软件安全开发

——属性驱动模式

宋明秋　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

软件安全开发——属性驱动模式

宋明秋 编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

在日益严峻的信息安全背景下，软件的安全性已经成为信息安全问题的重中之重。本书针对信息安全领域这一核心问题，站在软件开发过程控制的视角，从系统工程基本理论思想出发，借鉴当前国际最先进的软件安全开发的理论和方法，提出安全属性驱动的软件开发方法。

全书以软件安全属性为核心，将安全属性贯穿于软件开发生命周期的每一个阶段，通过对软件开发生命周期全过程的安全质量管理和控制，以期减少开发过程中可能产生的各种漏洞，提高软件产品的本质安全性。

全书共分为 6 章，第 1 章是软件安全开发相关的基本概念，第 2 章介绍了软件安全开发方法的历史演化进程以及一些典型的软件安全开发模型，第 3 章基于需求工程原理阐述了软件安全属性需求获取方法，第 4 章从系统架构角度出发阐述了软件安全架构的设计方法以及相关安全技术，第 5 章介绍了软件开发编码过程中的安全问题，第 6 章对于软件安全性测试进行了全面的阐述。

本书的特点是既注重系统性和科学性，又注重实用性，全面地介绍软件开发生命周期全过程的安全质量保证方法，可作为软件开发组织者、系统分析师、软件架构师、软件设计人员、开发人员、测试人员、系统运维人员以及软件相关专业的在校大学生和研究生学习与实践的较好的参考书。

本书由国家自然科学基金面上项目（71171028）与大连理工大学管理与经济学部出版基金资助出版。

图书在版编目（CIP）数据

软件安全开发：属性驱动模式/宋明秋编著. —北京：电子工业出版社，2016.5

ISBN 978-7-121-28750-3

Ⅰ. ①软… Ⅱ. ①宋… Ⅲ. ①软件开发－安全技术 Ⅳ. ①TP311.52

中国版本图书馆 CIP 数据核字（2016）第 095240 号

策划编辑：张 楠
责任编辑：刘真平
印 刷：北京中新伟业印刷有限公司
装 订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：19 字数：425.6 千字
版 次：2016 年 5 月第 1 版
印 次：2016 年 5 月第 1 次印刷
定 价：58.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254579。

序言

Preface

当前随着社会经济的发展和科学技术的进步，计算机的应用日益广泛，人们不但直接使用了从微型计算机、平板电脑、智能手机直到超级计算机的不同信息与计算工具，而且在生产装备、运输工具甚至家庭生活用具中也嵌入了各式各样的计算装置。互联网的日益普及主要得益于计算机的应用，在现代生活和工作中人们享受着计算机带来的巨大效益和便利，与此同时对计算机安全工作的依赖性也日益增加。计算机在安全方面的问题不但会影响到生产和生活的正常运行，有时候甚至造成人身伤亡、装备损毁等重大事故，因此近年来人们对日益严重的计算机系统的安全问题开始密切重视。

在计算机系统的硬件和软件两个方面，人们历来重视的是硬件方面的安全性和可靠性，而对比较隐蔽的软件安全性却关注得不够。但是许多安全事故却是出在软件方面，发生在20世纪90年代的Ariane 5运载火箭、SOHO太空飞船等五起航天器事故的罪魁祸首就是软件，而通过软件安全事件每年给全球造成的经济损失已经高达4500亿美元。因此近年来人们开始以很大的注意力关注软件的安全性问题，因为这不仅影响到个人或者企业自身，而且已经上升到国家安全的高度。

软件的安全性可以理解为软件在系统中运行不至于在工作中造成不可接受的风险（如人身伤亡、设备损坏、财产重大损失、严重污染环境等）的能力。为构建这种能力，人们采取了一系列的方法和技术，逐步形成了计算机软件安全的理论。

为了提高软件的安全性，在软件的开发过程中就应该对安全问题加以认真考虑，由此近年来逐步形成了软件安全开发的概念和方法。由于这是一个新的领域，有关的方法和技术还局限于某些具体应用，尚缺少比较系统介绍的著作，本书正是为了填补这一空白而撰写的。

本书作者在书中一开始先介绍了软件安全的基本概念，对软件安全的基本属性进行了深入细致的描绘，分析了软件安全实现的基本方法，对属性驱动的软件安全开发方法的基本思想进行了阐述。然后利用系统工程思想将安全属性嵌入软件开发的整个生命周期。在回顾软件开发方法的演化过程和对各种方法进行对比的基础上，提出了属性驱动的软件安全开发的基本方法和过程。在总揽全局的基础上，依次详尽地探讨了软件安全需求分析、软件安全保障设计、软件安全编码、软件安全性测试问题。全书贯穿了系统工程整体性和

有序性的理念和方法而又不失对技术细节的阐述，形成了本书的特点。

由于软件安全开发方法涉及的学科比较多，涵盖了多方面的技术细节，因此建立系统的开发理论和方法体系是一项艰苦的工作。深切希望本书作者能在这本著作的基础上进一步深入探索，以满足日益增长的软件安全开发的要求。

大连理工大学系统工程研究所 王众托

2015 年 12 月

目录

Contents

第1章

理解软件安全开发

1.1 信息安全面临的困境

随着互联网技术的快速发展，网络应用（包括社交网络、即时通信、电子邮件、门户网站、网络游戏、手机游戏、电子商务、智慧城市）迅速普及，各种新型网络接入技术（移动网络、云计算、物联网）与传统互联网相融合，为人们提供了更加方便快捷的信息服务，然而同时也带来了日益严重的安全问题。黑客攻击、恶意代码、信息泄露、拒绝服务、权限提升等安全事件层出不穷，每年给全球经济造成的损失超过4500亿美元。更有甚者，2013年“棱镜”事件敲响了国家安全的警钟，信息安全不再只是企业自身的问题，而已经上升到了国家安全的层面。

调查数据显示，企业的信息安全预算中主要的投资方向仍集中于传统的防病毒、防火墙、VPN及身份认证等方法，这些以网络边界安全防护为主的传统安全解决方案可以减少漏洞被利用的机会，然而却不能有效减少系统本身漏洞的存在，仍属于检测型或补偿型控制的被动防护方法。尽管如微软等核心软件公司能够定期发布安全补丁，较为及时地对操作系统、数据库等核心软件的漏洞进行修复，但对于一些零日攻击系统几乎没有防范能力；加之大多数的应用软件开发人员没有能力及时地对应用软件漏洞进行修复，使得系统的运行处于一种危机四伏的状态。传统的安全控制效果不尽如人意，信息安全问题越来越多，攻击形势越来越隐蔽（如APT攻击），智能程度越来越高（技术水平越来越高），组织方式多样化（由最初的单个人员入侵发展到利益驱动的有组织、有计划的产业行为），危害程度日益严重。

分析这一现象产生的根本原因是软件产品本身存在安全漏洞，这些漏洞不止发生在操作系统、数据库或者Web浏览器，也发生在各种应用程序中，特别是与关键业务相关的应用程序系统中。据统计，有超过70%的漏洞来自于应用程序软件，而当前最为热点的移动互联网App存在安全漏洞的比例高达90%以上。众所周知，系统安全漏洞可以为Internet

远程访问、进行系统穿透、实现系统破坏大开方便之门。目前通行的系统开发后期进行测试以消除编码中 Bug 的方式，对于减少软件产品的漏洞数量具有一定的作用，但该方法是以企业为软件开发人员不断犯同样的错误而支付相当的开发成本为代价的，并且一些系统设计逻辑上的缺陷在测试阶段是无法发现的，这些漏洞会增加后期系统维护的成本，并给用户带来巨大的潜在风险。

软件产品存在大量的漏洞是当前信息安全领域面临的最大困境。由于漏洞的产生、利用以及相互作用的机理复杂，因此，如何有效减少系统漏洞数量，提高信息系统整体安全性成为当前亟待解决的挑战性问题。

1.2 软件安全基本概念

我们从软件的基本定义出发，根据需求产生技术的基本原则，从软件错误的类型以及产生的原因分析，提出软件安全属性的概念，并对每一种属性进行描述，根据各属性的原子特性将它们划分为核心安全属性与非核心安全属性。这些安全属性将是软件开发整个生命周期安全保障的基础和目标。

1.2.1 软件的定义

IEEE 给出的软件的定义是计算机程序、方法、规则和相关文档资料，以及在计算机上运行时所需的数据。软件并不只是包括可以在计算机上运行的电脑程序，与这些电脑程序相关的文档一般也被认为是软件的一部分。简单地说，软件就是程序、数据加文档的集合体。

与软件的定义紧密相关的是信息系统的概念，这是一个更加复杂的体系。GB/T 20438.4—2006 对系统（System）的定义是根据设计相互作用的一组元素，可能包括相互作用的硬件、软件和人等。本书只关注软件的安全开发问题，对于硬件及人员的问题暂不涉及。

1.2.2 软件安全错误

“错误”一词在软件安全文献中很少使用，大部分人都习惯于用“漏洞”或者“脆弱点”，有时候软件缺陷也指代错误。

软件安全错误是软件开发生命周期各阶段中错误的真实体现，这些错误会导致软件的漏洞或者脆弱点。

如果与安全威胁相关联的话，软件安全错误可以包含下面几种情况：

（1）需求说明错误。由于软件开发生命周期需求分析过程的错误而产生的需求不正确或缺失的需求，如缺少用户输入验证，这会导致数据格式错误或缓冲区溢出漏洞。

（2）设计错误。由于设计阶段引入不正确的逻辑决策、决策本身错误或者由于决策表达错误而导致的系统设计上的错误，如不正确的口令恢复程序。

（3）代码编写错误。由于软件生命周期实施阶段的错误而导致的设计决策的不正确表达。

（4）配置错误。由于软件在应用环境中配置不当而产生的错误，如防火墙采用默认口令。

软件安全错误是软件错误的一个子集，两者之间唯一的差别是软件安全错误导致漏洞或脆弱点，而软件错误可能会产生与安全无关的不期望的行为。

对于软件安全错误的解决方法基本有两种途径：

第一种途径是采用各种检测、分析、挖掘技术对安全错误进行发现、分析、评价，然后采取各种安全控制措施进行错误修复和风险控制，如传统的打补丁、防病毒、防火墙、入侵检测、应急响应等。这种方法是将安全保障措施开始于软件发布运行之时，是当前系统安全保障普遍采用的方法。历史经验证明，该方法在时间和经济上投入产出比较低，信息系统的安全状况没有得到有效改善。

第二种途径是分析软件安全错误发生的原因，将安全错误的修正考虑嵌入到软件开发生命周期的早期阶段。通过对需求分析、设计、实现、测试、发布，以及运维等各阶段相关的软件安全错误的分析与控制，以期大大减少软件产品的漏洞数量，使软件产品的安全性得到有效提高。该方法是将安全保障的实施开始于软件发布之前，尤其强调从软件生命周期的早期阶段开始安全考虑，从而减少软件生命周期的后期系统运行过程中安全运维的工作量，提高安全保障效果。研究结果表明，在系统维护阶段才考虑安全问题比从系统开发需求阶段就引入安全要素，所花费的错误修复成本要高 30～100 倍。

1.2.3　软件安全的定义

在传统领域，安全的定义是“使伤害或者损害的风险控制在可接受的水平内”（ISO8402）。在软件工程国际标准 ISO/IEC15026 及国家标准 GB/T 18492—2001 中对于安全性的定义是“系统在规定的条件下不导致危害人类生命、健康、财产和环境的一个状态的期望值”。

在此基础之上，软件安全的主要研究人员 McGraw 在他早期的文献[1]中将软件的安全性定义为“在面临蓄意威胁其可靠性的事件的情形下依然能够提供所需功能的能力”，这是一种广义的对于软件应用安全状态的理解。而在我国国家标准 GB/T 16260.1—2006/ISO/IEC9126-1:2001 中，软件的安全性被定义为“软件产品保护信息和数据的能力，以使未授权人员或系统不能阅读或修改这些信息和数据，而不拒绝授权人员或系统对它们的访问”。这一标准定义包含了保密性、完整性、可用性三个方面的安全特性，体现了软件安全与数据保护的密切关系。

尽管“软件安全”本身是一个系统性问题，但软件安全仅仅与软件内部的失效有关，与硬件、人为操作等因素无关。也就是说，作为系统重要组成要素的软件，本身不直接涉

及系统中硬件的物理安全问题，也不涉及软件人机接口实现而可能带来的因为软件安全失效或者人员误操作而产生危险的问题，以及对系统中相关操作人员的管理问题。软件安全只是软件在系统上下文环境中对系统安全性贡献的速记形式[2]。

安全性是软件质量的一个重要属性，描述了软件在系统工作中避免不可接受风险的能力，以及系统正常运行而不会引起事故的能力。软件在系统运行、危险控制以及关键安全功能实现等方面正发挥着越来越重要的作用，成为系统安全保障、避免重大人员伤亡和财产损失的一个重要环节。

现有的关于软件安全性问题的方法和技术主要包含软件安全属性认知、软件安全测试、软件安全评估、信息系统安全工程以及软件安全开发几个方面。

（1）软件安全属性的认知。安全是整体性的概念。根据国家标准 GB/T 16260.1—2006/ISO/IEC9126-1:2001，软件安全既离不开它所存储、传输、处理的数据的安全，也离不开相关文档的安全，因此软件安全应涵盖数据及其信息处理过程本身的三个基本安全要素：保密性、完整性和可用性；同时软件需要接收外界信息输入才能实现预期的功能产生输出结果，信息来源的安全性必然成为软件安全重要的组成部分。基于这些分析，我们将保密性、完整性、可用性、认证性、授权、可记账性作为软件安全的核心属性；而软件自身的实现质量，即软件产品包含的漏洞情况也应该是软件安全性的主要内容，因为这些漏洞会直接导致安全性问题，这也是传统的软件安全关注的问题；此外，站在不同的管理者视角，抗抵赖性、审计性、可信性、可控性、可靠性、软件弹性等也成为软件被关注的其他安全属性。

（2）软件安全测试用来验证与软件相关的系统风险已被消除，或者被控制在可接受的风险水平，并通过测试在软件中发现和排除隐蔽的重大错误及漏洞。

（3）软件安全性评估是为度量软件产品的安全性和系统保障措施而提供的一种客观可信的方法，帮助消费者确定软件产品和相应的保障措施的可信级别。

（4）系统安全工程是一项复杂的系统工程，需要运用系统工程的思想和方法，系统地分析信息系统存在的安全漏洞、风险、事件、损失、控制方法以及效果之间复杂的对应关系，对信息系统的安全性进行分析与评价，以期建立一个有效的安全防御体系，而不是简单的安全产品堆砌。

确切地说，系统安全工程是系统的安全性问题而不仅是软件产品的安全性问题，是一种普适性的信息系统安全工程理论与实践方法，可以用于构建各种系统安全防御体系。系统安全工程可以在系统生命周期的不同阶段对安全问题提供指导，例如，对于已经发布运行的软件，可以采用系统测试、风险评估与控制等方法构建安全防御体系；而对于尚待开发的系统，也可以应用系统安全工程的思想方法来提高目标系统的安全性。这是一项具有挑战性的工作，也是本书的出发点。

（5）软件安全开发关注的是如何运用系统安全工程的思想，以软件的安全性为核心，将安全要素嵌入软件开发生命周期的全过程，有效减少软件产品潜在的漏洞数量，提高软