•聚焦国家重点研发计划•

DOI:10.15961/j.jsuese.201701043

软件与系统漏洞分析与发现技术研究构想和成果展望

饶志宏,方恩博

(中国电子科技网络信息安全有限公司,四川 成都 610041)

摘　要:软件与系统漏洞是国家网络空间安全的重要战略资源。中国关键基础设施和重要信息系统部分核心技术受制于人,软件与系统漏洞普遍存在的现状短期之内无法根除,需要开展深层次、大规模、智能化漏洞挖掘研究;随着移动互联网、工业控制网和物联网等领域的新技术和新应用的推广,现有漏洞挖掘分析技术体系不能满足新的需求;此外,中国漏洞研究团队资源相对分散,国家层面漏洞研究协作机制尚未形成,难以支撑国家对漏洞战略资源的把控。以提升国家开展漏洞战略资源把控能力为导向,针对软件与系统漏洞研究现状,目前亟待解决的四大难题,即漏洞挖掘分析智慧性弱、大流量监测精度低、危害评估验证难、规模协同能力缺。围绕四大难题开展攻关:一是,软件与系统漏洞智慧挖掘方法及关键技术,包括模糊推理经验库的构建方法、基于基因图谱的漏洞挖掘方法、智能引导优化问题、基于策略的漏洞识别方法。二是,软件与系统漏洞分析与可利用性判定技术,包括漏洞成因分析技术、程序异常路径构造技术、同源性漏洞分析技术、漏洞可利用性判定技术、多场景漏洞分析平台建设。三是,基于网络流量的漏洞分析与检测技术,包括利用动静态方法的漏洞攻击样本检测技术、研制软件漏洞攻击样本自动化检测原型系统、针对疑似网络攻击流量的深度检测与智能识别技术、网络攻击样本自动化分析与精准验证、面向攻击流量的漏洞检测与综合服务平台。四是,漏洞危害评估与验证技术,包括基于硬件虚拟化的动态污点分析技术、漏洞自动利用技术、研制基于虚拟环境的漏洞自动化验证系统、漏洞危害性评估体系和危害性评估算法。五是,漏洞规模化协同挖掘分析技术研究与应用,包括多任务多引擎自适应均衡规模化漏洞挖掘技术、多维度多任务智能协同技术、开放协作的知识复用技术、面向多计算环境的规模化协同漏洞发掘的一体化平台、规模化协同条件下漏洞挖掘、分析和可利用性评估技术、规模化协同漏洞发掘一体化平台在典型行业的应用验证。通过以上研究内容实现以下五个方面创新:一是,基因图谱定式复盘,基于基因图谱构建与经验知识复用的漏洞智慧挖掘技术;二是,多源分析多态利用,基于多源漏洞分析的多态可利用性评估技术;三是,动静结合意图推演,大流量环境下基于数据驱动与行为认知关联的攻击检测技术;四是,状态切片叠加复现,活体漏洞库构建技术;五是,智能连接迭代适应,多任务多引擎自适应均衡规模化漏洞挖掘技术。最终,构建集漏洞挖掘、分析、监测、评估、验证于一体的规模协同平台,形成知识复用、智能连接、开放协作的生态系统,为国家摸清网络空间安全家底、扭转攻防博弈被动局面提供技术支撑。

关键词:软件与系统漏洞;智慧挖掘;可利用性判定;大流量安全监测;漏洞危害评估;规模化协同

中图分类号:TP393　　**文献标志码**:A　　**文章编号**:2096-3246(2018)01-0009-13

Research Plan and Achievements Prospects for the Analysis and Discovery Technology of Vulnerabilities in Software and System

RAO Zhihong, *FANG Enbo*

(China Electronics Technol. Cyber Security Co.,Ltd.,Chengdu 610041,China)

Abstract: The vulnerability in software and system is an important resource for national cyberspace security.By now,some key techniques of Chinese critical infrastructures and significant information system are controlled by other countries.The ubiquity of vulnerabilities in software and system cannot be eliminated in a short while.Therefore,it is necessary to carry outin-depth,large-scale,intelligent vulnerability mining research.With the popularization of new technologies and applications in the fields of mobile Internet,indus-

收稿日期:2017 – 11 – 10

基金项目:国家重点研发计划资助项目(2017YFB0802900)

作者简介:饶志宏(1970—),男,高级工程师(研究员级).研究方向:网络安全.E-mail:charao@tom.com

网络出版时间:2018 – 01 – 19 11 : 35 : 31　　**网络出版地址**: http://kns.cnki.net/kcms/detail/51.1773.tb.20180119.1135.001.html

trial control network and Internet of Things,the existing technical architecture of vulnerability mining and analysis cannot meet the new requirements.Besides,China's vulnerability research teams are relatively fragmented and collaboration mechanisms at the national level have not yet been established,which makes it difficult to support the country's control of vulnerability resources.In view of the current situation of software and system vulnerability research,four major problems are urgently needed to be solvedin order to enhance the country's ability to control the strategic resources of vulnerabilities:1)The weak intelligence of vulnerability mining;2)The low monitoring accuracy of large flow;3)The difficulty in verifying hazard assessment;4)The lacking in large-scale collaborative ability.Focusing on the four major problems above,this paper carries out the following five aspects of research.1)Intelligent vulnerability mining methods and key techniques in software and system,including the construction method of fuzzy inference experience base,the genetic map based method of vulnerability mining,optimization problem guided by intelligence,the strategy-based method of vulnerability identification.2)The techniques to parse vulnerabilities in software and system and judge whether they could be exploited,including techniques of analyzing the causes of vulnerabilities,construction techniques of the abnormal path,analytical techniques of homology vulnerabilities,techniques on the exploitability determination of vulnerabilities,the construction of multi-scene vulnerability analysis platform.3)The network flow-based analytical techniques to parse and detect vulnerabilities,including:The techniques to detect the vulnerability attack samples with dynamic and static methods,development of the prototype system to automatically detect vulnerabilities in software,the techniques to detect and identify the suspected network attacks,automatic analysis and precise verification of the network attacks samples,the attack-oriented platform to offer the vulnerability detection and comprehensive service.4)The techniques to evaluate and verify the vulnerability damages,including:The dynamic hardware virtualization-based techniques to parse stains,the techniques to automatically exploit vulnerabilities,development of the virtual environment-based system to automatically verify the vulnerabilities,the system and algorithm to evaluate the damages of vulnerabilities.5)The study and application of large-scale cooperative vulnerabilities mining techniques,including:The multi-tasking multi-engine adaptive large-scale vulnerability mining techniques;the multi-dimensional multi-tasking intelligent collaborative techniques;the open and collaborative techniques to reuse knowledge;the study of the multi-computing environments-oriented integration platform for large-scale collaborative vulnerability mining;vulnerability mining,analysis and availability evaluation techniques under large-scale collaborative conditions;the verification of the large-scale collaborative vulnerability mining integration platform application in typical industries.The project realized the innovation in the following five aspects with the research mentioned above:1)The fixed reconstruction of gene mapping,in detail,the gene mapping construction and knowledge reuse-based intelligent vulnerability mining techniques;2)Multi-source analysis and polymorphism utilization,in detail,the multi-source vulnerability analysis-based techniques to evaluate availability of polymorphism;3)Dynamic and static intention deduction,in detail,the data driven and behavior recognition-based techniques to detect attacks in the large-flow;4)Status slice overlay recurrence,in detail,the techniques to build the living vulnerability library;5) Iterative adaptation of intelligent connection,in detail,the multi-tasking multi-engine adaptive large-scale vulnerability mining techniques.Finally,a large-scale collaborative platform,that integrating vulnerability mining,analysis,monitoring,evaluation and verification,is build.It forms an ecosystem with knowledge reuse,intelligent connectivity and open collaboration,which provides technical support for our country to find out the security circumstances of cyberspace and reverse the passive situation of the game of attack-and-defense.

Key words: vulnerabilities in software and system;intelligence mining;expolitable inference;safety monitoring of large flow;vulnerability assessment;large-scale collaboration

软件与系统漏洞是网络空间安全威慑和防御的基础，已成为国家网络空间安全的重要战略资源。大量外国信息技术产品已深度渗透至中国的电信、金融、石油、交管等关键网络基础设施，导致中国关键基础设施和重要信息系统部分核心技术受制于人[1]，软件与系统漏洞普遍存在的现状短期之内无法根除[2]。随着移动互联网、工业控制网和物联网[3−5]等新技术、新应用的推广，软件漏洞的形态越来越复杂和多样化，从最初的栈溢出和堆溢出等溢出型漏洞，到跨站脚本、SQL注入等网页漏洞，以及最近的HeartBleed等敏感数据泄漏漏洞[6−8]，使得现有漏洞挖掘分析技术体系不能满足新的需求；此外，中国漏洞研究团队资源相对分散，国家层面漏洞研究协作机制尚未形成，难以支撑国家开展漏洞战略资源把控。

为提升中国对软件与系统漏洞资源的掌控能力，亟需围绕漏洞挖掘分析智慧性弱、大流量监测精度低、危害评估验证难、规模协同能力缺等问题开展攻关，研究软件与系统漏洞智慧挖掘方法及关键技术、软件与系统漏洞分析与可利用性判定技术、基于网络流量的漏洞分析与检测技术、漏洞危害评估与验证技术、漏洞规模化协同挖掘分析技术。最终，构建集漏洞挖掘、分析、监测、评估、验证于一体的规模协同平台，形成知识复用、智能连接、开放协作的生态系统，为国家摸清网络空间安全家底、扭转攻防博弈被动局面提供技术支撑。

1　国内外现状及趋势

如何有效地分析发现软件与系统漏洞已经成为世界各国在信息安全领域的重点研究目标。

1.1　人工智能辅助漏洞挖掘分析

早期的漏洞挖掘分析一般使用程序分析、模糊测试和符号执行等确定性的程序推理测试方法。随着技术的发展，业界开始尝试多种技术组合的方式以提高分析能力，如KLEE[9–11]、Mayhem[12]等系统采用基于优化的符号执行技术进行漏洞挖掘，RE-Tracer[13]、CREDAL[14–15]等系统采用基于内核转储和程序分析定位漏洞点。当前研究方向已开始转向利用人工智能辅助漏洞挖掘分析[16–17]，研究人员试图从程序执行历史中总结出漏洞的特征和发生原因，但因缺少先验知识的指导，无法挖掘分析深层漏洞。

国际上，德国布伦瑞克工业大学系统安全研究所的Yamaguchi、Rieck等在总结与利用人工漏洞挖掘定式发现新漏洞方向走在国际前列[18–20]。2014～2016年，Yamaguchi总结了基于污点传播形式的通用漏洞模型，在抽象语法树、程序控制流图、程序依赖图基础上创造了代码属性图（code property graph）的表达方式，结合机器学习技术在多款开源软件中发现大量类似模式的安全漏洞[21–23]。2015年，Yamaguchi巧妙回避了针对大规模代码库直接进行分析的难题，专门针对66个C／C++语言开发的开源项目新增代码（commit）进行模式分析，采用基于支持向量机（support vector machine）的分类方法，快速识别容易引入安全问题的新增代码片段[24–25]。综上，人工漏洞挖掘经验指导自动化挖掘的效果十分明显。

国内漏洞挖掘分析技术研究起步较晚，中国自“十一五”规划开始，国内研究者们逐渐重视漏洞挖掘技术研究，投入大量资源。国内高校、研究机构和企业积极开展漏洞挖掘相关技术研究[26]，研究成果已应用于互联网、移动终端、工业控制网等领域。其中，“软件与系统漏洞分析与发现技术”研究团队中的中国人民解放军信息技术安全研究中心和中国人民解放军信息工程大学承担了“十二五”科技部发布的“863”漏洞领域主题项目[27–29]，利用该项目成果已发现各类未知高危漏洞百余个。

1.2　漏洞可利用性分析、评估与验证

基于模式的可利用性分析是当前漏洞利用验证研究的主要方法。AEG（automatic exploit generation）工具[30–31]针对源码进行漏洞抽象，利用符号执行和约束求解构造exploit，判定漏洞是否可用。Mayhem[32]和CRAX[33]工具分别在PIN和QEMU的支持下获取漏洞相关信息，优化符号执行效率，较好地对识别的漏洞进行exploit自动化构造。Grieco[34–35]等利用符号执行和模式匹配的方法可对缓冲区溢出的可利用性进行判定，但是，由于漏洞模式众多，模式提取是一项十分具有挑战的工作，限制了该方法的适用面。Miller等[36]基于二进制分析平台Bitblaze开发了一套异常判定工具，通过对程序执行路径进行追踪获取和异常相关的信息，并检查异常指令是否能被程序输入影响，提高了异常可利用性判定的精确度，但是它利用虚拟机仿真技术，开销很大，同时，能被输入控制的指令不一定在异常指令附近，并且可能会相距很远，依然会产生很多漏报的可用异常。此外，学者们研制出了AEG[37]、CRAX[38–40]、Driller[41]等半自动工具，但这些工具严重依赖于对漏洞模式的抽象，应用范围有限。这些方法或工具依赖于人工经验难以规模化，或缺少全路径的数据流分析，无法确定数据与用户输入的关系，较易造成误报。

漏洞的危害评估主要依据美国的通用漏洞评分标准CVSS[42]，其度量标准笼统，对漏洞危害性的评估不够准确。目前在大流量环境下，漏洞攻击数据包具有复杂度高，攻击行为具有高隐蔽性、持续性的特点，导致传统流量攻击检测方法精度低。

1.3　漏洞分析与发现规模化协同

目前，Google研制的并行漏洞挖掘与分析系统，能够并发数万个节点进行漏洞挖掘和漏洞分析，该系统可以处理16 TB的初始样本集，支持栈溢出、堆溢出、整数溢出、UAF和Double Free等类型漏洞的自动化挖掘。中国人民解放军信息工程大学已达到并行700个节点的规模，中国科学院信息工程研究所已达到1 000个节点的规模，中国人民解放军总参谋部第五十四研究所已达到并行4 000个节点的规模，处于国内并行大规模漏洞挖掘研究的领先水平。

综上所述，目前国内外在漏洞分析与发现领域已经取得了一定的成果，但是随着现代软件工业的发展，软件规模不断扩大，复杂度越来越高，大大增加了软件漏洞挖掘的难度，亟需实现更精准的漏洞分析验证能力、更高的漏洞发现效率、更具规模的协同漏洞挖掘分析平台以满足新形势下的漏洞分析与发现需求。

2　软件与系统漏洞分析与发现技术的研究内容

针对目前软件与系统漏洞研究中存在的漏洞挖

掘分析智慧性弱、流量监测精度低、危害评估验证难、规模协同能力缺等四大难题，从漏洞“挖掘、分析、监测、评估、验证”环节入手，提出五个方面的研究内容，开展技术攻关，最终研制出集漏洞“挖、析、监、评、验”于一体的规模化的协同平台。

2.1 亟需解决的四大难题

1）漏洞挖掘分析智慧性弱

现有的漏洞挖掘手段缺少对人工经验的有效继承，没有吸收机器学习与深度学习的先进成果，面向深层次漏洞的自动化挖掘缺乏智慧性[43−44]。漏洞的成因多种多样，触发环境复杂多变，不同表征的漏洞挖掘行为差异巨大，对人工漏洞挖掘行为的数据收集与知识表达、经验沉淀和转化复用提出了挑战。以下方面值得研究：如何提出基于定式可复盘的模糊推理经验库和基于基因图谱的漏洞智慧挖掘方法，研究协同条件下如何合理实现知识复用，构建迭代反馈式人机交互、动态均衡自动化挖掘与人工辅助分析模式；如何在漏洞形态从编码安全、逻辑安全到组合安全的演化过程中，有效融合深度学习等领域的技术方法，拓展漏洞挖掘理论与方法；如何综合利用程序分析技术，探索程序执行空间导向性搜索的优化策略，对漏洞挖掘各环节进行归约切分，满足高效弹性的并行分析需求。

2）大流量安全监测精准度低

随着网络泛在化、攻击多样化、应用个性化趋势日益凸显，网络攻击威胁呈有组织、大规模、高隐蔽、长持续性的趋势，网络攻击技术层出不穷，攻击方式花样翻新[45−47]。传统的技术手段主要是基于特征匹配的方式进行检测[48−49]，面对大流量设置的复杂规则匹配库，直接影响检测效率，同时难以在误报率和漏报率之间制定合理的平衡点，难以对大流量漏洞利用攻击行为进行有效识别，安全监测精准度低，对深度检测技术方法提出更高的要求[50−52]。为提高大流量安全监测精准度，需研究海量元数据提取、高级威胁判定因素分析、深度包检测和应用识别、多会话多协议及双向数据流关联等挖掘分析等技术，以提高安全大数据分析监测效能；需研究深度学习、神经网络等人工智能算法，以提升未知威胁攻击监测水平。

3）漏洞危害评估验证难

由于影响漏洞危害性的因素众多且存在复杂关系，使得当前漏洞危害性评估无法定量描述漏洞威胁程度，缺乏针对不同漏洞在不同情境下的评估模型和方法[53−55]。同时，面对目前漏洞类型多样，利用方式层出不穷的环境，传统的漏洞机理分析和漏洞可利用性评估依赖于人工，而自动化可利用性评估所适用的漏洞类型少且准确性低，影响了漏洞危害性评估准确度。为提高漏洞危害性的快速和准确评估能力，需研究可感知不同环境、场景、利用模式的漏洞危害性评估的指标、算法和模型。为提高漏洞可利用性的准确评估能力，需研究海量样本环境中的漏洞机理分析、漏洞信息提取、利用模型抽象、可利用性评估等技术。针对不同环境和场景下出现不同的漏洞利用模式，需开展漏洞利用点定位以及缓解机制绕过方法，解决漏洞利用代码自动生成问题。

4）漏洞挖掘分析规模化协同能力缺

目前，业界应对规模化漏洞挖掘问题的传统方法是“分布式并行计算平台+虚拟机堆叠”，该方法存在平台通用性差、虚拟机单点资源受限、协同方式单一等缺陷[56−57]。如何融合异构多引擎计算资源，构建接口统一、高并发和自适应均衡的多引擎作业平台，是提高规模化漏洞挖掘能力的核心问题；具体可考虑如何将异构引擎的计算资源进行统一定义、抽取和调度，解决异构多引擎计算资源融合的问题。如何将不同研究团队的知识经验在规模化协同平台上进行共享，对漏洞挖掘分析任务进行归约切分，发挥最大效能，是提高规模化协同平台挖掘分析能力的关键；具体可考虑如何研究开放协作的知识复用模型、建立任务智能连接机制，实现“人人”“人机”“团队”间任务级可定制协同。

2.2 研究内容

围绕第2.1节所述的4个难题，开展5个方面的内容研究，研究内容分解图如图1所示。

1）软件与系统漏洞智慧挖掘方法及关键技术。具体内容为：研究协同条件下大规模智慧漏洞挖掘技术与方法；研究基于基因图谱的漏洞模式学习、分析、检测技术[58−60]；研究基于定式可复盘的漏洞挖掘模糊推理经验库构建；研究基于包络的智能导向路径搜索优化方法；研究基于策略的多形式自增型漏洞模式匹配技术。

2）软件与系统漏洞分析与可利用性判定技术。具体内容为：研究基于区间分解的层次化污点分析技术[61]；研究基于证据链的自适应性多策略异常溯源技术；研究基于行为逻辑的广谱漏洞利用建模和跨函数的异常点前向影响分析技术[62]。

3）基于网络流量的漏洞分析与检测技术。具体内容为：研究软件强制执行、控制流完整性监控等技术；研究未知Web漏洞自动提取分析与攻击样本检测优化方法；研究攻击流量识别、溯源与黑客画像等技术；研究多源易构海量攻击数据汇聚分析与预警技术。

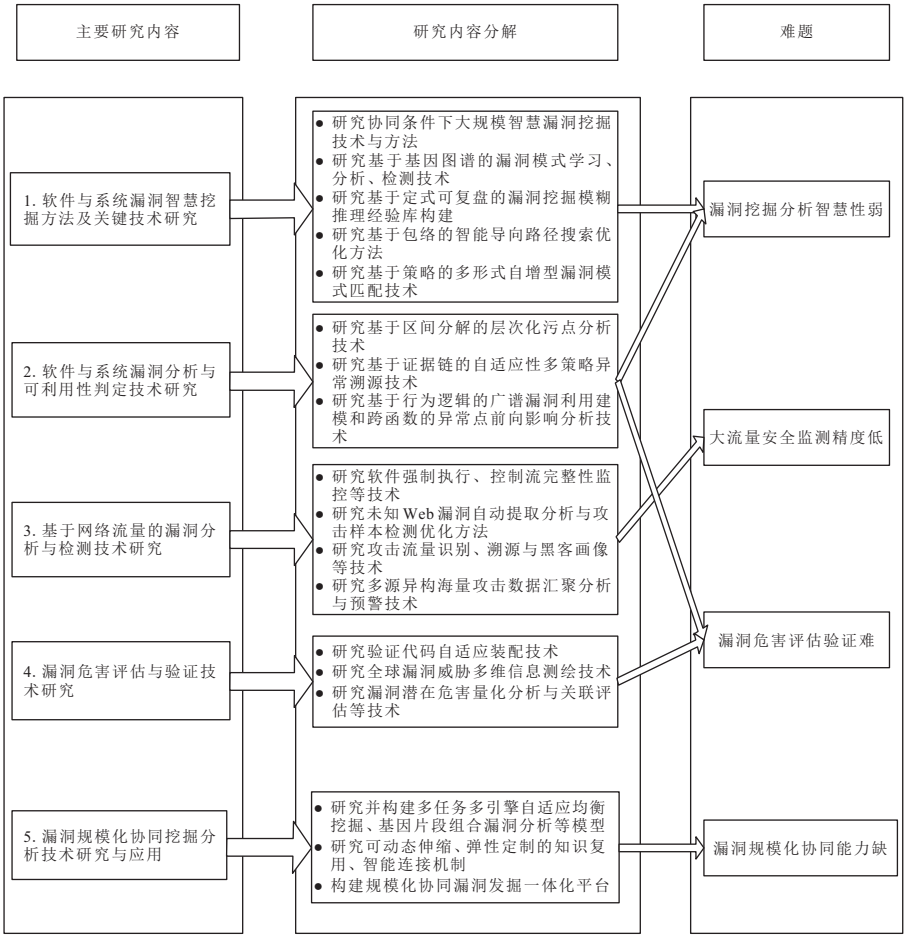

图 1　研究内容分解图

Fig.1　Decomposition diagram of research content

4）漏洞危害评估与验证技术。具体内容为：研究验证代码自适应装配技术；研究全球漏洞威胁多维信息测绘技术；研究漏洞潜在危害量化分析与关联评估等技术。

5）漏洞规模化协同挖掘分析技术研究与应用。具体内容为：研究并构建多任务多引擎自适应均衡挖掘、基因片段组合漏洞分析等模型[63]；研究可动态伸缩、弹性定制的知识复用、智能连接机制；构建规模化协同漏洞发掘一体化平台，支撑典型行业的应用验证。

3　软件与系统漏洞分析与发现技术的技术路线

软件与系统漏洞分析与发现技术的技术路线如图2所示。由图2可以看出，以软件与系统漏洞智慧挖掘方法及关键技术为基础，支撑软件与系统漏洞分析与可利用性判定技术、基于网络流量的漏洞分析与检测技术、漏洞危害评估与验证技术，研制漏洞规模化协同发掘一体化平台。

3.1　软件与系统漏洞智慧挖掘方法及关键技术

针对漏洞挖掘分析智慧性弱的问题，融合大数据与深度学习等技术，创新传统漏洞挖掘模式，研究协同条件下大规模智慧漏洞挖掘技术与方法。重点研究基于定式可复盘的模糊推理经验库构建技术；研究基于基因图谱的漏洞模式学习分析检测技术；研究基于包络的智能导向路径搜索优化方法；研究基于策略的多形式自增型的漏洞识别技术。软件与系统漏洞智慧挖掘方法及关键技术示意图如图3所示。

1）研究基于定式可复盘的模糊推理经验库构建技术。主要内容包括：将人工漏洞挖掘过程作为学习样本，刻画人工漏洞挖掘经验模式[64]。采集人工漏洞挖掘中核心变量关联、污点数据追踪、关键代码回溯分析、疑似漏洞的判定等行为特点，提取人工漏洞挖掘中对代码模糊推理的特征。设计准确的人工先验知识表现方法，构建大规模代码量情境下的模糊推理经验库。

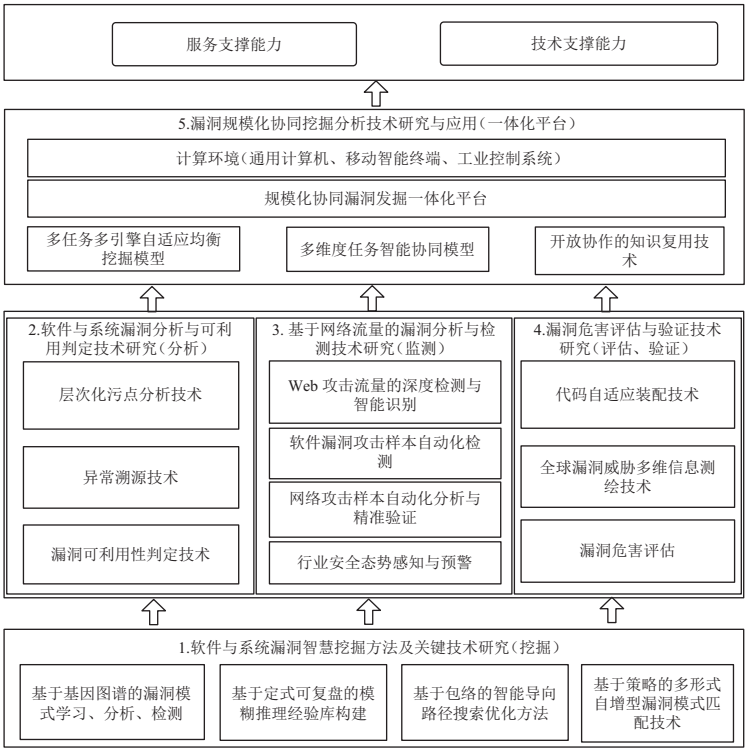

图 2　技术路线示意图

Fig.2　Schematic diagram of technical route

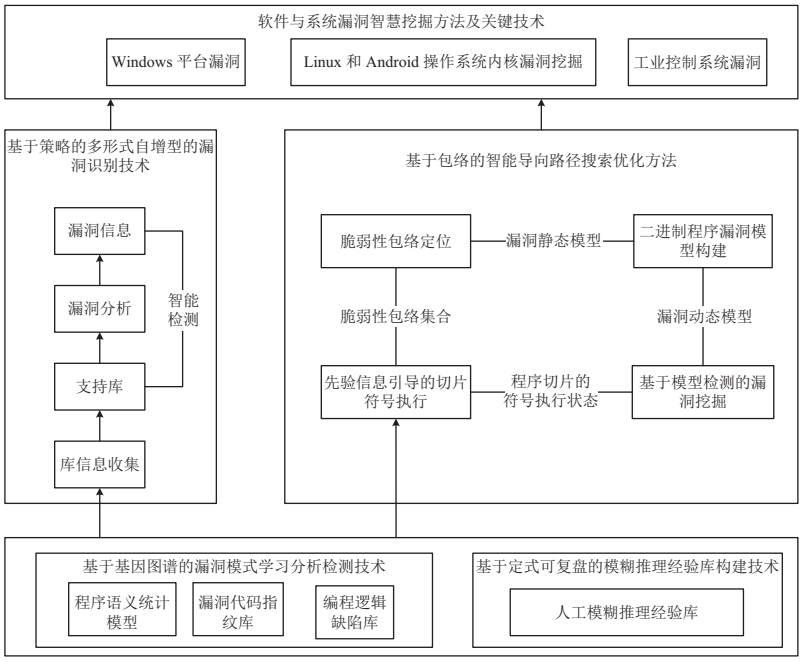

图 3　软件与系统漏洞智慧挖掘方法及关键技术示意图

Fig.3　Schematic diagram of software and system vulnerability intelligence mining methods and key technologies

2）研究基于基因图谱的漏洞模式学习分析检测技术。主要内容包括：研究漏洞基因图谱绘制方法、漏洞模式学习方法、基于深度学习的漏洞识别等技术；研究漏洞基因抽象与程序语言模型，融合漏洞知识与深度学习理论，对多平台、多系统中的漏洞进行挖掘；在基因图谱的基础上，研究协同条件下漏洞挖掘的知识复用。

3）研究基于包络的智能导向路径搜索优化方法。主要内容包括：研究二进制程序中脆弱性包络的检测定位方法，进行脆弱性包络的可达分支路径分

析，研究先验信息引导的切片符号执行技术；提出外部输入相关的前向动态切片提取方法，结合可达分支路径导向，在规模可控的前提下优化程序执行空间搜索过程。

4）研究基于策略的多形式自增型的漏洞识别技术。主要内容包括：研究基于安全策略、静态策略、动态策略、数据策略等构建漏洞识别的方法，深入分析利用中间形式高效表示程序的方法，提高静态程序分析效率并降低误报率。研究在动态测试中实现策略集的动态调度方法，优选测试策略以提高漏洞挖掘效率。

3.2　软件与系统漏洞分析与可利用性判定技术

研究多种知识条件下的大规模软件漏洞的分析技术，确定漏洞位置、发现漏洞与输入的关联信息，以及构造程序异常路径，判断漏洞真实性，并依赖这些信息对漏洞的可利用性进行判定。软件与系统漏洞分析与可利用性判定技术如图4所示。

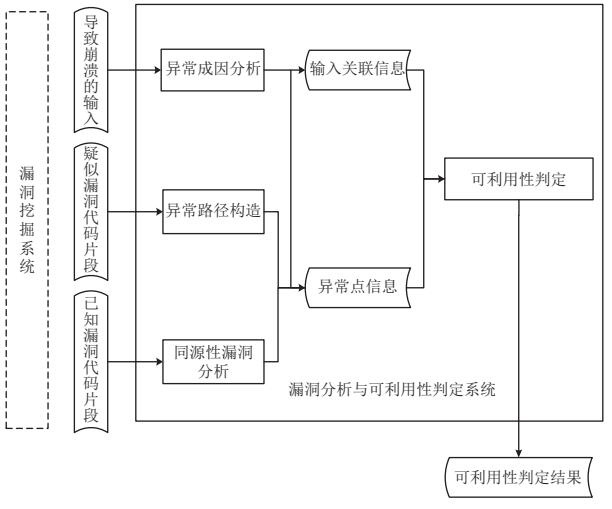

图 4　软件与系统漏洞分析与可利用性判定技术示意图

Fig.4　Schematic diagram of software and system vulnerability analysis and available decision technology

1）异常成因分析技术。研究基于指针分析和动态插桩的程序异常捕捉技术，实现多种类型程序异常的准确识别和定位；研究基于动态污点追踪的异常关联输入分析，完成程序异常的关联数据流和控制流构建，确定漏洞成因。涉及的方法和技术包括：面向大型程序的需求驱动的指针分析方法、基于指针分析和动态插桩的程序异常识别和定位、逻辑分离的正向动态污点传播技术、基于轻量级路径日志的数据流回溯分析技术。

2）异常路径构造技术。研究给定疑似漏洞代码片段条件下程序异常路径的自动构造技术，针对漏洞变量的位置、类型自适应匹配分析算法，实现跨函数的异常路径构造，对漏洞挖掘阶段获得结果的真实性进行判定。涉及的方法包括：支持多种复杂数据类型（结构体、指针等）的多种跨函数异常路径分析方法、基于值依赖的动静结合的异常路径构造方法。

3）同源性漏洞分析技术。研究并建立面向大规模软件库的漏洞特征模式库，基于机器学习方法提高同源性漏洞的分析能力，构造可扩展的漏洞智能分析平台，实现针对同源性漏洞的高效分析与确认。涉及的方法和技术包括：研究支持大数据的漏洞特征抽取技术，准确刻画漏洞片段在程序属性、语义、行为等方面表现出的特征；基于机器学习的迭代式漏洞分析算法，实现同源性漏洞的快速分析与确认。

4）漏洞可利用性判定技术。剖析典型漏洞的利用机理，研究数据流和控制流构造规律，建立漏洞利用模型，研究基于路径搜索和指针分析的漏洞利用路径构造技术，实现漏洞可利用性判定。涉及的方法包括：基于漏洞触发模式的漏洞利用模型抽象方法、基于污点分析和符号执行的漏洞触发点前向可控可达路径搜索方法、关键指针引用的局部有效性和约束关系分析方法、基于路径构造的控制流劫持类漏洞的可利用性判定技术。

3.3　基于网络流量的漏洞分析与检测技术

针对大流量安全监测精准度低的问题，研究利用动态与静态方法的漏洞攻击样本检测、软件漏洞攻击样本自动化检测、针对疑似网络攻击流量的深度检测与智能识别、网络攻击样本自动化分析与精准验证、面向攻击流量的漏洞检测与综合服务平台。基于网络流量的漏洞分析与检测技术如图5所示。

1）研究利用动态与静态方法的漏洞攻击样本检测技术。主要研究内容包括：建成动态与静态分析系统装置，检测范围包括已知的各种漏洞的利用样本，同时支持对0day利用样本的启发检测；基于大数据的机器学习方法研究漏洞利用方法、漏洞成因快速定位和检测技术。

2）软件漏洞攻击样本自动化检测。主要研究内容包括：①基于控制流完整性的程序控制流异常检测技术，构建攻击特征库，使用多种机器学习方法进行检测。②研究防篡改控制流。构建程序正常情况下所有可能的控制流，生成全程序控制流图，并采用二进制重写技术检测网络攻击。

3）针对疑似Web攻击流量的深度检测与智能识别。主要研究内容包括：基于智能算法的Web攻击流量识别，进行数据挖掘和关联分析，对黑客攻击者进行追踪溯源，实现攻击流量识别的自动化。

4）网络攻击样本自动化分析与精准验证。主要研究内容包括：①研究基于灰盒测试的Web攻击检

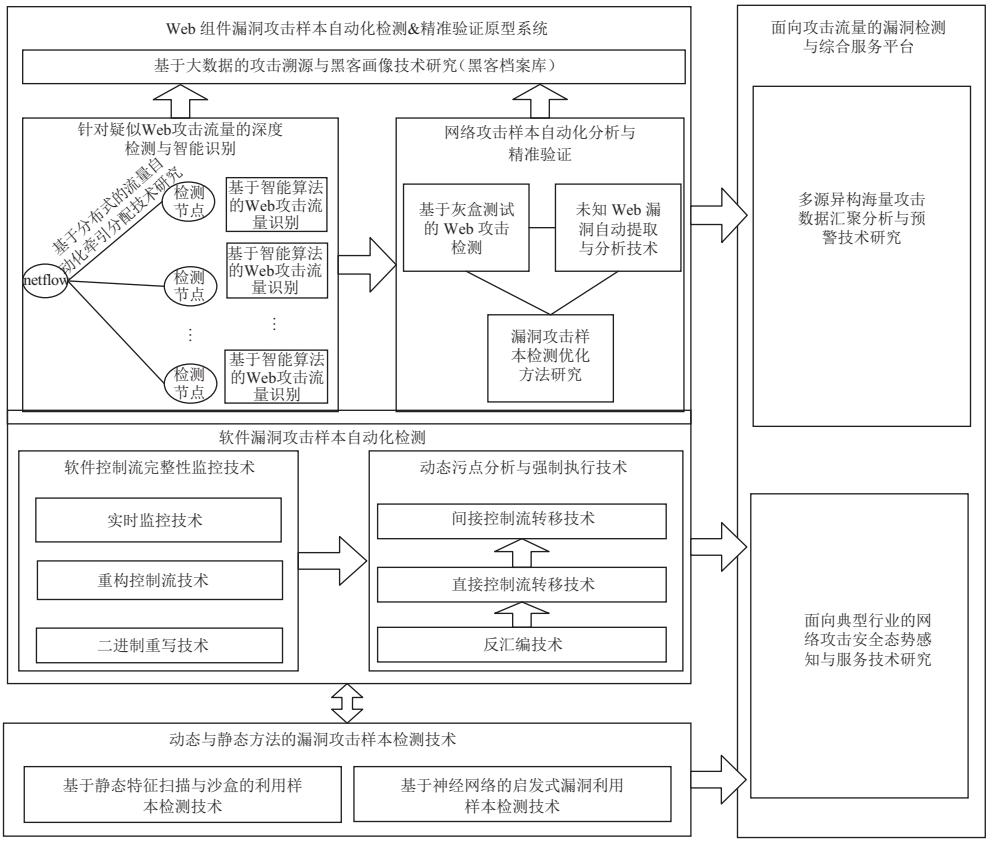

图 5 基于网络流量的漏洞分析与检测技术示意图

Fig.5 Schematic diagram of vulnerability analysis and detection technology based on network traffic

测,针对网络流量中攻击样本,结合动态行为分析技术,识别流量中的恶意行为,验证攻击流量的威胁性。②研究未知Web漏洞自动提取与分析技术。针对恶意攻击的流量,回溯跟踪整个攻击的过程并形成一条完整的攻击链,获取攻击流量的利用机理特点。③研究漏洞攻击样本检测优化方法。采用加权值分析技术与多沙箱并行模式,降低误报,提升性能,避免因性能不足造成的威胁漏报等情况。

5)面向攻击流量的漏洞检测与综合服务平台。主要研究内容包括:①多源异构海量攻击数据汇聚分析与预警技术,研究统一描述的大吞吐量分布式多源异构汇聚融合方法,通过分层模块化架构实现灵活存储及访问,实现大吞吐量并行数据融合与管理。②面向典型行业的网络攻击安全态势感知与服务技术,研究面对网络攻击威胁大数据化、跨时/空域化的特点,提出基于威胁关联依赖度统计方法,实现未知攻击发现。针对动态持续诊断及预警技术和综合服务,提出一种基于偶图理论的情景仿真技术,支撑复杂数据关系下的安全预警与综合服务。

3.4 漏洞危害评估与验证技术

针对漏洞危害评估与验证需要大量人工参与和自动化程度低的问题,从软件崩溃状态点回溯,研究漏洞利用模式提取技术和判定技术、可以绕过内存保护机制的漏洞验证代码组装生成方法、多维度漏洞危害性评估指标体系,提出漏洞危害性评估算法。漏洞危害评估与验证技术如图6所示。

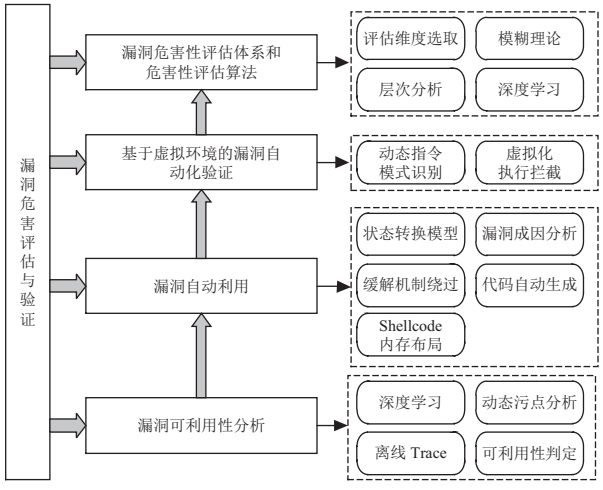

图 6 漏洞危害评估与验证技术示意图

Fig.6 Schematic diagram of vulnerability assessment and verification techniques

1)研究漏洞可利用性分析技术,实现多污染源的传播分析,能够精确查找污染源与关键控制权指令的影响关系。具体内容包括:研究动态污点分析技

术，寻找适合于污染源且标记规模不少于1M的污点标记方法，确保形成的漏洞自动判定技术能够适合于大型复杂（代码规模大于100万行）软件的分析；实现二进制代码的污点传播技术，指令类别不少于200类；离线trace文件的分析技术，能够基于漏洞利用模式，实现漏洞可利用性的自动化判定；建立漏洞可利用性样本库，利用深度学习方法训练可利用性样本训练模型，实现海量漏洞样本的自动筛选评估。

2）研究漏洞自动利用技术。具体内容包括：分析典型漏洞利用代码的执行流程，研究利用代码对程序控制流和数据流的影响方法，基于有限状态机、计算模型等建立能包含漏洞利用主流方法的状态转换模型[65]；基于代码切片、污点分析等方法，定位导致异常的输入数据位置，判断漏洞类型；基于解释器的内存布局、面向返回地址编程等的技术，设计代码片段高效搜索算法，实现对典型缓解机制的绕过；基于符号执行、测试用例生成等方法，在漏洞利用模型和缓解机制绕过技术的指导下，实现对目标程序控制流和数据流的劫持和导向，自动生成可利用性代码；基于快速搜索、约束求解等方法，跟踪目标软件对输入数据的处理流程，将shellcode合理、快速地布局于目标软件的内存空间。

3）研制基于虚拟环境的漏洞自动化验证系统。具体内容包括：采用动态指令模式识别技术快速定位漏洞程序的指令，解决静态分析无法识别的加壳、加密和花指令的处理问题。通过虚拟化指令行为拦截技术，对程序的某条指令或某个函数入口指令进行拦截，获取当前指令的数据流、资源流、执行流、系统服务调用流等，从而判断漏洞被触发的原因和危害以及漏洞是否已经被利用或者被规避。基于虚拟环境实现动态指令模式识别、虚拟化执行拦截等技术实现的漏洞动态验证系统，保证漏洞代码执行过程被全面地隔离、处理、监控及验证。

4）研究漏洞危害性评估体系和危害性评估算法。具体内容包括：研究评估维度选取方法，分析典型漏洞引发的危害性类型研究典型危害性的机理，研究漏洞危害性相关的评估维度及各维度的相关关系；研究漏洞危害性量化标准，建立漏洞危害性评估指标体系。对基于模糊理论、层次分析方法、深度学习理论的漏洞危害性评估算法进行研究；研究漏洞各属性与其危害等级的关联关系，提高漏洞危害性评估的准确性。建立统一的漏洞危害性评估模型，提高评估的效率和自动化水平。

3.5　漏洞规模化协同挖掘分析技术研究与应用

针对漏洞挖掘分析规模化协同能力缺的问题，研究多维度多任务智能协同、知识复用、多任务多引擎自适应均衡规模化漏洞挖掘等技术，实现规模协同条件下的漏洞挖掘、可利用性评估与分析等技术，构建活体漏洞库，研制规模化协同漏洞发掘一体化平台，支撑典型行业的应用验证。漏洞规模化协同挖掘分析技术研究与应用如图7所示。

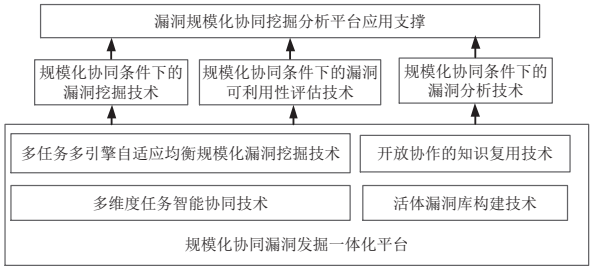

图 7　漏洞规模化协同挖掘分析技术研究与应用示意图

Fig.7　Schematic diagram of vulnerability scale collaborative mining analysis technology research and application

1）多任务多引擎自适应均衡规模化漏洞挖掘技术。具体内容包括：针对漏洞挖掘业务数据种类多样、数据密集型应用交互复杂、规模化自动化漏洞挖掘资源池调度等难题，通过研究任务分发、任务交互、任务导出、任务展示等漏洞挖掘环节，深入分析细粒度的资源调度与分配技术，从而避免不同挖掘引擎任务对资源进行争夺。针对漏洞挖掘平台各子系统自成体系、业务流程复杂、资源需求差异大等问题，研究多任务多引擎自适应均衡技术、资源隔离模型与技术、漏洞挖掘平台细粒度资源管理与迁移监控技术，实现大规模快速并发运行的持久化存储和容错技术，进而支持大规模节点的快速扩展与漏洞挖掘接口的整体联动。

2）多维度多任务智能协同技术。具体内容包括：研究面向多维度多任务协同模型，实现“人人”“人机”“团队”间任务级可定制协同。研究任务智能分解、智能重构和智能连接关键技术，实现任务目标的智能分解、模块优化重组和工作序列智能组装。建立任务效能量化评估体系和反馈学习模型，通过迭代实现对任务连接智能优化。研究满足任务智能连接的资源调度管理模型，实时掌握任务及资源使用情况，对任务工作效能和产出质量进行精细化的量化评估，为规模化协同、高效并行提供重要支撑。

3）开放协作的知识复用技术。具体内容包括：研究知识复用规则智能模型、人工知识的机器语言转化模型等，实现知识复用技术，将漏洞人工挖掘流程中的经验知识转化为可被机器识别的智能符号描述语言，实现对人工经验知识的机器语言转化模型[66–68]。同时，依据漏洞挖掘知识管理的业务逻辑，对异常发现、漏洞定位、漏洞分析、漏洞利用等环节知识处理流程进行分离，并研究环节知识的表示方法与推理

算法。通过人机交互平台，形成开放协作的生态系统，实现漏洞挖掘知识的动态复用与动态重组，增强知识管理系统的分布式处理和规模可扩展能力。

4）面向多计算环境的规模化协同漏洞发掘的一体化平台。具体内容包括：针对目前缺乏适用于通用计算机系统、移动智能终端和工业控制系统等[69−71]多计算环境的规模化协同漏洞发掘系统的问题，研究规模化协同技术，实现异构漏洞挖掘系统融合。设计满足多目标系统接入与协同的统一接口协议和数据规范，构建活体漏洞库，动态描述漏洞信息。研制基于云计算与资源容器的规模化协同漏洞发掘一体化平台，支撑在典型行业的应用验证。

5）规模化协同条件下漏洞挖掘、分析和可利用性评估技术。具体内容包括：在规模化多漏洞引擎协同工作条件下，研究基于高效、定向、深度，以及可定制性、规模化的漏洞挖掘、分析和可利用性评估技术，设计一种适用于规模化协同漏洞挖掘分析系统框架，并用于规范规模化协同定制及各子课题间的多维度多任务执行能力。

6）规模化协同漏洞发掘一体化平台在典型行业的应用验证。具体内容包括：针对典型行业，搭建测试环境，选取典型行业的应用软件与行业数据组成测试样本集，验证规模化协同漏洞发掘平台的漏洞挖掘、分析和可利用性评估能力；针对典型行业的真实运行环境进行漏洞挖掘、分析和可利用性评估验证。例如，以电力行业作为行业应用验证的典范。

4 结论与展望

围绕目前存在的漏洞挖掘分析智慧性弱、流量监测精度低、危害评估验证难、规模协同能力缺等难题展开攻关，最终构建集漏洞挖掘、分析、监测、评估、验证于一体的规模协同平台，形成知识复用、智能连接、开放协作的生态系统，为国家摸清网络空间安全家底、扭转攻防博弈被动局面提供技术支撑。

探索形成国家层面漏洞研究协同机制，以成都、北京、郑州为核心，拓展上海、杭州、南京等科技基地；在漏洞分析与发现领域，汇聚国内漏洞挖掘与利用创新团队，促进国家层面漏洞研究协作机制的建立，通过“产、学、研、用”协同运作，形成漏洞挖掘生态产业链，将极大促进国内漏洞挖掘产业的发展。

本研究的实施将全面提升网络空间新技术新应用的漏洞分析与发现、复杂软件漏洞分析和挖掘、大流量环境下的漏洞攻击样本检测、漏洞的快速利用验证和危害性评估、软件漏洞综合分析、规模化协同漏洞挖掘分析等方面的能力。其研究成果可广泛应用于通用计算机、移动终端、工业控制系统等领域，将有效促进国家网络安全态势全天候、全方位感知，加快网络安全审查制度的建设，增强国家网络空间安全防御和威慑能力。

本研究对漏洞智慧挖掘、规模化智能协同等技术做了初步的探索，后续研究将进一步加强人工智能与漏洞挖掘技术的结合，培育机器漏洞挖掘的智慧性，扭转漏洞挖掘以人为主、以机器挖掘为辅的现状，全面提升漏洞分析与发现的智能化水平。

[致谢]目前，本研究正处于理论研究和技术攻关阶段。感谢广州大学方滨兴院士，中国信息通信研究院安全研究所魏亮所长，中国人民解放军信息工程大学王清贤教授、魏强教授，中国科学院软件研究所高级工程师张阳，中国人民解放军（国家）信息技术安全研究中心副主任李冰，中国人民解放总参谋部第五十四研究所高级工程师吴志勇，以及所有参研人员的支持。

参考文献：

[1] Feng Yanchun.Speeding up the construction of secure national key information infrastructure system[J].China Information Security,2016(11):42–46.[冯燕春.加快构建国家关键信息基础设施安全保障体系[J].中国信息安全,2016(11):42–46.]

[2] Xi Jinping.Speech on the network security and information technology forum[J].China Emergency Management,2016(4):12–16.[习近平.在网络安全和信息化工作座谈会上的讲话[J].中国应急管理,2016(4):12–16.]

[3] Meeker M.Internet trends 2017-code conference[EB/OL].(2017-05-31)[2017-12-08].http://www.kpcb.com/internet-trends.

[4] Al-Sabbagh A,Alsabah R.Internet of things and big data analysis:Recent trends and challenges[M].Anaheim:United Scholars Publication,2016.

[5] Roman R,Najera P,Lopez J.Securing the internet of things[J].Computer,2011,44(9):51–58.

[6] Liu Jian,Su Pu,Yang Min,et al.Software and cyber security—A survey[J].Journal of Software,2018,29(1):42-68.[刘剑,苏璞睿,杨珉,等.软件与网络安全研究综述[J].软件学报,2018,29(1):42-68.]

[7] OpenSSL.CVE-2014-0160[EB/OL].(2014-04-07)[2017-12-08].http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160.

[8] Surhone L M,Tennoe M T,Henssonow S F,et al.Common vulnerabilities and exposures[M].Whitefis:Betascript Publishing, 2010.

[9] Li You,Su Zhengdong,Wang Linzhang,et al.Steering symbolic execution to less traveled paths[C]//Proceeding of the 2013 ACM SIGPLAN International Conference on Object Oriented Programming Systems Languages & Applications.

New York: ACM,2013:19-32.

[10] Wiggers M H,Prasad M R,Ghosh I.Software regression testing using symbolic execution:US9021449[P].2015-04-28.

[11] Yi Qiuping,Yang Zijiang,Guo Shengjian,et al.Eliminating path redundancy via postconditioned symbolic execution[J]. IEEE Transactions on Software Engineering,2017,44(1): 25–43.

[12] Cha S K,Avgerinos T,Rebert A,et al.Unleashing mayhem on binary Code[C]//Proceeding of the 2012 IEEE Symposium on Security and Privacy.San Francisco:IEEE,2012: 380-394.

[13] Cui Weidong,Peinado M,Cha S K,et al.RETracer:Triaging crashes by reverse execution from partial memory dumps[C]// Proceeding of the 38th International Conference on Software Engineering.Austin:IEEE,2016:820-831.

[14] Xu Jun,Mu Dongliang,Chen Ping,et al.CREDAL:Towards locating a memory corruption vulnerability with your core dump[C]//Proceeding of the 2016 ACM SIGSAC Conference on Computer and Communications Security.New York:ACM,2016:529-540.

[15] Fu Yangchun,Lin Zhiqiang,Brumley D.Automatically deriving pointer reference expressions from binary code for memory dump analysis[C]//Proceeding of the 2015 10th Joint Meeting on Foundations of Software Engineering.New York:ACM,2015:614-624.

[16] Behzadan V,Munir A.Vulnerability of deep reinforcement learning to policy induction attacks[M]//Machine Learning and Data Mining in Pattern Recognition.Cham:Springer, 2017:262-275.

[17] Dhingra M,Jain M,Jadon R S.Role of artificial intelligence in enterprise information security:A review[C]//Proceeding of the 2016 Fourth International Conference on Parallel,Distributed and Grid Computing.Waknaghat:IEEE,2017:188-191.

[18] Gascon H,Yamaguchi F,Arp D,et al.Structural detection of android malware using embedded call graphs[C]//Proceedings of the 2013 ACM Workshop on Artificial Intelligence and Security.New York:ACM,2013:45-54.

[19] Shastry B,Leutner M,Fiebig T,et al.Static program analysis as a fuzzing aid[M]//Research in Attacks,Intrusions,and Defenses.Cham:Springer,2017:26-47.

[20] Wressnegger C,Freeman K,Yamaguchi F,et al.Automatically inferring malware signatures for anti-virus assisted attacks[C]//Proceeding of the 2017 ACM on Asia Conference on Computer and Communications Security.New York:ACM, 2017:587-598.

[21] Yamaguchi F,Lottmann M,Rieck K.Generalized vulnerability extrapolation using abstract syntax trees[C]//Proceedings of the 28th Annual Computer Security Applications Conference.New York:ACM,2012:359-368.

[22] Yamaguchi F,Golde N,Arp D,et al.Modeling and discovering vulnerabilities with code property graphs[C]//Proceeding of the 2014 IEEE Symposium on Security and Privacy. Piscateway:IEEE,2014:590-604.

[23] Yamaguchi F,Maier A,Gascon H,et al.Automatic inference of search patterns for taint-style vulnerabilities[C]// Proceeding of the 2015 IEEE Symposium on Security and Privacy.Piscateway:IEEE,2015:797-812.

[24] Perl H,Dechand S,Smith M,et al.VCCFinder:Finding potential vulnerabilities in open-source projects to assist code audits[C]//Proceeding of the 22nd ACM SIGSAC Conference on Computer and Communications Security.New York:ACM,2015:426-437.

[25] Jiang Junfang,Chen Xingshu,Chen Lin.A vulnerability scanning framework based on monitoring agents for iaas platforms[J].Journal of Sichuan University(Engineering Science Edition),2014(Suppl 2):116–121.[姜俊方, 陈兴蜀, 陈林.基于监视代理的IaaS平台漏洞扫描框架[J].四川大学学报(工程科学版),2014(增刊2):116–121.]

[26] Chen Ting,Li Xiaoqi,Luo Xiapu,et al.System-level attacks against android by exploiting asynchronous programming[J/OL]. Software Quality Journal(2017-05-31) [2017-12-08].https://doi.org/10.1007/s11219-017-9374-6.

[27] 魏强,王清贤,曹琰,等.一种动静态结合的软件安全性测试方法:CN102360334A[P].2012-02-22.

[28] Zhang Youchun,Wei Qiang,Liu Zengliang,et sl.Architecture of vulnerability discovery technique for information systems[J].Journal on Communications,2011,32(2): 42–47.[张友春, 魏强, 刘增良, 等.信息系统漏洞挖掘技术体系研究[J].通信学报,2011,32(2):42–47.]

[29] Cao Yan,Wang Qingxian,Wei Qiang,et al.arallel constraint solution method combining search and consistency[J]. Journal of Central South University(Science and Technology),2013,44(Suppl 2):268–272.[曹琰,王清贤,魏强,等.基于相容和搜索结合的并行约束求解方法[J].中南大学学报(自然科学版),2013,44(增刊2):268–272.]

[30] Avgerinos T,Cha S K,Rebert A,et al.AEG:Automatic exploit generation[J].Communications of the ACM,2014, 57(2):74–84.

[31] Huang S K,Huang M H,Huang P Y,et al.Software crash analysis for automatic exploit generation on binary programs[J].IEEE Transactions on Reliability,2014,63(1): 270–289.

[32] Portokalidis G,Slowinska A,Bos H.Argos:An emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation[C]//Proceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems 2006.New York:ACM,2006:15-27.

[33] Yeh C C,Chung H,Huang S K.CRAXfuzz:Target-aware symbolic fuzz testing[C]//Proceeding of the 2015 IEEE 39th Annual Computer Software and Applications Conference. Taichung:IEEE,2015:460-471.

[34] Grieco G,Grinblat G L,Uzal L,et al.Toward large-scale vulnerability discovery using machine learning[C]//Proceeding of the Sixth ACM Conference on Data and Application Security and Privacy.New York:ACM,2016:85-96.

[35] Grieco G,Mounier L,Potet M L,et al.A stack model for symbolic buffer overflow exploitability analysis[C]//Proceeding of the 2013 IEEE Sixth International Conference on Software Testing,Verification and Validation Workshops.Luxemboung:IEEE,2013:216-217.

[36] Miller C.Mobile attacks and defense[J].IEEE Security &Privacy,2011,9(4):68–70.

[37] Wang Minghua,Su P,Li Qi,et al.Automatic polymorphic exploit generation for software vulnerabilities[M]//Security and Privacy in Communication Networks.Cham:Springer,2013:216-233.

[38] Huang S K,Huang M H,Huang P Y,et al.CRAX:Software crash analysis for automatic exploit generation by modeling attacks as symbolic continuations[C]//Proceeding of 2012 IEEE Sixth International Conference on Software Security and Reliability.Gaithersburg:IEEE,2012:78-87.

[39] Chao C Y,Lu H L,Chen C Y,et al.CRAXDroid:Automatic android system testing by selective symbolic execution[C]//Proceeding of the 2014 IEEE Eighth International Conference on Software Security and Reliability-Companion.San Francisco:IEEE,2014:140-148.

[40] Huang S K,Lu H L,Leong W M,et al.CRAXweb:Automatic web application testing and attack generation[C]//Proceeding of the 2013 IEEE 7th International Conference on Software Security and Reliability.Gaithersburg:IEEE,2013:208-217.

[41] Stephens N,Grosen J,Salls C,et al.Driller:Augmenting fuzzing through selective symbolic execution[C].The 2016 Network and Distributed System Security Symposium,San Diego,2016:1-16.

[42] Ou Xinming,Singhal A.The common vulnerability scoring system (CVSS)[M]//Quantitative Security Risk Assessment of Enterprise Networks.New York:Springer,2012:9-12.

[43] Thilina A,Attanayake S,Samarakoon S ,et al.Intruder detection using deep learning and association rule mining[C]//Proceeding of the 2016 IEEE International Conference on Computer and Information Technology.Nadi:IEEE,2016:615-620.

[44] Wang Song,Liu Taiyue,Tan Lin.Automatically learning semantic features for defect prediction[C]//Proceedings of the 2016 IEEE/ACM 38th International Conference on Software Engineering.Austin:IEEE,2016:297-308.

[45] Sikorski M,Honig A.Practical malware analysis:The hands-on guide to dissecting malicious software[M].San Francisco:No Starch Press,2012.

[46] Dittrich D,Dietrich S.P2P as botnet command and control:A deeper insight[C]//Proceeding of the 3rd International Conference on Malicious and Unwanted Software.Fairfax:IEEE,2008:41-48.

[47] Xu Zhaoyan,Zhang Jialong,Gu Guofei,et al.Goldeneye:Efficiently and effectively unveiling malware's targeted environment[M]//Research in Attacks,Intrusions and Defenses.Cham:Springer,2014:22-45.

[48] Chen Qing,Yang Zhenghua,Zeng Aihua.Based on the P2P traffic detection signature feature matching study[J].Electronic Design Engineering,2012,20(9):71–73.[陈庆,杨正华,曾爱华.基于P2P流量检测的签名特征匹配研究[J].电子设计工程,2012,20(9):71–73.]

[49] Cui Baojiang,He Shanshan,Jin Haifeng.Multi-layer anomaly detection for internet traffic based on data Mining[C]//Proceeding of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.Blumenau:IEEE,2015277-282.

[50] Mueller M L,Asghari H.Deep packet inspection and bandwidth management:Battles over bittorrent in canada and the United States[J].Telecommunications Policy,2012,36(6):462–475.

[51] Liu Cong,Wu Jie.Fast deep packet inspection with a dual finite automata[J].IEEE Transactions on Computers,2013,62(2):310–321.

[52] Liu Cong,Pan Yan,Chen Ai,et al.A DFA with extended character-set for fast deep packet inspection[J].IEEE Transactions on Computers,2014,63(8):1925–1937.

[53] Enck W,Gilbert P,Han S,et al.Taintdroid:An information-flow tracking system for realtime privacy monitoring on smartphones[J].Communications of the ACM,2014,57(3):99–106.

[54] Ten C W,Liu C C,Manimaran G.Vulnerability assessment of cybersecurity for scada systems[J].IEEE Transactions on Power Systems,2008,23(4):1836–1846.

[55] Gleichauf R,Shanklin S,Waddell S,et al.System and method for rules-driven multi-phase network vulnerability assessment:US6324656[P].2001-11-27.

[56] Ma Ke,Sun Dujing,Li Lingjuan,et al.Distributed parallel algorithm of mining frequent pattern on data stream[J].Computer Technology and Development,2016,26(7):75–79.[马可,李玲娟,孙杜靖.分布式并行化数据流频繁模式挖掘算法[J].计算机技术与发展,2016,26(7):75–79.]

[57] Zhao Xianghui,Peng Yong,Zhai Zan,et al.Research on parallel vulnerabilities discovery based on open source database and text mining[C]//Proceeding of the 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing.Adelaide:IEEE,2016:327-332.

[58] Kaynar K,Sivrikaya F.Distributed attack graph generation[J].IEEE Transactions on Dependable and Secure Computing,2016,13(5):519–532.

[59] Shar L K,Briand L C,Tan H B K.Web application vulnerab-

ility prediction using hybrid program analysis and machine learning[J].IEEE Transactions on Dependable and Secure Computing,2015,12(6):688–707.

[60] Feng Nan,Wang H J,Li Mianqiang.A security risk analysis model for information systems:Causal relationships of risk factors and vulnerability propagation analysis[J].Information Sciences,2014,256:57–73.

[61] Fang Chen,Mao Bing,Xie Li.Memory-related vulnerabilities localization technology based on dynamic tainting[J].Computer Engineering,2010,36(7):139–141.

[62] Buczak A L,Guven E.A survey of data mining and machine learning methods for cyber security intrusion detection[J].IEEE Communications Surveys & Tutorials,2016,18(2):1153–1176.

[63] Li Zhoujun,Zhang Junxian,Liao Xiangke,et al.Survey of software vulnerability detection techniques[J].Chinese Journal of Computers,2015,38(4):717–732.[李舟军,张俊贤,廖湘科,等.软件安全漏洞检测技术[J].计算机学报,2015,38(4):717–732.]

[64] Wang Jin.Online public opinion situation and threat assessment technology research based on intuitionistic fuzzy reasoning[D].Zhengzhou:PLA Information Engineering University,2011.[王瑾.基于直觉模糊推理的网络舆情态势分析与威胁估计技术研究[D].郑州:解放军信息工程大学,2011.]

[65] Li Xiaoqi,Liu Qixu,Zhang Yuqing.Automatically exploiting system of kernel privilege escalation vulnerabilities based on imitating attack[J].Journal of University of Chinese Academy of Sciences,2015,32(3):384–390.[李晓琦,刘奇旭,张玉清.基于模拟攻击的内核提权漏洞自动利用系统[J].中国科学院大学学报,2015,32(3):384–390.]

[66] Huang Jianjun,Zhang Xiangyu,Tan Lin,et al.AsDroid:Detecting stealthy behaviors in android applications by user interface and program behavior contradiction[C]//Proceeding of the 36th International Conference on Software Engineering.New York:ACM,2014:1036-1046.

[67] Yang Zhemin,Yang Min,Zhang Yuan,et al.Appintent:Analyzing sensitive data transmission in android for privacy leakage detection[C]//Proceeding of the 2013 ACM SIGSAC Conference on Computer & Communications Security.New York:ACM,2013:1043-1054.

[68] Roesner F,Kohno T.Securing embedded user interfaces:Android and beyond[C]//Proceeding of the 22nd USENIX Conference on Security. Berkeley:USENIX Association,2013:97-112.

[69] Zhang Wei,Cao Chengzhi,Liu Wenqing,et al. Vulnerability mining techniques in android platform[C]//Proceedings of the The 1st International Workshop on Cloud Computing and Information Security.Paris:Atlatis Press,2013:535-540.

[70] Li Wei,Tang Yaoping,Li Yuliang,et al.Application of risk assessment in the industrial control system based on simulation system and vulnerability testing[J].Information Security and Technology,2015,6(44):87–91.[李威,汤尧平,李钰靓,等.基于模拟系统和脆弱性测试的风险评估在工控系统中的应用[J].信息安全与技术,2015,6(44):87–91.]

[71] Chae H S,Shahzad A,Irfan M,et al.Industrial control systems vulnerabilities and security issues and future enhancements[J].Advanced Science and Technology Letters,2015,95:144–148.

饶志宏，现任中国电子科技集团公司网络安全与对抗首席专家、中国电子科技网络信息安全有限公司总工程师、国防科技工业网络安全创新中心主任。享受国务院政府津贴，是国家“863”专家组专家、国家“973”重大信息安全基础技术专业组专家、国家中青年科技创新领军人才，G20峰会网络安全保卫工作专家组专家。开创性地主持、指导了多个网络安全与对抗预研和重点型号，在漏洞挖掘与分析、国家关键基础设施网络安全、无线通信系统与网络安全等方面有很深造诣。主持了漏洞安全测试与验证、国家关键基础设施网络安全主动防御技术、关键基础设施安全测试验证、网络空间监测预警系统等多个国家重大项目。是国内首位提出基于物理、链路、网络、业务等多层次漏洞挖掘与系统验证方法，网络对抗矛盾博弈论、网络对抗系统枪弹理论等系列网络安全与对抗理论和方法的学者，为网络安全与对抗技术研究和系统研制提供了理论和方法支撑，推动了相关领域的研究，为中国网络安全与对抗能力的提升做出了突出贡献。著有专著《工业SCADA系统信息安全技术》、译著《网电空间战》《网电空间作战》，在国内外核心刊物上发表多篇高影响的论文。曾获省部级科技进步一等奖1项、二等奖4项、三等奖2项。

（编辑　赵　婧）

引用格式:Rao Zhihong,Fang Enbo.Research plan and achievements prospects for the analysis and discovery technology of vulnerabilities in software and system[J].Advanced Engineering Sciences,2018,50(1):9–21.[饶志宏，方恩博.软件与系统漏洞分析与发现技术研究构想和成果展望[J].工程科学与技术,2018,50(1):9–21.]