重点大学信息安全专业规划系列教材

恶意代码与计算机病毒

——原理、技术和实践

刘功申　孟魁　编著

清华大学出版社

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒

——原理、技术和实践

刘功申 孟魁 编著

清华大学出版社

内 容 简 介

本书详细介绍了恶意代码(含传统计算机病毒)的基本原理和主要防治技术,深入分析和探讨了恶意代码的产生机理、寄生特点、传播方式、危害表现以及防范和对抗等方面的技术。本书主要内容包括恶意代码概述、恶意代码模型及机理、传统计算机病毒、宏病毒、特洛伊木马、Linux 恶意代码技术、蠕虫、移动智能终端恶意代码、其他恶意代码、恶意代码防范技术、常用杀毒软件及其解决方案、恶意代码防治策略。

本书通俗易懂,注重理论与实践相结合,所设计的教学实验覆盖了所有类型的恶意代码,使读者能够举一反三。为了便于教学,教材附带教学课件、实验用源代码以及辅助应用程序版本说明等内容,下载地址为 www.tup.com.cn。下载并解压缩后,就可按照教材设计的实验步骤使用。

本书可作为高等院校信息安全专业和计算机相关专业的教材,也可作为广大系统管理员、计算机安全技术人员的参考书。

图书在版编目(CIP)数据

恶意代码与计算机病毒:原理、技术和实践/刘功申,孟魁编著.--北京:清华大学出版社,2013
重点大学信息安全专业规划系列教材
ISBN 978-7-302-33592-4

Ⅰ.①恶… Ⅱ.①刘… ②孟… Ⅲ.①电子计算机-安全技术-高等学校-教材 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2013)第 203896 号

责任编辑:魏江江 王冰飞
封面设计:常雪影
责任校对:焦丽丽
责任印制:杨 艳

出版发行:清华大学出版社
网 址:http://www.tup.com.cn, http://www.wqbook.com
地 址:北京清华大学学研大厦 A 座 邮 编:100084
社 总 机:010-62770175 邮 购:010-62786544
投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn
质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn
课 件 下 载:http://www.tup.com.cn,010-62795954
印 装 者:北京国马印刷厂
经 销:全国新华书店
开 本:185mm×260mm **印 张**:20.25 **字 数**:490 千字
版 次:2013 年 11 月第 1 版 **印 次**:2013 年 11 月第1次印刷
印 数:1~2000
定 价:39.00 元

产品编号:041399-01

INTRODUCTION

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

（1）反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

（2）反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点。规划教材建设把重点放在专业核心（基础）课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

（4）支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

（5）依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

重点大学信息安全专业规划系列教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

FOREWORD

前言

恶意代码作为信息安全领域的重要一环，近年来在军事战争、社会稳定方面发挥了双刃剑的作用，引起了社会各界的广泛重视。

传统的计算机病毒是一个非常狭义的定义，它仅仅概括了感染文件（可执行文件及数据文件）和引导区的恶意代码，无法描述各种新兴恶意代码的特征和内涵。鉴于此，本书采用“恶意代码”这个概念来概括书中内容。

本书的主要内容来源于作者所在大学本科计算机病毒和恶意代码7年教学经验、5年研发基础，以及前期编写的3本教材。本书的前身《计算机病毒及其防范技术》、《计算机病毒及其防范技术（第2版）》和《恶意代码防范》被多所高校作为教材，得到了大家的认可。同时，这些教材也获得了“上海交通大学优秀教材特等奖”、“上海市高等教育教材一等奖”。

本书重点分析恶意代码的运行机制，并通过实验的方式讲解常见恶意代码。在分析恶意代码技术的基础上，重点分析恶意代码的检测和清除技术。此外，还对预防恶意代码的策略和防治方案进行了探讨。全书共分12章，具体内容如下。

第1章恶意代码概述，主要介绍恶意代码的基本概念，并在此基础上讲述恶意代码的关键历史转折点、技术分类、传播途径、感染症状、命名规则及未来发展趋势等相关问题。

第2章恶意代码模型及机理，主要介绍恶意代码的理论模型，如基于图灵机、递归函数和传染病的数学模型，恶意代码的预防理论模型，传统计算机病毒的结构及工作机制等。

第3章传统计算机病毒，主要介绍在DOS、Windows 9x、Windows 2000平台下传统病毒的工作机制和编制技术，并以3种平台下的可执行文件结构为线索，在分析这些文件结构的基础上，引入不同平台的病毒编制技术。为了保证教材的系统性，本章还简要介绍了引导型病毒。

第4章宏病毒，以Microsoft Word宏病毒为主线介绍宏病毒的基本概念、作用机制、宏病毒实验和防范方法等内容。

第5章特洛伊木马，为了使读者充分了解特洛伊木马，本章详细分析了木马的技术特征、木马入侵的一些常用技术以及木马入侵的防范和清除方

法。此外，还对几款常见木马程序的防范经验做了较为详细的说明。

第6章 Linux恶意代码技术，在了解Linux安全问题的基础上，探讨了Linux恶意代码的概念，分析了Linux可执行文件格式(ELF)的运行机理。本章还精心设计了两个实验，以直观的方式分别讲解了Linux操作系统的恶意脚本和感染ELF格式文件的病毒原理。

第7章蠕虫，主要介绍近年来破坏力非常大的蠕虫(Worm)的基本特征、技术特征和工作机理，并且详细介绍了基于RPC漏洞和U盘传播的蠕虫技术。

第8章移动智能终端恶意代码，以手机恶意代码为主线，介绍移动终端恶意代码的概念、技术进展和防范工具，使读者了解未来移动终端设备上的威胁。特别是详细介绍了Android下开发恶意行为程序的技术。

第9章其他恶意代码，对近年来新兴的流氓软件、Outlook漏洞恶意代码、Webpage恶意代码、僵尸网络和Rootkit恶意代码做了介绍，并对其中典型恶意代码的编制技术做了详细讲解。

第10章恶意代码防范技术以检测、清除、预防、免疫、防范策略、备份及恢复6个层次为主要思路，介绍恶意代码的诊断原理和方法、清除原理和方法、主动和被动防治技术以及数据备份和数据恢复等。

第11章常用杀毒软件及其解决方案，通过介绍企业网络的典型结构、典型应用和网络时代的病毒特征，得出企业网络防恶意代码体系对技术和工具的需求，从而给出一些典型恶意代码防治体系解决方案。

第12章恶意代码防治策略，通过讨论防御性策略得到的不同建议，来避免计算机受到恶意代码的影响。本章侧重于全局策略和规章，并且针对企业用户所讲述的内容比针对单机用户的要多一些。本章还就如何制订一个防御计划、如何挑选一个快速反应小组、如何控制住恶意代码的发作，以及安全工具的选择等问题提出了一些建议。

在本书完稿之际，作者对上海交通大学教材出版基金的资助表示衷心感谢；感谢教学7年来听过作者计算机病毒原理和恶意代码防范课程的所有学生，他们为作者的讲义提出了很多宝贵意见；感谢各类参考资料的提供者，这些资料既充实了作者的教材，也丰富了作者的知识；感谢清华大学出版社的各位编辑，他们耐心地加工我的书稿；感谢我的妻子和孩子，该书稿的完成离不开家人的默默支持。

为便于教学，本教材提供教学课件和实验用源代码，可通过http://www.tup.com.cn下载。作者在教学资源网站(http://scholar.eastday.com)上提供最新资源索引，敬请参考。

由于水平有限，书中难免有疏漏之处，恳请读者批评指正，以使本书得以进一步改进和完善。

作　者

2013年8月于上海交通大学思源湖畔

参考文献

[1] Scott K. Jones, Clinton E. White, Jr. The IMP model of computer virus management, Computers and Security[J], Volume 9, Issue 5 (August 1990): 411-418.

[2] 郑辉. Internet 蠕虫研究[D]. 天津：南开大学，2003.

[3] 张友生，米安然. 计算机病毒与木马程序剖析[M]. 北京：北京科海电子出版社，2003.

[4] 吴万铎. 计算机病毒的分析诊断与防治[M]. 北京：海洋出版社，1993.

[5] 崔广才，孙文生. 计算机病毒及其防治基础[M]. 长春：吉林科学技术出版社，1994.

[6] 张小磊. 计算机病毒诊断与防治[M]. 北京：中国环境科学出版社，2003.

[7] David Harley, Robert Slade, Urs E. Gattiker 著. 计算机病毒揭秘[M]. 朱代祥译. 北京：人民邮电出版社，2002.

[8] Edina Arslanagic. A Personal Firewall in Mobile Phone[D]. Faculty of Engineering and Science, Agder Unibersity College, 2004. 5.

[9] 李晓丽. 手机病毒的分析及对策研究[D]. 武汉大学计算机学院，2004. 11.

[10] 程胜利，谈冉，熊文龙，等. 计算机病毒及其防治技术[M]. 北京：清华大学出版社，2004.

[11] Roger A. Grimes 著. 恶意传播代码——Windows 病毒防护[M]. 张志斌，贾旺盛译. 北京：机械工业出版社，2004.

[12] 傅建明，彭国军，张焕国. 计算机病毒分析与对抗[M]. 武汉：武汉大学出版社，2005.

[13] 韩筱卿，王建锋，钟玮，等. 计算机病毒分析与防范大全[M]. 北京：电子工业出版社，2006.

[14] 《黑客防线》编辑部. 黑客防线 2006 精华奉献本(上、下册)[M]. 北京：人民邮电出版社，2006.

[15] Excutable and Linkable Format (ELF) Specification Version 1. 2[M]. TIS Committee. May 1995.

[16] Alexander Bartolich. The ELF Virus writing HOWTO[M]. 2003.

[17] 刘功申，张月国，孟魁. 恶意代码防范[M]. 北京：高等教育出版社，2010.

CONTENTS

目录

CHAPTER 1

恶意代码概述 第1章

随着信息技术、互联网技术，特别是信息安全技术的发展，计算机病毒的概念越来越不能全面反映其内涵了，恶意代码的概念被适时地提出，并逐渐为人们接受和使用。随着恶意代码技术的发展，恶意代码的数量也在迅速增加。卡巴斯基实验室声称，至2008年底，全球大约有1 400 000种不同形式的恶意代码。2011年，安天实验室共捕获新增恶意代码11 532 980个，其数量是2007年的9倍。德国杀毒厂商G Data的安全实验室报道，恶意代码的数量在2011年底估计达到250万的新高。究竟有多少恶意代码存在于世，这是个不可解问题！

为什么会提出恶意代码的概念？恶意代码和计算机病毒究竟有怎样的关系？恶意代码究竟包含哪些内容？恶意代码是怎样一步一步从无到有发展壮大的？请读者带着这些问题来阅读本章内容。

本章主要介绍恶意代码的基本概念，并在此基础上介绍恶意代码的发展历史、分类、传播途径、感染症状、命名规则及未来发展趋势等相关问题。

本章学习目标：

- 明确恶意代码的基本概念；
- 了解恶意代码的发展历史；
- 熟悉恶意代码的种类；
- 熟悉恶意代码的命名规则；
- 了解恶意代码的未来发展趋势。

1.1 恶意代码的产生

国务院颁布的《中华人民共和国计算机信息系统安全保护条例》，以及公安部出台的《计算机病毒防治管理办法》将计算机病毒均定义为：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，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

我国刑法规定，故意制作、传播计算机病毒等破坏性程序，影响计算机系

统正常运行，后果严重的，依照破坏计算机信息系统罪定罪处罚。而在互联网中流行的蠕虫、木马是否属于刑法上的计算机病毒等破坏性程序，目前还没有立法或者司法解释。而根据上述有关计算机病毒的定义，感染文件的普通病毒属于计算机病毒，但是蠕虫（部分）、木马（绝大部分）并不进行自我复制，因此不符合病毒的特征，不属于计算机病毒，而它的危害性却是巨大的，因为它包含能够在触发时导致数据丢失甚至被窃的恶意代码。

有关专家认为，如果根据相关部门发布的条例来理解，将蠕虫和木马解释为计算机病毒是不符合刑法定罪原则的，而蠕虫和木马是否属于“计算机病毒等破坏性程序”，我国法律没有对此做出解释。蠕虫和木马的大量出现对刑法的部分规定提出了挑战，对刑法规定的破坏性程序必须做出明确的界定。由此可见，网络恶意代码技术的发展，导致刑法在这方面的规定显现滞后。因此，必须通过立法将木马、蠕虫等恶意代码纳入破坏性程序范围。

在美国，有些州（如加利福尼亚、西弗吉尼亚等）的地方法规中，把恶意代码解释成计算机系统的污染物。显然，它们的法律适用面更加宽泛。

在信息安全技术领域，重新审视目前流行的破坏性程序，有很多已经不能用“计算机病毒”这个概念来解释了。以下从两个方面进一步说明。

（1）就恶意代码的类型而言，这些破坏性程序除了木马之外，还有网络僵尸、流氓软件、逻辑炸弹、网络钓鱼、恶意脚本等。

（2）就感染平台而言，传统的计算机病毒的定义仅仅局限于计算机平台，而今后必将流行的智能手机恶意代码则运行于手机平台。关于手机上的恶意代码就不能简单地归类于传统的计算机病毒概念了。

在法律领域，专家们努力的方向是扩大法律解释范围，把新型的破坏性程序及时补充到法律条文中。在技术领域，专家们的责任更是责无旁贷，因此，需要一个新的概念来概括这些破坏性程序。这个新的概念就是“恶意代码”。

1.2 恶意代码的概念

Malware: Fighting Malicious Code 给出的恶意代码定义为：运行在目标计算机上，使系统按照攻击者意愿执行任务的一组指令。

在维基百科中，恶意代码的英文对照词是 Malware，也就是 Malicious Software 的混成词。恶意代码的定义描述为：恶意代码是在未被授权的情况下，以破坏软硬件设备、窃取用户信息、扰乱用户心理、干扰用户正常使用为目的而编制的软件或代码片段。这个定义涵盖的范围非常广泛，它包含了所有敌意、插入、干扰、讨厌的程序和源代码。一个软件被看作是恶意代码主要是依据创作者的意图，而不是恶意代码本身的特征。

依据这个定义，恶意代码将包括计算机病毒（Computer Virus）、蠕虫（Worm）、特洛伊木马（Trojan Horses）、Rootkits、间谍软件（Spyware）、恶意广告（Dishonest Adware）、流氓软件（Crimeware）、逻辑炸弹（Logic Boom）、后门（Back Door）、僵尸网络（Botnet）、网络钓鱼（Phishing）、恶意脚本（Malice Script）、垃圾信息（Spam）、智能终端恶意代码（Malware In Intelligent Terminal Device）等恶意的或讨厌的软件及代码片段。国际上目前新出现了一种以“扰乱用户心理”为目的的软件，也应该属于恶意代码范畴。由于这类软件的使用范