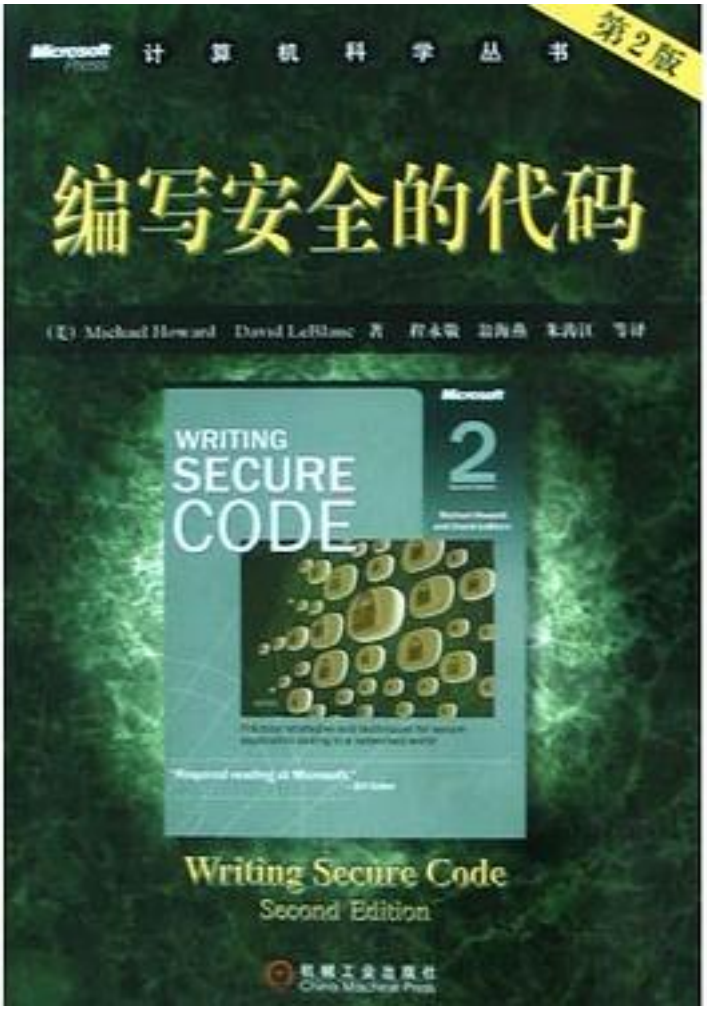
编写安全的代码



编写安全的代码_下载链接1_

著者:〔美〕Michael Howard Da

出版者:

出版时间:2002-1

装帧:

isbn:9787111102854

对于“是否有这个必要”的疑问，在书中（第1章）作者是如此回答的：首先，时代在

变，从“World Wide Web”（万维网）到“Wild Wild Web”（混乱无序的网）绝非文字游戏。在如今这个充满了敌意的网络环境里面，编写的代码必须经得起考验，而再用旧的思维模式去思考新的问题是非常危险的。其次，安全的产品同时也是高质量的产品，安全是高质量产品的一个子集。再次，媒体和竞争对手都喜欢在安全问题上大做文章，这些都是能上头条新闻的信息，屡屡成为牺牲品的公司不厌其烦，微软即是一个典型的例子。最后一点就是，修补安全漏洞的代价是十分高昂的。除了直接的人力和误工等损失之外，还包括改善公共关系和客户信任度的降低的损失，我把它称之为“商誉”上的损失。这四点从企业的角度对此做出了回答。

对于个人而言，也有着种种的不解（附录D）：①没有人会做那事！②我们从来没有受到过攻击。③我们使用了密码、ACL和防火墙，所以安全。④检查过代码，没有安全bug。对这些问题，作者显然有着丰富的实践经验：

①当苦口婆心地告诉某个开发小组一定要做缓冲溢出测试时，大家显然不相信。于是作者现场编写了一个Perl的小脚本，它神奇地生成了一个伪造的包，发送给产品打开的Socket后，轻易地就击溃了他们的服务器。②作者与一个产品开发组工作之时，对方信誓旦旦地说他们从来没有受到过攻击，没有问题。然而就在他们被第一次攻击之时，突然就涌现了另外的数个安全漏洞。黑客的嗜好就是发现漏洞，然后广而告之，然后继续探查你的其他漏洞，问题迅速扩大化。③作者告诫大家要避免以下错误：自创“加密”算法；不安全地存储密码；使用“任何人”的ACL。防火墙只是安全体系的一环，并非全部。例如，很多攻击都是通过HTTP，也就是一个通常开放的端口来进行的。④如果不知道安全bug是什么样子，当然就没有那个问题了。

正如书中前言所提到的那样，《编写安全的代码》一书“教你以安全的方式设计、编写和测试应用程序是本书惟一的目的”，始终围绕着应用程序安全的话题进行讨论，从实践的角度对代码安全进行了全程的指导。同时，这也是“第一本指导程序员从内部加强软件安全的书籍”，是一本主要面向程序员，涉及各种攻击漏洞的安全分析，并指导人们从开发阶段即开始加强软件安全的书。在此，我把它推荐给所有关心代码安全的朋友们阅读。

作者介绍:

目录:

编写安全的代码_下载链接1_

标签

安全

计算机

Security

编程

Programming

M$

评论

关注微软产品安全的人不能不读的书

编写安全的代码_下载链接1_

书评

编写安全的代码_下载链接1_