络与信息安全意识一直不强的现实原因之一。2002 年的安全事件彻底改变了这种“旗鼓相当”的规则，无论是人为破坏，还是技术故障，均需要我们付出相当昂贵的代价。据粗略估计，2002 年为防范和应对网络与信息安全问题，我国付出的代价是攻击者的数百倍之多，网络与信息安全的不对称性表露无余。

可以说，2002 年的网络与信息安全事件将彻底改变中国对网络与信息安全的认识和策略，这些活生生的威胁和挑战不仅极大地刺激了政府对网络与信息安全的管理，而且也会极大地震撼中国信息安全产业界和学术界的看法和思路，尤为重要的是，这会极大地促进全社会对网络与信息安全问题的重视和关注。从这个意义上说，2002 年的信息安全问题对刚刚开始的政府信息化进程不啻是一件好事。

2. 2002 年国内信息安全管理的重要举措

针对我国信息化发展尤其是电子政务发展中存在的信息安全隐患，中国政府在大力推进电子政务建设的同时，将信息安全作为重点工作之一，从总体规划和跨部门协调等方面采取了一系列举措：

2.1 高度重视网络与信息安全工作，紧急出台相应的管理政策

2002年我国先后发生的多起网络与信息安全事件引起了党和国家的高度重视，2002年7月初召开的第二次国家信息化领导小组会议决定加强国家网络与信息安全的协调工作。针对国内出现的一系列重大信息安全事件所带来的严峻的信息安全形势，国家从管理的角度就涉及网络安全、互联网内容安全、网吧治理、非法经营 IP 电话以及有线和卫星电视等几个方面的信息安全问题紧急出台了相应的信息安全管理政策，大大加强了信息安全管理的力度。2002年国内出台的重要管理政策有：

4月，广电总局《有线广播电视传输覆盖网安全管理办法》；

5月，文化部《关于加强网络文化市场管理的通知》、信息产业部《互联网上网服务营业场所管理办法》；

6月，信息产业部《建立卫星通信网和设置使用地球站管理规定》、《国际通信出入口局管理办法》、《国际通信设施建设管理规定》；

8月，信息产业部、公安部《关于清理整顿卫星通信网和地球站的通告》；国家新闻出版总署、信息产业部《互联网出版管理暂行规定》。

2.2 开展专项治理工作，加大信息安全管理力度

在国家政策的指导下，各主管部门开展了一系列网络与信息安全专项治理工作：

（1）加强对网吧的专项安全治理

网吧作为普及互联网和推动信息化的有效方式在近几年得到了很快发展，但由于疏于安全方面的管理，不良信息内容通过网吧自由泛滥，使网吧似乎成了“游戏+聊天+色情”的代名词，弄得“家长操心、教师烦心、学校忧心”，不少家长已视之为“精神鸦片”，社会普遍呼吁整治网吧。2002年6月16日北京“蓝极速”网吧大火烧死24人的重大事件震动了全国，文化部、公安部、信息产业部和国家工商总局从2002年6月29日起对“网吧”等互联网服务营业场所进行专项治理，重点取缔非法经营的“网吧”，并于10月1日前对现有网吧予以严格的重新登记工作。四部局联合发布的文件规定，向未成年人开放的“网吧”，不得容留未成年人夜间上网；不得经营含有色情、赌博、暴力、愚昧迷信等不健康内容的电脑游戏；不得制作、复制、传播有害信息。违反规定者将被从严处罚，直至吊销经营证照。

截止2002年10月底，针对网吧的专项治理工作达到了预期的效果。

（2）加强对互联网不良信息内容的安全治理

2002年10月15日开始，由公安部牵头组织，文化部、信息产业部、教育部等8个部委，部署互联网内容安全的整治工作，并组成联合检查组再次对10个省市进行全面检查，依据分工负责制度、许可制度、总量布局调控和最低标准制度、区位禁入制度、立项审批制度、局域网接入制度、非网络游戏禁入制度、技术监控制度和场内巡查制度、未成年人禁入制度、限时营业制度、上网登记制度、责任追究制度和限期禁入制度进行检查，强化互联网有害信息以及互联网经营场所专项治理，取得了良好的效果。

（3）对非法经营 IP 电话的专项治理

《中华人民共和国电信条例》明确规定，未取得电信业务经营许可证，任何组织或者个人不得从事电信业务经营活动。但仍然有少数单位和个人未经国家通信主管部门批准擅自从事 IP 电话经营活动，制作、出售 IP 电话卡，扰乱了电信业务市场的正常秩序。更有甚者，有的不法分子利用 IP 电话传播不良信息，骚扰政府机关，干扰他人正常生活，引起了社会公愤，滋生了新的安全问题。为了保护国家的整体利益，维护电信业务市场的正常秩序，信息产业部、公安部等相关职能部门纷纷公布了制止非法经营 IP 电话的通告，各地通信行业管理部门将对 IP 电话业务市场加强了市场监管，对非法经营 IP 电话业务的活动进行严厉打击。

（4）实施有线电视和卫星通信网络安全的专项治理

针对 2002 年有线电视网络受到“法轮功”邪教非法插播的事件，国家广电总局加强了对有线电视网络的安全管理，增强技术防范措施，建立网络安全监控机制，以确保广播电视的安全播出、安全输出和安全运行。国家广播电影电视总局于 2002 年 4 月 3 日发布了第 13 号局长令《有线广播电视传输覆盖网安全管理办法》，具体规定了全国乃至地方各级有线广播电视传输覆盖网安全管理工作，国家广电总局还发出了《关于迅速建立健全广播电视宣传监督管理机制的通知》，加大对广播电视宣传网络的安全监督。

近年来，我国卫星通信事业发展迅速，在公众通信、专用通信和广播电视节目传输等方面得到了广泛应用。但是，未经审批，擅自设置、使用卫星通信地球站，擅自改变地球站特性和所使用的卫星，甚至随意向与其工作无关的卫星发射信号的行为时有发生，严重干扰合法用户的通信业务，扰乱通信秩序，影响社会安定。由于卫星电视接收设施的专项治理工作关系到社会稳定、信息安全和舆论导向，情况复杂、涉及面大，为打击违法、违规设置地球站和使用卫星转发器的行为，消除有害干扰，维护合法用户和群众的权益，今年根据国务院专门颁布的《卫星电视广播地面接收设施管理规定》，相关部门如工商、海关、公安等一系列部门携手全面开展卫星电视接收设施的专项治理工作，有关部门还专门发布了“全国范围内对卫星通信网和地球站进行清理整顿的公告”，重点打击非法生产、销售、运输、安装卫星电视接收设施的违法犯罪活动。

2.3 加强和健全国家信息安全保障体系的建设

2002 年 7 月 3 日，中共中央政治局常委、国务院总理、国家信息化领导小组组长朱镕基主持召开国家信息化领导小组第二次会议强调，要高度重视信息安全保障体系建设。坚持一手抓信息化，一手抓网络信息安全。要改进技术手段，全面强化管理，建立健全信息安全保障体系和防范机制。

国务院信息办积极组织对国家信息安全保障体系的研究工作，信息安全保障体系的思想和思路在各部委、各地方的信息化建设中得到广泛重视，并逐步开展探索和实践。

2.4 加强信息安全标准建设

经国家标准化管理委员会批准，全国信息安全标准化技术委员会（简称信息安全标委会，TC260）于 2002 年 4 月 15 日在北京正式成立。该标委会的成立标志着我国信息安全标准化工作步入了“统一领导、协调发展”的新时期。信息安全标委会协调各有关

部门，本着平等、公开、协商的原则组织信息安全标准的研究等，向国家标准化管理委员会提出本专业标准化工作的方针、政策和技术措施的建议，以信息安全标准体系为工作依据，有步骤、有计划地进行信息安全标准的制定工作。

2.5 部署网络与信息安全应急工作

对先后出现的网络与信息安全事件，我国政府十分重视，国家信息化领导小组果断决策，统一部署了国家网络与信息安全协调应急工作；根据“谁主管，谁负责，谁经营，谁负责”的原则，加强了对互联网内容安全、广电网播出安全、基础通信网传输安全、重要应用系统运行安全等方面的保护；各部门领导高度重视，在制定预案、采取措施、实行演练、抽查检查等方面狠抓落实，综合利用国家的制度优势和群众力量，发挥专家队伍的作用，进行社会动员，开展群防群治。在很短的时间内迅速建立起行之有效的安全应急体系，并最终取得了网络与信息安全应急工作的胜利。

3. 2002年国内信息安全科研、市场及投资情况

3.1 信息安全技术应用的进展

从我国信息安全技术应用的整体情况看，以下五个方面的进展在2002年较为明显：

（1）安全策略趋向合理化

近年，尤其是“9·11”事件发生之后，安全策略日趋走向合理化，具体表现在以下几个方面的转变：一是传统的静态措施已经不能满足高度网络化的需求，静态防范开始向动态防护转变。二是局部网络化的集中安全管理向分布式安全管理转变。三是由本单位信息系统管理人员负责安全问题向职业化安全外包的解决方向转变。四是理论性探讨向实用性转变。过去的讨论基本都建立和立足于理论探索，例如安全分为机密性、完整性、可用性等，目前这种方式已经向比较实用的安全解决方案过渡。一些理论薄弱但确有实际效用的技术在现实中得到应用。五是从被动防范改变为积极防御。近年网络攻防技术尤其是黑客群体的发展使得在技术和产品开发上越来越注重积极防御，而不是一味被动防范。六是从基于特征转变到基于行为。改变原先的特征分析方法，即通过收集黑客攻击或病毒的各种特征进行分析以抵御安全事件的发生，采取基于行为的防范手段，通过发放安全通行证和合格证的方法预防安全事故于未然，事实也证明该种手段非常有效。

（2）边界控制仍然是产品和技术发展的主流

边界控制就是在内部网和外部网之间实施的安全控制，主要有三类：访问控制（AC）；行为控制（BC）；内容控制（CC）。访问控制主要指防火墙和网络隔离设备。行为控制方面，主要是控制网络访问的行为，例如入侵检测系统（IDS），呈现硬件化、高速化、智能化以及分布式趋势。内容控制更为复杂，除了传统的防病毒，还包括对恶意代码的过滤及对不良信息内容的处理，这些以前均依赖于特征分析，目前则发展到定位于基于行为或语意分析，此外关于语意学的研究和网络行为的研究也支持这方面的技术进步。国内外已经有这方面新的技术出现，有望到2003年转化到产品里去。

（3）网络取证，炙手可热

由于网络犯罪现象越来越多，安全问题日趋复杂，执法部门不得不面临如何处理网络犯罪这一现实性很强的问题。由于网络是高度技术化的产物，因此，取证技术对于执法部门打击网络犯罪就变得至关重要，并在近年以及未来的两年内始终成为一个热点领域。取证技术具体包括磁盘调查、网络取证，包括电子邮件或者互联网以及源代码等，关键的问题是如何从网络上收集到相应的能够表明是犯罪证据的信息，以及怎样从大量的信息流里，获得支持打击犯罪所需要的信息。

（4）3A 技术发展迅速

3A 技术是指授权、认证和管理。网络化改变了先前的行为模式，现在不仅仅用户和用户之间需要认证，用户和设备之间，用户和应用之间，设备和设备、应用和应用之间也越来越多地需要认证。解决方案有很多，但从技术上归纳，主要包括两方面：一是采用基于密码技术，即数字签名或认证的技术方法，PKI/PMI 即属此类；二是采用相应的支持口令字的应用，以及采用专用协议。存在的技术上的难题之一是必须满足网络化的移动性，随时随地能够进行鉴别，这就需要简洁、高强度的方法，并通过软件实现移动。此外还要解决跨域的问题，要求相互之间交叉或者跨安全域、跨管理域，也能做到认证。

（5）生物识别，异军突起

近年，生物识别技术越来越多地被引入信息安全领域。尤其是“9·11”事件发生之后，许多安全防范措施中都加入了生物识别方法，例如用于飞机场安检，这对信息安全技术的发展，提供了一个良好的视角。但是，其成本较高，而且判断这些技术是否发展和进步的重要指标是根据其证实率和证伪率的高低。目前的技术应用受到了终端设备的限制，终端设备，如摄像头或指纹的识别系统，须将用户数量控制在一定的范围内，才能进行准确的探测，如若对上万、上亿个用户进行测试，则误报率会相当高。虽然存在上述缺陷，生物识别仍具有广阔的市场前景和发展空间。预计这类技术，将不仅仅用于飞机场安全保障以及敏感部门的门禁控制，将会很快打入信息安全领域，作为识别终端用户的有效手段。

3.2 国内信息安全的热门技术

相对于引人注目的信息安全问题和事故，信息安全技术在 2002 年内显得有些低沉。但这并不表明技术领域的萎靡不振，相反，2002 年的网络与信息安全事件，使得以下几种技术成为本年的“热门”：

（1）广电网络安全技术：包括保障广播电视节目在各种信道上安全传输的技术、广播电视网络运行安全监测技术、无线电信号干扰源的监测与定位技术、视频终端用户的条件接收技术等。

（2）高速、大规模 IDS 技术：包括针对基础骨干网络环境的信息捕获技术、高复杂性的网络行为与特征的分析技术、高速和大容量背景下的信息统计技术以及百兆、千兆相结合的综合性入侵防范技术等。

（3）防 DDoS 技术：包括防范大规模分布式拒绝服务攻击的技术和防范采用 DDoS 的方法大规模发布垃圾邮件和不良信息的技术。