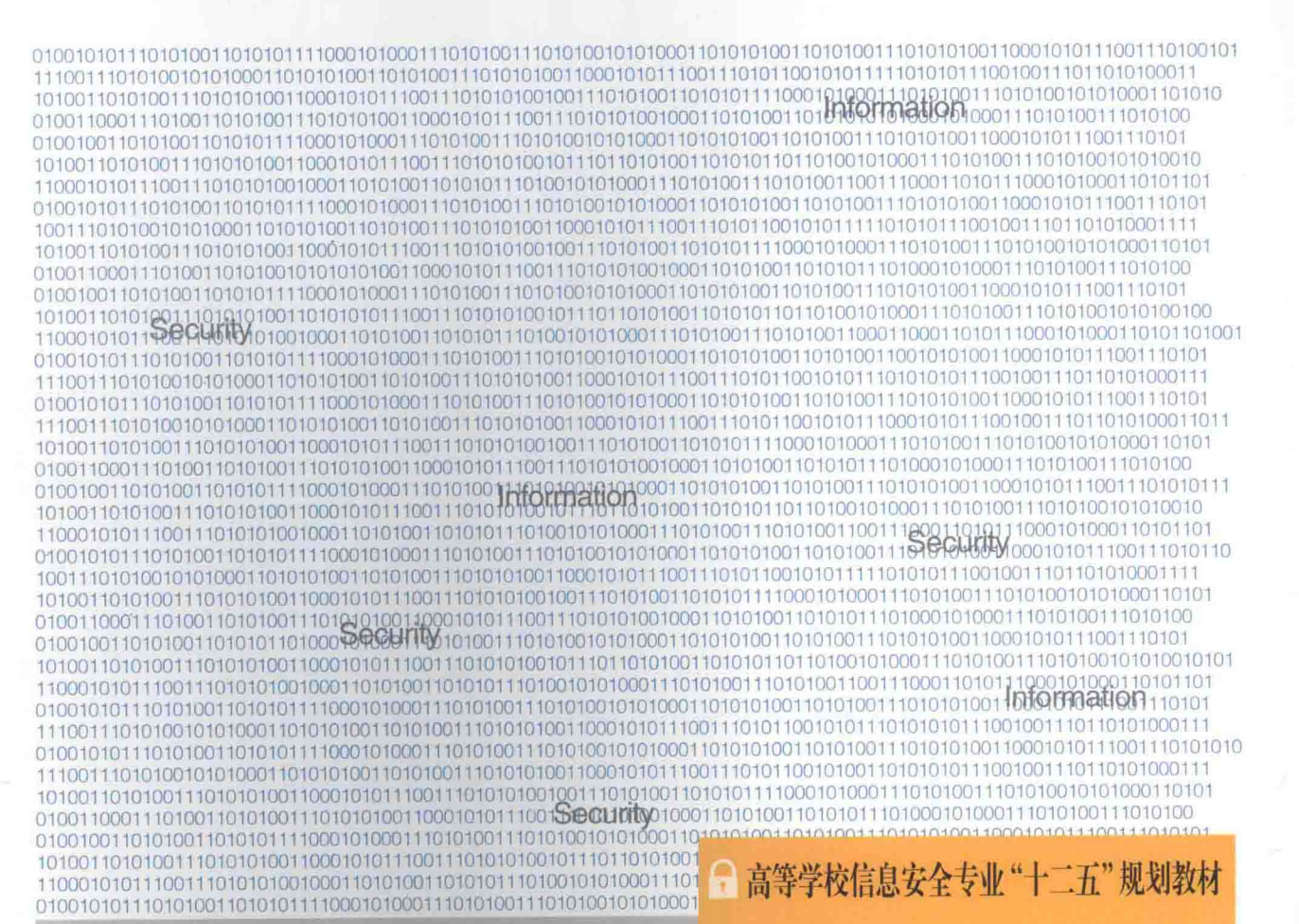

高等学校信息安全专业“十二五”规划教材

彭国军　傅建明　梁玉　编著

软件安全

WUHAN UNIVERSITY PRESS
武汉大学出版社

高等学校信息安全专业“十二五”规划教材

软件安全

彭国军　傅建明　梁玉　编著
张焕国　审校

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

软件安全/彭国军,傅建明,梁玉编著. —武汉:武汉大学出版社,2015.9
高等学校信息安全专业“十二五”规划教材
ISBN 978-7-307-16496-3

Ⅰ.软… Ⅱ.①彭… ②傅… ③梁… Ⅲ.软件开发—安全技术—高等学校—教材 Ⅳ.TP311.52

中国版本图书馆 CIP 数据核字(2015)第 186904 号

责任编辑:林 莉 责任校对:汪欣怡 版式设计:马 佳

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)
(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)
印刷:湖北金海印务有限公司
开本:787×1092 1/16 印张:20.75 字数:525 千字 插页:!
版次:2015 年 9 月第 1 版 2015 年 9 月第 1 次印刷
ISBN 978-7-307-16496-3 定价:45.00 元

高等学校信息安全专业“十二五”规划教材

编委会

前 言

软件是计算机系统的灵魂、信息化的核心以及互联网应用的基石。现代社会对信息系统的依赖主要体现为对软件的依赖，而且信息系统的缺陷在很大程度上也是因为软件问题产生的。

目前，软件安全正面临严峻挑战。一方面，随着软件规模的不断增大，软件的开发、集成和演化变得越来越复杂，这导致软件产品在推出时总会含有很多已知或未知的缺陷，这些缺陷对软件系统安全的可靠运行构成了严重的威胁。另一方面，软件的运行和开发环境从传统的静态封闭状态演变成互联网环境下动态开放的状态，越来越多的软件漏洞和缺陷被发现。更为重要的是，受经济利益驱使，目前计算机病毒及黑客地下产业链活动非常猖獗，软件漏洞被广泛利用，恶意代码急剧增加，且传播速度大大加快，另外 APT（Advanced Persistent Threat，高级可持续性威胁）攻击活动不断，攻击手段防不胜防，触及国家关键基础设施和各类重要信息系统，其对我国网络空间安全甚至国家安全形成了巨大威胁。

为了进一步增强学生对目前软件安全所面临的各类威胁的本质与其实现机理的理解，促使学生掌握目前系统安全防护领域的各类核心技术与理论，以提升学生的实践创新能力和学生综合利用专业基础知识来设计和研发信息安全防护产品的能力，我们编写了本教材。同时，希望借此可为学生今后的发展提供一定的专业引导，进一步激发学生的专业兴趣，增强学生的专业使命感，期盼越来越多的优秀人才投入到我国的网络空间安全事业中来，为我国的网络空间安全保障不断添砖加瓦。

本书第一部分对软件安全的基础知识进行了介绍。

其中，第 1 章从信息的概念入手，介绍了信息、信息安全的定义、属性、发展，进而描述了软件安全的概念、面临的具体威胁和来源，最后对目前典型的软件安全防护手段进行了介绍。通过本章的学习，读者将能较全面了解软件安全的基本概念、其面临的主要问题和挑战，以及目前典型的安全防护手段。

软件安全涉及较多的计算机基础知识，如磁盘结构、文件系统、CPU、内存管理、操作系统、文件格式等。第 2 章介绍了计算机的磁盘管理、Windows 的文件系统、处理器的工作模式、Windows 内存结构与管理、计算机的引导过程、EXE 文件格式等与软件安全相关基础知识。该章将为读者继续学习后续各章的专业知识打下必要的基础。

本书第二部分对软件安全的重要威胁之一“软件漏洞”的机理、利用方法与防护技术手段进行了讲解和分析。

第 3 章重点阐述了软件漏洞的概念、分类及其对系统的具体威胁，同时分析了软件漏洞产生的具体原因，攻击者利用软件漏洞的具体方式，最后还对一部分典型的软件漏洞进行了介绍。

第 4 章对两类典型的软件漏洞（缓冲区溢出漏洞及 Web 类漏洞）进行了具体的机理分析。

第5章描述了软件漏洞的具体利用方法，包括Exploit与ShellCode的编写机理，同时对软件漏洞利用的平台和框架进行了介绍，最后还对软件漏洞挖掘技术及工具进行了介绍。

第6章对微软在Windows系统中针对漏洞利用的典型防护手段和机制进行了介绍，包括数据执行保护（DEP）、栈溢出检查（GS）、地址空间分布随机化（ASLR）及SafeSEH等。通过本章的学习，可以掌握目前操作系统在漏洞防护方面的一些具体措施，同时还能够了解攻击者与操作系统在漏洞攻防方面的博弈过程。

针对目前存在的各类软件安全问题，第7章基于软件开发的整个过程介绍了安全软件设计的具体流程和方法。

恶意软件是软件安全的重大安全隐患。作为本书内容的重中之重，第三部分重点讲解和分析了恶意代码的攻防技术与手段。

其中，第8章介绍了恶意代码的定义及具体分类，第9章重点详细地介绍了几类典型的恶意代码（包括计算机病毒、网络蠕虫、木马、Rootkit，以及手机恶意软件等）的具体实现机理。

第10章主要描述了目前流行的各类反病毒技术和手段。本章对特征值检测技术、校验和检测技术、虚拟机检测技术、启发式扫描技术、主动防御技术及云查杀技术等进行了介绍，接着讲解了恶意软件的部分针对性自我保护方法。

第11章重点介绍了恶意软件的样本捕获与分析手段，包括恶意样本的捕获方法，样本分析环境的搭建，以及恶意软件的分析手段等。

本书第四部分对软件的知识产权与自我保护手段进行了讲解。

其中，第12章介绍了软件知识产权验证及保护的具体手段和机制，第13章介绍了软件的自我保护技术，包括反静态分析、反动态调试以及软件的自校验技术。

在本书编写过程中，我们从各种学术论文、书籍、期刊以及互联网中引用了大量的资料，有的在参考文献中列出，有的无法一一查证，在此特别感谢这些文献作者的贡献。

在本书的编著过程中，郑美凤、王丹、叶青晟、周源、万开、张志峰、许静、郑祎、周英骥、郭颖、鲁雄锋、王滢、李晶雯及邵玉如等同学进行了本书部分章节的资料收集、文字整理及校对工作，在此向他们表示感谢。

另外，在“软件安全”课程建设和教材编写的过程中，得到了Intel公司的支持，同时，在网易云课堂平台的支持下，与本教材配套的视频课程已顺利上线，在此向他们表示感谢。

由于时间和水平有限，难免存在部分错误，恳请读者批评指正，以使本书得以不断改进和完善。

作　者

2015年6月

目 录

第一部分 软件安全基础知识

第二部分 软件漏洞利用与防护

第三部分 恶意代码机理及防护

第四部分 软件自我保护

第一部分 软件安全基础知识

第 1 章　软件安全概述

1.1　信息与信息安全

1.1.1　信息的定义

“信息”一词有着很悠久的历史，早在两千多年前的西汉，即有“信”字的出现。“信”常可作消息来理解。

信息是信息论中的一个重要术语，人们常常把消息中有意义的内容称为信息，或者说有价值的消息即为信息。

1948 年，美国数学家、信息论的创始人香农(C. E. Shannon)在题为《通讯的数学理论》的论文中指出：“信息是用来消除随机不定性的东西。”1948 年，美国著名数学家、控制论的创始人维纳(N. Weiner)在《控制论》一书中，指出：“信息就是信息，既非物质，也非能量。”

以下是一些关于信息的描述和定义：

- 信息是主体相对于客体的变化。
- 信息是确定性的增加。
- 信息是事物现象及其属性标识的集合。
- 信息是反映客观世界中各种事物特征和变化的知识，是数据加工的结果，信息是有用的数据。
- 信息以物质介质为载体，传递和反映世界各种事物存在的方式和运动状态的表征。
- 信息(Information)是物质运动规律总和，信息不是物质，也不是能量！
- 信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。

虽然关于信息的定义很多，但我们可以总结出信息的一个重要特征：价值，即其可用来消除不确定性。

目前，信息已经成为一种资产，与其他类别的业务资产一样，其对于组织和个人来说都是不可或缺的，因此要妥加保管。

信息可以以多种形式表现，可以打印或书写在纸上，也可以以电子数据的方式存储，通过邮寄或电子邮件方式传播，或以胶片形式显示或者通过交谈表达出来。总之，信息无处不在。

1.1.2　信息的属性

信息是具有价值的，而其价值则是通过其具体属性来体现的。以下是人们通常最关注的