<<C安全编码标准>>

图书基本信息

书名：<<C安全编码标准>>

13位ISBN编号：9787111284420

10位ISBN编号：7111284429

出版时间：2010-1

出版时间：机械工业出版社

作者：Robert C. Seacord

页数：496

译者：徐波

前言

在C编程语言中，安全编码的一个本质要素是具有良好文档的、可实行的编码标准。
编码标准鼓励程序员遵循一组根据项目或组织的要求所确定的统一指导方针，而不是根据程序员的熟悉或偏好来作出决定。
编码标准一经确立之后，就可以作为标尺，对源代码进行评估（使用手工或自动的过程）。
《CERTc安全编码标准》（TleCERTCSecureCodingStandard）提供了在c编程语言中进行安全编码的指导方针。
这些指导方针的目标是消除不安全的编码实践以及可能被利用而导致潜在风险的未定义行为。
在开发代码时遵循这些标准将会产生高质量的软件系统，使它们具有更健壮的行为，对攻击的抵抗性也更强。
本标准受到软件工程协会（SEI）和其他得到许可的伙伴培训部门的支持，并可以作为全球信息保证认证（GIAC）安全软件程序员一c（GSSP-C）考试和认证的基础。
安全软件的需求　　1988年11月发生的Morris蠕虫事件导致10%的Internet系统中止，并使人们对安全软件系统有了一个新的、准确的认识。
20年后，许多安全分析师、软件开发人员、软件用户和策略制定者都在问同一个问题：“为什么软件不能变得更安全？
”　　首要的问题是“软件安全”这个术语用在当今已经没有意义。
和其他人一样，我也试图定义这个术语，但是并不存在被广泛接受的定义。
这是为什么呢？
人们已经提出了软件不能变得更安全的各种原因：工具不够充足、程序员缺乏足够的培训、开发周期太短等。
但是，这些都是可以克服的问题。
问题的根源在于其他方面。
软件不能变得更安全的原因是缺少对安全软件的需要。
简单地说，如果一家开发商已经推出了一种功能更丰富、性能更出色的产品，而另一家开发商却提供了一种虽然安全但功能和性能稍差的产品，并且6个月之后才能上市。
毫无疑问，顾客会购买第一种产品，生产商也深知这一点。
为什么顾客不愿购买安全产品呢？
这是由于“安全”这个词在这种情况下是没有意义的。
顾客为什么要放弃看得到的好处，而去购买一种定义不明确的、不可触摸的属性呢？
本编码标准就致力于解决这个问题。
虽然在开发代码时遵循这个标准并不保证软件系统的安全性，但是它向我们提供了大量与代码的质量和安全有关的知识。
它告诉我们在开发软件时应该遵循一组由该领域的前沿专家所开发的行业标准的规则和建议。
它还告诉我们在开发软件时遵循这个标准可以使我们把注意力和精力集中在编写代码上，而不会受到一些常见的编码错误的困扰。
在过去的20年里，CERT协作中心已经接到报告并发表了无数由于这些编码错误导致的潜在风险。
它告诉我们生产代码的软件开发人员对违反这个标准可能导致并被利用的各种潜在风险具有深入的理解，因此在开发软件时头脑中已经形成了真正的安全思想。
因此，我们在本书中已经着手处理的一个“小”问题是改变开发和购买软件系统的市场动态。
通过为C语言程序产生一个“可供行动参考的和可测量的”定义，即遵循这个标准中的规则和建议。
我们定义了一种机制，顾客可以通过这种机制来要求安全的软件系统，而生产商也可以根据这种机制来满足顾客的要求。

<<C安全编码标准>>

内容概要

本书提供了在C编程语言中进行安全编码的指导方针，描述了C语言程序中导致软件潜在风险根源的编码错误，并根据严重性、被利用的可能性以及修补成本设置了优先级。
每个指导方针提供了不安全代码的例子以及安全的替代方案。
如果统一应用这些指导方针，可帮助消除导致缓冲区溢出、格式字符串潜在风险、整数溢出和常见的软件潜在风险的关键编码错误，从而创建更健壮的高质量软件系统。
本书内容新颖，讲解详尽，可作为软件开发技术人员的参考用书。
软件安全性对于公司的运作和财富具有很大的影响，与个人的生活也息息相关。
为了创建安全的软件，开发人员必须知道什么地方存在危险。
C的安全编码要比许多经验丰富的程序员所想像的更为困难。
本书是一本重要的桌面参考手册，记录了《CERT C安全编码标准》的第一次官方发布。
这个标准逐项描述了C语言程序中导致软件潜在风险根源的编码错误，并根据严重性、被利用的可能性以及修补成本设置了优先级。
每个指导方针提供了不安全代码的例子以及安全的替代方案。
如果统一应用这些指导方针，可以消除可能导致缓冲区溢出、格式字符串潜在风险、整数溢出和常见的软件潜在风险的关键编码错误。

作者简介

RobertC.Seacord，在位于宾夕法尼亚州匹兹堡市的软件工程协会（SEI）的CERT小组倡导了安全编码活动。
除了其他与安全相关的活动，CERT还定期分析软件潜在风险报告，并评估它们对Intemet和其他关键的基础结构的风险。
Robea是CarnegieMellon大学计算机科学系和信息网络协会的助理教授，并在Pittsburgh大学兼职。
作为一名电子技术专家，Rob.err已经出版了SecureCodeinginCandC++》（Addison.Wesley，2005）、（BuildingSystemfromCommercialcomponents}（Addison-Wesley，2002）和《ModernizingLegacysystems））（Addison-Wesley，2003）3本书，并发表了40余篇有关软件安全、基于组件的软件工程、基于Web的系统设计、遗留系统的现代化、组件仓库、搜索引擎以及用户界面设计和开发的论文。
Rob.ert于1982年开始在IBM做一名专业的程序员，致力于通信和操作系统软件开发、处理器开发和软件工程。
Robea还在XConsortium工作过，为通用桌面环境和XWindow系统开发和维护代码。
他是CarnegieMellon大学在PL22.11（ANSI“C”）的代表，并且是c编程语言的JTCl／SC22／WGl4国际标准化工作组的一位技术专家。

<<C安全编码标准>>

书籍目录

章节摘录

本标准中的规则可以用特定组织的规则进行扩展，但是后者必须遵循本标准中的规则，以实现与本标准的顺应性。

软件专业人员可以通过培训，理解如何正确地应用安全编码标准。
通过考试，这些经过培训的程序员可以认证为安全编码专业人员。

当一种安全编码标准确立之后，可以开发或修改一些工具，以确定与标准的顺应性。
编码实践中的某个条件是否可以看成是规则取决于是否可以验证它的顺应性。
验证可以手工进行，也可以用自动化工具完成。
手工验证不仅需要很大的工作量，而且很容易出错。
工具验证也存在问题，由于可能存在回归错误，所以静态分析工具检测规则的所有偏离的能力必须在每个产品发布中都得到证明。
即使面临这些挑战，自动化验证仍然是经济上惟一可行的用于验证编码标准顺应性的解决方案。

软件分析工具可以认证为能够验证与这个安全编码标准的顺应性。
顺应性软件系统可以由一个得到适当授权的认证机构通过使用认证工具认证为是顺应性的。
系统质量　　安全性是在选择和应用编码标准时必须考虑的系统属性之一。
其他需要考虑的属性还有可移植性、可靠性、可用性、可维护性、可读性和性能等。

在这些属性中，有许多属性以有趣的方式相互关联。
例如，可读性是可维护性的一个属性，它们对于在维护时防止产生可能导致安全漏洞或可靠性问题的缺陷是极为重要的。
另外，可读性有助于提高代码的检查效率。
可靠性和可用性都要求适当的资源管理，与系统的安全密切相关。
像性能和安全这样的系统属性常常存在冲突，需要考虑两者之间的权衡。

这个安全编码标准的目的是提高软件的安全性。
但是，由于安全性和其他系统属性之间的关系，主要针对其他系统属性的建议对于系统的安全性往往也具有重要的意义。

媒体关注与评论

“我是CERT安全编码活动的热情支持者。
程序员可以找到关于正确性、清晰性、可维护性、性能等方面的很多建议，但对于特定的语言特性如何影响安全性方式的建议则明显缺乏。
本书填补了这个空白。
”——RandyMeyers，ANSIC主席 “在过去的几年里，我们依赖于CERT/CC公布各种建议，它们记录了无尽的安全问题。
现在，CERT已经汇集了前沿技术专家的建议，向程序员和项目经理提供了实用的指导方针，避免在新的应用程序中出现这些问题，并帮助实现安全的遗留系统。
干得好！
”——ThomasPlum，PlumHall，Inc.创始人 “互联网的存在极大地增加了对安全、防黑客应用程序的需要。
通过组合这个CERT标准和其他安全指导方针，顾客可以获得全面的保护以及创建零缺陷软件的方法。
”——ChrisTapp，领域应用程序工程师，LDRALtd “我觉得这个标准是无可代替的，它汇集了许多专家信息，让我们了解现代的软件系统在实践中是如何失败的。
它是创建一个国际安全编码指导方针的良好起点。
其他地方找不到这样的信息。
就软件安全这个问题而言，你不知道的东西常常会给你带来伤害。
”——JohnMcDonald，《TheArtofSoftwareSecurityAssessment》的作者之一

<<C安全编码标准>>

编辑推荐

一本重要的桌面参考手册，记录了《CERTC安全编码标准》的第一次官方发布　　每一位C程序员的案头必备　　内容新颖，讲解详尽　　实现C安全编程的权威指南

<<C安全编码标准>>

版权说明