国家精品课程主讲教材

高等学校信息安全系列教材

信息安全对抗系统工程与实践

罗森林　高平　苏京霞　潘丽敏　编著

高等教育出版社
HIGHER EDUCATION PRESS

国家精品课程主讲教材
高等学校信息安全系列教材

信息安全对抗系统工程与实践

Xinxi Anquan Duikang Xitong Gongcheng yu Shijian

罗森林　高　平　苏京霞　潘丽敏　编著

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容简介

本书是国家精品课程主讲教材。全书共分为6章，主要内容包括：绪论，操作系统攻防技术实践，TCP/IP网络通信技术实践，网络攻击基础技术实践，数据加密解密技术实践，网络防御基础技术实践。

本书可作为信息安全、信息对抗、计算机应用等相关专业的正式教材，也可供相关实验选修课程、开放实验课程、专业课程设计以及信息安全对抗相关技术竞赛培训使用，还可供科研人员参考和对信息安全感兴趣者自学使用。

图书在版编目(CIP)数据

信息安全对抗系统工程与实践/罗森林等编著. --北京:高等教育出版社,2012.12

ISBN 978-7-04-036509-2

Ⅰ.①信… Ⅱ.①罗… Ⅲ.①信息系统-安全技术-高等学校-教材 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2012)第286006号

策划编辑	武林晓	责任编辑	武林晓	封面设计	于文燕	版式设计	马敬茹
责任校对	殷　然	责任印制	张泽业				

出版发行	高等教育出版社	咨询电话	400-810-0598
社　　址	北京市西城区德外大街4号	网　　址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印　　刷	北京机工印刷厂	网上订购	http://www.landraco.com
开　　本	787mm × 1092mm　1/16		http://www.landraco.com.cn
印　　张	22.5	版　　次	2012年12月第1版
字　　数	510千字	印　　次	2012年12月第1次印刷
购书热线	010-58581118	定　　价	32.00元

物 料 号　36509-00

前　言

信息系统在社会中起到“增强剂”和“催化剂”的作用，信息安全问题是信息系统所固有的本征矛盾发展的问题，在极大推动生产力发展的同时，人们对信息网络的依赖程度也日益提高，也因此使国家和社会面临着日益严重的信息安全威胁。国家政治、经济、文化、国防等各个领域面临着非传统的安全挑战，国家安全和社会稳定受到新的安全威胁，并表现得更为尖锐和复杂。在技术、管理和人才三要素中，人才是核心，信息安全与对抗的竞争归根结底是人才的竞争，信息安全的双刃剑作用要求大学生要充分了解和掌握信息安全现状及其主要技术，信息安全人才的培养有着时代的迫切性、突出性和专业性。

目前全国有多所高校建立了信息对抗或信息安全专业，本教材符合现代社会和科技发展以及社会对人才培养的需求，而且是各高校中急需解决的共性的、长期发展的问题，也是北京理工大学军工优势和特色的充分体现。该教材同专业的《信息系统与安全对抗理论》（国防特色优秀教材，北京市精品教材，国家和北京市精品课程用书）和《信息系统安全与对抗技术》（北京市精品教材，北京市精品课程用书）两本教材一起构成了上下贯通和互为延伸的高素质信息安全人才培养的配套教材。

北京理工大学是 1998 年教育部首批批准建立信息对抗技术专业的学校，其学科专业、教学科研、实践创新、人才梯队的建设已初见成效。本教材是在原《信息系统安全与对抗技术实验教程》教材的基础上，通过多年教学经验总结而重新认真构架而成的。在充分理解、掌握信息系统安全对抗理论与技术的基础上，考虑“研究型”教学的特点，让学生能够有效运用信息安全与对抗技术，发挥学生的主观能动性，重点培养学生的系统构建、工程实施、实践动手以及创新意识和思维能力。首先，该教材定位于“研究型”，信息安全对抗是信息系统中不可缺少的重要功能组成，在系统构建之初就应置于顶层来考虑，且需贯穿于系统的整个生命周期。同时，信息安全对抗问题涉及面很广，知识内容庞大，在有限的学时内如何形成有效的教学（传授知识）是首要解决的问题。教材基于丰厚和繁杂的专业知识，内容上从顶至下，理论分析、系统工程设计与实践相结合，同时与其他专业课互相贯通和延伸，构成完整的信息安全对抗专业知识体系和完善的“研究型”教材和教学内容。其次，该教材内容系统、先进、有实效。信息安全问题涉及内容极为复杂，其本身是一个系统性问题，遵守“全量大于各分量之和”的原理，单就分门别类的具体技术讲解，很难理清脉络，容易“只见树木，不见森林”。本教材从信息系统出发，层层推进，在注重安全对抗科学领域的核心思想、原理、方法的基础上，加强系统工程思想和创新实践能力的培养，内容上基于信息安全对抗基础、先进性技术和系统工程设计，充分考虑学生的兴趣（既有理论内容又有技术应用的系统设计与实践，还有需

要思考的创新性内容）和讲授内容的灵活性（既可以作为独立的理论教材，又可以用于辅助的实践类教材，讲授时可根据学生的情况灵活运用），同时在内容、方法上保证专业人才培养的需求，具有前瞻性和可持续发展性。此外，注重教材使用和实施的附加效果，加强信息安全知识普及传播和网络安全环境的建设，为提高全民信息安全意识提供切实可行的服务。

教材的主要内容涉及操作系统攻防技术，基于 TCP/IP 的网络通信保障技术，网络攻击和检测基础技术和系统，数据加密解密技术和系统，网络防御基础技术和系统，网络应用安全技术和系统，无线网络攻防技术和系统等。实验安排建议："基础型实验"学时数控制在每个实验 4 学时左右；"提高型实验"主要是优秀学生利用课上和课余时间完成，也可作为课程设计（或小学期）的综合性、创新性实践内容；建议采用学生小组形式，每小组人数控制在 2～3 人。

本书由罗森林、高平、苏京霞、潘丽敏共同撰写，其中第 2.2 节、第 3 章、第 4.3～4.7 节由高平负责撰写，第 4.8 节由苏京霞负责撰写，第 5 章、第 6.7 和 6.8 节由潘丽敏撰写，其余各章节由罗森林负责撰写。由罗森林负责全书的章节设计、内容规划和统稿。本书的全部例程都经过认真的编制和调试（读者可通过邮件直接与作者联系，电邮：gaoping@bit.edu.cn）。参与编写和程序调试的还有张蕾、陈燕颖、王坤、闫广禄、韩磊、韩龙飞、郭亮等。

在本书的编写过程中，得到了王越院士、仲顺安教授、扬煜祥老师等多方面的帮助，在此一并表示衷心的感谢。

由于时间所限，对于书中的不足和疏漏之处敬请广大读者批评指正，以便使其更加完善。

罗森林

2011 年 2 月于北京理工大学

目　录

第1章 绪 论

1.1 信息安全与对抗的概念

1.1.1 信息和信息系统

“信息是客观事物运动状态的表征和描述”，其中“表征”是客观存在的表征，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”，与人的认识实践结合，进而与人类生存发展相结合，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，经身体的感知功能及人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的复杂的多层次、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”，它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。

帮助人们获得信息、存储信息、传输信息、交换信息、处理信息、利用信息和管理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和不断扩大的含义，信息系统是有着各种以“信息”为媒介、不同功能和特征服务人类的系统的总称。

信息系统具有如下理论上的特征：①现代信息系统一般叠套多个相互交织作用的子系统；②信息系统符合系统理论中通过涨落达到新的有序原理；③信息系统作为人类社会及为人类服务的系统，伴随社会进化而发展，并有明显的共同进化作用，且越发展越复杂、越高级；④每一种信息系统的存在发展都有一定的约束，新发展又会产生新约束，也会产生新矛盾，如性能提高是一种“获得”，得到它必然付出一定的“代价”。

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、技术和人等方面；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。从功能的角度上分析，信息系统由下列部分交织或有选择

交织而组成，即信息的获取、存储、传输、交换、处理、管理与控制和应用部分，且各部分都有以下特征：软硬件相结合、离散数字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。

1.1.2 信息安全的概念

“安全”是损伤、损害的反义词，“信息”是运动状态的表征与描述，“信息安全”的含义是指“信息”的表征和描述未发生损伤性变化（即意味着运动状态“表征”的篡改、删除、以假代真等，形成上述结果的方法多种多样，也与多种因素有关）。就“信息”的篡改、删除、以假乱真而言，也往往与信息表达形式相关。信息或信息作品的安全问题关联很多内容，涉及很多学科分支，是一个开放性的复杂问题。

1.1.3 信息攻击与对抗的概念

信息安全问题的发生原因，很多与人有关，按人的主观意图分为：过失性，这与人总会有疏漏、犯错误有关；另一类是人因某种意图、有计划地采取各种行动，破坏一些信息和信息系统的运行秩序（以达到某种破坏目的），这种事件可称为信息攻击。

受攻击方当然不会束手待毙，总会采取各种措施反抗信息攻击，包括预防、应急措施，力图使攻击难以奏效，减小己方损失，以至惩处攻击方、反攻对方等，这种双方对立行动事件称为信息对抗。

信息对抗是一组对立矛盾运动的发展过程，过程是动态、多阶段、多种原理方法措施介入的对立统一的矛盾运动。信息对抗过程可用一个时空六元关系组概括表示，即：

$$\text{对抗过程} \leftarrow\rightarrow R^n[G,P,O,E,M,T]$$

其中，G 为目的域，n 表示对抗回合数，P 为参数域（提示双方对抗的重要参数），O 为对象域，E 为约束域，M 为方法域，T 为时间，R^n 表示六元间复杂的相互关系。

1.1.4 信息系统安全问题分类

信息与其运行相关的信息系统是紧密相关且互相不可分割的，这种特性体现在信息安全问题上同样紧密关联，与信息系统相关联的信息安全问题主要有以下三种类型。

第一种类型，“信息”与信息作品内容被篡改、删除、以假乱真，虽直接体现在“信息”或信息作品上，但发生过程却体现在信息系统的运行上，离不开作为运行平台的信息系统，这正体现了“信息”与信息系统在信息安全问题上相互关联不可分割。

第二种类型，信息系统发生信息安全问题则意味着系统的有关运行秩序被破坏（在对抗

情况下主要是人有意所为），造成正常功能被破坏而严重影响应用，体现在某时发生对某“信息”的破坏；此外，还会发生其他如“信息”传输不到正确目的地，传输延时过长影响应用。同样，不正常信息的泄漏也会严重影响应用。信息系统产生安全问题的具体原因多种多样，总体上认为信息系统及其应用的发展必含矛盾运动，安全对抗问题是众多矛盾对立的一类表现形式。

第三种类型，安全问题是攻击者直接对信息系统进行软、硬破坏，其使用方法可以不直接属于信息领域，而是其他领域的方法。例如，利用反辐射导弹对雷达进行摧毁，通过破坏线缆对通信系统进行破坏，利用核爆炸形成多种破坏信息系统的机理，化学能转换为强电磁能用以破坏各种信息系统等。

1.2 信息安全对抗基础理论概述

1.2.1 基础层面原理

1．特殊性存在与保持原理

在各种信息系统中，其工作规律、原理可以概括地理解为在普遍性（相对性）基础上对某些“特殊性”的维持和转换，如信息的存储和交换、传递、处理等。“安全”可理解为“特殊性”的有序保持和运行，各种“攻击”可理解为对原有的序和“特殊性”进行有目的的破坏、改变、以至渗入，实现攻击目的的“特殊性”。在抽象概括层次，信息安全与对抗的斗争是围绕特殊性而展开的，信息安全主要是特殊性的保持和利用。

2．信息存在相对性原理

伴随着运动状态的存在，必定存在相应的“信息”。同时，由于环境的复杂性，具体的“信息”可有多种形式表征运动，且具有相对的真实性。信息作为运动状态的表征是客观存在的，但信息不可能被绝对隐藏、仿制和伪造，这是运动的客观存在及运动不灭的本质所形成的，信息存在具有相对性。

3．广义空间维及时间维信息的有限尺度表征原理

各种具体信息存在于时间与广义空间中，即信息是以某种形式与时间、广义空间形成的某些“关系”来表征其存在的。信息的具体形式在广义空间所占大小以及时间维中所占长度都是有限的。在信息安全领域，可将信息在时间、空间域内进行变换和（或）处理以满足信息对抗的需要。如信息隐藏中常用的低截获概率信号，便是利用信息、信号在广义空间和时间维的小体积难以被对方发现截获的原理。

4．在“共道基础上反其道而行之相反相成”原理

该原理是矛盾对立统一律在信息安全领域的一个重要转化和体现。“共其道”是基础和前

提，也是对抗规律的一部分，在信息安全对抗领域以“反其道而行之”为核心的“逆道”阶段是对抗的主要阶段，是用反对方的“道”以达到己方对抗目的的机理、措施、方法的总结。运用该原理研究信息安全对抗问题，可转化为运用此规律研究一组关系集合中复杂的动态关系的相互作用。相反相成机理表现在对立面互相向对方转换，借对方的力帮助自己进行对抗等，都是事物矛盾时空运动复杂性多层次间“正”，“反”并存斗争，在矛盾对立统一律支配下产生的辩证的矛盾斗争运动过程。

5.“共其道而行之相成相反”原理

信息安全对抗双方可看做互为“正”“反”，在形式上以对方共道同向为主，实质上达到反向对抗（逆道）效果的原理，称为共其道而行的相成相反原理。“将欲弱之，必固强之，将欲废之，必固兴之，欲将取之，必固与之”，在信息安全对抗领域该原理中的“成”和“反”常具有灵活多样的内涵。如攻击方经常组织多层次攻击，其中佯攻往往吸引对方的注意力，以掩护主攻易于成功，而反攻击方识破佯攻计谋时往往也佯攻来吸引对方主攻早日出现，然后痛击之。

6. 争夺制对抗信息权及快速建立系统对策响应原理

根据信息的定义和信息存在相对性原理，双方在对抗过程中所采取的任何行动，必定伴随产生“信息”，这种“信息”称为“对抗信息”。它对双方都很重要，只有通过它才能判断对方攻击行动的“道”，进而为反对抗进行“反其道而行之”提供基础，否则无法“反其道而行之”，更不要说“相反相成”了。围绕“对抗信息”所展开的双方斗争是复杂的空、时域的斗争，除围绕“对抗信息”隐藏与反隐藏体现在空间的对立斗争外，在时间域中也存在着“抢先”、“尽早”意义上的斗争，同样具有重要性。时空交织双方形成了复杂的“对抗信息”斗争，成为信息安全对抗双方斗争过程第一回合的前沿焦点，并对其胜负起重要作用。

1.2.2 系统层面原理

1. 攻击方全局占主动地位，被攻击方居被动地位及局部争取主动，全局获胜原理

本原理说明，发动攻击方全局占主动地位，理论上它可以在任何时间、以任何攻击方法、对任何信息系统及任何部位进行攻击，攻击准备工作可以隐藏进行。被攻击方在这个意义上处于被动状态，这是不可变更的，被攻击方所能做的是在全局被动下争取局部主动。争取局部主动的主要措施有：①尽可能隐藏重要信息；②事前不断分析己方信息系统在对抗环境下可能遭受攻击的漏洞，事先预定可能遭受攻击的系统性补救方案；③动态监控系统运行，快速捕捉攻击信息并进行分析，科学决策并快速采取抗攻击有效措施；④在对抗信息斗争中综合运筹争取主动权；⑤利用假信息设置陷阱，诱使攻击方发动攻击而加以灭杀等。

2. 信息安全问题置于信息系统功能顶层综合运筹原理

信息安全问题是嵌入到信息系统功能中的一项非常重要的功能，但毕竟不是全部功能而是只起保证服务作用。因此，对待安全功能应根据具体情况，科学处理、综合运筹，并置于恰

当的“度”范围内。但需着重说明的是，特别是针对安全功能要求高的系统，必然要考虑并在系统设计之初就应考虑信息安全问题。

3．技术核心措施转移构成串行链结构，从而形成“脆弱性”原理

任何技术的实施都是相对有条件地发挥作用，必依赖于其充要条件的建立，而“条件”再作为一个事物又不可缺少地依赖其所需条件的建立（条件的条件），每一种安全措施在面对达到“目的”实施的技术措施中，即由达到目的的直接措施出发逐步落实效果过程中，必然遵照从技术核心环节逐次转移至普通技术为止这一规律，从而形成串行链结构规律。

4．变换、对称与不对称性变换应用原理

“变换”可以指相互作用的变换，可以认为是事物属性的“表征”由一种方式向另一种方式转变，也可认为是关系间的变换，即变换关系。在数学上可将变换看做一种映射，在思维方法中将进行变换看做是一种“化归”。这种原理也可用于信息安全对抗领域，即利用对称变换保持自身功能，同时利用对方不具备对称变换条件以削弱对方达到对抗制胜目的。

5．对抗过程多层次、多剖面动态组合对抗特性下间接对抗等价原理

设系统构成可划分为 $L_0,L_1,L_2,\cdots,L_n$ 的层次结构，且 $L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n$，如在 L_i 层子系统受到信息攻击，采取某措施时可允许在 L_i 层性能有所下降，但支持在 L_{i+j} 层采取有效措施，使得在高层次的对抗获胜，从而在更大范围获胜。因此，对抗一方绕开某层次的直接对抗而选择更高、更核心层进行更有效的间接式对抗称为间接对抗等价原理。

1.2.3 系统层面安全对抗方法

在信息安全对抗问题的运行斗争中，基础层次和系统层次原理在应用中，你中有我，我中有你，往往相互交织相辅相成地起作用，而不是单条孤立地起作用，重要的是利用这些原理观察、分析掌握问题的本征性质，进而解决问题。人们称实现某种目的所遵循的重要路径和各种办法为“方法”。“方法”的产生是按照事物机理、规律找出具体的一些实现路径和办法，因此对应产生办法的“原理”集，它是“方法”的基础。在信息安全与对抗领域，重要的问题是按照实际情况运用诸原理灵活地创造解决问题的各种方法。

（1）“反其道而行之相反相成”方法。本方法具有指导思维方式和起核心机理的作用，“相反相成”部分往往巧妙地利用各种因素，包括对方“力量”形成有效对抗方法。

（2）“反其道而行之相反相成”方法与“信息存在相对性原理”、“广义空间维及时间维信息的有限尺度表征原理”相结合可以形成信息攻击或反攻击的方法。

（3）“反其道而行之相反相成方法”与“争夺制对抗信息权及快速建立系统对策响应原理”相结合为对抗双方提供的一类对抗技术方案性方法。

（4）“反其道而行之相反相成方法”与“争夺制对抗信息权及快速建立系统对策响应原理”、“技术核心措施转移构成串行链结构而形成脆弱性原理”相结合形成的一类对抗技术方案性方法。

（5）“反其道而行之相反相成方法”及“变换、对称与不对称变换应用原理”相结合指导形成或直接形成的一类对抗技术方案性方法。

（6）重视对抗复合式攻击方法。复合攻击指攻击方组织多层次、多剖面时间、空间攻击的一种攻击模式，其特点是除在每一层次、剖面的攻击奏效都产生信息系统安全问题外，实施中还体现在对对方所采取对抗措施再形成新的附加攻击，这是一种自动形成连环攻击的严重攻击。对抗复合攻击可利用对方攻击次序差异（时间、空间）各个击破，或使对抗攻击措施中不提供形成附加攻击的因素等。

（7）“共其道而行之相成相反”方法。“相成相反”展开为：某方在某层次某过程对于某事相成；某方在某层次某过程对于某事相反。前后两个“某方”不一定为同一方。在实际对抗过程中，对抗双方都会应用“共其道而行之相成相反”方法。

1.3 信息安全对抗基础技术概述

1.3.1 安全攻击与检测技术

一个攻击行为的发生一般有三个阶段，即攻击准备、攻击实施和攻击后处理。当然这种攻击行为有可能对攻击目标未造成任何损伤或者说攻击未成功。攻击行为过程示意图如图 1.1 所示。

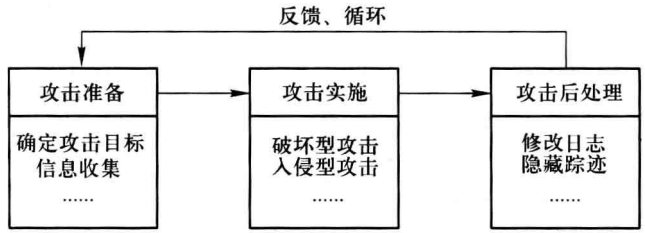

图 1.1 攻击行为过程示意图

攻击的准备阶段可分为确定攻击目标和信息收集两个子过程。攻击前首先确定攻击目标，而后确定要达到什么样的攻击目的，即给对方造成什么样的后果，常见的攻击目的有破坏型和入侵型两种。当收集到足够的信息后，攻击者就可以实施攻击了，对于破坏型攻击只需利用必要的工具发动攻击即可。但作为入侵型攻击，往往要利用收集到的信息找到系统漏洞，然后利用该漏洞获得一定的权限，有时获得一般用户的权限就足以达到攻击的目的，但一般攻击者都想尽办法获得系统最高权限，这不仅为了达到入侵的目的，在某种程度上也是为了显示攻击者的实力。

信息系统安全攻击和检测技术，涉及的内容很多，包括网络安全扫描技术、网络数据获取技术、计算机病毒技术、特洛伊木马技术、IP/Web/DNS 欺骗攻击技术、ASP/CGI 安全性分析、拒绝服务攻击、缓冲区溢出攻击、信息战和信息武器等。下面简要介绍其中的几项主要技术。

1．安全扫描技术

安全扫描技术是在攻击进行前的主动检测。安全扫描技术与防火墙、安全监控系统互相配合就能够为网络提供较高的安全性。安全扫描技术从扫描的方式主要分为两类：基于主机的安全扫描技术和基于网络的安全扫描技术。基于主机的安全扫描技术主要针对系统主机的脆弱性、弱密码，以及针对其他与安全规则、策略相抵触对象的检查等。基于网络的安全扫描技术是一种基于网络的远程检测目标网络或本地主机安全性脆弱点的技术，通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞。

2．网络数据获取技术

无论从攻击及检测的角度，还是从防御和对抗的角度，网络数据获取是不可缺少的步骤。如通过网络监听可以侦听到网上传输的密码等信息；通过截获网络数据可以获取秘密或重要信息；入侵检测系统必须通过获取网络数据达到攻击检测的目的等。网络数据获取可以通过多种方式实现，如利用以太网的广播特性，或通过设置网络设备的监听端口，或通过分光技术来实现等。随着网络带宽的不断增加，网络数据获取的技术要求也越来越高，要很好地解决丢包和海量数据的存储等问题。网络数据获取只是安全对抗的第一步，关键是获取数据后的处理能力和处理结果的有效性。

3．计算机病毒技术

《中华人民共和国计算机信息系统安全保护条例》第 28 条指出：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”计算机病毒一般具有以下特性：程序性（可执行性）、传染性、寄生性（依附性）、隐蔽性、潜伏性、触发性、破坏性、变种性（衍生性）等。按攻击的系统分为：DOS 系统病毒、Windows 系统病毒、UNIX 系统病毒。按链接方式可将计算机病毒分为以下几类：源码型病毒、嵌入型病毒、外壳型病毒、操作系统型病毒等。按寄生部位或传染对象分为：磁盘引导区型病毒、操作系统型病毒、可执行程序型病毒等。计算机病毒破坏计算机系统数据、抢占系统资源、影响计算机运行速度以及会造成不可预见的危害，如给用户造成严重的心理压力。计算机病毒的检测有手工检测和自动检测两种，具体方法包括比较法、搜索法、分析法、感染实验法、软件模拟法、行为检测法等，其消除也有手工消毒和自动消毒两种方法。

4．特洛伊木马技术

特洛伊木马（Trojan Horse）是隐蔽在计算机程序里面并具有伪装功能的一段程序代码，实质上是一个网络客户端服务器程序。木马被激活运行后，潜伏在后台监视系统的运行，能实现合法软件的功能，包括复制、删除文件，格式化硬盘、发电子邮件、释放病毒等。根据木马