<<安全模式>>

图书基本信息

书名：<<安全模式>>

13位ISBN编号：9787302145875

10位ISBN编号：7302145873

出版时间：2007-4

出版时间：舒马赫、 等 清华大学出版社 (2007-05出版)

作者：舒马赫

内容概要

安全问题近来越来越受到人们的关注，很显然较高的安全级别应是所有业务流程基本的先决条件，无论是商业部门还是公共部门都是如此。
安全事故报告数量的稳步增长表明企业需要得到更多的帮助以解决安全问题——从软件系统到操作实践的企业计划。

通常，安全问题在企业及其构建和运行的系统中并没有得到充分的解决。
原因之一是安全覆盖了很多领域。
无论是定义安全业务流程，还是安全地开发及运行相应系统和应用程序都是一项难度很大的挑战。
由于系统和企业的开放程度不断提高，而且主要是Internet和电子商务技术存在的巨大风险，使得安全形势变得越来越紧张。
同时，实现安全本身就很难，尤其是在分布式环境中，因为分布式环境涉及不同的组织、个体、技术组件和机制。
除此之外，信任关系的频繁变化，也使得全面分析安全需求变得愈加困难。
随着现代业务流程变得越来越复杂，对于涉及其中的人员，理解整个问题空间不再是容易的事。
尤其是以下三个重要问题：
在系统设计和实现中经常最后才考虑安全问题。
推进系统安全的企业上下文和需求不能得以清晰的表述，也不能融合在系统体系结构中。
我们需要预先解决安全问题，而不是如今的“修理服务”方法。

多数安全危机都可以归为那些反复出现的著名安全问题。
记录在软件手册上的默认密码就是一例。
在公共Web服务器上存储敏感信息是另一例。
这些例子都说明人们对安全问题的重视程度不高，而且对安全问题也缺乏了解。
在这些例子当中，主要目标是增强功能和性能，而不是降低风险。

企业规划师、系统架构师、开发人员和运营经理安全知识匮乏。
正因如此，他们严重依赖安全专家了解自身安全需求和提供安全解决方案。
但是，安全专家的数量远不能满足这种需求。
而且，安全专家发现在许多情况中，他们为每家企业或每个系统开发项目在重复地解决相同的问题。
对于专家来说，这浪费了他们宝贵的时间，使他们无法抽身去解决更复杂的问题。

虽然目前出现许多更新、更复杂的问题，但解决这些问题的关键是更好地理解企业上下文中存在的大量基本安全问题，并为它们建立恰当的解决方案。
随着时间的推移，遇到同一基本安全问题的安全专家们发现自己总是重复地解决同一问题，而他们早就对这些问题了如指掌并且建立了相应的解决方案。
在某种程度上，这些解决方案已收录在安全文献和相关安全标准之中，但是这些著作和标准需要专业人士才能看懂。

本书的目标就是收集其中一些基本问题和解决方案，使它们能够为企业规划师、系统架构师、开发人员和运营经理所用。
使用哪种形式记录这些信息，才能易于阅读和使用呢？
我们如何从以前的错误中汲取经验，如何制定成熟的解决方案以避免问题的再度发生呢？

本书借鉴使用了“模式”的概念，它是一种成型的软件开发技术。
模式背后的基本思想是，以具有特定结构的文档形式记录专家经验，从而记录指定域中反复出现的问

题的成熟解决方案。
尤其是安全模式，当对企业或系统负责的人员安全经验不足时便可使用安全模式。
这使他们自己就能够解决基本的安全问题，而不用每次都依靠安全专家解决这些问题。
同时这也使安全专家能够抽身解决更新、更复杂的安全问题。

人们将继续开发和使用二类安全解决方案。
即使相对初级的计算机用户，如果他们执意要恶意攻击，也能够使用到处可见的脚本工具造成巨大的破坏。
开发一类解决方案是一个巨大的难题，存在的问题有：需求不充分、设计概念不当、劣质的体系结构、不充分的规范、不成熟的软件开发实践、对系统管理的过度依赖、低劣的操作和高管层的消息闭塞等。
我们越早对安全问题给予应有的重视，我们的解决方案就能更快地进化发展。
这会在很大程度上减少在敏感环境中使用软件应用程序和系统所带来的风险。
我们越来越依赖安全的系统和系统化的解决方案。
我们相信安全模式是朝着这一方向迈出的关键一步。

本书读者对象：本书面向那些对安全知识了解不多，但因工作要求或认识到安全重要性而需要为组织或系统增加基本安全功能的读者。
本书也适合安全专家用做设计指导、系统比较和教授安全知识。

本书结构：第1章“模式方法”概要介绍了整个模式范例。
除了讨论模式方法外，本章还介绍了该书使用的模式模板。

第2章“安全基础”介绍了几个重要的安全概念。
本章提供了安全概览、安全区域分类和一组常用的安全资源。

将模式应用在安全区域，产生了新的特定于域的模式类型：安全模式。
第3章“安全模式”介绍了安全模式的进化历程，描述了它们的特点。
同时也讨论了使用安全模式的好处，以及确定安全模式的数据源。

第4章“模式作用域和企业安全”描述了安全模式的作用域和上下文，并解释了它们在本书中的组织方式。

第5章“安全模式作用域”简要介绍了本书中的所有模式，以及本书引用但未包含的相关安全模式。
在许多情况中，这些模式发表在其他地方。

第6章到第13章介绍了安全模式本身。

第6章“企业安全和风险管理”介绍了企业级安全模式。
这些模式侧重于规划师在企业级战略开发、活动计划、业务模型、目标和策略中要进行的安全性考虑。

第7章“身份识别和验证（I&A）”介绍了支持该系统的I&A服务和已有的服务模式。
身份识别和验证（I&A）服务解决了识别与业务系统交互的用户、流程和其他系统的问题。

第8章“访问控制模型”介绍的模式将大家接受的访问控制模型指定为面向对象的声明性模式，这些模式可用于指导构建安全的系统。

本章还介绍了一个模式，该模式根据声明性模型定义的约束记录评估请求动态。
本章最后介绍的模式可以帮助找到与基于角色的访问控制（RBAC）模型中角色相关联的权限。

第9章“ 系统访问控制体系结构 ”介绍了体系结构级别的访问控制模式。
本章还介绍了一个模式，该模式展现了在考虑一般访问控制需求的情况下收集系统底层需求的原因和方法。
本章剩余部分讨论处理受访问控制保护的软件系统体系结构的模式。

第10章“ 操作系统访问控制 ”介绍了针对操作系统的访问控制服务和机制的模式，这些模式描述了操作系统如何对资源实施访问控制，例如，内存地址空间和I/O设备。

第11章“ 统计 ”介绍了审计和统计的服务和机制的模式。
决策者需要了解任何发生的、涉及其资产的安全事件。
安全审计和统计模式可以满足这种需求。

第12章“ 防火墙体系结构 ”介绍了描述不同类型防火墙的模式语言。
该模式语言可用于指导为系统选择合适的防火墙类型，或帮助设计者构建新系统。

第13章“ 安全的Internet应用程序 ”介绍了Internet安全模式，它们是第8章“ 访问控制模型 ”和第12章“ 防火墙体系结构 ”针对Internet应用程序领域的具体化模式。

第14章“ 案例研究：IP电话 ”介绍了一项新兴技术的案例研究，示范了如何使用安全模式将安全融入到实际系统工程方案中。
将本书中讨论的最适宜的模式应用到从IP电话系统挑选的用例中。

第15章“ 辅助概念 ”讨论了挑选的补充概念，这些概念对安全模式是一个补充。
要特别指出的是，本章还介绍了安全原理的模式相关概念和所谓的“ 误用例 ”。

第16章“ 结束语 ”给出了本书的结论，并对未来有关安全模式和相关概念的工作进行了展望。

作者简介

作者：(美)舒马赫 等

<<安全模式>>

书籍目录

版权说明