高等院校密码信息安全类专业系列教材

中国密码学会教育工作委员会推荐教材

软件安全

任 伟 编著

RUANJIAN ANQUAN

国防工业出版社
National Defense Industry Press

高等院校密码信息安全类专业系列教材
中国密码学会教育工作委员会推荐教材

软件安全

任伟 编著

国防工业出版社
·北京·

内 容 简 介

本书内容主要包括：软件安全概述、预备知识（介绍了 Windows API 编程简介、Win32 汇编语言程序设计、PE 文件格式布局及其装载的相关背景知识）、软件缺陷和漏洞、恶意代码分析、安全软件开发生命周期、软件体系安全分析、软件安全需求分析、安全编码、软件安全测试、软件保护以及软件安全的国际研究现状。

每章都给出小结归纳全章的内容，便于复习。每个章节都有扩展阅读的建议和参考文献，指导进一步的课外自主学习。每个章节还配备了习题可供读者自测和引申思考。部分打 * 号的内容具有一定深度，可以选学。本教材各部分内容既相互联系又相对独立，可依据教学对象的特点组织编排，方便读者根据需要进行选择。

本书可作为大学本科相关课程的教材，内容实用，也可供广大信息安全从业人员和爱好者自学之用。本书还有配套的书籍网站，提供电子版、教案（课件）以及相关参考文献的下载。

图书在版编目（CIP）数据

软件安全 / 任伟编著. —北京：国防工业出版社，2010.7

（高等院校密码信息安全类专业系列教材）

ISBN 978-7-118-06903-7

Ⅰ. ①软… Ⅱ. ①任… Ⅲ. ①软件开发-安全技术-高等学校-教材 Ⅳ. ①TP311.52

中国版本图书馆 CIP 数据核字（2010）第 115882 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号 邮政编码 100048）

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 14½ **字数** 322 千字

2010 年 7 月第 1 版第 1 次印刷 **印数** 1—3000 册 **定价** 30.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)68428422 发行邮购：(010)68414474

发行传真：(010)68411535 发行业务：(010)68472764

总　序

信息系统所面临的各种安全威胁日益突出，信息安全问题已成为涉及国家政治、军事、经济和文教等诸多领域的战略安全问题。我国政府对网络与信息安全问题高度重视，国办印发的文件《关于网络信任体系建设的若干意见》明确指出了要特别重视网络安全的6方面内容；中办、国办印发的《国家2006年至2020年长期科学发展规划》中也突出了对各种网络安全问题的关注，将建设国家信息安全保障体系列为我国信息化发展的战略重点；国家“十一五”计划中也包含了提升国家信息安全保障服务能力的战略要求。西方发达国家纷纷制订了本国的网络与信息安全战略。比如，美国奥巴马政府正在采取措施加强美国网络战的备战能力，其中一项措施是创建网络战司令部，这表明美国的网络与信息安全战略已经由克林顿时代的“全面防御”、布什时代的“攻防结合”，转到奥巴马时代的“攻击为主，网络威慑”。

当前，制约我国网络与信息安全事业发展的瓶颈之一就是人才极度匮乏，为此，教育部从2001年起，陆续批准了包括北京邮电大学在内的近百所各类高校开设信息安全本科专业。但是，毕竟与其他经典的本科专业相比，信息安全本科专业的建设问题还面临许多挑战，需要全国同行共同努力，早日探索出一条办好信息安全专业的捷径。可喜的是，现在国内若干高校的教授团队都纷纷行动起来，各尽所能在信息安全本科专业建设方面取得了不少业绩。比如，灵创团队（http://www.cleader.net）就是众多热心于信息安全本科专业建设的创新团队，该团队中的“信息安全教学团队”被教育部和财政部批准为“2009年度国家级教学团队”；其完成的成果“信息安全专业规范研究与专业体系建设”获得了国家级教学成果奖二等奖；其带头人也被评为“国家级教学名师”并受到了胡锦涛等党和国家领导人的接见。希望国内能够有更多的类似教学团队投身于信息安全本科专业建设。

由于教材建设是信息安全专业建设的重点和难点之一，中国密码学会教育工作委员会自成立以来就一直致力于推进密码学与信息安全方面的教学和教材建设，比如，与国防工业出版社联合主办了“密码学与信息安全教学研讨会”等一系列研讨活动，并成立“普通高等教育本科密码信息安全类系列教材”编审委员会来组织策划相关系列教材。编审委员会在充分研究信息安全本科专业规范的基础上，经过细致研究，多次反复讨论，规划了与信息安全本科专业规范相配套的本系列教材。

本系列教材参照荣获国家级教学成果奖的信息安全最新专业规范，确定教材题目，组织教材书稿内容。所有教材严格按照“规范”要求，结合信息安全专业的学制、培养规格、素质结构要求、知识结构要求撰写，使其所含知识点完全覆盖“规范”中的要求，确保能够达到“规范”中的学习目标。由于本系列教材涉及的内容比较多，在教材内容选择时，一

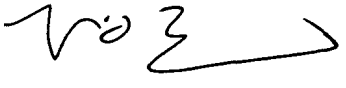
方面要考虑教材内容相互的衔接，另一方面要考虑许多课程相互之间有内容交叉的现象；同时，充分考虑了先进性和成熟性之间的和谐关系，确保教材既能够反映信息安全领域的前沿科研状态，又能使学生掌握基础的核心知识和较成熟稳定的技能；编审委员会多次召开会议，审定教材的大纲，落实教材的主要知识点，避免了内容的重复。

本系列教材的作者都是在我国信息安全领域具有丰富教学和实践经验的一流专家，部分教材已经被评为“普通高等教育‘十一五’国家级规划教材”。

为便于高校教师选用本套教材，我们将为高校教师提供完善的教学服务，免费为选用本套教材的教师提供所有教材的电子教案和部分教材的习题答案。同时我们还提供信息安全专业本科教学实验室建设方案与实验教学指导咨询和信息安全专业本科生实习、实训与技能认证咨询。

本系列教材尽管通过反复讨论修改，但限于作者水平和其他客观条件限制，难免存在不足和值得商榷之处，敬请批评指正。

教授　博士生导师　国家级教学名师
灾备技术国家工程实验室主任
网络与信息攻防教育部重点实验室主任
北京邮电大学信息安全中心主任



2009年9月30日星期三

高等院校密码信息安全类专业系列教材
编委会名单

前　言

本书是由中国密码学会教育工作委员会组织编写的信息安全专业系列教材之一，是一本严格按照信息安全专业最新专业规范的要求编写的适合信息安全专业本科生使用的教材。同时，该书也是国内第一本关于软件安全的高等学校教材。

目前全国有多所开办了信息安全专业的高等院校，“软件安全”是信息安全专业中一门重要的专业课，同时也是一门综合学科，其研究内容涉及到程序设计语言、编译原理、操作系统内核、软件工程、汇编语言程序设计等，需要综合应用这些课程的知识来研究和体会。同时，软件安全又是一门还不成熟的学科，它需要更多的研究者关注和发展，以及需要更多的实践者在工程实践中总结和论证。

软件安全一直是软件开发中的一个关键问题，开发安全性高的软件是软件开发人员必须追求的目标。开发人员如何在开发的全过程中从根本上提高软件的安全性，是每个软件人员（包括系统分析人员、项目经理、编码人员、测试人员等）必须思考的问题。但是，由于软件安全是一门新兴学科，国内并没有类似的教材，国外也只是在近几年才出现了几本相关的专著。

本书在写作的过程中遵循了以下思路：

（1）理解软件安全的内涵和外延。软件安全的概念其实并不是十分清晰，目前也没有统一的定义。因而第1章特别介绍了与软件安全相关的研究领域以示区别和联系，如软件工程、软件保证、软件质量、软件可靠性、软件容错及应用安全。

（2）预备知识的介绍。通过预备知识总结和回顾了全书需要的相关基础知识，包括Windows API编程、汇编语言程序设计、PE文件格式等基础知识。

（3）先从攻击者角度介绍软件的缺陷和漏洞产生的机理和防范措施，恶意代码的分类、特征和机理，以及防范措施，然后转到讲述如何通过软件开发的各个过程确保软件安全。

（4）将安全的考虑嵌入到软件开发的整个生命周期之中，包括软件体系安全分析、软件安全需求分析、安全编码、安全测试和软件保护。

（5）提供软件安全工具供实践中参考，并简要讨论软件安全研究的现状和研究热点问题。

本书系统地、循序渐进地介绍了软件安全的各个方面。全书共分11章：第1章对软件安全做一个概述；第2章给出了全书需要的预备知识；第3章对软件缺陷和漏洞进行了介绍；第4章介绍了恶意代码分析；第5章介绍了安全软件开发生命周期；第6章介绍了软件体系安全分析；第7章介绍了软件安全需求分析；第8章介绍了安全编码；第9章介绍了软件安全测试；第10章介绍了软件保护方面的知识；最后，第11章介绍了软件安全

的国际研究现状。

全书根据教学特点精心安排了示例。这些示例全部在 MinGW Studio 系统或 Visual C ++ 系统上运行通过并有正确的结果，结果附在程序之后。为加深读者对内容的理解，本书还提供了一些补充材料：用于复习每一章内容的复习题以及用于深化读者理解层次的思考题、继续阅读的书籍、论文以及网站。打 * 号的章节作为选学章节。

本书面向的主要对象包括从事软件开发工作的软件技术人员，从事软件漏洞分析的安全人员以及学习“软件安全”课程的高等院校信息安全、计算机科学、软件工程类专业本科高年级学生和研究生。

成书之中，研究生叶敏、刘宇靓协助翻译了部分英文资料，在此一并表示感谢。

由于作者水平有限、时间仓促，不足和疏漏之处在所难免，在此衷心希望读者提出意见和建议，不吝赐教。我的 E-mail 是：weirencs@ cug. edu. cn。

任 伟

2010 年 3 月 15 日于武汉南望山

目　录

第 1 章　软件安全概述 …… 1
1.1　软件的概念 …… 1
1.1.1　软件的定义 …… 1
1.1.2　软件的分类 …… 1
1.2　软件安全的概念 …… 2
1.3　软件安全的知识体系 …… 9
1.4　软件安全与其他相关领域的关系* …… 10
1.4.1　软件工程 …… 10
1.4.2　软件保证 …… 11
1.4.3　软件质量 …… 11
1.4.4　软件可靠性 …… 14
1.4.5　软件容错 …… 15
1.4.6　应用安全 …… 15
1.5　专有名称及定义 …… 16
1.6　软件安全工具简介 …… 19
1.6.1　反汇编器 …… 19
1.6.2　调试器 …… 21
1.6.3　反编译器 …… 24
1.6.4　系统监控工具 …… 24
1.6.5　修补和转储工具 …… 28
小结 …… 33
参考文献 …… 33
习题 …… 34
第 2 章　预备知识 …… 35
2.1　Windows API 编程简介 …… 35
2.1.1　Windows 应用程序的组成 …… 35
2.1.2　Windows API …… 35
2.1.3　Windows 编程的基本概念 …… 37
2.1.4　Win32 数据类型、句柄、命名法 …… 38
2.1.5　函数指针 …… 41
2.1.6　消息结构、类型与机制 …… 41
2.2　Win32 汇编语言程序设计简介 …… 48

2.2.1 80x86 处理器寄存器 …… 48
2.2.2 IA－32 指令系统 …… 50
2.2.3 Win32 汇编程序举例 …… 51
2.2.4 函数调用时栈的变化 …… 53
2.3 PE 文件格式布局及其装载 …… 60
2.3.1 PE 文件结构布局 …… 60
2.3.2 PE 文件中的地址概念 …… 61
2.3.3 PE 文件内存映射方法 …… 63
2.3.4 载入并执行 PE 文件的过程 …… 64
2.3.5 PE 文件执行时的内存布局 …… 65
小结 …… 66
参考文献 …… 66
习题 …… 66
第 3 章 软件缺陷和漏洞 …… 67
3.1 缺陷和漏洞简介 …… 67
3.1.1 缺陷和漏洞的定义 …… 67
3.1.2 软件缺陷存在的原因 …… 67
3.1.3 软件安全漏洞存在的原因 …… 68
3.2 软件漏洞产生的机理 …… 68
3.2.1 栈溢出漏洞 …… 69
3.2.2 堆溢出漏洞* …… 83
3.2.3 格式化串漏洞 …… 88
3.2.4 SQL 注入漏洞 …… 94
3.3 漏洞的分类 …… 95
小结 …… 96
参考文献 …… 96
扩展阅读建议 …… 97
习题 …… 97
研究参考题 …… 97
第 4 章 恶意代码分析 …… 98
4.1 恶意软件的分类和区别 …… 98
4.2 病毒的机理与防治 …… 100
4.2.1 病毒的定义 …… 100
4.2.2 病毒的分类 …… 101
4.2.3 文件型病毒的感染技术 …… 102
4.2.4 病毒的检测* …… 109
4.3 蠕虫的机理与防治 …… 112
4.3.1 蠕虫和病毒的区别及联系 …… 112
4.3.2 蠕虫的分类 …… 113

4.3.3 蠕虫与软件漏洞的关系 …… 113
4.3.4 蠕虫的基本结构 …… 114
4.3.5 蠕虫的工作方式 …… 115
4.3.6 蠕虫技术的发展 …… 115
4.3.7 蠕虫的防治与检测* …… 116
4.4 木马的机理与防治 …… 117
4.4.1 木马的定义 …… 117
4.4.2 木马的结构 …… 117
4.4.3 木马实施网络入侵的基本步骤 …… 118
4.4.4 木马的基本原理 …… 119
4.4.5 木马的传播方式 …… 120
4.5 其他恶意代码的机理 …… 120
4.5.1 移动代码 …… 120
4.5.2 广告软件和间谍软件 …… 121
4.5.3 粘人软件 …… 121
4.5.4 网页恶意脚本程序 …… 121
4.5.5 即时通信病毒 …… 121
4.5.6 手机病毒 …… 122
4.5.7 宏病毒 …… 123
4.6 恶意代码分析技术* …… 124
4.6.1 分析前的准备 …… 124
4.6.2 分析过程(脱壳与动态分析) …… 124
小结 …… 128
参考文献 …… 128
扩展阅读建议 …… 128
习题 …… 129
研究思考题 …… 129
第5章 安全软件开发生命周期 …… 130
5.1 软件开发生命周期概述 …… 130
5.1.1 软件过程 …… 130
5.1.2 软件生存周期 …… 131
5.2 传统软件开发生命周期* …… 132
5.3 安全软件开发生命周期 …… 135
5.4 其他安全软件开发生命周期模型 …… 136
5.4.1 微软可信计算安全开发生命周期 …… 137
5.4.2 安全软件开发的小组软件过程* …… 137
5.4.3 安全敏捷开发* …… 139
5.4.4 软件可信成熟度模型* …… 140
5.4.5 软件安全框架* …… 141

5.4.6 BSI 成熟模型* …… 143
小结 …… 144
参考文献 …… 144
扩展阅读建议 …… 144
习题 …… 144
研究思考题 …… 145
第 6 章 软件体系安全分析 …… 146
6.1 风险分析简介 …… 146
6.2 基于标准的风险分析 …… 147
6.2.1 NIST ASSET …… 147
6.2.2 CMU SEI 的 OCTAVE …… 147
6.2.3 信息系统审核与控制协会的 COBIT …… 147
6.3 STRIDE 模型 …… 148
6.3.1 STRIDE 威胁模型 …… 148
6.3.2 威胁建模的过程 …… 149
小结 …… 151
参考文献 …… 151
习题 …… 151
第 7 章 软件安全需求分析 …… 152
7.1 安全规则与规章简介 …… 152
7.1.1 OWASP 的 WASS …… 152
7.1.2 HIPPA …… 152
7.1.3 FISMA …… 153
7.2 软件安全原则 …… 154
7.3 软件安全相关标准 …… 160
7.4 安全需求工程 …… 161
7.4.1 安全需求的基本概念 …… 161
7.4.2 安全需求分析 …… 164
7.4.3 安全需求工程工具 …… 166
7.4.4 基于滥用和误用案例的安全需求 …… 166
小结 …… 167
参考文献 …… 167
习题 …… 167
研究思考题 …… 168
第 8 章 安全编码 …… 169
8.1 安全编码原则 …… 169
8.1.1 CERT 安全编码建议 …… 169
8.1.2 CERT C 语言的安全编码标准 …… 170
8.1.3 避免缓冲区溢出 …… 170

8.2 源代码审核 …… 173
8.2.1 源代码审核概述 …… 173
8.2.2 代码审核方面的工具 …… 174
8.3 二进制代码审核 …… 176
小结 …… 177
参考文献 …… 177
扩展阅读建议 …… 178
习题 …… 178
研究思考题 …… 178
第9章 软件安全测试 …… 179
9.1 传统软件测试方法回顾 …… 179
9.1.1 传统软件测试的类型 …… 179
9.1.2 软件测试的步骤 …… 179
9.2 软件安全测试简介 …… 182
9.2.1 安全测试的基本步骤 …… 183
9.2.2 软件安全测试与传统软件测试的差别 …… 183
9.2.3 软件安全测试的原则 …… 183
9.3 白箱、黑箱、灰箱测试 …… 184
9.3.1 白箱测试 …… 184
9.3.2 黑箱测试 …… 185
9.3.3 灰箱测试 …… 185
9.4 Fuzz 测试 …… 186
9.4.1 Fuzz 测试的步骤及其分类 …… 186
9.4.2 三种常见的 Fuzz 测试 …… 187
9.5 软件渗透测试* …… 189
9.5.1 软件渗透测试简介 …… 189
9.5.2 渗透测试工具及其使用 …… 189
9.6 基于风险分析的软件安全测试* …… 191
9.6.1 风险评估模型 …… 191
9.6.2 风险分析方法 …… 191
9.7 测试计划 …… 194
9.7.1 基于风险分析的测试时间安排 …… 194
9.7.2 测试计划举例 …… 194
小结 …… 196
参考文献 …… 196
习题 …… 196
研究思考题 …… 197
第10章 软件保护 …… 198
10.1 常见软件保护技术 …… 198

10.1.1 基于介质的保护 …… 198
10.1.2 序列号(注册码) …… 198
10.1.3 基于硬件的保护 …… 199
10.2 高级软件保护技术 …… 200
10.2.1 密码处理器 …… 200
10.2.2 数字水印技术 …… 201
10.2.3 可信计算 …… 202
10.2.4 软件即服务(SaaS) …… 203
10.3 反逆向技术* …… 203
10.3.1 逆向工程简介 …… 203
10.3.2 防御反编译——消除符号信息 …… 204
10.3.3 防御反汇编——代码混淆法 …… 205
10.3.4 防御反调试——添加反调试器代码 …… 206
小结 …… 208
参考文献 …… 208
习题 …… 209
第 11 章 软件安全的国际研究现状 …… 210
11.1 新的研究热点 …… 210
11.2 重要论文与书籍 …… 210
小结 …… 215
参考文献 …… 216
后记 …… 217

第1章 软件安全概述

本章从软件的概念开始介绍，引出软件安全的概念，并通过软件安全威胁的现状指明软件安全的重要性和应用价值，然后简介软件安全的知识体系，最后区分软件安全和其他相关领域的关系。

1.1 软件的概念

1.1.1 软件的定义

1983 年 IEEE 为软件下的定义是：计算机程序、方法、规则和相关的文档资料以及在计算机上运行时所需的数据。目前对软件通俗的解释为：

软件 = 程序 + 数据 + 文档资料

其中，程序是完成特定功能和满足性能要求的指令序列；数据是程序运行的基础和操作的对象；文档资料是与程序开发、维护和使用有关的图文资料。

1.1.2 软件的分类

对软件的类型进行必要的划分，根据不同类型的工程对象采用不同的安全方法是很有价值的，因此有必要从不同的角度讨论计算机软件的分类情况。

1. 按软件的功能分类

按软件的功能进行划分，软件可分为系统软件、支撑软件和应用软件三类，它们有如下的特点。

1）系统软件

系统软件是计算机运行的必不可少的组成部分，它与计算机硬件紧密配合，控制并协调计算机系统各个部件、相关的软件和数据高效地工作。例如，操作系统、设备驱动程序以及通信处理程序等。

2）支撑软件

支撑软件是协助用户开发软件的工具性软件，其中包括帮助程序人员开发软件产品的工具，也包括帮助管理人员控制开发进程的工具。例如，支持需求分析，支持设计，支持编码，支持测试等。

3）应用软件

应用软件是指在特定领域内开发，为特定目的服务的软件。目前，计算机已经成为大多数日常工作的必需工具，在很多应用领域都需要专门的软件支持，在这些种类繁多的应用软件中，商业数据处理软件所占比例最大，此外还有工程与科学计算软件、系统仿真软件、人工智能软件及各类办公自动化软件和信息处理软件等。

2. 按软件规模分类

按软件规模分类即按照开发软件所需的人力、物力、时间以及完成的源程序行数进行分类，可将软件分为微型、小型、中型、大型、甚大型、极大型6种，见表1.1所列。

表1.1 软件规模的分类

类 别	参加人员数	研制期限	产品规模(源程序行数)
微型	1	1周~4周	500行
小型	1	1月~6月	1000行~2000行
中型	2~5	1年~2年	5千行~5万行
大型	5~20	2年~3年	5万行~10万行
甚大型	100~1000	4年~5年	100万行以上
极大型	2000~5000	5年~10年	1000万行以上

3. 按软件工作方式分类

按照软件的工作方式，可以将软件划分为以下几种形式：实时处理软件、分时软件、交互式软件、批处理软件。

4. 按软件服务对象的范围分类

按软件服务对象的范围，可将软件分为面向部分客户的项目软件和面向市场的产品软件。

(1) 项目软件也称定制软件，是受某个特定客户(或少数客户)的委托，由软件开发机构在合同的约束下开发出来的软件。

(2) 产品软件是面向市场需求，由软件开发机构开发出来后直接提供给市场，或是为千百个用户服务的软件，如办公处理软件、财务处理软件和一些常用工具软件等。

1.2 软件安全的概念

根据ISO 8402的定义，安全性是“使伤害或损害的风险限制在可接受的水平内”。因此，软件的安全性是软件的一种内在属性。

软件安全(Software Security)是指：采取工程的方法使得软件在敌对攻击的情况下仍能够继续正常工作。即采用系统化、规范化、数量化的方法来指导构建安全的软件。

软件安全是一个相对较新的领域，直到2001年才出现了软件安全方面的著作以及学术课程，这说明开发人员、软件架构师、计算机科学家们才开始系统地思考如何构建安全的软件。这方面的实践准则还没有得到广泛的推广和普遍采用。

从风险分析的角度出发，软件安全是关于如何理解软件所引起的安全风险以及如何管理这些风险的学科。McGraw博士提出“使安全成为软件开发的必需部分(Build Security In，BSI)”的观点，已经得到工业界和政府机构的认同，美国国土安全部下属的国家网络安全处(NCSD)专门建立了BSI网站(http://buildsecurityin.us-cert.gov/protal)，并与美国国家标准技术研究所(NIST)、国际标准化组织(ISO)以及电气电子工程师协会(IEEE)一起共同维护这个网站。

McGraw博士提出软件安全工程化的三个支柱：风险管理、软件安全切入点，以及安全知识。风险管理是一种贯穿软件开发生命周期的战略性方法；软件安全切入点是在软件

开发生命周期中保障软件安全的一套最佳实际操作方法，这其中包括代码审核、体系结构风险分析、渗透测试、基于风险的安全测试、滥用案例、安全需求和安全操作。

软件安全是计算机安全问题中的一个关键问题。软件的缺陷，包括实现中的错误（如缓冲区溢出 buffer overflow），以及设计中的错误（如不周全的错误处理），已经出现很多年了。同时，敌对分子常常通过利用软件漏洞入侵到系统中。因此，基于互联网的应用软件往往成为风险最高的软件。同时随着软件系统的不断增加和越来越复杂，使得安全的潜在隐患也不断增多。据统计，软件中的安全漏洞逐年增长。

最近，卡巴斯基病毒实验室给出 2010 年恶意软件的预报：

2010 年，攻击方式会从 Web 转移到文件共享网络。这是演变链中最新的一个环节：在 2000 年—2005 年间，攻击通过 E－mail 完成；在 2005 年—2006 年间，主要攻击对象是互联网；在 2006 年—2009 年间，攻击主要通过 Web 站点（包括社会网络）。在 2009 年，大量的传播是通过 Torrent 站点分发的恶意文件，不但 TDSS 和 Virut 都是通过这种方式传播，而且 Mac OS 操作系统的第一个后门程序也是这样传播的。表 1.2 列出了 2009 年互联网上 20 个攻击次数最多的恶意程序。在 2010 年，与 P2P 网络相关的安全事件将明显增加。

表 1.2 2009 年互联网上 20 个攻击次数最多的恶意程序

序号	名 称	攻击次数	百 分 比
1	HEUR:Trojan. Script. Iframer	9858304	13.39
2	Trojan-Downloader. JS. Gumblar. x	2940448	3.99
3	not-a-virus:AdWare. Win32. Boran. z	2875110	3.91
4	HEUR:Exploit. Script. Generic	2571443	3.49
5	HEUR:Trojan-Downloader. Script. Generic	1512262	2.05
6	HEUR:Trojan. Win32. Generic	1396496	1.9
7	Worm. VBS. Autorun. hf	1131293	1.54
8	Trojan-Downloader. HTML. IFrame. sz	935231	1.27
9	HEUR:Exploit. Script. Generic	752690	1.02
10	Trojan. JS. Redirector. l	705627	0.96
11	Packed. JS. Agent. bd	546184	0.74
12	Trojan-Clicker. HTML. Agent. aq	379872	0.52
13	HEUR:Trojan-Downloader. Win32. Generic	322166	0.44
14	Trojan. JS. Agent. aat	271448	0.37
15	Trojan-Downloader. Win32. Small. aacq	265172	0.36
16	Trojan-Clicker. HTML. IFrame. ani	224657	0.31
17	Trojan-Clicker. JS. Iframe. be	216738	0.3
18	Trojan-Downloader. JS. Zapchast. m	193130	0.27
19	Trojan. JS. Iframe. ez	175401	0.24
20	not-a-virus:AdWare. Win32. GamezTar. a	170085	0.23
	Total:	27443757	37.3
注：每个程序被发现的次数多于 17 万次，全部恶意程序占安全事故的 37%，共 27443757 次			