软件漏洞分析技术

吴世忠　郭涛　董国伟　张普含　著

科学出版社

软件漏洞分析技术

吴世忠　郭　涛
董国伟　张普含　著

科学出版社
北京

内 容 简 介

本书通过对概念的规范、方法的归纳、实例的分析和技术的对比，从白盒到黑盒、从静态到动态、从理论到实践、从传统到新兴，全面深入地阐述了软件漏洞分析技术的各方面内容，是国内第一部系统性介绍漏洞分析技术的著作。

本书共分 5 部分 17 章。其中，第 1 部分介绍软件漏洞的基本概念、影响和发展历程，并提出漏洞分析技术的总体框架；第 2 部分～第 4 部分从源代码漏洞分析、二进制漏洞分析、软件架构与运行系统漏洞分析三个维度对软件漏洞分析技术进行了深入阐述；第 5 部分为前沿技术及未来展望，对移动智能终端、云计算、物联网和工控系统等新兴领域中的漏洞分析技术及挑战进行了总结，探讨了漏洞分析未来发展方向。

本书面向从事信息安全、软件安全和漏洞分析学习、研究、实践和管理的各类专业人士，为他们提供了理论的指南、实践的指导和趋势的指引，是一本必备的宝典，也可作为信息安全相关专业师生教材，以及 IT 专业培训教材。

图书在版编目（CIP）数据

软件漏洞分析技术 / 吴世忠等著 . —北京：科学出版社，2014.9
ISBN 978-7-03-041890-6

Ⅰ . 软… Ⅱ . ①吴… Ⅲ . 软件可靠性 Ⅳ . TP311.53

中国版本图书馆 CIP 数据核字（2014）第 211384 号

责任编辑：杨 凯 / 责任制作：魏 谨
责任印制：赵德静 / 封面设计：于启宝
北京东方科龙图文有限公司 制作
http://www.okbook.com.cn
科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.Longmenbooks.com
骏杰印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2014 年 11 月第 一 版 开本：787×1092 1/16
2014 年 11 月第一次印刷 印张：33 1/2
字数：770 000
定 价：88.00
（如有印装质量问题，我社负责调换）

前言

随着社会信息化进程的不断推进和互联网络的日益普及，计算机及信息技术在国民经济和社会生活的各个领域中都得到了广泛的应用。软件，作为计算机系统功能实现的重要载体，更是提供了丰富多彩的信息化体验。然而，随着社交网络、微博、移动互联网、云计算、物联网等新技术、新应用的不断出现，由软件引发的信息安全事件也层出不穷，“震网病毒”、“火焰病毒”事件的发酵引发了人们对国家关键信息基础设施保护的关注；“维基泄密”等事件引起了人们对网络上个人隐私的担忧；而斯诺登披露的“棱镜门”事件更是把信息安全问题推到了风口浪尖。分析发现，所有这些信息安全事件都存在一个共同点——信息系统或软件自身存在可被利用的漏洞，软件安全漏洞是绝大多数信息安全事件的根源。通过深入探究安全漏洞的本质可以发现在信息技术研发、应用的整个生命周期中，漏洞广泛存在，而且几乎不可避免。首先，冯·诺依曼计算机体系自身的缺陷以及基于TCP/IP协议栈的互联网体系的不安全性等问题，导致了安全漏洞的不可避免性；其次，随着计算机软件系统规模的快速增长以及新技术和新应用的推陈出新，软件系统影响范围的扩展和复杂度的提高，增大了产生漏洞的概率；最后，软件开发生命周期的各个环节都有人为参与，实践经验的缺乏和防范意识的疏忽都有可能导致安全漏洞。

“千里之堤，溃于蚁穴”，漏洞对网络信息安全的重要性和关键性不言自明，以漏洞挖掘、漏洞检测、漏洞应用、漏洞消除和漏洞管控等为主要内容的漏洞分析工作在信息安全保障工作中的重要性和基础性同样不言而喻。

中国信息安全测评中心长期致力于信息安全漏洞分析和风险评估工作，在国家相关部委和社会各界的支持下，结合国家信息安全的战略需求和现实需要，积极开展漏洞分析专项工作，取得了可喜的成效。已有的漏洞分析技术主要针对软件的源代码形态和二进制形态。在现代软件开发环境下，通常将源代码编译或解析成二进制代码，因此源代码中的安全缺陷更可能会直接导致软件漏洞的产生，从而引发重大信息安全事件；针对源代码的漏洞分析较为直观，但是无法发现编译、链接过程中引入的漏洞，同时出于商业利益保护等原因，大部分软件的源代码难以获得，因此，面向二进制程序的漏洞分析技术应用范围也较为广泛。我们的工作实践表明，漏洞分析除了涵盖软件代码分析范畴以外，还应对需求规约、架构设计等开发文档，以及实际运行系统开展安全性分析。架构安全性分析可以发现软件设计方面存在的缺陷，从而在较早的阶段发现安全问题；而软件发布后，在配置、部署、运行、维护和升级等过程中会有意或者无意地引入一些漏洞，因此还要对运行系统进行漏洞分析，以保证其安

全性。本书通过对概念的规范、方法的归纳、实例的分析和技术的对比，从白盒到黑盒、从静态到动态、从理论到实践、从传统到新兴，试图对软件漏洞分析技术的各个方面作一阶段性总结。同时还针对新技术、新应用、新产品的出现分析了漏洞分析所面临的机遇和挑战，并探讨该领域未来的发展趋势。

本书共分为5部分17章。其中，第1部分介绍了软件漏洞的基本概念、影响和发展历程，并提出漏洞分析技术的总体框架；第2部分至第4部分从源代码漏洞分析、二进制漏洞分析、软件架构与运行系统漏洞分析三个维度对软件漏洞分析技术进行了深入阐述；第5部分为前沿技术及未来展望，对移动智能终端、云计算、物联网和工控系统等新兴领域中的漏洞分析技术及挑战进行总结，探讨漏洞分析未来发展方向。信息化发展前景无限，网络空间精彩纷呈，信息安全至关重要，漏洞分析任重道远，我们深感这项工作充满“道高一尺，魔高一丈”的对抗和挑战，我们的技术探索和工作努力不能懈怠，不可止息。本书只是漏洞分析的一个方面，相关内容还没有经过更广的实践和更长时间的检验，我们诚挚欢迎得到各界专家学者的建议和批评。我们希望能够通过本书为从事信息安全和漏洞分析学习、研究、实践和管理的人员提供帮助，为漏洞分析技术的突破和创新提供支撑，并吸引更多的有志之士参与到漏洞分析工作中来，以增强我国的信息安全保障能力。

在本书编写过程中，中国信息安全测评中心的王欣、邵帅、辛伟、朱龙华、张翀斌、贾依真、时志伟、郝永乐、王眉林、柳本金、邓辉，北京邮电大学的梁洪亮和崔宝江老师、解放军信息工程大学的魏强老师、中国人民大学的梁彬和石文昌老师、中国科技大学的程绍银老师、北京神州绿盟科技有限公司安全研究部的左磊高级研究员和忽朝俭博士、湖北大学的张奘老师等给予了大力支持。此外，中国科学院软件研究所的冯登国研究员和张健研究员、中国科学院信息工程研究所的荆继武教授和邹维研究员、北京大学的陈钟教授和王千祥教授、北京邮电大学的宫云战教授，中国信息安全测评中心的章磊、王嘉捷、侯元伟、康凯、刘德、连一汉、覃日鸿、吴健雄、苏权、郑亮、杨诗雨、张丹、崔晓雷，以及北京科技大学的甄平、哈尔滨工业大学的景慧昀、北方工业大学的曲泷玉和北京邮电大学的朱京晶等也对本书提出了宝贵的意见。在此，对他们一并表示由衷的感谢！

本书得到了中国信息安全测评中心“漏洞分析与风险评估”专项工程、国家自然科学基金项目(61272493、61100047)和国家高技术研究发展技术(863计划)项目(2012AA012903)的支持。

吴世忠

2014年7月于北京上地

目 录

第1部分 漏洞分析基础

第 1 章 软件中的漏洞

第 2 章 漏洞分析发展历程

第3部分 二进制漏洞分析

第 9 章 模糊测试

第 10 章 动态污点分析

第5部分 前沿技术及未来展望

第 16 章 漏洞分析领域新挑战

第 17 章 漏洞分析技术展望

第1部分

漏洞分析基础

随着全球信息化的迅猛发展，计算机软件已成为世界经济、科技、军事和社会发展的重要引擎。在当前日益严峻的信息安全大环境下，信息窃取、资源被控、系统崩溃等各类信息安全事件层出不穷，给国民经济、国家安全、社会稳定等带来严重威胁。究其根源，所有这些信息安全事件都存在一个共同点，那就是信息系统或软件自身存在可被利用的漏洞。因此，漏洞分析日益成为信息安全领域理论研究和实践工作的焦点，越来越引起世界各国的关注与重视。

软件产业的蓬勃发展是信息化应用能够如此丰富的主要原因，但同时也带来了软件漏洞数量的激增，近年来，由于软件漏洞被恶意利用而引发的重大信息安全事件越来越多。因此，了解软件中漏洞的基本概念和特性，熟悉漏洞分析的经验和方法，对减少漏洞的危害、降低信息系统运营成本将会起到良好作用，进而尽量降低重大信息安全事件发生的概率。

本部分从定义、分类、分级、管理及所具备的突出特点等方面介绍软件漏洞的基本概念，并说明软件漏洞的巨大危害；在此基础上，分四个阶段说明学术界、企业界、各国政府机构等一直以来在漏洞挖掘、检测、消除和管控等方面进行的研究和开展的工作；最后分别以软件架构、源代码、二进制代码和运行系统为对象，从整体上分析现有漏洞分析技术的框架，并从基本原理、优缺点和应用范围等方面对它们进行对比。