



JISUANJI WANGLUO XINXI ANQUAN
JI GUANLI JISHU YANJIU

计算机网络信息安全 及管理技术研究

王晓霞 刘艳云 著

非
外
借

中国原子能出版社

计算机网络信息安全 及管理技术研究

王晓霞 刘艳云 著

中国原子能出版社

图书在版编目(CIP)数据

计算机网络信息安全及管理技术研究 / 王晓霞, 刘艳云著. -- 北京: 中国原子能出版社, 2019. 6

ISBN 978-7-5022-9869-2

I. ①计… II. ①王… ②刘… III. ①计算机网络—信息安全—安全管理—研究 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2019)第 134626 号

内 容 简 介

随着国民经济信息化进程的推进、网络应用的发展和普及,各行各业对计算机网络的依赖程度越来越高,这种高度依赖将使社会变得十分“脆弱”,一旦计算机网络受到攻击,不能正常工作,甚至全部瘫痪时,就会使整个社会陷入危机。因此,对于网络信息安全技术的研究就显得十分必要。本书重点论述了与网络信息安全有关的一些技术及其实现方法,主要内容包括:计算机系统安全、数据库与数据安全、加密与认证技术、防火墙与网络隔离技术、安全检测技术、计算机病毒防范技术、VPN 与 NAT 技术及安全协议、计算机信息安全管理等。本书结构合理,条理清晰,内容丰富新颖,是一本值得学习研究的著作,可作为从事网络信息安全技术的科研和工程技术人员的参考书。

计算机网络信息安全及管理技术研究

出版发行 中国原子能出版社(北京市海淀区阜成路 43 号 100048)

责任编辑 张琳

责任校对 冯莲凤

印刷 三河市铭浩彩色印装有限公司

经销 全国新华书店

开本 787mm×1092mm 1/16

印张 19.75

字数 256 千字

版次 2019 年 9 月第 1 版 2019 年 9 月第 1 次印刷

书号 ISBN 978-7-5022-9869-2 定价 90.00 元

网址: <http://www.aep.com.cn>

E-mail: atomep123@126.com

发行电话: 010-68452845

版权所有 侵权必究

前 言

21 世纪是互联网时代,网络安全的内涵发生了根本性的变化。网络安全在信息领域中的地位从一般性的防卫手段变成了非常重要的安全防御措施,网络安全技术也从之前只有少部分人研究的专门领域变成了生活中无处不在的应用。当人类步入 21 世纪这一信息化社会的时候,网络安全问题成为了互联网的焦点,我们每个人都时刻关注着与自身密不可分的网络系统的安全,从应用和管理的角度建立起一套完整的网络安全体系,无论对于单位还是个人都显得尤为重要。

近年来,国家实施的信息系统工程和信息基础设施建设,已经使计算机系统成为当今社会特征的一个重要组成部分。黑客对信息系统的攻击一直都没有停止过,其手段也越来越高明,这无疑给计算机信息安全带来了更大的威胁。我国网络基础设施和信息系统安全保障建设远滞后于信息化发展,尽管安全意识不断增强,但缺乏信息安全防护措施。特别是国家强制实施信息安全等级保护工作以来,越来越多的相关专业技术人员需要学习和掌握信息安全技术与应用技能。

本书以网络面临的常见安全问题以及相应的防护、安全技术为主线,系统地介绍了网络安全的基本概念、安全基础、安全防护、安全管理等内容。全书共分为 9 章,第 1 章网络信息安全综述,第 2 章计算机系统安全,第 3 章数据库与数据安全,第 4 章加密与认证技术,第 5 章防火墙与网络隔离技术,第 6 章安全检测技术,第 7 章计算机病毒防范技术,第 8 章 VPN 与 NAT 技术及安全协议,第 9 章计算机信息安全管理。

本书以加强实践性、提高实用性为目的进行写作,讲究知识性、系统性、条理性、连贯性,注重知识概念,强调深入浅出。本书以清晰的思路、合理的体系、通俗的语言,向读者介绍计算机网络安全的基本理论、基本知识和常用技术。本书的特点是文字简明、图表准确、通俗易懂,用循序渐进的方式叙述网络安全知识,对网络信息安全及管理技术难点的介绍适度,内容安排合理,力求反映计算机网络安全管理的新问题、新技术和新应用。

本书是结合作者多年相关科研成果而撰写的,凝聚了作者的智慧、经验和心血。在撰写过程中参考了大量的书籍、专著和文献,在此向这些专家、编辑及文献原作者表示衷心的感谢。

由于作者水平有限以及时间仓促,书中难免存在一些不足和疏漏之处,敬请广大读者和专家给予批评指正。

作 者

2019年3月

目 录

第 1 章 网络信息安全综述	1
1.1 计算机技术与互联网的发展	1
1.2 网络信息安全简介	6
1.3 网络信息安全概念与目标	12
1.4 研究网络信息安全的意义	14
第 2 章 计算机系统安全	15
2.1 操作系统安全技术	15
2.2 计算机硬件安全	19
2.3 物理安全	22
2.4 系统访问控制	25
2.5 程序系统安全	37
第 3 章 数据库与数据安全技术	46
3.1 数据库系统的缺陷和威胁	46
3.2 数据库的安全特性	48
3.3 推理泄露问题与控制机制	50
3.4 数据库的安全保护技术	55
3.5 数据库的多级安全问题	58
第 4 章 加密与认证技术	70
4.1 加密技术与 DES 加解密算法	70
4.2 电子邮件加密软件 PGP	85
4.3 加密算法	90
4.4 密钥管理技术	96
4.5 数字签名、数字证书及其应用	101
4.6 认证技术	110
第 5 章 防火墙与网络隔离技术	136
5.1 防火墙技术及 Windows 防火墙配置	136
5.2 网络隔离技术与网闸应用	179

第 6 章 安全检测技术	184
6.1 入侵检测技术与网络入侵检测系统产品	184
6.2 入侵检测的分析及发展	189
6.3 漏洞检测技术和微软系统漏洞检测 工具 MBSA	195
第 7 章 计算机病毒防范技术	201
7.1 计算机网络病毒的特点及危害	201
7.2 病毒防范技术与杀病毒软件	204
7.3 解析计算机典型病毒	224
7.4 反垃圾邮箱技术	235
7.5 计算机病毒发展的新技术	238
第 8 章 VPN 与 NAT 技术及安全协议	243
8.1 虚拟专用网 VPN 及 VPN 的安全性	243
8.2 VPN 应用	254
8.3 网络地址转换 NAT	256
8.4 因特网的安全协议 (IPSec)	260
8.5 因特网商务中的安全协议	265
8.6 PGP 协议	268
第 9 章 计算机信息安全管理	271
9.1 网络风险分析与评估	271
9.2 信息安全相关标准	274
9.3 互联网单位管理	278
9.4 网络用户的上网行为管理	290
9.5 互联网监控与不良信息过滤系统	292
9.6 信息安全等级保护与测评	296
9.7 信息安全管理新发展:基于云计算的大数据 安全管理	300
参考文献	304

第 1 章 网络信息安全综述

计算机网络是利用通信线路把地理位置上分散的计算机和通信设备连接起来,在系统软件和协议的支持下,以实现数据通信和资源共享为目的的复杂计算机系统。网络的基本资源包括硬件资源、软件资源和数据资源等。网络的广泛应用,使得网络与人们的生活、工作密切相关,网络已经成为维系社会正常运作的支柱。网络中的信息关乎企业甚至国家的发展,因此,网络信息安全也事关个人、企业,甚至国家的安危。

1.1 计算机技术与互联网的发展

信息技术(Information Technology, IT),广义上指充分利用和扩展人类器官功能进行信息处理的各种方法、工具与技能的总和。自人类诞生以来,信息技术已经历了五次革命:第一次是语言的产生,发生在距今 35 000~50 000 年,开启了人类系统传递信息之幕;第二次是文字的发明,大约发生于公元前 3500 年,使信息传递第一次突破了时间和空间的限制;第三次是造纸术和印刷术的发明与普及,始于公元 1040 年中国活字印刷的发明,大大降低了信息传递的成本,提升了信息传递的效率,初步为大众传播时代的到来奠定了基础;第四次是电报、电话、广播、电影和电视的发明与普及,始于 1837 年有线电报机的问世,电磁波的运用使信息传播再次显著突破时空限制,全面进入大众传播时代;第五次信息技术革命始于 20 世纪 40 年代,其标志是电子计算机的

普及,计算机与现代通信技术的有机结合带领人类进入了数字信息传播时代。

1.1.1 计算机技术发展简史

迄今为止,计算机技术的发展历程大致可以划分为五个阶段:电子管计算机时代、晶体管计算机时代、集成电路计算机时代、大规模集成电路计算机时代和智能化计算机时代。

第一阶段:电子管计算机时代(1943—1957)。1943年,英国推出一款内含2 400个真空电子管、可编程的计算机,每秒能解译5 000个字符。同年,约翰·莫克利(John Mauchly)和约翰·伊克特(John Eckert)在美国政府的资助下开始研制用于计算弹道的电子装置。1946年,他们在费城推出的ENIAC(Electronic Numerical Integrator and Computer),标志着现代计算机的诞生。ENIAC使用了18 000个电子管、70 000个电阻器,有500万个焊接点,占地170平方米,重30吨,每秒可进行5 000次加法运算。ENIAC使用的是真空电子管和磁鼓存储数据,体积大、能耗高、故障多、成本高等缺点大大制约了它的普及应用。1949年,第一台使用磁带的计算机EDVAC(Electronic Discrete Variable Automatic Computer)诞生,在计算机存储技术方面取得了革命性的突破。1951年,约翰·伊克特和约翰·莫克利共同设计的一台商用计算机系统UNIVAC-1被用于美国人口普查,标志着计算机进入了商业应用时代。

第二阶段:晶体管计算机时代(1958—1963)。1954年,美国电报电话公司(AT&T)贝尔实验室成功研制了第一台半导体计算机(TRADIC)。晶体管和磁芯存储器的应用标志着计算机技术发展进入了第二代。1958年以后的计算机开始大量采用晶体管和印刷电路板。IBM公司推出的晶体管化7090型计算机被作为第二代电子计算机的代表载入了史册。晶体管计算机体积大幅度缩小、能耗更低、速度更快、功能更强。在计算机语言发展方

面:1957年,IBM公司的巴克斯(Bacchus)及其研究小组开发出第一种高级计算机语言 FORTRAN;1960年,第一种结构化程序设计语言 ALGOL(ALG Orithmic Language)问世;1961年,APL编程语言(A Programming Language 或 Array Processing Language)被推出。各种高级计算机语言的升级发展逐步降低了计算机编程的难度,促使程序员、数据分析师和系统专家等一批与计算机相关的新职业诞生。

第三阶段:集成电路计算机时代(1964—1972)。1958年,美国工程师杰克·基尔比(Jack Kilby)将多种电子元件集成到半导体芯片上发明了集成电路。1964年,IBM公司推出了首套系列兼容机,此后到1972年基本上是集成电路主导计算机的时代。采用集成电路后,计算机的体积变得更小,能耗也进一步降低,运算速度更快,性能更加稳定。英特尔(Intel)公司名誉董事长戈登·摩尔(Cordon Moore)经过长期观察发现,集成电路上可容纳的晶体管的数目大约每隔18个月便可增加一倍,性能也随之提升一倍,这就是著名的“摩尔定律”。这一时期,计算机技术取得的其他重要成就,还包括鼠标的设想、操作系统的出现,以及后来被称为现代互联网雏形的 RPANET 的成功运行。

第四阶段:大规模集成电路计算机时代(1972—1989)。1971年,英特尔公司成功开发出第一款微处理器4004,其含有2300个晶体管,每秒可执行6万条指令,这标志着大规模集成电路时代的到来。随着大规模集成电路和微处理器技术的发展,个人计算机得到了快速发展。1972年,英特尔公司推出了面向个人计算机的微处理器8080。1975年,比尔·盖茨(Bill Gates)创办了微软公司(Microsoft)。1976年,史蒂夫·乔布斯(Steve Jobs)创立苹果计算机公司,并推出Apple人工计算机。1981年,IBM公司推出的个人计算机开始应用于家庭、办公室和学校。微软公司接受委托开发用于个人计算机的DOS操作系统。1982年,英特尔公司推出了80286型微处理器,之后又不断对其进行升级换代,陆续推出80386、80486、奔腾(PENTIUM)、奔腾二代(PENTI-

UM II)、奔腾三代(PENTIUM III)。为了与 IBM 公司个人计算机竞争,苹果公司于 1984 年推出了使用 Motorola 6800 微处理器的 Apple Macintosh 系列电脑,提供图形界面,可以通过鼠标方便地操作。从 1990 年开始,微软公司开始推出 Windows 系列操作系统,并逐步放弃研发 DOS 系统。

第五阶段:智能化计算机时代(20 世纪 90 年代至今)。20 世纪 90 年代以来,计算机的性能大幅提升。微处理技术向单芯多核心、单芯片多线程以及系统级芯片(System on a Chip, SOC)方向发展,集成电路进入了纳米时代。与此同时,信息存储技术和传播技术也随着纳米光电技术、光通信技术和光存储技术的不断发展而提升。信息显示技术从最初的阴极射线管发展到了液晶显示器、等离子显示器和场发射显示器等。软件系统则快速向智能化方向发展。计算机进入人们的生活后,人机互动技术向着更简单、更丰富、更便捷的方向发展。这一技术发展趋势不断推动着个人计算机和智能终端的快速普及,同时也是全球计算机网络得以形成的必要条件。

1.1.2 互联网发展简史

现代信息通信技术构筑了电信网、广播电视网、互联网等多种网络,其中互联网是对人类现实生活影响最为广泛和深远的网络,毫无疑问,互联网已经成为人类发展史上的一座重要的里程碑,标志着网络信息社会的来临。总体来看,互联网从萌芽至今大致经历了四个主要发展阶段。

第一阶段:阿帕网时期(20 世纪 60 年代至 20 世纪 70 年代中期)。1961 年,美国麻省理工学院的伦纳德·克兰罗克(Leonard Kleinrock)博士发表了分组交换技术的论文,提出以分组交换网为中心的计算机网络中的通信双方都是具有自主处理能力的计算机,功能以系统计算和资源共享为主,该技术后来成为互联网的标准通信方式;1962 年,同校的克利德(J. C. R. Licklider)提出

了“银河系网络”概念,构想了一套由世界各地计算机相互连接而成的系统。在上述研究的基础上,1969年,美国国防部高级研究计划署建立了世界上第一个远程分组交换网——阿帕网(ARPANET),成为互联网诞生的标志;1971年,位于英国剑桥的BBN科技公司的工程师雷·汤姆林森(Ray Tomlinson)开发出了电子邮件,此后阿帕网技术逐渐向美国大学等研究机构普及;1972年,罗伯特·卡恩(Robert Kahn)在计算机通信国际会议上首次向大众公开演示了阿帕网技术,并提出了开放式架构网络的设想,后来,这个设想成为分组无线网项目中一个异军突起的独立项目,被称为“网络之间”(Interneting)，“互联网络”一词正式进入信息技术领域,随后卡恩又开发了一个能够满足开放式架构网络环境需要的传输控制协议/互联网协议(TCP/IP),以分组交换技术和开放式网络架构为代表的技术原型为互联网的产生奠定了基础。作为互联网的雏形,当时的阿帕网的应用主要局限于政府和军事领域,其网络范围并未超出美国国界。在此阶段,电子邮件功能的推出开辟了一个人与人交流信息的新渠道,同时也成为计算机网络社会化应用的开端。

第二阶段:局域网时期(20世纪70年代中后期至20世纪90年代初期)。随着阿帕网应用的深入发展,其数据传输、资源共享和分布处理等优越性已经非常显著。局域网在产业部门的应用也得到了进一步的拓展。1974年英国剑桥大学计算机研究室开发了著名的剑桥环局域网(Cambridge Ring),1976年Xerox公司的梅特卡夫研制了以太网,标志着局域网时代的开始。技术专家致力于推动计算机网络向更大规模互连和更加开放方向发展。为了管理大量独立的局域计算机网络,保罗·莫卡派乔斯(Paul V. Mockapetris)发明了域名系统(DNS),单一路由分布式算法被分层路由模式取代,通过内部网关协议(IGP)和外部网关协议(EGP)把各局域网连接成规模更大的广域网。1984年,国际标准化组织正式颁布了“开放系统互连基本参考模型”的国际标准,推动计算机网络走上了标准化发展轨道。这一标准化进程为形成

全球互联网奠定了接口和兼容基础。

第三阶段：全球互联网时期（20 世纪 90 年代至 21 世纪初）。随着现代信息通信技术的迅猛发展，尤其是 1993 年美国宣布实施国家信息基础设施（NII）的行动计划后，全球其他国家陆续跟进，推动了人类进入全球互联网发展的新阶段。1991 年，欧洲粒子物理研究所（CERN）的科学家提姆·伯纳斯李（Tim Berners-Lee）开发的万维网（World Wide Web）首次公开亮相。万维网使用的是超文本传输协议，是一个分布式的超媒体系统，可以便捷地从一个站点链接到另一个站点。在此技术支撑下，大量商业资讯门户网站以及企业和政府机构等纷纷涌现，一方面使信息的供给呈几何倍数增长，另一方面以计算机网络为基础的虚拟社会快速成型。1993 年，第一款图形界面浏览器的问世使计算机的操作难度大大下降。计算机社会化应用的步伐进一步加快。

第四阶段：智能互联网时期。进入 21 世纪以后，网络技术加速向智能化、社会化、泛在化、移动化、宽带化等方向发展，面向互联网的电信网、计算机网和广播电视网三网融合成为大势所趋，而云计算（Cloud Computing）、移动互联网、物联网等新兴技术得到了广泛应用和深度融合，对全球网络空间的形成再一次发挥了重大推进作用，新技术、新应用带动了网络数据资源的爆发式增长，一个基于大数据的“按需应变”的智能互联网时代正在到来。为此，美国政府在 2012 年 3 月发布《大数据研究和发展倡议》，并作为新一轮的国家信息化发展战略，同时全力打造 Data. Gov，推行政府数据开放。由此可以预见，围绕大数据的开发利用正成为全球网络空间新一轮发展的重要引擎，将进一步强化人类对网络空间的依赖。

1.2 网络信息安全简介

计算机网络中存储、传输和处理的信息多种多样，许多是敏

感信息,甚至是国家机密,例如,政府宏观调控决策、商业经济信息、股票证券、科研数据等重要信息。由于网络安全漏洞等原因,可能会造成信息泄露、信息窃取、数据篡改、数据破坏、计算机病毒发作、恶意信息发布等事件,由此造成的经济损失和社会危害难以估量。互联网已经渗透到生活的方方面面,习近平主席曾说过,“没有网络安全,就没有国家安全”。在频发的安全事件催化下,网络信息安全已经上升至国家战略高度。

1.2.1 网络信息安全的重要性

尽管网络的重要性已经被广泛认同,但对网络信息安全的忽视仍很普遍,缺乏网络信息安全意识的状况仍然十分严峻。不少企事业单位极为重视网络硬件的投资,但没有意识到网络信息安全的重要性,对网络信息安全的投资较少。这也使得目前不少网络信息系统都存在先天性的安全漏洞和安全威胁,有些甚至产生了非常严重的后果。下面是近年来发生的一些重大网络信息安全事件。

2014年12月25日,乌云漏洞报告平台称,大量12306用户数据在互联网疯传,内容包括用户账号、明文密码、身份证号码、手机号码和电子邮箱等。这次事件是黑客首先通过收集互联网某游戏网站,以及其他多个网站泄露的用户名和密码信息,然后通过撞库^①的方式利用12306安全机制的欠缺获取了13万多条用户数据。

2015年12月23日,乌克兰发生了一次影响很大的通过有组织、有预谋的定向网络攻击,致使乌克兰境内近1/3的地区持续断电的安全事件。

2016年5月7日,根据路透社报道,黑客在黑市上交易高达

^① 撞库是指黑客利用从某些网站或渠道获取的用户账号和密码,在其他网站上进行登录尝试。这主要是由于目前有相当一部分互联网用户喜欢在不同网站上使用统一的用户名和密码。

3 亿条被盗的邮件账户用户名和密码,其中,5 700 万条为俄罗斯 Mail.ru 邮件账户、4 000 万条为雅虎邮件账户、3 300 万条为 Hotmail 邮件账户,以及 240 万条为 Gmail 邮件账户。另外,还包含成千上万的德国和中国的电子邮件账户,以及数以千计的涉及美国银行业、制造业和零售业公司员工的用户名和密码。

2017 年 5 月 12 日,一款名为“想解密”(又称“想哭”)的勒索病毒在全球范围内疯狂传播。欧洲刑警组织 5 月 14 日称,已经有上百个国家和地区,数十万台计算机被感染,而后需要支付高额赎金,才能解锁计算机中被感染的文件。我国部分高校和大型企业的内网也遭受到病毒的侵袭。

以上仅仅是一些个案,事实上,这样的案例不胜枚举,而且计算机犯罪案件有逐年增加的趋势。因此,网络系统必须有足够强大的安全体系,无论是局域网还是广域网,无论是单位还是个人,网络信息安全的目标是全方位防范各种威胁以确保网络信息的保密性、完整性和可用性。

1.2.2 常见计算机网络的信息安全问题种类

计算机网络的信息安全问题,是指计算机程序在实际应用中,可能存在的数据信息丢失、被盗等情况,对计算机正常运行产生干扰的问题。随着计算机网络技术不断开发,计算机网络的信息安全受到的重视程度也越来越高。相关部分研究资料显示:截止到 2018 年上半年,个人信息丢失,商业信息被盗,以及金融资产窃取等问题,占现代计算机网络应用问题的 70.19%~88.93%。同比 2017 年增长了 1~1.5 倍,由此而言,加强对社会计算机网络的信息安全问题的综合管理刻不容缓。

结合当代计算机网络应用的实际情况,将常见的计算机网络的信息安全问题归纳为计算机系统风险和网络运行风险两大类。计算机系统风险是指计算机硬件系统中所包含的风险类型,如计算机系统访问权限安全设计问题、硬件应用故障等问题。网络运

行风险是指计算机在联网操作的环境下,出现的信息运行问题、数据传输/接收问题,这些问题一般都具有连锁反应,对计算机用户造成的损害要远比计算机硬件问题更大,如病毒入侵、文件传输干扰、恶性信息破坏等。

1.2.3 计算机网络的信息安全体系结构的建设要点

当代计算机网络的信息安全体系结构建设,已经逐步从初级阶段的信息安全管理,向着“预防、应对、反击”三方结合的趋势转变,这为现代计算机网络信息技术的综合探索带来了更加明晰的方向,由此,笔者将计算机的信息安全体系结构管理要点归纳为以下几点。

1.2.3.1 计算机网络信息安全预警结构

网络信息安全预警系统,是网络信息安全管理的基础环节,该模块可对计算机网络的信息安全情况进行诊断,是计算机网络安全管理中的初步评估环节。

(1) 对象控件的安全预警

计算机安全预警系统借助对象控件的检测结果,对计算机网络信息调控情况进行判断。假设计算机当前登录界面包括 A 和 B 两个小页面,但 A 界面中存在病毒侵入的风险,B 网页正常。计算机预警控件程序同时对 A 和 B 界面进行监控,控件检测到 A 界面中有病毒入侵后,会立即跳出程序运转风险入侵预警信号提示框。

(2) 传输环境的安全预警

计算机信息安全预警系统是通过信息传输环境预警法对可能存在的运行风险进行警报。如,当我们通过计算机 USB 接口,向计算机系统内导入文件时,计算机程序自动对新导入文件进行快速扫描。若导入新文件中存在风险问题,系统将第一时间关闭 USB 信息接收窗口,实行相应的信息安全预防保护。即,计算机

安全信息预警系统中传输环境预警,主要是从计算机硬件安全问题上进行信息探究,从这一层面来说,计算机信息安全预警系统,基本实现了内部程序与外部程序的安全预防^①。

1.2.3.2 计算机信息安全保护结构

计算机信息安全保护结构,主要是对网络信息交流过程中存在的风险问题进行防护。常见的信息安全保护结构,包括防火墙技术和 PKI 技术。

防火墙技术,是指在计算机硬件基础上,建立与硬件程序相互关联的信息安全保护结构。如,利用计算机主体信息传输 IP 地址,建立多个计算机信息传输网址。信息传输时,只有传输的 IP 代码对应,计算机程序才会接收外部信息。

而 PKI 技术,是指利用计算机信息安全保护程序的历史记录,对计算机当前网络运行情况进行安全状况反馈。如,计算机本次运行共跳转了 30 次网页,计算机信息系统进行安全保护时,PKI 会借助公共信息传输钥匙,逐一对计算机历史网页进行传输安全验证。一旦界面安全验证公共钥匙与密码不够匹配,说明当前网页运行界面不够安全,PKI 程序将终止界面跳转操作,返回安全界面。即,计算机信息安全调控界面,可在第一时间对传输信息进行安全保护,实现界面信息的安全管理。

1.2.3.3 计算机信息安全检测结构

(1) 动态安全检测反馈

计算机信息安全检测结构,主要是利用信息安全检测结构,对计算机程序运行中的隐藏性风险进行检测,以实现计算机信息传输安全管理的目的。计算机信息安全管理系统,可有效防止电

^① 刘向东,陈晨.分析计算机网络的信息安全体系结构[J].电子世界,2018(21):85+87.