

<<计算机安全>>

图书基本信息

书名：<<计算机安全>>

13位ISBN编号：9787505386006

10位ISBN编号：750538600X

出版时间：2003-7

出版时间：电子工业出版社

作者：朱海林

页数：208

字数：333

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<计算机安全>>

书籍目录

第1章 计算机系统的安全性1.1 计算机犯罪及其法律责任1.1.1 计算机犯罪概念1.1.2 计算机犯罪的手段与特点1.1.3 有关计算机安全的法律、法规与法律责任1.2 计算机系统的安全性1.2.1 计算机系统安全性的构成1.2.2 加强信息安全, 迎接时代挑战第2章 计算机病毒概述2.1 计算机病毒的发生和发展2.1.1 计算机病毒的起源2.1.2 计算机病毒的发展历史2.2 计算机病毒的定义2.2.1 计算机病毒的定义2.2.2 计算机病毒的特点2.3 计算机病毒的分类2.4 计算机病毒的构成2.4.1 计算机病毒的基本模块2.4.2 计算机病毒的引导机制2.4.3 计算机病毒的传染机制2.4.4 计算机病毒的表现和破坏机制2.5 计算机病毒的检测与防范2.5.1 计算机病毒的检测2.5.2 计算机病毒的清除2.5.3 计算机病毒的预防思考题第3章 典型计算机病毒分析3.1 大麻病毒3.1.1 大麻病毒的表现症状3.1.2 大麻病毒的工作原理3.1.3 大麻病毒的防治3.2 米开朗基罗病毒3.2.1 “米氏”病毒的特点3.2.2 病毒的作用机制3.2.3 诊治3.3 磁盘杀手病毒3.3.1 病毒的工作原理3.3.2 病毒的检测和消除3.4 黑色星期五病毒3.4.1 黑色星期五病毒的特点3.4.2 病毒的工作原理3.4.3 病毒的诊治3.5 DIR-2病毒3.5.1 DIR-2病毒的作用机制3.5.2 DIR-2病毒的检测和消除3.6 新世纪病毒3.6.1 新世纪病毒的作用机制3.6.2 新世纪病毒的检测和清除3.7 宏病毒3.7.1 宏病毒作用机制3.7.2 宏病毒的检测和清除3.7.3 典型宏病毒3.8 CIH病毒3.9 网络计算机病毒3.9.1 网络计算机病毒的传播方式3.9.2 网络计算机病毒的特点3.9.3 网络计算机病毒的预防3.9.4 几种网络计算机病毒3.9.5 “爱虫(I Love you)”病毒代码解析和杀毒方法3.9.6 欢乐时光(happy time,help.script)3.10 新一代计算机病毒3.10.1 变形多态病毒3.10.2 Retro病毒3.10.3 “红色代码”病毒(Code red,Code redII)3.10.4 蓝色代码(CodeBlue)病毒3.10.5 尼姆达病毒(Worms.Nimda)思考题第4章 密码学概论4.1 信息加密的基本概念4.2 古典密码学4.2.1 单表代换密码4.2.2 多表代换密码4.2.3 多字母代换密码4.3 Shannon理论4.3.1 信息量和熵4.3.2 完善保密性4.3.3 实际保密性4.5 序列密码4.5.1 序列密码加密方式分类4.5.2 密钥流的生成4.5.3 混沌密码4.6 量子密码思考题第5章 加密算法5.1 分组密码5.1.1 分组密码设计原则5.1.2 分组密码中的常用函数和S盒设计5.2 DES算法和Rijndael算法5.2.1 数据加密标准DES算法5.2.2 新一代分组迭代加密算法——Rijndael算法5.3 分组密码的工作方式5.4 密码攻击方法5.4.1 典型密码攻击5.4.2 差分密码分析法5.4.3 线性攻击5.5 双钥密码体制5.5.1 双钥密码体制概述5.5.2 RSA密码体制5.5.3 ElGamal密码体制5.5.4 椭圆曲线体制5.6 概率加密和零知识证明5.6.1 概率加密5.6.2 零知识证明思考题第6章 密码应用6.1 数字签名协议6.1.1 RSA签名体制6.1.2 数字签名标准6.1.3 几个特殊的数字签名6.2 Hash函数6.2.1 生日攻击6.2.2 MD5算法6.2.3 SHA算法6.3 身份识别协议6.3.1 Schnorr身份识别方案6.3.2 Okamoto身份识别方案6.3.3 Guillou-Quisquater身份识别方案6.3.4 基于身份的身份识别方案6.4 CA与数字证书6.4.1 CA的基本概念6.4.2 申请签发证书流程6.4.3 申请撤销证书流程6.5 公开密钥基础设施6.5.1 证书的类型以及所包含的内容6.5.2 CA、证书主体、证书用户的关系6.5.3 CA的排列6.5.4 强身份认证和不可否认6.5.5 X.思考题第7章 网络攻击与防范7.1 网络攻击的概念7.1.1 网络的安全漏洞7.1.2 网络攻击与原因7.2 黑客攻击7.2.1 黑客的界定7.2.2 黑客攻击策略7.2.3 黑客攻击技术7.3 防火墙7.3.1 防火墙技术7.3.2 防火墙的体系结构及组合形式7.3.3 防火墙的局限性7.4 入侵检测7.4.1 入侵检测的过程与技术7.4.2 入侵检测系统分类7.4.3 入侵检测系统的选择和评价7.5 网络安全防护7.5.1 多层次网络安全防护7.5.2 网络安全策略思考题第8章 Web安全8.1 Web安全分析8.1.1 Web安全威胁8.1.2 Web攻击类型8.2 Web安全维护8.2.1 网络安全协议8.2.2 Web服务系统安全维护8.3 Web客户端安全防范8.3.1 Java和Java Applet8.3.2 ActiveX8.3.3 脚本语言(Scripting Language)8.3.4 Cookie8.3.5 浏览器的安全问题8.4 Web服务器安全防范8.4.1 CGI安全8.4.2 ASP和JSP8.4.3 Web服务器安全管理8.5 电子商务安全8.5.1 电子商务信息安全8.5.2 电子商务信息安全典型方法8.5.3 安全套接字层SSL8.5.4 安全电子交易SET思考题

章节摘录

3.3.2病毒的检测和消除对磁盘杀手的检测比较方便，无论是软盘还是硬盘都可以借助于像Pctools和Debug等工具软件直接观察引导扇区内容，进行比较即可。

清除软盘中的病毒的方法是：从引导扇区中的病毒程序处找出存放原引导扇区内容在盘上的相对扇区号，进而读出正常引导扇区内容并写回引导扇区，然后把坏簇标志改为可用簇。

清除硬盘中病毒的方法是借助工具软件从隐含扇区的最后一个扇区中读出引导记录并写回到引导扇区，即可清除病毒。

3.4黑色星期五病毒黑色星期五病毒从字面上理解不难看出它一定与星期五有关。

那何为黑色呢？

黑色指的就是13日。

这种病毒在13日且又是星期五时发作，删除磁盘上的所有被执行文件。

由于在西方13是一个不吉利的数字，因此对于既是13日又是星期五，就称为黑色星期五。

最初这种病毒出现在以色列希伯莱大学，故也称为希伯莱病毒。

因为该大学位于耶路撒冷，又称为耶路撒冷病毒。

3.4.1黑色星期五病毒的特点黑色星期五病毒是一种流行广且危害很大的恶性病毒。

它是一种文件型病毒，传染对象是后缀为COM和EXE的可执行文件。

已感染病毒的.com文件，病毒程序位于最前端，而对于.exe文件则位于文件的后面。

但当运行含有病毒的文件时，最先运行的总是病毒程序，且首先获得系统的控制权。

感染黑色星期五病毒的文件属性和建立日期是不变的。

对于后缀是COM的文件，只感染一次，使其增加1813个字节，且病毒程序位于该文件的首部。

而对于后缀是EXE的文件，则可无限次的感染，其每次感染时都将病毒程序放在文件的尾部。

必须指出的是，病毒程序在对文件感染时，先是修改DOS的出错处理中断INT24H，从而使病毒的感染过程能悄悄地进行。

黑色星期五病毒的破坏分为两种。

一种是利用所截获的INT8H中断向量，在病毒程序内部设置计数器，当值为2时，在屏幕上显示“长方形”，若值为0时，则通过执行无用的字符循环程序来减慢系统速度。

另一种是日期和星期计数，当系统日历为13日且是星期五时，在系统中运行的EXE和COM文件就会被删除。

3.4.2病毒的工作原理黑色星期五病毒包含三个模块：引导模块、传染模块和表现/破坏模块。

运行受感染的文件时，病毒程序首先运行，对于尚未感染该病毒的系统，它将修改系统的INT21H

和INT8H中断向量，使其指向病毒的传染模块和表现破坏模块，并把病毒程序（约1.8KB）移到内存某个地方驻留。

在完成把自身引导驻留在内存的工作后才去执行原来的可执行文件。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>