计算机百科知识

计算机网络安全

(九)

本书编写组　编

山东科学技术出版社

图书在版编目(CIP)数据

计算机百科知识/本书编写组编．—济南：山东科学技术出版社，2003

ISBN 7-5331-1651-8
Ⅰ．计… Ⅱ．本… Ⅲ．计算机网络—基本知识—汇编
Ⅳ．TP39
中国版本图书馆 CIP 数据核字(2003)第 004271 号

山东科学技术出版社出版发行
(济南市玉函路 16 号 250001)
全国各地新华书店经销 莒县新华印刷厂印刷
开本：787×1092 1/32 印张：240 字数：4 000 千字
2003 年 7 月第 1 版 2003 年 7 月第 1 次印刷
印数：1～1 000 册
书号：ISBN 7-5331-1651-8/D·112
定价：698.00 元

目 录

计算机犯罪侵害客体之再研讨

计算机犯罪在我国 1997 年新修订的刑法典中确立，规定在妨害社会管理秩序罪一章的扰乱公共秩序罪一节中。计算机犯罪尽管在刑法上确立了，但确实也对传统刑法的某些领域产生了冲击，并且用规范“原子世界”的立法理论制定规范“比特世界”的法律原本不可避免地就带有缺陷。本文从立法现状、立法原意对我国计算机犯罪侵犯客体进行剖析，对计算机犯罪侵犯客体进行了再研讨。

就像托夫勒所说，当未来以一种人们所预料不到的速度和形态出现时，他们对所接触到的各种“新、奇、快”的东西，会产生剧烈的心理反应，他把这称为“冲击”，也可以叫做“震荡”。计算机的特性使得用传统刑法的理论对计算机犯罪进行规范必然会带来对传统刑法的冲击。尼古拉?尼葛洛庞蒂在《数字化生存》中谈到：“我觉得我们的法律就仿佛是在甲板上吧嗒吧嗒挣扎的鱼一样。这些垂死挣扎的鱼拼命喘着气，因为数字世界是个截然不同的地方。大多数法律都是为了原子世界，而不是为了比特世界而制订的。”尼古拉尼葛洛庞蒂所说尽管有些绝对，但这也给我们提出了一个不得不面对的现实：由于计算机世界与现实世界的不同，计算机犯罪尽管在刑法上确立

了，但确实也对传统刑法的某些领域产生了冲击，并且用规范“原子世界”的立法理论制定规范“比特世界”的法律原本不可避免地就带有缺陷。这些缺陷不可避免地引起了一系列地争论。本文从计算机犯罪侵犯客体的归属的角度进行剖析。

计算机犯罪在我国 1997 年新修订的刑法典中确立，规定在妨害社会管理秩序罪一章的扰乱公共秩序罪一节中。关于计算机犯罪归于哪一章、节，有很多争议，有的建议列入危害公共安全罪一章中，还有的建议单列，甚至有人建议另立计算机犯罪法。这些争议并非简单的对计算机犯罪归属的争议，而是涉及计算机犯罪客体的内容和一系列同计算机犯罪客体有关问题的解决。包括非法侵入计算机信息系统罪保护对象之外延、以计算机为犯罪工具实施的犯罪之定性、制作、传播计算机病毒等破坏性程序罪的犯罪形态、计算机犯罪的刑事责任年龄、计算机犯罪刑罚轻重的规定等当前计算机犯罪争议较大的一些问题的解决。那么计算机犯罪侵犯客体到底是什么？

对于计算机犯罪客体的研究有必要从立法原意上来分析。有关计算机犯罪法条的最初起草单位——公安部修改刑法领导小组——在小组办公室所颁布的《危害计算机信息系统安全罪方案》中就重点强调

计算机信息系统安全问题。计算机信息系统安全主要是指计算机的物理组成部分的安全性、信息系统的安全性和计算机信息系统功能的安全性。我国规定的计算机犯罪是对后两种安全特别保护。信息安全保护主要针对信息的完整性、可用性和保密性，防止非法使用、更改,防止窃取、破坏,防止遗失、损害和泄露。功能安全保护主要保障计算机信息系统的控制能力、恢复能力，如防止非法存取信息，防止系统故障影响信息处理的正常工作等。由于计算机本身的脆弱性，上述安全性被破坏，就会导致：服务可能被拒绝，计算机资源可能被滥用，数据可能被破坏，数据可能被丢失，数据可能被窃取等。自问世以来至今仅仅半个世纪，计算机经历了好几代。第四代集中解决了可用性问题，随之大力开发各种各样应用软件，计算机应用得以深入到社会各个领域。正是由于计算机应用日益广泛和深入，它已经并将汇集人类社会的财富、机密和智慧于一体，成为现代化社会的基础和支柱。在解决了性能可靠性、准确性和适用性之后，安全性又成为一个新的大难题。我国把计算机犯罪限定在计算机信息系统安全上，这不能不说是必要的。2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过的《全国人民代表大会常务委员会关于

维护互联网安全的决定》明确阐明了立法的背景和目的。目的就是：兴利除弊，促进我国互联网的健康发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益。而当前的计算机界的问题主要是安全问题。当前的背景是：我国的互联网在国家大力倡导和积极推动下，在经济建设和各项事业中得到日益广泛的应用，使人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化，对于加快我国国民经济、科学技术的发展和社会信息化进程具有重要作用。同时，如何保障互联网的运行安全和信息安全问题已经引起全社会的普遍关注。根据这一明确的表述，我国刑事法律对计算机犯罪规制出于对计算机安全保护的目的再次得到印证。

犯罪对象是计算机信息系统、计算机信息系统数据和应用程序、计算机信息系统功能。计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目的和规则对信息采集、加工、存储、检索等处理的人机系统。从概念上分析，计算机信息系统的内涵包括（1）计算机信息系统是在一定计算机硬件、软件、数据和各种接口等实体上生成的。（2）这些实体是按照一定的应用目的和规则组织起来。（3）计算机信息系统具有特定的功

能：采集、加工、存储、检索信息等功能。所谓采集，是指在数据处理中，对要集中处理的数据进行鉴别、分类和汇总的过程；所谓加工，是指计算机为求解某一问题而进行的数据运算，也叫数据处理。所谓存储，是指将数据保存在某个存储装置中，供以后取用；所谓传输，是指把信息从一个地点发送到另一个地点，而不改变信息内容的过程。所谓检索，是指计算机从文件中找出和选择所需数据的一种运作过程。计算机安全保护条例第 5 条第 2 款规定，未联网的微型计算机的安全保护办法另行规定。可见，最初保护计算机安全是对联网的计算机着重考虑的，1997 年修订的刑法中计算机犯罪的侵害对象也是联网的计算机信息系统。但 1998 年公安部关于未联网的微型计算机信息系统是否适用《刑法》第 286 条的请示的批复（1998 年 11 月 25 日公复字[1998]7 号）把未联网的微型计算机信息系统也纳入了第 286 条保护范围之内。计算机信息系统数据在广义上是指存储于计算机系统中的所有信息，从狭义上讲是指存储于计算机系统中的除计算机程序以外的一切信息资料，也就是那些由计算机系统所有者及用户采集的并输入计算机系统的，并非系统本身运行所不可缺少的信息。《计算机软件保护条例》第 3 条规定了计算机程序的概念，是指为

了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列或符号化语句序列。应用程序就是操作系统程序以外的，为特定目的而设计、编写的具有某种特定用途的程序。应用程序包括与系统联系紧密能影响系统功能和由系统支持才能运行的自身不影响系统功能的应用程序两种。前者有些是组成系统的最重要的部分，遭到破坏会影响整个系统的功能，后者遭到破坏不会影响整个系统功能。我国对于应用程序没有做这一区分。

综观世界各国的计算机犯罪立法，计算机犯罪侵犯的客体种类主要有：(1)财产类。这类计算机犯罪主要是指：A、窃取类。此类是指：利用计算机盗窃金钱、财产等和有价值的数据。如美国《概括犯罪规制法》及《伪造存取手段与计算机欺诈与滥用法》规定的“从计算机获取机密情报罪”及“从计算机获取金融或信用情报罪”；德国刑法第 202 条规定的“刺探资料罪”(“探知数据罪”)；英国 1984 年《资料保护法》规定的“非法获取计算机中已申报保护的个人资料罪”等等。B、破坏类。此类是指：改动或毁坏计算机的信息和文件也属于此种类型。如我国刑法第 286 条规定的计算机犯罪。第 286 条规定：违反国家规定，对计算机信息系统功能进行删除、修改、增加、

干扰，造成计算机信息系统不能正常运行，后果严重的，处 5 年以下有期徒刑或者拘役；后果特别严重的，处 5 年以上有期徒刑；违反国家规定，对计算机信息系统中储存、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚；故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。(2)计算机信息系统安全类。如我国刑法第 285 条规定的“非法侵入计算机信息系统罪”是指未经允许非法使用计算机及与计算机有关系的设备；法国的“侵入资料自动处理系统罪”等。(3)伪造、诈骗类。比如利用计算机或计算机网络进行的欺骗活动。包括骗取情报信息及数字财产等,如德国的“计算机欺诈罪”、英国的“伪造文书罪”等。我国的计算机犯罪行为只有上述行为中第一类和第二类，主要是第二类。第一类破坏财产，即“改动或毁坏计算机的信息和文件”“未经允许非法使用计算机及与计算机有关系的设备”也是从计算机信息系统安全的角度规定的，所以确切地说，我国计算机犯罪只有指第二类。而“利用计算机盗窃金钱、财产等及有价值的数据”和“利用计算机或计算机网络进行的欺骗活动”不属于计算机犯罪，按照传统刑法定罪处罚。根

据以上分析可知，我国刑法中计算机犯罪重点是保护计算机信息系统安全，我国计算机犯罪的客体是计算机信息系统安全。

从我国计算机犯罪确定的现实情况来看把计算机犯罪侵犯的客体确立为计算机信息系统安全是合理的。这一犯罪客体的确立是同计算机的发展阶段相适应的，同我国以及世界各国的应用计算机的目的相适应的，同计算机领域目前以及今后可能出现的危害重点相适应的。计算机犯罪是与社会的发展阶段相联系的一种犯罪，始于 20 世纪 40 年代末，也就是说计算机开始进入社会就引发了计算机犯罪案件。但在 60 年代，“财产”和“隐私”的概念还没有进入计算机空间，计算机还不是社会所不可或缺的东西。那时还没有多少用以储存专有信息的数据库，当然也就谈不上对数据库的非法拷贝、销毁、篡改和破坏了。最初计算机的使用权掌握在特权人物手中，应用的领域也是很窄的，上述的计算机犯罪的条件不充足，所以，计算机多是作为犯罪工具实施传统犯罪出现的。比如在美国 1958 年实施直到 1966 年 10 月被发现的有关计算机滥用事件，是世界上第一例受到刑事追诉的计算机犯罪案件。此案中犯罪分子就是利用计算机作为犯罪工具。70 年代计算机犯罪迅速增长，1971 年美

国正式研究计算机犯罪和计算机滥用事件，此前只有零散的调查研究报告。80 年代计算机犯罪形成威胁，各国纷纷立法加以规制。90 年代以来计算机在多媒体技术和网络技术的支持下应用领域越来越广泛，人们对计算机的依赖越来越大。随着社会的网络化，计算机犯罪的对象从金融犯罪到个人隐私、国家安全、信用卡密码、军事机密等等，无所不包。而且犯罪发展迅速，黑客攻击越来越频繁，危害也越来越大。根据美国官方人士称，近年来企图闯入五角大楼计算机系统的“黑客”多达 25 万人次，其中有 65%即 16.25 万人次获得成功。这些闯入者对防务造成的麻烦，需要花数百万美元才能消除。

计算机的通用性使今天计算机广泛应用于各个领域成为可能，其广泛应用又使世界各国普遍对计算机产生很大程度上的依赖。在信息化社会中，计算机信息系统将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。社会对网络下的计算机信息系统的依赖也日益增强。各种各样完备的计算机信息系统，使得秘密信息和财富高度集中于计算机中。另一方面，这些计算机信息系统都依靠计算机网络接收和处理信息，实现其相互间的联系和对目标的管理、控制。而随着网络的开放性、共享性、互连

程度的扩大，网络的重要性和对社会的影响也越来越大人们对其的依赖性就越来越强。而计算机的脆弱性等缺陷使得计算机信息系统极易遭受破坏，这种破坏在网络环境下会在极短的时间内扩大到全球。无论是黑客攻击还是破坏性程序，它们本身就具有极大的破坏性。比如计算机病毒。1989 年 4--5 月间,我国西南铝加工厂发现了首例计算机病毒——小球病毒。该病毒的发作破坏了该厂近 5 年的数据信息,造成了巨大的经济损失。随着计算机技术的高速发展,计算机病毒也开始以每天2--3种的速度产生,目前计算机病毒在国际上已达到 36 万多种， 并且已经有“病毒生成器”这样的软件,它可以迅速地产生病毒。现实中，计算机信息系统安全极其脆弱。据美《时代》周刊报道，美国防部安全专家对其挂接在 Internet 网上的 12000 台计算机系统进行了一次安全测试，结果 88%入侵成功，96%的尝试破坏行为未被发现。美国每年因信息与网络安全问题所造成的经济损失高达 75 亿美元，企业电脑安全受到侵犯的比例为 50%，美国防部全球计算机网络平均每天遭受两次袭击的有关报道就足以说明对于计算机信息系统安全保障的重要性。正如尼尔·巴雷特所说：“各种各样的安全性防范措施已经存在，从塞恩组织者（Psion organisers）

中的文件口令的使用到克勃罗斯环系统（Kerberos-based token system）在大型计算机网络的应用。任何的黑客和数字化犯罪都是通过破坏系统的安全性而达到目的的。”我国计算机信息系统的安全形势也是很严峻的。法新社 1998 年 8 月 1 日报道：美、英、加、中、法、日六国在网络安全方面受到威胁最大，中国列第四。随着计算机的连接越来越多，网络安全也面对越来越大的挑战。在这种背景下，说计算机信息系统的安全是我国的计算机犯罪的客体无论从实际立法还是现实需要都是准确的。

反计算机犯罪效果差的原因剖析

反计算机犯罪就是指对计算机犯罪预防和打击的总称。通过反计算机犯罪活动所获得的收益就是“反计算机犯罪收益”，也就是反计算机犯罪成本投入之后的产出减去成本支出的差额。目前，虽然世界各国加大力度，增加经费来预防和降低计算机犯罪，即实施了反计算机犯罪的活动，但计算机犯罪还是让各国损失惨重。一个很明显的事实摆在我们面前，即反计算机犯罪的收益不高。本文就从反计算机犯罪成本、立法、执法和技术四个方面进行分析，以供同仁参考。

反计算机犯罪成本投入不高

计算机犯罪给各国造成重大的损失，虽然各国都采取相应的各种措施预防和打击计算机犯罪，但在成本方面投入还是不多，主要表现在：

1．对计算机犯罪的犯罪分子惩罚不高。

JamesA。SchweltzeR 在他的《计算机犯罪和商业信息》中一针见血地指出：“计算机犯罪本身就是法律不力造成的恶果”。在计算机犯罪中，罪犯多数以获取钱财为目的且数额巨大。据统计：美国由于计算机犯罪而遭受损失每年达百亿美元，德国由于计算机犯罪造成的经济损失每年也高达 150 亿马克，相当于国民生产总值的 1%。但对计算机罪犯的处罚上，从现有的法律和相关的案例来看表现为财产刑很低，生命刑、自由刑偏轻，资格刑几乎没有，法定惩罚成本不高使得对计算机罪犯的惩罚有些法不责众。蠕虫病毒导致美国军事基地和国家航天航空局的 6000 多台电脑全部瘫痪，给美国造成直接经济损失近一亿美元，而 1990 年 1 月 22 日联邦法院判处制造者莫里斯 5 年监禁和 25 万美元的罚款。凯文 v 密特里，他是第一个闯入美国国防部网络系统的黑客。他在 1987 年 12 月使用非法的信用卡盗窃了加州的一个软件公司的软件，给这家软件公司造成几乎毁灭性的打击，而

他本人只判了 36 个月的缓刑。

2．动员全社会参与反计算机犯罪的投入不多

反计算机犯罪在一定程度上还要依靠全社会网民的参与，由于计算机犯罪的跨国性等特点，必然要求对计算机犯罪的打击和预防是一项“全民事业”。但是在现实中，对于计算机犯罪的危害、预防的宣传不够，没有得到公众的理解和支持，造成反计算机犯罪措施的不力。计算机犯罪的实施者大都是网络上数一数二的高手，被人们称为“网络英雄”并极力加以推崇和模仿。公众对计算机犯罪也是十分的大度和宽容。因为计算机犯罪没有直接的人员伤害，损失的大都是政府和公司的财产，而且会有人认为这不是犯罪，而是安全系统的工作没做好。而且对于计算机技术和知识方面的天才，惩治当然不能太过分。这些不正常的现象在很大程度上刺激了犯罪分子为了“英雄事业”而“鞠躬尽瘁，死而后已”。

3.预防计算机犯罪的成本投入低，尤其是网络安全的维护成本低下。

在我国电脑应用单位 80%未设立相应的安全管理组织，58%无严格的调存管理制度，59%无应急措施，48%无事故发生后的系统恢复方案。对网络安全意识的落后和安全维护同投入的低廉使得计算机罪犯有

恃无恐。

但所谓网络安全是一种相对的安全，而且安全系数越高，付出的代价就越高，就越多的消耗网络资源或者限制网络资源的使用，网民就越觉得受到限制。尽管这种灵活、高效的抑制措施不可避免的加大了应用成本，而且还极有可能防护不了，但是面对各式各样的计算机犯罪，尤其是侵害计算机信息系统的犯罪，只有不断的加强对网络安全的维护才能一定程度的预防。

立法方面

1．立法滞后，无法可依。

法律的相对稳定性和技术的飞跃性在短时间内难以达成平衡，表现在立法滞后特性上。对诸如无国界犯罪的管辖权问题、犯罪行为人低龄化的问题、法无明文不为罪的问题、证据的取得和认定问题等等，世界各国都程度不同地存在着困惑。

比如我国现行的《刑法》规定处以刑罚要满 16 周岁（除了故意杀人罪、故意重伤至人死亡罪等以外），而计算机犯罪一个很明显的特点就是低龄化趋势严重。按照我国刑法，计算机罪犯即使造成很大的损失，甚至是不可弥补的，但因为未达到刑事责任年龄不能对其处罚。再比如，现行的法律对某些计算机

犯罪量刑尺度过轻。我国刑法第二百八十五条规定“违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。”对这种危害国家安全、影响社会稳定的计算机犯罪才处三年以下有期徒刑或拘役，显然属量刑过轻，对此应该加以修改。对未满 16 周岁却构成了计算机犯罪的，给国家、社会带来了危害，影响他人工作、生活的，笔者认为也要给以应有的惩处。而且，除了对现有《刑法》加以修改和完善外，还可增设滥用计算机罪、计算机金融资产诈骗罪、盗用计算机内部秘密数据罪等，并给出其量刑的尺度。这些都是对我国传统法律的挑战，我们只有做到立法的及时，对计算机犯罪才能“有法可依”，便于司法操作。

2．各国立法的多样，使得罪犯可以规避法律。

各国对反计算机犯罪的立法“百家争鸣”，某行为在一个国家是触犯了刑法，而在另一个国家却与法无缘，最多只是对罪犯进行舆论上的谴责的现象。比如在澳大利亚的刑法典上尚不存在“盗窃数据”的罪名。

浅谈计算机犯罪和利用计算机犯罪的异同

随着计算机信息系统的广泛建立和运用，计算机系统日益成为国家和社会中财富、信息集中的要实部

门，关系到国计民生的事务管理、经济建设、国防建设、尖端科学技术领域的计算机信息系统的安全运行；对于保障国家安全、经济发展以及人民生命财产安全等方面，起着重要作用。也正因为如此，这些系统就成为罪犯攻击的目标。如果系统一旦成为犯罪对象而被非法侵入，就可能导致其中的重要数据遭破坏或者某些重要、敏感信息被泄露，事关国家安全、经济发展等。因此修订后的刑法在第二百八十五条和二百八十六条中，规定了几种计算机犯罪，包括非法侵入计算机系统罪、破坏计算机信息系统罪。与此同时，少数犯罪分子亦利用计算机系统实施其他犯罪活动。利用计算机实施金融诈骗、盗窃、贪污、挪用公款，窃取国家秘密的犯罪活动在司法实践中越来越多，为明确利用计算机实施有关犯罪的定罪处刑问题，修订后的刑法第二百八十七条规定上述的五个具体罪名，这是根据我国目前计算机应用的具体情况而设定的。另外，犯罪分子还不断利用计算机实施其他犯罪活动。以当今世界上最流行的全球互联网络 Internet 为例，其管理者是美国，对于我国用户来说，主要是享用其信息资源。但在利用该网络时，还可能涉及到其他几个方面的犯罪，如：利用网络电子布告板免费发送软件、非法复制软件，侵犯著作权，给国家或个

人造成重大利益损失的，可以按侵犯知识产权罪中的有关规定定罪量刑；利用网络发表反政府言论、恐怖言论和从事颠覆破坏活动，可以按危害国家安全罪中的有关规定定罪量刑；利用网络传播内容淫秽的视听资料的，可以按传播淫秽物品罪中的有关规定定罪量刑。

利用计算机犯罪和计算机犯罪在犯罪形式上都是通过计算机这种载体来实施某种犯罪，都是行为人将所掌握的计算机专业知识与计算机及其相关设备相结合实施犯罪，属新型的智能化犯罪。行为人均是有较高甚至极高的操作技能和计算机专业知识，犯罪行为的技术含量较高，往往表现为多样的技术手段，两种犯罪都有较强的隐蔽性和反侦查性，行为人可在任何时间、任何地点、任何终端实施犯罪行为，往往是输入一条非法指令或简单程序，就完成了犯罪行为。由于上述犯罪行为的方法、手段、特征都极为相似，因此我们在司法实践中往往难以区分。但笔者认为它们具有实质上的区别：

1、主观故意不同。利用计算机犯罪是金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密的犯罪故意；而计算机犯罪是侵入计算机信息系统、破坏计算机信息系统的犯罪故意。

2、侵害的客体不同，利用计算机犯罪侵害的客体是国家的金融管理秩序、经济管理秩序、公私财产的安全等；而计算机犯罪侵害的客体是计算机信息系统的运行管理秩序，两者属于不同的同类客体。

3、犯罪的目的不同。利用计算机犯罪是为了非法占有公私财物、危害国家安全等；而计算机犯罪是为了扰乱计算机系统的正常运行及管理。

4、对计算机系统的操作手法和影响不同。利用计算机犯罪只是将计算机作为犯罪的工具，操作手段只是对计算机功能的某些应用，既不会影响计算机系统的正常运行状态，也不会造成系统功能的破坏，计算机系统仍能一如既往运行，完成其日常的工作。如：利用计算机进行金融诈骗、贪污、挪用公款等犯罪，行为人一般采取的是首先窃取计算机系统中各种相互关联的业务系统的操作密码（按正常程序，这些密码只能分别掌握在不同环节的人手中），当这些密码被同一个人知晓后，就相当于通过层层关口，进入了金库的大门，然后在计算机上任意调取资金，将公款或他人款项调入自行开设的帐户之中，最后即可通过正常的取款途径，实现其犯罪的目的。计算机犯罪的操作手法则不同，为了达到破坏的目的，行为人会采取各种技术手段，违背操作程序，任意删改系统功能、

删改技术数据，最终的结果是使计算机系统无法正常运行甚至瘫痪。

5、运行的环境不同。利用计算机犯罪一般犯罪分子在专业局域网中实施，计算机犯罪则一般在互联网中实施。

6、定罪量刑的依据不同。利用计算机进行犯罪的，应当分别依照修订后的刑法有关金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或其它犯罪的条款，进行定罪量刑；计算机犯罪则应依照修订后的刑法第二百八十五条和第二百八十六条的规定定罪量刑。

笔者认为，利用计算机犯罪与计算机犯罪在管辖权的确定，犯罪的既遂与未遂，竞合与牵连犯罪等方面亦存在诸多可探讨之处。本文只起抛砖引玉作用。

美国计算机犯罪活动剧增

据美国联邦调查局和美国计算机安全研究所 12 日公布的一项有关计算机犯罪 情况的调查报告显示，美国的计算机犯罪活动剧增，使美国公司和政府部门蒙受巨额经济损失。

这是联邦调查局和美国计算机安全研究所发表的关于计算机安全的第六次年 度报告。有 538 家美国公司、政府机构和大学接受了调查，85%的受调查者称曾遭到计算机攻击，其中有 64%因此蒙受经济损

失。

调查报告称，168 家受调查的公司和部门所遭受的损失总数高达 3.78 亿美元。在去年的调查中，249 家公司和部门报告说它们蒙受了 2.49 亿美元的经济损失。专 家指出，由于受调查的公司和部门出于保密等原因大多不愿意透露所遭受的经济损失情况，因此计算机犯罪所造成的实际经济损失要大大高于这个数目。

这次调查结果表明，计算机犯罪重点已经从来自部门内的攻击向来自因特网 的攻击转移。70%的受调查者反映曾遭到通过因特网发动的计算机攻击，而在去年 的调查中，这个比率是 59%。专家认为这是由因特网带动的电子商务活动增加的必 然结果。

调查结果还显示，造成损失最严重的计算机犯罪行为是窃取知识产权资料和 金融诈骗。

计算机犯罪的犯罪构成要件分析

计算机犯罪并非新事物，早在二十世纪四十年代，最早应用计算机的军事和科学工程领域就开始出现计算机进行犯罪的活动，只是较为罕见，未能引起人们的重视和注意。到七十年代中后期计算机在全球开始普及，随着操作系统简化、人机对话功能的增强，越来越多的人开始使用、掌握计算机，特别是进入九

十年代以后，计算机的应用领域扩展至银行、保险、航空、证券、商务等领域，计算机犯罪呈滋生蔓延趋势。所谓计算机犯罪是指行为人利用计算机操作所实施的危害计算机信息系统（包括内存数据和程序）安全和其他严重危害社会的犯罪行为。本文就计算机犯罪的犯罪构成要件进行剖析，以便更好的认清计算机犯罪。

一、计算机犯罪的主体。犯罪主体是达到法定责任年龄，能承担刑事责任能力的人。目前对计算机犯罪主体的认识众说纷纭，有的认为是特殊主体即“白领犯罪”，有的认为是一般主体，还有的认为是两者兼有。笔者对最后的观点持认同态度。计算机犯罪主体有一般主体和特殊主体构成。

计算机犯罪的一般主体，就是指达到法定责任年龄，具有刑事责任能力，实施计算机犯罪行为的人（包括自然人和法人）。计算机在计算机犯罪中一方面是作为不可或缺的犯罪工具即利用计算机操作实施犯罪，另一方面，计算机信息系统又成为罪犯的攻击对象，即计算机成为“受害者”。因此，笔者将计算机犯罪的定义为：“行为人利用计算机操作所实施的危害计算机信息系统（包括内存数据和程序）安全和其他严重危害社会的犯罪行为。”无论将计算机信息系

统（包括内存数据和程序）安全为攻击对象的犯罪还是以计算机为犯罪工具的计算机犯罪，犯罪主体并不都是特殊主体。因为大多计算机犯罪离不开两种方法：直接法和间接法。即或是行为人直接把计算机作为犯罪工具实施犯罪，实施这种犯罪行为的人当然要相当的计算机专业知识，故其犯罪主体只能是特殊主体；或是行为人通过中间人利用计算机实施的侵害计算机信息系统或其他严重危害社会的犯罪。其犯罪主体可以是一般主体。因为存在一种可能是——中间人是具备计算机专业知识的人，但是并不知道自己的行为给犯罪分子钻了空子。同时，计算机犯罪主体也包括特殊主体。计算机犯罪是一种新型犯罪，具有不同于其他普通刑事犯罪的特点，尤其是它明显地带有智能性。不论是以计算机信息系统为犯罪工具还是犯罪对象，其犯罪主体大多具备计算机专业知识，或者通过具备计算机专业知识的人员（具备计算机专业知识的人员在不知道自己的行为被他人利用时）才能实施。不可避免的，其犯罪主体有一部分是特殊主体。即“具有一定的计算机专业知识，从事计算机信息系统操作、管理、维修以及其它有关人员”。将“掌握计算机专业技术知识”作为认定计算机犯罪的特殊主体，有利于我国刑法理论进一步完善。从我国计算机

犯罪的实践来看，金融系统的很多计算机罪犯是内部人员，对计算机信息构成威胁、破坏、入侵的“黑客”在计算机技术领域中也都是佼佼者。因此笔者认为强调计算机犯罪主体的复杂性很有必要。

根据 97 年刑法第十七条第二款的规定：已满十四周岁不满十六周岁的人，犯故意杀人、故意伤害致人重伤或者死亡、强奸、抢劫、贩卖毒品、放火、爆炸、投毒的，应当负刑事责任。这也就是说，凡未满十六岁的人，只要不是进行以上八类罪的就不用承担刑事责任。我国宪法之所以这么规定：

一方面是考虑到未满十六岁的人对行为的社会危害性的辨别力不是很强.

另一方面是考虑到这些人所进行的一般犯罪的社会危害性都不是很大，因此对他们进行的一般犯罪都免除处罚。但笔者从已有的计算机犯罪案例来看，进行计算机犯罪的，有很大一部分是少年儿童，比如“少年黑客”，他们中绝大多数都未满十六岁。那么如何对待未成年人实施的这类行为呢？这将是我们所面临的新的问题。依据现有刑法，我们不能要求实施计算机侵害行为且对社会造成严重危害的青少年承担刑事责任，因为“法无明文不为罪”。但是在计算机犯罪中，只要他能够进行这类犯罪，无论是成年

人还是未成年人，他们对社会所造成的危害都相差无远。作为一名能够进行计算机犯罪的行为人，虽然他的年纪可能不大，但是他的关于计算机的知识水平都在相当的程度之上，他的能力都比较强，哪怕是未成年人。怎样对待他们的行为将是我们必须面对和解决的棘手问题。二、计算机犯罪的客体。刑法理论认为：犯罪客体是指犯罪行为所侵害的又为我国刑法所保护的社会关系。计算机犯罪的跨国性、广范围、犯罪结果的潜在性和隐蔽性等特点都使得计算机犯罪侵犯的客体变得复杂，社会危害性增大。计算机犯罪的客体是指计算机犯罪所侵害的，为我国刑法所保护的社会关系。由于计算机犯罪是以犯罪的手段和对象，不是以犯罪的同类客体为标准而划分的犯罪类型，因此计算机犯罪侵害的客体具有多样性。虽然我国刑法将计算机犯罪列入妨害社会管理秩序罪一章，但其侵害的客体不限于社会管理秩序，也涉及公共安全、公私财产所有权、国防利益等。计算机犯罪它一方面对计算机系统的管理秩序造成严重破坏，另一方面也往往会直接严重危害到其他社会利益。具体分析，计算机犯罪侵犯的是复杂客体，即计算机犯罪是对两种或者两种以上直接客体进行侵害的行为。比如在非法侵入计算机系统犯罪中，一方面侵犯了计算机系统所有

人的排他性的权益，如所有权、使用权和处置权，另一方面又扰乱、侵害甚至破坏了国家计算机信息管理秩序，同时还有可能对受害的计算机系统当中数据所涉及的第三人的权益造成危害。进行计算机犯罪，必然要违反国家的管理规定，从而破坏这种管理秩序。这是计算机犯罪在犯罪客体方面的显著特征。三、计算机犯罪主观方面刑法认为：犯罪主观方面是指行为人实施犯罪时，对其实施的严重危害社会的行为极其造成的危害结果所持的心理态度。主要有犯罪故意和过失之分，其他的比如犯罪动机、犯罪目的等也是较为重要的因素。计算机犯罪中的故意表现在行为人明知其行为会造成对计算机系统内部信息的危害破坏或其他严重危害社会的结果，他对此持希望或放任态度。计算机犯罪中的过失则表现为行为人应当预见到自己行为可能会发生破坏系统数据的后果或其他严重危害社会的结果，但是由于疏忽大意而没有预见，或是行为人已经预见到这种后果但轻信能够避免这种后果而导致系统数据的破坏。所谓明知，是指行为人在表现出来的认知水平上他所应该知道自己的行为会产生什么样的后果。只有行为人确实知道行为的后果才构成故意。计算机犯罪中对犯罪后果的预见应该区别于一般犯罪。在计算机犯罪中，并不需要行为

人对其行为的后果有很清楚的认识。只要行为人作为一个合理的小心的计算机系统使用者应当知道自己不被允许作某些行为，知道这些行为具有对数据进行破坏的可能，那么就可以认为行为人对其行为的后果有预见。而并不需要行为人对其操作具体会引起社会多大的危害、对计算机信息系统有多大的改变有清楚的认识。我们常常对看到，实际生活中有些人由于计算机知识缺乏，错误操作计算机而引起系统数据的破坏，但是这并不是行为人主观上希望发生的。这种行为我们认为同样也是出于故意。计算机犯罪的主观要件中犯罪目的和犯罪动机也是我们判断罪与非罪、此罪与彼罪的重要因素。从计算机犯罪的目的和动机来说，无论犯罪人的主观动机如何，只要其存在着犯罪的故意，就必然要以侵害计算机系统内部的数据为目的，虽然犯罪人同时还可能具有其他的犯罪目的。因此，特定的犯罪目的是计算机犯罪构成的特别要件，这也是区分计算机犯罪同其他犯罪的标志。但由于计算机犯罪的复杂性和我国相关法律法规的相对滞后性，对计算机犯罪的主观要件很难断定。实际中，许多计算机罪犯是向自己智力的挑战，对自己知识水平的检测或是为了寻求刺激或是为了维护自己的软件产品，打击盗版而使用计算机病毒，如“巴基斯坦病

毒”就是典型的一例。如何断定是不是计算机犯罪，笔者认为应该要具体分析行为人的情况，比如行为人的知识水平、行为人是否尽了谨慎使用计算机系统的义务、行为人对其行为导致的危害后果的态度和行为人是否严格遵守有关计算机系统使用的规章制度等来把握计算机犯罪的主观要件。四、计算机犯罪的客观方面刑法原理认为：犯罪客观方面是指行为人实施了什么样的行为，侵害的结果怎样，以及行为和结果之间的因果关系。计算机犯罪的客观方面是指刑法规定的，犯罪活动表现在外部的各种事实。其内容包括：犯罪行为、犯罪对象、危害结果，以及实施犯罪行为的时间、地点和方法等。在计算机犯罪中，绝大多数危害行为都是作为，即行为通过完成一定的行为，从而使得危害后果发生。也有一部分是不作为，如行为人担负有排除计算机系统危险的义务，但行为人拒不履行这种义务的行为至使危害结果发生的。从犯罪构成的客观方面来看，计算机犯罪是单一危害行为，即只要行为人进行了威胁或破坏计算机系统内部的数据的行为或其他严重危害社会的行为，就可以构成计算机犯罪。与常规的犯罪相比，计算机犯罪在客观方面具有犯罪形式的极大隐蔽性、犯罪手段的多样性和危害结果的严重性特点。在计算机犯罪的客观方面，

值得强调的是：第一，关于计算机犯罪的犯罪对象。计算机犯罪的犯罪对象是计算机犯罪所直接指向的对象。许多计算机犯罪以信息系统作为犯罪对象。该行为必然要侵害计算机系统内部的数据，这种侵害可能是直接地破坏数据，也可能是间接地威胁数据的安全性和完整性，这就必然要侵害计算机系统所有人对系统内部数据的所有权和其他权益。有些数据可能是具有价值的程序和资料，也可能是以数据形式存在的财产例如电子货币。同时计算机犯罪的犯罪对象又有很多不确定的因素。一方面，计算机犯罪随着罪犯的犯罪手段和犯罪技术的不断提高而出现出日新月异之趋势，所以它侵害的对象也不能一言以蔽之；另一方面，计算机犯罪侵害客体的复杂性、犯罪的跨国际性和隐蔽性必然导致对象的复杂性。这些必然的会对我们传统的法律法规造成很大的冲击。所以，笔者在定义中强调计算机犯罪是“利用计算机操作所实施的其他严重危害社会的犯罪行为”。也就是侵犯计算机信息系统只是计算机犯罪中的一部分。第二，关于计算机犯罪的犯罪工具问题。笔者认为计算机犯罪的工具具有唯一性和依赖性，换言之，真正意义上的计算机犯罪，计算机是实施该犯罪的唯一工具，同时，也只能利用计算机操作实施，通过其他工具不可能实施

此类犯罪或顺利达到犯罪的目的并进而构成计算机犯罪。所以笔者在计算机犯罪的定义中强调计算机犯罪是“利用计算机操作”来实施的。计算机作为计算机犯罪的工具有“不可或缺性”，以免定义的外延太大。基于以上剖析，笔者认为，由于不能正确把握计算机犯罪的犯罪构成，尤其是犯罪客观方面和客体，使得理论界对计算机犯罪的界定众说纷纭。目前较为流行的折衷型观点将计算机犯罪定义为针对计算机或者以计算机作为工具的犯罪。这一定义虽然认识到计算机本身在犯罪中的重要地位，但它将计算机的犯罪工具作用与犯罪对象人为地割裂开来，从而使计算机犯罪于无所不包。因此，真正意义上的计算机犯罪应该是指行为人利用计算机操作所实施的危害计算机信息系统（包括内存数据和程序）安全和其他严重危害社会的犯罪行为。实际上我国新刑法典及有关计算机安全的法规所规定的计算机犯罪类型的打击重点也在于此。

电子商务与计算机犯罪

20 世纪 90 年代以来，基于 Internet 的电子商务（以下简称电子商务）迅速发展起来，这种新经济模式一开始就预示出巨大的商业利润，促使世界各国纷纷全力发展本国的电子商务，我国也十分重视电子商

务建设，但是，电子商务发展毕竟发展时间很短，在技术、管理、法律规范等方面远没有成熟，存在很多阻碍电子商务发展的因素，其中包括电子商务领域计算机犯罪。

一、电子商务及其安全运营

所谓电子商务，国内外有广义和狭义两种定义。广义的电子商务，或称商业电子化，是指电信工具（包括电报、电话、传真以及互联网络等）在商务活动中的应用；狭义的电子商务是指在信息社会中，掌握信息技术和商业事务活动，不仅包括进行买卖而直接带来利润的事务，而且包括产生对产品和服务的需求、提供销售支持和客户服务、促进业务伙伴之间通信支持、利润产生的事务，如售后服务等。广义的定义给出了电子商务的基本范畴，狭义的定义更加符合电子商务的现代特征，更具有现实意义。

电子商务出现的时间不长，但发展极为迅猛，有信息表明，1996年全球电子商务市场的规模已达1500亿美元了。另据估计，到2001年，全球10％的商务将实现电子化，涉及到的商品与服务将达到6000亿美元。从亚洲市场来分析，Idc预测因特网的电子商务到2001年将以100倍的速度增长，营业额在各种销售渠道销售总额中将占有42％的份额。电子商务之

所以取得如此快速的发展，是因为它具有传统商务模式不可比拟的优点，如低廉的营运成本、广泛的客户市场、不受时空限制、交易速度快、商户和客户处理的交易手续简单、使用多媒体手段方便客户选购、与客户双向互动交流、以顾客为中心提供个性化服务等等。按照交易事务是否全部通过通信网络完成，电子商务可以分为两类，一类是不完全的电子商务，只有部分交易事务通过互联网络完成；另一类是完全的电子商务，包括商品递送在内的所有事务全部通过互联网络上完成，这类电子商务交易的商品一般是计算机数据类商品（以下简称数据商品）。按照电子商务涉及的交易方式分类，可以分为三类，即商家与消费者间业务（business to customer ）、商家与商家间业务（business tobusiness）和公共服务。

目前电子商务运作方式有多种，在其运作过程中，一般都涉及到五个直接关系主体：客户、商户、电子商务认证机构、结算机构和通信机构。通信机构提供 Internet 数据通信服务，传输其他四个主体之间的业务信息数据，甚至数据商品。客户在能够进行电子商务消费前，必须向结算机构申请用于网络支付的帐户，客户通过 Internet 浏览商户网站，确定要购买的商品服务后填写电子定购表格，并署上客户的

帐户信息，所有这些数据经加密后传输给电子商务认证机构。电子商务认证机构（certification authority,ca， 以下简称认证机构）是为交易方验证的机构，认定电子商务活动中交易方的身份、资信，维护交易活动的安全，保障电子商务交易活动顺利进行。电子商务商户为进行网上经营，不仅要具备进行电子商务的基本计算机信息处理设备设施，而且还必须在结算机构，一般是银行，有特种商业帐户，在认证机构取得从事电子商务的“身份证”。认证机构把客户传输来的信息分为两类，一类是客户帐户和认购的商品服务价格信息，另一类是商户身份证信息。前者被传输到结算机构， 结算机构确认客户帐户资金余额可以进行交易后返回肯定的信息，后者经认证机构判断后确定商户是否登记的合法电子商务商户，以及接受资金的帐户是否登记的特种商业帐户，如果判断肯定，则交易可以进行，如果以上有任何项目未获通过，则向客户和商户返回交易被拒绝的信息。交易被授权后，商户向认证机构提供电子发票，在商品、服务被交付给客户后，客户和商户向认证机构发送已经签收的数字签名，结算机构收到电子商务认证机构发送来的可以过户资金的信息后，将客户帐户中交易的资金划拨到商户帐户上，从而完成整个商品或者服

务的交易过程。

电子商务发展的核心和关键问题是交易的安全性，为保障电子商务的安全运营，人们提出安全控制要求，有信息保密性、交易者身份的确定性、不可否认性、不可修改性等，并提出安全电子交易协议（set :secure electronic transaction）等技术规范，构筑电子交易的安全体系。但是，电子商务的安全运营不仅涉及技术问题，同时也涉及管理问题和法律问题，如电子商务交易管理规则、电子商务认证机构管理规则以及涉及电子商务的刑法、民法、行政法律规范等等。我国成功交易的第一笔 Internet 上电子商务是在 1998 年 3 月 6 日，电子商务系统内机构的组合协调工作远没有完成，电子商务体系建设刚刚起步，其正常运行有待规范化，电子商务交易的管理标准还没有系统制定，电子商务法制建设尚处于摸索阶段，这表明我国电子商务建设正处于规范化过程中。但是，由于电子商务领域急剧集中了巨额社会财富，对社会生活的影响日益强大，而电子商务的安全建设才蹒跚学步，这一状况必然对各类犯罪具有巨大的吸引力，我国起步中的电子商务发展面临犯罪的严峻挑战。

二、电子商务领域计算机犯罪的表现形式与基本

特征

1.盗用客户网上支付帐户的犯罪。网上支付的帐户是客户进行电子商务消费的金融工具，目前保护客户网上支付帐户的安全措施，一般是设置帐户密码，或者使用公私密钥加密和消息认证等手段，但是这些安全保密措施可能被他人破解，从而导致客户帐户里的资金被盗用。

2.伪造并使用网上支付帐户的犯罪。电子商务交易过程中，结算机构要确认网上支付帐户是否有效和是否有足够支付交易的电子资金？电子商务认证机构根据结算机构的判断向商户发出交易能否进行的信息。如果行为人使用计算机技术方法等手段，非法修改结算机构的计算机信息系统中的相关数据，非法虚设网上支付帐户，就能够达到欺骗结算机构检查，骗取财物的目的，使金融机构遭受损失。

3.盗用商户电子商务身份证行骗的犯罪。在电子商务过程中，客户和商户不能直接见面，客户只能凭借商户的电子商务身份证，来判断商户能否履行合约。行为人如果盗用合法商户的电子身份证，就可以假冒合法企业的名义，骗取广大被害人的财物，同时损害合法商户的信誉。

4.电子商户诈骗的犯罪。电子商务使素未谋面、

远隔千万里的人们能够简便地进行商务活动，也使商务诈骗更加难以追究，国内外电子商户可能以电子商务交易为幌子，骗取被害人财物，不履行或者不按合同规定履行交货义务。

5.虚假认证的犯罪。认证机构在电子商务体系中地位十分重要，它监督管理交易各方签约、履约，交易各方有义务接受认证机构的监督管理，因此，认证机构提供的信息对交易方决策有着重要的导向作用，如果认证机构工作人员恶意地虚假认证，可能使交易对方蒙受巨大的损失。

6.侵犯电子商务秘密的犯罪。电子商务依靠公私密钥、消息认证、数字签名等方法保护交易各方之间的商业信息，电子商务系统中的这些商用密码信息和商业信息中有相当一部分是商业秘密，甚至是国家秘密。行为人违反法律规定，利用计算机技术或者其他方法，窃取他人私钥、消息认证程序、数字签名或者商业秘密，给被害人造成严重的损害。

7.非法截获、复制数据商品的犯罪。数据商品包括计算机软件、数据库和服务信息等。在电子商务系统中不仅用于传输交易各方之间的信息，还可以传送数据商品。由于 Internet 具有开放性，并且计算机数据容易被复制，数据商品在互联网络上传输的过程

中，可能被他人非法截获或者复制，给权利人造成严重的损失。

8.电子商务逃税的犯罪。是否对电子商务征税，世界各国的态度不同，美国克林顿政府认为“不应该对全球ec征收关税”，而多数国家只同意不向电子商务征收歧视性关税和税收，却不认为互联网络网应当成为“全球的免税商店”。电子商务的重要特征是网络化、信息化和虚拟化，这一特征使得电子商务活动可以隐蔽地跨地区跨国界进行，通过网络完成交易，而后直接将货物运送给买方，如果交易的是数据商品，商品的递送都可以通过互联网络完成。无论是跨境交易还是国内网上贸易，都可能被犯罪人用于逃避国家关税和税收征管。

9.侵犯电子商务计算机信息系统的犯罪。电子商务是建立在计算机信息基础设施基础上的、高度自动化、分工合作高度密切的在机系统，系统的正常运行有赖于计算机信息系统的安全正常运行，犯罪人如果非法侵入、破坏电子商务计算机信息系统，可能造成电子商务秩序的混乱，给国家电子商务的稳定发展和交易各方利益造成严重损害。

电子商务领域计算机犯罪的主要特征。

1.内部人员犯罪可能性大。电子商务系统通常具

有较好的安全性，而且随着信息安全技术的发展和管理的完善，电子商务将会更加安全，外部人员单凭计算机技术破解电子商务安全防护措施比较困难。而电子商务系统内部人员实施犯罪，成功的可能性就要大得多，如认证机构的工作人员利用工作之便，窃取秘密信息后而实施犯罪。另外，电子商务内部管理着数额极为庞大的社会财富，如果技术防范欠缺，管理疏漏，有些人可能铤而走险，实施犯罪。

2.犯罪高智能性。能够顺利完成犯罪的人大都具有精湛的计算机操作技能，有的甚至是网络技术和安全技术的专家。

3.共同犯罪居多。电子商务是多个社会部门分工协作组成的严密体系，单个人实施犯罪是很困难的，多个部门的内部人员相勾结，或者电子商务系统内部人员和外部人员相勾结作案，完成犯罪的可能性较大。

4.犯罪隐蔽性强。因特网虚拟空间的特性，决定电子商务犯罪的隐蔽性和较高的犯罪黑数。原因有三：

一是利用计算机信息系统开展电子商务，业务处理的速度快，行为人的犯罪行为被快速的计算机信息处理所掩盖，犯罪行为不容易被发觉；

二是行为人大多是内部人员，容易销毁作案痕迹；

三是由于公众对电子商务安全性存在疑虑，对于已发案件，有些单位担心报案会影响自己安全经营的信誉而隐匿不报。

5.社会危害性大。一次恶劣的电子商务领域的计算机犯罪就可能给国民经济和社会稳定造成严重危害，此外，这类犯罪的隐蔽性强，多次犯罪累计造成的社会危害可能达到十分严重的程度。

电子商务建设是国民经济信息化的主要组成部分，关系到我国经济在二十一世纪世界经济中的地位，我们一定要稳健、迅速地发展我国的电子商务，决不能错失发展良机，决不能重蹈屡次经济风潮的一哄而上、遗害无穷的老路。我们应该从技术、管理、法制等方面同时着手，保障电子商务安全迅速发展，目前我国特别需要制定《电子商务法》，对电子商务领域的违法、犯罪进行有效的法律控制。

20 世纪 90 年代，因特网飞速发展，计算机犯罪概念逐步演变为网络犯罪或信息犯罪。利用网络窃取国家政治、军事以及商业秘密、销售毒品、传播黄色淫秽物品、侵犯知识产权和个人隐私以及洗黑钱。由此可见，计算机犯罪有两个演变方向：一是由钱对钱

财的犯罪逐步向针对多领域的犯罪发展；二是由单机犯罪逐步向网络犯罪发展。

刑法意义上的计算机犯罪概念，最高人民法院在1998年发布的《关于确定犯罪罪名》的司法解释中，明确将《刑法》第285条和286条的罪名分别概括为："非法侵入计算机信息系统罪"和"破坏计算机信息系统罪"。如果将这两个罪名进行刑法意义上的表述，可概括为：非法侵入受国家保护的重要计算机信息系统以及破坏计算机信息系统并造成严重后果的应受刑罚处罚的危害社会的行为。简言之，即："侵入或破坏计算机信息系统的犯罪行为。"犯罪客体是社会管理秩序，直接客体是信息系统安全运行秩序；犯罪的客观方面是对计算机信息系统实施了侵入，对其功能、数据、程序及其运行实施了破坏；犯罪主体是"白领"居多的一般主体；犯罪的主观方面是故意。

犯罪学上的计算机犯罪概念可表述为：针对或利用计算机信息系统及其所处理的信息而实施的违法犯罪或将来可能发展为违法犯罪的具有社会危害性的行为。

技术形态上的计算机犯罪概念，可表述为：凡运用计算机知识和技术实施的危害社会的行为，就是计算机犯罪。我国已发生的计算机犯罪可分为以下四

类：

一是突破系统环境技术防范机制的直接或间接犯罪，包括非法进入机房操作计算机，利用技术设备拦截电磁信号，利用技术手段阻挡信息传输等；

二是逾越访问控制机制实施各类犯罪，包括偷窃、猜测、绕过、闯过各类口令及防火墙和虚拟专用网控制区；

三是破译密码实施各类犯罪，包括截取、盗窃、破解各类算法；四是植入、传播或利用非正常程序实施犯罪，包括病毒、定时炸弹、逻辑炸弹以及其他非系统所需程序。

计算机安全——对电子邮件型病毒怎么办

类似于 Hom ep age 这种邮件型病毒让人防不胜防，实在让人有些头疼，由于 Windows 脚本宿主（Scripthost）功能强大，Vbscript 和 Jscrip 脚本语言可以完成操作系统的大部分功能，于是他们也就成了病毒编写者的最爱，所以传统的杀毒软件对这种类型病毒的防治总会有一定的滞后性，所以我们必须自己采取一些有效措施来防治这类病毒，以保护我们的数据和邮件免受侵害。

一、通用规则

1.发现邮箱中出现不明来源的邮件应小心谨慎

对待，尤其是带有可执行附件的邮件，如.EXE、.VBS、.JS等。

2.如非必要，尽量关闭邮件“预览”特性。很多嵌入在HTML格式邮件中的病毒代码会在预览的时候执行，我们经常从媒体看到这样一种恐怖说法：“用户只要收到这些带病毒的邮件，即使不打开，病毒也能发作”，其实就是病毒代码在邮件预览的时候执行的。

目前的邮件型病毒绝大多数由Vbscript（Jscript）编写或是在HTML格式邮件中嵌入Script，针对这些现状，提出以下几点解决办法：

二、防止病毒发作

Windows ScriptHost本来是被系统管理员用来配置桌面环境和系统服务，实现最小化管理的一个手段，但对于大部分一般用户而言，WSH并没有多大用处，所以最好禁止WSH，也就是禁止VBScR Ipt（Jscript）文件的运行环境，如果在企业环境中，系统管理员禁止那些不需要Vbscript（Jscript）的客户机，甚至比一台台地安装防病毒软件更为简单有效。禁止了WSH后，可以防止大部分邮件型病毒的发作。

禁止Vbscript（Jscript）文件执行的几个办法：

1.在“我的电脑”—“工具”—“文件夹选项”对话框中，点击“文件类型”，删除 VBS、VBE、JS、JSE 文件后缀名与应用程序的映射

2.在 Windows 目录中，找到 Wscript。exe 和 Jscript。exe，更改其名称或者干脆删除

3.在 W In9X 和 W Ind ow s NT4.0 上，可以通过控制面板中“添加／删除程序”项来安全删除 WSH 另外，为了防止可能包含在 Ou t－Look 邮件中出现的宏病毒的发作，请在选择菜单“工具”—“宏”—“安全性”，然后将安全级别设置为“高安全性”。

把好网络安全的大门

随着信息技术与信息产业的发展，网络与信息安全问题及其对经济发展、国家安全和社会稳定的重大影响，正日益突出地显现出来。在信息化的进程中，国家的安全与经济的安全越来越不可分割，经济安全越来越依赖于信息化基础设施的安全程度。信息安全已经成为维护国家安全及社会稳定的热点问题。将国家信息安全放在战略高度来进行审视，是我们当前面临的一项十分紧迫的任务。

当今，计算机网络已经在各行各业中广泛应用，如何加强网络安全是人们普遍关注的一个重要问题。保证电子信息的有效性、安全性成为突出的大问题。

如果不能保障信息安全，就不能获得信息化的效率和效益，在国际“信息战”威胁和国内外高技术犯罪的干扰下，社会的经济生活就难以健康、有序地进行，国家的安全更无法确保。21 世纪的战争很可能告别“残酷”和“漫长”而变得“斯文”和“迅速”：人们听不到恐怖的爆炸声、看不见血肉横飞的场面，但突然之间所有的电视频道充斥着入侵者的嘴脸、电脑因病毒的侵袭而损坏、军队的指挥系统陷入瘫痪。此时的军队成了“盲军”，经济也全面崩溃……面对这种网络闪电战，遭到打击的国家全无还手之力。

在挑战面前，我国上到党和国家领导人，下到专家学者和普通百姓，对网络的信息安全都十分关心。国务院有关领导在听取了何德全院士所做的信息安全知识讲座后说，有关部门要认真研究制定信息安全的有关政策，采取有力措施，推进信息安全技术的研究和开发。专家和学者认为，信息网络是高科技发展的结晶，要保护信息网络安全，必须在技术、法规等方面进行完善，这也是最基础、最重要的措施。网络安全的现状

中国信息安全的形势是比较严峻的。其主要表现在：基础信息产业薄弱，严重依赖国外，如一些关键技术和设备掌握在国外的网络产品提供商手中；信息

与网络安全的防护能力比较弱，据调查显示，我国有高达百分之七十三的计算机曾遭受过病毒感染，而且多次感染现象非常严重；全社会的信息安全意识不高，特别是部分网管人员的安全意识较淡薄，对安全问题存在侥幸心理，没有做任何的安全措施，导致许多网站的安全防护水平很低；对引进的技术和设备缺乏有效的管理和技术改造；国家信息安全立法不完善，难以适应规范网络发展和打击网络犯罪的需要；信息犯罪在我国有快速发展蔓延的趋势；等等。

基础信息产业比较薄弱。电脑硬件面临外国的遏制和封锁的威胁。我国电脑制造业对许多核心部件的研发、生产能力很弱，关键部位完全处于受制于人的地位。本土的信息技术企业相当程度上还处在“装配”阶段。电脑软件面临市场垄断和价格歧视。目前，计算机、通信、广播电视等与信息化相关的核心技术，基本被国外公司所垄断。信息与网络安全的防护能力很弱，许多应用系统处于不设防状态，具有极大的风险性和危险性。在所披露的网络安全事件中，80％是“黑客”破解了登录密码设置程序而直接侵入计算机的。在普遍使用的 UNIX 操作系统中，仅采用 8 位字符进行登录密码的设置，“黑客”通过对总共 128 个字符进行重新组合，利用当前网络协议存在的缺陷，

很容易窃得密码而进入网络。

为阻止“黑客”们通过反复尝试而侵入计算机，应当安装防火墙和防止病毒入侵的软件，并在网络层采取诸如一次性登录密码、智能卡、生物统计校验技术等安全保护机制，在应用层编码传输过程中也要尽可能地采用先进、复杂的加密技术，从而有效地阻止“黑客”的侵入。对引进的信息技术和设备缺乏保护信息安全所必不可少的有效管理和技术改造。从国外引进的电脑硬件、软件中可能隐藏着“特洛伊木马”，一旦发生重大情况，那些隐藏在电脑芯片和操作软件中的着“特洛伊木马”就有可能在某种秘密指令下激活，造成电脑网络、电信系统瘫痪。海湾战争期间，由于隐伏在伊拉克从国外购进的军事设备中的病毒大规模地爆发，导致伊拉克防空系统瘫痪，从而使其丧失了制空权。

近年来，我国陆续出台了一些规范信息网络的法律、法规及行政规章，可以说在“加强管理”方面迈出了一大步，但存在的问题仍不容忽视：缺少必要的基本法，立法层次低、多头管理，难以适应规范网络发展和打击网络犯罪的需要。比如，我国刑法对计算机犯罪的主体仅限定为自然人，而对其处罚却既没有罚金刑，也没有资格刑；而在诉讼法中也缺少对“电

子证据”的规定；另外，缺少大多数发达国家及一大批发展中国家有关电子商务的法律。我国网络基础设施已列世界第二，但网上经营的数额在世界上还排不上名次，原因之一就是我们缺乏法律规范，阻碍了网络市场的发展。信息犯罪在我国有快速发展蔓延的趋势。现在我国网络应用和建设还不成熟，黑客行为严重威胁着在网上传输的各类金融交易、机密文件和科技情报等。

网络安全建设的对策

我国信息安全研究经历了通信保密、计算机数据保护两个发展阶段，正在进入网络信息安全的研究阶段。在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。但是，信息安全是一个国家的综合集成系统，它的规划、管理需要国家进行科学的、强有力的干预和导向。推动信息安全产业的发展。要加强自主的信息和网络技术的开发，尽快推动开发和生产我国自己的电脑核心硬件和电脑软件操作平台，并予以优惠政策。从安全体系整体的高度开展强力度的研究工作，从而为解决我国的信息与网络安全提供一个整体的理论指导和基础构件的支撑，并为信息网络安全的工程实现奠定坚实基

础。

当前，急需重点组织研究开发以下关键技术：唯一性身份识别技术、数字签名技术、信息的完整性校验检测技术、信息的加解密保护技术、密钥管理技术、安全审计跟踪技术、安全信息系统的构作集成技术、系统的安全评测技术、电子信息系统电磁信息泄露防护技术等。加快信息安全立法。应该加快有关法规的研究，及早建立我国信息安全的法规体系。首先应当考虑制订以下法规：信息安全法、电子信息犯罪法、电子信息出版法、电子信息知识产权保护法、电子信息个人隐私法、电子信息教育法、电子信息进出境法。江泽民总书记提出的“积极发展，加强管理，趋利避害，为我所用，努力在全球信息网络化的发展中占据主动地位”的指示，为我国运用法律手段保障和促进信息网络的健康发展指明了方向。

加大信息安全投入。信息安全设备设施的研制需要高强度的资金投入，建议通过国家投入、部门投入和社会融资的途径筹措。按照国家保密委的政策，安全设施建设费用应不低于基础设施 15％的投入；具体到电子政务方面，计委有关文件中提出了大型设备的定点采购的政策。以北京为例，打造 2008 年奥运会，北京市决定在未来 5 年中，对城市基础设施建设投入

1800 亿元人民币，其中 300 亿元用于信息化建设，奠定“数字北京”的基础，初步实现电子政务和电子商务。而确保奥运信息系统的安全性则是重中之重。它不仅涉及到加密的保障体系，还要提防远程攻击。

我国专家建议，我们应当尽快研发出符合国家信息安全要求、先进、实用的本土网络技术，建立具有自主知识产权的民族网络，从而实现动态、全方位、经得起攻击的网络安全体系；建立计算机病毒防治和应急体系以及病毒事故分析制度，对系统风险进行评估，以减少损失。此外，还应当加强对国内用户进行多方面的计算机安全知识教育，以防患于未然。借鉴国外网络安全建设经验

加强国家信息安全机构及职能。应当尽早成立计算机紧急反应小组，切实保证我国的信息安全技术和装备体系，使我们有足够的能力预防和抗击敌对势力可能对我国发动的信息战争和高技术犯罪活动。目前，在美国、英国和法国等许多国家，计算机紧急反应小组（CERT）已经建立并担负任务，对侵入政府信息系统的突发事件能做出快速的反应。比如，美国国防情报系统局的 CERT 和美国国家安全局的国家安全行动中心的信息保护组织及国防情报安全局的自动化系统安全事件处理小组，一年四季全天候对各种非

法侵入计算机的行为做出紧急反应。

建立计算机网络安全评估指导小组。目前，北约的许多国家都已成立专门的机构，对那些 IT 安全保护产品（比如加密技术、杀毒软件和防火墙）进行严格的评价、验证和批准。欧盟对 IT 产品的评估遵循两种标准：一是由 12 个国家共同签署的信息技术安全评估细则；二是相互监督准则。这是在 1998 年由 5 个国家签署的标准，2000 年 10 月澳大利亚和新西兰也加入了进来。1999 年 2 月，法国成立了信息系统安全指导小组（DSIC），在计算机网络设备的采办和建立过程中发挥咨询指导的作用，并负责这些设备在使用过程中的安全问题。英国国防发展研究局（DERA）也行使同样的作用。

重视信息安全基础研究和对计算机网络管理人员的训练。大力培养信息安全的专业人才，为各部门输送信息基础设施安全运行的骨干力量。各国在招募和吸收计算机网络防御骨干的同时，都重视对计算机网络管理人员的训练，因为计算机网络的防护依赖于经验的积累。去年，美军进行了 TuRboChallenge 等多项计算机防护演习，其中包括计算机进攻战，并加强了日常的训练。在防御演练及对病毒的实际防护中，既对计算机网络的防护进行了检验，又训练了人

员。

发展具有识别和确认能力的公共基础设施，对不同层次的信息网络进行安全保护十分重要。英国正在进行一项加强信息安全的法案，目的在于将各个层次、级别的网络连接起来的同时，减少信息泄露的危险，以保护信息安全。英国国家发展研究局建成了名为“紫色珀涅罗珀”的演示方案，此方案使用自选标号处理方法，允许计算机系统在使用像 WindowsNT 的软件的情况下，使信息在不同层次上安全传输。欧盟的其它一些国家也相继开始了类似的工作，以适应不同层次网络互联的趋势，同时保证信息的安全。

在网络信息建设中，安全是基础。在发展和建设网络工程的时候，千万不能忘了网络安全这块基石。令人兴奋的是，我们国家已充分认识这一问题的重要性并已开始着手行动。今年《财富》论坛科技版块的首要议题就是网络安全，今后我们无疑要大力发展网络安全产业。我们应当抓住机遇，调整管理体系和管理手段。这个时候，任何懈怠和无所作为就成了亟需克服的障碍。这绝非危言耸听!

计算机安全——缓冲区溢出:十年来攻击和防卫的弱点

在过去的十年中，以缓冲区溢出为类型的安全漏

洞占是最为常见的一种形式了。更为严重的是，缓冲区溢出漏洞占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权！如果能有效地消除缓冲区溢出的漏洞，则很大一部分的安全威胁可以得到缓解。在本文中，我们研究了各种类型的缓冲区溢出漏洞和攻击手段，同时我们也研究了各种的防御手段，这些手段用来消除这些漏洞所造成的影响，其中包括我们自己的堆栈保护方法。然后我们要考虑如何在保证现有系统功能和性能不变的情况下，如何使用这些方法来消除这些安全漏洞。

一、前言

在过去的十年中，以缓冲区溢出为类型的安全漏洞占是最为常见的一种形式了。更为严重的是，缓冲区溢出漏洞占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权！由于这类攻击使任何人都有可能取得主机的控制权，所以它代表了一类极其严重的安全威胁。

缓冲区溢出攻击之所以成为一种常见安全攻击手段其原因在于缓冲区溢出漏洞太普通了，并且易于实现。而且，缓冲区溢出成为远程攻击的主要手段其

原因在于缓冲区溢出漏洞给予了攻击者他所想要的一切：殖入并且执行攻击代码。被殖入的攻击代码以一定的权限运行有缓冲区溢出漏洞的程序，从而得到被攻击主机的控制权。

比如，在 1998 年 Lincoln 实验室用来评估入侵检测的的 5 种远程攻击中，有 3 种是基于社会工程学的信任关系，2 种是缓冲区溢出。而在 1998 年 CERT 的 13 份建议中，有 9 份是是与缓冲区溢出有关的，在 1999 年，至少有半数的建议是和缓冲区溢出有关的。在 Bugtraq 的调查中，有 2/3 的被调查者认为缓冲区溢出漏洞是一个很严重的安全问题。

缓冲区溢出漏洞和攻击有很多种形式，我们会在第二部分对他们进行描述和分类。相应地防卫手段也随者攻击方法的不同而不同，我们会放在第三部分描述，它的内容包括针对每种攻击类型的有效的防卫手段。我们还要要介绍堆栈保护方法，这种方法在解决缓冲区溢出的漏洞方面很有效果，并且没有牺牲系统的兼容性和性能。在第四部分，我们要讨论各种防卫方法的综合使用。最后在第五部分是我们的结论。

二、缓冲区溢出的漏洞和攻击

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使得攻击者取得程序的

控制权，如果该程序具有足够的权限，那么整个主机就被控制了。一般而言，攻击者攻击 Root 程序，然后执行类似“exec(sh)”的执行代码来获得 Root 的 sheLL，但不一直是这样的。为了达到这个目的，攻击者必须达到如下的两个目标：

1.在程序的地址空间里安排适当的代码。

2.通过适当地初始化寄存器和存储器，让程序跳转到我们安排的地址空间执行。

我们根据这两个目标来对缓冲区溢出攻击进行分类。在 2.1 部分，我们将描述攻击代码是如何放入被攻击程序的地址空间的（这个就是“缓冲区”名字的的由来）。在 2.2 部分，我们介绍攻击者如何使一个程序的缓冲区溢出，并且执行转移到攻击代码（这个就是“溢出”的由来）。在 2.3 部分，我们介绍综合在 2.1 和 2.2 部分所讨论的代码安排和控制程序执行流程的技术。

2.1 在程序的地址空间里安排适当的代码的方法

有两种在被攻击程序地址空间里安排攻击代码的方法：

殖入法：

攻击者向被攻击的程序输入一个字符串，程序会

把这个字符串放到缓冲区里。这个字符串包含的数据是可以在这个被攻击的硬件平台上运行的指令序列。在这里攻击者用被攻击程序的缓冲区来存放攻击代码。具体的方式有以下两种差别：

1.攻击者不必为达到此目的而溢出任何缓冲区，可以找到足够的空间来放置攻击代码

2.缓冲区可以设在任何地方：堆栈（自动变量）、堆（动态分配的）和静态数据区（初始化或者未初始化的数据）

利用已经存在的代码：

有时候，攻击者想要的代码已经在被攻击的程序中了,攻击者所要做的只是对代码传递一些参数，然后使程序跳转到我们的目标。比如，攻击代码要求执行“exec(”/bin/sh“)”，而在 Libc 库中的代码执行“exec(arg)”，其中 arg 使一个指向一个字符串的指针参数，那么攻击者只要把传入的参数指针改向指向“/bin/sh”，然后调转到 Libc 库中的相应的指令序列。

2.2 控制程序转移到攻击代码的方法

所有的这些方法都是在寻求改变程序的执行流程，使之跳转到攻击代码。最基本的就是溢出一个没有边界检查或者其他弱点的缓冲区，这样就扰乱了程

序的正常的执行顺序。通过溢出一个缓冲区，攻击者可以用近乎暴力的方法改写相邻的程序空间而直接跳过了系统的检查。

这里分类的基准是攻击者所寻求的缓冲区溢出的程序空间类型。原则上是可以任意的空间。比如，最初的 MorrisWwrm 使用了 fingerd 程序的缓冲区溢出，扰乱 fingerd 要执行的文件的名字。实际上，许多的缓冲区溢出是用暴力的方法来寻求改变程序指针的。这类程序的不同的地方就是程序空间的突破和内存空间的定位不同。

激活纪录（Activationrecords）：

每当一个函数调用发生时，调用者会在堆栈中留下一个激活纪录，它包含了函数结束时返回的地址。攻击者通过溢出这些自动变量，使这个返回地址指向攻击代码，如图 1 所示。通过改变程序的返回地址，当函数调用结束时，程序就跳转到攻击者设定的地址，而不是原先的地址。这类的缓冲区溢出被称为“stacksmashingattack”，使目前常用的缓冲区溢出攻击方式。

函数指针（Functionpointers）：

“void(*foo)()”声明了一个返回值为 void 函数指针的变量 foo。函数指针可以用来定位任何地址

空间，所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区，然后溢出这个缓冲区来改变函数指针。在某一时刻，当程序通过函数指针调用函数时，程序的流程就按攻击者的意图实现了！它的一个攻击范例就是在 Linux 系统下的 supeRpRobe 程序。

长跳转缓冲区（Longjmpbuffers）：

在 C 语言中包含了一个简单的检验/恢复系统，称为 setjmp/Longjmp。意思是在检验点设定“setjmp(buffer)”，用“Longjmp(buffer)”来恢复检验点。然而，如果攻击者能够进入缓冲区的空间，那么“Longjmp(buffer)”实际上是跳转到攻击者的代码。象函数指针一样，Longjmp 缓冲区能够指向任何地方，所以攻击者所要做的就是找到一个可供溢出的缓冲区。一个典型的例子就是 Perl5.003，攻击者首先进入用来恢复缓冲区溢出的的 Longjmp 缓冲区，然后诱导进入恢复模式，这样就使 Perl 的解释器跳转到攻击代码上了！

2.3 综合代码殖入和流程控制技术

现在我们研究综合代码殖入和流程控制的技术。

最简单和常见的缓冲区溢出攻击类型就是在一个字符串里综合了代码殖入和激活纪录。攻击者定位

一个可供溢出的自动变量，然后向程序传递一个很大的字符串，在引发缓冲区溢出改变激活纪录的同时殖入了代码。这个是由 Levy 指出的攻击的模板。因为 C 在习惯上只为用户和参数开辟很小的缓冲区，因此这种漏洞攻击的实例不在少数。

代码殖入和缓冲区溢出不一定要在在一次动作内完成。攻击者可以在一个缓冲区内放置代码，这是不能溢出缓冲区。然后，攻击者通过溢出另外一个缓冲区来转移程序的指针。这种方法一般用来解决可供溢出的缓冲区不够大（不能放下全部的代码）的情况。

如果攻击者试图使用已经常驻的代码而不是从外部殖入代码，他们通常有必须把代码作为参数化。举例来说，在 Libc（几乎所有的 C 程序都要它来连接）中的部分代码段会执行“exec(something)”，其中 somthing 就是参数。攻击者然后使用缓冲区溢出改变程序的参数，然后利用另一个缓冲区溢出使程序指针指向 Libc 中的特定的代码段。

3.缓冲区溢出的保护方法

目前有四种基本的方法保护缓冲区免受缓冲区溢出的攻击和影响。在 3.1 中介绍了强制写正确的代码的方法。在 3.2 中介绍了通过操作系统使得缓冲区不可执行，从而阻止攻击者殖入攻击代码。这种方法

有效地阻止了很多缓冲区溢出的攻击，但是攻击者并不一定要殖入攻击代码来实现缓冲区溢出的攻击（参见 2.1 节），所以这种方法还是存在很弱点的。在 3.3 中，我们介绍了利用编译器的边界检查来实现缓冲区的保护。这个方法使得缓冲区溢出不可能出现，从而完全消除了缓冲区溢出的威胁，但是相对而言代价比较大。在 3.4 中我们介绍一种间接的方法，这个方法在程序指针失效前进行完整性检查。这样虽然这种方法不能使得所有的缓冲区溢出失效，但它的的确确阻止了绝大多数的缓冲区溢出攻击，而能够逃脱这种方法保护的缓冲区溢出也很难实现。然后在 3.5，我们要分析这种保护方法的兼容性和性能优势（与数组边界检查）。

3.1 编写正确的代码

编写正确的代码是一件非常有意义但耗时的工作，特别象编写 C 语言那种具有容易出错倾向的程序（如：字符串的零结尾），这种风格是由于追求性能而忽视正确性的传统引起的。尽管花了很长的时间使得人们知道了如何编写安全的程序，具有安全漏洞的程序依旧出现。因此人们开发了一些工具和技术来帮助经验不足的程序员编写安全正确的程序。

最简单的方法就是用 grep 来搜索源代码中容易

产生漏洞的库的调用，比如对 strcpy 和 sprintf 的调用，这两个函数都没有检查输入参数的长度。事实上，各个版本 C 的标准库均有这样的问题存在。

为了寻找一些常见的诸如缓冲区溢出和操作系统竞争条件等漏洞，代码检查小组检查了很多的代码。然而依然有漏网之鱼存在。尽管采用了 strncpy 和 snprintf 这些替代函数来防止缓冲区溢出的发生，但是由于编写代码的问题，仍旧会有这种情况发生。比如 LpRm 程序就是最好的例子，虽然它通过了代码的安全检查，但仍然有缓冲区溢出的问题存在。

为了对付这些问题，人们开发了一些高级的查错工具，如 faultinjection 等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。还有一些静态分析工具用于侦测缓冲区溢出的存在。

虽然这些工具帮助程序员开发更安全的程序，但是由于 C 语言的特点，这些工具不可能找出所有的缓冲区溢出漏洞。所以，侦错技术只能用来减少缓冲区溢出的可能，并不能完全地消除它的存在。除非程序员能保证他的程序万无一失，否则还是要用到以下 3.2 到 3.4 部分的内容来保证程序的可靠性能。

3.2 非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行，从而使得攻击者不可能执行被殖入被攻击程序输入缓冲区的代码，这种技术被称为非执行的缓冲区技术。事实上，很多老的 Unix 系统都是这样设计的，但是近来的 Unix 和 MSWindows 系统由于实现更好的性能和功能，往往在在数据段中动态地放入可执行的代码。所以为了保持程序的兼容性不可能使得所有程序的数据段不可执行。

但是我们可以设定堆栈数据段不可执行，这样就可以最大限度地保证了程序的兼容性。Linux 和 Solaris 都发布了有关这方面的内核补丁。因为几乎没有任何合法的程序会在堆栈中存放代码，这种做法几乎不产生任何兼容性问题，除了在 Linux 中的两个特例，这时可执行的代码必须被放入堆栈中：

信号传递：

Linux 通过向进程堆栈释放代码然后引发中断来执行在堆栈中的代码来实现向进程发送 Unix 信号。非执行缓冲区的补丁在发送信号的时候是允许缓冲区可执行的。

GCC 的在线重用：

研究发现gcc在堆栈区里放置了可执行的代码作

为在线重用之用。然而，关闭这个功能并不产生任何问题，只有部分功能似乎不能使用。

非执行堆栈的保护可以有效地对付把代码殖入自动变量的缓冲区溢出攻击，而对于其他形式的攻击则没有效果（参见 2.1)。通过引用一个驻留的程序的指针，就可以跳过这种保护措施。其他的攻击可以采用把代码殖入堆或者静态数据段中来跳过保护。

3.3 数组边界检查

殖入代码引起缓冲区溢出是一个方面，扰乱程序的执行流程是另一个方面。不象非执行缓冲区保护，数组边界检查完全放置了缓冲区溢出的产生和攻击。这样，只要数组不能被溢出，溢出攻击也就无从谈起。为了实现数组边界检查，则所有的对数组的读写操作都应当被检查以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作，但是通常可以采用一些优化的技术来减少检查的次数。目前有以下的几种检查方法：

3.3.1Compaqc 编译器

Compaq 公司为 ALphacpu 开发的 C 编译器（在 Tru64 的 Unix 平台上是 cc，在 ALphalinux 平台上是 ccc）支持有限度的边界检查（使用-check_bounds 参数)。这些限制是：

只有显示的数组引用才被检查，比如“a[3]”会被检查，而“*(a+3)”则不会。

由于所有的 C 数组在传送的时候是指针传递的，所以传递给函数的的数组不会被检查。

带有危险性的库函数如 strcpy 不会在编译的时候进行边界检查，即便是指定了边界检查。

由于在C语言中利用指针进行数组操作和传递是如此的频繁，因此这种局限性是非常严重的。通常这种边界检查用来程序的查错，而且不能保证不发生缓冲区溢出的漏洞。

3.3.2Jones&kelly:C 的数组边界检查

Richardjones和Paulkelly开发了一个gcc的补丁，用来实现对 C 程序完全的数组边界检查。由于没有改变指针的含义所以被编译的程序和其他的gcc模块具有很好的兼容性。更进一步的是，他们由此从没有指针的表达式中导出了一个“基”指针，然后通过检查这个基指针来侦测表达式的结果是否在容许的范围之内。

当然，这样付出的性能上的代价是巨大的：对于一个频繁使用指针的程序如向量乘法，将由于指针的频繁使用而使速度比本来慢 30 倍。

这个编译器目前还很不成熟；一些复杂的程序

（如 elm）还不能在这个上面编译，执行通过。然而在它的一个更新版本之下，它至少能编译执行 ssh 软件的加密软件包。其实现的性能要下降 12 倍。

3.3.3Purify：存储器存取检查

Purify 是 C 程序调试时查看存储器使用的工具而不是专用的安全工具。Purify 使用“目标代码插入”技术来检查所有的存储器存取。通过用 Purify 连接工具连接，可执行代码在执行的时候数组的所有引用来保证其合法性。这样带来的性能上的损失要下降 3-5 倍。

3.3.4 类型-安全语言

所有的缓冲区溢出漏洞都源于C语言缺乏类型安全。如果只有类型-安全的操作才可以被允许执行，这样就不可能出现对变量的强制操作。如果作为新手，可以推荐使用具有类型-安全的语言如 Java 和 ML。

但是作为Java执行平台的Java虚拟机是C程序，因此通过攻击 Jvm 的一条途径是使 Jvm 的缓冲区溢出。因此在系统中采用缓冲区溢出防卫技术来使用强制类型-安全的语言可以收到意想不到的效果。

3.4 程序指针完整性检查

程序指针完整性检查和边界检查由略微的不同。

与防止程序指针被改变不同，程序指针完整性检查在程序指针被引用之前检测到它的改变。因此，即便一个攻击者成功地改变了程序的指针，由于系统事先检测到了指针的改变，因此这个指针将不会被使用。

与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题；采用其他的缓冲区溢出方法就可以避免这种检测。但是这种方法在性能上有很大的优势，而且在兼容性也很好。

程序完整性检查大体上有三个研究方向。在3.4.1中会介绍Snarskii为Freebsd开发了一套定制的能通过监测cpu堆栈来确定缓冲区溢出的Libc。在3.4.2中会介绍我们自己的堆栈保护方法所开发的一个编译器，它能够在函数调用的时候自动生成完整性检测代码。最后在3.4.3，我们介绍正在开发中的指针保护方法，这种方法类似于堆栈保护，它提供对所有程序指针的完整性的保护。

3.4.1 手写的堆栈监测

Snarskii 为 Freebsd 开发了一套定制的能通过监测cpu堆栈来确定缓冲区溢出的Libc。这个应用完全用手工汇编写的，而且只保护 Libc 中的当前有效纪录函数。这个应用达到了设计要求，对于基于Libc库函数的攻击具有很好的防卫，但是不能防卫其它方

式的攻击。

3.4.2 堆栈保护：编译器生成的有效纪录完整性检测

堆栈保护是一种提供程序指针完整性检查的编译器技术，通过检查函数活动纪录中的返回地址来实现。堆栈保护作为 gcc 的一个小的补丁，在每个函数中，加入了函数建立和销毁的代码。加入的函数建立代码实际上在堆栈中函数返回地址后面加了一些附加的字节。而在函数返回时，首先检查这个附加的字节是否被改动过。如果发生过缓冲区溢出的攻击，那么这种攻击很容易在函数返回前被检测到。

但是，如果攻击者预见到这些附加字节的存在，并且能在溢出过程中同样地制造他们，那么他就能成功地跳过堆栈保护的检测。通常，我们有如下的两种方案对付这种欺骗：

终止符号：

利用在 C 语言中的终止符号如 0(null)，cr，lf，-1(eof)等不能在常用的字符串函数中使用，因为这些函数一旦遇到这些终止符号，就结束函数过程了。

随机符号：

利用一个在函数调用时产生的一个 32 位的随机数来实现保密，使得攻击者不可能猜测到附加字节的

内容。而且，每次调用，附加字节的内容都在改变，也无法预测。

通过检查堆栈的完整性的堆栈保护法是从 Synthetix 方法演变来的。Synthetix 方法通过使用准不变量来确保特定变量的正确性。这些特定的变量的改变是程序实现能预知的，而且只能在满足一定的条件才能可以改变。这种变量我们称为准不变量。

Synthetix 开发了一些工具用来保护这些变量。

攻击者通过缓冲区溢出而产生的改变可以被系统当做非法的动作。在某些极端的情况下，这些准不变量有可能被非法改变，这是就需要堆栈保护来提供更完善的保护了。

实验的数据表明，堆栈保护对于各种系统的缓冲区溢出攻击都有很好的保护作用，并能保持较好的兼容性和系统性能。早先我们报告的堆栈保护所能抑制的漏洞都在表一中列出。随后，我们用堆栈保护的方法重新构造了一个完整的 Linux 系统(Redhat5.1)。然后我们用 Xfree86-3.3.2-5 和 Lsof 的漏洞对此进行了攻击，结果表明，这个系统有效地抵御了这些攻击。这些分析表明，堆栈保护能有效抵御现在的和将来的基于堆栈的攻击。

堆栈保护版本的 RedhatLinux5.1 已经在各种系

统上运行了多年，包括个人的笔记本电脑和工作组文件服务器。从我们的Web服务器上可以得到这个版本，而且在我们的邮件列表里已经有了 55 个成员。出了仅有的一次例外，这个系统和本来的系统工作完全一样，这表明堆栈保护并不对系统的兼容性构成很大的影响。

我们已经用各种性能测试来评测堆栈保护的性能。

Mircobenchmarks 的结果表明在函数的调用，堆栈保护中增加了系统的开销。而在网络的测试中（需要用到堆栈保护的地方），则表明这种开销不是很大。

我们的第一个测试对象是 SSH，它提供了极强的加密和认证，用来替代 Berkeley 的 R 系列指令。SSH 使用了软件加密，因此系统的占用的带宽不大，我们用网络间复制一个大的文件来测试带宽：

scpbigsourcelocalhost:bigdest

测试结果表明：堆栈保护几乎不影响 SSH 的网络吞吐性能。

第二个测试使用了 Apacheweb 服务器。如果这种服务器存在基于堆栈的攻击，那么攻击者就可以轻易地取得 Web 服务器的控制权，允许攻击者阅读隐秘的内容和肆意篡改主页的内容。同时，Web 服务器也是

对性能和带宽要求较高的一个服务器部件。

我们用 Webstone 对带有和不带堆栈保护的 Apacheweb 服务器进行了测试，测试的结果在表二中列出。

和 SSH 一样，他们的性能几乎没有区别。在客户数目较少的情况下，带有保护的服务器性能比不带保护的略微好些，在客户端数目多的时候，不带保护的性能好些。在最坏的情况下，带保护的服务器比不带保护的要差 8%的连接性能，而在平均延时上保持优势。象以前一样，我们把这些归结为噪声的影响。因此，我们的结论是：堆栈保护对 Web 服务器系统性能没有重大的影响。

3.4.3 指针保护：编译器生成程序指针完整性检查

在堆栈保护设计的时候，冲击堆栈构成了缓冲区溢出攻击的常见的一种形式。有人推测存在一种模板来构成这些攻击（在 1996 年的时候）。从此，很多简单的漏洞被发现，实施和补丁了，很多攻击者开始用在第二部分中描述的更一般的方法实施缓冲区溢出攻击。

指针保护是堆栈保护针对这种情况的一个推广。通过在所有的代码指针之后放置附加字节来检验指

针在被调用之前的合法性。如果检验失败，会发出报警信号和退出程序的执行，就如同在堆栈保护中的行为一样。这种方案有两点需要注意：

附加字节的定位：

附加字节的空间是在被保护的变量被分配的时候分配的，同时在被保护字节初始化过程中被初始化。这样就带来了问题；为了保持兼容性，我们不想改变被保护变量的大小，因此我们不能简单地在变量的结构定义中加入附加字。还有，对各种类型也有不同附加字节数目。

检查附加字节：

每次程序指针被引用的时候都要检查附加字节的完整性。这个也存在问题；因为“从存取器读”在编译器中没有语义；编译器更关心指针的使用，而各种的优化算法倾向于从存储器中读入变量。

还有随着不同类型的变量，读入的方法也各自不同。

我们已经开发了指针保护的一个原型（还是基于gcc 的），通过附加字节来保护静态分配的函数指针，但不适用于结构和数组类型。这个计划还远没有完成。一旦这个项目完成了，那么用它和堆栈保护构成的可执行代码将不会受到缓冲区溢出的攻击了。

目前为止，只有很少一部分使用非指针变量的攻击能逃脱指针保护的检测。但是，可以通过在编译器上强制对某一变量加入附加字节来实现检测，这时需要程序员自己手工加入相应的保护了。

3.5 兼容性和性能的考虑

程序指针完整性检查与边界检查相比，并不能防止所有的缓冲区溢出问题。然而在执行的性能和兼容性上具有相当的优势：

性能：

边界检查必须在每个数组元素操作时完成一次检查。相比之下，程序指针检查只在被引用的时候实现检查。无论在 C 还是在 C++中，这种花在程序指针引用上的开销始终比数组的指针引用小。

应用效能：

边界检查最难实现之处在于在 C 语言中，很能确定数组的边界。这是由于在 C 中，数组的概念和通用指针的混用造成的。由于一个指针是一个独立的对象，没有与特定的边界条件关联，只有一个系统的机器字来存储它，而标识边界信息的数据却没有存放。因此需要特殊的方法来恢复这些信息；数组的引用将不在是一个简单的指针，而是一个对缓冲区描述的指针组。

与现有代码的兼容性：

一些边界检查方法为了与现有的代码保持兼容而在系统的性能上得到了损失。而另一些则用别的方法达到目的。这样就打破的传统的 C 的转换规则，转而产生了一类新的 C 编译器，只能编译 C 的一个子集，有的还不能使用指针或者需要别的改变。

4.有效的组合

在这里我们研究、比较在第二部分描述的各种漏洞攻击和在第三部分描述的防卫方法，以此来确定何种组合能完全消除缓冲区溢出问题。我们把关于缓冲区溢出的攻击和防卫的方法都列在表 3 中，但是我们没有把边界检查计算在内，因为它能有效地防止所有的缓冲区溢出，但是所需的开销也是惊人的。

最普通的缓冲区溢出形式是攻击活动纪录然后在堆栈中殖入代码。这种类型的攻击在 1996 年中有很多纪录。而非执行堆栈和堆栈保护的方法都可以有效防卫这种攻击。非执行堆栈可以防卫所有把代码殖入堆栈的攻击方法，堆栈保护可以防卫所有改变活动纪录的方法。这两种方法相互兼容，可以同时防卫多种可能的攻击。

剩下的攻击基本上可以用指针保护的方法来防卫，但是在某些特殊的场合需要用手工来实现指针保

护。全自动的指针保护需要对每个变量加入附加字节，这样使得指针边界检查在某些情况下具有优势。

最为有趣的是，第一个缓冲区溢出漏洞--MorRIs蠕虫使用了现今所有方法都无法有效防卫的方法，但是却很少有人用到，也许是这种方法过于复杂的缘故吧。

5.结论

在本文中，我们详细描述和分析了缓冲区溢出的攻击和防卫方法。由于这种攻击是目前常见的攻击手段，所以进行这个方面的研究工作是有意义和成效的。研究的结果表明，堆栈保护方法和非执行缓冲区方法对于当前绝大多数的攻击都能有效地防御，指针保护的方法可以对剩下的攻击进行有效的防御。最后声明的是对于 Morris 蠕虫的攻击，迄今还没有有效的防御手段。

如何防止宽带网络 IP 地址被盗用

随着网络技术在国内的蓬勃发展，宽带网在许多大楼和社区应运而生。但在享受各种多媒体信息的同时，有个问题经常困扰着网络管理员和用户，那就是宽带网络内分配的 IP 地址经常被盗用，授权用户用自己的 IP 地址在网络中产生冲突，无法进入网络。这种现象导致了网络管理的混乱，影响授权用户的利

益，也对用网络流量来进行计费的宽带网带来较大的影响。

一、开放系统互联模型结构

要清楚 IP 地址盗用的方法，首先必须了解国际电联规定的开放系统互联模型（OSI）的结构层次。需要传输的数据在传输层被分割并重组为数据串（segment），然后在网络层加入源和目的 IP 地址，封装成包（packet），再在数据链路层附加数据链的帧头和帧尾，将数据包放进帧（frame）里，最后在物理层转换成以比特为单位的数据。所以，IP 地址是网络层用来标识不同地点的逻辑地址，它的长度是 32 位；而在数据链路层则是用 MAC（媒介存取控制）地址来标识网络节点的位置，它的长度是 48 位，它也是设备的物理地址。

二、盗用 IP 地址的几条途径

1.修改静态 IP 地址

在修改 TCP/IP 协议属性配置时，使用的不是网络管理员分配的 IP 地址，而是已知的授权的 IP 地址。由于 IP 地址是一个逻辑地址，是一个需要用户设置的值，因此无法限制用户对于 IP 地址的静态修改，当盗用者修改 IP 地址后，也可以通过网关访问外网。

2.成对地修改 IP 地址和 MAC 地址

为防止静态 IP 地址被修改，一般采用静态路由技术予以解决。针对静态路由技术，IP 盗用技术又有了新的门路，即成对修改 IP-MAC 地址。MAC 地址是设备的物理地址，对于我们常用的以太网来说，俗称为计算机网卡地址。每一个网卡的 MAC 地址在所有以太网设备中必须是唯一的，它由 IEEE 分配，是固化在网卡上的，一般不能随意改动。但是，目前的一些兼容网卡，其 MAC 地址可以使用网卡配置程序进行修改。如果将一台计算机的 IP 地址和 MAC 地址都改为一台合法主机的 IP 地址和 MAC 地址，那静态路由技术就无能为力了。另外，对于那些 MAC 地址不能直接修改的网卡来说，高明的盗用者还可以采用软件的办法来修改 MAC 地址。

三、几种防止 IP 地址被盗的方法

1. 锁定交换机端口

对于交换机的每一个以太网端口，采用 MAC 地址表（MAC-address-tabLe）的方式对端口进行锁定。只有网络管理员在 MAC 地址表中指定的网卡的 MAC 地址才能通过该端口与网络连接，其他的网卡地址不能通过该端口访问网络。我们可以在计算机上先运行 Ping 命令，然后用 arp-a 命令就可以看到网络用户相应的 IP 地址对应的 MAC 地址，这样就使 MAC 地址和

物理顺序对应起来，使得一根网线、一个端口对应一个 MAC 地址。这种方法比较适合于单幢大楼的宽带用户，在每一层楼或每个单元放置一台交换机，对交换机的每一个以太网端口进行限定，让每个用户单独占用一个端口，如果有人盗用了 IP 地址也将无济于事。下面用一段程序，举例说明指定交换机的 e0/9 口对应 MAC 地址 083c.0000.0002，只有这个 MAC 地址可以通过该端口访问网络。

```
Switch#configterminal
Switch(conf)#mac-address-tablepermanent0
83c.0000.0002e0/9
Switch(conf)#Inte0/9
Switch(conf－If)#portsecuremax-mac-count
1
Switch(conf－If)#exIt
Switch(conf)#exIt
```

2. 应用 ARP 绑定 IP 地址和 MAC 地址

ARP（Address Resolution Protocol）即地址解析协议，这个协议是将 IP 地址与网络物理地址一一对应的协议。每台计算机的网卡的 MAC 地址都是唯一的。在三层交换机和路由器中有一张称为 ARP 的表，用来支持在 IP 地址和 MAC 地址之间的一一对应关系，

它提供两者的相互转换，具体说就是将网络层地址解析为数据链路层的地址。

我们可以在 ARP 表里将合法用户的 IP 地址和网卡的 MAC 地址进行绑定。当有人盗用 IP 地址时，尽管盗用者修改了 IP 地址，但由于网卡的 MAC 地址和 ARP 表中对应的 MAC 地址不一致，那么也不能访问网络。以 Cisco 交换机为例，在 Ciscocatalyst5000 网络交换机上，关于 ARP 表的设置和删除有以下几条命令：

Setarp[dynamiclstatic]{IP_addrhw_addr}（设置动态或静态的 ARP 表）；

IP_addr（IP 地址），hw_addr（MAC 地址）；

Setarpstatic20.89.21.100-80-1c-93-80-40（将将 IP 地址 20.89.21.1 和网卡 MAC 地址 00-80-1c-93-80-40 绑定）；

Setarpstatic20.89.21.300-00-00-00-00-00（对未用的 IP 进行绑定，将 MAC 地址设置为 0）；

Setarpagingtimeseconds（设置 ARP 表的刷新时间，如 Setarpagingtime300）；

showarp（用来显示 ARP 表的内容）；

cleararp[dynamic|static]{IP_addrhw_addr}（清除 ARP 表中的内容）。

其他品牌的三层交换机也有类似的命令和功能，用其他交换机来构建宽带网络时，也可以采用这种设置 ARP 表的办法来防止盗用 IP 地址，以达到限制每个 IP 地址的流量和根据网络流量进行计费的目的。这种方法比较适合于社区的宽带用户，但它只能防止盗用者静态地修改 IP 地址。

3.用 PPPOE 协议进行用户认证

对于盗用者使用第二种方法同时修改 IP 地址和 MAC 地址时，可以使用 PPPOE 协议进行用户认证。现在有很多基于 PPPOE 协议的软件，在 ADSL 的宽带网中广泛使用。PPPOE 全称是 PoInttoPoIntPRotocoLoverethernet（基于局域网的点对点通讯协议），这个协议是为了满足越来越多的宽带上网设备和网络之间的通讯而最新制定开发的标准，它基于两个广泛接受的标准，即以太网和 PPP 点对点拨号协议。对运营商来说，在现有局域网基础上不必花费巨资来做大面积改造，使得 PPPOE 在宽带接入服务中比其他协议更具有优势，因此逐渐成为宽带上网的最佳选择。PPPOE 的实质是以太网和拨号网络之间的一个中继协议，它兼有以太网的快速性和 PPP 协议拨号的简易性以及用户验证和 IP 分配等优势。在 ADSL 宽带网的实际应用中，PPPOE 利用以太网的工作原理，将 ADSLModem

的 10BASE－T 接口与内部以太网络互联，PPPOE 接入利用在网络侧和 ADSLModem 之间建立一条 PVC（永久虚电路）就可以完成以太网上多用户的共同接入，实际组网方式简单易行，大大降低了网络的复杂程度。

在客户端，其设置和拨号上网方式一样，安装虚拟拨号软件，通过虚拟拨号的方式完成。在客户机接入网络后，由 PPP 服务器或 RADIUS 服务器来进行认证，其使用的验证协议有两种：PAP 和 CHAP。

PAP 是密码身份验证协议，它使用原文（不加密）密码，是一种最简单的身份验证协议。如果网络的接入不能用更安全的验证方式，一般就使用 PAP。

CHAP 是质询握手身份验证协议，它是使用 MD5（messagedigest5 一种工业标准）的一种散列方案，散列方案是一种转换密码的方法，它生成的结果是唯一的且不能被改回到原始形式。CHAP 在响应时使用质询-响应机制和单向 MD5 散列。用这种方法，可以向服务器证明用户知道密码，但不必实际将密码发送到网络上。通过支持 CHAP 和 MD5，网络和拨号连接能够安全地连接到几乎所有其他的 PPP 服务器上。

当用户合法身份通过 RADIUS 服务器验证后，由宽带接入服务器给客户机分配 IP 地址，避免了 IP 地址被盗用的情况。这种由宽带接入服务器和 RADIIUS

服务器配合来完成用户身份并分配 IP 地址的方法，还可以分配不同性质的 IP 地址（如公网地址或私有地址），并且符合 RFC2138 和 RFC2139 建议，支持 Radiusproxy 功能，可实现用户的漫游认证。在现有的很多宽带网里，使用网络防火墙也具有同样的用户认证功能。

用 PPPOE 协议进行用户认证的方式适合于大范围安装 ADSL 和局域网的宽带用户群，是可以较好地防止盗用 IP 地址的一种方法。

Internet 时代信息安全要有新思维

2001 年以来，Internet 安全形势和网络攻击模式正在发生重大变化，网上攻击数比 2000 年增加一倍，具有讽刺意味的是：

Internet 网络协议原是按照在核打击下仍能生存的要求构思的，雅虎等网站也有相当好的安全设施，但在一些公开的黑客工具攻击下却显得十分脆弱。

“红色代码”蠕虫以缓存器溢出的形式攻击装有 IIS 服务器的 Windows 操作系统，取得了系统管理员级的权限，竟与 1988 年小莫里斯释放第一个蠕虫的形式很类似，蔓延速度极快，这值得网络安全界反思。

一份调查报告说：截至 2001 年 10 月，有 88％的

网站承认在最近一年内受到了病毒感染和入侵，而在它们中间有 90％却已安了防火墙和入侵监测等安全设备。

针对这些情况，世界上若干有识之士提出：现在迫切需要安全的“范式转换”。

安全不是绝对的

如何处理好 Internet 这样一个高度分布、边界模糊、层次欠清、动态演化，而用户又在其中扮演主角的极为复杂而又巨大的系统的安全问题，人们是缺乏思想和技术准备的，但又在苦苦探索着。

人们对 Internet 安全的认识方法，是把这个事物相对的两个方面在不同视角下进行比较、对照、鉴别和选择。

我们可以看到信息安全问题有以下的一些共同点：

安全不是 0 与 1 的关系，没有绝对的安全；

在两个对立面的关系上要把握好“度”，“度”既包括比例关系，也包括结构和顺序；

把握“度”的问题就是组织管理和决策；

组织管理、决策的核心是人，人的因素贯穿在所有的关系中。

总之，在人们已经总结出的这些规律中，哪一条

也离不开管理，离不开人的因素。

人、网结合是网络时代信息安全的本质特征

人是网络的建设者和使用者、网上内容的提供者和消费者，Internet 作为网络是在自组织机制上发展起来的，极大数量的用户互联、互动使之产生了全新的网络动力学特性，因此网络的两大因素结点和连接是很不均匀的，在用户点击行为偏好、通信价格规模效应等等人—网交互作用下，Internet 在竞争演化中形成了少数结点（路由器或 Web 页面）集中了大量的连接（线路或 URL），往往成万上兆，而绝大多数的其他结点却只有少数几个连接。这是非指数型的拓扑结构。

最近美国的复杂性理论家经过计算得出结论：这种不均匀的非指数型的网络结构对随机和散落的黑客攻击有很强的抗损力，因此 Internet 基本上是正常运转的，甚至 9·11 事件后电话网瘫痪的一段时间内，Internet 成了主要的通信手段。但是如果攻击目标集中在关键网站又采取集团攻击的方式，那么 Internet 就很容易形成大范围的损伤。这个复杂性理论解释了本文一开始提出的悖论。

Internet 的复杂性在很大程度上体现为软件的复杂性，成百上千万行程序的操作系统和应用软件存

在大量 BUG，是不可避免而又极难分析和检测的，要求全世界上亿用户都及时打补丁也是不现实的。因此网络的脆弱性将长期存在，并会随着 Internet 应用的快速发展与日俱增。

必须指出：黑客工具、病毒的制造者是人，Internet 防线最薄弱的环节也是人，80％以上的成功入侵都是利用了人的无知、麻痹和懒惰，所以人的安全意识对 Internet 的安全具有决定作用。

用复杂巨系统的概念对网络安全进行再思考

观察和思考作为开放、复杂巨系统的 In－teRnet 的网络安全行为不能单纯靠还原论的方法把组件分解、分别分析，否则就只能看到复杂性对安全的麻烦。但是我们一旦掌握了它的整体性规律，却又可以反过来为我所用。实际上自由软件 Linux 的出现已经说明网络能为集全球各角落网民智慧之大成提供前所未有的条件。

既然网络被攻击乃至被入侵是不可避免的，那么我们与其站在系统之内，还不如站在系统之上来观察网络安全问题着眼于网络整体的健壮性（鲁棒性）和可生存能力。这种能力意味着网络可以被入侵，可以部分组件受损，乃至某些部件并不完全可靠，但只要系统能在结构上合理配置资源；能在攻击下资源重

组；具有自优化、自维护、自身调节和功能语义冗余等自我保护能力，就仍可完成关键任务。

复杂性使网络对抗的非对称性进一步加强，因为守者要在巨量的弱点上处处设防，而攻者可以攻其一点。因此，谋略具有重要意义，人与信息隐蔽、陷阱、诱骗等技术相结合又通过网址、程序的不断变异和多样性都可以使攻者不知何以攻，这就用得上孙子兵法了。

通过人与信息系统强自学习机制相结合，以及基于人的行为模式和活动特征的积极主动防御技术，特别有利于对未知外部黑客病毒工具和内部滥用犯罪的发现与控制，并走在他们的前面。

用“厅体系”研究和解决网络安全问题

从以上的讨论中可以看出：

Internet 安全对象不是一般的系统，而是开放、人在其中、与社会系统紧密耦合的复杂巨系统；

Internet 安全过程不是一般工程化的过程，而是一个时时处处有人参与的、自适应的、不断演化的、不断涌现出新的整体特性的过程。

Internet 安全管理不是一般的管理手段的叠加和集成，而是综合集成，两者的本质区别在于后者强调人的关键作用，是人网结合、人机结合、充分发挥

各自优势的方法。经过综合集成，系统将涌现出崭新的安全性质整体大于部分之和。

总之，网络安全需要法律、管理和技术的有机结合形成合力，也需要情报、知识和谋略的融合。

在网络安全领域中，现已有丰富的全球网络安全统计数据和案例（主要在网上），但未能下载整理，还有一批有志于此的法律、管理、技术、军事专家，但缺乏彼此的专业知识和相互沟通。

我们认为，钱学森院士提出的“从定性到定量的综合集成研讨厅体系”能把各行专家智慧、群众经验、古今安全知识与我国已具备的高性能计算机、海量存储器、宽带网络和数据融合、挖掘、过滤等处理技术结合起来。各种形式的研讨厅（虚拟的和网上的）是能使群体思维高度激发的“发酵器”，大量的意见在其中碰撞、协同，并通过模型化（形式化与非形式化）及人机结合逐步收敛和递归，必能为形成 Internet 安全新的范式做出贡献。

发掘 Foxmai4.1 的六个隐患

Foxmai4.1 正式版“千呼万唤始出来”，我欣喜之余立即下载并安装了一个试用。毫无疑问，较之以先前的版本，正式版在功能上更为创新与完善，这里我并不想谈它的新功能，而是提醒大家，要注意使用中

的安全问题，因为正式版本中依然存在安全隐患！

破解账户口令

在以前的版本中存在着本地账户口令的漏洞，这个问题在 Foxmai4.1 正式版中依然没有得到解决，不能不令人遗憾。

打开 Foxmai 的安装路径，一般为 C:\Programfiles\Foxmai，找到 Mail 目录下的用户账户目录，比方说有用户的账户为“yzscholar”，则一定存在着一个“yzscholar”目录，打开这个目录，找到一个名为“account.stg”文件，这就是账户配置文件，包含有账户名、邮箱参数、账户口令等重要信息。将之删除或者改名后再运行 Foxmai(建议改名，因为该文件后面还用得着)，这时该目录下会重新生成一个“account.stg”文件，与此同时，原账户的口令也就消失得无影无踪！

邮件泄密

口令既已消除，这样只要运行 Foxmai 就可以轻易打开你的信箱、查看邮件甚至删除邮件！

在测试的过程中，我们发现这样一个问题：使用这种方法只能查看到系统默认的四个信箱，而对于用户自己创建的信箱则无能无为。也就说：只能打开“收件箱”、“发件箱”、“已发送邮件箱”和“废件箱”。

地址簿泄密

点击工具栏中的［地址簿］按钮，可以看到个人地址簿，不仅可以看到好友列表，甚至连好友的分组都一览无余！

签名档泄密

再试试点击工具栏中的［撰写］按钮，弹出图 3 的画面，注意新邮件的底部，看看是什么？哈哈，签名档就这样被轻易盗用了！

冒用邮箱

通过上面的几项简单操作，不难发现，在破解了账户口令之后，我们可以偷窥其邮件、地址簿、签名档等个人资料。那么，是否存在冒名顶替用原用户的邮箱给其好友发信的可能吗？

首先让我们检查一下账户的信息，选定账户名，点击“账户”菜单中的“属性”，结果弹出一个内容为空的窗口，原来我们在破除口令的同时，将邮箱参数也破坏掉了。既然无法得到最重要的邮箱配置信息，也就无法冒用原用户给他人发送邮件了。不过，由此引出了另一个问题：我们可以在不破解账户口令的情况下直接用该账户发送邮件！

有可能吗？是的，可以。还记得我们将“account.stg”文件改名为 INI 吗？现在关闭

Foxmai4.1 正式版，然后将已改名的“account.stg”文件恢复原形，再次启动 Foxmai4.1 正式版。然后打开资源管理器，随便找到一个文件，点击鼠标右键，选择［发送到］→［Foxmai］，瞧，出现了什么窗口？在上图的“收件人”中填上一个邮箱地址，点击［发送］，现在你已经可以原用户的身份给别人发信了！

另一隐患

另一个值得注意的危险地方是 Foxmai4.1 正式版主目录中的 accounts.cfg 文件。

假设你的 Foxmai 安装在 C 盘中，则该文件为 c:\Programfiles\Foxmai\accounts.cfg，将之删除或改名，然后运行 Foxmai，结果会弹出“Foxmai 用户向导”，要求你建立新的用户账户，由此可见，原用户的信息已经“丢失”(姑且这么认为)。我们新建了一个账户“Coolwang”，进入 Foxmai 后点击［地址簿］按钮，可以查看到原用户的好友资料，当然也可以编辑。点击“撰写”图标也可以看到原用户的签名档。所以，这个文件对 Foxmai 的安全也构成了一定的威胁。

以上是我使用 Foxmai4.1 正式版中发现的一些问题，在此提醒大家注意。无疑的 Foxmai 是优秀的国产软件，白璧微瑕，我们共同的心愿是：用好软件，

好软件要让用户用得称心，用得放心！

WindowsXP 中的免费防火墙

在微软最新发布的操作系统 WindowsXP 中，我们会发现许多新的特性，其中有一项不太引人注目的功能，就是互联网连接防火墙（Internetconnecttonfirewall）,那么这个 WindowsXP 中的新东东到底能对我们的爱机起到什么样的保护作用呢，我们究竟应该怎样使用它呢，就请大家随小编我来一起探讨探讨它吧。

首先需要说明的是什么是防火墙，从新华词典中我们可以查到防火墙就是为了防止火势蔓延而在建筑物之间搭建的一道障碍物，而在电脑中，防火墙的作用和现实中也差不了多少，它是在你的个人电脑和外部 Internet 世界建立的一个虚拟的障碍物，当然，它不是为了防止火势蔓延，而是为了防备黑客的攻击。

随着互联网技术的发展，网络给人们带来无限便利的同时也产生了许多问题，黑客问题就是其中一个显著的问题。黑客们的攻击基本上都是通过 Ping 命令查找一个能够连通 IP 地址的主机开始的。当找到这台主机后，通常是使用一些专门的黑客软件来进行端口扫描，来找到系统的漏洞，从而进行攻击。既然

知道黑客攻击的手段是通过 Ping 命令，那么我们只要不响应 Ping 命令，那么黑客就会认为这台主机无法连通从而放弃对它的攻击，微软当然清楚地知道这一点，所以 XP 中的互联网连接防火墙当然就不响应 Ping 命令，而且，它还禁止外部程序对本机进行端口扫描，抛弃所有没有请求的 IP 包。所以，它可以在一定的程度上很好地保护我们的个人电脑。但是，它毕竟只提供了一些基本的防范黑客的手段，所以并不能替代一些商业的个人防火墙，更不宜使用在服务上。

我说了那么多，大家一定已经厌烦了，好了，下面就由本小编进入大家感兴趣的部分，怎样设置互联网连接防火墙。

打开开始菜单-〉网上邻居，点击查看网络连接，选中本地连接，单击鼠标右键

点击高级选中通过限制或阻止来自 Internet 的对此计算机的访问来保护我的计算机和网络。这时右下方的设置就变为可选。

点击设置

互联网连接防火墙的设置主要有三部分：第一部分是服务项。通过设定这一部分可以让防火墙禁止和允许哪些服务。第二部分是关于日志的。它可以记录

所有允许和拒绝进入的数据包以便可以让你进行进一步的分析。第三部分就是关于 ICMP 的，我的建议是禁止所有的 ICMP 响应。

但是在局域网中应该尽量不使用互联网连接防火墙，因为它会给一些网络应用带来影响。比如说访问共享文件夹，使用 OICQ 的语音功能。解决这样的问题也很简单，一种当然是取消防火墙，但这不是推荐的方法。另一种方法就是找到到底 OICQ 使用哪个端口来实现语音功能，在前面介绍的属性→高级→设置→服务中来添加一项自定义设置从而使防火墙忽略这个端口的检测。这样，OICQ 的语音功能就可以正常使用了。

好了，防火墙的使用我们已经介绍完了，需要说明的是，它并不能完全替代一些商业的防火墙软件，但是，对于拨号上网的个人电脑用户，它确实能起到很好的防护作用，另外一点重要的是它是免费的，并且基本上不占用什么系统资源。

入侵检测技术综述(1)

系统风险与入侵检测

计算机网络的安全是一个国际化的问题，每年全球因计算机网络的安全系统被破坏而造成的经济损失达数百亿美元。进入新世纪之后，上述损失将达

2000 亿美元以上。

政府、银行、大企业等机构都有自己的内网资源。从这些组织的网络办公环境可以看出，行政结构是金字塔型，但是局域网的网络管理却是平面型的，从网络安全的角度看，当公司的内部系统被入侵、破坏与泄密是一个严重的问题，以及由此引出的更多有关网络安全的问题都应该引起我们的重视。据统计，全球80%以上的入侵来自于内部。此外，不太自律的员工对网络资源无节制的滥用对企业可能造成巨大的损失。

当商户、银行与其他商业与金融机构在电子商务热潮中纷纷进入 Internet，以政府上网为标志的数字政府使国家机关与 Internet 互联。通过 Internet 实现包括个人、企业与政府的全社会信息共享已逐步成为现实。随着网络应用范围的不断扩大，对网络的各类攻击与破坏也与日俱增。无论政府、商务，还是金融、媒体的网站都在不同程度上受到入侵与破坏。网络安全已成为国家与国防安全的重要组成部分，同时也是国家网络经济发展的关键。

据统计：信息窃贼在过去 5 年中以 250%速度增长，99%的大公司都发生过大的入侵事件。世界著名的商业网站，如 Yahoo、Buy、Ebay、Amazon、CNN 都

曾被黑客入侵，造成巨大的经济损失。甚至连专门从事网络安全的 RSA 网站也受到黑客的攻击。

对入侵攻击的检测与防范、保障计算机系统、网络系统及整个信息基础设施的安全已经成为刻不容缓的重要课题。

网络安全是一个系统的概念，有效的安全策略或方案的制定，是网络信息安全的首要目标。网络安全技术主要有，认证授权、数据加密、访问控制、安全审计等。本文着重讨论的入侵检测技术是安全审计中的核心技术之一，是网络安全防护的重要组成部分。

入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。违反安全策略的行为有：入侵—非法用户的违规行为；滥用—用户的违规行为。

利用审计记录，入侵检测系统能够识别出任何不希望有的活动，从而达到限制这些活动，以保护系统的安全。入侵检测系统的应用，能使在入侵攻击对系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击。在入侵攻击过程中，能减少入侵攻击所造成的损失。在被入侵攻击后，收集入侵攻击的相关信息，作为防范系统的知识，添加入知识库内，

以增强系统的防范能力。

入侵检测产品分析

1. 入侵检测产品

经过几年的发展，入侵检测产品开始步入快速的成长期。一个入侵检测产品通常由两部分组成：传感器(Sensor)与控制台(ConsoLe)。传感器负责采集数据(网络包、系统日志等)、分析数据并生成安全事件。控制台主要起到中央管理的作用，商品化的产品通常提供图形界面的控制台，这些控制台基本上都支持WindowsNT平台。

从技术上看，这些产品基本上分为以下几类：基于网络的产品和基于主机的产品。混合的入侵检测系统可以弥补一些基于网络与基于主机的片面性缺陷。此外，文件的完整性检查工具也可看作是一类入侵检测产品。

2.基于网络的入侵检测

基于网络的入侵检测产品（NIDS）放置在比较重要的网段内，不停地监视网段中的各种数据包。对每一个数据包或可疑的数据包进行特征分析。如果数据包与产品内置的某些规则吻合，入侵检测系统就会发出警报甚至直接切断网络连接。目前，大部分入侵检测产品是基于网络的。值得一提的是，在网络入侵检

测系统中，有多个久负盛名的开放源码软件，它们是Snort、NFR、Shadow等，其中Snort的社区(http://www.snort.org)非常活跃，其入侵特征更新速度与研发的进展已超过了大部分商品化产品。网络入侵检测系统的优点：

网络入侵检测系统能够检测那些来自网络的攻击，它能够检测到超过授权的非法访问。

一个网络入侵检测系统不需要改变服务器等主机的配置。由于它不会在业务系统的主机中安装额外的软件，从而不会影响这些机器的CPU、I/O与磁盘等资源的使用，不会影响业务系统的性能。

由于网络入侵检测系统不像路由器、防火墙等关键设备方式工作，它不会成为系统中的关键路径。网络入侵检测系统发生故障不会影响正常业务的运行。布署一个网络入侵检测系统的风险比主机入侵检测系统的风险少得多。

网络入侵检测系统近年内有向专门的设备发展的趋势，安装这样的一个网络入侵检测系统非常方便，只需将定制的设备接上电源，做很少一些配置，将其连到网络上即可。

网络入侵检测系统的弱点:

网络入侵检测系统只检查它直接连接网段的通

信，不能检测在不同网段的网络包。在使用交换以太网的环境中就会出现监测范围的局限。而安装多台网络入侵检测系统的传感器会使布署整个系统的成本大大增加。

网络入侵检测系统为了性能目标通常采用特征检测的方法，它可以检测出普通的一些攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。

网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少回传的数据量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器。这样的系统中的传感器协同工作能力较弱。

网络入侵检测系统处理加密的会话过程较困难，目前通过加密通道的攻击尚不多，但随着 IPv6 的普及，这个问题会越来越突出。

3．基于主机的入侵检测

基于主机的入侵检测产品（HIDS）通常是安装在被重点检测的主机之上，主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果其

中主体活动十分可疑(特征或违反统计规律)，入侵检测系统就会采取相应措施。

主机入侵检测系统的优点:

主机入侵检测系统对分析“可能的攻击行为”非常有用。举例来说，有时候它除了指出入侵者试图执行一些“危险的命令”之外，还能分辨出入侵者干了什么事：他们运行了什么程序、打开了哪些文件、执行了哪些系统调用。主机入侵检测系统与网络入侵检测系统相比通常能够提供更详尽的相关信息。

主机入侵检测系统通常情况下比网络入侵检测系统误报率要低，因为检测在主机上运行的命令序列比检测网络流更简单，系统的复杂性也少得多。

主机入侵检测系统可布署在那些不需要广泛的入侵检测、传感器与控制台之间的通信带宽不足的情况下。主机入侵检测系统在不使用诸如“停止服务”、“注销用户”等响应方法时风险较少。

主机入侵检测系统的弱点:

主机入侵检测系统安装在我们需要保护的设备上。举例来说，当一个数据库服务器要保护时，就要在服务器本身上安装入侵检测系统。这会降低应用系统的效率。此外，它也会带来一些额外的安全问题，安装了主机入侵检测系统后，将本不允许安全管理员

有权力访问的服务器变成他可以访问的了。

主机入侵检测系统的另一个问题是它依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必需重新配置，这将会给运行中的业务系统带来不可预见的性能影响。

全面布署主机入侵检测系统代价较大，企业中很难将所有主机用主机入侵检测系统保护，只能选择部分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，入侵者可利用这些机器达到攻击目标。

主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。对入侵行为的分析的工作量将随着主机数目增加而增加。

入侵检测技术综述（2）

1.技术分类

入侵检测系统所采用的技术可分为特征检测与异常检测两种。

特征检测

特征检测(Signature-baseddetection)又称Misusedetection，这一检测假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已有的入侵方法检查出来，但

对新的入侵方法无能为力。其难点在于如何设计模式既能够表达“入侵”现象又不会将正常的活动包含进来。

异常检测

异常检测(Anomalydetection)的假设是入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的“活动简档”，将当前主体的活动状况与“活动简档”相比较，当违反其统计规律时，认为该活动可能是“入侵”行为。异常检测的难题在于如何建立“活动简档”以及如何设计统计算法，从而不把正常的操作作为“入侵”或忽略真正的“入侵”行为。

2.常用检测方法

入侵检测系统常用的检测方法有特征检测、统计检测与专家系统。据公安部计算机信息系统安全产品质量监督检验中心的报告，国内送检的入侵检测产品中 95％是属于使用入侵模板进行模式匹配的特征检测产品，其他 5％是采用概率统计的统计检测产品与基于日志的专家知识库系产品。

特征检测

特征检测对已知的攻击或入侵的方式作出确定性的描述，形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时，即报警。原理上与专

家系统相仿。其检测方法上与计算机病毒的检测方式类似。目前基于对包特征描述的模式匹配应用较为广泛。

该方法预报检测的准确率较高，但对于无经验知识的入侵与攻击行为无能为力。

统计检测

统计模型常用异常检测，在统计模型中常用的测量参数包括：审计事件的数量、间隔时间、资源消耗情况等。常用的入侵检测 5 种统计模型为：

操作模型，该模型假设异常可通过测量结果与一些固定指标相比较得到，固定指标可以根据经验值或一段时间内的统计平均得到，举例来说，在短时间内的多次失败的登录很有可能是口令尝试攻击；

方差，计算参数的方差，设定其置信区间，当测量值超过置信区间的范围时表明有可能是异常；

多元模型，操作模型的扩展，通过同时分析多个参数实现检测；

马尔柯夫过程模型，将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化，当一个事件发生时，或状态矩阵该转移的概率较小则可能是异常事件；

时间序列分析，将事件计数与资源耗用根据时间

排成序列，如果一个新事件在该时间发生的概率较低，则该事件可能是入侵。

统计方法的最大优点是它可以“学习”用户的使用习惯，从而具有较高检出率与可用性。但是它的“学习”能力也给入侵者以机会通过逐步“训练”使入侵事件符合正常操作的统计规律，从而透过入侵检测系统。

专家系统

用专家系统对入侵进行检测，经常是针对有特征入侵行为。所谓的规则，即是知识，不同的系统与设置具有不同的规则，且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达，是入侵检测专家系统的关键。在系统实现中，将有关入侵的知识转化为 If-then 结构（也可以是复合结构），条件部分为入侵特征，then 部分是系统防范措施。运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性。

入侵检测产品选择要点

当您选择入侵检测系统时，要考虑的要点有：

1.系统的价格

当然，价格是必需考虑的要点，不过，性能价格

比、以及要保护系统的价值可是更重要的因素。

2.特征库升级与维护的费用

象反病毒软件一样，入侵检测的特征库需要不断更新才能检测出新出现的攻击方法。

3.对于网络入侵检测系统，最大可处理流量(包/秒 PPS)是多少

首先，要分析网络入侵检测系统所布署的网络环境，如果在 512K 或 2M 专线上布署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。

4.该产品容易被躲避吗

有些常用的躲开入侵检测的方法，如：分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等。

5.产品的可伸缩性

系统支持的传感器数目、最大数据库大小、传感器与控制台之间通信带宽和对审计日志溢出的处理。

6.运行与维护系统的开销

产品报表结构、处理误报的方便程度、事件与事志查询的方便程度以及使用该系统所需的技术人员数量。

7.产品支持的入侵特征数

不同厂商对检测特征库大小的计算方法都不一

样，所以不能偏听一面之辞。

8.产品有哪些响应方法

要从本地、远程等多个角度考察。自动更改防火墙配置是一个听上去很“酷”的功能，但是，自动配置防火墙可是一个极为危险的举动。

9.是否通过了国家权威机构的评测

主要的权威测评机构有：国家信息安全测评认证中心、公安部计算机信息系统安全产品质量监督检验中心。

入侵检测技术发展方向

无论从规模与方法上入侵技术近年来都发生了变化。入侵的手段与技术也有了“进步与发展”。入侵技术的发展与演化主要反映在下列几个方面：

入侵或攻击的综合化与复杂化。入侵的手段有多种，入侵者往往采取一种攻击手段。由于网络防范技术的多重化，攻击的难度增加，使得入侵者在实施入侵或攻击时往往同时采取多种入侵的手段，以保证入侵的成功几率，并可在攻击实施的初期掩盖攻击或入侵的真实目的。

入侵主体对象的间接化，即实施入侵与攻击的主体的隐蔽化。通过一定的技术，可掩盖攻击主体的源地址及主机位置。即使用了隐蔽技术后，对于被攻击

对象攻击的主体是无法直接确定的。

入侵或攻击的规模扩大。对于网络的入侵与攻击，在其初期往往是针对于某公司或一个网站，其攻击的目的可能为某些网络技术爱好者的猎奇行为，也不排除商业的盗窃与破坏行为。由于战争对电子技术与网络技术的依赖性越来越大，随之产生、发展、逐步升级到电子战与信息战。对于信息战，无论其规模与技术都与一般意义上的计算机网络的入侵与攻击都不可相提并论。信息战的成败与国家主干通信网络的安全是与任何主权国家领土安全一样的国家安全。

入侵或攻击技术的分布化。以往常用的入侵与攻击行为往往由单机执行。由于防范技术的发展使得此类行为不能奏效。所谓的分布式拒绝服务（DDoS）在很短时间内可造成被攻击主机的瘫痪。且此类分布式攻击的单机信息模式与正常通信无差异，所以往往在攻击发动的初期不易被确认。分布式攻击是近期最常用的攻击手段。

攻击对象的转移。入侵与攻击常以网络为侵犯的主体，但近期来的攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统，且有愈演愈烈的趋势。现已有专门针对 IDS 作攻击的报道。攻击者详细地分析了 IDS 的审计方式、特征描述、通信模式

找出 IDS 的弱点，然后加以攻击。

今后的入侵检测技术大致可朝下述三个方向发展。

分布式入侵检测：第一层含义，即针对分布式网络攻击的检测方法；第二层含义即使用分布式的方法来检测分布式的攻击，其中的关键技术为检测信息的协同处理与入侵攻击的全局信息的提取。

智能化入侵检测：即使用智能化的方法与手段来进行入侵检测。所谓的智能化方法，现阶段常用的有神经网络、遗传算法、模糊技术、免疫原理等方法，这些方法常用于入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用的方法之一。特别是具有自学习能力的专家系统，实现了知识库的不断更新与扩展，使设计的入侵检测系统的防范能力不断增强，应具有更广泛的应用前景。应用智能体的概念来进行入侵检测的尝试也已有报道。较为一致的解决方案应为高效常规意义下的入侵检测系统与具有智能检测功能的检测软件或模块的结合使用。

全面的安全防御方案：即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测多方位全面对所关注的

网络作全面的评估，然后提出可行的全面解决方案。

来自德国的魔法师帮您找回丢失的密码

如果你的 QQ 密码不见了，你很不幸，和 MM 挥手告别，重新上路吧！如果你的信用卡密码不见了，你惨了，算一算你的卡里还有多少钱，争取赶在小偷把你的钱取走之前，去挂失吧！如果你把系统管理员密码弄丢了，那你死定了！准备收拾收拾，回家吧！

让我们请出来自德国的魔法师 O&Oblueconv4professional，它是一款 WindowsNT4/2000/XP 的系统管理和修复工具，支持 NTFS 文件系统。在这位魔法师的帮助下，你可以轻轻松松恢复系统管理员的密码。

创建启动盘

启动盘通过运行软件中的“O&Obootwtzardpro”程序生成，而且要准备六张软盘。

选择创建启动盘的方式，可创建光盘启动盘或软盘启动盘，一般是选“Floopydisk”。

输入操作系统的安装路径，可以是光盘驱动器路径或网络路径。只有正确输入，才能进行下一步操作，同时检测出你的操作系统的类型。

为启动盘指定保存路径，可以为硬盘中的某个目录，然后选中“Copydisk folderstoflopydisk”。

若有硬件不能够被 WindowsNT4/2000 本身自动支

持，请选中“Useoemcontrollerdrivers”后再点“Add”添加。

为启动盘添加一些有用的工具，当创建启动盘的时候，这些工具会被拷贝至启动盘中。选中“Copytools”后再自行选择添加。

选择加密保护以保证启动盘的安全，连续输入二次密码确认。

将开始创建并配置启动盘文件，并将文件拷贝至软盘。

恢复密码

首先插入第一张软盘，开机后听到“滴”的一声，按下[DeL]键进入 CMOS，将系统参数改为用软盘启动。待重新启动计算机后，按照屏幕的提示依次插入剩余的软盘，直至启动完成。出现一个蓝色的界面，即软件独特的“Bluescreen”模式，相当于一个小型的字符式操作系统。

恢复密码通过敲入命令 Passwd 实现，格式为：Passwd[account][newpassword]比如你想把新的管理员密码设为 ABC，则相应的命令为：

PasswdadministratorABC 当密码成功修改，会显示“Passwordwassuccessfullychanged”字样。

注意：若 Passwd 命令后面为空，则意味着清空

密码，这样做并不安全。

入侵检测系统技术现状及其发展趋势

1 引言

随着网络技术的发展，网络环境变得越来越复杂，对于网络安全来说，单纯的防火墙技术暴露出明显的不足和弱点，如无法解决安全后门问题；不能阻止网络内部攻击，而调查发现，50％以上的攻击都来自内部；不能提供实时入侵检测能力；对于病毒等束手无策等。因此很多组织致力于提出更多更强大的主动策略和方案来增强网络的安全性，其中一个有效的解决途径就是入侵检测。入侵检测系统（Idsintrusiondetectionsystem）可以弥补防火墙的不足，为网络安全提供实时的入侵检测及采取相应的防护手段，如记录证据、跟踪入侵、恢复或断开网络连接等。这引发了人们对入侵检测技术研究和开发的热情。

2 入侵检测系统的概念

入侵行为主要是指对系统资源的非授权使用，可以造成系统数据的丢失和破坏、系统拒绝服务等危害。对于入侵检测而言的网络攻击可以分为 4 类：

①检查单 IP 包（包括 TCP、UDP）首部即可发觉的攻击，如 Winnuke、Pingofdeath、Land.c、部分

Osdetection、sourceroutIng 等。

②检查单 IP 包，但同时要检查数据段信息才能发觉的攻击，如利用 CGI 漏洞，缓存溢出攻击等。

③通过检测发生频率才能发觉的攻击，如端口扫描、Synflood、smuRf 攻击等。

④利用分片进行的攻击，如 teadrop，nestea，jolt 等。此类攻击利用了分片组装算法的种种漏洞。若要检查此类攻击，必须提前（在 IP 层接受或转发时，而不是在向上层发送时）作组装尝试。分片不仅可用来攻击，还可用来逃避未对分片进行组装尝试的入侵检测系统的检测。

入侵检测通过对计算机网络或计算机系统中的若干关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合就是入侵检测系统。

入侵检测系统执行的主要任务包括：监视、分析用户及系统活动；审计系统构造和弱点；识别、反映已知进攻的活动模式，向相关人士报警；统计分析异常行为模式；评估重要系统和数据文件的完整性；审计、跟踪管理操作系统，识别用户违反安全策略的行为。入侵检测一般分为 3 个步骤，依次为信息收集、数据分析、响应（被动响应和主动响应）。

信息收集的内容包括系统、网络、数据及用户活动的状态和行为。入侵检测利用的信息一般来自系统日志、目录以及文件中的异常改变、程序执行中的异常行为及物理形式的入侵信息 4 个方面。

数据分析是入侵检测的核心。它首先构建分析器，把收集到的信息经过预处理，建立一个行为分析引擎或模型，然后向模型中植入时间数据，在知识库中保存植入数据的模型。数据分析一般通过模式匹配、统计分析和完整性分析 3 种手段进行。前两种方法用于实时入侵检测，而完整性分析则用于事后分析。可用５种统计模型进行数据分析：操作模型、方差、多元模型、马尔柯夫过程模型、时间序列分析。统计分析的最大优点是可以学习用户的使用习惯。

入侵检测系统在发现入侵后会及时作出响应，包括切断网络连接、记录事件和报警等。响应一般分为主动响应（阻止攻击或影响进而改变攻击的进程）和被动响应（报告和记录所检测出的问题）两种类型。主动响应由用户驱动或系统本身自动执行，可对入侵者采取行动（如断开连接）、修正系统环境或收集有用信息；被动响应则包括告警和通知、简单网络管理协议（SNMP）陷阱和插件等。另外，还可以按策略配置响应，可分别采取立即、紧急、适时、本地的长期

和全局的长期等行动。

3 入侵检测系统技术及分类

3.1 入侵检测系统技术

可以采用概率统计方法、专家系统、神经网络、模式匹配、行为分析等来实现入侵检测系统的检测机制，以分析事件的审计记录、识别特定的模式、生成检测报告和最终的分析结果。

发现入侵检测一般采用如下两项技术：

①异常发现技术，假定所有入侵行为都是与正常行为不同的。它的原理是，假设可以建立系统正常行为的轨迹，所有与正常轨迹不同的系统状态则视为可疑企图。异常阀值与特征的选择是其成败的关键。其局限在于，并非所有的入侵都表现为异常，而且系统的轨迹难于计算和更新。

②是模式发现技术，它是假定所有入侵行为和手段（及其变种）都能够表达为一种模式或特征，所有已知的入侵方法都可以用匹配的方法发现。模式发现技术的关键是如何表达入侵的模式，以正确区分真正的入侵与正常行为。模式发现的优点是误报少，局限是只能发现已知的攻击，对未知的攻击无能为力。

3.2 入侵检测系统的分类

通常，入侵检测系统按其输入数据的来源分为 3

种：

①基于主机的入侵检测系统，其输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。

②基于网络的入侵检测系统，其输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。

③分布式入侵检测系统，能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，系统由多个部件组成，采用分布式结构。

另外，入侵检测系统还有其他一些分类方法。如根据布控物理位置可分为基于网络边界（防火墙、路由器）的监控系统、基于网络的流量监控系统以及基于主机的审计追踪监控系统；根据建模方法可分为基于异常检测的系统、基于行为检测的系统、基于分布式免疫的系统；根据时间分析可分为实时入侵检测系统、离线入侵检测系统。

4 入侵检测的主要方法

4.1 静态配置分析

静态配置分析通过检查系统的当前系统配置，诸如系统文件的内容或者系统表，来检查系统是否已经或者可能会遭到破坏。静态是指检查系统的静态特征（系统配置信息），而不是系统中的活动。

采用静态分析方法主要有以下几方面的原因：入侵者对系统攻击时可能会留下痕迹，这可通过检查系统的状态检测出来；系统管理员以及用户在建立系统时难免会出现一些错误或遗漏一些系统的安全性措施；另外，系统在遭受攻击后，入侵者可能会在系统中安装一些安全性后门以方便对系统进行进一步的攻击。

所以，静态配置分析方法需要尽可能了解系统的缺陷，否则入侵者只需要简单地利用那些系统中未知的安全缺陷就可以避开检测系统。

4.2 异常性检测方法

异常性检测技术是一种在不需要操作系统及其防范安全性缺陷专门知识的情况下，就可以检测入侵者的方法，同时它也是检测冒充合法用户的入侵者的有效方法。但是，在许多环境中，为用户建立正常行为模式的特征轮廓以及对用户活动的异常性进行报警的门限值的确定都是比较困难的事，所以仅使用异常性检测技术不可能检测出所有的入侵行为。

目前这类入侵检测系统多采用统计或者基于规则描述的方法建立系统主体的行为特征轮廓：

①统计性特征轮廓由主体特征变量的频度、均值以及偏差等统计量来描述，如 SRI 的下一代实时入侵

检测专家系统，这种方法对特洛伊木马以及欺骗性的应用程序的检测非常有效。

②基于规则描述的特征轮廓由一组用于描述主体每个特征的合法取值范围与其他特征的取值之间关系的规则组成（如 TIM）。该方案还可以采用从大型数据库中提取规则的数据挖掘技术。

③神经网络方法具有自学习、自适应能力，可以通过自学习提取正常的用户或系统活动的特征模式，避开选择统计特征这一难题。

4.3 基于行为的检测方法

通过检测用户行为中那些与已知入侵行为模式类似的行为、那些利用系统中缺陷或间接违背系统安全规则的行为，来判断系统中的入侵活动。

目前基于行为的入侵检测系统只是在表示入侵模式（签名）的方式以及在系统的审计中检查入侵签名的机制上有所区别，主要可以分为基于专家系统、基于状态迁移分析和基于模式匹配等几类。这些方法的主要局限在于，只是根据已知的入侵序列和系统缺陷模式来检测系统中的可疑行为，而不能检测新的入侵攻击行为以及未知的、潜在的系统缺陷。

入侵检测方法虽然能够在某些方面取得好的效果，但总体看来各有不足，因而越来越多的入侵检测

系统都同时采用几种方法，以互补不足，共同完成检测任务。

5 入侵检测系统的结构及标准化

目前，通用入侵检测架构（CIDF）组织和 IETF 都试图对入侵检测系统进行标准化。CIDF 阐述了一个入侵检测系统的通用模型，将入侵检测系统分为 4 个组件：事件产生器、事件分析器、响应单元及事件数据库。CIDF 将入侵检测系统需要分析的数据统称为事件，它可以是网络中的数据包，也可以是从系统日志等其他途径得到的信息。

事件产生器是从整个计算环境中获得事件，并向系统的其他部分提供此事件；事件分析器分析得到的数据，并产生分析结果；响应单元则是对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以是简单的报警。事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。在这个模型中，前三者以程序的形式出现，而最后一个则往往是文件或数据流。

入侵检测系统的几个组件往往位于不同的主机上。一般会有 3 台机器，分别运行事件产生器、事件分析器和响应单元。

IETF 的 Internet 草案工作组（IDWG）专门负责定义入侵检测系统组件之间，及不同厂商的入侵检测系统之间的通信格式，目前只有相关的草案（dRaft），还未形成正式的 RFC 文档。IDWG 文档有：入侵警报协议（IAP），该协议是用于交换入侵警报信息、运行于 TCP 之上的应用层协议；入侵检测交换协议（IDXP），这个应用层协议是在入侵检测实体间交换数据，提供入侵检测报文交换格式（IDMEF）报文、无结构的文本，二进制数据的交换；IDMEF 是数据存放格式隧道（TUNNEL）文件，允许块可扩展交换协议（BEEP）对等体能作为一个应用层代理，用户通过防火墙得到服务。IAP 是最早设计的通信协议，它将被 IDXP 替换，IDXP 建立在 BEEP 基础之上，TUNNEL 文件配合 IDXP 使用。

6 入侵检测系统面临的主要问题及发展趋势

6.1 入侵检测系统面临的主要问题

6.1.1 误报

误报是指被入侵检测系统测出但其实是正常及合法使用受保护网络和计算机的警报。假警报不但令人讨厌，并且降低入侵检测系统的效率。攻击者可以而且往往是利用包结构伪造无威胁“正常”假警报，以诱使收受人把入侵检测系统关掉。

没有一个入侵检测无敌于误报，应用系统总会发生错误，原因是：缺乏共享信息的标准机制和集中协调的机制，不同的网络及主机有不同的安全问题，不同的入侵检测系统有各自的功能；缺乏揣摩数据在一段时间内行为的能力；缺乏有效跟踪分析等。

6.1.2 精巧及有组织的攻击

攻击可以来自四方八面，特别是一群人组织策划且攻击者技术高超的攻击，攻击者花费很长时间准备，并发动全球性攻击，要找出这样复杂的攻击是一件难事。

另外，高速网络技术，尤其是交换技术以及加密信道技术的发展，使得通过共享网段侦听的网络数据采集方法显得不足，而巨大的通信量对数据分析也提出了新的要求。

6.2 入侵检测系统的发展趋势

从总体上讲，目前除了完善常规的、传统的技术（模式识别和完整性检测）外，入侵检测系统应重点加强与统计分析相关技术的研究。许多学者在研究新的检测方法，如采用自动代理的主动防御方法，将免疫学原理应用到入侵检测的方法等。其主要发展方向可以概括为：

（1）分布式入侵检测与 CIDF

传统的入侵检测系统一般局限于单一的主机或网络架构，对异构系统及大规模网络的检测明显不足，同时不同的入侵检测系统之间不能协同工作。为此，需要分布式入侵检测技术与 CIDF。

（2）应用层入侵检测

许多入侵的语义只有在应用层才能理解，而目前的入侵检测系统仅能检测 Web 之类的通用协议，不能处理如 LotusNotes 数据库系统等其他的应用系统。许多基于客户／服务器结构、中间件技术及对象技术的大型应用，需要应用层的入侵检测保护。

（3）智能入侵检测

目前，入侵方法越来越多样化与综合化，尽管已经有智能体系、神经网络与遗传算法应用在入侵检测领域，但这些只是一些尝试性的研究工作，需要对智能化的入侵检测系统进一步研究，以解决其自学习与自适应能力。

（4）与网络安全技术相结合

结合防火墙、PKIX、安全电子交易（SET）等网络安全与电子商务技术，提供完整的网络安全保障。

（5）建立入侵检测系统评价体系

设计通用的入侵检测测试、评估方法和平台，实现对多种入侵检测系统的检测，已成为当前入侵检测

系统的另一重要研究与发展领域。评价入侵检测系统可从检测范围、系统资源占用、自身的可靠性等方面进行，评价指标有：能否保证自身的安全、运行与维护系统的开销、报警准确率、负载能力以及可支持的网络类型、支持的入侵特征数、是否支持 IP 碎片重组、是否支持 TCP 流重组等。

总之，入侵检测系统作为一种主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。随着网络通信技术安全性的要求越来越高，为给电子商务等网络应用提供可靠服务，而由于入侵检测系统能够从网络安全的立体纵深、多层次防御的角度出发提供安全服务，必将进一步受到人们的高度重视。

学用在线杀毒

在线杀毒是一种由网站提供的、为本地硬盘进行在线病毒扫描的服务，它利用目前浏览器支持 ActIveX 标准的特性，通过访问者浏览网页并且下载杀毒引擎控件，从而达到对本地硬盘进行病毒查杀的目的。

在线杀毒的方法

首先，操作者要登录在线网站，并在“在线服务”中点击“在线杀毒”的链接，完成登录。第一次进行

在线杀毒，程序会自动将扫毒引擎与病毒代码下载到用户的硬盘上，电脑的速度就会很慢，需要用户耐心等待。一会儿后，一个需要操作者下载插件的页面就会弹出来，点击“是”按钮，下载就开始了。插件的下载进度显示在一个全英文的窗口中，这期间如果用户想放弃操作，只需点击“CanceL”按钮。当插件下载结束后，在屏幕上就会显示出“我的电脑”以及在线杀毒的介绍、使用方法和注意事项等。

接下来，操作者要在磁盘列表窗口中选择要扫描的目标，操作与在电脑上使用单机版杀毒软件一样，只需在“我的电脑”的下拉菜单里选择想要扫描的磁盘或者文件夹，并将其选中，点击“开始扫描”按钮，就开始进行本地硬盘的在线杀毒了。这时，屏幕就会出现显示窗口，其中正在扫描的文件夹与文件不停地显示在窗口中，在这个过程中如果发现病毒，病毒名称及染毒文件名称就会显示在下面的窗口中。一旦有病毒被扫描发现，在窗口的左边以前不可选的几个按钮就变成可选的了，使用者可以根据自己的情况选择“清除病毒”、“删除文件”等来对查获的病毒进行处理。如果扫描过程中没有发现病毒，在扫描完成后又会有对话框弹出，显示没有发现病毒。最后还会有一个对话框来询问是否进行另一次操作，如果选择“否”

就完成了这次在线杀毒的全部过程。

在线杀毒的注意事项

1．在操作开始之前有必要将电脑中正在运行的程序退出，尤其是占用系统资源较多的程序，以免造成软件之间的冲突或者系统资源的紧张，从而导致杀毒不能正常进行；

2．浏览器的 JavaScRIpt 不能关闭，否则将影响浏览器版本的自动判断和插件下载；

3．第一次进行在线杀毒时，由于需要一定的时间，因而最好选择网速较快的时段进行；

4．在线杀毒对于浏览器目前只支持 IE 或是 Netscape，并且 IE 的版本最好在 3．02 以上；

5．浏览器的菜单栏/工具/Internet 选项中的安全标签的安全级别要设置为“低”，这样在线杀毒才能进行得更为顺利，但切记在杀毒结束后要调回到适当的级别，以保证浏览的安全；

6．在线杀毒虽然免费好用，但是电脑中还是需要安装一个单机版的杀毒软件，这样才可以保证电脑的安全，而不至于被病毒侵害。

如何拒绝垃圾邮件

时下，电子邮件应用范围日趋扩大，用户收发的邮件也是越来越多，然而不幸的是收到的垃圾邮件也

越来越多。下面介绍在使用 Foxmai 的情况下，设置拒绝垃圾邮件：

比如你不想接收“123@123.com”的邮件，那么设置方法如下：

1.在“账户”菜单中单击“过滤器”，打开“过滤管理器”对话框。

2.单击“新建”按钮，选择“条件”选项卡，然后在“名字”栏中输入相应的名称，这仅仅是一个代号而已，实际价值不大。比如我们键入“黑名单 1”。

3.在“应用于”标题下，选择“来信”选项，则对收到的邮件进行过滤；选择“发信”选项，则对用户自己发出去的邮件进行过滤；选择“手工”选项，则由用户手工选择过滤。不过在选中了“手工”复选项后，用户不能设置“直接从服务器删除”邮件，因为两者是矛盾的。在此，我们选中“来信”复选框，即单击以使其前框中出现一个对号“✓”。

4.在“条件”标题下的“位置”栏中选择需要过滤的项目所在位置，可选位置有“收件人”、“发件人”、“主题”等。在此，我们选中“任何地方”。然后，在下面的下拉框中选择适当的判断方式，并在其后的框中输入过滤项目，如发件人姓名、主题内容中的某段文本、附件的文件名等。在此，我们选择“包含”

后，输入“123@123.com”(如下图)。

5.单击“动作”选项卡，在列表中选择对过滤邮件的处理方式，如“转移”、“拷贝”、“转发”、“重定向”、“回复”、“改变标签”、“发出声音”等。在此，我们选择“直接从服务器删除”复选框。单击“确定”按钮。至此，Foxmai 过滤器设置完成，以后你就再也不会收到“123@123.com”发给你的邮件了。

6.Foxmai 中除了设置过滤规则来拒绝垃圾邮件的功能,还有强大的远程管理邮箱的功能.在 Foxmai 的“工具”栏中点击“远程邮箱管理”,输入正确的邮件密码以后,就能在客户端远程管理自己的邮箱。用户可以根据收到的邮件头信息进行判断,如果邮件不是您需要的,那只要右键点击信件,选择“删除”,然后在上面工具栏中点“执行”,这样就可以把不受欢迎的邮件直接从服务器上删除掉。如果是需要的邮件,只需选择“收取”,并执行即可。

如何设定一个安全的密码

笔者在密码选取方法上却另辟蹊径，积累的一点体会现说出来与大家共同探讨交流。

一、尽量选用密码位数多的电子邮箱

现在的免费邮箱的密码位数一般都是 8 位，如 263 等。密码长度少，就容易被破解。但各省市的电

信门户网站提供的免费邮箱的密码长度往往达到了10位，甚至达到了14位。如果有人想破解这么长的密码，恐怕他们得仔细考虑破解这样的密码所花的上网费了。

二、巧设双邮箱

密码位数多了，问题也接着来了：怎么能记住呢？其实，按照我的方法根本不需要记忆密码。其诀窍就是：申请两个邮箱A、B。邮箱A公开(也就是别人可以知道你的登录用户名，即邮箱地址@前的字符)，邮箱B不公开。对于邮箱B(密码可以随意选用)，由于别人不会知道用户名(接收信件使用邮箱B，而发信时使用邮箱A)，因此就无法破解该邮箱的密码。仔细、慎重选好邮箱A的密码(密码选择技巧下面会谈到)，然后将该密码保存在邮箱B中(方法是：将密码保存在文本文件中，然后在邮箱B中作为附件自己给自己发信)。需要登录邮箱A时，先到邮箱B中取密码。这里需要对邮箱A进行一些设置：使用自动转信功能把邮件转发到邮箱B(现在的免费邮箱几乎都支持自动转发功能)，并且在邮箱A的服务器上不备份邮件。平常收发邮件使用邮箱B。由于邮箱A不备份邮件，只是作为转发邮箱使用，因此破解侵入该邮箱就显得毫无意义了，即使被破解也不会有多少损失，

而且不怕邮件炸弹。

三、注意事项

建立双邮箱尽管有很多好处，但是在使用过程中还应该注意：1、对于来历不明的邮件，需要回复时，使用邮箱 A 而不使用邮箱 B，否则很容易暴露邮箱 B。2、邮箱 B 中请不要使用自动回复功能，以免暴露该邮箱。3、在设置邮箱的“密码提示问题”时，提示回答最好不用英文，而是尽量用别人猜想不到的中文句子，以防止别人在邮箱的登录页面使用“密码遗忘”功能这条安全性非常脆弱的“路径”侵入你的邮箱。

四、善意提醒

为了更好保证邮箱的安全，还需注意：在网吧等公共场所收发邮件完毕后，一定要单击网页上的“退出”按钮，这样才算真正退出邮件系统(我经常看到网吧里电脑显示“你的信件已经成功发送”而发信人却走了。这是很不安全的，别人只要单击“后退”或者“返回”按钮，就可以侵入该邮箱了)；下网时要关闭所有的浏览器窗口，并且要清除上网的历史记录(或者直接删除 WindowsTemporaRy Internet Files 文件夹下的内容)；定期更换邮箱的密码。

五、总结

如何选择更为安全的密码呢？我的体会是：密码

最好选用键盘上找不到的字符，如特殊字符和汉字等(这些字符大多数是双字节的，每个字符占两位密码，多数免费邮箱均支持)。这些特殊字符如№、‰、五角星★☆、三角形等等。数字、字母、特殊字符和汉字等结合起来使用，这样组成的密码很难被破解。

几款声名显赫的反黑利器

具有类似功能的黑客软件还有很多，它们大都能利用扫描端口、系统后门、拥塞攻击、欺骗密码等手段，对广大网友进行骚扰。有了这些黑客软件，不管你计算机和网络技术水平高低，都能轻轻松松作黑客了。对于我们广大网友来说，个人防黑也就迫在眉睫了，不然，你的账号密码不说，可能写给女友的情书也会被人盗走。俗话说魔高一尺，道高一丈，下面阿拱介绍几款声名显赫专门对付黑客的反黑利器，拥有它们保准让你降妖除魔，手到擒来，此从再不用担心你的后门会泄密了。

木马克星是专门针对国产木马的软件，是动态监视网络与静态特征字扫描的完美结合。木马克星可以查杀 3759 种国际木马，并能查杀冰河所有版本、黑洞 2001 所有版本等等国产木马。木马克星采用监视硬盘技术，不占用 cpu 负荷，占用系统资源更少。木马克星是中英文软件，界面简单，初学者很容易上手。

不过木马克星在未注册情况下只能查而不能杀。

The CLeaneR

软件版本：3.2

软件大小：1825KB

The CLeaneR 是一款英文版的查杀“木马”的软件。它能帮助你查杀多达 100 多种特洛伊木马，几乎包括所有较出名的如 Netspy、BO、Netbus、GIRLfRIend、Happy99、BackDoor 以及它们的一些不同版本。还有一些比较特别的木马都能查杀。The CLeaneR 还提供了实时的监控功能，随时监控有没有黑客攻击和是否感染木马。

TRojan RemoveR

软件版本：4.2.0

软件大小：1429KB

Trojan Remover 专门用来清除特洛伊木马和自动修复系统文件的工具。能够检查系统登录文件、扫描 WIN.INI、SYSTEM.INI 和系统登录文件，且扫描完成后会产生 Log 信息文件，并帮你自动清除特洛伊木马和修复系统文件。每次启动系统，TRojan RemoveR 都会自动运行并查杀木马程序。

LockDown2000

软件版本：7.0.0.6d

软件大小：2413KB

黑客每天都在存取家用或者商用的电脑，而且绝大多数的黑客连接上你的电脑之后不会留下他光顾的痕迹。或许，黑客侵入之后，也许仅仅是运行一下简单的Windows程序，如果他对你的个人资料感兴趣，那么你的个人信息、数据库、信用卡信息、收支记录、电子邮件、源代码等信息，都有可能被公开。即使你使用密码保护你的电脑或者是局域网，黑客们还是有办法采用一些破解软件攻克它。Lockdown2000 充当你的电脑和 Internet 之间的防火墙，可以有效防范黑客的入侵。趁你的电脑尚未被不速之客光顾，快建起你的个人防火墙吧！

X-NetStat III

软件版本：3.0

软件大小：441KB

X-NetStat 监视当前网络和互联网络连接。XNS 可显示每一个当前连接的本地/远程网络地址、本地/远程端口和连接状态，支持 ICMP、UDP、TCP 协议。任何时候当你连接到一个网站、检查电子邮件、发送 ICQ 信息，或者系统内后门激活时，XNS 都能够探测到，并在其窗口中显示每一个连接的详细信息。X-NetStat 可让你深入到网络活动的细节，拥有直观

的接口界面，在装入系统时隐藏（在任务栏内无显示）。X-NetStat III 比较适合那些想研究攻击者身分的网络用户，它比较专业，但不提供查杀黑客木马功能。

天网防火墙个人版

软件版本：2.03.102 Beta

软件大小：646KB

最后是阿拱极力推荐的一款软件。抵御黑客的攻击应该防患于未然，应该在有可能感染前就堵住可能让你机器全军覆没的 BUG。天网防火墙个人版是目前国内普通用户选用最多的防黑工具，它能随着系统的启动时刻监查来自网络的攻击，同时还能根据用户设置的安全选项来截住攻击的路径。对于攻击，天网防火墙个人版能记录详细的信息，你可以透过双击某一个攻击记录来查看由天网提供的详细说明。天网防火墙个人版是免费的软件，你只需要到软件网站免费注册就能得到一个软件注册码了。

防“黑客”十大绝招

1、使用防病毒软件并且经常将其升级更新，从而使有破坏性的程序远离你的计算机。

2、不可允许网上的商家为了便于你以后购物而储存你的信用卡资料。

3、使用由数字和字母混排而成、难以被破译的口令密码，并且经常更换。

4、对不同的网站和程序，要使用不同口令，以防止被黑客破译。

5、使用最新版本的万维网浏览器软件、电子邮件软件以及其他程序。

6、只向有安全保证的网站发送信用卡号码，留意寻找浏览器底部显示的挂锁图标或钥匙形图标。

7、确认你要打交道的网站地址，留意你输入的地址，比如不要把 ama－zon．com 写成 amozon．com。

8、使用有对 cookIe 程序控制权的安全程序，cookIe 程序会把信息传送回网站。

9、如果你使用数字用户专线或是电缆调制解调器连接因特网，那就要安装防火墙软件，监视数据流动。

10、不要打开电子邮件的附件，除非你知道信息来源。

信息安全标准化简况

信息技术安全方面的标准化，兴起于 70 年代中期，80 年代有了较快的发展，90 年代引起了世界各国的普遍关注。特别是随着信息数字化和网络化的发展和应用，信息技术的安全技术标准化变得更为重

要。因此，标准化的范围在拓展，标准化的进程在加快，标准化的成果也在不断的涌现。现将信息技术安全技术标准的情况综述如下。

1.国内信息技术安全标准化

1.1 信息技术安全标准的制定情况

国内信息技术安全标准的制定工作是从 80 年代中期开始的。一方面是定信息技术设备和设施的安全标准，1985 年发布了第一个标准 GB4943；另一方面是制定信息安全技术标准，于 1994 年月发布了第一批标准。至 1997 年底，已制定、报批和发布了有关信息技术安全的国家标准 13 个和国家军用标准 6 个。现正在制定中的国家标准 14 个。特别是国务院信息化领导小组办公室重视和投入经费支持信息技术标准化以来，在国家技术监督局的组织和管理下，在全国信息技术标准化技术委员会支持下，在各单位的积极参与和协助下，使信息技术安全标准的制定工作有了更快的发展。

1.2 信息技术标准化的组织情况

国际标准化组织 ISO/TC97/SC20 于 1984 年 1 月建立了信息技术的数据加密分委员会，我国派代表参加了这次国际标准化会议。1984 年 7 月，在我国的全国计算机与信息处理标准化技术委员会下，建立了相

应的数据加密分技术委员会，在国家技术监督局和电子工业部的领导下，归口国内外的信息技术数据加密的标准化工作。随着信息技术的发和工作范围的扩大，在原数据加密分委员会的基础上，于 1997 年 8 月改组成了信息技术安全分技术委员会（与 ISO/IEC JTC1/SC27 信息技术的安全技术分委会对应）。它是一个具有广泛代表性、权威性和军民结合的信息安全标准化组织。参加的成员单位有电子工业部、安全部、公安部、国务院信息办、国家密管理委员会办公室、央办公厅机要局、军委保密委技检办、国家保密局、总参、邮电部、中国科学院、中国人民银行、有关公司和院校等 22 个部门和单位，共计 25 名委员。

该分委会是信息技术安全标准化的技术组织，其工作范围是负责信息和通信安全的通用框架、方法、技术和机制的标准化，归口国内外对应的标准化工作。技术安全包括：开放式安全体系结构、各种安全信息交换的语义规则、在有关的应用程序接口和协议引用安全功能度的接口等。

由于信息技术的发展，开放系统互连的网络体系结构的广泛应用，信息技术安全标准化越来越受到人们的重视。在信息技术安全分委会的成立会上，研究了信息技术安全标准化的发展规划，明确了指导思

想，确定了工作目标，制定了实施计划，提出了具体的措施，正在为建立完整的信息技术安全标准体系而积极组织开展研究工作和标准制定工作。

1.3 信息技术安全标准化的展望

信息安全关系到国家的安全、社会的安定、经济的发展，信息技术安全标准是信息安全规范化和法制化的基础，是实现技术安全和安全管理的重要手段。信息技术安全标准化必须统一领导、统筹规划、各方参与、分工合作进行，保证其顺利和协调发展。为此，国家技术监督局组织各方面专家参加的标准化技术委员会正在开展以下工作：

1.3.1 加强信息安全标准化的研究

信息技术的安全技术是比较新的和复杂的技术，也是在近年来才得到较快的发展，特别是它的标准化更是如此。为了全面认识和了解信息技术的安全标准，需要对国内外信息技术标准化的情况和发展趋势进行深入的研究。特别是庆将信息技术安全标准体和纱作为重点课题进行综合研究，并建立我国的信息技术安全标准体系，以便能够有目的、有组织、有计划地分期分批进行标准制定工作。这样才能避免标准项目重复和混乱，避免标准之间不协调，也可避免资金人才和时间的浪费。

国际上有很多制定信息安全标准的组织，他们工作各有特点，制定标准的层次不同，也有部分工作重迭，我们对此也应进行深入具体的分析研究。例如：ISO/IEC JTC1/SC27 的重点是制定通用的信息技术安全标准；而 ISO/TC68 则是针对银行系统制定行业具体应用的信息安全标准；ECMA 还制定信息技术设备的安全标准。我们应全面、系统地分析研究，结合我国情况，综合考虑我国的信息技术安全标准化工作。

1.3.2 加快信息技术安全标准的制定

国际互联网的开通，对信息安全标准的需求更加迫切，标准的数量也日益增加，因此应加快信息技术标准的制定工作。国际上 ISO 的信息技术安全标准，包括已正式发布、正在制定的标准项目已有近 70 项，国际互联网的 RFC 文中有 100 多项涉及信息安全，都是比较实用的。我们应在开展研究工作的基础上，建立标准体系，根据轻重缓急，有计划有步骤地安排标准制定项目，合理地组织各方面的力量，开展标准制定工作，最重要的是保证制定标准所必要的经费。

2 国外信息技术安全标准化的情况

国外早在 70 年代中期就开始了信息技术安全标准化工作，现将国际标准化组织、欧洲计算机厂商协会和美国开展信息技术标准化的情况简要介绍如下。

2.1 国际标准化组织的信息技术安全标准化

2.1.1 ISO/IEC JTC1/SC27 信息技术安全

随着跨国计算机网络的开发和不同计算机系统之间互连的要求，数据加密标准化工作也开始走向国际。英国于 1979 年向 ISO/TC97 提出开展数据加密技术标准化的建议，ISO/TC97 采纳了建议，并于 1980 年组建直属工作组。后来，TC97 认为，数据加密技术专业性很强，需幅个分技术委员会来专门开展这方面的标准化工作，于是，1984 年 1 月在联邦德国波恩正式成立分技术委员会 SC20。我国也派人出席了这次会议，并成为该分委员会的 P 成员。从此，数据加密技术标准化工作在 ISO/TC97 内正式蓬勃展开。

1984 年 SC20 成立后，就把在直属工作组期间已开始的密码算法的国际标准化工作接过来，并作为第一优先制定的标准。该算法其实就是美国的 DES，SC27 称其为 DEA-1，而且还指定由法国起草 DEA-2 报告，实际上是公苴算法 RSA。1985 年 1 月第二次分技委员会上同意推进到 DIS，但随后的一年里发生了很大变化。先是 1985 年夏天发布的美国总统令宣布政府将不再支持 DES，并由国家安全局 NSA 设计新的算法标准，算法细节不予公开。这就引起大家对 DES 安全强度的怀疑。有的成员国原本就一直反对密码算法的国

际标准化，认为一个国家采用什么样的密码算法是十分敏感的问题，别人无权干涉。1986 年第三次年会分歧很大，但多数仍赞成推进到国际标准，并交 TC97 处理。同年 5 月，TC97 年会形成决议，密码算法的国际标准化工作已不属技术性问题，而是政治性问题。同年 10 月，ISO 中央理事会决定撤消该项目，并且将密码算法的标准化工作从 SC20 的工作范围内以消，还明确写出不再研究密码算法的标准化。

SC20 的标准项目中包含 OSI 环境下使用加密技术的互操作要求，它与 SC6 和 SC21 的工作范围有重复。1986 年 5 月，TC97 要求三个分委员会主席开会协调，向技术委员会报告协调结果，再由技术委员会决定采以措施。至 1989 年 6 月正式决定撤消原来的 SC20，组建新的 SC27。在 SC20 存在的五年期间完成了两个正式标准：ISO 8372 和 ISO 9160。

1990 年 4 月瑞典斯德哥尔摩托车年会上正式成立 SC27，其名称为：信息技术-安全技术，并对其工作范围作了明晰表述，即信息技术安全的一般方法和技术的标准化，包括：

确定信息技术系统安全的一般要求（含要求方法）；

开发安全技术和机制（含注册程序和安全组成部

分的关系）；

开发安全指南（如解释性文件，风险分析）；

开发管理支撑性文件和标准（如术语和安全评价准则）。

1997 年国际标准化组织的信息技术标准化的技术领域又作了合并和重大调整，但信息技术安全检分委会仍然保留，并作为 ISO/IEC JTC1 安全问题的主导组织。运行模式是既作为了个技术领域的分委员运行，还要履行特殊职能。它负责信息的通信安全的通用框架、方法、技术和机制的标准化，信息技术安全的标准化工作将会更加集中统一和加强。该分委会负责制定标准的项目约为 40 项，进展情况见附件 1。

2.1.2 ISO/TC68 银行和有关的金融服务

在国际标准化组织内，ISO/IDC JTC1/SC27 负责通用信息技术安全标准的制定，ISO/TC68 负责争行业务应用范围内有关信息安全标准的制定。一个是制定通用基础标准，一个是制定行业应用标准，两者在组织上和标准之间都有着密切的联系。他们都是在 80 年代中期开始制定标准的，ISO/TC68 负责制定标准的项目约有 30 项。

2.2 欧洲计算机厂商协会（ECMA）标准

ECMA 人欧洲计算机厂商中吸收会员，经常向 ISO

提交标准提案。ECMA 内的一个组（TC32/TG9）已定义了开放系统应用层安全结构。它的 TC12 负责信息技术设备的安全标准。

它们的工作都假定终端用户控制着通过应用服务元素（ASE）进行通信的实体。ASE 是利用基本服务在恰当地点提供 OSI 环境能力的应用实体的一部分，如文件服务器和打印重绕器。这个小组涉及这些实体之间的安全通信尤其在分布式环境下的安全通信。它们所开发的结构把这些通信分成称为“设施”的单元，每个单元都在提供总体安全中扮演一定的角度，这些设施组合起来就形成了安全系统，这在方式上类似于 ISO 工作中所指的模型。

2.3 美国信息技术安全标准化情况

2.3.1 美国国家标准（ANSI）

美国标准化协会于 80 年代初开始数据加密标准化工作，只制定了三个通用的国家标准。

金融界是实行安全最自觉的早大商业实体，它直接涉及货币和证券的安全电子汇兑。因此，不得不把大量资源投入信息安全。虽然银行和公司的商贸人员属金融界最有形的部分，但也不乏它物。很多大公司已开始采用电子方式订购产品或支付业务费用。随着越来越多地采用电子方式传送货币或资产，计算机犯

罪可能性大增，安全方法变行十分重要。

为了解决安全问题，金融界正积极制定各种标准。美国国家标准化协会（ANSI）负责金融安全的小组是 ASC X9 和 X12。ASC X9 制定金融业务标准，ASC X12 制定商业交易标准。已与美国标准委员会（ASC）召开联席会，共同制定了汇兑的安全标准 9 个。

与此同时，金融领域也在进行金融交易卡、密码服务消息，以及实现商业交易安全等方面的工作。

2.3.2 美国联邦信息处理安全标准（FIPS）

美国联邦政府非常重视自动信息处理的安全，早在70年代初就开始了信息技术安全标准化工作，1974年就已发布标准。1987 年的“计算机安全法案”明确规定了政府的机密数据、发展经济有效的安全保密标准和指南。

联邦信息处理标准由国家标准局（NBS）颁发。FIPS 由 NBS 在广泛搜集政府各部门及私人部门的意见的基础上写成。正式发布之前，将 FIPS 分送给每个政府机构，并在“联邦注册”上刊印出版。经再次征求意见之后，NSB 局长把标准连同 NBS 的建议一起呈送美国商业部和工，由商业部长签字划押同意或反对这个标准。FIPS 安全标准的一个著名实例就是数据加密标准（DES）。至今，它已发布了信息技术安全标

准和指南约 20 个。

2.3.3 美国国防部的信息安全指令和标准（DOD）

美国国防部十分重视信息的安全问题，美国国防部发布了一些有关信息安全和自动信息系统安全的指令、指示和标准，并且加强信息安全的管理，特别是 DOD5200.28-STD《国防可信和计算机系统评估准则》，受到各方面广泛的关注。

信息技术安全标准目录

现将我国和世界的部分信息技术安全标准目录摘编如下：

一、我国信息技术安全标准

1 国家标准

1.1 已发布的标准

GB4943-1995 信息技术设备（包括电气事务设备）的安全世（IEC 950）

GB 9254-88 信息技术设备的无线电干扰极限值和测量方法

GB 9361-88 计算机场地安全要求

GB/T 9387.2-1995 信息处理系统 开放系统互连基本参考模型第 2 部分安全体系结构（IS07489-2：1989）

GB/T15277-1994 信息处理64位块加密算法操作

方式（ISO 8372：1987）

GB/T15278-1994 信息处理-数据加密-物理层互操作性要求（ISO 9160：1988）

GB15851-1995 信息技术-安全技术-带消息恢复的数字签名方案（ISO/IEC 9796：1991）

GB15852-1995 信息技术-安全技术-用块加密算法作校验函数的数据完整性机制（ISO/IEC 9797：1994）

GB15853.1-1995 信息技术-安全技术-实体鉴别机制第 1 部分：一般模型（ISO/IEC 9798-1：1991）

GB15853.2- 信息技术-安全技术-实体鉴别机制第 2 部分；使用对称加密算法的实体鉴别（ISO/IEC 9798-2：1994）

GB15853.3- 信息技术-安全技术-实休鉴别第 3 部分：用非对称签名技术的机制（ISO/IEC 9798-3：1997）

GB * * * *.7-信息技术-开放系统互连-系统管-安全报警报告功能（ISO/IEC10164-7：1992）

GB * * * *.8-信息技术-开放系统互连-系统管理-安全审计跟踪功能（ISO/IEC10164-8：1993）

1.2 正在制定中的标准项目

1）分组过滤防火墙标准：防火墙系统安全技术

要求

2）应用网关防火墙标准：网关安全技术要求

3）网络代量服务器和信息选择平台安全标准

4）鉴别机制标准

5）数字签名机制标准

6）安全电子交易标准第 1 部分；抗低赖机制

7）网络安全服务标准；信息系统安全性评价准则及测试规范

8）安全电子数据交换标准

9）安全电子商务标准化 第 1 部分：密钥管理框架

10）路由器安全技术要求

11）信息技术-n 位块密码算法的操作方式

12）信息技术-开放系统互连-上层安全模型

13）信息技术-开放系统互连-网络层安全协议

14）信息技术-安全技术-实体鉴别第 4 部分：使用加密校验函数的机制。

二、国际标准化组织（ISO）信息技术安全标准

1 ISO/IEC JTC1/SC27 信息技术的安全技术标准

1.1 已制定和发布的标准

ISO7498-2：1988 信息处理系统-开放系统互连-基本参考模型第 2 部分；安全体系结构

ISO 8372：1987 信息处理-64 位块加密算法的操作方式

ISO/IEC 9796：1996 信息技术-安全技术-带消息恢复的数字签名方案

ISO/IEC 9796：1993 信息技术-安全技术-用块密码算法作密码校验函数的数据完整性机制

ISO/IEC 9798-1：1991 信息技术-安全技术-实体鉴别机制-第 1 部分：一般模型

ISO/IEC 9798-2：1994 信息技术-安全技术-实体鉴别机制-第 2 部分；使用对称加密算法的实体鉴别

ISO/IEC 9798-3；1993 信息技术-安全技术-实体鉴别机制-第 3 部分：使用公开密钥算法的实体鉴别

ISO/IEC 9798-4：1995 信息技术-安全技术-实体鉴别机制-第 4 部分：使用加密校验函数的机制

ISO/IEC 9979：1991 加密算法的登记规程

ISO/IEC10116：1991 信息技术-n 位加块密算法的操作方式

ISO/IEC10118-1：1994 信息技术-安全技术-散列函数 第 1 部分：概述

ISO/IEC10118-2：1994 信息技术-安全技术-散

列函数 第 2 部分：用 n 位块密码算法的散列函数

ISO/IEC10164-7：1992 信息技术-开放系统互连-系统管理体制 第 7 部分：安全报警报告功能

ISO/IEC10164-8：1993 信息技术-开放系统互连-系统管理体制 第 8 部分：安全审计跟踪功能

ISO/IEC10745：1995 信息技术-开放系统互连-上层安全模型

ISO/IEC11577：1995 信息技术-开放系统互连-网络层安全协议

ISO/IEC11770-1 信息技术-安全技术-密钥管理 第 1 部分：框架

ISO/IEC11770-2 信息技术-安全技术-密钥管理 第 2 部分：使用对称技术的机制

ISO/IEC TR13335-1 信息技术安全管理指南 第 1 部分：IT 安全概念和模型

1.2 正在制定中的标准

ISO/IEC CD9798-5：信息技术-安全技术-实体鉴别机制 第 5 部分：使用零知识技术的机制

ISO/IEC DIS10118-1 信息技术-安全技术-散列函数 第 1 部分：概述

ISO/IEC DIS10118-2 信息技术-安全技术-散列函数 第 2 部分：使用 n 位块密码算法的散列函数

ISO/IEC DIS10118-3 信息技术-安全技术-散列函数 第 3 部分：专用散列函数

ISO/IEC DIS10118-4 信息技术-安全技术-散列函数 第 4 部分：使用模运算的散列函数

ISO/IEC DIS11770-1 信息技术-安全技术-密钥管理 第 1 部分：密钥管理框架

ISO/IEC11770-2 信息技术-安全技术-密钥管理第 1 部分：使用对称技术的机制

ISO/IEC DIS11770-3 信息技术-安全技术-密钥管理 第 3 部分：使用非对称技术的机制

ISO/IEC TR13335-1 信息技术-信息技术安全管理指南-第 1 部分：IT 的安全的概念和模型

ISO/IEC DTR13335-2 信息技术-信息技术安全管理指南-第 2 部分：管理和规划 IT 的安全

ISO/IEC FDTR13335-3 信息技术-信息技术安全管理指南-第 3 部分：IT 安全管理技缩

ISO/IEC WD13335-4 信息技术-信息技术安全管理指南-第 4 部分：基线途径

ISO/IEC WD13335-5 信息技术-信息技术安全管理指南-第 5 部分：IT 安全和机制的应用

ISO/IEC CD13888-1 信息技术-安全技术-抗低赖-第 1 部分；一般模型

ISO/IEC CD13888-2 信息技术-安全技术-抗低赖-第 2 部分：使用对称技术

ISO/IEC CD13888-3 信息技术-安全技术-抗低赖-第 1 部分：使用非对称技术

ISO/IEC WD14516-1 可信第三服务使用和管理指南 第 1 部分：概述

ISO/IEC PDTR14516-2 可信第三服务使用和管理指南 第 2 部分：技术方面（方向）

ISO/IEC CD14888-1 信息技术-安全技术-带附悠扬的数字签名方案第 1 部分：概述

ISO/IEC CD14888-2 信息技术-安全技术-带附悠扬的数字签名方案第 2 部分：基于身份的机制

ISO/IEC CD14888-3 信息技术-安全技术-带附悠扬的数字签名方案第 3 部分：基于证书的机制

ISO/IEC CD15408-1 信息技术安全的评估准则-第 1 部分：引言和一般模型

ISO/IEC CD15408-2 信息技术安全的评估准则-第 2 部分：安全功能要求

ISO/IEC CD15408-3 信息技术安全的评估准则-第 3 部分：安全保证要求

2 ISO/TC68/SC2 银行操作和规程（有关信息安全的标准）

ISO 8730：1990 银行业务-消息鉴别（批量）的要求

ISO 8731-1：1987 银行业务-认可的消息鉴别算法 第 1 部分：DEA

ISO 8731-2：1982 银行业务-认可的消息鉴别算法 第 2 部分：消息鉴别算法

ISO 8732：1988 银行业务-密钥管理（批量）

ISO 9564-1：1990 银行业务-个人标识号和管理安全 第 1 部分：PIN 保护原则和技术

ISO 9564-2：1991 银行业务-个人标识号和管理安全 第 1 部分：订可 PIN 加密算法

ISO 9807：1991 银行业务和相关金融服务-消息鉴别（零售）要求

ISO10126-1：1991 银行业务-消息加密（批量）规程 第 1 部分：一般原则

ISO10126-2：1991 银行业务-消息加密（批量）规程 第 2 部分：DEA 算法

ISO10202-1：1991 银行交易卡-使用集成电路卡金融交易系统的安全体系结构 第 1 部分：卡生存期

ISO/DIS10202-2：1991 银行交易卡-使用集成电路卡金融交易系统的安全体系结构 第 2 部分：交易过程

ISO/CD10202-3：1991 银行交易卡-使用集成电路卡金融交易系统的安全体系结构 第 3 部分：加密密钥关系

ISO/DIS10202-4：1991 银行交易卡-使用集成电路卡金融交易系统的安全体系结构 第 4 部分：保密应用模块

ISO/CD10202-5：1991 银行交易卡-使用集成电路卡金融交易系统的安全体系结构 第 5 部分：算法的使用

ISO/DIS10202-6：1991 银行交易卡-使用集成电路卡金融交易系统的安全体系结构 第 6 部分：卡持有者验证

ISO/CD10202-7：1991 银行交易卡-使用集成电路卡金融交易系统的安全体系结构 第 7 部分：密钥管理

ISO/WD10202-8：1991 银行交易卡-使用集成电路卡金融交易系统的安全体系结构 第 8 部分：一般原则和概述

ISO11131：1992 银行业务-金融机构接受签字和鉴别

ISO11166-1：1991 银行业务-借助非对称算法的密钥管理 第 1 部分：原则、规程和格式

ISO11166-2：1991 银行业务-借助非对称算法的密钥管理 第 2 部分：已批准的使用 RSA 加密体制算法

ISO11568-1：1994 银行业务-密钥管理（零售）第 1 部分；密钥管理引言

ISO11568-2：1994 银行业务-密钥管理（零售）第 2 部分；对称密码用的密钥管理技术

ISO11568-3：1994 银行业务-密钥管理（零售）第 3 部分；对称密码的密钥生存期

ISO/DIS11568-4：1994 银行业务-密钥管理（零售） 第 4 部分；使用公开密钥加密的密钥管理技术

ISO/WD11568-5：1994 银行业务-密钥管理（零售） 第 5 部分；公开密钥加密系统的生存期

ISO/WD11568-6：1994 银行业务-密钥管理（零售） 第 6 部分；密钥管理方案

ISO/WD13491-1 保密加密设备-第 1 部分：概念、特性、管理和依重性

ISO/CD13492 有关安全的控制信息

ISO/WD13569 银行业务和相关金融服务-银行业务信息安全指南

三、国际电信联盟标准（ITU-T）

ITU-T 建议 X.463 信息技术-MHS 管理:安全管理

功能（ISO11588-3）

四、欧洲计算机制造商协会信息安全标准（ECMA）

ECMA-83：1985 公共数据网 DTE 到 DCE 接口的安全要求

ECMA-97：1985 局域网-安全要求

ECMA-129：1988 信息处理设备的安全

ECMA-138：1989 开放系统安全-数据元素及服务定义

ECMA-166：1992 信息技术设备-生产中的例行安全试验

ECM-205：1993 专用远程通信网（PIN）-安全评估用商业贸易取向的功能性类别（COFC）

ECMA-206：1993 安全上下文管理的联系上下文管理

ECMA-219：1994 密钥分配功能的鉴别和特许属性安全应用

ECMA TR/46：1988 开放系统中安全-安全框架

ECMA TR/64：1993 保密信息处理与产品评估的角度

五、美国信息技术安全标准

1 美国国家标准（ANSI）

ANSI X3.92-1981 数据加密算法

ANSI X3.105-1983 信息系统-数据链加密

ANSI X3.106-1983 信息系统-数据加密算法-操作方式

ANSI X9.8-1982 标识号的管理和安全

ANSI X9.9-1986 金融机构的消息鉴别（批量）

ANSI X9.17-1985 金融机构的密钥管理

ANSI X9.19-1986 金融机构零售消息鉴别

ANSI X9.23-1988 批量金融消息的金融机构机密

ANSI X9.24-1992 金融机构零售密钥管理

ANSI X9.26-1990 批量金融系统用镨机构接受签名的鉴别

ANSI X9.28-1991 金融服务中心金融机构多中心密钥管理

ANSI X9.30-1993 公开密钥管理

2 美国联邦标准（FIPS）

FIPS-39：1976 计算机系统安全术语汇编

FIPS-41：1975 实现 1974 年保密措施的计算机保密性指南

FIPS-46：1977 数据内部密码标准

FIPS-73：1981 计算机应用安全指南

FIPS-74：1980 NBS 数据密码标准的使用导则

FIPS-88：1981 数据库管理完整性保证及控制导

则

FIPS-83：1981 计算机网络访问控制用户特许技术应用导则

FIPS-102：1983 计算机安全认证和鉴别指南

FIPS-113：1985 计算机数据加密鉴别

FIPS-140-1：1994 密码模块的安全要求

FIPS-171：1992 使用 ANSI X9.17 的密钥管理

FIPS-180：1992 安全的散列标准

FIPS-181：1993 自动的口令发生器

FIPS-185：1994 证书加密标准

FIPS-186：1994 数据签名标准

FIPS-188：1994 信息传送用标准安全标号

3 美国国防部指令（DODD）

DODI5200.1-1982 DOD 信息安全保密程序

DODI5200.1-R-1986 信息安全保密程序规章

DODI5200.28-1988 自动消息系统安全保密要求

DODI5200.28-M-1973 实现、解除、测试和评估用的 ADP 安全保密技术和规程

DODI5200.28-STD-1985 国防可信计算机系统评估准则

DODI5215.1-1982 计算机安全保密评估中心

DODI5215.1-1986 计算机安全保密技术脆弱性

报告程序

远程访问的一次性口令技术

在一般情况下，远程用户用 FTP、TELNET 等命令访问服务器时，需向服务器提供用户名和口令，用户名和口令都是以明文（cLeaRtext）方式在网上传输。一旦黑客在网上截获了这些用户名和口令，他们就可以利用截获的信息获取系统的访问权，对系统造成严重的威胁。因此在 80 年代初，美国科学家 LesLIeLamport 首次提出了利用散列函数产生一次性口令的思想，即用户每次同服务器连接过程中使用的口令在网上传输时都是加密的密文，而且这些密文在每次连接时都是不同的，也就是说口令密文是一次有效的。

1991 年贝尔通信研究中心（BeLLcore）首次研制出了基于一次性口令思想的身份认证系统 S/KEY。S/KEY 最初使用 DES（DataEncRyptIonStandaRd）作为散列算法，后因安全问题改用 MD4 作为其加密算法。现在，基于更安全的 MD5 散列算法的一次性口令验证系统已开发出来，如美国海军研究实验室的 OPIE2.31、荷兰 WIetseVenemaofEIndhoven 理工大学项目中的 LogDaemon5.0 等。

口令的基本原理

我们要了解加密的原理，就必须从散列函数谈起。单向散列函数（One 俺 wayHashFunctIon）是这样的函数：

y=f(x)

其中，给一个 x，很容易求出 y；但是给出 y，却很难求出 x。这就是说，求散列函数的逆函数在计算上是不可行的。

近年来，一种报文鉴别码的变种得到了广泛的关注，这就是报文摘要(MD，MessageDIgest)。它是将可变长度的报文 M 作为单向散列函数输入，然后得出一个固定长度的标志 H(M)。H(M)通常称为报文摘要(MD)，它主要用于下面三种情况。

通信双方共享一个常规的密钥。发送端先将报文 M 输入给散列函数 H，计算出 H（M）即 MD，再用常规的密钥对 MD 进行加密，将加密的 MD 追加在报文 M 的后面，发送到接受端。接收端先除去追加在报文 M 后面加密的 MD，用已知的散列函数计算 H(M)，再用自己拥有的密钥 K 对加密的 MD 解密而得出真实的 MD；比较计算出得 H(M)和 MD，若一致，则收到的报文 M 是真的。

和第一种情况类似，但此时对 MD 的加密是使用

公开密钥密码体制中的秘密钥匙，接收端使用公开密钥将加密的 MD 解密。这样做的好处在于省去了密钥分配给网络带来的负担。

通信的双方共享一小段其他人不知道的秘密数据块。发送端先将此秘密数据块追加在报文M的前面，然后输入到散列函数 H，计算出 MD；接着将 MD 追加在报文M的后面，同时去除一开始加上的秘密数据块，发送给接收端。接收端则先将加密的 MD 去除，然后在报文 M 的前面加上自己拥有的秘密数据块后，输入给散列函数 H，计算 H(M)；比较 H(M)和 MD，若一致，就认为收到的报文 M 是真的。

报文摘要除提供鉴别外，还提供数据完整性的检测。在传输过程中，报文里的任一比特出了差错，发送端和接收端的 MD 代码就会不一样。

MD5 报文摘要算法

MD5 报文摘要算法是由 R.RIvest 于 1992 年提出的 MD 算法的第五个版本。此算法可对任意长的报文进行运算，然后得出 128 位的 MD 代码。该算法的实现过程如下。

先将任意长的报文（M 位）按模 264 计算出余数（64 位），追加在报文的后面。即：最后得出得 MD 代码已包含了报文长度信息；

在报文和余数之间填充 1--512 位，填充后的总长度是 512 的整数倍。填充位序列的首位为 1，后面的其他位为 0；

将追加和填充后的报文分割成一个个 512 位的数据块，进行复杂的处理。

H 就是在计算中最为关键的散列函数。ABCD 是 4 个 32 位的寄存器，其 16 进制初始值（低字节在前）为：

A=01234567

B=89ABCDEF

C=FEDCBA98

D=76543210

512 位的报文数据分成 4 个 128 位的数据块，依次被送到不同的散列函数进行 4 轮计算；每一轮都按 32 位的小数据块进行复杂的运算，计算完成后全部写入 ABCD 寄存器，用于下一轮的计算。等到最后计算完毕，在寄存器 ABCD 中的数据就是我们要求的 MD5 代码。

依照上述方法计算出的 MD5 代码中的每一个比特，都与报文中的每一个比特有关。

口令的使用过程

当一个用户在服务器上首次注册时，系统给用户

分配一个种子值（seed）和一个迭代值（IteRatIon），这两个值就构成了一个原始口令，同时在服务器端还保留有仅用户自己知道的通行短语。

当用户每次向服务器发出连接请求时，服务器把用户的原始口令传给用户。用户接到原始口令以后，利用口令生成程序，采用 MD4 或 MD5 散列算法，结合通行短语计算出本次连接实际使用的口令，然后再把口令传回服务器；服务器先保存用户传来的口令，然后调用口令生成器，采用 MD4 或 MD5 散列算法，利用用户存在服务器端的通行短语和它刚刚传给用户的原始口令自行计算生成一个口令；服务器把这个口令与用户传来的口令进行比较，进而对用户进行身份确认；每一次身份成功认证后，原始口令中的迭代值数自动减 1。这里要指出的是，用户主机上采用的散列算法和服务器上采用的散列算法必须是一样的。

我们可以看出，用户通过网络传给服务器的口令是利用原始口令和通行短语经 MD4 或 MD5 散列算法生成的密文，用户本身的通行短语并没有在网上传播；在服务器端，因为每一次成功的身份认证后，用户原始口令中的迭代值就自动减 1。这样，下一次用户连接时使用的原始口令同上一次使用的原始口令是不一样的，因此，两次生成的口令也是不同的，从而有

效地保证了用户口令的安全。

钥体系结构中的几个概念及国际标准

基于非对称加密体系，可建立起一套优秀的安全体系结构，称为公钥体系结构（PubLIc Key InfRastRuctuRe,简称 PKI）。以下介绍公钥体系结构中的一些基本概念与结构组成：密钥对、证书和 CA。

1 密钥对

在基于公钥体系的安全系统中，密钥是成对生成的，每对密钥由一个公钥和一个私钥组成。在实际应用中，私钥由拥有者自己保存，而公钥则需要公布于众。为了使基于公钥体系的业务（如电子商务等）能够广泛应用，一个基础性关键的问题就是公钥的分发与管理。

公钥本身并没有什么标记，仅从公钥本身不能判别公钥的主人是谁。在很小的范围内，比如 A 和 B 这样的两人小集体，他们之间相互信任，交换公钥，在互联网上通讯，没有什么问题。这个集体再稍大一点，也许彼此信任也不成问题，但从法律角度讲这种信任也是有问题的。如再大一点，信任问题就成了一个大问题。

2 证书

互联网络的用户群决不是几个人互相信任的小

集体，在这个用户群中，从法律角度讲用户彼此之间都不能轻易信任。所以公钥加密体系采取了另一个办法，将公钥和公钥的主人名字联系在一起，再请一个大家都信得过有信誉的公正、权威机构确认，并加上这个权威机构的签名。这就形成了证书。

公钥

公钥主人的信息

权威机构的签名

由于证书上有权威机构的签字，所以大家都认为证书上的内容是可信任的；又由于证书上有主人的名字等身份信息，别人就很容易地知道公钥的主人是谁。

3 CA（Certificate Authority）

前面提及的权威机构就是电子签证机关（即 CA）。CA 也拥有一个证书（内含公钥，与上图所示相同），当然，它也有自己的私钥，所以它有签字的能力。网上的公众用户通过验证 CA 的签字从而信任 CA，任何人都应该可以得到 CA 的证书（含公钥），用以验证它所签发的证书。

如果用户想得到一份属于自己的证书，他应先向 CA 提出申请。在 CA 判明申请者的身份后，便为他分配一个公钥，并且 CA 将该公钥与申请者的身份信息

绑在一起，并为之签字后，便形成证书发给那个用户（申请者）。

如果一个用户想鉴别另一个证书的真伪，他就用 CA 的公钥对那个证书上的签字进行验证（如前所述，--CA 签字实际上是经过 CA 私钥加密的信息，签字验证的过程还伴随使用 CA 公钥解密的过程），一旦验证通过，该证书就被认为是有效的。

CA 除了签发证书之外，它的另一个重要作用是证书和密钥的管理。由此可见，证书就是用户在网上的电子个人身份证，同日常生活中使用的个人身份证作用一样。CA 相当于网上公安局，专门发放、验证身份证。

诺方宏证电子签证机关就是一个基于相关国际标准的网上 CA 系统。

相关国际标准

1.PKI (Public-Key Infrastructure) 公钥体系基础框架。

对于任何基于公钥体系的安全应用，必须确立其 PKI。而电子签证机关(CA)是 PKI 中的一个关键的组成部分，它主要涉及两方面的内容，即公钥证书的发放和公钥证书的有效性证明。

2.PKIX (PubLIc-Key Infrastructure Using

X.509)使用 X.509 的公钥体系基础框架。

3.X.500 由 ISO 和 ITU 提出的用于为大型网络提供目录服务的标准体系。

4.X.509 为 X.500 提供验证（AuthentIcatIng）体系的标准。

5.PKCS（Public Key Cryptography Standards）公钥加密标准，为 PKI 提供一套完善的标准体系。

X.509 最早的版本 X.509v1 是在 1988 年提出的，到现在已升级到 X.509v3，现将其涉及到的主要内容以及与前版本的比较列于下表。

论网络发展与安全对策

一、抓住网络发展带来的历史机遇

互联网的起飞是二十世纪末信息技术领域最使人振奋的重大事件。它已遍及 180 多个国家，容纳了 60 多万 个网络，接入了 2000 多万台计算机，为 1 亿多用户提供多样化的网络与信息服务，展示了未来信息高速公路的雏型。

Internet 中包容了人类文明共有的信息宝藏，600 多个大型联网图书馆，400 多个联网的学术文献库，2000 多种网上杂志，900 多种新闻报纸的网络板，50 多万个 Web 网页站点，总计近 100 多万个信息源正在为人类提供信息资源的交流和共享。有 400 多万学

者在网上进行学术交流和合作开发与研究，一种崭新的计算机支持下的合作模式（CSCW）正在网上发展之中，将成为面向二十一世纪科学研究的网络工作环境。除了原来电子邮件、新闻论坛等文本信息交流之外，网上电话（Internet Phone)、网上传真、静态图像及视频都正在 Internet 中不断发展与完善，为人类通信联络提供综合性工具的时代已经为时不远了。采用 Internet 体系结构的企业内网（IntRanet)和外网（ExtRanet）正在成为网络发展的新热点，在发达国家中，50—60%和大型企业正在构造 IntRanet，由于它适应当今“企业重构”（ReengIneRIng）和快速响应市场变化的潮流，因而展现出强大的生命力。

随着经济发展的全球化，以及电子商务模式、规范和软件的成熟，Internet 将会成为世界贸易的公共平台。当前已有近十万家企业和 2000 家银行开始参与网上的商业和金融业务。据估计，2000 年网络购物和网络交易额可能达到 2000 亿美元。Internet 的发展为市场带来了巨大的商机，除了为大企业带来展示其实力的广阔空间外，特别是对中小企业也提供了平等同步的机会，美国 Netscape、Yahoo、CheckpoInt 等一些小型网络产品公司的暴发即是利用了 Internet 提供的机遇。Internet 带来的大市场正在

催生一个 Internet 的产业，如网络的建设业、网络通信业、网络内容（Content)提供业、网络消费业和网络安全管理业等。据有关报导，到2000年，Internet的采购和服务带来的市场总额将达到 6000 亿美元。

以 Intetnet 为代表的信息网络正在成为二十一世纪全球最重要的基础设施，一个网络经济和网络社会的时代即将到来。我们要抓住当前网络发展带来的难得机遇，发展我国的网络，推动科研教育的发展，培养现代化人材，促进经贸发展，带动信息产业，加速我国信息化的进程。我国从 1994 年正式起动 Internet 的建设，发展迅速，目前用户已 70 万，入网计算机 30 万台，注册域名近 5000 个。但是我们基数还很小，作为一个最大的发展中国家还不相称。我国应抓住历史机遇，采取果断措施，迎头赶上世界潮流，加快我国 Internet/IntRanet 的发展。大力推动公网建设，积极鼓励专网的成长，促进网络的互连互通，推动高性能试验示范网的起动，扶持自主的网络产品和产业，完善网络建设和运行的标准与法规，迎接网络发展新高潮的到来。

二、正视网络发展带来的巨大风险

随着网络经济和网络社会时代的到来，网络将会进入一个无处不有、无所不用的境地。经济、文化、

军事和社会活动将会强烈地依赖网络，作为国家重要基础设施的网络的安全和可靠将成为世界各国共同关注的焦点。而 Internet 原有的跨国界性、无主管性，不设防性、缺少法律约束性，为各国带来机遇的同时也带来了巨大的风险。由于各国的文化传统、价值观念和政治信仰的差异也引起了新的冲突和忧虑。为了使

Internet/IntRanet 在我国能健康地发展必须要重视这些风险和冲突。

1.抵制不良信息的入侵和污染

Internet 是一个无政府的文化自由王国，特别是美国的一些色情内容经营商在上亿美元利益驱动下，开放淫秽网点，大量制作色情网页。各种流派人物也在网上散布邪教、暴力、教唆等内容。一些政客为了达到其政治目的，利用网络进行政治攻击和煽动。虽然这些不良信息在 Internet 的一百多万个信息源中不足 1%，但是危害和负面影响是不容忽视的。最大限度减少其负面影响已经引起了世界上众多国家的注意。我国政府对此采取了积极的对策，国务院信息办和国家各安全职能部门都从管理、教育、法规和技术上采取了明确的措施，并将继续采取进一步措施，维护我国的社会主义精神文明建设。

2.打击网上“黑客”和计算机犯罪

近年来随着 Internet 的发展，利用网络安全的脆弱性，黑客在网上的攻击活动每年正在以 10 倍的速度增长， 形形色色的黑客攻击者是一个各怀鬼胎的复杂群体，把网上任何漏洞和缺陷作为靶子，无孔不入。如：修改网页进行恶作剧，非法进入主机破坏程序，串入银行网络转移金额，窃取网上信息兴风作浪，进行电子邮件骚扰，阻塞用户和窃取密码等等。政府、军事和金融网络更是他们攻击的主要目标。美国司法部主页被纳粹标志所取代，美国空军站点由于黑客攻击不得不暂时关闭，美国金融界由于计算机犯罪造成的金额损失每年计近百亿美元。近几年来，我国网络受黑客侵犯事件也屡屡发生，且呈明显上升趋势。为了确保网络的健康发展和网络电子化业务的广泛应用，应加大对黑客和计算机犯罪的打击力度，加强对网络安全的防护。

3.抑制网络病毒的蔓延和破坏

计算机病毒被发现十多年来，其种类以几何级数在增涨。其活体病毒已达 14000 种，病毒机理和变种不断演变，为检测与消除带来更大的难度，成为计算机及其网络发展的一大公害。它破坏计算机的正常工作和信息正常的存贮，严重时使计算机系统陷于瘫

痪。1988 年美国的“莫里斯”网络病毒案件，一天之内使“Internet 上 6000 台计算机染上病毒，损失金额 9000 万美元。当前随邮件和数据包的网络病毒花样翻新，给 Internet 用户带来了很大麻烦。我国计算机病毒新样品每年都在增加，公安部门从病毒防治的各个方面进行了大力的有效工作。抑制网络病毒的蔓延已是当务之急。

4.严防网上机要信息的扩散

办公自动化和电子文档为提高管理的效率、改善管理质量和提供科学决策起到了极大的推动作用。Internet 的 Web 网站和电子邮件为信息交流和共享提供了方便的手段。网上电子商务正在展示出其美好的远景。在当今信息化网络开放的环境下，怎样使国家的机要信息、企业敏感性信息和个人隐私信息，不随着一般信息而扩散和流失，是当前保护国家利益、企业和个人权益的重要课题。应采用立法、管理、电子密级标签和其基础设施等综合配套办法，建立网络电子信息及电子文档的安全保密管理的新机制。

5.警惕信息间谍的潜入

利用网络获取政治情报和经济情报，在当前是政治间谍和经济间谍活动的重要领域之一。利用政府机构和企业在网上信息活动的漏洞，窃取高新技术领

域、经济决策以及军事战略等信息，是一种以较小代价获取重大利益的手段。根据美国联邦调查局的统计美国本身受谍报入侵事件正以每年 300%的速度增加，使其产业、经济和政治活动受很大的损失。我国网络的发展还处于起步的阶段，随着网络应用在政府、军事和经济的深化，必须保持足够的警惕，特别是对要害部门要防患于未然。

6.将网络的脆弱性减到最小

Internet 是逐步发展和演变来的，其可靠性和可用性存在很多弱点，特别是在网络规模迅速扩大，用户量猛增，业务类型多样化的情况下，系统资源不足将成为瓶颈，系统和应用工具可靠性的弱点也将暴露出来。1996 年，美国最大的联机信息服务网络(American Online)瘫痪了 10 小时，对其 700 万用户产生了巨大的影响。随着经济和管理活动对网络依赖程度的加深，网络的瘫痪将会对国家、部门和企业带来巨大的损失。因此在建设 Internet/Intranet 时高度重视其可靠性和可用性，使其保持在连续运转、高负荷和应急情况下的运行能力。

7.网络装备过分依赖国外产品的局面应改变

我国网络建设的软件和硬件产品基本上依赖于从国外进口，特别是网络安全产品在没有自主权和自

控权的情况下引进使用，潜伏着很大的风险。如嵌入式固件病毒，安全产品的隐性通道和可恢复密钥的密码等威胁因素都可带来很大危害和受制于人，必须认真对待。首先要解决信息网络安全产品的自主权和自控权问题，进一步则需尽快建立起自主的网络安全产品和产业。

8.要正视信息战的风险

在信息网络已经成为国家的重要基础设施情况下，信息战将是一种跨国界、隐蔽性、低花费和跨领域（军事、经济、社会、资源）进行的无硝烟的战争。基高技术性和战争情报的不确定性给信息战的防御带来较大的难度。美国国防部专门组织了”信息战执行委员会“研究国家信息战的战略，并对所属的网络和 InteRent 网点进行大量的攻击演练。国家级的金融支付中心、证券交易中心、空中管制中心、电信网管中心、铁路调度中心、军事指挥中心等等必将成为信息战的主攻目标。我国在信息化进程中对此必须早有准备。一个全局性的信息战防御战略在国家信息基础建设中将是至关重要的。

三、迎接网络发展提出的挑战

发展 Internet 及其应用是时代发展的需求，迎接挑战、抵制威胁和化解风险是社会的责任。我们要

最大限度地减少负面影响，兴利除弊，推动国家信息网络的健康发展。

1.健全国家信息网络安全组织机构

应从领导层、技术层、职能层和基础层全面进行组织建设。国务院信息化工作领导小组与国际联网成立了安全工作组及其专家组，国家安全部、公安部、国家保密局等职能部门，也进一步加强了信息化安全的组织和协调分工。基础层建设是指为了落实安全法规、政策、标准、运行和实施所必须建立的保障实体，即”安全基础设施“的建设。

2.开展信息网络安全战略研究

为了把握网络安全的全局，应对下列战略课题进行深入的研究：

在高收益和高风险条件下，网络发展与网络安全相互制约和依存的模式；

由于卫星移动通信和直播卫星的发展，应进一步探索在”信息海关“个人化趋势下，信息安全职责和安全机制的模式；

随着网络的发展，用户资源（个体和团体）还要进一步网络化（包括信息资源、软件资源、业务处理资源、文档资源等），保护知识产权、个人隐私、企业秘密、国家主权的机理和模式；

全局性、跨领域（军事、经济、政治、社会、资源等）的信息战的防御战略。

3.加强安全技术的开发和应用

密码技术是安全的核心技术，特别是商业密码在未来电子商务中将有大量的需求，要求开放又安全，既要保密又能被监视，使之成为为社会提供普遍性服务的一种安全工具。应加速对商业密码标准、芯片、算法、协议、CAPI 加密框架、密钥恢复等技术的开发。

认证技术可对责任者进行授权、监督、审计和仲裁。应开展对数字签名、证书授权（CA）、动态口令、统一代码制度和认证基础设施的开发和研究。

开展访问控制技术的研究，包括内容选择平台（PICS）、系统和数据库的访问控制、防火墙和安全隧道等技术。

病毒的检测、预防、清除技术。

文本、声音、图片和视频的内容识别、分类和过滤技术。

网络隐患扫描技术。

系统安全监测、报警和审计技术。

4.开发网络安全标准

随着 Internet 的发展和电子商务的应用，国际上一些大的标准化集团都在制定相关的安全标准，

如：ISO、ITU、IEEE、ECMA、ANSI、NCSC、SA、DOD。特别是 Internet 的 IETF 和 W3C 以及大的信息产业集团，都在 Internet 安全标准方面作了大量的工作，对 Internet 安全技术开发和安全产品研制起到了推动作用。

我国应尽快跟踪和形容下列标准：SNMP3（ISOC）、IPV6（IETF）、PICS（W3C）、SSL（Netscape)、S-HTTP（ELT 等）、SET（VIsa、MasteRcaRd）、X509（ITU）、FPKI（NIST）、EES（NIST、NSA、KRA）、CA（NIST）、PKCS（RSA 等）、ICF（HP 等）、ADS（NIST）、CC（6 国集团）、TCSEC（NCSC）、CAPI（NIST、NSA、X/OPEN、Microsoft),以及 S/MIMI、PEM、PGP 等。

在与国际标准等同、等效和参照的原则下，尽快制订我国自己的 Internet 的安全标准，特别是商业密码算法、密码协议和 CAPI 等商业密码标准。

5.推动网络安全产品研制和产业的形成

由于网络建设市场的需求，美国现在涉足安全产品的厂商近 500 家，成为美国 Internet/IntRanet/ExtRanet 网络产业的重要组成部分，随着电子商务和企业网络的迅速发展，安全产品的市场每年正以 20—30%的速度增长，到二十一世纪初将形成近百亿美元的市场分额。我国目前安全产品的研究机构和生产厂

商有 50—60 家，成果的孵化率、产品化和市场占有率都很低，尚未形成规模和配套体系。

网络安全产品的自控权和自主权是网络安全的重要保障，抓紧网络安全产品的开发，将其作为网络产品市场的切入点，应该通过税收、贷款、授权和采购等相关政策扶持我国自主的网络安全产品产业，占领我国的网络市场。

国务院信息办已组织二十几个部门开展了安全技术和安全产品的研制，在国家有关部门的支持下已初见成效。

网络安全产品市场需要：防火墙、代理服务器、安全路由器、安全调制解调器、加密、安全 IC 卡、安全监控、安全隧道、防治病毒产品、数字签名、电子证书授权系统（CA）、电子标签、防隐患扫描工具、安全电子交易软件、安全系统平台、高安全加密芯片等产品。

6.强化网络安全管理和安全立法工作

随着网络安全威胁和增加和面临的巨大风险，为了规范网络建设者、运营者和使用者的网上行为，网络安全管理和安全立法成为各国政府共同关心的问题。据国家安全部 96 年对 42 个国家的调查统计：针对 Internet 安全制订专用法规的国家占 33%，修订原

有法规的占 70%，实行审查和监管的占 93%，已有执法案例的占 26%。涉及到打击黑客和计算机犯罪、抵制淫侮内容、保护知识产权、维护个人隐私、保障数据安全、信息流过境、网络经营、密码产品出口限制、密码产品进口许可证、文本和邮件加密限制……等。

我国政府十分重视 Internet 的管理立法工作，在国际联网安全工作组的领导下，国务院信息办协同国家有关安全职能部门，积极推动网络安全管理和安全立法工作。1996 年 2 月颁布了《中华人民共和国计算机信息网络国际联网管理暂行办法》，1997 年 12 月颁布了《中国互联网络域名注册暂行管理办法》和《中国互联网域名注册实施细则》等。

正在制订中的法规有”进行国际联网管理办法“、”互联网经营服务业管理办法“、”信息上网管理办法“。

尚需进一步考虑的法规，如”信息安全法“、”电子凭证（票据）法“、”计算机犯罪刑法“、”网上知识产权保护法“、”信息流过境法“、商业密码开发与应用法规”等。

7.逐步推进“安全基础设施”的建设

真正使安全管理和安全控制走向有序和有效的轨道，必须建立相应的“安全基础设施”，为网络安

全提供最基本的保障。

需要逐步建立的安全基础设施包括：“国际出入口(信息海关)监控中心”、“安全产品评测认证中心”、“病毒检测和防治中心”、“关键网络系统灾难恢复中心”、“系统攻击和反攻击中心”、“电子保密标签监管中心”、“网络安全紧急处置中心”、“电子交易证书授权中心”、“密钥恢复监管中心”、“公钥基础设施与监管中心”、“信息战防御研究中心”等。

在国务院信息化工作领导小组的领导下，“国际出入口监控中心”和“安全产品评测认证中心”已初步建成，一些中心正在建设和设想之中，大部分尚属空白，需要认真论证和具体筹划，应有计划推进它们的建立。

8.重视网络安全的教育，提高安全意识。

重视信息化的安全教育，培养一批信息化安全的专门人材是网络安全之本。提高全民的信息化的安全意识，使网络安全建立在法律约束之下的自律行为是实现网络安全的重要因素。

网上商贸交易的保护

各国主要针对电子贸易和电子货币，电子决算的方法及保密措施等作了规定。

欧盟反对美国网上自由贸易提法。看不见的钱将

以光速旅行，直接从买主的钱包里转到了汽车库经营者的钱包里。任何国家都无法提取过境税。这是一种不受限制的、绝对自由的贸易。客户要买的汽车或唱片，都可以在家里交货。

“这是一个自由贸易区”，美国总统克林顿就是这样看待 Internet 的，不会超过一年，即在他所希望举行的国际谈判结束之后，这个网络就会出现。

尽管一个国家与另一个国家的立场是不同的，但大西洋这一边的人们很难想象得到网络交易能逃过税务机关的眼睛，也难以想到在世界这个蜘蛛网上发出的这些信息的内容能逃脱当面的任何检查。

欧洲 15 国，或至少是它们当中的那些极顽固地反对电子自由贸易的国家，难道它们有技术方面的手段来对付美国的这种观点吗？

法国一家专门从事卫星与 Internet 连接的卫星互联网公司的贸易部主任雅克.卡永说，在欧洲很难阻止这个系统的运转。我可以在美国的一个地方购买一件法国产品，而不用纳税。Internet 不属于任何人。然而，每个国家都可以建立独立于世界网络的自己的一套网络。这就是伊朗、沙特阿拉和中国现在所做的事情。

由于在技术上无法对 Internet 上的走私活动加

以控制，所以，不只能靠警方采取一些手段。

我国的信息技术开发工作虽然起步较晚，但是发展很快。随着我国信息高速公路的建立和完善以及利用互联网人数的增加，在其他国家已经出现的问题也将或已经在我国发生了。与此相应，我国处理相关问题的法律制度也比较欠缺。因此，为了促进信息技术在我国的开发和利用。我们除了利用科学技术进行净化技术空间外，利用道德力量、行政力量以及法治力量来解决相关问题也应作为解决问题的手段加以考虑。