第一图书网, tushu007.com

<<计算机病毒原理与防治技术>>

图书基本信息

书名：<<计算机病毒原理与防治技术>>

13位ISBN编号：9787560966366

10位ISBN编号：7560966365

出版时间：2010-11

出版时间：华中科技大学出版社

作者：韩兰胜 编

页数：241

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

内容概要

本书分为基础篇、防治篇、提高篇和实验篇。
基础篇介绍了计算机病毒的概念、基本原理，详细阐述了病毒的自我复制、感染和传播机制，其中还包括蠕虫、木马和移动设备病毒的基本原理。
防治篇讲述了计算机病毒的检测、清除技术及当前处于发展中的一些检测和防治办法。
提高篇从机器、整体网络宏观的角度，讲述了计算机病毒的计算特性、传播模型和病毒的危害性测量。
本书对病毒原理的讲解细致而具体，对防治技术的讲解具体而又可操作，实验部分侧重具体技术的实现。
本书既注重基本原理的细致讲解，又能从宏观角度来把握病毒的规律，从发展的观点看待病毒新变化，对读者有一定的启示。

本书适合信息安全专业的本科生、研究生的教学，也可作为广大的计算机专业人士深入了解计算机病毒的参考用书。

书籍目录

基础篇
第1章 计算机病毒的概念
1.1 计算机病毒的由来及定义
1.2 计算机病毒分类及命名
1.3 计算机病毒的基本性质及特点
1.4 本章小结
第2章 计算机病毒的构造机制
2.1 计算机病毒的自我复制
2.2 计算机病毒的感染机制
2.3 计算机病毒的传播机制
2.4 计算机病毒的伪装及变种机制
2.5 本章小结
第3章 计算机病毒与生物病毒
3.1 生物病毒的相关概念
3.2 计算机病毒与生物病毒的相似性
3.3 计算机病毒与生物病毒的差异
3.4 本章小结
第4章 网络病毒
4.1 网络病毒的概念
4.2 网络蠕虫
4.3 木马
4.4 无线网络设备病毒
4.5 本章小结
防治篇
第5章 计算机病毒的防治技术
5.1 病毒检测技术
5.2 基于特征码的计算机病毒检测
5.3 计算机病毒的清除技术
5.4 本章小结
第6章 计算机病毒的行为检测技术
6.1 基于行为检测的背景
6.2 病毒的行为特征
6.3 行为特征集的构建
6.4 基于SVM的行为检测模型
6.5 实验与性能分析
6.6 本章小结
第7章 网络环境下的病毒防治
7.1 网络蠕虫的检测与抑制办法
7.2 木马的检测与防治技术
7.3 网络病毒的清除
7.4 网络环境中的病毒免疫策略
7.5 网络环境下病毒的隔离策略
7.6 本章小结
提高篇
第8章 计算机病毒的传播模型

8.1 传统反病毒技术的不足
8.2 主要的生物病毒传播模型
8.3 当前计算机病毒传播模型
8.4 几个蠕虫病毒传播模型
8.5 当前计算机病毒传播模型中的问题
8.6 本章小结
第9章 计算机病毒传播模型及其相关问题
9.1 通用计算机病毒传播模型....
9.2 普通网络环境下计算机病毒的门限值
9.3 邮件病毒的迭代模型
9.4 计算机病毒的求源模型
9.5 本章小结
第10章 计算机病毒的逻辑模型及危害测量
10.1 早期不具备存储功能的图灵机逻辑模型
10.2 基于图灵机的病毒抽象理论
10.3 具有存储功能的图灵机逻辑模型
10.4 基于递归函数的计算机病毒的模型
10.5 计算机病毒的危害性评估
10.6 本章小结
实验篇
第11章 计算机病毒原理及防治技术实验
11.1 单机病毒原理实验
11.2 远端进程嵌入式木马程序的设计
11.3 基于特征码的病毒查找算法的设计
11.4 病毒传播模型仿真实验
参考文献
编后语

章节摘录

版权页：插图：8.按照寄生方式和传染途径分类人们习惯于将计算机病毒按寄生方式和传染途径来分类。
计算机病毒按其寄生方式大致可分为以下两类。
（1）引导型病毒引导型病毒是一种在执行ROM BIOS之后，系统引导时出现的病毒，它先于操作系统运行，依托的环境是BIOS中断服务程序。
引导型病毒利用操作系统的引导模块放在某个固定的位置，并且控制权的转交方式是以物理位置为依据，而不是以操作系统引导区的内容为依据，因而病毒占据该物理位置即可获得控制权，而将真正引导区的内容转移或替换，待病毒程序执行后，将控制权交给真正的引导区内容，使得这个带病毒的计算机系统看似正常运转，而病毒已隐藏其中，并伺机发作、传染。
引导型病毒按其寄生对象的不同又可分为两类，即MBR（主引导区）病毒、BR（引导区）病毒。
MBR病毒也称为分区病毒，将病毒寄生在硬盘分区主引导程序所占据的硬盘0头0柱面第1个扇区中。
典型的病毒有大麻、2708、INT60病毒等。
BR病毒是将病毒寄生在硬盘逻辑0扇或软盘逻辑0扇（即0面0道第1个扇区）。
典型的病毒有Brain、小球病毒等。
引导型病毒的主要特征如下。
①引导型病毒在安装操作系统之前进入内存，寄生对象又相对固定，因此该类病毒基本上不得不采用减少操作系统所掌管的内存容量方法来驻留内存高端。
而正常的系统引导过程一般是不减少系统内存的。
②引导型病毒需要把病毒传染给软盘，一般是通过修改INT13H的中断向量，而新INT13H中断向量段址必定指向内存高端的病毒程序。
③引导型病毒感染硬盘时，必定驻留硬盘的主引导扇区或引导扇区，并且只驻留一次，因此引导型病毒一般都是在软盘启动的过程中把病毒传染给硬盘的。
而正常的引导过程一般不对硬盘主引导区或引导区进行写盘操作。
④引导型病毒的寄生对象相对固定，把当前的系统主引导扇区和引导扇区与干净的主引导扇区和引导扇区进行比较，如果内容不一致，可认定系统引导区异常。

编辑推荐

《计算机病毒原理与防治技术》是由华中科技大学出版社出版的。

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