高等学校网络空间安全专业规划教材

软件安全分析与应用

苏璞睿　应凌云　杨轶　编著

非外借

清华大学出版社

■ 高等学校网络空间安全专业规划教材

软件安全分析与应用

苏璞睿　应凌云　杨轶　编著

清华大学出版社
北京

内 容 简 介

本书作者根据其多年的软件安全研究成果，对软件安全分析方法进行了梳理和总结。全书由易到难、由浅入深地全面介绍了二进制程序分析所需的基础知识和基础分析工具，程序切片、符号执行、模糊测试、污点分析等软件分析基础方法，以及相关分析方法在恶意代码分析、软件漏洞挖掘分析、网络协议逆向分析、移动智能终端应用软件安全分析等方面的应用。本书不仅介绍了相关方法和原理，还分析了当前国际上相关的主流工具和系统，可供读者学习和参考；同时，在安全分析应用方面，也结合了大量的真实案例，有助于读者进一步深刻理解相关方法与技术的原理和价值。

本书不仅可作为网络空间安全专业本科生、研究生相关课程的教材，也可供对软件安全感兴趣的广大学者以及从事软件漏洞和恶意代码分析工作的专业人员参考。

图书在版编目(CIP)数据

软件安全分析与应用/苏璞睿，应凌云，杨轶编著. —北京：清华大学出版社，2017
(高等学校网络空间安全专业规划教材)
ISBN 978-7-302-47207-0

Ⅰ. ①软…　Ⅱ. ①苏…②应…③杨…　Ⅲ. ①软件开发－安全技术－高等学校－教材
Ⅳ. ①TP311.522

中国版本图书馆 CIP 数据核字(2017)第 125758 号

责任编辑：龙启铭　战晓雷
封面设计：傅瑞学
责任校对：李建庄
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：三河市君旺印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：26.75　　**字　　数**：653 千字
版　　次：2017 年 11 月第 1 版　　**印　　次**：2017 年 11 月第1次印刷
印　　数：1～2000
定　　价：59.00 元

产品编号：074426-01

序

网络空间安全已是世界各国关注的重要战略问题，各国政府、学术界、产业界都投入了大量的资源来改善网络空间安全状况，发展网络空间安全防护手段。为适应网络技术和应用的快速发展，各种新的安全技术、安全产品、安全方案层出不穷。当前网络系统中，从不同层次、不同角度实现的安全产品已广泛应用，但从近年来曝光的各类安全事件来看，各种攻击手段仍然防不胜防。究其原因，软件漏洞及其利用是攻击成功的关键，也是系统防御的难点。

“千丈之堤，以蝼蚁之穴溃；百尺之室，以突隙之烟焚。”纵然我们有完美的安全模型和设计方案，但在这些方案的实现中，开发人员的疏忽或个别技术的缺陷都可能引入软件漏洞，让整个方案失效，甚至直接威胁整个系统的安全。2010 年，震网蠕虫利用 7 个软件漏洞成功突破了伊朗核电站的物理隔离网络，造成严重破坏；2011 年，攻击者利用漏洞成功渗透进入了著名的安全公司 RSA 公司的内部网络，并窃取了大量敏感信息；2015 年，以擅长攻击著称的黑客团队 Hacking Team 的内部网络遭受攻击，大量的漏洞利用代码、内部研讨资料等敏感数据泄露。这些案例都给我们敲响了警钟，无论多么安全的防护方案都有可能因为“小小的”软件缺陷而被彻底突破。

近年来，各类安全事件的曝光让人们越来越关注软件的安全性问题。各类软件漏洞挖掘的高手也成为业界的宠儿，但随着软件复杂性的增加以及漏洞和漏洞利用模式的变化，仅仅依赖于少量有个人天赋的高手已经远远不能满足现实的需求。利用先进的技术方法来解决软件安全问题，一直是学术界、产业界共同关注的焦点问题，也是当前的一大难点问题。

2016 年，美国国防部组织的 DARPA CGC 比赛（Cyber Grand Challenge）更是将软件漏洞的自动化发掘、分析、利用、防御技术研究推向高潮，DARPA 组织该比赛的初衷之一也是为了吸引更多的社会资源关注、参与该问题的技术研究工作。这次比赛吸引了众多高校、科研机构和企业团队的关注。最终，来自卡耐基·梅隆大学的 ForAllSecure 团队获得第一。虽然 CGC 比赛中的场景设定与实际情况有很大差距，但这次比赛验证了自动化攻防的技术可能性，代表了未来的技术发展方向。随着未来软件技术的发展和广泛应用，软件安全问题将越来越突出，因此，发展新的软件安全技术是未来的主要发展方向。

我国是软件产业大国，也是软件应用大国。在软件安全方面面临的问

题尤为突出。究其原因，一方面是由于我国大量的软件产品，尤其是操作系统、数据库等基础软件产品依赖于国外厂商，我们不得不面对软件厂商不可信的现实问题；但更重要的是我们目前在软件产品安全方面的审查能力仍很薄弱，缺乏有效的技术手段对软件产品的安全问题实施监管。针对软件安全问题，我国相关部门和机构做了大量的部署，取得了一系列的成果和突破。在软件安全检测、软件漏洞分析等方面形成了一系列成果，大量成果也已经成功转化，为提升我国网络空间安全保障能力发挥了重要作用。

但软件安全问题是典型的对抗性问题，面对我国软件产业的快速发展，当前软件安全技术和成果仍远无法满足现实的需求。高技术对抗需要高技术手段支撑，从 2016 年的 DARPA CGC 比赛可以看出，污点传播分析、符号执行等以前主要在学术研究工作中采用的方法和技术已逐步可支撑一系列软件安全分析实践工作，如何进一步推进相关方法和技术的实用化是当前学术界和工业界共同关注的焦点问题。

本书作者苏璞睿研究员及其团队十多年来一直从事软件安全研究工作，曾主持了国家 863 计划、国家自然科学基金、国家科技支撑计划等一系列国家重点任务的攻关工作，在软件安全方面取得了一系列技术突破，在动态污点传播分析、恶意软件分析与检测、软件漏洞分析与利用等方面有重大创新与积累，主持研制了恶意软件分析检测系统、软件漏洞分析系统等多项成果，在软件安全方面具有丰富的研究和实践经验。

本书由他和他的团队根据多年的研究积累和实践凝练而成，从基本概念、方法原理、重要工具系统和关键应用场景等不同层面对目前国内外的软件安全分析相关技术和方法进行了系统的总结和梳理。本书兼顾了学术研究前沿技术方法和相关技术方法在工程实践中的应用，既剖析了软件安全分析中常用的动态污点分析、符号执行等基础方法，也结合真实应用场景和实际案例，阐述了相关技术方法在软件漏洞分析与利用、恶意软件分析、协议逆向分析等多个具体问题中的应用。

本书是软件安全分析方面一本难得的理论与实践紧密结合的书籍，我愿意把它推荐给从事软件安全研究与实践的科研人员、研究生和技术人员。

2017 年 9 月于北京

前言

软件的应用已经渗透到社会的方方面面，承载着重要的社会价值。软件开发过程无法做到完美，软件问题与漏洞难以避免，软件也成为攻击者的重要目标。当前曝光的各类网络安全事件中，绝大部分都与软件安全问题相关，软件安全问题已成为关乎个人利益、社会稳定、国家安全的重要问题。

软件安全问题中的软件漏洞和恶意软件是两大经典问题，前者是由于软件设计开发过程中的缺陷带来的安全隐患，后者则是攻击者有意设计的具有破坏性的软件工具。软件自身越来越复杂，规模越来越庞大，软件漏洞模式、利用方式也越来越多样化，这就对软件漏洞的发现、分析与评估等工作带来了一系列的挑战；而恶意软件自身的技术也在不断发展，出现了各种自我保护技术、隐蔽通信手段等，这也对恶意软件的分析和处置提出了新的要求。无论是软件漏洞分析还是恶意软件分析，软件自身的复杂性已经超越一般技术人员的分析能力和理解能力，复杂软件的深度分析能力是软件漏洞分析和恶意软件分析共同面临的瓶颈问题。

如何提高对复杂软件的深度分析能力，并针对具体的应用场景，设计相关的分析、检测方法，一直是软件分析领域乃至信息安全领域关注的焦点问题。特别是考虑到很多软件系统无法获得源代码的现实，如何实现不依赖于源代码的软件深度分析是近年来的研究热点。

面向软件安全问题，本书总结了一系列软件分析基础性方法，并重点介绍了软件安全分析工作中的典型场景和相关技术手段。考虑到技术内容的完整性，书中也对当前常见的成熟工具（如反汇编工具、调试工具等）和相关基础知识（如 Intel 指令集、操作系统内核等）进行了简单介绍。

本书的写作主要由中国科学院软件研究所可信计算与信息保障实验室（TCA 实验室）的信息对抗与网络保障团队共同完成，本书的撰写也是该团队对相关技术方法和研究进展的总结。该团队于 2004 年由冯登国研究员创建，后来由我组织。2004 年底，团队开始关注基于硬件虚拟化的恶意软件分析；2005 年底，组织开发了第一个基于开源系统 QEMU 的恶意软件分析系统，当时命名为 WooKon（取音“悟空”）；2010 年，面向恶意软件检测需求，在 WooKon 系统的基础上推出了基于硬件虚拟化的 APT（Advanced Persistent Threat）攻击检测引擎，并在多个部门和机构成功应用，2017 年我们根据新的需求与新的形势又推出了金刚恶意软件智能分析系统；从 2006 年起，开始关注将动态污点分析应用于恶意软件分析和漏洞分析的相关研究，

经过多年研发和逐步完善，2010 年研制了第一套基于硬件虚拟化的动态污点分析系统——AOTA 系统(Application-Oriented Analysis System)，并成功应用于漏洞利用自动生成研究；2013 年构建了一个多样性漏洞利用自动生成系统——PolyAEG 系统。

我们的工作也得到了一系列国家科技项目的支持。团队在最初建立的很长时间内没有得到相关项目的支持，在此要感谢时任信息安全国家重点实验室主任冯登国研究员的大力支持，保证了团队研究工作的持续发展。2006 年团队的工作获得了第一个国家 863 计划项目“恶意代码机理分析与特征提取技术研究”，此后得到了国家自然科学基金、国家科技支撑计划、国家信息安全产业化专项等一系列项目的支持，也在相关项目的支持下完成了从基础方法、关键技术、原型系统到成果转化的科研过程。

软件分析理论博大精深，软件安全问题错综复杂，因作者能力和精力所限，难于对相关技术和方法进行全面、系统的总结。因此，本书主要对使用较多的程序切片、污点分析、模糊测试、符号执行等方法进行了介绍，并对恶意软件分析、协议逆向分析、软件漏洞分析、Android 应用安全性分析等方法和技术进行了总结。

团队多位同事和同学参与了本书的写作或给予了支持和帮助。第 1 章黄桦烽提供了一系列案例素材；第 2、3 章由黄桦烽主要负责编写；第 4 章由闫佳博士主要负责编写；第 5 章由王衍豪博士主要负责编写，贾相堃博士负责修改校对；第 6 章由聂楚江博士主要负责编写；第 7 章由和亮博士主要负责编写；第 8 章主要由应凌云博士负责编写，聂眉宁博士协助提供素材；第 9 章主要由杨轶博士负责编写，闫佳博士协助修改校对；第 10 章由闫佳博士负责编写，闫佳博士协助修改校对；第 11 章由应凌云博士、谷雅聪博士、路晔绵博士及婧二霞共同完成。

本书的编写得到了国家自然科学基金项目“安全协议实现的逆向分析与安全评估方法研究”(NSFC：61572483)、“面向应用商店的移动智能终端恶意软件检测关键技术研究”(NSFC：61502468)、“虚拟化混淆代码逆向分析方法研究”(NSFC：61502469)等项目的支持，在此表示感谢！

本书的编写得到了冯登国研究员的指导和帮助，冯老师不仅对书稿内容的组织、编写大纲等给予了指导，还审阅了全部书稿，提出了宝贵的修改意见。同时，本书最终得以出版，与冯老师长期对我们团队发展的支持是分不开的，在此对冯老师长期的支持和帮助表示衷心感谢！

多位专家、同行的真知灼见也对本书的形成提供了重要参考，在此一并表示感谢！另外，本书初稿曾作为中国科学院大学 2016 年春季课程讲义，课上多位同学也对讲义提出了宝贵的修改意见，在此一并表示感谢！

由于本书涉及内容较多，编写时间仓促，书中难免存在疏漏和不足之处，恳请广大读者提出宝贵的意见和建议，以便我们不断改进和完善本书的内容。

苏璞睿

于中国科学院软件研究所

2017 年 8 月

目录

第 4 章 程序切片/99

第 5 章 符号执行/126

第 1 章 绪 论

软件应用越来越广泛，软件安全问题也越来越突出，恶意软件、软件漏洞、软件后门等安全问题层出不穷。如何对软件产品进行安全性分析，发现相关问题，剖析安全问题机理，进而研发设计相应的防御手段，是软件安全性分析的主要目标。本章主要介绍软件安全问题的背景、典型问题、软件安全性分析的主要技术方法以及本书的组织结构。

1.1 引 言

软件被称为信息系统的“灵魂”。随着信息技术的广泛应用，这一“灵魂”也渗透到了社会的各个角落，软件承载了越来越大的社会价值，涉及国民经济、社会稳定和国家安全。但当这一“灵魂”由世间凡人缔造时，则不可避免地引入了各种问题。

一方面，由于技术和应用的快速发展，软件自身越来越复杂，规模也越来越庞大。现在一般的软件产品开发，代码动辄千万行，单次执行的指令序列规模以 T(2^{40}量级)计；涉及的技术也越来越多样，可能涉及密码、协议、图像等。软件自身复杂性的增加造成软件开发人员在具体开发过程中不可避免地会出现一些错误而引入各种程序漏洞。如图 1-1 所示，根据国际权威漏洞发布组织 CVE 统计，1999 年发现软件漏洞数量不到 1600 个，而 2014 年新发现的软件漏洞数量已接近 10 000 个。软件产业的高度市场竞争造成软件产品开发周期越来越短，也在一定程度上使得这一问题更为严峻。

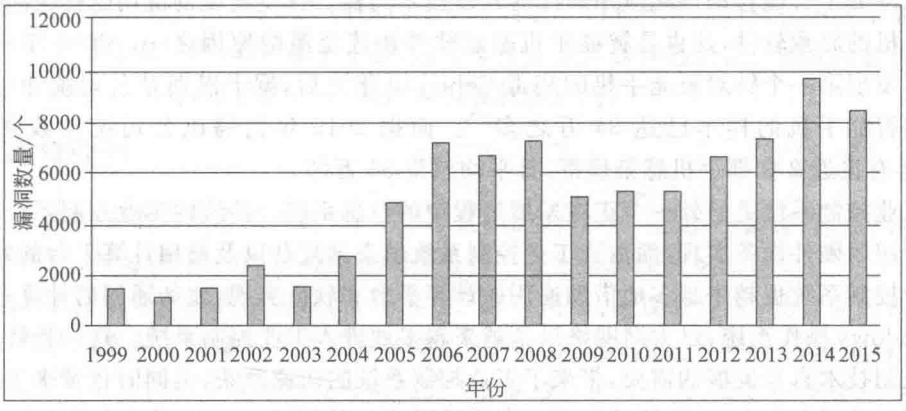

图 1-1 CVE 漏洞发布统计

另一方面，凡人都是有私欲的，当软件产品承载了越来越多的利益时，一些组织也在

利用软件的安全问题来获取利益。据报道，2015 年 2 月黑客团体入侵了约 30 个国家的银行，盗取了近 10 亿美元。同时，各种黑色产业链已经形成规模，朝规模化、集团化方向发展，窃取个人隐私信息、搜集各类账号、盗取虚拟资产、恶意敲诈勒索等案例屡见不鲜；同时，一些政府组织也将软件产品作为情报获取的手段，2013 年底，根据斯诺登曝光的机密文件显示，国际著名的网络安全公司 RSA 公司接受美国国家安全局提供的资金，在相关的软件产品 BSafe 中通过降低密码算法强度，为美国国家安全部门留下后门，使其便于获取情报。

从以上分析可以发现，无论是软件复杂性增加对人类认知带来的挑战，还是某些个人和团体组织受利益的驱使对软件问题的利用，都是无法有效解决的问题。可以预见，随着技术的发展和应用的深入，软件安全问题将越来越严峻。

软件安全问题虽是人为造成的，但也是其技术发展的必然。软件与硬件相比，具有研发技术门槛低、研发周期短、可扩展性强等特点，因此，当前硬件平台越来越向基础性、通用性方向发展，复杂性高、扩展性要求高的功能则越来越多地依赖于软件系统实现。

普通用户体会最深的就是手机终端的发展。现代意义的移动通信技术最早出现于 20 世纪 20 年代，但真正的手机出现于 20 世纪 70 年代中期。早期的移动终端主要是依赖于硬件实现，比如世界上第一台手机摩托罗拉 DynaTAC 8000X。而随着手机操作系统的出现，手机的软硬件分离越来越明显，智能手机带来了移动互联网的繁荣。智能移动终端操作系统最早主要应用于 PDA，20 世纪 90 年代，英国 Psion 公司推出 Psion Series 3 型 PDA，搭载了 EPOC 操作系统，该系统后续发展为 Symbian 系统。1996 年，Palm 公司发布 Pilot 1000 掌上电脑，使用 Palm OS 操作系统。而随着手机和 PDA 功能的融合，诺基亚、微软、黑莓等公司相继推出了针对智能手机的移动操作系统，争夺智能手机市场份额。2007 年 iPhone 上市，iOS 与 Android 操作系统的推出则将智能手机操作系统带入了一个新的时代。在移动终端硬件快速发展、移动网络带宽不断增加的同时，智能手机操作系统的出现不仅丰富了手机的功能，使各类应用层出不穷，也有效提高了系统的可扩展性，可以随时升级，安装新的功能应用。对于开发者而言，智能移动终端操作系统的出现也大大降低了智能移动终端应用软件的开发技术门槛。这里所说的应用软件也包括针对智能手机的恶意软件，这也是智能手机恶意软件快速泛滥的原因之一。2004 年，卡巴斯基公司发现第一个针对智能手机的病毒 Cabir，10 年之后，据卡巴斯基公司统计，其发现的针对智能手机的样本已达 34 万之多[2]。而据 2015 年初腾讯公司统计数据表明，2014 年有接近 2 亿部手机感染病毒，日平均感染 54 万部。

工业控制系统是另外一个正在发展过程中的信息系统。传统的工业控制系统主要依赖于专用的硬件设备实现，而由于工业控制系统越来越复杂以及通用计算平台的发展，当前工业控制系统也越来越多地借助通用的计算平台和软件实现，比如通用的计算机、常见的 Windows 操作系统、以太网网络设备越来越多地进入工业控制系统。这一趋势是工业自动控制技术自身发展的需要，带来了工业控制系统的快速繁荣，但同时也带来了新的安全问题。针对 Windows 系统的传统攻击手段适当迁移就可以实施对工业控制系统的破坏。2009 年 6 月检测到的震网(Stuxnet)蠕虫展示了传统的网络攻击对工业控制系统的破坏能力。在震网蠕虫的整个传播、破坏过程中，共利用了 4 个零日漏洞，攻击过程涉及

Windows 系统、西门子公司的 SIMATIC WinCC 与 PCS 7 等系统。它首先通过漏洞感染 Windows 系统，然后寻找西门子的 SIMATIC WinCC 与 PCS7 系统，并通过西门子公司总线协议 Profibus 注入木马，入侵可编程控制器(Programmable Logic Controller，PLC)，最后寻找使用变频器控制电机转速并在特定频率范围(800～1200Hz)的自动化设备，对其进行破坏。震网蠕虫被认为是第一款应用于实战的网络战武器，震网蠕虫的攻击成功改变了人们的很多传统认识。传统上我们认为，工业控制系统是相对封闭的，被攻击风险低，但实际上控制系统仍依赖于操作人员，操作人员的安全意识差，U 盘交叉使用、随意接入其他网络都可能直接破坏网络的隔离策略；传统上认为工业控制系统中的可编程控制器(PLC)、远程终端单元(RTU)等不是运行在现代操作系统上的，不存在相应的漏洞利用可能，不易受到攻击，而实际上 PLC 可以并且已经成为恶意软件感染的目标[1]。

芯片技术的发展也在改变人们对软硬件界定的传统认识。在传统观念看来，芯片是一个完全独立的硬件产品，但近年来，为了快速、灵活地扩展功能，芯片已支持微码方式对芯片进行更新或打补丁，即芯片的大量功能也靠软件方式——微码实现。同样，微码模式在提供芯片快速更新的灵活性时，也为破坏者开了一条小口子。虽然现在还没有直接攻击的案例出现，但这一风险是客观存在的。

因此，可以预见，随着技术的发展，软件的应用将越来越广泛，软件的功能也将越来越复杂，而市场竞争等因素造成软件的开发周期越来越短，问题也将越来越多，因此如何分析软件产品，发现安全问题，也是当前的技术热点，学术界、产业界、管理部门等社会各界也越来越关注这一问题。

1.2 典型安全问题

软件的安全问题应该说是从软件诞生之日起就存在的，但带来直接影响并受到广泛关注则是从软件承载了各种利益和价值开始的，特别是软件作为大众性商品被广泛应用时，其安全问题才得到足够的重视。一方面，随着研究、分析的深入，我们注意到软件安全的问题非常多样化，另一方面，试图利用软件安全问题获利的各类组织机构也在不断发展针对软件安全问题的利用、破坏技术手段，造成软件安全问题日趋复杂。当前的软件安全问题可粗略地分为 3 类，即恶意软件、软件漏洞和软件后门。

1.2.1 恶意软件

恶意软件的字面意思容易理解，即包含恶意功能的软件。但由于是否“恶意”也具有很强的主观性，因此，目前仍很难对恶意软件进行一个非常客观的标准定义。

传统的恶意软件主要是指病毒、木马、蠕虫、僵尸网络、间谍软件等，其共同的特点是在用户不知情的情况下实施一系列的破坏功能，或窃取信息，或远程控制，或实施破坏等。因此，传统的恶意软件一直在发展 3 方面的能力：渗透与扩散能力，即如何突破相关的防御机制，感染既定的目标系统；隐蔽能力，即如何有效隐蔽自身的各种特征，避免被用户察觉或被相关的安全检测工具发现，也包括在被发现的情况下，如何防止自身被进一步的分析，保护恶意软件的操控者身份；破坏能力，即具体如何搜集信息或实施破坏等。