

<<软件安全>>

图书基本信息

书名：<<软件安全>>

13位ISBN编号：9787121058899

10位ISBN编号：7121058898

出版时间：2008-3

出版时间：电子工业出版社

作者：麦克劳

页数：332

字数：484000

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：<http://www.tushu007.com>

<<软件安全>>

内容概要

本书是由软件安全领域的权威专家编著，讲授如何实施软件安全的专著。

本书在论述软件安全理论的基础上详细讲解了如何将软件安全付诸实践。

书中描述的软件安全最优方法（或者称为接触点）以优秀的软件工程方法为基础，并且在整个软件开发生命周期中都明确地仔细考量安全问题，即认识和理解普通的风险（包括实现缺陷和体系结构瑕疵）、基于安全进行设计，以及对所有的软件工件都进行彻底、客观的风险分析和测试。

本书的目的是使接触点方法为你所用。

采用本书的方法并不会从根本上改变你的工作方式，但是能够改善现有的软件开发生命周期，并能据此来创建自己的安全的开发生命周期。

本书还介绍了知识管理、培训与认知，以及企业级的软件安全计划等方面的内容。

本书适合与软件相关的任何机构的管理人员、商业人员、软件架构人员、软件开发人员、软件测试人员以及安全管理人员阅读，可以作为大学、研究机构和培训机构的计算机安全和软件安全课程的教材和参考书。

<<软件安全>>

作者简介

Gary McGraw, 博士, Cigital公司的首席技术官和董事会成员。

他也是软件安全领域的世界级权威, 与人合著了5部最畅销的安全方面的著作: 与rootkit.com的Greg Hoglund合著《利用软件的弱点》(Exploiting Software; Addison-Wesley出版社, 2004); 与John Viega合著《建造安全的软件》(Building Secure Software; Addison-Wesley出版社, 2001); 与普林斯顿大学的Ed Felten教授合著《Java的安全性: 有害的小程序、漏洞和解决方法》(Java Security: Hostile Applets, Holes, and Antidotes; Wiley出版社, 1996)。

<<软件安全>>

书籍目录

第1部分 软件安全基础	第1章 学科定义	1.1 安全问题	1.2 软件中的安全问题	1.3 解决问题：软件安全的三根支柱	1.4 安全工程的兴起软件安全人人有责	第2章 风险管理框架	2.1 实际应用风险管理	2.2 如何使用本章	2.3 活动的五个阶段	2.4 RMF是一种多重循环	2.5 应用RMF：KillerAppCo的iWare 1.0 Server	2.6 测量的重要性	2.7 Cigital Workbench	2.8 风险管理是软件安全的一种框架																																
第2部分 软件安全的七个接触点	第3章 软件安全接触点简介	3.1 概述：七个极好的接触点	3.2 黑与白：紧密难分地缠绕在一起的两种思路	3.3 向左移动	3.4 接触点是最优方法	3.5 谁应该实施软件安全建立一个软件安全组	3.6 软件安全是一种多学科工作	3.7 走向成功的接触点	第4章 利用工具进行代码审核	4.1 (用工具)尽早发现实现中的缺陷	4.2 目标是良好，而不是完美	4.3 古老的历史	4.4 静态分析的方法	4.5 进行研究的工具	4.6 商业工具供应商	4.7 接触点方法：代码审核	4.8 利用工具查找安全缺陷	第5章 体系结构风险分析	5.1 安全风险分析方法中的共同主题	5.2 传统风险分析的术语	5.3 知识要求	5.4 森林级视图的必要性	5.5 一个传统的风险计算的例子	5.6 传统方法的局限	5.7 现代风险分析	5.8 接触点方法：体系结构风险分析	5.9 风险分析入门	5.10 体系结构风险分析是必需的																		
第6章 软件渗透测试	6.1 渗透测试的现状	6.2 软件渗透测试——一种更好的方法	6.3 在开发过程中应用反馈回来的测试结果	6.4 利用渗透测试来评估应用程序的状态	6.5 正确的渗透测试是有益的	第7章 基于风险的安全测试	7.1 安全问题为何与众不同	7.2 风险管理与安全测试	7.3 如何实现安全测试	7.4 考虑(恶意的)输入	7.5 摆脱输入	7.6 与渗透测试一起交替向前推进	第8章 滥用案例	8.1 安全并不是一组功能特性	8.2 你不能做的事情	8.3 创建有用的滥用案例但是根本没有人会这样做！	8.4 接触点方法：滥用案例开发	8.5 一个滥用案例的例子	8.6 滥用案例很有用处	第9章 软件安全与安全操作相结合	9.1 请别站得离我太近	9.2 (软件安全的)万全之策	9.3 (立即)一起协同工作	9.4 未来如此光明，我必须戴墨镜了	第3部分 软件安全的崛起	第10章 企业级的软件安全计划	10.1 商业氛围	10.2 分步进行	10.3 制订一个改进计划	10.4 建立一种衡量方法一种分三步进行的企业实施方法	10.5 持续不断地改进	10.6 商业现货软件(以及现有的软件应用程序)又该怎么办一种企业信息体系结构	10.7 采用一种安全的开发生命周期	第11章 软件安全知识	11.1 经验、专业知识与安全	11.2 安全知识：一种统一的观点	11.3 安全知识与接触点	11.4 美国国土安全部的Build Security In门户网站	11.5 知识管理不断发展	11.6 现在开始实施软件安全	第12章 编码错误分类法	12.1 关于简化：七加二或者减二	12.2 门需要更多门	12.3 一个完整的例子	12.4 清单、堆和集合	12.5 (与分类法一起)前进并取得成功
第13章 附说明的参考书目和文献	13.1 附说明的参考书目：最近发表的作品	13.2 软件安全的难题基础科学：还需继续研究的领域	第4部分 附录	附录A Fortify源代码分析套件指南	A.1 审核工作台简介	A.2 手工审核源代码	A.3 确保一个可用的建造环境	A.4 运行源代码分析引擎	A.5 研究基本的SCA引擎命令行参数	A.6 理解原始分析结果	A.7 集成一种自动建造过程	A.8 使用Audit Workbench	A.9 审核开源应用程序	附录B ITS4规则	附录C 关于风险分析的练习：Smurfware	C.1 Smurfware SmurfScanner风险评估案例研究	C.2 Smurfware SmurfScanner安全设计	附录D 术语表索引																												

<<软件安全>>

媒体关注与评论

“我讨厌充满了愚蠢的安全漏洞的软件。

如果你要编写一款我将来可能会使用的软件，那你就需要阅读并理解这本书。

” “Gary的书告诉了我们早就应该知道的知识：在你开发软件时，最好使安全成为必需的组成部分，而且，他还说明了如何使安全成为必需的组成部分。

” ——Marcus J. Ranum 防火墙的发明人Tenable Security公司首席科学家 “对于软件安全来说，最难缠的就是实现细节。

本书解决了其中的细节问题。

” ——Bruce Schneier Counterpane公司的CTO和创建人

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:<http://www.tushu007.com>