

# 《安全软件开发之道》

## 图书基本信息

书名：《安全软件开发之道》

13位ISBN编号：9787111459156

出版时间：2014-3-20

作者：[美]John Viega,Gary Mcgraw

页数：314

译者：殷丽华,张冬艳,郭云川,颜子夜

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《安全软件开发之道》

## 内容概要

本书被誉为安全技术领域的“黄帝内经”，由安全技术大师倾力打造，畅销全球，数位安全技术专家联袂推荐。综合论述如何在软件开发整个生命周期内建立安全屏障，对于设计安全的软件给出了高屋建瓴的指南，全面翔实，深入浅出。对于任何关注安全软件开发的人来说，都是一本必备之书。

本书分为两大部分。第一部分介绍在编写代码之前应该了解的软件安全知识，讲解如何在软件工程的实践中引入安全性，任何涉及软件开发的人都应该阅读。主要内容包括：软件安全概论、软件安全风险管 理、技术的选择、开放源代码和封闭源代码、软件安全的指导原则、软件审计。第二部分涉及软件开发实现的细节，介绍如何在编程中避免一些常见的安全问题，适合编程一线的技术人员参考。主要内容包括：缓冲区溢出、访问控制、竞争条件、随机性和确定性、密码学的应用、信任管理和输入验证、口令认证、数据库安全、客户端安全、穿越防火墙等。

# 《安全软件开发之道》

## 作者简介

### 作者简介

John Viega 美国安全软件解决方案公司 ( www.securesw.com ) 的CTO，是软件安全领域知名的专家。他设计并发布了安全领域内的许多工具，包括代码扫描器 ( ITS4和RATS )、随机数套件 ( EGADS )、自动修补工具以及安全编程库等。他还是Mailman的原始开发者、GNU邮件列表的管理者。

Gary McGraw 美国Cigital公司的CTO，在安全风险领域从事软件安全性研究和技术规划工作。他是美国空军研究实验室、DARPA、美国国家科学基金以及NIST高级技术项目的资助对象和首席调研员。曾经撰写了多本信息安全技术图书。

### 译者简介

殷丽华 博士，IEEE会员，现任职于中国科学院信息工程研究所。主持和参加国家973、863、自然科学基金、发改委安全产品专项等多项国家级重大项目，具有丰富的软件开发与组织管理经验。研究领域包括网络与信息安全、安全性分析、物联网安全技术等。

张冬艳 博士，计算机学会会员，任职于北京科技大学计算机与通信工程学院，承担或参与了多项相关领域的重大课题，积累了丰富的项目开发与管理经验。主要研究方向是网络与信息安全、基于P2P网络的多媒体传输等。

郭云川 博士，曾参与多项国家级网络与信息安全项目建设，目前主要从事物联网隐私保护研发工作。主要研究方向为安全分析、物联网安全技术、形式化方法等。

颜子夜 博士，曾参与分布式、嵌入式、高性能计算等类型的多个软件系统的开发工作，目前主要从事医学图像处理研究和大型医疗装备系统的开发工作。

## 书籍目录

译者序

对本书的赞誉

序

前言

致谢

第1章 软件安全概论 1

1.1 都是软件惹的祸 1

1.2 对安全问题的处理 4

1.2.1 Bugtraq 5

1.2.2 CERT 公告 5

1.2.3 RISKS文摘 6

1.3 影响软件安全的技术趋势 6

1.4 非功能性需求 9

1.4.1 什么是安全 10

1.4.2 难道只是可靠性 10

1.5 “渗透-修补”是个坏方法 11

1.6 艺术和工程 12

1.7 安全目标 12

1.7.1 预防 13

1.7.2 跟踪与审计 13

1.7.3 监控 13

1.7.4 隐私和保密 14

1.7.5 多级安全 14

1.7.6 匿名 14

1.7.7 认证 15

1.7.8 完整性 16

1.8 常见软件安全缺陷 16

1.9 软件项目目标 17

1.10 结论 18

第2章 软件安全风险 19

2.1 软件安全风险概述 19

2.2 安全人员的任务 21

2.3 软件生命周期中的软件安全人员 22

2.3.1 获取需求 22

2.3.2 风险评估 23

2.3.3 安全设计 24

2.3.4 实现 25

2.3.5 安全测试 25

2.4 现实的权衡 26

2.5 让人们去思考安全性 26

2.6 软件风险管理实践 26

2.6.1 当开发走向歧途 27

2.6.2 当安全分析走向歧途 27

2.7 通用准则 28

2.8 结论 30

第3章 技术的选择 31

3.1 语言的选择 31

- 3.2 分布式对象平台的选择 34
  - 3.2.1 COBRA 34
  - 3.2.2 DCOM 35
  - 3.2.3 EJB和RMI 37
- 3.3 操作系统的选择 37
- 3.4 认证技术 38
  - 3.4.1 基于主机的认证 39
  - 3.4.2 物理令牌 40
  - 3.4.3 生物认证 40
  - 3.4.4 密码认证 41
  - 3.4.5 深度防御与认证 41
- 3.5 结论 42
- 第4章 开放源代码和封闭源代码 43
  - 4.1 通过隐藏实现安全 43
    - 4.1.1 逆向工程 45
    - 4.1.2 代码混淆 46
    - 4.1.3 紧包软件的安全 47
    - 4.1.4 通过隐藏实现安全并非万能 47
  - 4.2 开源软件 47
  - 4.3 “多眼球现象”是真的吗 47
    - 4.3.1 漏洞检测是困难的 49
    - 4.3.2 其他的忧虑 50
  - 4.4 关于发布加密算法 51
  - 4.5 另外两个关于开源的谬论 51
    - 4.5.1 微软谬论 51
    - 4.5.2 Java谬论 52
  - 4.6 例子：GNU Mailman的安全 52
  - 4.7 证据：特洛伊木马 53
  - 4.8 开放源码还是不开放源码 54
  - 4.9 另一个来自于缓冲区溢出的安全教训 54
  - 4.10 忠告 55
  - 4.11 结论 55
- 第5章 软件安全的指导原则 56
  - 5.1 确保最薄弱环节的安全 57
  - 5.2 深度防御 59
  - 5.3 失效安全 60
  - 5.4 最小特权 62
  - 5.5 分割 63
  - 5.6 尽可能简单 64
  - 5.7 提升隐私权 66
  - 5.8 记住隐藏信息很困难 68
  - 5.9 不要轻信 69
  - 5.10 使用社会资源 70
  - 5.11 结论 70
- 第6章 软件审计 71
  - 6.1 架构的安全性分析 73
    - 6.1.1 攻击树 74
    - 6.1.2 报告分析结果 78
  - 6.2 实现安全性分析 79

- 6.2.1 审计源代码 79
- 6.2.2 源码级的安全审计工具 80
- 6.2.3 在分析中使用RATS 81
- 6.2.4 安全扫描软件的有效性 82
- 6.3 结论 83
- 第7章 缓冲区溢出 84
  - 7.1 什么是缓冲区溢出 86
  - 7.2 为什么缓冲溢出是安全问题 87
  - 7.3 缓冲区溢出的防御 89
  - 7.4 主要的陷阱 89
  - 7.5 内部缓冲区溢出 93
  - 7.6 更多的输入溢出 93
  - 7.7 其他风险 94
  - 7.8 帮助工具 94
  - 7.9 堆破坏和栈破坏 96
  - 7.10 堆溢出 98
  - 7.11 栈溢出 101
    - 7.11.1 破译堆栈 101
    - 7.11.2 陷入无限循环.....并更糟 105
  - 7.12 代码攻击 113
    - 7.12.1 UNIX漏洞利用 114
    - 7.12.2 关于Windows 119
  - 7.13 结论 119
- 第8章 访问控制 120
  - 8.1 UNIX访问控制模型 120
    - 8.1.1 UNIX权限工作原理 121
    - 8.1.2 修改文件属性 122
    - 8.1.3 修改文件的所有权 124
    - 8.1.4 umask命令 125
    - 8.1.5 编程接口 125
    - 8.1.6 Setuid编程 127
  - 8.2 Windows NT的访问控制 130
  - 8.3 分割 132
  - 8.4 细粒度权限 134
  - 8.5 结论 134
- 第9章 竞争条件 135
  - 9.1 什么是竞争条件 135
  - 9.2 检查时间与使用时间 138
    - 9.2.1 攻破passwd 139
    - 9.2.2 避免 TOCTOU 问题 142
  - 9.3 安全的文件访问 143
  - 9.4 临时文件 146
  - 9.5 文件锁定 146
  - 9.6 其他竞争条件 147
  - 9.7 结论 148
- 第10章 随机性和确定性 149
  - 10.1 伪随机数发生器 149
    - 10.1.1 伪随机数发生器实例 151
    - 10.1.2 Blum-Blum-ShubPRNG 152

- 10.1.3 Tiny PRNG 153
- 10.1.4 对PRNG的攻击 153
- 10.1.5 在网络赌博游戏中作弊 153
- 10.1.6 PRNG的统计测试 155
- 10.2 熵的收集和估计 155
  - 10.2.1 硬件解决方案 156
  - 10.2.2 软件解决方案 158
  - 10.2.3 糟糕的熵收集示例 163
- 10.3 处理熵 164
- 10.4 实用的随机数据来源 166
  - 10.4.1 Tiny 166
  - 10.4.2 Windows的随机数据 167
  - 10.4.3 Linux的随机数 167
  - 10.4.4 Java中的随机数 169
- 10.5 结论 171
- 第11章 密码学的应用 172
  - 11.1 一般性建议 172
    - 11.1.1 开发者并不是密码专家 173
    - 11.1.2 数据完整性 174
    - 11.1.3 密码出口的有关法律 174
  - 11.2 常用密码库 175
    - 11.2.1 Cryptlib 175
    - 11.2.2 OpenSSL 176
    - 11.2.3 Crypto++ 177
    - 11.2.4 BSAFE 178
    - 11.2.5 Cryptix 179
  - 11.3 利用密码学编程 180
    - 11.3.1 加密 180
    - 11.3.2 散列算法 184
    - 11.3.3 公共密钥加密 185
    - 11.3.4 多线程 189
    - 11.3.5 cookie加密 189
  - 11.4 加密散列更多的应用 191
  - 11.5 SSL和TLS 192
  - 11.6 Stunnel 194
  - 11.7 一次一密 195
  - 11.8 结论 198
- 第12章 信任管理和输入验证 199
  - 12.1 关于信任 200
  - 12.2 不恰当信任的例子 201
    - 12.2.1 信任是传递的 201
    - 12.2.2 预防恶意的调用者 204
    - 12.2.3 安全地调用其他程序 208
    - 12.2.4 源自Web的问题 210
    - 12.2.5 客户端安全 212
    - 12.2.6 Perl问题 214
    - 12.2.7 格式字符串攻击 215
  - 12.3 自动检测输入问题 216
  - 12.4结论 219

第13章 口令认证	220
13.1?口令存储	220
13.2?向口令数据库中添加用户	222
13.3?口令认证的方式	231
13.4?口令选择	235
13.4.1?更多的建议	236
13.4.2?掷骰子	237
13.4.3?口令短语	240
13.4.4?应用程序选择的口令	241
13.5?一次性口令	242
13.6?结论	252
第14章 数据库安全	253
14.1?基础知识	253
14.2?访问控制	254
14.3?在访问控制中使用视图	256
14.4?字段保护	257
14.5?针对统计攻击的安全防卫	260
14.6?结论	263
第15章 客户端安全	264
15.1?版权保护方案	266
15.1.1?许可证文件	273
15.1.2?防范偶然性盗版	274
15.1.3?其他的许可证特性	275
15.1.4?其他的版权保护方案	275
15.1.5?对不可信客户端的身份认证	276
15.2?防篡改	277
15.2.1?反调试措施	277
15.2.2?校验和	279
15.2.3?应对滥用	279
15.2.4?诱饵	280
15.3?代码混淆	280
15.3.1?基本的代码混淆技术	281
15.3.2?加密部分程序	282
15.4?结论	284
第16章 穿越防火墙	285
16.1?基本策略	285
16.2?客户端代理	287
16.3?服务器代理	288
16.4?SOCKS	289
16.5?对等网络	290
16.6?结论	292
附录A 密码学基础	293
参考文献	310

# 《安全软件开发之道》

## 精彩短评

1、翻译一般。

# 《安全软件开发之道》

## 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:[www.tushu000.com](http://www.tushu000.com)