SEI软件工程译丛

CERT安全指南

The CERT Guide to System and Network Security Practices

[美] 朱莉娅·H·艾伦 [Julia H. Allen] 著
周 赟 译

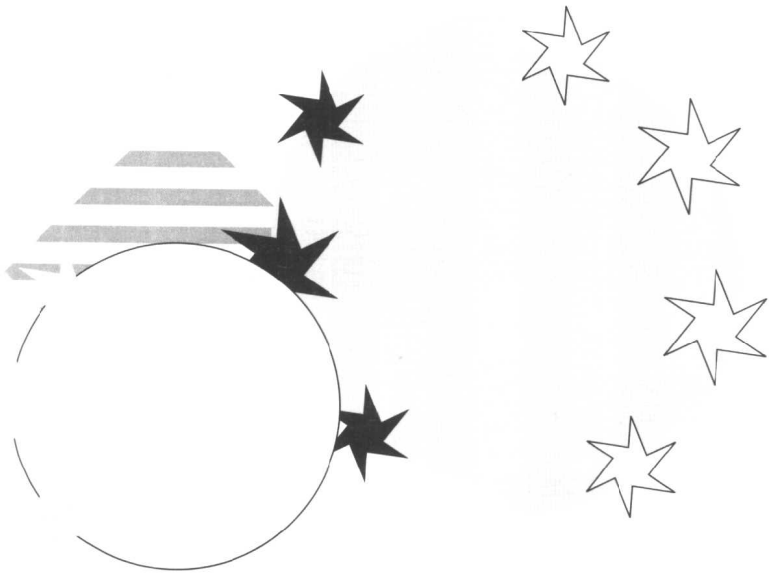
清华大学出版社

SEI软件工程译丛

CERT安全指南

The CERT Guide to System and Network Security Practices

[美] 朱莉娅·H·艾伦 [Julia H. Allen] 著
周 赟 译



清华大学出版社

（京）新登字 158 号

内 容 简 介

本书取材于卡内基·梅隆大学软件工程研究所（SEI）和美国 CERT/CC 合作编写的安全实践与实现文档，是一本专门讲述计算机系统和网络安全的权威指南。它主要围绕着安全缺陷和安全漏洞展开描述，弥补了传统安全问题解决方案的不足。书中以渐进、步步进阶的方式，详细阐述了保护系统和网络安全、检测和响应入侵各阶段所涉及到的每个步骤。通过本书的阅读，管理员可有效保护系统和网络，减少损失。

本书适合各种规模的系统和网络管理员阅读，同时适合他们的直属经理阅读。

图书在版编目（CIP）数据

CERT 安全指南/（美）艾伦著；周赟译.—北京：清华大学出版社，2002
（SEI 软件工程译丛）
书名原文：The CERT Guide to System and Network Security Practices
ISBN 7-302-06021-5
Ⅰ.C... Ⅱ.①艾...②周... Ⅲ. ①计算机网络－安全技术②计算机系统－安全技术 Ⅳ.①TP393.08②TP309
中国版本图书馆 CIP 数据核字（2002）第 083381 号

出 版 者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
http://www.tup.com.cn
http://www.tup.tsinghua.edu.cn
责任编辑：文开祺
印 刷 者：北京牛山世兴印刷厂
发 行 者：新华书店总店北京发行所
开 本：787×960 1/16 印张：24.25 插页：2 字数：453 千字
版 次：2002 年 11 月第 1 版 2002 年 11 月第 1 次印刷
书 号：ISBN 7-302-06021-5/TP·3590
印 数：0001～3000
定 价：49.00 元

出版说明

1984年，美国国防部出资在卡内基·梅隆大学设立软件工程研究所(Software Engineering Institute，简称SEI)。SEI于1986年开始研究软件过程能力成熟度模型(Capability Maturity Model，简称CMM)，1991年正式推出了CMM 1.0版，1993年推出CMM 1.1版。此后，SEI还完成了能力成熟度模型集成(Capability Maturity Model Integration，简称CMMI)。目前，CMM 2.0版已经推出。

CMM自问世以来备受关注，在一些发达国家和地区得到了广泛应用，成为衡量软件公司软件开发管理水平的重要参考因素，并成为软件过程改进的事实标准。CMM目前代表着软件发展的一种思路，一种提高软件过程能力的途径。它为软件行业的发展提供了一个良好的框架，是软件过程能力提高的有用工具。

SEI十几年的研究过程和成果，都浓缩在由SEI资深专家亲自撰写的SEI软件工程丛书(SEI Series In Software Engineering)中。为增强我国软件企业的竞争力，提高国产软件的水平，经清华大学出版社和三联四方工作室共同策划，全面引进了这套丛书，分批影印和翻译出版。这套丛书采取开放式出版，不断改进，不断出版，旨在满足国内软件界人士学习国外经典软件工程高级教程的愿望。

SEI
软件工程译丛

“SEI 软件工程译丛”
编　委　会

SEI
软件工程译丛

总　序

——为清华大学出版社出版“SEI 软件工程译丛”而作

美国卡内基·梅隆大学软件工程研究所(CMU/SEI)是美国联邦政府资助构建的研究单位,由美国国防部主管。他们确认,为了保证软件开发工作的成功,由软件开发人员、软件采办人员和软件用户组成的集成化团队必须具有必要的软件工程知识和技能,以保证能按时向用户交付正确的软件。所谓“正确的”就是指在功能、性能和成本几个方面都能满足用户要求且无缺陷;所谓“无缺陷”就是指在编码后对软件系统进行了彻底的穷举测试修复了所有的缺陷,或保证所编写的代码本身不存在缺陷。

CMU/SEI 为了达到这个目的,提出了创造、应用和推广的战略。这里的“创造”是指与软件工程研究社团一起,共同创造新的实践或改进原有的实践,而不墨守成规。这里的“应用”是指与一线开发人员共同工作,以应用、改进和确认这些新的或改进的实践,强调理论联系实际。这里的“推广”是指与整个社团一起,共同鼓励和支持这些经过验证和确认的、新的或改进的实践在世界范围内的应用,通过实践进行进一步的检验和提高。如此循环,往复无穷。

他们把所获得的成就归纳为两个主要领域。一个是倡导软件工程管理的实践,使软件组织在采办、构建和改进软件系统时,具有预测的能力与控制质量、进度、成本、开发周期和生产效率的能力。另一个是改进软件工程技术的实践,使软件工程师具有分析、预测和控制软件系统属性的能力,其中包括在采办、构建和改进软件系统时,能进行恰当的权衡,作出正确的判断和决策。CMU/SEI 通过出版软件工程丛书,总结他们的研究成果和实践经验,是推广这两个领域经验的重大举措。

SEI 软件工程丛书由 CMU/SEI 和 Addison-Wesley 公司共同组织出版,共分 4 个部分:计算机和网络安全(已出版了 2 本著作),工程实践(已出版了 8 本著作),过程改进和过程管理(已出版了 11 本著作),团队软件过程和个体软件

过程(已出版了3本著作)。前两者属于软件工程技术实践,后两者属于软件工程管理实践。目前这4个部分共出版了24本著作,以向软件工程实践人员和学生方便地提供最新的软件工程信息。这些著作凝聚了全世界软件工程界上百位开拓者和成千上万实践者的创造性劳动,蕴含了大量的宝贵经验和沉痛教训,很值得我们学习。

清华大学出版社邀请我和郑人杰教授共同组织SEI软件工程译丛编委会。清华社计划首先影印6本著作,翻译出版15本著作。据我所知,在Addison-Wesley公司出版的SEI软件工程丛书中,人民邮电出版社已经翻译出版了《个体软件过程》和《团队软件过程》,还拟影印出版《个体软件过程》和《软件工程规范》;电子工业出版社已经翻译出版了《净室软件工程的技术与过程》、《能力成熟度模型CMM 1.1指南》、《能力成熟度模型集成CMMI》和《软件项目管理》;北京航空航天大学出版社已经翻译出版了《统计过程控制》。这些出版社共计影印2本著作,翻译出版7本著作。这样,可以预期我国在今年年底共可影印8本著作,翻译出版22本著作。各个出版社的有远见的辛勤劳动,为我们创造了"引进、消化、吸收、创新"的机遇。我们应该结合各自的实践,认真学习国外的先进经验,以大大提高我国软件工程的理论和实践水平。

在这套丛书中,特别值得一提的是,在过程工程领域被誉为软件过程之父的Humphrey先生所撰写的《软件过程管理》、《技术人员管理》、《软件工程规范》、《个体软件过程》、《团队软件过程》和《软件制胜之道》等6本著作,将于今年年内全部翻译出版,其中《软件过程管理》、《技术人员管理》、《软件工程规范》、《个体软件过程》和《软件制胜之道》这5本著作亦已经或将于今年年内影印出版。

《软件过程管理》是软件过程领域的开创性著作,是为软件公司经理和软件项目经理撰写的。用这本书提出的原理来指导软件开发,可以有效地按照预定进度得到高质量的软件,同时还可了解如何持续进行过程改进。美国CMU/SEI按照这本书提出的原理开发了能力成熟度模型,在国际上得到绝大多数国家的认可和广泛采用,是改进软件过程能力的有力武器。在信息技术迅速发展和企业激烈竞争的今天,能否持续改进过程往往决定企业的命运。

作为一个软件经理,在改进组织的能力之前,首先必须明确绝大多数软件问题是由管理不善所引起的。因此,要改进组织的性能,首先需要改进自己的管理模式。同时还要认识到软件开发是一项智力劳动,需要拥有掌握高技能和忘我工作的技术人员。因此,有效的软件管理需要充分注意技术人员的管理。

《技术人员管理》这本著作就是为达到这个目的而撰写的。高质量的技术

工作要求没有差错，这就要求人们高度专心和高度献身。因此要求人们对他所从事的工作不仅具有高度的责任感，而且具有浓厚的兴趣和高度的热忱。在当前知识经济群龙相争的今天，一个能激励人们进行创造性工作的领导群体，是众多竞争因素中最重要的因素。本书提供了大量的实用指南，可用来有效地改进工程人员、经理和组织的性能。

Humphrey 先生还认为这本书特别适合于在我国工作的软件经理。我国是一个人口大国，拥有大量能干的知识分子，而且信息领域的劳动力价格比国际市场的价格要低，因此吸引了许多国家到我国来投资。但若不提高人员的素质，不在产品质量和进度方面也狠下功夫，就不能在这方面持续保持优势。

《软件工程规范》是为编程人员撰写的。它精辟地阐述了个体软件过程(PSP)的基本原理，详尽地描述了人们如何来控制自己的工作，如何与管理方协商各项安排。在软件工程界，这本著作被誉为是软件工程由定性进入定量的标志。目前在世界范围内，有成千上万的软件工程技术人员正在接受有关 PSP 的培训，以便正确地遵循 PSP 的实践、开发和管理工作计划，在他们承诺的进度范围内，交付高质量的产品。

《软件制胜之道》这本著作描述了团队软件过程的基本原理，详尽地阐述了在软件组织中如何应用 PSP 和 TSP 的原理以及它所能带来的效益。此外，虽然 CMM 同样适用于小型组织，但在其他著作中都没有描述如何应用 CMM 于个体或小型团队，这本书填补了这个空白。应该指出，如果一个组织正在按照 CMM 改进过程，则 PSP 和 TSP 是和 CMM 完全相容的。如果一个组织还没有按照 CMM 改进过程，则有关 PSP 和 TSP 的训练，可以为未来的 CMM 实践奠定坚实的基础。

在软件工程技术实践方面目前共出版了 10 本著作，其中《用商业组件构建系统》、《软件构架实践》和《软件构架评估——方法和案例研究》等 3 本著作详尽地阐述了软件构架的构建、实践和评估。鉴于是否有一个稳定的软件构架，对软件的质量和成本影响很大，因此如何获得一个良好的构架就成为当今软件界研究的重点。我相信这几本著作的出版，将对我国软件构架领域的研究与实践有重要的参考价值。此外，众所周知，计算机与网络的安全问题对信息系统的可靠使用关系极大，《CERT 安全指南》的出版将会对我国在这一领域的研究和实践起积极的促进作用。《风险管理——软件系统开发方法》、《软件采办管理——开放系统和 COTS 产品》、《项目管理原理》、《软件产品线——实践和模式》和《系统工程——基于信息的设计方法》等 5 本著作，分别从风险管理、软件采办、项目管理、软件产品线以及信息系统设计方法等几个方面阐述了大型、复

杂软件系统的开发问题，是有关发展软件产业的重要领域，很值得我国软件产业界借鉴。目前我们所处的时代是信息化时代，是人类进入能够综合利用物质、能量和信息三种资源的时代。千百年来以传统的物质产品的生产、流通、消费为基本特征的物质型经济，将逐步进入以信息产品的生产、流通、利用和消费为基本特征的知识型经济。在这个历史任务中，建造和广泛应用各类计算机应用系统是其公共特征。计算机软件是计算机应用系统的灵魂，没有先进的软件产业，不可能有先进的信息产业，从而也不可能建成现代化的知识型经济。

我们应该看到，在软件领域中我国在总体上离世界先进水平还有相当大的差距。但是，我们不能跟随他国的脚印，走他人的老路。我们应该抓住机遇，直接针对未来的目标，在软件工程技术和软件工程管理两个方面，注意研究 SEI 软件工程丛书中倡导的原理和方法，联系实际，认真实践，并充分利用我国丰富优秀的人力资源和尊重教育的优良传统，大力培养各个层次的高质量的软件工程人员，使其具有开发各类大型、复杂软件系统的能力。我衷心地预祝清华大学出版社影印和翻译出版这套丛书，在把我国建设成为一个真正现代化的软件产业大国的历史任务中起到推波助澜的作用，并请读者在阅读这些译著时，对这套丛书的选题、译文和编排等方面都提出批评和建议。

周伯生

于北京

2002 年 8 月 18 日

前 言

随着 Internet 和其他国际、国内信息基础设施的日益普及，其复杂程度和相互依赖程度也在增加，接入网络的系统也频频遭受未经授权的入侵，而其严重程度也呈增长态势。因此，对于已接入公共网络的企业级网络系统，无论从可能性还是从实用性而言，保障其安全都极为重要。

《CERT[①]安全指南》讲述了保护系统和网络，以防恶意和无意侵害[②]的方法，这些方法实用，将逐步指导您动手进行实践。这些实践主要是为中级系统和网络管理员所写——这些人的日常活动包括安装、配置、操作并维护系统和网络。这些实践提供了易于实现的指南，使管理员保护并安全地操作组成信息技术基础设施的系统、网络、硬件、软件和数据。本书还适合管理员的管理人员（经理）阅读，如果没有管理层的介入和支持，许多实践将不可能实现。

CERT 安全实践讲述了关键的、普遍的安全问题。实践主题是基于 CERT 的安全缺陷方面（2000 年 21 756 条）和安全漏洞方面（2000 年 774 条）的大量数据来拟定的，这些数据提供了其他安全组织无法获得的一些观察结果。这些实践弥补了传统意义上的解决方案（一般为操作系统专用）或常规建议的不足（如缺乏“如何做”的细节）。在本书的帮助下，管理员即可采取行动，增强网络系统的安全。

通过实现这些安全实践，管理员针对 CERT 报告的 75～80％的安全事件，提供融为一体的解决方案和保护机制。[③]每个实践都写成一系列技术性并不强

---

① CERT 已在美国专利和商标局注册。

② 一般指一起或多起机密性、完整性和可用性的违背。

③ 就如 CERT 漏洞分析和 2000 年第四季度事件分析中所确定的那样，2.4 节讨论如何及时更新操作系统和应用程序软件，2.5 节讨论在服务器主机上只提供基本要素，3.3 节描述如何用适宜的对象、设备和文件访问控制来配置 Web 服务器是最高优先级的实践，其中包括了绝大多数已知的漏洞和事件。此外，CRET 安全实践要定期分析，检验是否能抵挡由其他组织发布的顶级安全威胁列表，并坚持提供用于应付至少 80％这类威胁的解决方案。

教训来改进安全性。这部分讲述了实现这些方法所需的实践。

- 附录 A:安全实现。附录包含了几个基于操作规程和工具的实现,其中提供了一个或多个实践的技术特定准则(在支持的实践中提到了适当的实现)。本书所选的实践根据 CERT 的经验,特别适合 Sun Solaris (UNIX)操作环境。它们主要给出最基本的说明,而不一定反映最新版的操作系统。最新的 70 多条 UNIX 和 Windows NT 实现和技术技巧可以在 CERT 网站获得。我们还计划为 Windows 2000 和 Linux 开发其他实现。
- 附录 B:实践级策略考虑事项。这一附录中包含了贯穿本书的所有安全策略事项的指导原则。把这些资料收集到一处,可以帮助您重新审阅并选择策略主题以及生成策略语言。也可把本附录和每章末出现的实践核对清单看作本书的全面总结。

本书最好作为参考。我们不打算让您逐页阅读,最好先浏览每部分和每章的概述,再查阅最感兴趣的实践。

本书所用到的网站地址(URL)在本书出版时是准确的。此外,我们创建了包含书中提及的所有 URL 链接的 CERT 网站。我们计划更新 URL,提供本书勘误表,并在本书出版后加入新的参考内容。在本书的网站(*http://www.cert.org/security-improvement/practicesbk.html*),可找到所有本书提及的参考书、信息来源、工具、出版物、文章和报告的链接。我们还会定期提供所有能在 CERT 网站 *http://www.cert.org* 上发现的 CERT 咨询报告、事件记录、漏洞记录、技术技巧和报告。"CERT 网站"就是指这个 URL。

《CERT 安全指南》取自卡内基·梅隆大学软件工程研究所(SEI)和 CERT 协调中心编制的安全调查与实现文档。CERT/CC 成立于 1988 年,是硕果仅存的、资格最老的计算机安全响应组。该中心为 Internet 上遭受安全入侵的站点提供技术援助和建议,并设立工具和技巧使典型用户和管理员能够有效地保护系统,避免入侵者所导致的损失。软件工程研究所是由美国联邦政府资助的研究和开发中心,该研究所有大量广泛的特许证书,以改进软件工程实践。

5 年以来,本书主要内容一直放在 CERT 网站,并在那里更新。外部商业、联邦政府和学院级学术研究机构中的安全专家和 SEI 工作人员反复评审并使用这些资料。所有资料都已经过定期评审(并尽可能测试),以保持准确性和实时性。

目 录

第Ⅰ部分 计算机安全