

# 《安全模式最佳实践》

## 图书基本信息

书名：《安全模式最佳实践》

13位ISBN编号：9787111501071

出版时间：2015-5-21

作者：（美）爱德华多B. 费尔南德斯（Eduardo B. Fernandez

译者：董国伟，张普含，宋晓龙，刘晓舟，邵帅，王欣，辛伟

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.tushu111.com](http://www.tushu111.com)

## 内容概要

译者序

序

前言

第一部分 概述

第1章 动机与目标 2

1.1 为什么需要安全模式 2

1.2 基本定义 4

1.3 安全模式的历史 6

1.4 安全模式的工业级应用 6

1.5 其他建设安全系统的方法 6

第2章 模式与安全模式 8

2.1 什么是安全模式 8

2.2 安全模式的性质 9

2.3 模式的描述与目录 11

2.4 安全模式的剖析 12

2.5 模式图 16

2.6 如何对安全模式分类 17

2.7 模式挖掘 19

2.8 安全模式的应用 19

2.9 如何评估安全模式及其对安全的影响 20

2.10 威胁建模和滥用模式 21

2.11 容错模式 21

第3章 安全系统开发方法 22

3.1 为模式增加信息 22

3.2 基于生命周期的方法 23

3.3 采用模型驱动的工程方法 25

第二部分 模式

第4章 身份管理模式 28

4.1 概述 28

4.2 信任环 30

4.3 身份提供者 32

4.4 身份联合 34

4.5 自由联盟身份联合 39

第5章 身份认证模式 45

5.1 概述 45

5.2 认证器 46

5.3 远程认证器/授权者 50

5.4 凭据 55

第6章 访问控制模式 62

6.1 概述 62

6.2 授权 65

6.3 基于角色的访问控制 68

6.4 多级安全 71

6.5 基于策略的访问控制 74

6.6 访问控制列表 79

6.7 权能 83

6.8 具体化的引用监控器 87

- 6.9 受控的访问会话 90
- 6.10 基于会话和角色的访问控制 93
- 6.11 安全日志和审计 97
- 第7章 安全进程管理模式 101
  - 7.1 概述 101
  - 7.2 安全进程/线程 104
  - 7.3 受控进程创建器 109
  - 7.4 受控对象工厂 111
  - 7.5 受控对象监控器 114
  - 7.6 受保护的入口点 117
  - 7.7 保护环 120
- 第8章 安全执行模式和文件管理模式 126
  - 8.1 概述 126
  - 8.2 虚拟地址空间访问控制 127
  - 8.3 执行域 129
  - 8.4 受控执行域 131
  - 8.5 虚拟地址空间结构选择 135
- 第9章 安全操作系统体系结构和管理模式 141
  - 9.1 概述 141
  - 9.2 模块化操作系统体系结构 143
  - 9.3 分层操作系统体系结构 146
  - 9.4 微内核操作系统体系结构 150
  - 9.5 虚拟机操作系统体系结构 155
  - 9.6 管理员分级 158
  - 9.7 文件访问控制 162
- 第10章 网络安全模式 166
  - 10.1 概述 166
  - 10.2 抽象虚拟专用网 168
  - 10.3 IPSec虚拟专用网 172
  - 10.4 传输层安全虚拟专用网 174
  - 10.5 传输层安全 176
  - 10.6 抽象入侵检测系统 184
  - 10.7 基于签名的入侵检测系统 189
  - 10.8 基于行为的入侵检测系统 193
- 第11章 Web服务安全模式 198
  - 11.1 概述 198
  - 11.2 应用防火墙 200
  - 11.3 XML防火墙 207
  - 11.4 XACML授权 212
  - 11.5 XACML访问控制评估 217
  - 11.6 Web服务策略语言 221
  - 11.7 WS策略 224
  - 11.8 WS信任 231
  - 11.9 SAML断言 238
- 第12章 Web服务密码学模式 243
  - 12.1 概述 243
  - 12.2 对称加密 246
  - 12.3 非对称加密 252
  - 12.4 运用散列法的数字签名 257

- 12.5 XML加密 263
- 12.6 XML签名 271
- 12.7 WS安全 279
- 第13章 安全中间件模式 285
  - 13.1 概述 285
  - 13.2 安全经纪人 287
  - 13.3 安全管道和过滤器 293
  - 13.4 安全黑板 299
  - 13.5 安全适配器 303
  - 13.6 安全的三层结构 307
  - 13.7 安全企业服务总线 310
  - 13.8 安全的分布式发布/订购 315
  - 13.9 安全的“模型-视图-控制器” 319
- 第14章 误用模式 324
  - 14.1 概述 324
  - 14.2 蠕虫 330
  - 14.3 VoIP中的拒绝服务 336
  - 14.4 Web服务欺骗 341
- 第15章 云计算架构模式 347
  - 15.1 简介 347
  - 15.2 基础设施即服务 349
  - 15.3 平台即服务 357
  - 15.4 软件即服务 364
- 第三部分 模式应用
- 第16章 构建安全的架构 372
  - 16.1 列举威胁 373
  - 16.2 分析阶段 375
  - 16.3 设计阶段 378
  - 16.4 法律案例的安全处理 381
  - 16.5 SCADA系统 387
  - 16.6 医疗应用 392
    - 16.6.1 医疗记录及其规程 393
    - 16.6.2 病人治疗记录模式 394
    - 16.6.3 病人记录模式 395
  - 16.7 环境辅助生活 397
  - 16.8 无线网络安全 399
  - 16.9 本章小结 402
- 第17章 安全模式总结及安全模式的未来 403
  - 17.1 安全模式总结 403
  - 17.2 安全模式的未来研究方向 412
  - 17.3 安全原则 414
  - 17.4 未来展望 415
- 附录A XACML访问控制评估的伪代码 416
- 术语表 418
- 参考文献 423

# 《安全模式最佳实践》

## 作者简介

### 译者序

随着信息技术的飞速发展，互联网日益成为人们生活中不可缺少的一部分，社交网络、微博、移动互联网、云计算、物联网等各种新技术、新应用层出不穷。但不管是Facebook、Twitter等新兴互联网公司的迅速崛起，还是Android日益成为智能手机市场的主流操作系统，信息安全一直都是永恒的话题。安全模式是在给定的场景中，为控制、阻止或消减一组特定的威胁而采取的通用解决方案。在信息系统和软件设计中使用安全模式，可以有效地增强信息系统和软件的架构安全性，降低其安全风险。本书系统地阐述了安全模式的由来、基本概念、重要作用和主要应用，尤其是详细描述了大量具体安全模式的实例，对信息系统和软件架构设计与分析人员有重要的参考价值。对于每一个安全模式实例，本书均描述其应用场景，并针对应用场景所面临的威胁和亟需解决的问题，提出对应的解决方案（即模式），再通过直观的UML图说明模式的具体实现、优点和已知应用。由于作者采用了“提出问题 分析问题 解决问题 总结”的思路，即使读者对安全模式知之甚少，只要有一定的架构设计和信息安全基础，都能很快理解某一安全模式并加以应用。此外，本书内容翔实、图文并茂，非常适合架构设计和分析人员快速掌握安全模式，从本书“按图索骥”。

本书得到国家自然科学基金项目（61100047、61272493）的支持。参与本书翻译的人员有：董国伟、张普含、宋晓龙、刘晓舟、邵帅、王欣、辛伟，在此真诚感谢特约编辑朱筱丹女士，她对本书提出了许多建设性意见，为内容质量的提升付出了大量心血。由于时间和水平有限，书中错漏在所难免，敬请广大读者批评指正。

董国伟

2015年2月

# 《安全模式最佳实践》

## 精彩短评

1、很不错。条理清晰。简洁实用。访问控制模式那章写的挺好。

# 《安全模式最佳实践》

## 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.tushu111.com](http://www.tushu111.com)