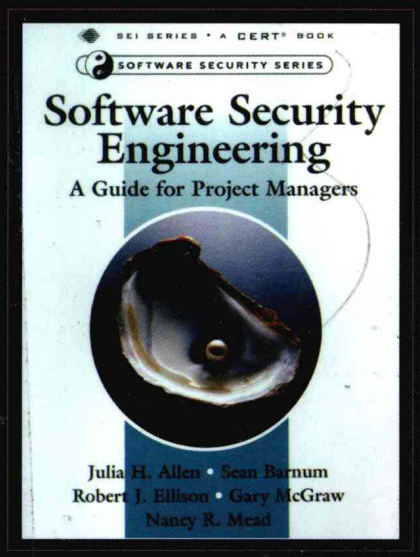
HZ BOOKS
华章程序员书库

软件安全工程

Software Security Engineering

A Guide for Project Managers



（美）Julia H. Allen　Sean Barnum　Robert J. Ellison
Gary McGraw　Nancy R. Mead　著
郭超年　周之恒　译

软件项目经理必备指南

将软件安全解决方案引入到软件开发生命周期之中

机械工业出版社
China Machine Press

华章程序员书库

软件安全工程

Software Security Engineering

A Guide for Project Managers

（美）Julia H. Allen　Sean Barnum　Robert J. Ellison
Gary McGraw　Nancy R. Mead　著
郭超年　周之恒　译

机械工业出版社
China Machine Press

本书系统阐述了软件安全工程的知识。具体内容包括：软件安全的构成、安全软件的需求、安全软件的架构和设计、安全编码和测试、系统集成、安全管理，等等。

本书从软件开发和漏洞攻击两个角度，以对立的观点深刻阐述了构建软件安全的最佳实践。同时，本书不遗余力提高阅读的针对性，对高级经理、项目经理和技术管理人员的适用要点，各有强调论述。

本书适合作为从事软件开发、软件测试、软件安全及软件工程管理的技术人员的参考用书。

本书版权登记号：图字：01-2009-1155

图书在版编目（CIP）数据

软件安全工程/（美）艾伦（Allen, J. H.）等著；郭超年，周之恒译. —北京：机械工业出版社，2009.4

（华章程序员书库）

书名原文：Software Security Engineering: A Guide for Project Managers

ISBN 978-7-111-26483-5

Ⅰ. 软…　Ⅱ. ①艾…　②郭…　③周…　Ⅲ. 软件开发-安全技术　Ⅳ. TP311.52

中国版本图书馆 CIP 数据核字（2009）第 029232 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）

责任编辑：盛东亮

北京京北印刷有限公司印刷

2009 年 4 月第 1 版第 1 次印刷

186mm × 240mm · 15 印张

标准书号：ISBN 978-7-111-26483-5

定价：45.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

译 者 序

很荣幸能够翻译 Julia H. Allen，Sean Barnum，Robert J. Ellison，Gary McGraw 和 Nancy R. Mead 的著作。正如作者所讲到的：软件在我们的生活中已经无处不在，同时这些软件大多涉及个人隐私、金融和保险信息等，个人信息越来越依赖于复杂的、互联的、软件集中和安全的信息系统。当前，软件还不能完全抵御入侵攻击，因此如何最有效地防御攻击已成为软件开发者面临的严峻问题。

作者在书中始终坚持他们数十年来的开发经验和最新的研究成果，积极地寻求能够给软件开发者带来最大受益的组织方式，嵌入了大量的开发研究案例，使读者一目了然。该书推荐在软件开发周期的各个阶段都要遵循安全理念，这样开发出来的软件能更有效地抵御、容忍攻击并从攻击中恢复。软件的安全性，应该在企业高层的领导、中层的技术管理人员和低层的开发测试人员心中占有很重的分量。软件安全应该提升到软件开发组织的企业文化高度来推广，并应用管理学的知识了理解和应用。

在翻译本书的过程中，我们力求做到语言平实无华，期望能给读者带来一个轻松的阅读过程。翻译期间得到了刘胜利和郑东老师的很多帮助，在此深表谢意；另外，也十分感谢实验室的其他老师和同学，感谢一直给我们鼓励的家人。

译者

2009 年 3 月

序

大家都知道，软件因安全缺陷而漏洞百出，乍一看，这似乎很令人惊讶。我们知道如何利用一种能够提供适度安全等级和健壮性的方法来编写软件，那么为什么软件开发者们不使用这些技术呢？

在这个问题数以万计的答案之中，本书讨论了其中的两种。第一，安全软件的意义。事实上，“安全软件”这个术语是一个误称。安全是一个软件加上环境所组成的产品。一个程序如何使用、在何种情况下使用以及其必须达到的安全需求，决定了这个软件是否安全。术语“安全驱动的软件”关注了满足特定安全需求的软件开发和设计理念，但在其他环境下这些软件基本的假设（以及其他隐含的需求）不再有效的情况下，软件就可能不安全。本书以一种易于理解的方式描述了软件精确而又有意义的安全需求的必要性，以及他们的开发方法。不同于很多有关安全软件的书籍，本书并没有做安全需求已知的假设，而是深入讨论了安全需求的来源和分析，以及同样重要的、关于需求的确认。

第二个答案在于项目的行政主管、管理者以及技术主管。他们必须支持安全性增强在软件中的采用，以及健壮编码的实现（这是一项真正的安全性增强）。此外，他们必须理解整个过程，为其提供进度表、预算和人员配置方面的更多支持。本书出色地向这些人们展示了软件安全的过程，使得他们可以切实地评估其影响。同时，本书也指出了在某些情况下，开发过程中遇到的状况是全新的，或者缺乏足够经验，以至于找不到可被证明有效的方法或是被大家广泛接受的方法。针对这种情况，作者提供了一些思路来帮助开发出有效的方法。这样，行政主管、管理者和技术主管就能明白在他们的环境中哪一种方法才能最为有效。

另外，最为关键的，从项目开始就针对安全性进行设计和实现，切实保证了软件符合安全需求。这大大减少了给软件打补丁和填补安全漏洞的必要——这些工作本身就会引起很多安全问题，给软件制造商的声誉和财政状况带来不良影响。信用的丧失，尽管是无形的，也会对有形资产产生影响。从一开始就正确地开发软件，为此支付额外成本能减少软件投入使用之后的维护费用，并且会产生一个更好的、更健壮的、更安全的软件。

本书讨论了多种开发软件的方法，在这些方法中对安全性的考虑扮演着重要的角色。本书面向行政主管、每一级的项目经理和技术主管，从这个意义上来说，是非常独到的。本书也面向学生和开发人员，使他们理解以安全的理念进行软件开发的过程并能找到相关资源来帮助他们进行开发。

本书的一个潜在主题是我们使用的软件可以变得更好。本书的内容向行政主管、项目经理和技术主管提供了一个基础，使得他们可以改善他们开发的软件，改善软件的质量和安全性。

Matt Bishop
Davis, California
March 2008

前　言[1]

本书讨论的问题

软件在生活中无处不在。许多公司使用或提供的产品、服务和加工都很大程度上依赖于软件，这些软件用来处理关系到个人隐私、生计和日常生活中敏感而有价值的数据。例如，国家安全，甚至公民的个人安全依赖于越来越复杂化、互联的、软件集中的信息系统。在很多情况下，这些信息系统使用 Internet 或与 Internet 相联的专用网络来进行交互和传输数据。

这种对信息技术无所不在的依赖使得软件安全成为了关系到业务连续性、灾难恢复、紧急事件处理和国家安全的重要因素。软件漏洞会危害到知识产权、消费者的信赖、商业运作和服务，以及一系列关键性的应用和基础设施——从过程控制系统到商业应用产品的几乎所有一切。

关键性的数字资产（系统、网络、应用软件和信息）的完整性依赖于那些运用控制这些资产的软件的可信度和安全性。然而，商业巨头和消息灵通的消费者越来越认识到：拥有从事软件安全的必要资历的从业者相当缺乏这一事实[Carey 2006]。软件供应商是否能开发、提供可放心使用而不必担心泄露信息的软件，他们对此尤其怀疑。应用软件是涉及敏感信息的主要途径。根据 Deloitte 公司对 169 家全球主要的金融机构的一项调查（名为《2007 Global Security Survey：The Shifting Security Paradigm》[Deloitte 2007]），当前应用软件不再能完全抵御入侵攻击。Gartner 公司认为应用软件安全是首席信息官们需要首先解决的问题。

如今，软件开发过程缺乏必要的安全措施，这导致了许多可能被人利用的漏洞。如果要开发出比目前软件更可靠、安全的软件，那么加强安全要素的开发过程和安全条例，以及有丰富经验和技术的开发者就是必须的。

有一种经济学上的反驳论据，或者至少是一种观点：一些商业巨头和项目经理认为，开发安全软件会减缓开发进程并增加看不到实际意义的开销。很多时候，当决策简化为“现在就发送”或“做安全了再发送”时，那些控制着财政却对安全威胁一无所知的人们总是会选择“现在就发送”。本书的第 1 章（1.6 节，尽早检测软件安全缺陷的益处）和第 7 章（7.5.3 目，“知识和专业领域”中讨论微软安全开发周期的经验部分）讨论了与此相反的观点，包括软件安全如何潜在地减少了开发成本和加速开发进程。

软件易被攻击的漏洞

针对软件的威胁的数量正在不断增加，现在大多数的网络系统级别的攻击利用了应用级别软件的漏洞。根据卡耐基·梅隆大学的 CERT[2]分析师的说法，绝大多数成功的攻击都是针对和利用

---

[1] 前言中所引用的内容参考了《Security in the Software Lifecycle：Making Software Development Processes——and Software Produced by Them——More Secure》[Goertzel 2006]。

[2] CERT 已由卡耐基·梅隆大学在美国专利商标局注册。

已知的、未打补丁的软件漏洞和不安全的软件配置，而这些问题都是在软件设计和开发过程中产生的。

这些条件导致了与软件功能相关的风险的增加，并使攻击的威胁进一步加剧。在这种不确定的氛围之下，众多的利益相关者需要充分的证据来相信那些负责他们的核心事务处理的软件能够可靠地执行。

我们为何编写这本书

软件安全工程的挑战

软件安全工程需要利用安全条例、过程、工具和技术来解决软件开发周期(软件开发周期)中每一阶段的安全问题。遵循安全理念开发的软件能够更好地抵御人为攻击和非人为的故障。对于安全软件的一种看法是，它被设计成"在恶意攻击下能持续地保证正确运行"[McGraw 2006]，同时能识别、抵御、容忍那些威胁其可靠性的人为事件，并从中恢复。很多概念可能与软件安全相似(比如，软件保险性、可信赖性和容错能力)，包括面对非人为故障和意外事故以及无意的误用和滥用等情况软件的正常运行，以及尽可能地减少软件缺陷和漏洞。本书讨论的是狭义的观点。

软件安全工程的目的是开发出更健壮、无缺陷的软件。软件密集型系统如果更多地使用考虑了安全的软件，就能够在以下方面做得更好：

- 抵御利用软件缺陷进行的攻击，或是容忍这些攻击所带来的故障，使得软件能在大多数的攻击之下仍然能正确运行。
- 面对攻击引起的错误，软件发生故障，若它无法及时抵御、容错或是从中恢复，它至少必须能够将损失降到最小。

没有哪一个例子可以向软件安全提供万能的解决方案，请不要忘了这句话。与此同时，本书切实地向项目经理提供了很多很好的实例，使他们可以评估并适当地使用这些实例来重构他们自己的项目安全条例。本书的目的是通过这些实践，提高软件在开发和运行过程中的安全性和可靠性。

读者能得到什么

通过阅读本书，读者能提升对软件设计开发过程中安全问题的认识。本书也能帮助读者理解软件开发安全条例既可能促成软件的安全，也可能导致软件不安全。

本书(以及后面会提到的在 Build Security In 网站上引用的资料)会让读者识别和比较潜在的、新的实例，这些实例能够被扩充到项目现有的软件开发安全条例中去，从而更有可能开发出安全性好的软件并达到特定的安全需求。举个例子，保证案例可以应用于声明和指定具体的安全特性，包括安全条例能满足安全需求的程度。保证案例将在第 2 章中(2.4 节)讨论。

使用本书中所介绍的实例进行开发和集成的软件，其缺陷将显著地减少，并且这些软件能够更好地抵御、容忍攻击以及从中恢复，因而可以更加安全地在操作环境中运行。负责保障软件和系统在软件开发周期中切实落实安全需求的项目经理应该回顾、选择、适当修改本书中以及 BSI 网站上的指导内容，和本书中引用的众多资源，这应该成为他们日常管理工作的一部分。

给本书读者的五条现成经验：

1) 软件安全不仅仅关注修复漏洞和执行入侵检测。项目经理要用系统化的方法将本书所讨论

的优秀实例融合到他们的开发过程中去(所有章节)。

2)网络安全机制以及IT基础安全服务并不能充分保障应用软件免受安全隐患的威胁(第1、2章)。

3)软件安全的出发点,是在认识到安全风险在软件开发周期的任何阶段都有可能改变的情况下,使用一种风险管理的方法来鉴别安全优先级以决定哪个安全级别最好(第1、2、7章)。

4)开发安全的软件取决于对软件运行环境的理解程度(第6章)。

5)项目经理和软件工程师需要学会从攻击者的角度来审视软件的负面效应,以及软件如何更好地抵御、容忍攻击并从中恢复(第2~5章)。

谁应该读这本书

本书主要面向负责软件密集型系统开发的项目经理,同时,首席需求分析师、经验丰富的软件和安全设计师、架构师、系统整合师以及他们的经理也能从中获益。本书为软件安全和软件密集型系统的管理提供了指导,不管该系统是重新开发的还是由现有的软件封装、集成而来的。

本书会帮助读者理解与软件工程相联系的安全问题,并且帮助他们掌握软件管理和开发的安全条例,从而开发出能更好地抵御威胁的软件。本书假设读者熟悉一般的系统、软件工程管理方法、安全条例和技术。

本书是如何组织的

本书以两章介绍性的内容作为开端,中间四章详述技术性细节,最后以一章控制、管理方面的内容和一章综述性内容结尾。

第1章,介绍大多数软件面对的威胁,说明在开发方法不成熟的情况下,将导致软件更容易遭受这些威胁的攻击。该章详述了在软件开发周期的开始阶段检测安全缺陷的好处,包括商业案例的软件安全条例。最后,简要介绍了一些实用的解决方案,这些解决方案将在后面的章节进行详细的阐述。

第2章,详细研究核心而又有影响力的软件安全特性,实现这些特性过程中所采用的防御者和攻击者的不同角度分析,并讨论这些特性是如何提升安全性。该章介绍和定义了攻击模式和保证案例的关键资源,解释了如何在软件开发周期中使用他们。

第3章,描述安全需求工程条例,包括对安全需求的归纳、详述、分析、确认的一些特定过程。该章也研究了一些误用滥用的典型案例。

第4章,从软件安全性和可靠性方面,描述了架构、风险分析和评估,以及确认软件系统的规格说明书、架构和设计方面的安全条例。

第5章,概述进行代码分析的安全条例,以发现错误从而提高代码质量。该章还讨论了关于安全测试、白盒测试、黑盒测试以及渗透测试的安全条例。其间,会涉及最新公布的安全代码和测试方面的成果,这些会在后面详述。

第6章,描述可信系统和多重系统的设计、汇编、集成和进化过程中的挑战和安全条例。向项目经理提供指南,帮助他们把最新的或已经升级的软件组件整合到已有的操作环境中去。

第7章,描述如何激发商业领导者在控制和管理层上给予软件安全以更多的关注。包括一些针对风险管理和项目管理,以及建立一个企业级安全框架的可行的安全条例。

第8章，概括了本书所讨论安全条例，给出了一些建议，来帮助读者确认哪些条例对于哪些人是最有意义的，以及从何处着手工作。

本书最后给出了参考书目以及相关术语。

给读者的备注

本书导读

为帮助读者更好地理解本书，我们使用了两类不同的描述性的图标来标记本书的段落以及关键的条例。

- 标识与“条例成熟度”相关的内容：
  - L1 这部分内容提供了针对如何思考问题的建议，这些问题没有已证明的或是公认的解决方案。描述的目的在于引起读者的注意并帮助他们思考问题的可能解决方案。这部分内容包括在一些特定的约束条件下验证成功而有望应用于实际的研究成果。
  - L2 这部分内容描述那些已投入前期应用并取得良好效果的安全实例。
  - L3 这部分内容描述的安全条例仅限于工业或政府部门使用，也就是说只针对特定的市场范围。
  - L4 这部分内容描述了已经成功部署并广泛应用的安全实例。读者可以完全放心地使用这些条例。这部分还包括一些典型经验报告和案例分析。
- 标识那些与每一章节或实例最有关的读者群：
  - E 主管和高级经理
  - L 项目经理和中层经理
  - M 技术主管，工程管理人员，前线管理者以及监督人员。

正如章节中的读者群标记那样，我们建议主管和高级经理们阅读第1章、第8章的所有内容，以及其他章中的以下各节：2.1、2.2、2.5、3.1、3.7、4.1、5.1、5.6、6.1、6.6、7.1、7.3、7.4、7.6、7.7。

项目经理和中层经理请务必阅读第1、2、4、5、6、7、8章以及3.1、3.3、3.7节。

技术主管、工程管理人员、前线管理者以及监督人员则能够在阅读全书过程中得到有用的信息和指导。

Build Security In：一项重要的资源

从2004年开始，美国国土安全局软件保证计划部门开始发起 Build Security In（BSI）网站（https：//buildsecurityin. us-cert. gov/）的开发，这是本书写作中最重要的资源之一。BSI 的内容基于如下原则：软件安全本质上是一个软件工程问题并且必须在整个软件开发周期中使用系统化的方法来进行管理。

BSI 提供和链接了范围广泛的信息，这些信息包括健全的安全条例、工具、指南、规则、原理以及别的知识，以帮助项目经理部署软件安全条例和开发安全、可靠的软件。该网站归功于本书以及 BSI 网上其他文章的作者，包括来自卡耐基·梅隆大学软件工程研究所（SEI）和 Cigital 公

司的高级职员，以及其他经验丰富的软件和安全专家。

本书的某些部分已经作为《IEEE Security & Privacy》杂志的文章出版，得到了 IEEE Computer Society Press 的许可而在此重新出版。当这些文章在本书中出现时，会有如下的脚注：

> 该部分首先作为文章在《IEEE Security & Privacy》上出版[引用]。在此得到出版者的许可而再版。

这些文章也能在 BSI 网站上找到。

本书自始至终引用 BSI 网站上的文章。读者们可以在 BSI 网站上得到关于本书内容的附加细节，以及本书的勘误表和当前的研究成果。

开始学习

一些优秀的书籍讨论安全体系和软件工程。而本书从一种软件安全工程学的角度，把整个软件开发周期嵌入到一整套健全的软件工程的安全条例下进行研究。

作为其广泛论述的一部分，本书同时讨论了标准的和新兴的软件安全条例，并解释了为什么需要使用他们来开发更加安全健壮的系统。而及早采取安全措施，并在软件开发周期中经常重复这些行为的理由，本书也将反复论述。

本书针对的不是第一次接触软件安全的项目经理。读者需要理解软件开发周期及其过程，包括其内部组织结构，由此才能理解所使用的各项技术的含义，从而能够对于给定的项目，选择出最适合的推荐的安全条例。

另外，也有一些书籍讨论了安全软件工程各个阶段的任务，然而很少能够使用一种简洁有效的方式来覆盖这些内容，而这正是我们力图做到的。

祝学习愉快！

感谢

很高兴能有机会答谢对于本书的编写给予支持的人们。我们的组织，软件工程研究所的 CERT 计划和 Cigital 公司激励着我们的写作并为我们提供闲暇时间以及其他的支持使我们能完成此书。Pamela Curtis，我们的技术编辑，认真地一遍又一遍地阅读了原稿，提出了许多宝贵的修改意见，同时还帮助我们组织问题以及指导本书中的图片的绘制工作。Jan Vargas 提供了 SEI 方面的管理支持，跟踪进度表和写作项目，并帮助会议日程管理。在本书写作的前期，Petra Dilone 提供了 SEI 方面行政上的支持，并对众多章节和多遍手稿布置管理。

我们也非常感谢 Joe Jarzombek 的鼓励，他是 BSI 网站的发起者。BSI 网站是本书写作的重要资源。

本书中的很多内容是基于和其他作者合作发表的文章，这些文章发表在 BSI 网站或是别的地方。我们非常高兴能有机会与这些作者合作，我们将在那些他们参与的段落直接或间接的列出他们的名字。

我们有众多的审稿者，他们的努力极具价值，引导我们做出了很多的改进。内部的审稿者包括 SEI 的 Carol Woody 和 Robert Ferguson。我们也非常感谢 Addison-Wesley 的审稿者们的努力和深思熟虑的评论，他们是 Chris Cleeland、Jeremy Epstein、Ronda R. Henning、Jeffrey A. Ingalsbe、

Ron Lichty、Gabor Liptak、Donald Reifer 和 David Strom。我们要给予 Steve Riley 特别的赞誉，他作为 Addison-Wesley 的审稿者审读了我们的初始计划以及每一遍的草稿。

我们非常感谢 Addison-Wesley 的联系人给予我们的鼓励和支持。他们是出版合伙人 Peter Gordon、编辑助理 Kim Boedigheimer、全面服务生产经理 Julie Nahil 和自由作家编辑 Jill Hobbs。我们也非常感谢 Addison-Wesley 和 SEI 的美术师和设计人员帮助我们进行封面设计、排版和绘图。

作者简介

Julia H. Allen

Julia H. Allen 是一位软件工程机构 CERT 项目的高级技术职员。这个机构隶属于美国宾夕法尼亚州位于匹兹堡的卡耐基·梅隆大学。Allen 除了从事软件安全保证工作以外，还从事企业安全和管理方面的行政性工作。在从事技术工作之前，Allen 曾做了六个月的 SEI 临时代理主管，也曾做过三年的操作人员的代理主任。她使 SEI 正式和工业组织建立了关系，创造了消费者关系团队。

在加入 SEI 之前，Allen 曾是 SAIC 副主席，负责创建一个新的软件分部，专门负责嵌入式系统软件。Allen 领导 SAIC 的最初成果在于软件进程的发展。Allen 也为 TRW（Northrop Grumman 的前身）工作，处理一系列从系统整合、测试和领域站点支持到管理大多数软件开发项目的工作。

她的学位包括从密歇根大学获得的计算机科学学士学位和从南加利福尼亚大学获得的电子工程硕士学位。Allen 的作品有《The CERT®Guide to System and Network Security Practices》（Addison-Wesley，2001），《Governing for Enterprise Security》（CMU/SEI-2005-TN-023，2005）和 CERT 播客系列："Security for Business Leaders（2006-2008）"。

Sean Barnum

Sean Barnum 是 Cigital 公司的首席顾问，为 Cigital 的联邦服务提供技术指导。他拥有二十多年的软件行业经验，包括软件发展、软件质量保证、质量管理、程序构建和改进、知识管理和保障等。Barnum 为了地方和国家软件安全和软件质量兴起，做了诸多的贡献和演讲。他频繁地活跃在软件安全团队之中，为众多知识标准的制定而努力，包括"公共的弱势列举（CWE）"，"攻击模式列举和分类（CAPEC）"，还有其他一些国土安全局和国防部的软件保证项目。他也是空军应用软件保证中心的首席技术专家。

Robert J. Ellison

作为一名软件工程机构 CERT 项目可持续系统工程团队成员，Robert J. Ellison 在团队里是十分重要的技术和管理角色。他是一个软件工程发展环境和相关开发工具的评估小组的领导成员。他也是一位为 SEI 提供建议的卡耐基·梅隆大学的小组成员；他于 1985 年作为参与者参与 FFRDC 新组织。

在进入卡耐基·梅隆大学之前，Ellison 在布朗大学的威廉斯学院和汉密尔顿学院讲授数学。在汉密尔顿学院任教期间，他指导了计算机科学课程的创新。同时，Ellison 也是美国计算机协会（ACM）会员和美国电气与电子工程师协会（IEEE）计算机分会会员。

Ellison 经常从安全和可靠性度量方面，参与软件架构的评估。他的研究主要是如何用经验将

安全问题集成到整个软件架构和设计中。他现在的工作集中于可论证框架的开发和研究，以帮助构建师挑选和精炼设计方案来应对网络攻击。他将在可持续分析框架的改进方面继续研究。

Gary McGraw

Gary McGraw 是总部位于华盛顿地区软件安全和质量咨询公司 Cigital 的首席技术官。他是一名全球公认的软件安全权威人士，也是六大软件安全畅销书的作者。最新的书是《Exploiting Online Games》(Addison - Wesley, 2008)，其他著作包括《Java Security》、《Building Secure Software》、《Exploiting Software》和《Software Security》。他也是 Addison - Wesley 软件安全系列的编辑。McGraw 博士已经撰写了 90 多篇同行评审的科技出版物，为 darkreading. com 撰写每月安全专栏，作为软件安全专家频繁地被新闻界引证。

除了作为一名为顶级商业和信息技术执行机构提供服务的战略顾问，McGraw 博士致力于防御软件和 Raven White 咨询平台。他从印第安那大学获得了认知科学和计算机科学双博士学位，在大学里他为信息情报学院的 Dean 咨询委员会服务。McGraw 博士也是 IEEE 计算机分会董事会的一名成员，每月都为《IEEE Security & Privacy》创作播客：Silver Bullet Security。

Nancy R. Mead

Nancy R. Mead 是一名可持续系统工程小组的高级技术职员，这个组是软件工程机构 CERT 计划的一部分。她也是一名卡耐基·梅隆大学的软件工程硕士和信息系统管理项目硕士。她的研究兴趣涉及信息安全，软件需求工程和软件构建领域。

在参加 SEI 之前，Mead 曾是 IBM 联邦系统的高级技术职员，在那里，她将其全部精力花在巨大的实时系统开发和管理上。她也在 IBM 软件工程技术领域和 IBM 联邦系统软件工程教育局工作过。她已经在许多大学和专业教育课上开展和教授了众多软件工程精品课程。

迄今为止，Mead 已经发表了超过 100 篇的出版物，也被邀演讲。她既是 IEEE 会员，也是 IEEE 计算机协会会员，同时也是 ACM 会员。Mead 从纽约大学获得数学学士和硕士，并从纽约工学院获得数学博士学位。

专业成就人生
立体服务大众

HZ BOOKS

www.hzbook.com

填写读者调查表 加入华章书友会
获赠精彩技术书 参与活动和抽奖

尊敬的读者：

感谢您选择华章图书。为了聆听您的意见，以便我们能够为您提供更优秀的图书产品，敬请您抽出宝贵的时间填写本表，并按底部的地址邮寄给我们（您也可通过www.hzbook.com填写本表）。您将加入我们的“华章书友会”，及时获得新书资讯，免费参加书友会活动。我们将定期选出若干名热心读者，免费赠送我们出版的图书。请一定填写书名书号并留全您的联系信息，以便我们联络您，谢谢！

书名：　　书号：7-111-(　　)

姓名：	性别：☐男 ☐女	年龄：	职业：
通信地址：		E-mail：	
电话：	手机：	邮编：	

1. 您是如何获知本书的：

☐朋友推荐 ☐书店 ☐图书目录 ☐杂志、报纸、网络等 ☐其他

2. 您从哪里购买本书：

☐新华书店 ☐计算机专业书店 ☐网上书店 ☐其他

3. 您对本书的评价是：

技术内容	☐很好	☐一般	☐较差	☐理由_____
文字质量	☐很好	☐一般	☐较差	☐理由_____
版式封面	☐很好	☐一般	☐较差	☐理由_____
印装质量	☐很好	☐一般	☐较差	☐理由_____
图书定价	☐太高	☐合适	☐较低	☐理由_____

4. 您希望我们的图书在哪些方面进行改进？

_____

_____

5. 您最希望我们出版哪方面的图书？如果有英文版请写出书名。

_____

_____

6. 您有没有写作或翻译技术图书的想法？

☐是，我的计划是_____ ☐否

7. 您希望获取图书信息的形式：

☐邮件 ☐信函 ☐短信 ☐其他_____

请寄：北京市西城区百万庄南街1号 机械工业出版社 华章公司 计算机图书策划部收

邮编：100037 电话：(010) 88379512 传真：(010) 68311602 E-mail: hzjsj@hzbook.com

目　录

第 1 章

为什么安全是软件的问题[⊖]

1.1 概述

软件无处不在，它在你的车里运行，它控制着你的手机；你通过软件来进行银行金融服务；你通过软件来接收水、电和天然气；你从一个海岸飞到另一个海岸也离不开软件［McGraw 2006］。不管我们是否意识到它的存在，我们都依赖于以因特网为信息交流和数据传输中介并且具有复杂性、互连性和软件密集性的信息系统。

构建、部署、操作和使用一个在开发过程中没有考虑安全性的软件是一个很大的风险，就像在高空走钢丝而下面没有保护网一样（见图 1-1）。风险的等级就好比你从多高的空中坠下和潜在的影响（没有双关的意思）。

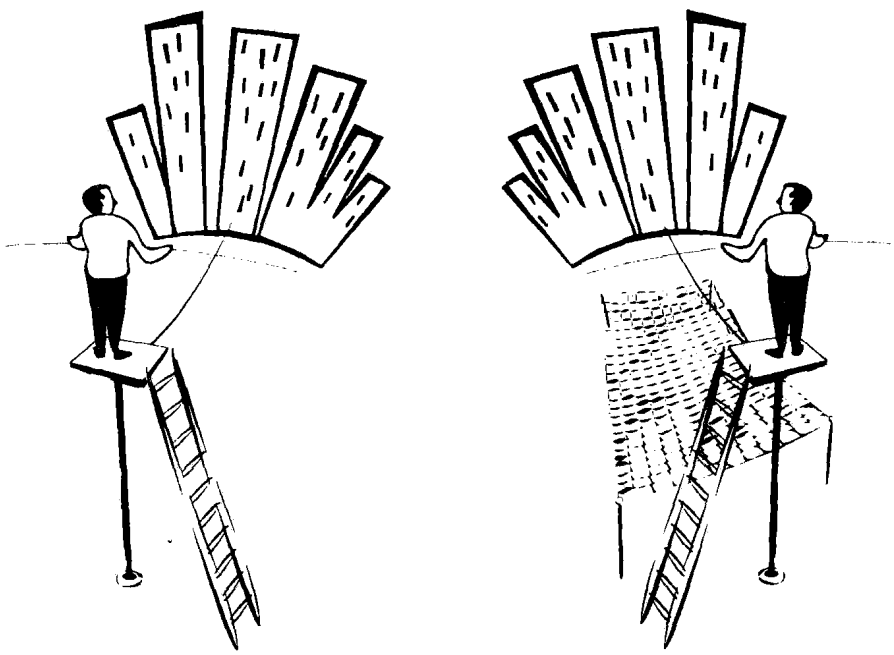


图 1-1 开发软件不考虑安全性和高空中走钢丝而下面没有保护网一样

⊖ 本章内容主要参考了《Security in the Software Lifecycle: Making Software Development Processes-and Software Produced by Them-More Secure》［Goertzel 2006］。有关方面更早的资料出现在［Allen 2007］中。