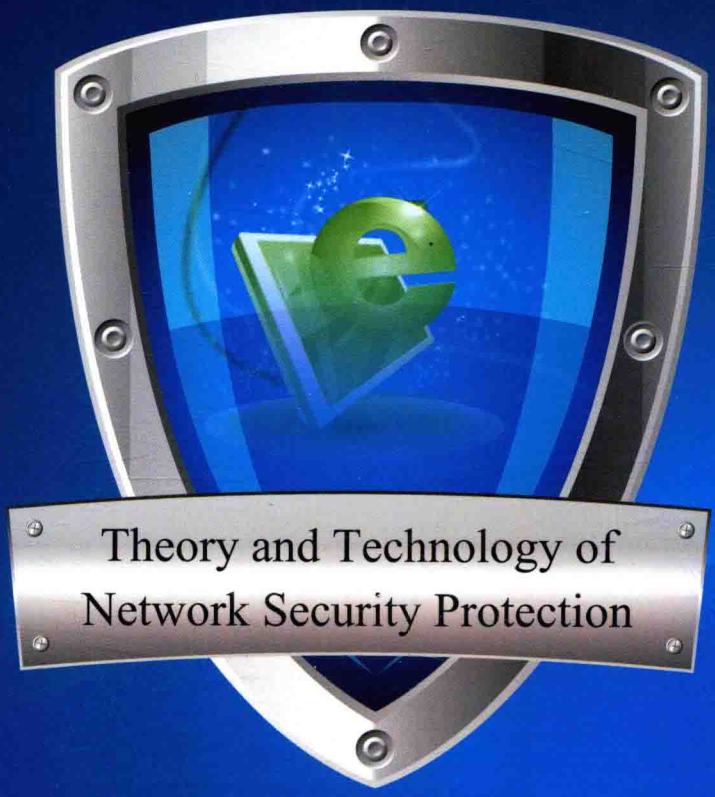

网络安全防护理论与技术

鲁智勇　杜 静　黄赫东　等编著

国防工业出版社
National Defense Industry Press

网络安全与技术

鲁智勇　杜　静　黄赪东　晋伊灿
刘迎龙　王学宇　韩　哲　李志勇　编著

国防工业出版社
·北京·

内容简介

本书在分析网络安全特性的基础上，深入探讨和研究了网络安全理论基础、信息网络安全防护理论和策略、信息网络安全防护技术、恶意代码运行机理和检测、网络安全评估建模等关键技术，以期为网络安全的防护起到借鉴作用。

本书可作为从事网络安全防护人员的必备参考资料，也可作为高等院校学生工程实践的参考用书。

图书在版编目（CIP）数据

网络安全防护理论与技术/鲁智勇等编著. —北京：国防工业出版社，2017.5

ISBN 978-7-118-11256-6

Ⅰ. ①网… Ⅱ. ①鲁… Ⅲ. ①计算机网络—网络安全 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 122746 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号　邮政编码 100048）

涿中印刷厂印刷

新华书店经售

*

开本 787×1092　1/16　**印张** 22¼　**字数** 528 千字

2017 年 5 月第 1 版第 1 次印刷　**印数** 1—3000 册　**定价** 78.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)88540777　　发行邮购：(010)88540776

发行传真：(010)88540755　　发行业务：(010)88540717

前　言

近年来，以 Internet 为代表的计算机网络技术突飞猛进，并在民用和军事信息领域得到广泛应用，计算机网络已成为国家信息基础设施和国防信息基础设施，也是军事上 C^4ISR（指挥，控制，通信，计算机，情报，监视，侦察）系统的基础。由于计算机网络在国防、民用的各个方面发挥着举足轻重的作用，但因其开放分布、广域互联特性，也给安全性带来了严峻的挑战，因此各国在竞相发展计算机网络的同时，也十分注重网络安全性，而在军事领域，对这一阵地的角逐越来越剧烈，并且已从理论走向实战。网络越发达，对网络的依赖程度越强，网络的安全和防御也就越重要，同时对其进行的网络攻击所造成的干扰和破坏也将是巨大的。因此，网络安全防护理论与技术的研究显得尤为重要和迫切。

基于此，本书在分析网络安全特性的基础上，对信息网络安全防护理论和策略、信息网络安全防护技术、恶意代码运行机理和检测、网络安全评估建模等方面进行深入研究，取得了一系列信息网络安全防护理论和技术方面有价值的研究成果，主要体现在以下几方面。

1. 提出网络安全防护理论

本书提出了基于物理防范、系统安全、应用程序安全、人员管理和安全技术的网络安全防护理论。

2. 设计实现了网页恶意代码主动检测系统

在对网页恶意代码原理深入分析的基础上，本书提出利用搜索引擎程序主动对指定链接进行抓取，首先对下载的网页进行干扰、自动识别编码并进行解码统一编码、提取隐藏链接、提取脚本链接，将该网页全部直接引用链接进行合并成一个网页文件，然后提交检测模块进行检测。系统经过这几年的不断改进和完善，设计实现的网页恶意代码主动检测系统由最初的单机 C/S 模式，改进为 B/S，并增加多种接口，以便与其他渠道产生的告警进行交互。

3. 提出基于链接分析的网页恶意代码检测方法

在网页中存在的链接分为两种：直接引用标签链接和间接引用标签链接。直接引用标签链接的内容会在当前网页中直接运行，而间接引用标签链接需人工点击才会触发去访问新的网页内容。在正常的网页中引用的链接，不能直接调用已有链接内容，而连接的含恶意代码的网页，通过下载、激活可执行的病毒、木马程序来传播病毒，这些程序必然是可执行文件，利用这一特征可以分析出病毒、木马程序所在位置和所引用激发的网页。这一分析方法适合在最终触发病毒木马的网页恶意代码检测，而对其中间引用的跳转链接关系进行分析可追踪各分支链接的域名、IP 进行链接危害权重赋值，以便搜索引擎程序优先抓取和检测，并结合历史记录产生的黑白名单来减少检测数目和分支，加快检测速度。

4. 提出基于统计判断矩阵的网页恶意代码检测方法

在清除掉网页中的干扰语句后对网页中的非常见字符进行统计，未经过加密处理的正常网页脚本中的字符除了正常断句的标点符号以及空格外，多数字符都是英文字母，而经过加密处理的恶意脚本中的字符多为一些难以识别的乱码，因此，可以通过统计网页中的非常见字符来判断网页中是否有恶意脚本。本书探讨了一种指标权重系数确定方法，即判断矩阵法。通过这种方法可以得到各种统计方法的权重系数，如字符比例统计、字典匹配统计，最后利用加权几何平均法精确地得到一个综合统计结果值。实验结果表明，本方法可以有效地检测网页中经过加密的恶意脚本，从而对含有加密的可疑网页进行危害权重加权，以便解密模块优先处理。如果解密模块不能处理，也可起到一定的预先告警功能，以便提醒人工排除是否是新的加密样式，进一步完善解密模块。

5. 提出基于 shellcode 检测的网页恶意代码检测方法

网页恶意代码运行方式主要有两种：跨安全域执行非法操作和利用浏览器溢出漏洞执行非法操作。对于跨安全域的网页恶意代码采用特征匹配检测还是比较有效的，且跨安全域的 clsid 和关键执行函数也非常限，然而更多的网页恶意代码是溢出型网页恶意代码，这种恶意代码会采用 Heap Spray 技术来实现溢出，对这种恶意代码检测其中的 shellcode 是十分有效的方法。对网页脚本源码进行 unicode 字节反序解码，如果解码结果中有系统调用函数或是有明显的 URL 下载链接，则使对其危害进行加权，对解码后的内容进行反汇编查看是否存在空操作性质的汇编语句和长跳转以及高位内存空间的系统函数调用代码，从而对该恶意代码进行危害判断。在实际系统测试中该方法还有效地发现了没有公开的 0day 漏洞。

6. 提出基于行为分析的网页恶意代码检测方法

利用上述方法可以很好地对网页恶意代码进行检测，然而恶意代码的检测不仅在于对某些链接提出危害警告，更重要的是获得最终病毒木马存放的位置。上述方法有时检测不够全面，会检测到前段告警后，后续链接无法追踪下去。基于行为分析的网页恶意代码检测方法借鉴轻量级客户端蜜罐的设计思想，在沙箱中启动浏览器程序将待检测的网页打开以后，立即运行进程监控程序来监视进程的变化。采用简化网页脚本执行逻辑来加速脚本运行过程，并可防范浏览器崩溃。采用不完全执行状态监督解决蜜罐检测网页恶意代码配置不完备的缺陷，观察进程列表中是否有新的进程产生，如果没有经过任何人工确定，以浏览器为父进程启动了新的可执行进程，则可断定该网页还有恶意代码。该方法对抗网页恶意代码的变形加密非常有效，不用考虑具体是如何加密解密的，只需检测沙箱的运行状态，然而该方法毕竟要依赖浏览器执行，速度上比前面的方法慢很多，因而该方法的使用是在前方法检测基础上，对危害权重较高的链接进行检测。

7. 建立了基于 AHP 的信息网络安全定量评估模型

对于层次分析法中不满足一致性要求的判断矩阵，本书提出了基于预排序和上取整函数的 AHP 判断矩阵生成算法，此算法在充分利用专家给出的初始判断矩阵信息的基础上，以比较矩阵为基准找出一个既能满足一致性要求，矩阵相异度和调整的元素幅度又较小的目标判断矩阵，并能确保生成目标判断矩阵的元素在 1～9 及其倒数范围内。在此算法基础上，建立了基于 AHP 的信息网络安全定量评估模型。

8. 建立了基于等效分组级联 BP 的信息网络安全评估模型

为解决有限的测试数据情况下高维 BP 网络对于信息网络安全测试评估的和预测问题，本书提出了松弛的和紧密的等效分组级联 BP 网络模型等概念，并给出了 BP 网络等效性的定义和相关定理。在构建并证明与 BP 网络等效的分组级联网络模型的基础上，建立了基于等效分组级联 BP 的信息网络安全评估模型。

本书作者近几年一直致力于网络安全防护技术的研究和应用，取得了一些研究成果。在撰写此书的过程中，查阅了大量的文献和资料，并将近几年来我们在理论和工程应用的成果融入到有关章节中。编写本书的目的是促进信息网络安全防护技术的研究和开发提供应用思想与可操作性技术。

本书由中国洛阳电子装备试验中心的鲁智勇、杜静、黄赪东、晋伊灿、刘迎龙、王学宇和韩哲，以及海军航空工程学院的李志勇博士共同撰写，本书的完成体现了团队精神。

感谢电子装备试验中心的领导们，他们对本书的撰写给予悉心关心和指导。还要感谢电子装备试验中心研究所七室的同志们，感谢周颖、耿宝军、陶业荣、郭荣华、陈远征、张红林、焦波、李鹏飞、董德帅、付海鹏、鲁刚、李博、袁学军、黄飞、周云彦、程若思、白永强、徐秋波、许世平、杜嘉薇、王金锁、岁赛、庞训龙等，他们对本书的研究和撰写给予了热情的帮助并提出了宝贵的建议。同行专家撰写的论文和专著，给了我很多启发和借鉴，在此一并感谢。

网络安全防护是一个崭新的领域，涉及的内容范围又比较广，书中难免有不妥之处，敬请广大读者提出宝贵意见，并给予批评指正。

撰写此书的过程中，参考和引用了国内外同仁们的一些前瞻性研究成果，在此表示衷心感谢。

作者

目　录

第1章 绪 论

1.1 网络安全

计算机网络系统的安全威胁来自多方面，可以分为被动攻击和主动攻击两类。被动攻击不修改信息内容，如偷听、监视、非法查询、非法调用信息；主动攻击则破坏数据的完整性，删除冒充合法数据，制造假数据进行欺骗，甚至干扰整个系统的正常进行。归纳起来，系统的安全威胁常表现为以下特征：①窃听：攻击者通过监视网络数据获得敏感信息；②重传：攻击者事先获得部分或全部信息，而以后将此信息发送给接收者；③伪造：攻击者将伪造的信息发送给接收者；④篡改：攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者；⑤拒绝服务攻击：攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务；⑥行为否认：通信实体否认已经发生的行为；⑦非授权访问：没有预先经过同意，就使用网络或计算机资源被看作非授权访问，非授权访问主要有假冒身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等几种形式；⑧传播病毒：通过网络传播计算机病毒，其破坏性非常高，而且用户很难防范，如众所周知的 CIH 病毒，最近出现的“爱虫”病毒都具有极大的破坏性。

对网络安全的需求是众所周知的，而“病毒”“特洛伊木马”“蠕虫”和由于违反安全性措施而造成的商业损失的事例不胜枚举。由于联网的计算机已成为商业、研究所和政府部门的重要组成部分，未经授权的访问会造成灾难性的后果。所有与管理计算机相关的人员都要预先十分关注安全性问题，以避免为恢复被破坏的系统而付出太多的代价。

近年来，“电脑黑客”、计算机病毒受到了各国军方高度重视，它在军事领域的应用也已从理论走向实战。每年全球黑客攻击事件造成的上亿损失，掌握防御技术可以避免这上亿元损失，掌握攻击技术就可以使敌方造成上亿元损失。

而从军事作战角度从发，基于国际互联网的攻击只是在民意、舆论导向上实施心理战，我们更希望能直接对军事战场网络利用网络攻击技术实施攻击，这种攻击有别于传统火力武器硬摧毁，利用网络攻击技术使敌方战场网络局部被入侵后，注入敌方战场网络的病毒或后门自动通过其网络扩散到敌方整个战场网络，并对其指挥、控制产生破坏和干扰。

基于此，网络安全防护理论和技术的研究显得尤为重要和迫切。本书在分析网络安全特性的基础上，深入探讨和研究了网络安全理论基础、信息网络安全防护理论和策略、信息网络安全防护技术、恶意代码运行机理和检测、网络安全评估建模等关键技术。

1.2 网络安全形式

从计算机、网络的基本概念，论述网络安全特性，研究网络安全关键技术。

1.2.1 计算机网络的基本概念

1.2.1.1 计算机网络的定义

凡将地理上位置不同的多台具有独立功能的计算机通过某种通信介质连接起来，并借助于某种网络硬件和软件（网络协议和网络操作系统等）来实现网络上的资源共享和通信的系统称为计算机网络。通信介质可以是有线的，如双绞线、同轴电缆、光纤等，也可以是无线的，如卫星信道、微波、红外光波、超短波等。

计算机网络按通信距离或地理范围的大小又可分为局域网和广域网。距离近的（通常在几千米以内）为局域网，距离远的（通常在几千米以上）为广域网。

1.2.1.2 局域网（Local Area Network，LAN）

美国电子电器工程师协会 IEEE 曾对局域网做了如下定义："局部地区网络在下列方面与其他类型的数据网络不同：通信一般被限制在中等规模的地理区域内，如一座办公楼、一个仓库或一所学校；能够依靠具有从中等到较高数据率的物理通信信道进行通信，而且这种信道具有始终一致的低误码率；局部地区网是专用的，由单一组织机构所使用。"

上述定义比较全面地反映了目前局域网的一些根本特点。不难发现，局域网的主要特点大都源于网络覆盖的地理范围比较小。由于地理范围比较小，可以使用特殊的传输介质和电路技术来得到较高的通信速率，且维持很低的误码率；由于地理范围小，有可能建成由某单位专用的网络；等等。

目前，广泛流行的局域网一般具有以下五个特点。

（1）遵循 ISO（国际标准化组织）的 OSI（开放系统互连）七层网络协议参考模型，并且遵循 IEEE802 委员会对局域网络的底部两层协议（物理层和数据链路层）提出的五个标准文件，即 IEEE802.1 ~ IEEE802.5。

（2）网络覆盖的地理范围有限，通常在 1 ~ 20km 范围以内。

（3）数据传输率很高，通常在 220Mb/s，而快速以太网已经达到 1000Mb/s，还在向更高的传输速率发展。

（4）数据传输可靠，误码率低。

（5）一般都用基带信号传输，且广泛采用广播式传输。

局域网中的工作站和服务器等可以包含微机、高性能的工作站甚至大型主机。如果局域网中的工作站和服务器等都是由微机组成，则称为微机局域网网络，这是目前发展最快和应用面最广的局域网。

1.2.1.3 广域网（Wide Area Network，WAN）

广域网的特点是分布的地理范围很广，所以又称远程网络。它可以分布在一个城市、一个国家，甚至跨过许多国家分布到全球。

几个不同地域的局域网(包括远程单机)相互连接则构成一个广域网。广域网往往是借助于公共传输/通信网来实现的。例如,两个不同地点的局域网,可以通过公共电话网(Public Switch Telephone Network,PSTN)或公共数据网(Public Switch Data Network,PSDN),利用两个局域网中的路由器与调制解调器相互连接起来构成一个广域网。

此外还有企业网(Intranet),它是企业内部的计算机网络,但它采用 Internet 的一些标准通信协议(包括 HTML、HTTP 和 TCP/IP)及图形化 Web 浏览器以支持内部应用,提供部门内部和部门之间的直至全公司范围的通信。也就是说,Intranet 利用 Internet 的工具和标准在自己的公司范围内建立一种仅仅允许本公司人员访问的结构。Internet 可以简单到只让雇员访问工作手册和电话号码表的一台内部的 Web 服务器,也能实现电视电话会议,组内专门讨论以及多媒体传输等诸多功能,甚至于完成与数据库的复杂交互应用。Intranet 也可以利用新闻服务器和邮件服务器为自己建立专用的新闻组,为自己的用户发送电子邮件。

1.2.2 计算机网络的形成与发展

1.2.2.1 早期的计算机网络

自从有了计算机,就有了计算机技术和通信技术的结合。早在 1951 年,美国麻省理工学院林肯实验室就开始为美国空军设计称为 SAGE 的半自动化地面防空系统。该系统分为 17 个防区,每个防区的指挥中心装有两台 IBM 公司的 AN/FSQ-7 计算机,通过通信线路连接防区内各雷达观测站、机场、防空导弹和高射炮阵地,形成联机计算机系统。由计算机程序辅助指挥员决策,自动引导飞机和导弹进行拦截。SAGE 系统最先使用了人机交互作用的显示器,研制了小型计算机形成的前端处理机,制定了 1600b/s 的数据通信规程,并提供了高可靠性的多种路径选择算法。这个系统最终于 1963 年建成,被认为是计算机技术和通信技术结合的先驱。

计算机通信技术应用于民用系统方而,最早的当数美国航空公司与 IBM 公司在 20 世纪 50 年代初开始联合研究,60 年代初投入使用的飞机订票系统 SABRE-1。美国通用电气公司的信息服务系统(GE Information Service)则是世界上最大的商用数据处理网络,其地理范围从美国本土延伸到欧洲、澳洲和日木。该系统于 1968 年投入运行,具有交互式处理能力和批处理能力。网络配置为分层星型结构;各终端设备连接到分布于世界上 23 个地点的 75 个远程集中器,各主计算机也连接到中央集中器;中央集中器经过 50kb/s 线路连接到交换机。

在这一类早期的计算机通信网络中,为了提高通信线路的利用率并减轻主机的负担,已经使用了多点通信线路(图 1-1)、集中器以及前端处理机(图 1-2)。这些技术对以后计算机网络的发展有着深刻的影响。

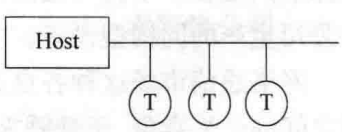

图 1-1 多点通信线路

1.2.2.2 计算机网络的发展时期

20 世纪 60 年代中期出现了大型主机,因而也提出了对大型主机资源远程共享的要求。以程控交换为特征的电信技术的发展则为远程通信提供了实现手段。虽然在早期的计算机网络发展过程中,计算机厂商和通信公司各行其是,但技术方面的互相借鉴和

促进终于导致了这两大技术领域的沟通和合作。最终产生了当今能够联系世界各个地方,深入到国民经济和社会各个领域的规模宏大的计算机互联网络。现代意义上的计算机网络是从1969年美国国防高级研究计划局(DARPA)建成的ARPANET测试网络开始的。该网的主要特点是:①资源共享;②分散控制;③分组交换;④采用专门的通信控制处理机;⑤分层的网络协议。这些特点往往被认为是现代计算机网络的基本特征。

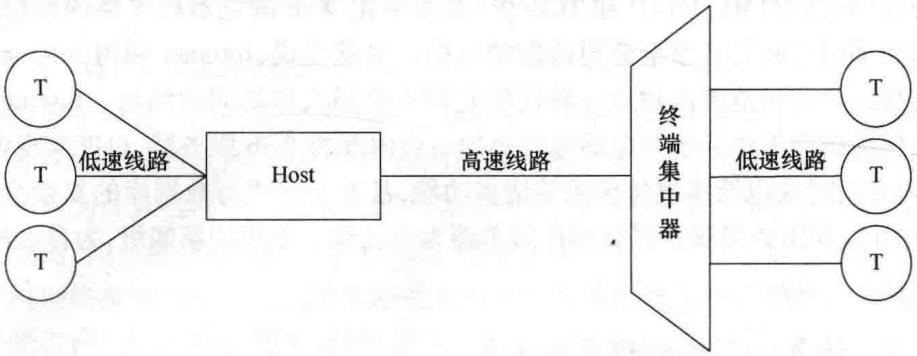

图1-2 使用终端集中器的通信系统

20世纪70年代后期是广域网大发展的时期。各发达国家的政府部门、研究机构和电报电话公司都在发展自己的分组交换网络。例如,英国邮政局的EPSS公用分组交换网络,法国信息与自动化研究所的CYCLADES分布式公用数据网,加拿大的DATAPAC公用分组交换网,日本电报电话公司的DDX-3公用数据网。这些网络都以实现远距离的计算机之间的数据传输和信息共享为主要目的,通信线路大多采用租用电话线路,少数铺设专用线路,数据传输速率在50kb/s左右。这一时期的网络被称为第二代网络,以远程大规模互连为其主要特点。

1.2.2.3 计算机网络标准化阶段

经过20世纪60年代和70年代前期的发展,人们对组网的技术、方法和理论的研究日趋成熟。为了促进网络产品的开发,各大计算机公司纷纷制定自己的网络技术标准。IBM首先于1974年推出了该公司的系统网络体系结构(System Network Architecture,SNA),为用户提供了该公司能够互连的成套通信产品;1975年DEC公司宣布了自己的数字网络体系结构(Digital Network Architecture,DNA);1976年UNIVAC宣布了该公司的分布式通信体系结构(Distributed Communication Architecture,DCA);等等。这些网络技术标准只是在一个公司范围内有效,遵从某种标准的、能够互连的网络通信产品,只是同一公司生产的同构型设备。

网络通信市场这种各自为政的状况使得用户在投资方向上无所适从,也不利于多厂商之间的公平竞争,于是要求制定同一标准的呼声日益高涨。1977年,国际标准化组织ISO的SCI6分技术委员会开始着手制定开放系统互连参考模型(Open System Interconnection/Reference Model,OSI/RM)。作为国际标准,OSI规定了可以互连的计算机系统之间的通信协议,遵从OSI协议的网络通信产品都是所谓的开放系统。今天,几乎所有的网络产品厂商都声称自己的产品是开放系统,不遵从国际标准的产品则逐渐失去了市场。这种统一的、标准化产品互相竞争的市场给网络技术的发展带来了更大的繁荣。

20世纪80年代,微型计算机有了极大的发展,因而局域网技术也得到了相应发展。1980年2月IEEE802局域网标准出台。局域网的发展道路不同于广域网,局域网厂商从一开始就按照标准化、互相兼容的方式展开竞争。用户在建设自己的局域网时选择面更宽,设备更新更快。经过20世纪80年代后期的激烈竞争,局域网厂商大都进入专业化的成熟时期。今天在一个用户的局域网中,工作站可能是IBM的,服务器可能是Compaq的,网卡可能是3COM的,集线器可能是DEC的,而网络上运行的软件则是Microsoft的。

1.2.3 计算机网络安全概述

1.2.3.1 网络安全

在20世纪80年代,大家都意识到只有一台孤立的计算机构成的"孤岛"没有太大意义,于是就把这些孤立的系统组在一起形成网络。随着这样的发展,到了20世纪90年代,人们又逐渐认识到这种由单个网络构成的新的更大的"岛屿"同样没有太大的意义,于是又把多个网络连在一起形成一个网络的网络,或称为互联网(Internet)。一个互联网就是一组通过相同协议族互连在一起的网络。随着互联网的日益扩大和人们在网上的活动不断增多,网络已经变得和人们的经济活动和日常生活密不可分了。随着现代通信技术的发展和迅速普及,特别是随着由通信与计算机相结合而诞生的计算机互联网络全面进入千家万户,使得信息共享应用日益广泛与深入。世界范围的信息革命激发了人类历史上最活跃的生产力,但同时也使得信息的安全问题日渐突出而且情况也越来越复杂。从大的方面来说,信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域。因此,很早就有人提出了"信息战"的概念并将信息武器列为继原子武器、生物武器、化学武器之后的第四大武器。从小的方面来说,信息安全问题也是人们能否保护自己个人隐私的关键。例如:

病毒感染事件1998年增加了2倍,宏病毒入侵案件占60%,已超过1300种,而1996年只有40种。

网上攻击事件大幅上升,对50个国家的抽样调查显示:2014年有73%的单位受到各种形式的入侵,而1996年是42%。据估计,世界上已有2000万人具有进行攻击的潜力。

网上经济诈骗增长了5倍,估计金额达到6亿美元,而同年暴力抢劫银行的损失才5900万美元。一份调查报告中说:有48%的企业受过网上侵害,其中损失最多的达100万美元。

欧盟正式发表了对网上有害和非法信息内容的处理法规。

电子邮件垃圾已被新闻界选为1998年Internet坏消息之一,美国一家网络公司一年传送的电子邮件中有1/3是电子垃圾。

网上违反保密和密码管制的问题已成为各国政府关注的一个焦点。

暴露个人隐私问题突出,如通过美国一个网站很容易得到别人的经济收入信息,另一网址只要输入车牌号码就可查到车主地址,为此这些网址已被封闭。在电子邮件内传播个人隐私的情况更为严重。

带有政治性的网上攻击在1998年有较大增加,包括篡改政府机构的网页,侵入竞选对手的网站窃取信息,在东南亚经济危机中散布谣言,伪造世界热点地区的现场照片,煽

动民族纠纷等,已引起各国政府的高度重视。

我国的情况也大致相仿。一方面 Internet 上网人数增加;另一方面,同一时期内外电对在我国发生的 Internet 安全事件的报道数量也大增,其中包括经济犯罪、窃密、黑客入侵,造谣惑众等。以上报道只是全部景观的一角,却预示着全球信息安全形势不容乐观。我国正处于网络发展的初级阶段,又面临着发达国家信息优势的压力,要在信息化进程中趋利避害,从一开始就做好信息安全工作十分重要。

信息安全研究所涉及的领域相当广泛。从消息的层次来看,包括消息的完整性(保证消息的来源、去向、内容真实无误)、保密性(保证消息不会被非法泄露扩散)、不可否认性(保证消息的发送和接收者无法否认自己所做过的操作行为)等。从网络层次来看,包括可靠性(保证网络和信息系统随时可用,运行过程中不出现故障,若遇意外打击能够尽量减少损失并尽早恢复正常)、可控性(保证营运者对网络和信息系统有足够的控制和管理能力)、互操作性(保 E 协议和系统能够互相连接)、可计算性(保证准确跟踪实体运行达到审计和识别的目的)等。从设备层次来看,包括质量保证、设备备份、物理安全等。从经营管理层次来看,包括人员可靠、规章制度完整等。如果再从行业层次来看,那么所包含的内容就更无法穷尽了。例如,安全移动通信、安全数据通信、安全卫星通信、安全智能网、安全工 SDN、安全计算机、安全网络、安全多媒体、安全 HDTV、安全数据库、安全路由器、安全浏览器等。

1.2.3.2 通信安全

虽然人为因素和非人为因素都可以对通信安全构成威胁,但是精心设计的人为攻击威胁最大。攻击可分为主动攻击和被动攻击。被动攻击不会导致对系统中所含信息的任何改动,而且系统的操作和状态也不被改变。因此,被动攻击主要威胁信息的保密性,常见的被动攻击手段有:①偷窃:用各种可能的合法或非法的手段窃取系统中的信息资源和敏感消息,如对通信线路中传输的信号进行搭线监听,或者利用通信设备在工作过程中产生的电磁泄露截获有用信息等;②分析:通过对系统进行长期监视,利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究,从而发现有价值的信息和规律。主动攻击则意在窜改系统中所含信息,或者改变系统的状态和操作。因此,主动攻击主要威胁信息的完整性、可用性和真实性。常见的主动攻击手段有:①冒充:通过欺骗通信系统(或用户)达到非法用户冒充成为合法用户,或者特权小的用户冒充成为特权大的用户的目的;②篡改:改变消息内容,删除其中的部分内容,用假消息代替原始消息,或者将某些额外消息插入其中,目的在于使对方误认为修改后的信息合法;③抵赖:这是一种来自合法用户的攻击,例如,否认自己曾经发布过的某条消息、伪造一份对方来信、修改来信等;④其他:如非法登录、非授权访问、破坏通信规程和协议、拒绝合法服务请求、设置陷阱和重传攻击等。要保证通信安全就必须想办法在一定程度上克服以上种种威胁。最后,需要指出的是无论采取何种防范措施都不可能保证通信系统的绝对安全。安全是相对的,不安全才是绝对的。在具体实用过程中,经济因素和时间因素是判别安全性的重要指标。换句话说,过时的“成功”攻击和“赔本”的攻击都被认为是无效的。

(1) 通信安全技术之信息加密。信息加密是保障信息安全的最基本、最核心的技

术,也是现代密码学的主要组成部分。信息加密过程是以加密算法来具体实施,它以很小的代价提供很大的安全保护。在多数情况下,信息加密是保证信息机密性的唯一方法。

据不完全统计,到目前为止,已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类,可以将这些加密算法分为常规密码算法和公钥密码算法。在常规密码中,收信方和发信方使用相同的密钥,即加密密钥和脱密密钥是相同或等价的。比较著名的常规密码算法有:美国的 DES 及其各种变形,如 TripleDES、GDES、NewDES 和 DES 的前身 Lucifer;欧洲的 IDEA;日本的 FEAL N、LOKI 91、Skipjack、RC4、RC5 以及以代换密码和转轮密码为代表的古典密码等。在众多的常规密码中影响最大的是 DES 密码。DES 由 IBM 公司研制,并于 1977 年被美国国家标准局确定为联邦信息标准中的一项。ISO 也已将 DES 定为数据加密标准,DES 是世界上最早被公认的实用密码算法标准,目前它已经受住了长达 20 年之久的实践考验。DES 采用 56b 长的密钥将 64b 长的数据加密成等长的密文。在 DES 的加密过程中,先对 64b 长的明文块进行的数据加密成等长的密文。在 DES 的加密过程中,先对 64b 长的明文块进行初始置换,然后将其分割成左右各 32b 长的子块,经过 16 次迭代,进行循环移位与变换,最后再进行逆变换得出 64b 长的密文。DES 的脱密过程与加密过程很相似,只需将密钥的使用顺序进行颠倒。DES 算法采用了散布、混乱等基本技巧,构成其算法的基本单元是简单的置换、代替和模 2 加。DES 的整个算法结构都是公开的,其安全性由密钥保证。DES 的加密速度很快,可用硬件芯片实现,适合于大量数据加密。在公钥密码中,收信方和发信方使用的密钥互不相同,而且几乎不可能由加密密钥推导出脱密密钥。比较著名的公钥密码算法有:RSA,背包密码、McEliece 密码、Diffe Hellman、Rabin、Ong Fiat Shamir、零知识证明的算法、EllipticCurve、ElGa mal 算法等。最有影响的公钥加密算法是 RSA,它能够抵抗到目前为止已知的所有密码攻击。RSA 诞生于 1978 年,目前它已被 ISO 推荐为公钥数据加密标准。RSA 算法基于一个十分简单的数论事实:将两个大素数相乘十分容易,但是想分解它们的乘积却极端困难,因此可以将乘积公开作为加密密钥 RSA 的优点是不需要密钥分配,但缺点是速度慢。当然在实际应用中人们通常是将常规密码和公钥密码结合在一起使用,例如:利用 DES 或者 IDEA 来加密信息,而采用 RSA 来传递会话密钥。按照其具体目的,信息确认系统可分为消息确认、身份确认和数字签名。消息确认使约定的接收者能够验证消息是否是约定发信者送出的且在通信过程中未被篡改过的消息。身份确认使得用户的身份能够被正确判定。最简单但却最常用的身份确认方法有个人识别号、口令、个人特征(如指纹)等。数字签名与日常生活中的手写签名效果一样,它不但能使消息接收者确认消息是否来自合法方,而且可以为仲裁者提供发信者对消息签名的证据。其中,最著名的算法也许是数字签名标准(DSS)算法。

(2) 防火墙技术。它是一种允许接入外部网络,但同时又能够识别和抵抗非授权访问的网络安全技术。防火墙扮演的是网络中的“交通警察”角色,指挥网上信息合理有序地安全流动,同时也处理网上的各类“交通事故”。防火墙可分为外部防火墙和内部防火墙。前者在内部网络和外部网络之间建立起一个保护层,从而防止“黑客”的侵袭,其方法是监听和限制所有进出通信,挡住外来非法信息并控制敏感信息被泄露;后者将内部