<<软件安全工程>>

图书基本信息

书名：<<软件安全工程>>

13位ISBN编号：9787111264835

10位ISBN编号：7111264835

出版时间：2009-4

出版时间：机械工业出版社

作者：艾伦

页数：222

译者：郭超年,周之恒

前言

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。

<<软件安全工程>>

内容概要

本书系统阐述了软件安全丁程的知识。
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、软件安全及软件丁程管理的技术人员的参考用书。

与其他软件相比，遵循安全理念开发的软件可以更为有效地抵御、容忍攻击并从攻击中恢复。尽管并不存在软件安全的万能解决方案，但是项目经理可以从中获益的实例还是存在的。
通过本书，你能找到一些可靠的实例，这些实例有助于提高软件在开发和运行过程中的安全性和可信度。

本书会帮助你理解：　　软件安全不仅仅是消灭漏洞和执行入侵检测。

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。

软件安全的主动行为必须伴随一种危险控制的方法，从而识别优先级以及定义什么才是“足够好的”——对软件安全危险的理解随着软件开发生命周期而不断改变。

项目经理和软件工程师需要学会以攻击者的方式来思考，从而指出软件不能运行的功能范围，以及软件如何更好地抵御、容忍攻击并从攻击中恢复。

作者简介

艾伦，曾获得密歇根大学的计算机科学学士学位和南加利福尼亚大学的电子工程硕士学位，目前是SEI的CERT项目的高级研究员。

<<软件安全工程>>

书籍目录

章节摘录

插图：第1章 为什么安全是软件的问题1.2 问题各种机构逐渐使用直接连接到因特网的软件密集型系统来存储、处理和传输敏感的数据。
人们在网上开户、购物、付税、买保险、投资、给孩子注册学校、参加各种组织和社交网络的私人金融交易数据常常被暴露。
由全球互联引起的信息暴露使得敏感的数据和处理互联的软件系统在面对非蓄意和未经授权的使用时更加脆弱。
总之，软件密集型系统与其他具有软件功能的系统已经提供了比以前更开放、更广泛的敏感信息的访问，包括个人身份信息。
当前，信息战[Denning1998]、网络恐怖主义和电脑犯罪的时代已经来临。
恐怖分子、罪犯团伙和其他罪犯时刻都在觊觎整个软件密集型系统，他们经过努力成功地进入了这些系统。
这些系统，大多数都没有抵御攻击的能力或攻击反弹的能力去和入侵者对抗。
在一份给美国总统的标题为“网络安全——优先级之间的危机”的报告中[PITAC2005]，总统信息技术顾问委员会把不安全软件存在的问题归结为：软件开发还不是一门严格的学科，并且开发过程基本上没有控制其受攻击者攻击可能性的最小化。
当前，那些存在漏洞的软件如同生物体被病魔感染，被入侵和篡改，从而使先前正常的软件遭到破坏，同时被感染的软件可以自身复制并通过网络传播来破坏其他系统。
而这些具有破坏性的漏洞也正如病魔一样，不易被病人发现，即使专家们发现了，他们的威胁也一直在增长。

媒体关注与评论

“这本书的系统论述可以为一些组织提供帮助，使它们能够选择一组符合其安全成熟性，抗风险能力和开发风格的工序，策略或技术；可以帮助你理解如何将实用的安全技术纳入到开发周期的各个阶段之中。”

——微软高级安全专家 Steve Riley“有一些书讨论了本书中的某些问题，也有一些书论述了安全系统工程；但却很少像本书一样，通俗易懂地描述和讨论关子整个软件开发周期的最新动态和主题。”

——Harrls高级软件安全专家 Ronda Henning

版权说明