http://www.phei.com.cn

计算机安全防护技术研究

龙 珑 著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

计算机安全防护技术研究

龙 珑 著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书针对计算机安全防护方面的技术做了一般性介绍，重点介绍和分析了其中的加密技术、防火墙技术、访问控制技术、入侵检测技术、病毒防范技术五种关键技术，并阐述了融合技术是计算机安全防护技术的未来发展方向。本书内容覆盖了世界流行的计算机安全技术和当前的热点技术，并阐述了各种技术的技术原理、发展趋势、技术应用和产品等。

本书既适合高等院校、成人教育、高职高专院校的计算机网络技术、计算机应用、信息管理与信息系统等专业作为教材使用，也可供计算机网络技术自学者学习参考。

图书在版编目（CIP）数据

计算机安全防护技术研究 / 龙珑著. —北京：电子工业出版社，2005.11
ISBN 7-121-01919-1

Ⅰ. 计… Ⅱ. 龙… Ⅲ. 电子计算机－安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2005）第 129584 号

责任编辑：张燕虹　范劲松
审　　校：于秀山
印　　刷：北京市顺义兴华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：10.25　字数：235 千字
印　　次：2005 年 11 月第 1 次印刷
定　　价：16.80 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

在你的计算机连接上网络的时候，特别是连接上 Internet 时，你可以享受到如收发 E-mail，与朋友线上聊天，透过浏览器浏览 Internet，下载程序档案等的服务。但同时你的计算机也正暴露在计算机病毒以及木马程序的威胁中。此外，你也可能执行到隐藏在 E-mail 附件文件中的病毒，并且将病毒大量地传播给你的朋友及客户们。

计算机安全问题越来越引起世界各国的严密关注，随着计算机网络在人类生活各个领域的广泛应用，不断出现网络被非法入侵，重要资料被窃取，网络系统瘫痪等严重问题，网络、应用程序的安全漏洞越来越多；各种病毒泛滥成灾。这一切，已给各个国家以及众多商业公司造成巨大的经济损失，甚至危害到国家安全。

对计算机系统的安全防护过去主要依赖于发展网络防火墙、入侵检测、安全操作系统等技术。随着通信与计算机技术的迅猛发展，作为软件系统基础平台的计算机硬件系统的安全，已成为一个亟待解决的课题。计算机安全防护的新型技术，如用户身份识别和访问控制、系统硬件完整性检测、文件系统静态保护、动态数据实时备份与恢复等，这些技术的不断涌现和广泛的应用，将极大提高计算机系统的安全性、可靠性和抗毁性。

本书针对计算机安全防护方面的技术做了一般性介绍，然后重点介绍和分析了其中的加密技术、防火墙技术、访问控制技术、入侵检测技术、病毒防范技术这 5 种关键技术。

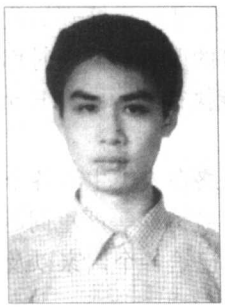
在编写过程中，我们以培养技术应用能力和职业素质教育为主线，采取与以理论教学为本位、为目标、为标准的普通高等教育不同的教学模式，建立真正以培养技术应用型人才为目标的教育教学模式，以能力为本位设计教材体系和教学内容，尽量避免理论内容过于追求系统性、完整性、严密性的现象，以及高新技术含量低的现象。力求思路清晰、结构合理、内容丰富、资料翔实，既反映和吸收本专业领域的最新进展，又融入我们自己的研究成果，使之具有较强的科学性、新颖性和实用性。

本系列教材既适合高等院校、成人教育、高职高专院校的计算机网络技术、计算机应用、信息管理与信息系统等专业作为教材使用，也可供计算机网络技术自学者学习参考。

限于认知和水准，书中可能存在疏漏和失当之处，敬请专家、学者及各位读者海涵、斧正。

龙　珑

作 者 介 绍



龙珑，汉族，1980 年 5 月出生于广西钦州市。1998 年 7 月于广西钦州市第二中学高中毕业，2002 年 7 月毕业于株洲工学院（现湖南工业大学），荣获工学学士学位，2002 年 9 月至 2005 年留学于英国赫德福得大学（University of Hertfordshire），荣获计算机科学硕士学位。2000 年至 2005 年期间，从事计算机科学与技术领域的技术研究、产品开发工作，主要研究方向有网络安全、人工智能、软件工程等。参与的项目“文件防弹衣”获 2004 年国家电子信息产业发展基金立项支持、2004 年广西科技厅立项支持、2003 年广西南宁市科技局立项支持、2004 年广西计算机推广应用成果一等奖、广西“优秀软件产品”等奖励。

目　录

第 1 章　计算机安全技术

21 世纪，全世界的计算机都通过 Internet 连到一起，随着 Internet 的发展，网络丰富的信息资源给用户带来了极大的方便，但同时也给上网用户带来了安全问题。由于 Internet 的开放性和超越组织、国界等特点，使它在安全性上存在一些隐患。而且，计算机安全的内涵也发生了根本的变化。它不仅从一般性的防卫变成了一种非常普通的防范，而且还从一种专门的领域变成了无处不在。

1.1　计算机安全简介

计算机安全涵盖的范围非常广泛，基本上包括了计算机设备、网络、软件、用户、组织、政府等各个层面上的问题。下面主要从其定义、内容、产品、状况和发展前景这几个方面来进行了解。

1.1.1　计算机安全的定义

国际标准化组织曾建议将计算机安全定义为："计算机系统受到保护，计算机系统的硬件、软件、数据不被偶然或故意地泄露、更改和破坏"。计算机系统安全可以分为实体安全、运行安全和信息安全 3 个方面。

（1）实体安全包括环境安全、设备安全和媒体安全 3 个方面。

（2）运行安全包括风险分析、审计跟踪、备份与恢复、应急处理 4 个方面。

（3）信息安全包括操作系统安全、数据库安全、计算机安全、病毒防护、访问控制、加密和鉴别 7 个方面。

计算机安全是指系统的硬件、软件及其系统中的数据受到保护，不被偶然或者恶意地破坏、更改、泄露，系统连续可靠地正常运行，网络服务不中断。对于一般用户而言，计算机安全是指保证其在网络上的私人信息或商业信息内容的安全保密性和完整性；对于网络运行和管理者而言，计算机安全的侧重点为信息处理和传输系统的安全性、网络信息的可用性和可控性；对于安全保密部门而言，则注重的是信息的机密性和可控性；而从社会、道德和教育的角度来说，对网络信息内容的可控性，是目前要解决的主要问题。计算机安全根据其本质的界定，应具有以下的基本特征。

（1）保密性：是指信息不泄露给非授权的个人、实体和过程，或供其使用的特性。

（2）完整性：是指信息未经授权不能被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对网络信息安全进行攻击的最终目的就是破坏信息的完整性。

（3）可用性：是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息及相关资产。

（4）可控性：是指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及方式。

（5）可审查性：在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

1.1.2 计算机安全的主要研究内容

一切影响计算机信息系统资源和信息资源的安全性问题，都是计算机安全应考虑的问题。它所研究的主要内容不仅涉及信息的安全性，更涉及系统的安全性，包括软件系统、硬件系统、网络系统及运行环境等诸多方面。

（1）实体安全性研究。是指为了确保计算机网络设备、设施及其他媒体免遭地震、水灾、火灾等环境事故，人为操作失误或错误，以及各种计算机犯罪行为破坏而进行的研究，是网络信息安全的最基本保障，是整个安全系统不可缺少和忽视的组成部分。它的研究内容主要包括3个方面：环境安全、设备安全、媒体安全。

（2）软件系统安全性研究。包括针对所有计算机程序和文档资料免受破坏和非法拷贝的技术研究，制定并掌握产品的安全质量标准，为开发使用的软件产品建立严格的开发、控制、质量保障机制，确保软件满足安全保密技术标准的要求，确保软件系统的正常运转。

（3）运行安全性研究。包括为保障系统功能的安全实现所应提供的安全措施，包括风险分析、审计跟踪、备份与恢复和应急技术等的研究。

（4）数据信息安全性研究。包括信息传输安全（动态安全）、数据加密、数据完整性鉴别和防抵赖技术的研究。

（5）网络防护和反病毒技术的研究。各种计算机安全防护技术和反病毒技术的研究是针对各种计算机网络系统所面临的威胁和自身的脆弱性而展开的，它包括安全服务、安全机制和配置方法、安全策略的研究及计算机安全设计的基本原则的制定等，还包括病毒的检测、诊断、清除等技术的研究和产品的开发。

1.1.3　主要计算机安全产品介绍

（1）扫毒 / 侦毒产品。扫毒软件可针对系统中的程序文件、文档文件、软件组件等进行侦测，或持续监视系统是否有异常情况，以避免系统遭受病毒的侵扰。

（2）访问控制类产品。通过对计算机的所有资源进行访问控制，并禁止非授权用户对资源对象进行访问，确保资源保密、访问安全。

（3）入侵检测系统。入侵检测系统监听网络上的特定包，检查系统是否遭到攻击。若发现异常情况，能够通知管理人员，同时对受攻击系统进行控制和管理，避免对其他系统造成损害。

（4）防火墙。防火墙是目前最基本的网络防护设备。它可以针对网络信息的来源及目的地进行过滤，避免网络灾情的蔓延，一方面减少来自外界的攻击机会，另一方面阻挡内部异常传到外部。

（5）VPN——虚拟专用网。在跨越不安全网段时，VPN 提供各个私有网段之间传输的安全性。私有网段可以是公司内部网络 Intranet，也可以是合作厂商网络 Extranet、出差在外的公司员工使用的笔记本电脑或跨国公司在海外的网络等。VPN 可保证在 VPN 设备间传输信息的完整性及私密性，使 Internet 或其他公用网络上的通信达到相当高的安全性。

（6）PKI——公钥相关软件及服务。达到高度计算机安全要求的另一个因素就是身份鉴别和授权。目前，普遍采用的是公钥基础建设 PKI，用户可取得公钥凭证，获取难以伪造的身份和难以破解的私密性。

（7）除上述计算机安全产品之外，还有许多其他的产品或服务，如咨询服务、提供安全模块、安全的存储或备援服务、实体保全产品、安全漏洞通报整合服务等。

1.1.4　计算机安全的状况

2004 年，公安部公共信息计算机安全监察局与中国计算机学会计算机安全专业委员会共同举办了全国首次信息计算机安全状况调查活动。此次调查共对 7072 家分布在政府、金融证券、教育科研、电信、广电、能源交通、国防和商贸企业等重要信息网络、信息系统使用单位的安全管理情况进行了调查。调查结果表明，大多数被调查单位的信息网络规模比较小，其中计算机数量在 50 台以下的占 50%以上，在 500 台以上的具有一定规模的只占调查总数的 10%。从信息网络的用途看，主要集中在办公应用方面，比例为 77%；其次是用于业务经营、互联网上网和网上信息服务，比例分别为 30%。其中，被调查单位信息网络接入互联网占 56%，建立专网和内部局域网的分别占 26%和 18%。

被调查单位信息网络使用的操作系统主要是 Windows 操作系统，其中 Windows 9x 和 Windows Me 占 35%，Windows NT 和 Windows 2000 占 37%，Windows XP 占 28%。此外，

UNIX 和 Linux 操作系统分别占 22%和 10%。调查的结果和数据如下：

（1）在 7072 家被调查单位中有 4057 家单位发生过信息计算机安全事件，占被调查总数的 58%。其中，发生过 1 次的占总数的 22%，2 次的占 13%，3 次以上的占 23%，此外，有 7%的调查对象不清楚是否发生过计算机安全事件。从发生安全事件的类型分析，遭受计算机病毒、蠕虫和木马程序破坏的情况最为突出，占安全事件总数的 79%；其次是垃圾邮件，占 36%；拒绝服务、端口扫描和篡改网页等网络攻击情况也比较突出，共占到总数的 43%。

（2）从计算机安全事件的发现途径分析，以人工监测和技术手段发现为主，其中由网络（系统）管理员通过技术监测发现的占 63%，通过安全产品报警发现的占 45%，通过事后分析发现的占 27%，有关部门通知后发现的占 15%。

（3）从计算机安全事件造成的破坏和损失看，有 54%的被调查单位认为计算机安全事件造成的损失轻微或比较轻微，认为损失严重和非常严重的只占 10%。

（4）从网络攻击来源分析，造成信息计算机安全事件的主要网络攻击来自外部，占安全事件总数的 46%，来自内部的占 7%，来自内外部的占 24%。

（5）调查结果表明，造成计算机安全事件发生的主要原因是安全管理制度不落实和安全防范意识薄弱。其中，由于未修补或防范软件漏洞导致发生安全事件的占安全事件总数的 66%，登录密码过于简单或未修改密码导致发生安全事件的占 19%。

（6）按照行业对安全事件进行分析，金融证券行业发生计算机安全事件的比例相对较低，为 44%；在发生 3 次以上安全事件的单位中，教育科研和互联网服务行业最多，分别为 33%和 31%。安全事件分析如表 1.1 所示。

表 1.1　安全事件分析

被调查的行业或单位	无	1 次	2 次	3 次以上	有，但次数不详
政府（1541 家）	40%	22%	14%	18%	5%
金融证券（1017 家）	56%	18%	10%	12%	4%
教育科研（976 家）	26%	23%	13%	33%	6%
电信（503 家）	33%	23%	13%	25%	6%
互联网和信息技术（934 家）	29%	23%	17%	26%	5%
广电和新闻（106 家）	29%	24%	16%	24%	8%
制造（386 家）	27%	21%	13%	31%	8%
商业贸易（211 家）	25%	19%	15%	27%	13%
能源水利（185 家）	26%	28%	12%	25%	8%
交通运输（96 家）	26%	30%	17%	21%	6%
医疗卫生等社会公共服务（157 家）	41%	22%	10%	18%	10%
其他（938 家）	32%	19%	11%	23%	14%
注：总数不为 100%，是因为某些问卷未得到回复					

调查表明，近年来，使用单位对信息计算机安全管理工作的重视程度普遍提高，80%的被调查单位有专职或兼职的安全管理人员，12%的单位建立了安全组织，2%的单位请信息安全服务企业提供专业化的安全服务。调查还表明，认为单位的信息计算机安全防护能力“较高”和“一般”的比较多，分别占44%。但是，被调查单位普遍反映用户安全观念薄弱，安全管理人员缺乏培训，安全经费投入不足和安全产品不能满足要求等问题，也说明目前安全管理水平和社会化服务的程度还比较低。

1.1.5 计算机安全的发展趋势

从上节的数据中可以看出，全球企业和政府在未来将遇到计算机安全的严峻挑战，因为它们将更加依赖整合网络与合作伙伴、客户联系，其员工将更多地使用移动技术办公，此外，他们需面对网络恐怖分子和网络罪犯对企业和政府的破坏活动。2005年或未来计算机安全领域将面临下列挑战和发展趋势。

1）应用软件漏洞将导致《产品缺陷法（Lemon laws）》出台

浏览器和操作系统的供应商经常由于企业安全漏洞成为被批评的焦点。应用和相关软件也同样容易遭受攻击，但很多时候都被忽略了。随着应用程序更加接近互联网的边缘，某些厂商的应用或数据库产品遭受攻击而导致客户损失，客户因而对软件供应商提出法律起诉，这种事件的爆发将只是时间的问题。基于《产品缺陷法》而对应用软件安全漏洞提出法律诉讼的个案将涌现，这将显著改变应用软件提供商和购买者之间的经济地位。

2）业务伙伴和其他方的可靠网络将成为风险来源

由于企业通过公司网络与业务伙伴、供应商和客户进行的业务交往日益频繁，企业IT基础架构和重要业务信息遭受破坏的可能性也随之增加。由于企业预计大多数网络攻击来自内部人员和外部黑客，很少对来自合作伙伴或客户人员的攻击予以防备，然而此等人士进行恶意行动的意图可能和内部员工相仿。

企业必须将安全重点从简单的信息安全演进成更有计划的、面向流程的方法，以保护基础架构和核准的用户，包括合作伙伴达成的全面策略、代理防火墙的技术保护以及联合身份管理等。总而言之，使用可靠网络的电子商务方针必须从“相信我”迅速演进为“检验它”。

3）移动领域将成为滋生安全事件的黑点

随着第三代网络、手机和PDA等移动环境和设备的日益智能化，它们对业务变得不可或缺，企业IT基础架构的边界已经超出了目前安全基础架构能够覆盖的范围。广泛使用的蓝牙和其他公共移动环境的保护技术尚显稚嫩，并且难以使用，从而为无线数据盗窃提供了可乘之机。

解决上述挑战的方法就是采取集中及谨慎的投资战略。企业必须从商业而不是技术

角度来看待移动安全。他们需要实事求是地分析目前和未来威胁的可能影响，然后，他们还必须进行业务决策，决定资金和资源的投入程度，以降低下一代移动安全威胁带来的风险。

4）网络攻击方式将更加凌厉

一些攻击者会企图制造一些带来长期影响、而非一次性的攻击，这些行为可能纯粹出于恶意，但大多数背后都怀有经济动机。我们预计未来会出现第一种具有真正危险效果的蠕虫或病毒，能够改变或破坏记录层的信息，由此产生的影响将无法通过简单手段来挽救，例如从先前备份的数据版本恢复。企业将花费大量时间和资金来寻找和替代被改动的内容。最糟糕的是这些恶意攻击将破坏受害者的运营和业务诚信，这对电子商务来说是十分严重的冲击。

5）互联网暴徒的有组织攻击将会增加

新的网络犯罪组织不断涌现，它们与其前辈不同，经常纯粹为经济动机而犯罪，而且不计后果，热衷于发动更具破坏力的攻击。迄今为止，网络勒索者通常为经济目的敲诈个人或单位，并不断地制造破坏，例如清除计算机硬盘上的内容或破坏数据指针等。如果威胁没有得逞，他们将使用多种攻击手段，从有目标的拒绝服务攻击到破坏记录层信息，真正造成严重破坏。

6）由于需要进一步保护业务的安全，企业将转向主动式的“深入防御”策略

企业管理层将更加意识到多层端到端解决方案的价值，以及实施它们的必要性。这种解决方案能够满足各种要求，从威胁和漏洞分析，到多种技术和可管理安全服务策略的开发和实施。他们通常会发现，将这些解决方案的设计、实施和管理外包给专业合作伙伴，是实现优化风险管理和投资回报的高效方式。

7）信用报告机构将更多地参与管理身份盗窃的后果

许多身份偷窃都涉及信用卡账户信息，罪犯可以使用这些信息，来尝试访问其他系统，例如银行和经纪账户，以偷窃更多的信息或访问其他资源。报告机构需要帮助设计用户身份验证方法，从而防止身份窃贼使用偷窃的身份信息来访问其他来源的信息。如果信用报告机构不通过消费者教育和其他主动措施来更多地参与其中，政府将会介入，开始为他们解决这个问题。

8）加快采用联合体系结构，进行身份和访问管理

通过联合身份管理，参与的企业能够共享彼此的验证和授权服务。同样，企业要与外部合作伙伴、提供商或公司内部业务部门之间安全地共享信息，协作也是至关重要的。用户在未来将采用合作方式，以解决来自可靠网络日益增多的威胁。Unisys 公司在 2004 年 10 月进行的一次研究调查表明，37%的被调查者表示他们将在明年内实施协作方针。由于

行业采用了OASIS安全宣示标记语言2（SAML 2）标准的最新版本，这种新兴技术的采用率可能会进一步提高。

9）企业将重新采用RBAC进行身份和访问管理

RBAC（基于角色的访问权限控制）是根据用户的职能而非个人身份来授予访问权限的。通过采用RBAC，更改访问权限使用者的工作将大幅度简化。由于要界定企业每个角色颇为困难和花费不菲，RBAC的采用率过去不高，直到最近才逐渐提升。例如，一家使用多个系统、拥有40 000员工的企业用了12个月的时间才能界定不同角色。然而，只为这40 000名员工定义2 500个角色，就可以极大地降低设置和管理的工作量。更新的技术将使RBAC的优点更加迅速地实现，尤其是在提高工作效率和减低成本方面。Unisys公司在2004年10月进行的研究调查表明，RBAC的采用率正在提高。32%的接受调查者表示他们可能在2005年实施RBAC。

10）虚拟目录技术将成为身份集成项目的重要组成部分

虚拟目录技术提供了一种可从多个系统查看和整合身份信息的途径，而无需实际合并数据库。随着虚拟目录技术的成熟，虚拟目录解决方案也得以实现，这种解决方案对整合新系统和传统系统来说十分重要。例如，在一个整合的司法系统中，处于不同管辖权限范围、使用不同计算机系统的地方检察官办公室、警察局和司法部，在经过授权后都可以虚拟查看一名已知罪犯的全面信息。

新的虚拟目录技术正在消除实际移动和整合数据的必要性。通过这种做法，它们解决了相关的数据所有权问题，加快了身份整合时间并降低了成本。企业用户将充分了解虚拟目录的这些优点，并在其安全战略中采用虚拟目录。

在2005年及更长远的未来，我们会看到安全挑战将对业务造成重大影响，这将涵盖法律、经济及技术等方面。企业将面临前所未有的挑战，它们必须在安全方面进行集中的、战略性及全面的投资。对于任何寻求实现“可信企业”目标的企业而言，这些投资都是必要的，风险管理必须成为业务战略的不可缺少部分，建立安全的环境，实现与合作伙伴和客户的最佳协作，并推动业务发展。

从总体趋势上看，计算机安全涉及计算机系统的多个层次和多个方面，同时，它也是动态变化的过程。因此，计算机安全实际上是一项系统工程。它既涉及对外部攻击的有效防范，又包括制定完善的内部安全保障制度；既涉及防病毒攻击，又涵盖实时检测、防黑客攻击等内容。因此，计算机安全解决方案不应仅仅提供对于某种安全隐患的防范能力，而是应涵盖对于各种可能造成计算机安全问题隐患的整体防范能力；同时，它还应该是一种动态的解决方案，能够随着计算机安全需求的增加而不断改进和完善。

因此，整合立体防护的计算机安全系统是未来安全的必由之路，而立体防护系统是由各种安全防护技术有机组合而成的。下面将介绍各种主流的安全防护技术。

1.2 计算机安全防护技术概况

计算机系统遭受的攻击主要来自三种人：黑客、恶意的内部人员、商业间谍。

（1）黑客攻击网络的手段可分为非破坏性攻击和破坏性攻击两大类。非破坏性攻击一般是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹一类的特殊工具软件，在短时间内向目标服务器发送大量超出系统负荷的信息，消耗可用系统、带宽资源，最后致使网络服务瘫痪。破坏性攻击则采用穷举搜索法发现后门程序，并利用其侵入他人计算机系统，盗窃系统保密信息，破坏系统数据，或者采用网络监听的方法截获网上传输的信息。

（2）来自“内部”的威胁越来越受到人们的注意。内部人员（Insider）可以是授权用户、CERT 人员、网络管理员、系统维护人员、系统管理员、建筑物维修人员、信息安全官员或建筑物安全人员等。内部人员犯罪具有“危害大、难抵御、难发现”的特点，他们最容易接触核心数据资源，威胁的针对性强，而且防不胜防。同时，他们对要攻击的目标非常熟悉，使攻击性行为具有隐蔽性，很难被发现。

（3）商业间谍的攻击是具有明确动机的，即通过窃取竞争对手的商业机密而获得竞争优势。

因此，如果能最大程度地预防此类攻击或恶意访问，事实上就会把计算机系统的安全提升到一个很高的级别。由此可见，计算机防护技术在计算机安全问题中的重要地位。从技术层面而言，计算机系统受到安全威胁主要来自以下几个方面：

（1）系统本身的脆弱性。软件不可能百分之百无缺陷和无漏洞，而这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件，大部分都是因为网络软件有漏洞，安全措施不完善。另外，软件的“后门”是软件公司的编程人员为自己方便而设置的，一般不为外人所知，但一旦“后门”洞开，造成的后果将不堪设想。

（2）数据库管理系统的脆弱性。大量信息存储在各种类型的数据库系统中，数据库系统的安全性是否与操作系统的安全性匹配是应引起重视的问题。

（3）信息泄露或丢失。是指敏感数据在有意或无意中被泄露出去或丢失，通常包括：信息在传输中丢失或泄露（如“黑客”利用电磁泄露或搭线窃听等方式截获机密信息，或者通过对信息流向、流量、通信频度和长度等参数的分析，推测出有用信息，如用户口令、账号等重要信息），以及信息在存储介质中丢失或泄露等。

（4）数据完整性被破坏。以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。