工业和信息化部“十二五”规划专著

信息系统安全等级保护原理与应用

蔡皖东　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

工业和信息化部“十二五”规划专著

信息系统安全等级保护原理与应用

蔡皖东　编著

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

内 容 简 介

信息系统安全等级保护是国家制定和推行的一项信息系统安全保护制度，并有一系列配套的技术标准和法律法规。由于信息系统安全等级保护标准比较多，覆盖了等级保护的各个阶段，因此不太容易理解和掌握。

本书对相关标准进行了梳理，以第三级系统安全保护为主线，介绍了信息系统安全等级保护的概念、原理和应用。全书分为8章，介绍了信息系统安全概论、信息系统安全等级保护定级、信息系统安全等级保护要求、信息系统等级保护安全设计、信息系统安全等级保护实施、信息系统安全等级保护测评、信息系统安全等级保护应用、工业控制系统信息安全等内容。

本书为研究和应用信息系统安全等级保护制度及相关标准提供了参考，也可作为信息系统安全等级保护培训的教材。

图书在版编目(CIP)数据

信息系统安全等级保护原理与应用/蔡皖东编著. —北京：电子工业出版社，2014.11
工业和信息化部“十二五”规划专著
ISBN 978-7-121-20349-7

I. ①信… II. ①蔡… III. ①信息系统－安全技术－研究 IV. ①TP309

中国版本图书馆 CIP 数据核字(2014)第 252612 号

策划编辑：索蓉霞
责任编辑：张 京
印 刷：三河市双峰印刷装订有限公司
装 订：三河市双峰印刷装订有限公司
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
开 本：787×1092 1/16 印张：12.5 字数：336.2 千字
版 次：2014 年 11 月第 1 版
印 次：2014 年 11 月第 1 次印刷
定 价：45.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

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。

服务热线：(010)88258888。

前　言

随着互联网技术的不断发展，计算机网络越来越显示出在社会信息化中的巨大作用，已经成为当前知识经济和社会生活的基础设施，推动了企业信息化、新兴服务行业、信息产业的快速发展，带动了国民经济发展和社会进步。

由于网络系统的开放性，以及现有网络协议和软件系统固有的安全缺陷，使任何一种网络系统都不可避免地、或多或少地存在着一定的安全隐患和风险，使人们在享受网络所带来的方便和效益的同时，也面临着网络安全提出的巨大挑战，如黑客攻击、病毒传播、非法联络、信息获取等，给网络信息安全带来严重的威胁，网络安全事件屡有发生，给国家安全、企业利益和个人权益带来极大的危害，并造成了巨大的经济损失。

近年来，随着信息化的发展，国内各行各业建设了大量的网络信息系统，信息安全问题变得日益突出。为了应对信息安全方面的挑战，国家制定了两种信息系统安全保护制度：信息系统安全等级保护制度和涉密信息系统分级保护制度，前者主要针对非密信息系统，而后者针对涉密信息系统，并制定了一系列相关技术标准和法律法规，推动了网络信息安全技术的发展，规范了网络信息系统建设和管理。

本书主要介绍信息系统安全等级保护的概念、原理和应用，包括信息系统安全等级保护的定级方法、基本要求、安全设计、实施流程、测评要求及应用实例等，主要内容来源于信息系统安全等级保护相关标准。由于信息系统安全等级保护标准比较多，覆盖了等级保护的各个阶段，并且对每个保护等级都做了详细的规定和描述，阅读起来难免有些眼花缭乱，不易理解和掌握。因此，本书对相关标准进行了梳理，主要以第三级系统安全保护为主线来介绍等级保护的原理和方法，为进一步掌握和运用相关标准打下良好的基础。

本书没有对相关的信息安全技术做详细的介绍，读者最好具有一定的信息安全基础知识，这样有助于理解和掌握本书的内容。

全书分为 8 章，第 1 章为信息系统安全概论，介绍了网络安全威胁、信息安全技术、信息安全相关国家标准、信息安全相关法律法规、等级保护和分级保护等内容；第 2 章为信息系统安全等级保护定级，介绍了系统定级原理和方法；第 3 章为信息系统安全等级保护要求，主要介绍了第三级系统安全保护的基本技术要求、基本管理要求、整体保护能力要求、基本安全要求的应用等内容；第 4 章为信息系统等级保护安全设计，介绍了第一级到第四级系统安全保护环境设计、第三级系统安全保护环境设计示例等内容；第 5 章为信息系统安全等级保护实施，介绍了信息系统定级、总体安全规划、安全设计与实施、安全运行与维护、信息系统终止等工作流程；第 6 章为信息系统安全等级保护测评，介绍了第三级安全技术测评、第三级安全管理测评、等级测评结论、等级测评过程等内容；第 7 章为信息系统安全等级保护应用，以一个信息系统安全等级保护方案为例，介绍了信息系统描述、信息系统定级、安全保护方案、安全风险评估等内容；第 8 章为工业控制系统信息安全，介绍了工业控制系统及通信协议、工业控制系统信息安全风险、工业控制系统信息安全标准、工业控制系统安全等级保护等内容。

本书主要内容来源于国家相关标准，这里谨向相关标准制定者表示敬意和感谢。如果本书能够对信息系统安全等级保护制度的推广应用及人才培养起到有益作用，则作者的目的便达到了。

最后，感谢西北工业大学专著出版基金对本书的大力资助。

编　者

于西安·西北工业大学

目　录

第1章　信息系统安全概论

1.1　概　　述

随着互联网技术的不断发展，计算机网络越来越显示出在社会信息化中的巨大作用，已经成为当今社会经济活动和社会生活的基础设施，推动了工业信息化、新兴服务业、信息产业的快速发展，带动了国民经济发展和社会进步。

由于网络系统的开放性，以及现有网络协议和软件系统固有的安全缺陷，使任何一种网络系统都不可避免地、或多或少地存在着一定的安全隐患和风险，使人们在享受网络所带来的方便和效益的同时，也面临着网络安全提出的巨大挑战，如黑客攻击、病毒传播、非法联络、情报获取等，给网络信息安全带来严重的威胁，安全事件屡有发生，给国家安全、企业利益和个人权益带来极大的危害，并造成了巨大的经济损失。

以获取经济利益为目的的黑客经济兴起，网络侵权和犯罪活动屡禁不止，手法日益翻新，包括篡改网站内容、攻击网络服务器、传播盗版数字作品、窃取网银账号、组建僵尸网络等，直接危害了网络安全和社会和谐。

不法分子利用互联网传播黄色信息、邪教信息、虚假新闻、垃圾邮件等有害信息，严重扰乱了人们的思想，特别是给青少年的身心健康带来了极大的危害。

国内外敌对势力利用互联网进行非法联络，通过加密邮件、即时通信、语音通信、P2P 通信等手段进行秘密联络，策划和实施恐怖活动，直接威胁着国家安全和社会稳定。

网络间谍利用互联网盗窃国家机密信息、企业内部信息和个人隐私信息，网络窃密和泄密事件不断发生。尤其是海外间谍机关利用木马技术有预谋性地窃取国家政治、军事和经济情报，直接危害了国家安全和利益。根据国家安全保密部门统计，在我国每年发生的泄密案件中，70%是海外间谍机关通过互联网和木马窃取信息，并且有逐年增长的趋势，对国家安全和利益造成了极大的危害。在这些窃密木马中，大部分由中国台湾地区和美国所控制，其中台湾地区占 65%，美国占 8%。网络窃密问题已经给国家安全和利益带来了极大的危害。

针对不断增长的信息安全挑战，必须采取有效的信息安全技术来提高信息系统安全防护和入侵检测能力，保障信息系统安全。信息系统安全保护工作是一项系统工程，需要采用工程化方法来规范信息系统安全建设，将信息安全技术贯穿于信息系统建设的各个阶段，而不是单一信息安全技术的简单应用，这样才能达到信息系统安全保护的整体要求。

本章主要介绍了网络安全威胁、网络攻击技术、信息安全技术、信息安全工程及信息安全法规等，使读者对信息系统安全问题有整体上的了解和认知。

1.2 网络安全威胁

1.2.1 网络环境下的安全威胁

所谓的安全威胁是指对系统安全性的潜在破坏。一个系统可能受到各种各样的安全威胁，只有认识到这些安全威胁，才能采取相应的安全措施进行防范。

通常，在开放的网络环境中，可能面临如下的安全威胁。

（1）身份假冒：一个实体通过身份假冒而伪装成另一个实体，威胁源是用户或程序。

（2）非法连接：在网络实体与网络资源之间建立非法逻辑连接，威胁源是用户或程序。

（3）非授权访问：入侵者违反访问控制规则越权访问网络资源，威胁源是用户或程序，威胁对象是各种网络资源。

（4）拒绝服务：拒绝为合法的用户提供正常的网络服务，威胁源是用户或程序。

（5）操作抵赖：用户否认曾发生过的数据报发送或接收操作，威胁源是用户或程序。

（6）信息泄露：未经授权的用户非法获取了信息，造成信息泄密，威胁源是用户或程序，威胁对象是网络通信中的数据报或数据库中的数据。

（7）通信业务流分析：入侵者通过观察和分析通信业务流（如信源、信宿、传送时间、频率和路由等）来获得敏感信息，威胁源是用户或程序，威胁对象是网络通信中的数据报。

（8）数据流篡改：对正确的数据报序列进行非法修改、删除、重排序或重放，威胁源是用户或程序，威胁对象是网络通信中的数据报。

（9）数据篡改或破坏：对网络通信中的数据报和数据库中的数据进行非法修改或删除，威胁源是用户或程序，威胁对象是网络通信中的数据报或数据库中的数据。

（10）信息推测：根据公布的概要信息（如统计数据、摘要信息等）来推导原有信息中的数据值，威胁源是用户或程序，威胁对象是数据库中的数据。

（11）程序篡改：篡改或破坏操作系统、通信软件或应用软件，威胁源是用户或程序，威胁对象是系统中的程序。

1.2.2 TCP/IP 协议的安全弱点

在制定 TCP/IP 协议之初，并没有过多地考虑安全问题。随着 TCP/IP 协议的广泛应用，尤其是成为互联网的基础协议后，TCP/IP 协议暴露出一些安全弱点，被攻击者利用，作为攻击网络系统的重要手段。

TCP/IP 协议的安全弱点主要表现在两个方面：一是没有提供任何安全机制，如数据保密性、数据完整性及身份真实性等，不能直接用于建立安全通信环境，必须通过附加安全协议来提供安全机制和安全服务，如 IP 安全（IPSec）协议、安全套接层（SSL）协议等都是基于 TCP/IP 协议的安全协议；二是本身有安全隐患，往往被攻击者利用，作为攻击网络系统的一种手段，如 IP 地址欺骗、ICMP Echo flood、TCP SYN flood 和 UDP flood 攻击等，它们大都属于拒绝服务（DoS）攻击。

所谓 DoS 攻击是指非法占用和消耗一个系统资源，使该系统不能提供正常的服务，造成该系统暂时瘫痪，严重时可能引起系统崩溃。DoS 攻击有很多方法，其中 ICMP Echo flood、

TCP SYN flood 和 UDP flood 等都是基于 TCP/IP 协议的 DoS 攻击。下面简要介绍 ICMP Echo flood 和 TCP SYN flood 攻击的基本原理。

1．ICMP Echo flood 攻击

ICMP Echo flood 攻击是一种常见的 DoS 攻击，它利用了 ICMP 协议中的回送（Echo）请求/响应报文来实现 DoS 攻击。

ICMP Echo 报文主要用于测试网络目的节点的可达性。源节点向某一指定的目的主机发送 ICMP Echo 请求报文，目的节点收到请求后必须使用 ICMP Echo 响应报文进行响应。在 TCP/IP 实现系统中，Ping 命令就是利用这种 ICMP Echo 报文来测试目的可达性的。

由于一个主机所创建的接收缓冲区总是有限的，如果攻击者在短时间内向一个主机发送大量的 ICMP Echo 请求报文，则会造成该主机的接收缓冲区阻塞和溢出，使它无法接收其他正常的处理请求，于是拒绝服务，造成该主机的网络功能暂时瘫痪。

2．SYN flood 攻击

TCP SYN flood 攻击是一种常见的 DoS 攻击，它利用 TCP 协议在建立连接时的“三次握手”过程来实现 DoS 攻击。

TCP 协议为什么要通过“三次握手”过程来建立连接呢？主要是为了防止因 TCP 报文的延迟和重传可能带来的不安全因素。由于 TCP 报文是在 IP 通信子网上进行传输的，如果通信子网比较拥挤，则 TCP 报文将被会延迟，进而产生重复的 TCP 报文。对于 TCP 数据报文，可以通过报文中的序号来滤除重复的 TCP 报文。对于 TCP SYN 报文（建立连接）和 TCP FIN 报文（关闭连接），重复的 TCP 报文将带来一定的安全隐患。例如，在电子交易中，一个客户与银行建立一个 TCP 连接，客户通知银行给某个商家的账户里转入一大笔款项，然后便释放该连接。如果在建立连接时产生了重复的 TCP SYN 报文和数据报文，并因网络拥挤被暂存在某个路由器上，在该连接释放后，这些被重复的报文却又顺序地到达目的端，请求建立一个新的连接并再次转账，结果给客户造成了很大的损失。因此，TCP 协议在建立连接和关闭连接时双方必须进行认证，即必须执行一个“三次握手”过程。建立连接和关闭连接的情况基本相同，下面以建立连接为例来说明这个问题。

在正常情况下，主机 A 向主机 B 发送一个起始序号为 i 的 TCP SYN 报文请求建立连接；主机 B 收到后发送一个应答报文，同时请求建立一个反向连接（TCP SYN+ACK），且起始序号为 j；主机 A 在发送数据报文的同时捎带对反向连接请求进行应答（TCP DATA+ACK）。

在出现被延迟的重复 TCP SYN 报文情况下，重复的 TCP SYN 报文到达主机 B 后，请求在已关闭的连接上再次建立连接，主机 B 发送一个应答报文并请求建立一个反向连接（TCP SYN+ACK）；主机 A 便可以发现这个建立连接请求是虚假的，并拒绝主机 B 的请求，不作任何应答；主机 B 超时后将放弃该连接。这样，通过“三次握手”过程可以避免因 TCP 报文的延迟和重传可能带来的不安全因素。

然而，“三次握手”却会引起另一种安全问题，即 TCP SYN Flood 攻击问题。通常，在 TCP 接收程序中设有一个最大连接请求数的参数。如果某个时刻的连接请求数已经达到最大连接请求数，则后续到达的连接请求将被 TCP 丢弃。除非某一连接被关闭，在 TCP 连接请求队列中出现空位置，才能接受新的连接请求。这就是 SYN flood 攻击的基本原理。

如果攻击者 A 向 B 主机发送多个 TCP SYN 报文请求建立连接，并将源 IP 地址替换成一个不

存在的虚假主机 X，则 B 向 X 发送 TCP SYN+ACK 报文进行响应，但肯定不会收到来自 X 的 TCP ACK 报文。于是，B 主机的 IP 层向 TCP 层报告一个错误信息：X 主机不可达，但 B 主机的 TCP 层对此不予理睬，认为只是暂时的，继续等待。由于 TCP 连接请求队列被这种虚假的连接请求所填满，因而不能再接收正常的连接请求，结果产生拒绝服务，造成 B 主机的网络功能暂时瘫痪。

由于信息系统和通信协议存在着大量的安全漏洞和弱点，被攻击者利用，发动网络攻击，对信息系统构成很大的威胁，人们不得不耗费大量的人力和物力开发各种信息安全产品，用于增强系统安全性，防范各种网络攻击。

1.3 网络攻击技术

在开放的互连网络系统中，不仅包含各种交换机、路由器、安全设备和服务器等硬件设备，还包含各种操作系统平台、服务器软件、数据库系统及各种应用软件等软件系统，系统结构十分复杂。从系统安全角度讲，任何一部分要想做到万无一失都是非常困难的，而任何一个疏漏都有可能导致安全漏洞，给攻击者以可乘之机，形成安全威胁，并可能带来严重的后果。

在现实网络世界中，网络攻击是安全威胁的具体实现，常见的网络攻击行为主要有如下几种：一是网络监听，通过监听和分析网络数据包来获取有关重要信息，如用户名和口令、重要数据等；二是信息欺骗，通过篡改、删除或重放数据包进行信息欺骗；三是系统入侵，通过网络探测、IP 欺骗、缓冲区溢出、口令破译等方法非法获取一个系统的管理员权限，进而植入恶意代码（如木马、病毒等），获取重要数据或实施系统破坏；四是网络攻击，通过分布式拒绝服务、计算机病毒等方法攻击一个网络系统，使该系统限于瘫痪或崩溃。

下面主要介绍计算机病毒、特洛伊木马、DDoS 攻击、缓冲区溢出攻击、IP 欺骗攻击等几种典型的网络攻击技术。

1.3.1 计算机病毒

1. 计算机病毒概述

计算机病毒（简称病毒）是指一种人为制造的恶意程序，通过网络、存储介质（如 U 盘）等途径进行传播，传染给其他计算机，从事各种非法活动，包括控制计算机、获取用户信息、传播垃圾信息、吞噬计算机资源、破坏计算机系统等，成为计算机及其网络系统的公害。

计算机病毒一词最早诞生于 20 世纪 70 年代中期美国的科幻小说之中，那时人们更多地把它当作一个杞人忧天的想法来谈论。1984 年美国计算机专家 Fred Cohen 在美国国家计算机安全会议上演示了计算机病毒实验，目的在于引起有关部门的注意。根据有关的资料，第一例广泛传播的计算机病毒是在 1986 年诞生的巴基斯坦病毒，主要目的是为了保护软件版权，用户使用盗版软件就会染上这个病毒。到 1987 年后，计算机病毒在全球蔓延起来。

1988 年 11 月 1 日，美国康奈尔大学的研究生 Robert Morris 在网络上试验计算机病毒的可行性时，释放了一种实验性的网络蠕虫程序，在 8 小时之内，这一程序入侵了 3000～6000 台运行 UNIX 操作系统的 VAX 和 Sun 计算机，由于蠕虫程序以极快的速度在网络中的计算机之间进行复制，这些计算机的所有计算时间都被蠕虫程序占用，导致系统瘫痪，造成了大约 9200 万美元的重大经济损失。从此，人们开始认识到通过网络传播病毒的危害性。

我国第一次发现计算机病毒是在 1988 年年底。在此之后，计算机病毒的增长速度十分迅速，根据 1992 年公安部门的统计，全国 70%～80%的计算机都被感染过。在这一阶段，国内

计算机病毒主要是从国外传入的。在 20 世纪 90 年代之后，开始出现了国产病毒，例如广州一号、中国炸弹等。

目前，全世界流行的计算机病毒已超过 8 万余种，并以每月 300～500 种的速度不断增长。据国际计算机安全协会（ICSA）的抽样调查结果，在被抽样的计算机中，几乎所有计算机都有过被计算机病毒感染的经历。虽然有 91%的服务器和 98%的客户机都使用了防病毒软件，但被计算机病毒感染和破坏的事件仍然有增无减。同时，随着互联网的普及，通过钓鱼网站、电子邮件等传播的计算机病毒和黑客程序越来越多，互联网成为计算机病毒的重要传播途径。

当前，计算机病毒呈现多样化发展的态势，其破坏性也在不断增加，包括破坏计算机硬件、随机修改和删除文件、篡改网页信息、设置后门程序、获取秘密信息、攻击网络系统、传播垃圾信息等，造成很大的危害。

2010 年 9 月 24 日，伊朗核设施遭到震网（Stuxnet）病毒攻击，导致其核设施不能正常运行。震网病毒是世界上首个专门攻击工业控制系统的计算机病毒，通过 U 盘将震网病毒“摆渡”到内部网络进行传播，进而攻击内部网络中的工业控制系统。据网络安全公司赛门铁克公司的统计，全球大约有 45 000 个网络被该病毒感染。信息安全界将震网病毒攻击伊朗核设施事件列为 2010 年十大信息技术事件之一。

2011 年出现的毒区（Duqu）病毒和 2012 年出现的火焰（Flame）病毒等都是专门攻击工业控制系统的计算机病毒，说明计算机病毒已经成为一种强大的网络战武器。

2．震网病毒的工作原理

震网病毒主要通过 U 盘传入内部网络进行传播，它利用 5 个 Windows 系统漏洞及西门子公司的工业控制软件 WinCC 中的漏洞，伪装 RealTek 与 JMicron 两大公司的数字签名，通过一套完整的入侵传播流程，突破工业控制网络的物理隔离，对西门子的数据采集与监视控制（SCADA）系统实施特定的攻击。

SCADA 系统是一种广泛用于能源、交通、水利、铁路交通、石油化工等领域的工业控制系统。SCADA 系统不仅能实现生产过程控制与调度的自动化，而且具备现场数据采集、状态监视、参数调整、信息报警等多项功能。震网病毒被激活后，以 SCADA 系统为攻击目标，修改可编程逻辑控制器（PLC），劫持 PLC 发送控制指令，给工业控制系统造成控制混乱，最终造成业务系统异常、核心数据泄露、停产停工等重大事故，给企业造成难以估量的经济损失，甚至给国家安全带来严重威胁。

震网病毒传播的过程是：首先感染外部主机，然后感染 U 盘，利用快捷方式解析漏洞，传播到内部网络。在内部网络中，通过快捷方式解析漏洞，包括 RPC 远程执行漏洞、打印机后台程序服务漏洞等，实现连网计算机之间的传播。如果病毒感染了运行 WinCC 软件的计算机，则对工业控制系统发起攻击。

震网病毒采取多种手段进行渗透和传播，其工作过程如下：

（1）通过感染震网病毒的 U 盘感染目标系统中的某台计算机；

（2）通过被感染计算机将震网病毒传播给内部网其他计算机；

（3）震网病毒尝试与外网的控制台服务器进行通信；

（4）震网病毒感染内部网中安装有 WinCC 软件的工作站；

（5）当被感染的工作站连接 PLC 时，震网病毒向 PLC 部署恶意代码；

（6）恶意代码向工业控制设备发送特定的指令实施攻击。

震网病毒可以在 Windows 2000、Windows XP、Windows Vista、Windows 7 及 Windows Server 等操作系统中激活运行。该病毒被激活后，将利用 WinCC 7.0、WinCC 6.2 等版本的工业控制系统软件漏洞，实施对 CPU 6ES7-417 和 6ES7-315-2 型 PLC 的攻击和控制。可见，震网病毒最终的攻击目标是 PLC，这也是震网病毒区别于其他传统病毒的主要特点。

PLC 是工业控制系统自主运行的关键，PLC 中的控制代码通常由一台运行 WinCC/step 7 等软件的工作站进行远程配置，同时工作站还可以通过管理软件检测 PLC 代码的合法性和安全性。PLC 中的代码一旦配置完成，就可以脱离工作站独立地运行，自主完成对生产现场的数据采集、监视、调度等工作。

震网病毒被激活后，首先将原始的 s7otbxdx.dll 文件重命名为 s7otbxsx.dll，然后用自身取代原始的 DLL 文件。这时，震网病毒就可以拦截来自其他软件的任何访问 PLC 的命令了。被震网病毒修改后的 s7otbxdx.dll 文件保留了原来的导出表，导出函数仍为 109 个，其中 93 个导出命令会转发给真正的 DLL，即重命名后的 s7otbxsx.dll，而剩下的 16 种涉及 PLC 的读、写、定位代码块的导出命令，则被震网病毒改动后的 DLL 所拦截。

此外，震网病毒为了防止其写入 PLC 的恶意数据被 PLC 安全检测软件和防病毒软件发现，震网病毒利用 PLC rootkit 技术将其代码隐藏于假冒的 s7otbxdx.dll 中，主要监测和截获对自己的隐藏数据模块的读请求、对受感染代码的读请求及可能覆盖震网病毒自身代码的写请求，通过修改这些请求，能够保证震网病毒不会被发现或被破坏，如劫持 s7blk_read 命令，监测对 PLC 的读数据请求，读请求涉及震网病毒在 PLC 中的恶意代码模块，将返回一个错误信息，以规避安全检测。

震网病毒在感染 PLC 后，将改变控制系统中两种频率转换器的驱动，修改其预设参数。频率转换器用来控制其他设备的运行速度，如发动机等，大量应用于供水系统、油气管道系统等工业设施中。震网病毒主要针对伊朗德黑兰 Fararo Paya 公司和芬兰 VACON 公司生产的变频器，导致其控制设备发生异常。

震网病毒与传统蠕虫病毒相比，除了具有极强的隐蔽性与破坏力外，还具备如下特点。

（1）病毒攻击具有很强的目的性和指向性。震网病毒虽然能够像传统的蠕虫病毒一样在互联网上进行传播，但并不是以获取用户数据或牟利为目的，其最终的攻击目标是重要基础设施的 SCADA 系统，修改 SCADA 系统的数据采集、监测、调度等命令逻辑，造成 SCADA 系统的采集数据错误、命令调度混乱，甚至完全操纵控制系统的指控逻辑，按攻击者的意图对工业生产实施直接破坏。

（2）漏洞利用多样化和攻击技术复杂化。震网病毒从感染、传播，到实现对工业控制系统的攻击，综合利用了多个层次的系统漏洞，涉及 Windows 等通用系统和 SCADA 等专用系统的开发和利用技术，对病毒设计者的技术能力要求很高。例如，在设计入侵 PLC 的攻击代码时，至少需要精通 C/C++ 和 MC7 两种编程语言，同时还要熟练掌握进程注入、程序隐藏等高级编程技术。此外，为了防止防病毒软件的查杀，该病毒还利用安全证书仿冒技术、Rootkit 技术等精心设计了一套自保护机制。国外的信息安全专家称，震网病毒具备高端性，其背后有强大的技术支撑和财政支持。

（3）面向物理隔离的内部网络的攻击。一般情况下，工业控制系统所在的内部网络是与互联网物理隔离的。为了攻击这种内部网络中的工业控制系统，震网病毒设计者专门设计了通过 U 盘向内部网络进行“摆渡”的传播方式，以感染物理隔离的内部网络，最终达到攻击工业控制系统的目的。

震网病毒是高级持续性威胁（Advanced Persistent Threat，APT）的典型代表，通过对特定目标的网络环境及软件和硬件系统的刺探分析，寻找可能被利用的安全漏洞和脆弱性，针对这些安全漏洞和脆弱性设计系统攻击方案和流程，将多种攻击手法组合成更复杂的攻击方式，对特定目标进行长时间、持续的攻击，攻击成功率很大，具有更大的危害性。

当前计算机病毒具有如下特点。

（1）计算机病毒通过钓鱼网站、游戏网站、黄色网站、P2P 网络及电子邮件等媒介进行传播，其传播速度更快，感染范围更广。

（2）计算机病毒越来越多地利用系统安全漏洞，尤其是 Windows 系统平台安全漏洞，波及面非常广。

（3）计算机病毒采用多种手法来隐藏自己，试图避开防病毒软件的检测和杀除。

（4）计算机病毒攻击与网络攻击手段紧密结合，使计算机病毒具有更大的破坏力和危害性。

（5）计算机病毒种类越来越多，传播途径多样化，传播速度更快，破坏性增大，并呈现无国界的态势。

针对网络时代的计算机病毒特点，必须采取有效的防病毒措施。全方位地建立全面的计算机病毒防范和监测体系，做到防“毒”于未然。

计算机病毒主要采用防病毒软件来防范。从目前的防病毒软件来看，一般都采取被动杀毒和主动防毒相结合的策略，将静态扫描杀毒和实时监控杀毒有机结合起来。静态扫描杀毒功能能够查杀各种已知病毒，但不具备防范病毒功能，只能被动地杀毒。实时监控杀毒功能将动态地监测计算机用户操作，包括上网浏览、接收电子邮件、打开网络文件、插入移动盘等，在这些操作过程中能够动态检测和查杀病毒，防止系统被病毒感染，这是主动的防病毒措施，从而提高了计算机病毒检测和查杀能力。

目前，市场上的防病毒软件产品有很多种，包括单机版防病毒软件、网络版防病毒软件及基于云计算的防病毒系统等。用户在使用计算机上网时必须安装被市场广泛认可的防病毒软件，并且要及时升级软件版本和更新病毒模式库，防范新病毒的入侵和破坏。

1.3.2　特洛伊木马

特洛伊木马（简称木马）也是一种恶意程序，木马程序具有短小精悍、隐蔽性强、技术含量高等特点，与计算机病毒不同的是，木马程序一般不具有传播功能，很少破坏计算机系统。

攻击者通过各种手段将木马程序植入目标计算机，使目标计算机成为受控主机，然后通过控制台对受控主机进行远程控制和信息获取，并通过代理服务器将控制台隔离保护起来，难以从受控主机追踪到控制台，图 1-1 所示为木马系统工作模型。

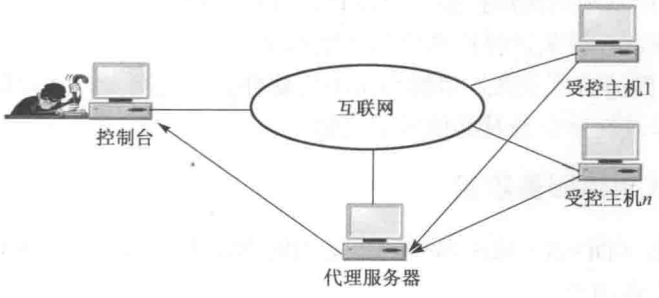

图 1-1　木马系统工作模型

对目标计算机实施木马攻击的首要条件是将木马程序悄然植入目标计算机。常用的植入技术手段有渔叉式攻击、诱骗式攻击、利用预留后门等，一般需要利用系统安全漏洞。

（1）渔叉式攻击：将木马程序隐藏在各种文件中，通过电子邮件等方式定向传送给目标用户，引诱目标用户点击，进而在所使用的计算机上植入木马程序。

（2）诱骗式攻击：将木马程序隐藏在 Web 网页文件、FTP 文件、图片文件或其他文件中，引诱目标用户点击访问，进而在所使用的计算机上植入木马程序。

（3）利用预留后门：利用预留在计算机上的系统后门植入木马程序。

在目标计算机开机启动时，木马程序随系统进程加载而自动激活运行。木马程序激活后，主动向外发出连接请求（即反向连接），与控制台建立网络连接。这时目标计算机便受控于控制台，等待执行控制台命令，并返回执行结果。

一般的木马程序都具有如下基本功能：

（1）远程操作受控主机文件（上传/下载/删除/修改）；

（2）远程获取受控主机键盘记录；

（3）远程获取受控主机当前屏幕；

（4）远程获取受控主机系统信息和窗口信息；

（5）远程操作受控主机注册表；

（6）远程操作受控主机服务与进程；

（7）远程关闭和锁定受控主机等。

木马程序比较健壮，采用了隐蔽隐身、防火墙穿透、追踪隔离、抗查杀保护等技术，具有难发现、难阻断、难追踪、难清除等特点。

木马程序是一种利用互联网窃取敏感信息的重要工具，网络间谍主要采用对目标计算机进行定点式植入，利用木马程序有预谋地窃取国家政治、国防和经济等方面的情报，危及国家安全和利益。网络黑客主要采用“广种薄收”式植入，甚至利用病毒传播机制来传播和植入木马程序，窃取个人网银账号、用户口令等个人隐私信息及企业内部信息，对个人和企业带来财产和信誉等方面的损失。

因此，木马程序具有更大的危害性，必须增强木马防范意识。

（1）坚持“上网不涉密，涉密不上网”的基本原则，绝不能在上网的计算机上处理涉密信息，防止涉密信息被植入的木马窃取。

（2）增强信息安全意识，提高木马防范技能。

① 加强防护：在计算机上必须安装防病毒软件，并及时更新病毒库和升级软件版本，增强计算机系统的防护能力。

② 堵住漏洞：经常利用漏洞扫描工具检查计算机上可能存在的系统安全漏洞，并及时安装补丁程序来修补漏洞，提高计算机系统的健康水平。

③ 谨防陷阱：提倡绿色上网，审慎点击不明邮件、不良网页、共享软件等，不放过任何可疑的网络连接、系统提示信息及其他异常现象。

1.3.3 分布式拒绝服务攻击

分布式拒绝服务（DDoS）攻击是一种常见的网络攻击技术，能迅速导致被攻击网站服务器系统瘫痪、网络服务中断。

DDoS 攻击通过产生大量虚假的数据包来耗尽网络系统的资源，如 CPU 时间、内存和磁盘空间、