第 1 章　信息安全简介

1.1　信息安全重要性

21 世纪是信息的时代，信息无所不在。著名的控制论专家维纳曾经说过：“信息既不是物质，也不是能量，信息就是信息”。因此信息和物质、能量是任何系统的三大组成要素。美国著名未来学家阿尔温托尔勒说过：“谁掌握了信息，控制了网络，谁将拥有整个世界”。随着信息技术和产业蓬勃发展以及信息高速公路的提出和建设，无所不在的信息网络给我们的生产、生活带来了巨大的方便并极大地推动了人类社会的进步和发展，在人类社会中发挥着越来越至关重要的作用。然而，另一方面，不断发生的信息安全事件也给社会和人民带来了巨大的精神和物质上的损失，甚至危及国家和整个人类社会的稳定和发展。

信息安全指的是保证信息在传输、存储和变换过程中信息的机密性（Confidentiality）、完整性（Integrity）、不可否认性（Non-Repudiation）以及可用性（Availability）等基本安全属性，即保证信息系统在运行过程中不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。信息安全问题对于一个国家来说，是涉及政治、军事、社会和经济各方面的综合问题。同时，信息安全问题对于个人来说，也是至关重要的。

信息安全首先是一个政治问题。随着因特网（Internet）的普及，因特网已经成为了一个新的思想文化斗争和思想政治斗争的阵地。2002 年至 2003 年，不法分子曾多次攻击鑫诺卫星，将正常播出的电视节目篡改为反动的宣传资料片。1999 年至 2001 年爆发的数次中美黑客大战，更是将信息安全的政治属性体现得淋漓尽致。因此，信息安全问题首先必须从政治的高度来认识它，在互联网上保证健康安全的政治信息的发布和监管。

信息安全更是一个军事问题。信息安全和战争军事是密不可分的，如何保密己方军事机密以及如何窃取到对方的军事机密是人类战争史上一个永恒的话题。而在现代，各国都在军队里面设立了信息战部队，可以说现代战争就是信息战，也就是信息安全的直接对抗。在科索沃战争和伊拉克战争中，美军都使用了电磁炸弹，瘫痪了对方的信息系统，从而占据了战争的信息制高点。而以前的南联盟也曾经组织过黑客联盟对北约信息系统造成一定的破坏。另外各国都积极组织收集互联网上的军事情况，由于互联网造成的军事信息泄密屡见不鲜。

信息安全是一个社会问题。首先，网络上的虚假信息极容易传播和造成社会动荡。1999 年，某商都热线一个 BBS，一张关于某银行支行行长携巨款外逃的帖子，造成了社会的动荡，10 万人上街排队，提取了 10 亿元现金。其次，互联网上的赌博、黄色等信息泛滥严重败坏了社会风气，造成了大量的社会问题。再者，对一些互联网基础设施的攻击也严重扰乱了社会管理秩序。2001 年 2 月 8 日，新浪网遭受攻击，电子邮件服务器瘫痪了 18 小时，造成几百万用户无法正常联络。2009 年 6 月 25 日，广东电信骨干网由于受到攻击大面积瘫痪，造成广大用户不能正常使用业务。

信息安全也是一个经济问题。由于信息产业在各国的经济构成比重越来越大，信息安全问题造成的经济损失就不可估量，有许多犯罪分子瞄上了黑客攻击行为带来的巨大经济利

益。1999 年 4 月 26 日，CIH 病毒大爆发，有统计说，我国受其影响的计算机总量达 36 万台之多。有人估计在这次事件中，经济损失高达近 12 亿元。2000 年 2 月 7 日起的一周内，黑客对美国的雅虎等著名网站发动攻击，致使这些网站瘫痪，造成直接经济损失 12 亿美元。2009 年，中央电视台“3·15”晚会上揭秘黑客攻击已经形成了一个完整的产业链，每年给用户和社会带来上百亿元的经济损失。

信息安全问题对于个人也是至关重要。现在人们经常碰到的电话诈骗案就是由于个人信息被泄露而使得犯罪分子有机可乘。犯罪分子可能通过在 ATM 上的摄像头或者偷看甚至采用绑架逼问等暴力手段获取用户的银行卡密码，将用户账户上的钱财洗劫一空。犯罪分子还可能通过病毒、木马、间谍软件等盗取用户的网上银行账户密码、QQ 账户密码、淘宝账户密码、网游账户密码等，给用户带来巨大的精神上和物质上的损失。著名的香港艺人陈冠希“艳照门”事件，也是由于其个人隐私信息遭到恶意泄露而对其个人以及相关女艺人和家庭都造成了巨大的负面影响。

各国领导人都非常重视信息安全问题，纷纷就信息安全问题公开发表了自己的观点。克林顿：谁掌握了信息，谁就掌握了主动。普京：信息资源及其基础设施成为角逐世界领导地位的舞台。

我国政府历来重视信息安全问题。2003 年 9 月，中办发[2003]27 号文《国家信息化领导小组关于加强信息安全保障工作的意见》，提出建立国家信息安全的十大任务。2005 年 4 月，教育部发布了《教育部关于进一步加强信息安全学科、专业建设和人才培养工作的意见》的文件，对信息安全学科的建设和信息安全人才培养给出了指导性意见。2007 年，公安部、国家保密局、国家密码管理局、国务院信息工作办公室四部委联合发布了《信息安全等级保护管理办法》，对信息安全保护做了文件性规定。另外，国家在成都、武汉和上海建立了信息安全产业基地，支持信息安全产业的发展。我国在立法上重视保证信息安全，从 1994 年的《中华人民共和国计算机信息系统安全保护条例》起，我国颁布的全面规范信息安全的法律法规有 18 部之多，包括《电子签名法》、《保守国家秘密法》等。

在信息化的浪潮下，在信息社会里，信息安全问题是一个非常重要的问题，不但关系着普通老百姓的生产、生活，更维系着国家的安定繁荣和中华民族的全球竞争力，必须引起我们的高度重视。

1.2 信息安全重大事件

信息安全的历史十分悠久。最早可以追溯到古巴比伦时代的费斯托斯（Phaistos）圆盘，它是一种直径约为 160mm 的黏土圆盘，始于公元前 17 世纪，表面有明显字间空格的字母。古希腊斯巴达开始出现原始的密码器，用一条带子缠绕在一根木棍上，沿木棍纵轴方向写好明文，解下来的带子上就只有杂乱无章的密文字母。解密者只需要找到相同直径的木棍，再把带子缠上去，沿木棍纵轴方向即可读出有意义的明文。公元前 1 世纪，著名的恺撒（Caesar）密码被用于高卢战争中，这是一种简单易行的单字母替代密码。公元 9 世纪，阿拉伯的密码学家阿尔·金迪（Al′Kindi），也被称为伊沙克（Ishaq），他同时还是天文学家、哲学家、化学家和音乐理论家，提出解密的频度分析方法，通过分析计算密文字符出现的频率来破译密码。公元 16 世纪中期，意大利的数学家卡尔达诺（G．Cardano，1501—1576）发明了卡尔达诺漏格板，覆盖在密文上，可从漏格中读出明文。公元 16 世纪晚期，英国的菲利普斯

（Philips）利用频度分析法成功破解苏格兰女王玛丽的密码信，信中策划暗杀英国女王伊丽莎白，这次解密将玛丽送上了断头台。几乎在同一时期，法国外交官维热纳尔（Blaise de Vigenere）提出著名的维热纳尔方阵密表和维热纳尔密码（Vigenerecypher），这是一种多表加密的替代密码，可使阿尔·金迪和菲利普斯的频度分析法失效。在中国古代，也有一些加密的雏形。宋曾公亮、丁度等编撰《武经总要》记载，北宋前期，在作战中曾用一首五言律诗的 40 个汉字，分别代表 40 种情况或要求，这种方式已具有了密本体制的特点。

自 19 世纪以来，由于电报特别是无线电报的广泛使用，为密码通信和第三方的截收都提供了极为有利的条件。通信保密和侦收破译形成了一条斗争十分激烈的隐蔽战线，有时候甚至为扭转战局起到了关键性的作用。1894 年，中日甲午海战中方失败的原因之一是日方战前破译了大量的清政府密电。1917 年，英国破译了德国外长齐默尔曼的电报，促成了美国对德宣战。1942 年，美国从破译日本海军密报中获悉日军对中途岛地区的作战意图和兵力部署，从而能以劣势兵力击破日本海军的主力，扭转了太平洋地区的战局。1943 年 4 月 13 日，日本海军司令山本五十六视察所罗门群岛基地的行程等由日第 8 舰队司令用最新的 JN25 版本发往基地，美情报人员根据经验破译了这份密报，导致 5 天后美机准确地击落了山本五十六的座机。

在近代，随着计算机网络的普及应用，国内外信息安全事件更是层出不穷，而且造成的影响也越来越大。1983 年，当凯文·保尔森（Kevin Poulsen）还是一名学生的时候，他就成功入侵 ARPANet（因特网的前身）。他当时利用了 ARPANet 的一个漏洞，能够暂时控制美国地区的 ARPANet。1990 年，为了获得在洛杉矶地区 Kiis-fm 电台第 102 个呼入者的奖励——保时捷 944 s2 跑车，凯文·保尔森控制了整个地区的电话系统，以确保他是第 102 个呼入者。最终，他如愿以偿获得跑车并为此入狱 3 年。他现在是《有线新闻》（Wired News）的高级编辑。1993 年，自称为骗局大师（MOD）的组织，将目标锁定美国电话系统。这个组织成功入侵美国国家安全局（NSA）、AT&T 和美利坚银行，他们建立了一个可以绕过长途电话呼叫系统而侵入专线的系统。1995 年，来自俄罗斯的黑客范德米尔·列文（Vladimir Levin）在互联网上上演了精彩的“偷天换日”。他是历史上第一个通过入侵银行计算机系统来获利的黑客。他侵入美国花旗银行并盗走 1000 万美元。之后，他把账户里的钱转移至美国、芬兰、荷兰、德国、爱尔兰等地。1999 年，梅丽莎（Melissa）病毒是世界上首个具有全球破坏力的病毒。大卫·史密斯（David Smith）在编写此病毒的时候年仅 30 岁。梅丽莎病毒使世界上 300 多家公司的计算机系统崩溃。整个病毒造成的损失接近 4 亿美元。大卫·史密斯随后被判处 5 年徒刑。仅 15 岁的“黑手党男孩”（MafiaBoy，由于年龄太小，因此没有公布其真实身份）于 2000 年 2 月 6 日到 2 月 14 日情人节期间成功侵入包括 eBay、亚马逊（Amazon）和雅虎（Yahoo）在内的大型网站服务器，他成功地阻止了服务器向用户提供服务。2002 年 11 月，伦敦人加里·麦金农（Gary McKinnon）在英国被指控非法侵入美国军方 90 多个计算机系统。从 1999 年至 2002 年期间，中美黑客爆发了数次黑客大战，对双方都造成了重大损失。2007 年，“武汉男孩”李俊编写的“熊猫烧香”病毒肆虐网络，据保守估计，中国境内有百万余台计算机被感染。2009 年 5 月 18 日，域名解析服务器遭到攻击，造成中国多个省区的网络大瘫痪。

根据 Incapsula 报告，通过 14 个月的时间跟踪 DDoS 攻击的威胁，在 2013 年 2 月攻击的流量是每秒 4Gbps。2013 年 7 月，60Gbps 及其以上 DDoS 流量攻击基本上每周必发生一次。在 2014 年 2 月，Incapsula 报道一次 NTP 放大攻击最高流量达到 180Gbps。其他报告发

现的 NTP 放大攻击流量高达 400 Gbps。2013 年 6 月，前中情局（CIA）职员爱德华·斯诺登将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》，并告之媒体何时发表。按照设定的计划，2013 年 6 月 5 日，英国《卫报》先扔出了第一颗舆论炸弹：美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。6 月 6 日，美国《华盛顿邮报》披露称，过去 6 年间，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果、雅虎等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。2014 年 5 月 22 日，财务 500 强、著名在线拍卖网站 eBay 遭黑客入侵，大量用户数据可能被窃，这些数据包含用户的姓名、登录账号、密码、邮件地址、联系地址、电话号码以及出生日期。据 eBay 官方发布的消息称，黑客使用蠕虫的方式攻击，获得了少数 eBay 员工的登录凭据，并利用这些凭据进行了 APT 攻击，获得了 eBay 的用户数据，数据泄露发生在 2014 年 2 月月底至 3 月月初，不过，这一数据库并不包含任何财务信息和其他敏感的个人信息。2014 年 4 月，OpenSSL 爆出本年度最严重的安全漏洞，此漏洞在黑客社区中被命名为“心脏出血”漏洞。360 网站卫士安全团队对该漏洞分析发现，该漏洞不仅涉及以 https 开头的网址，还包含间接使用了 OpenSSL 代码的产品和服务，例如，VPN、邮件系统、FTP 工具等产品和服务，甚至可能会涉及其他安全设施的源代码。同时，对这个漏洞，安全专家 Robert David Graham 发布文章称，全球仍有 30 万台服务器存在 OpenSSL Heartbleed 漏洞（简称“滴血”漏洞）。Graham 称，“Whereas my previous scan a month ago found 600000 vulnerable systems, today's scan found roughly 300 000 thousand systems（318 239 to be precise）.”[在一个月前，我发现有 60 万个系统存在（滴血）漏洞，今天的扫描结果显示仍有约 30 万（准确数字是 318239）个系统存在该漏洞]。

信息安全重大事件不断发生，造成的影响和损失也越来越大，而且攻防双方之间的战争将不断持续下去，因此我们更应该关注信息安全问题，了解相关的知识。只有这样，我们才能够在信息海洋里畅游的同时，具备抗风防浪的本领。

1.3 信息安全的主要领域

目前互联网上各种严重的信息安全问题基本上都是由以下几个方面的问题引起的。

（1）个人计算机的安全结构过于简单。随着集成电路技术的飞速发展和计算机功能的不断丰富和拓展，计算机逐渐从科学研究的实验室步入了普通的家庭，从而产生了个人计算机。出于对成本的考虑以及对安全问题的严重性缺乏足够的警惕，个人计算机中缺乏足够的安全机制，如存储器的隔离保护机制、程序安全保护机制等。这样使得程序可以不经过认证就执行，程序可以被随意修改，数据区存储的数据也可以随意被修改或者删除，病毒、蠕虫、木马等恶意程序为所欲为。

（2）个人计算机又变成了公用计算机。随着技术的不断发展，个人计算机的功能不断丰富，使得个人计算机又变成了办公室、网吧甚至家庭多人使用的公用计算机。在公用环境下，缺乏安全机制的计算机成为了攻击的靶子。

（3）计算机通信网络把计算机连接到了因特网（Internet）。通过因特网，个人计算机就成为了巨大的网络中的一个节点。因特网使得用户可以通过个人计算机与全世界各个地方相连，同时也使得全世界各个地方的用户可以突破物理地域的限制，随意地访问这些计算机。这些缺乏安全保护措施的个人计算机自然而然成为网络黑客们的“肉鸡”。另外，现在的网

络通信协议本身并没有考虑安全问题，从而使得网络更成为了一个隐藏着巨大的鳄鱼的黑泥潭，任何一台连接在其上面的计算机都可能成为它的美食。

（4）操作系统存在缺陷。操作系统是计算机的主要软件。但是由于操作系统太复杂庞大（如 Windows 操作系统有上千万行的代码），这使得其往往难以保证全部安全，因此存在安全漏洞的可能性大大增加。这些安全漏洞很容易被黑客利用，成为黑客攻击的标靶。由 Windows 操作系统引发的安全事件屡见不鲜，微软公司不得不一次又一次地发布补丁来解决问题，然而这种补丁的方式只是“头痛医头、脚痛医脚”。尽管目前关于 Linux 操作系统的安全漏洞事件很少发生，但这并不意味着 Linux 操作系统是安全的，只是由于 Linux 操作系统目前普通用户用得比较少，从而黑客攻击的兴趣和目标没那么大而已。

从系统上说，信息安全主要包括以下几个方面的问题[1]。

（1）信息设备安全。即保障存储、传输、处理信息的设备的安全，如服务器、个人计算机、PDA、手机等。

（2）数据安全。即确保信息通信网络中传输的数据的安全。数据安全包括：机密性，即保证传输的数据不被非授权的人读取；完整性，即数据在传输过程中不被非法篡改等；认证性，保证数据来源于预定的提供者；不可否认性，保证数据的发送者和接收者无法否认自己的行为。

（3）内容安全。即保证信息通信网络中传输的内容不含有黄色、反动、盗版等非法的内容，对传输的数据进行监管。

（4）行为安全。行为安全是信息安全的终极目标，包含行为的秘密性、行为的完整性和行为的可控性。所谓行为的秘密性，是指行为不能危害数据的秘密性。所谓行为的完整性，是指行为不能危害数据的完整性，行为的过程和目标都是可预期的。所谓行为的可控性，是指当行为的过程出现偏离预期时，能够发现、控制并纠正。

从技术上讲，信息安全包含以下的技术。

（1）信息加密技术[2,3]。信息加密技术是最基本、最核心也是最重要的信息安全技术。所谓信息加密技术，是指双方约定一种方法对传输的信息进行变化，只有指定的接收者借助预先设定的关键信息才能够将信息还原，从而保证了信息的机密性。信息加密技术包括对称加密技术和非对称加密技术。在对称加密技术中，发送者和接收者双方共享一个相同的密钥。对称加密技术根据加密数据的长度分为分组加密（如 DES、AES、IDEA 等）和流加密（如 RC4、A5 等）。而非对称密码[4]中的密钥则是由两个不同部分组成的密钥对：一部分公开，称为公钥；一部分保密，称为私钥。因此非对称加密算法又称为公钥密码算法（如 RSA、ECC 等）。

（2）信息确认技术。信息确认技术通过严格限定信息的共享范围来达到防止信息被非法伪造、篡改和假冒的目的。一个安全的信息确认方案应该具有以下特点：① 合法的接收者能够验证他收到的消息是否真实；② 发信者无法抵赖自己发出的消息；③ 除合法发信者外，别人无法伪造消息；④ 发生争执时可由第三方仲裁。按照其具体目的不同，信息确认系统可分为消息确认、身份确认和数字签名。

（3）网络控制技术[4,5]。网络控制技术种类繁多且没有严密的理论，主要包括如下技术。

① 防火墙技术[6]。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不会泄露；后者将内部网络分隔成多个局域网，从而限制外部攻击造成的损失。

② 审计技术。它忠实地记录下信息系统中发生的各种事件，为后续的分析问题、解决问题提供翔实而可靠的资料。审计技术如同飞机上的黑匣子，它为信息系统异常的原因提供查询、定位，以及对网络攻击进行预测、报警，并为攻击发生后的实时处理提供详细可靠的依据或支持。

③ 访问控制技术[7]。访问控制技术确保只有拥有该权限的用户才能够对信息系统中的数据进行访问、修改、删除、复制等操作。访问控制采用最小特权原则：即在给用户分配权限时，根据每个用户的任务特点使其获得完成自身任务的最低权限，不给用户赋予其工作范围之外的任何权力。

④ 安全协议[8]。安全协议是网络安全的一个重要组成部分。它严格规定了一套交互式的操作来保证通信各方的安全属性，如身份认证、密钥协商、不可否认等。目前广泛采用的安全协议包括 IPsec/IKE、SSL、SSH、PGP 等。

1.4 信息安全与立法

由于信息安全的重要性和影响力，各国都从立法高度上来保证信息安全。美国先后制定了《信息自由法》、《个人隐私法》、《伪造访问设备和计算机欺骗滥用法》、《电子通信隐私法》、《计算机安全法》、《数字签名法》等多部与信息安全密切相关的法律，并将密钥长度超过 128 位的安全产品视为武器而禁止出口。欧共体也制定了一系列的法律以保障信息安全，包括：产品责任、商标和广告规定、知识产权保护、保护软件、数据和多媒体产品及在线版权、数据保护等，并规定当成员国内部法律与这些法律抵触时，以这些法律为准。1996 年 9 月 23 日，英国政府颁布了第一个网络监管行业性法规《三 R 安全规则》，对信息安全相关的法律问题做了严格规定。俄罗斯也于 1995 年颁布了《联邦信息、信息化和信息保护法》，其中明确界定了信息资源开放和保密的范畴，提出了保护信息的法律责任。

我国历来重视信息安全的立法问题。目前我国现行法律法规及规章中，与信息安全直接相关的是 65 部，它们涉及网络与信息系统安全、信息内容安全、信息安全系统与产品、保密及密码管理、计算机病毒与危害性程序防治、金融等特定领域的信息安全、信息安全犯罪制裁等。全面规范信息安全的法律法规有 18 部，包括 1994 年的《中华人民共和国计算机信息系统安全保护条例》等法规，也包括 2003 年的《广东省计算机信息系统安全保护管理规定》等地方法规。其中 2005 年 4 月 1 日起施行的《中华人民共和国电子签名法》更是在信息安全立法中占据了重要地位。这些法律法规中，侧重于互联网安全的有 7 部，包括 2000 年《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》等法律层面的文件，也包括 1997 年的《计算机信息网络国际联网安全保护管理办法》等部门规章；侧重于信息安全系统与产品的有 3 部，包括 1997 年的《计算机信息系统安全专用产品检测和销售许可证管理办法》等部门规章；侧重于保密的有 10 部，既包括 1989 年的《中华人民共和国保守国家秘密法》等法律，也包括 1998 年的《计算机信息系统保密管理暂行规定》等部门规章；侧重于密码管理及应用的有 5 部，包括 1999 年的《商用密码管理条例》等法规，也包括 2005 年

的《电子认证服务管理办法》等部门规章；侧重于计算机病毒与危害性程序防治的有 9 部，包括 2000 年的《计算机病毒防治管理办法》等部门规章，也包括 1994 年的《北京市计算机信息系统病毒预防和控制管理办法》等地方法规或规章；侧重于特定领域信息安全的有 9 部，包括 1998 年的《金融机构计算机信息安全保护工作暂行规定》等部门规章，也包括 2003 年的《广东省电子政务信息安全管理暂行办法》等地方法规或规章；侧重于信息安全监管的有 3 部，包括 2004 年的《上海市信息系统安全测评管理办法》等地方法规或规章；侧重于信息安全犯罪处罚的主要是我国刑法第 285 条、286 条、287 条等相关规定。

虽然我国与信息安全相关的法律法规为数不少，但仍然有很多问题亟待完善。首先，我国缺少一部像美国《联邦信息安全管理法》以及俄罗斯《联邦信息、信息化和信息保护法》那样确立信息安全的基本原则、基本制度及一些核心内容的基本大法。其次，绝大部分相关法律都篇幅偏小，行为规定极其简单。而且这些法律法规主要内容集中在对物理环境的要求、行政管理的要求等方面，对于涉及信息安全的行为规范一般规定得比较简单，在具体执行上指引性还不是很强；在处罚措施方面规定得也不够具体，导致在信息安全领域实施处罚时法律依据的不足；另外，在一些特定的信息化应用领域，如电子商务、电子政务、网上支付等，相应的信息安全规范相对欠缺，有待于进一步发展。同时，与信息安全相关的其他法律有待完善。这些都需要在以后的立法过程中不管完善和修正。

习 题 1

1．简述信息安全的含义。
2．目前互联网上各种严重的信息安全问题大致是由哪几个方面的问题引起的？
3．从系统上说，信息安全主要包括几个方面的问题？
4．数据安全的机密性、完整性、认证性、不可否认性分别指什么？
5．什么是行为安全？行为的秘密性、完整性、可控性分别指什么？
6．简述信息安全所包含的技术。
7．谈谈你对信息加密技术的认识。
8．网络控制技术主要包括哪几项技术？
9．防火墙可分为外部防火墙和内部防火墙，它们分别有什么作用？
10．讨论信息安全立法现状。

参 考 文 献

[1] 沈昌祥，张焕国，冯登国．信息安全综述．中国科学 E 辑，2007，37(2):129-150.

[2] 孟扬．网络信息加密技术分析．信息网络安全，2009(4):7-9.

[3] 黄志清．网络安全中的数据加密技术研究．计算机系统应用，2000(7).

[4] 冯登国．国内外密码学研究现状及发展趋势．通信学报，2002，23(5):18-26.

[5] 朱其新，胡寿松．网络控制系统的分析与建模．信息与控制，2003，32(1):5-8.

[6] 王正．网络安全中的防火墙技术探讨．通信技术，2008(8).

[7] 刘宏月，范九伦，马建峰．访问控制技术研究进展．小型微型计算机系统，2004，25(1).

[8] 卿斯汉．安全协议 20 年研究进展．软件学报，2003，14(10):1740-1752.