安全技术经典译丛

Security Patterns
Integrating Security and Systems Engineering

安全模式
——集成安全性和系统工程

Markus Schumacher
(美) Eduardo Fernandez-Buglioni 等著
Duane Hybertson
徐 璐 译

WILEY
清华大学出版社

安 全 模 式

—— 集成安全性和系统工程

(美) Markus Schumacher
Eduardo Fernandez-Buglioni
Duane Hybertson
等著

徐 璐
译

清华大学出版社

北 京

Markus Schumacher,Eduardo Fernandez-Buglioni,Duane Hybertson, et al
Security Patterns: Integrating Security and Systems Engineering
EISBN：0-470-85884-2

北京市版权局著作权合同登记号　图字：01-2006-0569

图书在版编目(CIP)数据

安全模式——集成安全性和系统工程/(美)舒马赫(Schumacher, M.)，(美)费尔南德斯-巴哥兰尼(Fernandez-Buglioni, E.)，(美)海布尔森(Hybertson, D.)著；徐璐译. —北京：清华大学出版社，2007.4
(安全技术经典译丛)
书名原文：Security Patterns: Integrating Security and Systems Engineering
ISBN 978-7-302-14587-5
Ⅰ. 安…　Ⅱ. ①舒…②费…③海…④徐…　Ⅲ. 电子计算机—安全技术—研究　Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2007)第 016407 号

责任编辑：王　军　梁卫红
装帧设计：孔祥丰
责任校对：成凤进
责任印制：孟凡玉
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：北京市世界知识印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：26　**字　数**：633 千字
版　　次：2007 年 4 月第 1 版　　**印　　次**：2007 年 4 月第1 次印刷
印　　数：1～4000
定　　价：49.00 元

序

对于多数软件系统，安全已成为一个非常重要的课题。随着 Internet 的成功发展，计算机和软件系统也越来越网络化。研究人员已着手建立一种场景，其中数百万台设备互相连接、共同协作运行基于 Web 的商业、政府、医疗以及其他类型的安全敏感系统，而研究重点就是安全问题。

在一个常见的医疗场景中，附着在病人身上的无线传感器收集心脏数据，然后再由 PDA 上的软件进行预处理。如果这些数据在传送到医生的途中被未经授权的人员拦截并操控，那么其后果将会是怎样呢？请再考虑这样一个场景，汽车制造商的服务器被黑客入侵，汽车上的软件被远程更新。如果这些“更新”后的汽车，将制动信号变成了线传加速信号，那么其后果将会是怎样呢？假设在不久的将来，您所乘坐的飞机不再听从驾驶员或机场指挥塔台的命令，而是任凭劫机者操作，那么其后果将会是怎样呢？也许最糟糕的是，某些恐怖分子控制了核电厂，那么……

我们当然不希望这些事情发生！换句话说，在信赖和使用某个系统之前，需要它能够确保一定程度的保密性和完整性。

虽然大家都知道安全很重要，但只有少数项目给予它相应的重视。在许多项目中，安全仍然是最后考虑的事情。翻阅一下您所喜爱的 IT 杂志中有关安全的最新文章，会看到很多有关成功入侵和拒绝服务攻击的报告，它们涵盖了各类企业级系统。最具有讽刺性的是，这些大都不是专家所为，而只不过是高中生和安全爱好者通过脚本一类的简单工具实现的。

为什么对安全的肯定和安全在软件开发中的地位如此不符呢？这当然不仅仅是因为安全仍是软件开发中未探索的领域。除此之外，安全需求的表达也常常很模糊，而且目前的软件体系结构在安全方面的相关决策也非常有限。为了挽救当代网络化、开放式的计算环境，超越身份验证领域是至关重要的。

项目经理、软件架构师、开发人员、测试人员和其他软件系统参与者需要确保将安全视为所有软件项目中不可或缺的一部分。

下面是本书引人入胜的地方。与市面上介绍最新研究思想和安全技术的书籍不同，本书着重于介绍实际知识和国际安全专家的宝贵经验。本书使用模式(一种广泛采用的成功技术)描述、交流和分享知识经验。本书作者将带您一起征服安全领域，帮您答疑解惑，为您清晰地展现如何构建安全系统并展示相应的成熟解决方案。

例如，如何确定组织或系统的安全需求，如何定义相应的安全方法来满足这些需求？系统需要的安全属性是保密性、完整性、可用性还是责任性？或者是四者的混合？如何通过预防、检测和响应方法来确保这些属性？需要通过身份识别和验证(I&A)吗？或者系统需

要访问控制和授权，还是统计和审计？所有服务如何交互才能为系统提供一致连贯的安全概念？一旦知道了需要哪些安全服务，以及这些服务如何互操作，那么它们的不同实现选项又是什么呢？例如，基于密码的 I&A 和基于 PKI 的 I&A 哪一个更能满足安全需求呢？哪些不同的选项对您可用呢？智能卡？RFID 标签？或者，为系统提供一个请求用户 ID 和密码的登录服务是否足够呢？

您可能还会想到更多更细节的问题，不仅是身份识别和身份验证，还有所有能够提供访问控制和授权、统计和审计等的其他安全服务和机制。

所以安全是一个宽泛且重要的领域，在构建成功的软件系统时恰当地表述安全仍很重要。因为无知或缺乏大局观而忽略安全问题可能会造成灾难性的后果。我不是安全专家，但在研读完这本著作后，我对安全问题有了更好的了解，它使我在作为软件架构师的日常工作中能够更加清晰、出色和建设性地表述安全问题。

除了在技术方面的重要价值和贡献外，本书还有一点很特别。本书的作者是模式社区的精英，他们都仔细地编写模式作用域以避免重叠。他们综合整理了模式间的所有关系，确保了模式具有共同的风格。努力的最终结果是一个互补互助的模式网络，它详细覆盖了各个重要安全区域。这个网络的价值远胜于所有单个模式价值的总和，通过该网络您可以看到全局，而不是局部的碎片。

最后，让我们一起阅读和分享本书所收集的模式。希望书中讨论的相关安全问题可以丰富您的设计知识，增强您对安全的全面了解。

相信您会和我一样对这本书爱不释手。

Frank Buschmann
高级总工程师
Siemens AG，Corporate Technology

前 言

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。

本书的主要目标读者是：

- 在企业级别，关注企业安全的人员，例如，企业规划师、企业架构师、战略制定者、策略制定者、业务流程工程师和业务流程再造专家。这部分人的主要问题是了解如何定义基本的企业安全需求和约束。面向这部分人的安全模式在第 6 章“企业安全和风险管理”中讨论。同时，我们还推荐这部分人阅读第 7 章到第 13 章中描述的模式，以了解如何在企业运营中反映或实现企业安全计划。
- 在 IT 系统级别，关注系统安全的人员，例如，系统架构师、软件设计人员和开发人员、项目经理、产品供应商和服务提供商。这部分人必须了解如何设计基本的系统安全功能并将这些功能融入系统体系结构和设计之中，以及如何挑选已有的安全解决方案。我们为这部分读者汇编了一套相应的安全模式，收录在第 7 章到第 13 章中。在这个级别，了解在第 6 章“企业安全和风险管理”中描述的企业安全约束以及它们对系统安全需求的影响也是非常重要的。
- 在运营级别，关注运营安全的人员，例如，运营经理和运营人员等。这部分人主要关注在企业和系统运行当中，如何定义和采用基本的安全实践。包含与此相关的安全模式的章节有：第 7 章“身份识别和验证(I&A)”、第 10 章“操作系统访问控制”、第 11 章“统计”、第 12 章“防火墙体系结构”和第 13 章“安全的 Internet 应用程序”。

很明显，所有这些级别都会相互影响。要想全面了解安全，就需要在某种程度上了解各个级别。

本书对于以下读者也非常有用，他们可以阅读任何有兴趣的章节：

- 安全专家会比较感兴趣于我们的安全分类与其他安全分类的比较。他们可能还希望看到如何以模式的形式来表达熟悉的安全解决方案。且还可以使用或引用模式来减少回答相同安全问题的次数。
- 研究员、教师和学生可以通过本书了解目前最佳的安全实践。他们还可能找到潜在的区域来扩展我们的方法。例如，他们可能会检查安全分类以找出当前模式没有覆盖到的区域。安全模式可以帮助这些人设计新系统、了解复杂系统、比较系统和教授知识。例如，安全模式可以用于大学安全课程的教学中。
- 通过使用这种新的最佳安全实践表达方式，安全审计人员可以对审计对象增进了解。收集的模式还包括要注意的因素和缺憾。在模式社区中，我们使用术语“因素”描述目标和约束，它们揭示了问题的错综复杂，定义了在遇到矛盾时必须要进行的各种利弊权衡。
- 政府采购专家可以通过了解新的最佳安全实践表达方式来获得帮助，这种形式可能会包含在采购文件中，例如，工作建议或声明的要求。

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。

读者指南

除了可以选择从头至尾地阅读本书外，还可以选择其他顺序阅读本书。

本书从逻辑上分为 3 部分。第 1 部分由第 1 章到第 3 章组成，介绍有关安全模式的背景知识。如果对模式不熟悉，请阅读第 1 章“模式方法”，该章简要介绍了软件模式背后的思想。如果对安全不熟悉，请阅读第 2 章“安全基础”，该章介绍了一些基本概念，并给出了具体安全知识的来源。基于以上内容，第 3 章“安全模式”讨论了安全模式的概念。

第 2 部分由第 4 章到第 13 章组成，包含一系列涵盖不同主题的安全模式。可以按章节大致浏览一遍，对不同级别的典型安全问题和成熟解决方案有个大致印象。

要了解安全模式的组织方式，请阅读第 4 章“模式作用域和企业安全”，该章建立了安全分类。如果希望快速得到安全模式的概览以及本书未介绍的相关模式，请阅读第 5 章“安全模式作用域”，该章可用作参考资料和导读。

第 6 章到第 13 章可按需要的顺序阅读，或只阅读某部分模式。在指定模式中，关键主题是“上下文”、“问题”和“解决方案”。其他主题可以选读，它们提供有关模式实现的进一步信息。我们还确定了模式间的关系，因此，读者可以从任何一个模式开始阅读，并通过相关模式的引用导读本书。

如果您已阅读完介绍性章节，而安全模式对您来说还是新事物。我们建议首先阅读易于理解和经常使用的安全模式，例如：

- 密码设计和使用(PASSWORD DESIGN AND USE)
- 单访问点(SINGLE ACCESS POINT)
- 前门(FRONT DOOR)

在本书的第 3 部分，我们讨论了应用程序、扩展和基于模式的安全方法的未来方向。如果想寻找描述如何应用安全模式的示例，请阅读第 14 章“案例研究：IP 电话”中的案例研究。如果关注能够扩展安全模式概念的技术，请阅读第 15 章“辅助概念”中的一些示例。第 16 章“结束语”对本书进行了最后总结，并对该工作的未来进行了展望。以上这些章节都以本书前面章节中的模式为基础，应放到最后阅读。

目　录