信息系统
安全与对抗技术

xinxi xitong
anquan yu
duikang jishu

编著／罗森林

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

信息系统安全与对抗技术

罗森林　编著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书根据信息对抗技术专业的特点和培养高素质专业人才的需要而编写。全书共分七章:绪论;信息系统安全概述;信息系统安全检测与攻击技术;信息系统防御与对抗技术;信息安全犯罪与立法;信息系统安全标准与安全评估;信息系统安全工程。本书可作为信息安全、信息对抗技术及相关专业的课程教材,也可作为专业技术人员的参考用书。

图书在版编目(CIP)数据

信息系统安全与对抗技术/罗森林编著 .—北京:北京理工大学出版社,2005.8

ISBN 7-5640-0549-1

Ⅰ.信… Ⅱ.罗… Ⅲ.信息系统-安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2005)第 062093 号

出版发行 / 北京理工大学出版社
社　　址 / 北京市海淀区中关村南大街 5 号
邮　　编 / 100081
电　　话 / (010)68914775(办公室)　68944990(发行部)
网　　址 / http://www.bitpress.com.cn
电子邮箱 / chiefedit@bitpress.com.cn
经　　销 / 全国各地新华书店
印　　刷 / 北京圣瑞伦印刷厂
开　　本 / 787 毫米 × 1092 毫米　1/16
印　　张 / 25.25
字　　数 / 601 千字
版　　次 / 2005 年 8 月第 1 版　2005 年 8 月第 1 次印刷
印　　数 / 1~4000 册　　责任校对 / 张　宏
定　　价 / 38.00 元　　责任印制 / 吴皓云

前　言

信息系统安全与对抗技术，是根据信息对抗技术专业的特点和培养高素质专业人才的需要编写的，是信息对抗技术专业不可或缺且极为重要的内容之一。本书具有以下特点：

1. 系统性强、层次分明。尽量覆盖有关信息、信息系统安全与对抗全方位的内容，注重其精要，但不能面面俱到。先从系统层次探讨信息系统的安全性，涉及信息、信息系统、工程系统理论，以及信息系统安全发展历程、不安全因素、安全需求、安全体系框架和安全组织管理；而后是信息系统的攻击与检测技术，包括网络攻击的基本概念、黑客、漏洞扫描、网络监听、计算机病毒、欺骗攻击、缓冲区溢出攻击等；其次是信息系统的防御和对抗技术，包括针对攻击的一般处理原则、密码技术、防火墙、访问控制、身份认证、信息隐藏技术、虚拟专用网技术以及实体安全技术等，最后论述信息安全犯罪、立法，信息安全标准与评估，以及信息安全工程。

2. 注重时空维动态发展。不仅注重基础性理论与技术，更注重信息安全与对抗的时间过程和空间的范围，概述中介绍了“5432”国家信息安全战略构想和我国信息安全保障体系建设的内容；攻击与对抗技术中讨论了一般攻击和对抗的过程，并构建了信息攻击与对抗的“共道－逆道”模型，该模型具有广泛的指导意义。同时，书中涉及了多项正在研究的技术，如自动响应技术。

3. 与相关教材配套。本书与《信息系统与安全对抗理论》、《信息系统安全与对抗技术实验教程》形成从理论到实践、“由顶层至底层”的互为延伸和贯通的信息对抗技术专业人才培养的系统性配套教材。《信息系统与安全对抗理论》中论述了信息系统安全对抗问题产生的主要根源，安全对抗过程的要点，信息安全对抗的基础层和系统层的基本原理，“共道－逆道”博弈模型，以及信息安全与对抗的原理性和技术性方法。《信息系统安全与对抗技术实验教程》中，面向本科生和研究生设计了七大类系列实验，涉及信息系统模型平台基础实验，典型信息系统及其信息采集、传输、处理、交换、存储、管理与控制实验，信息系统病毒实验，信息系统安全物理隔离集技术实验，信息隐藏技术实验，信息系统攻防技术实验，无线信息系统安全与对抗技术实验等。

在本书的编写过程中，得到了中国科学院、中国工程院两院院士王越教授、教务处闫达远教授、高平高级实验师及许多领导、同事以及硕士研究生冯磊等同学的多方面帮助，在此一并表示衷心的感谢。同时，感谢北京理工大学教务处及出版社对本书的出版给予的大力支持。

由于时间所限，加之笔者能力范围的限制，对于书中的不足和错误之处敬请广大师生批评指正，以便使其日渐完善。

作　者

2005年于北京理工大学

目　录

第1章 绪 论

1.1 引 言

信息是人类社会的宝贵资源，功能强大的信息系统是推动社会发展前进的催化剂和倍增器。信息系统越发展到它的高级阶段，人们对其依赖性就越强。本章主要介绍信息系统相关基础知识，包括信息、信息技术和信息系统的概念以及信息系统的组成要素分析，并在此基础上论述工程系统理论的分析、设计、评价的基本观点。

1.2 信息、信息技术、信息系统

1.2.1 信息

“信息”一词古已有之。在人类社会早期的日常生活中，人们对信息的认识比较广义而模糊，对信息和消息的含义没有明确界定。到了20世纪尤其是中期以后，随着现代信息技术的飞速发展及其对人类社会的深刻影响，迫使人们开始探讨信息的准确含义。

1928年，哈特雷（L.V.R.Hartley）在《贝尔系统电话》杂志上发表了题为《信息传输》的论文。他在文中将信息理解为选择通信符号的方式，并用选择的自由度来计量这种信息的大小。他注意到，任何通信系统的发送端总有一个字母表（或符号表），发信者发出信息的过程正是按照某种方式从这个符号表中选出一个特定符号序列的过程。假定这个符号表一共有 S 个不同的符号，发信者选定的符号序列一共包含 N 个符号，那么，这个符号表中无疑有 S^N 种不同符号的选择方式，也可以形成 S 个长度为 N 的不同序列。这样，就可以把发信者产生信息的过程看做是从 S 个不同的序列中选定一个特定序列的过程，或者说是排除其他序列的过程。然而，用选择的自由度来定义信息存在局限性，主要表现在这样定义的信息没有涉及信息的内容和价值，也未考虑到信息的统计性质；另一方面，将信息理解为选择的方式，就必须有一个选择的主体作为限制条件，因此这样的信息只是一种认识论意义上的信息。

1948年，香农（C.E.Shannon）在《通信的数学理论》一文中，在信息的认识方面取得重大突破，堪称信息论的创始人。香农的贡献主要表现在推导出了信息测度的数学公式，发明了编码的三大定理，为现代通信技术的发展奠定了理论基础。香农发现，通信系统所处理的信息在本质上都是随机的，因此可以运用统计方法进行处理。他指出，一个实际的消息是从可能消息的集合中选择出来的，而选择消息的发信者又是任意的，因此，这种选择就具有随机性，是一种大量重复发生的统计现象。香农对信息的定义同样具有局限性，主要表现在这一概念未能包容信息的内容与价值，只考虑了随机不定性，未能从根本上回答信息是什么的问题。

1948年，就在香农创建信息论的同时，维纳（N.Wiener）出版了专著《控制论——动物和机器中的通信与控制问题》，并创立了控制论。后来，人们常常将信息论、控制论以及系统论合称为“三论”，或统称为“系统科学”或“信息科学”。维纳从控制论的角度认为，“信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容的名称。”他还认为，“接受信息和使用信息的过程，就是我们适应外部世界环境的偶然性变化的过程，也是人们在这个环境中有效地生活的过程。”维纳的信息定义包容了信息的内容与价值，从动态的角度揭示了信息的功能与范围。但是，人们在与外部世界的相互作用过程中同时也存在着物质与能量的交换，不加区别地将信息与物质、能量混同起来是不确切的，因而也是有局限性的。

1975年，意大利学者朗高（G.Longo）在《信息论：新的趋势与未决问题》一书的序中指出，信息是反映事物的形成、关系和差别的东西，它包含在事物的差异之中，而不在事物本身。无疑，“有差异就是信息”的观点是正确的，但“没有差异就没有信息”的说法却不够确切。譬如，我们碰到两个长得一模一样的人，他（她）们之间没有什么差异，但人们会马上联想到“双胞胎”这样的信息。可见，“信息就是差异”也有其局限性。

1988年，中国学者钟义信在《信息科学原理》一书中，认为信息是事物运动的状态与方式，是事物的一种属性。信息不同于消息，消息只是信息的外壳，信息则是消息的内核。信息不同于信号，信号是信息的载体，信息则是信号所载的内容。信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。信息不同于情报，情报通常是指秘密的、专门的、新颖的一类信息，可以说所有的情报都是信息，但不能说所有的信息都是情报。信息也不同于知识，知识是认识主体所表达的信息，是序化的信息，而并非所有的信息都是知识。他还通过引入约束条件推导了信息的概念体系，对信息进行了完整而准确的论述。通过比较，中国科学院文献情报中心孟广均研究员等在《信息资源管理导论》一书中认为，作为与物质、能量同一层次的信息的定义，信息就是事物运动的状态与方式。因为这个定义具有最大的普遍性，不仅能涵盖所有其他的信息定义，而且通过引入约束条件还能转换为所有其他的信息定义。

2002年，中国科学院、中国工程院两院院士王越教授指出，事实上，定量广义全面地描述“信息”是不太可能的，至少是非常难的事，对“信息”本质的深入理解和科学定量描述有待持续长期进行，在此暂时给出一个定性概括性定义：“信息是客观事物运动状态的表征和描述”，其中“表征”是客观存在的，而描述是人为的。“信息”的重要意义在于它可表征一种“客观存在”，与人类认识实践结合，进而与人类生存发展相结合，所以信息领域科技的发展体现了客观与人类主观相结合的一个重要方面。对人而言，“获得信息”最基本的机理是映射（借助数学语言），即由客观存在的事物运动状态，经人的感知功能及脑的认识功能进行概括抽象形成“认识”，这就是“获得信息”、“加工信息”的过程，是一个由“客观存在”到人类主观认识的“映射”。由于客观事物运动是在非常复杂的广义空间（不限于三维）和时间维的动态展开，因此它的“表征”也必定是非常复杂的，体现、存在于广义空间维在复杂的多层次、多剖面相互“关系”及在多阶段、多时段的时间维的交织动态展开，进而指出“信息”必定是由反映各层次、各剖面不同时段动态特征的信息片段组成，这是“信息”内部结构最基本的内涵。

据不完全统计，信息的定义有100多种，它们都从不同侧面、不同层次揭示了信息的特

征与性质，但也都有这样或那样的局限性。信息来源于物质，但不是物质本身；信息也来源于精神世界，但又不限于精神的领域；信息归根到底是物质的普遍属性，是物质运动的状态与方式。信息的物质性决定了它的一般属性，主要包括普遍性、客观性、无限性、相对性、抽象性、依附性、动态性、异步性、共享性、可传递性、可变换性、可转化性和可伪性等。信息系统安全将处理与信息依附性、动态性、异步性、共享性、可传递性、可变换性、可转化性和可伪性有关的问题。

1.2.2 信息技术

任何技术都产生于人类社会实践活动的实际需要。按照辩证唯物主义观点，人类的一切活动都可以归结为认识世界和改造世界。而人类认识世界和改造世界的过程，从信息的观点来分析，就是一个不断从外部世界的客体中获取信息，并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出，最终把大脑中产生的决策信息反作用于外部世界的过程。

“科学”是扩展人类各种器官功能的原理和规律，而“技术”则是扩展人类各种器官功能的具体方法和手段。从历史上看，人类在很长一段时间里，为了维持生存而一直采用优先发展自身体力功能的战略，因此，材料科学与技术和能源科学与技术也相继发展起来。与此同时，人类的体力功能也日益加强。信息虽然重要，但在生产力和生产社会化程度不高的时候，人们仅凭自身的天赋信息器官的能力，就足以满足当时认识世界和改造世界的需要了。但随着生产斗争和科学实验活动的深度和广度的不断发展，人类信息器官的功能已明显滞后于行为器官的功能了，例如人类要“上天”、“入地”、“下海”、“探微”，但其视力、听力、大脑存储信息的容量、处理信息的速度和精度，已越来越不能满足同自然作斗争的实际需要了。只是到了这个时候，人类才把自己关注的焦点转到扩展和延长自己信息器官的功能方面。

经过长时间的发展，人类在信息的获取、传输、存储、处理和检索等方面的方法与手段，以及利用信息进行决策、控制、指挥、组织和协调等方面的原理与方法，都取得了突破性的进展，当代技术发展的主流已经转向信息科学技术。

对于信息技术，目前还没有一个准确而又通用的定义。为了研究和使用的方便，学术界、管理部门和产业界等都根据各自的需要与理解给出了自己的定义，估计有数十种之多。信息技术定义的多样化，不只是反映在语言、文字和表述方法上的差异，而且也有对信息技术本质属性理解方面的差异。

目前比较有代表性的信息技术的定义主要有以下几种：

(1) 信息技术是基于电子学的计算机技术和电信技术的结合而形成的对声音的、图像的、文字的、数字的和各种传感信号的信息，进行获取、加工处理、存储、传播和使用的能动技术。

(2) 信息技术是指在计算机和通信技术支持下用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频和声频以及语音信息，并包括提供设备和提供信息服务两大方面的方法与设备的总称。

(3) 信息技术是人类在生产斗争和科学实验中认识自然和改造自然过程中所积累起来的获取信息、传递信息、存储信息、处理信息以及使信息标准化的经验、知识、技能，以及体

现这些经验、知识、技能的劳动资料有目的的结合过程。

(4) 信息技术是在信息加工和处理过程中使用的科学、技术与工艺原理和管理技巧及其应用；与此相关的社会、经济与文化问题。

(5) 信息技术是管理、开发和利用信息资源的有关方法、手段与操作程序的总称。

(6) 信息技术是能够延长或扩展人的信息能力的手段和方法。

1.2.3 信息系统

自20世纪初泰罗创立科学管理理论以后，管理科学与方法技术得到迅速发展，在它同统计理论和方法、计算机技术、通信技术等相互渗透、相互促进的发展过程中，信息系统作为一个专门领域迅速形成和发展。同“信息”、“系统”的定义具有多样性一样，信息系统这种与“信息”有关的“系统”，其定义也远未达成共识。比较流行的定义有：

《大英百科全书》把“信息系统”解释为：有目的、和谐地处理信息的主要工具是信息系统，它对所有形态（原始数据、已分析的数据、知识和专家经验）和所有形式（文字、视频和声音）的信息进行收集、组织、存储、处理和显示。

M. 巴克兰德（M.Buckland）认为信息系统是“提供信息服务，使人们获取信息的系统，如管理信息服务、联机数据库、记录管理、档案馆、图书馆、博物馆等”。

N.M. 达菲（N.M.Dafe）等认为信息系统大体上是“人员、过程、数据的集合，有时候也包括硬件和软件，它收集、处理、存储和传递在业务层次上的事务处理数据和支持管理决策的信息”。

中国学者吴民伟认为信息系统是“一个能为其所在组织提供信息，以支持该组织经营、管理、制定决策的集成的人－机系统，信息系统要利用计算机硬件、软件、人工处理、分析、计划、控制和决策模型，以及数据库和通信技术”。

中国科学院、中国工程院院士王越教授给出的信息系统的定义是：“帮助人们获得信息、传输信息、处理信息和利用信息的系统称为信息系统，是以‘信息’服务于人的一种工具。”“服务”一词有着越来越广泛的含义，因此信息系统是一类各种不同功能和特征信息系统之总称。任何信息系统都是由下列部分交织或选择交织而组成。

信息的获取部分（各种传感器等包括在内）。任何一种信息系统其内部都要利用一种或多种媒体荷载信息进行运行，以达到发挥系统作为工具的功能，故首先应通过某种媒体获取“信息”并根据需要将其记录下来，这是信息系统的重要基本功能部分。应该注意到的是，人类不断地依靠科学和技术改进信息获取部分之性能和创造新类型的信息，获取信息的同时，科学技术的重要突破会对人类社会的发展带来重大影响。

信息的存储部分（如半导体存储器、光盘等）。因“信息”往往存在于有限时间间隔内，为了事后多次利用“信息”就需要以多种形式存储“信息”，把快速、方便、无失真、大容量、多次复用性作为这部分的主要性能指标。

信息的传输部分（无线信道、声信道、光缆信道及其变换器，如天线、接发收设备等）。这部分以大容量、少损耗、少干扰、稳定性、低价格等为科学研究技术进步为持续的目标。

信息的交换部分（如各种交换机、路由器、服务器）。这部分以少时延、易控制、安全性好、大容量、多种信号形式和多种服务模式相兼容为目标。

信息的变换处理部分（如各种“复接”，信号编解码、调制解调、信号压缩解压、信息

检测等，统称信号处理领域)。这部分可被认为是信息科技发展的瓶颈，近年来虽有很大进步，但尚不具备发展需要的类似人的信息处理能力，以实行人与机器的更紧密结合。实现这种结合，科学技术有漫长艰难的发展征程，但它是人类努力追求的目标之一。

信息的管理控制部分（如监控、计价、故障检测、故障情况下应急措施、多种信息业务管理等)。这部分功能的完成，除了随信息系统的复杂化而急骤增加变为更加复杂和困难外(如信息系统复杂的拓扑结构使管理监控领域科技基础涉及数学难题)，随着信息系统进一步融入社会，其管理控制的学科基础也发生了社会科学之进入交融而综合化。其管理控制功能也包括社科人文的复杂内容，导致“需要”与“实际水平”之间差距、矛盾更加明显。例如电子商务系统的管理控制涉及法律；多媒体文艺系统涉及管理及伦理道德、法律等领域。因此，信息的管理控制部分的发展涉及众多学科，具有重要性、挑战性及紧迫性。

信息系统的各个功能部分都有以下特征：软硬件相结合、离散数学型与连续模拟型相结合、各种功能部分交织融合支持形成主功能部分，如存储部分内含处理部分，管理控制部分内含存储、处理部分等。以上各部分发展都密切关联科学领域的新发现、技术领域的创新，并形成了信息科技与信息系统及社会之互相促进发展，发展中充满了挑战和机遇。

1.3 信息系统要素分析

信息系统从不同的角度划分，其要素的性质也不同。如可以划分为系统拓扑结构、应用软件、数据以及数据流；也可划分为管理、技术和人三个方面；还可划分为物理环境及保障、硬件设施、软件设施和管理者等部分。根据不同的应用可采用不同的划分方法，但无论采用哪种划分方法，都是利于对信息系统的理解、分析和应用的。下面根据上述最后一种划分方法分析信息系统的要素。

1.3.1 物理环境及保障

1. 物理环境

物理环境主要包括场地和计算机机房，是信息系统得以正常运作的基本条件。

(1) 场地（包括机房场地和信息存储场地)。信息系统机房场地条件应符合国家标准 GB 2887—2000 的有关具体规定，应满足标准规定的选址条件；温度、湿度条件；照明、日志、电磁场干扰的技术条件；接地、供电、建筑结构条件；媒体的使用和存放条件；腐蚀气体的条件等。信息存储场地，包括信息存储介质的异地存储场所应符合国家标准 GB 9361—1988 的规定，具有完善的防水、防火、防雷、防磁、防尘措施。

(2) 机房。在标准 GB 9361—1988 中将计算机机房的安全分为 A、B、C 三类，其中，A 类：对计算机机房的安全有严格的要求，有完善的计算机机房安全措施；B 类：对计算机机房的安全有较严格的要求，有较完善的计算机机房安全措施；C 类：对计算机机房的安全有基本的要求，有基本的计算机机房安全措施。标准中针对 A、B、C 三类机房，在场地选择、防火、内部装修、供配电系统、空调系统、火灾报警及消防设施、防水、防静电、防雷击、防鼠害等方面作了具体的规定。

2. 物理保障

物理安全保障主要考虑电力供应和灾难应急。

（1）电力供应：供电电源技术指标应符合 GB 2887—1989《计算机场地技术要求》中的规定，即信息系统的电力供应在负荷量、稳定性和净化等方面满足需要且有应急供电措施。

（2）灾难应急：设备、设施（含网络）以及其他媒体容易遭受地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）的破坏。信息系统的灾难应急方面应符合国家标准 GB 9361—1988 中的规定，应有防火、防水、防静电、防雷击、防鼠害、防辐射、防盗窃、火灾报警及消防等设施和措施，并应制订相应的应急计划。应急计划应包括紧急措施、资源备用、恢复过程、演习和应急计划关键信息，应有明确的负责人与各级责任人的职责，并应便于培训和实施演习。

1.3.2 硬件设施

组成信息系统的硬件设施主要有计算机、网络设备、传输介质及转换器、输入/输出设备等。为了便于叙述，在此也将存储介质和环境场地所使用的监控设备包含在硬件设施之中。

1. 计算机

计算机是信息系统的基本硬件平台。如果不考虑操作系统、输入/输出设备、网络连接设备等重要的部件，就计算机本身而言，除了电磁辐射、电磁干扰、自然老化以及设计时的一些缺陷等风险以外，基本上是不会存在另外的安全问题。常见的计算机有大型机、中型机、小型机和个人计算机（即 PC 机）。PC 机上的电磁辐射和电磁泄露主要在磁盘驱动器方面，虽然理论上讲主板上的所有电子元器件都有一定的辐射，但由于辐射较小，一般都不作考虑。

2. 网络设备

要组成信息系统，网络设备是必不可少的。常见的网络设备主要有交换机、集线器、网关、路由器、中继器、网桥、调制解调器等。所有的网络设备都存在自然老化、人为破坏和电磁辐射等安全威胁。

（1）交换机：交换机常见的威胁有物理破坏、欺诈、拒绝服务、访问滥用、不安全的状态转换、后门和设计缺陷等。

（2）集线器（HUB）：集线器常见的威胁有人为破坏、后门、设计缺陷等。

（3）网关或路由器：网关设备的威胁主要有物理破坏、后门、设计缺陷、修改配置等。

（4）中继器：对中继器的威胁主要是人为破坏。

（5）桥接设备：对桥接设备的威胁常见的有人为破坏、自然老化、电磁辐射等。

（6）调制解调器（Modem）：调制解调器是一种转换数字信号和模拟信号的设备，其常见威胁有人为破坏、自然老化、电磁辐射、设计缺陷、后门等。

3. 传输介质及转换器

常见的传输介质有同轴电缆、双绞线、光缆、卫星信道、微波信道等，相应的转换器有光端机、卫星或微波的收/发转换装置等。

（1）同轴电缆（粗/细）：同轴电缆由一个空心圆柱形的金属屏蔽网包围着一根内线导体组成。同轴电缆有粗缆和细缆之分。常见的威胁有电磁辐射、电磁干扰、搭线窃听和人为破坏等。

(2) 双绞线：一种电缆，在它的内部有一对自绝缘的导线扭在一起，以减少导线之间的电容特性，这些线可以被屏蔽或不进行屏蔽。常见的威胁有电磁辐射、电磁干扰、搭线窃听和人为破坏等。

(3) 光缆（光端机）：光缆是一种能够传输调制光的物理介质。同其他的传输介质相比，光缆虽较昂贵，但对电磁干扰不敏感，并且可以有更高的数据传输率。在光缆的两端通过光端机来发射并调制光波实现数字通信。常见的主要威胁有人为破坏、搭线窃听和辐射泄露。

(4) 卫星信道（收/发转换装置）：卫星信道是在多重地面站之间运用轨道卫星来转接数据的通信信道。在利用卫星通信时，需要在发射端安装发射转换装置，在接收端安装接收转换装置。常见的威胁有对信道的窃听和干扰，以及对收/发转换装置的人为破坏。

(5) 微波信道（收/发转换装置）：微波是一种频率为 1 ~ 30 GHz 的电磁波，具有很高的带宽和相对低的成本。在微波通信时，发射端安装发射转换装置，接收端安装接收转换装置。常见的威胁有对信道的窃听和干扰，以及对收/发转换装置的人为破坏等。

4. 输入/输出设备

常见的输入/输出设备主要有键盘、磁盘驱动器、磁带机、打孔机、电话机、传真机、识别器、扫描仪、电子笔、打印机、显示器和各种终端等设备。

(1) 键盘：键盘是计算机最常见的输入设备。常见的主要威胁有电磁辐射泄露信息和人为滥用造成信息泄露，如随意尝试输入用户口令。

(2) 磁盘驱动器：磁盘驱动器也是计算机中重要的输入输出设备，其主要威胁有磁盘驱动器的电磁辐射以及人为滥用造成信息泄露，如拷贝系统中重要的数据。

(3) 磁带机：磁带机一般用于大、中、小型计算机以及一些工作站上，既是输入设备也是输出设备，其威胁主要有电磁辐射和人为滥用。

(4) 打孔机：打孔机是一种早期使用的输出设备，可用于大、中、小型计算机上，其威胁主要有人为滥用。

(5) 电话机：电话机主要用于话音传输，严格地讲，它不是信息系统的输入输出设备，但电话是必不可少的办公用品。在信息系统安全方面，主要是考虑滥用电话泄露用户口令等重要信息。

(6) 传真机：传真机主要用于传真的发送和接收，严格地讲，它不是信息系统的输入输出设备。在信息系统安全方面，主要是考虑传真机的滥用。

(7) 麦克风：在使用语音输入时需要使用麦克风，其威胁主要是老化和人为破坏。

(8) 识别器：为识别系统用户，在众多的信息系统中都使用识别器。最常见的识别器有生物特征识别器、光学符号识别器等。其主要威胁是人为破坏摄像头等识别装置，以及识别器设计缺陷特别是算法运用不当等。

(9) 扫描仪：扫描仪主要用于扫描图像或文字。其主要的威胁是电磁辐射泄露系统信息。

(10) 电子笔（数字笔）：在手写输入法广泛使用的今天，电子笔或数字笔作为一种输入设备也越来越常见了，其主要的威胁是人为破坏。

(11) 打印机：打印机是一种常见的输出设备，但是部分打印机也可以将部分信息主动输入计算机。常见的打印机有激光打印机、针式打印机、喷墨打印机三种。打印机的主要威胁有电磁辐射、设计缺陷、后门、自然老化等。

（12）显示器：显示器作为最常见的输出设备，负责将不可见数字信号还原成人可以理解的符号，是人机对话所不可缺少的设备，其威胁主要是电磁辐射泄露信息。

（13）终端：终端既是输入又是输出设备，除了显示器以外，一般还带有键盘等外设，基本上与计算机的功能相同。常见的终端有数据、图像、话音等类之分。其威胁主要有电磁辐射、设计缺陷、后门、自然老化等。

5. 存储介质

信息的存储介质有许多种，但大家常见的主要有纸介质、磁盘、磁光盘、光盘、磁带、录音/录像带，以及集成电路卡、非易失性存储器、芯片盘等存储设备。

（1）纸介质：虽然信息系统中信息以电子形式存在，但许多重要的信息也通过打孔机、打印机输出，以纸介质形式存放。纸介质存在保管不当和废弃处理不当导致的信息泄露威胁。

（2）磁盘：磁盘是常见的存储介质，它利用磁记录技术将信息存储在磁性材料上。常见的磁盘有软盘、硬盘、移动硬盘、U 盘等。对磁盘的威胁有保管不当、废弃处理不当和损坏变形等。

（3）磁光盘：磁光盘是利用磁光电技术存储数字数据。对其威胁主要有保管不当、废弃处理不当和损坏变形等。

（4）光盘：光盘是一种非磁性的，用于存储数字数据的光学存储介质。常见的光盘有只读、一次写入、多次擦写等种类。对其威胁主要有保管不当、废弃处理不当和损坏变形等。

（5）磁带：磁带主要用于大、中、小型机或工作站上，由于其容量比较大，多是用于备份系统数据。对其威胁主要也是保管不当、废弃处理不当和损坏变形等。

（6）录音/录像带：录音带或录像带也是磁带的一种，主要用于存储话音或图像数据，这类数据常见的是监控设备获得的信息。其威胁主要是保管不当或损坏变形等。

（7）其他存储介质：除以上列举的一些常见的存储介质以外，磁鼓、IC 卡、非易失性存储器、芯片盘、Zip Disk 等介质也可以用于存储信息系统中的数据。对这些介质的威胁主要有保管不当、损坏变形、设计缺陷等。

6. 监控设备

依据国家标准规定和场地安全考虑，重要的信息系统所在场地应有一定的监控规程并使用相应的监控设备，常见的监控设备主要有摄像机、监视器、电视机、报警装置等。对监控设备而言，常见的威胁主要有断电、损坏或干扰等。

（1）摄像机：摄像机除作为识别器的一个部件以外，还主要用于环境场地检测，记录对系统的人为破坏活动，包括偷窃、恶意损坏和滥用系统设备等行为。

（2）监视器：在信息系统中，特别是交换机和入侵检测设备上常带有监视器，负责监视网络出入情况，协助网络管理。

（3）电视机：电视机同显示器一样，主要输出摄像机或监视器所捕获的图像或声音等信号。

（4）报警装置：报警装置就是发出报警信号的设备。常见的报警可以通过 BP 机、电话、声学、光学等多种方式来表现。

1.3.3 软件设施

组成信息系统的软件主要有操作系统，包括计算机操作系统和网络操作系统、通用应用软件、网络管理软件以及网络协议等。在风险分析时，软件设施的脆弱性或弱点是考察的重点，因为虽然硬件设施有电磁辐射、后门等可利用的脆弱性，但是其实现所需花费一般比较大，而对软件设施而言，一旦发现脆弱性或弱点，几乎不需要多大的投入就可以实现对系统的攻击。

1. 计算机操作系统

操作系统安全是信息系统安全的最基本、最基础的安全要素，操作系统的任何安全脆弱性和安全漏洞必然导致信息系统的整体安全脆弱性，操作系统的任何功能性变化都可能导致信息系统安全脆弱性分布情况的变化。因此从软件角度来看，确保信息系统安全的第一要事便是采取措施保证操作系统安全。

常见的操作系统有：

(1) UNIX：UNIX 是一种通用交互式分时操作系统，由 BELL 实验室于 1969 年开发出。自从 UNIX 诞生以来，它已经历过很多次修改，各大公司也相继开发出自己的 UNIX 系统。目前常见的有 California 大学 Berkeley 分校开发的 UNIX BSD；AT&T 开发的 UNIX System；SUN 公司的 Solaris；IBM 的 AIX 等多种版本。

(2) DOS：DOS 即磁盘操作系统，是早期的 PC 机操作系统。常见的 DOS 有微软公司的 MSDOS、IBM 公司的 PCDOS、Norton 公司的 DOS 系统以及我国的 CCDOS 等。

(3) Windows/NT：Windows 即视窗，是微软公司的一系列操作系统，其中常见的有 Windows 3.x、Windows 95/98，以及 Windows NT 和 Windows 2000、Windows XP 等。

(4) Linux：Linux 类似于 UNIX，是完全模块化的操作系统，主要运行于 PC 机上。目前有 RedHat、Slackware、OpenLinux、TurboLinux 等十多种版本。

(5) MACOS：是苹果公司生产的 PC 机 Macintosh 的专用操作系统。

(6) OS2：1987 年推出的以 Intel 80286 和 80386 微处理器为基础的 PC 机配套的新型操作系统。它是为 PC - DOS 和 MS - DOS 升级而设计的。

(7) 其他通用计算机操作系统：除以上的计算机操作系统以外还有 IBM 的 System/360 操作系统、DEC 公司的 VAX/VMS、Honeywell 公司的 SCOMP 等操作系统。

2. 网络操作系统

网络操作系统同计算机操作系统一样，也是信息系统中至关重要的要素之一。

(1) IOS：IOS 即 Cisco 互联网络操作系统，提供集中、集成、自动安装以及管理互联网络的功能。

(2) Novell Netware：Novell Netware 是由 Novell 开发的分布式网络操作系统，可以提供透明的远程文件访问和大量的其他分布式网络服务，是适用于局域网的网络操作系统。

(3) 其他专用网络操作系统：为提高信息系统的安全性，一些重要的系统曾选用专用的网络操作系统。

3. 网络通信协议

网络通信协议是一套规则和规范的形式化描述，即怎样管理设备在一个网络上交换信

息。协议可以描述机器与机器间接口的低层细节或者应用程序间的高层交换。网络通信协议可分为 TCP/IP 协议和非 IP 协议两类。

(1) TCP/IP 协议：TCP/IP 协议是目前最主要的网络互联协议，它具有互联能力强、网络技术独立和支持的协议灵活多样等优点，得到了最广泛的应用。国际互联网就是基于 TCP/IP 之上进行网际互联通信。但由于它在最初设计时没有考虑安全性问题，协议是基于一种可信环境的，因此协议自身固有许多安全缺陷，另外，TCP/IP 协议的实现中也存在着一些安全缺陷和漏洞，使得基于这些缺陷和漏洞出现了形形色色的攻击，导致基于 TCP/IP 的网络十分不安全，造成互联网不安全的一个重要因素就是它所基于的 TCP/IP 协议自身的不安全性。

(2) 非 IP 协议：常见的非 IP 协议有 X.25、DDN、帧中继、ISDN、PSTN 等协议，以及 Novell、IBM 的 SNA 等专用网络体系结构进行网间互联所需的一些专用通信协议。

4. 通用应用软件

通用应用软件一般指介于操作系统与应用业务之间的软件，为信息系统的业务处理提供应用的工作平台，例如 IE、OFFICE 等。通用应用软件安全的重要性仅次于操作系统安全的重要性，其任何安全脆弱性和安全漏洞都可以导致应用业务乃至信息系统的整体上的安全。

(1) Lotus Notes：IBM 公司的 Kitys Notes 作为信息系统业务处理的工作平台软件的代表，对其安全性的探讨目前主要集中在 Domino 服务器的安全上。

(2) MS Office：微软公司 Office 办公软件包括 Word、Power Point、Excel、Access 等软件，是目前较常见的信息处理软件。有关 MS Office 软件包的漏洞报道比较多，如 Word 的帮助功能就可以被利用来执行本机上的可执行文件。

(3) E - mail：电子邮件是互联网最常用的应用之一。邮件信息通过电子通信方式跨过使用不同网络协议的各种网络在终端用户之间传输。

(4) Web 服务、发布与浏览软件：World Wide Web (WWW) 系统最初只提供信息查询浏览一类的静态服务，现在已发展成可提供动态交互的网络计算和信息服务的综合系统，可实现对网络电子商务、事务处理、工作流以及协同工作等业务的支持。现有各种 Web 服务、发布与浏览软件，如 Mosaic、IE、Netscape 等。

(5) 数据库管理系统：数据库系统由数据库和数据库管理系统 (DBMS) 构成。数据库是按某种规则组织的存储数据的集合。数据库管理系统是在数据库系统中生成、维护数据库以及运行数据库的一组程序，为用户和其他应用程序提供对数据库的访问，同时也提供事件登录、恢复和数据库组织。

(6) 其他服务软件：在信息系统中，除了以上常见的一些通用应用软件以外，还有 FTP、TEI、NET、视频点播、信息采集等类型软件，这里不再赘述。

5. 网络管理软件

网络管理软件是信息系统的重要组成部分，其安全问题一般不直接扩散和危及信息系统整体安全，但可通过管理信息对信息系统产生重大安全影响。鉴于一般的网络管理软件所使用的通信协议 (例如 SNMP) 并不是安全协议，因此需要额外的安全措施。

常见的网络管理软件有：HP 公司的 Open View；IBM 公司的 Net View；SUN 公司的 Net Manager；3Com 公司的 Transcend Enterprise Manager；Novell 公司的 NMS；Cabletron 公司的