软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(5):1177−1178 [doi: 10.13328/j.cnki.jos.005509]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

软件安全漏洞检测专题前言*

王林章[1,2], 陈 恺[3,4], 王 戟[5]

[1](计算机软件新技术国家重点实验室(南京大学),江苏 南京 210023)

[2](南京大学 计算机科学与技术系,江苏 南京 210023)

[3](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100195)

[4](中国科学院大学 网络空间安全学院,北京 100195)

[5](国防科技大学 计算机学院,湖南 长沙 410073)

通讯作者: 王林章, E-mail: lzwang@nju.edu.cn

中文引用格式: 王林章,陈恺,王戟.软件安全漏洞检测专题前言.软件学报,2018,29(5):1177−1178. http://www.jos.org.cn/1000-9825/5509.htm

软件安全漏洞是软件中存在的可能被利用而造成损害的薄弱环节.随着互联网和移动互联网的快速发展,软件因为自身存在漏洞而遭受外界利用攻击,导致隐私泄漏、非法提权、勒索等严重不安全后果.尽早检测软件中存在的安全漏洞并及时实现修复、加固,是网络空间安全领域国内外学术界和产业界的共识与主要关注点.

本专题公开征文,共收到投稿 28 篇,其中 26 篇论文通过了形式审查,内容涉及软件安全漏洞检测的各个方面.特约编辑先后邀请了 20 多位专家参与审稿工作,每篇投稿至少邀请 2 位专家进行评审.稿件经初审、复审、全国软件与应用学术会议(NASAC 2017)宣读和终审 4 个阶段,历时 5 个月,21 篇论文通过复审在 NASAC 2017 会议上进行报告并接受质询,最终有 16 篇论文通过终审入选本专题,主要包括以下 4 个主题.

一、漏洞检测与度量

本主题收录了 5 篇论文.《缓冲区溢出漏洞分析技术研究进展》针对软件漏洞中危害最大、分布范围较广的缓冲区溢出漏洞进行了广泛调研,对主流的缓冲区溢出分析技术进行了分类,并讨论了缓冲区溢出分析领域未来可能的研究方向,对研究针对缓冲区溢出的漏洞检测方法具有积极的理论指导意义.《一种利用补丁的未知漏洞发现方法》提出了一种利用补丁进行同源漏洞检测的方法,该方法能够在有效减弱漏洞无关语句干扰的前提下提高相似漏洞检测的准确性.《面向漏洞生命周期的安全风险度量方法》构建了一种基于吸收 Markov 链的漏洞生命周期模型,以 CVE 的漏洞数据库为输入,依据历史先验漏洞信息,构造状态转移概率矩阵,通过矩阵推导,在时间维上对安全风险进行量化分析,真实、动态地呈现漏洞的时间风险.《数值稳定性相关漏洞隐患的自动化检测方法》提出了一种数值稳定性相关安全漏洞隐患的自动化检测方法,可实现对软件中由于数值稳定性而引发的安全漏洞隐患的高效检测.《大规模源代码增量式资源泄漏检测方法》提出了一种增量式的静态资源泄漏检测方法,实现了对大规模代码的即时缺陷分析与报告.

二、模糊测试

本主题收录了 4 篇论文.《可编程模糊测试技术》提出了一种可编程的模糊测试框架,基于该框架漏洞挖掘人员仅需编写模糊测试制导程序即可完成定制化模糊测试,有效地提高了模糊测试器的开发效率.《基于模式生成的浏览器模糊测试技术》提出了一种基于模式生成的浏览器模糊测试器自动构造方法,具有较好的未知漏洞发现能力.《一种面向模糊测试的 GUI 程序空转状态实时检测方法》提出一种基于函数执行迹的 Bi-Gram 模型来判断程序进入空转状态的时机的方法,提升了识别的准确率.《基于自适应模糊测试的 IaaS 层漏洞挖掘方法》实现了一种面向模糊测试的自适应监督系统——VirtualFuzz,该系统可在预测值的引导下实时地调整模

* 收稿时间: 2018-01-05

糊测试的方向和内容,有效、快速地实现了虚拟化漏洞的验证与挖掘.

三、安全加固和保护

本主题收录了 2 篇论文.《基于分布式信息流控制的无障碍辅助性服务安全加固》提出了一种基于分布式信息流控制的无障碍服务安全加固方法,并基于该方法构建了 Tassel 安全系统,可有效防止 Android 系统无障碍辅助性服务的滥用.《基于 IPT 硬件的内核模块 ROP 透明保护机制》构建了一套基于硬件的使用虚拟化手段来保护针对内核模块的 ROP 攻击的系统,该系统可在不影响虚拟机正常运行的前提下实现对 ROP 攻击的精确检测.

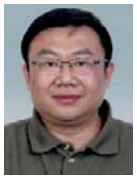
四、新兴系统与应用安全

本主题收录了 5 篇论文.《区块链的安全检测模型》提出一种根据区块链的结构来评估和检测其安全性的方法,该方法通过分析每个结构到达稳定状态的概率来评估系统的安全性,具有一定的通用性.《基于运行时验证的无人飞行系统安全威胁检测方法》提出了一种基于运行时验证的无人飞行系统安全威胁检测方法,该方法能够有效检测无人飞行系统的安全威胁,具有较好的运行效率.《面向 Android 生态系统中的第三方 SDK 安全性分析》对 Android 生态系统中第三方 SDK 的安全性进行了全面分析,发现其中超过 60%的 SDK 存在 HTTP 误用、SSL/TLS 配置不正确、敏感权限滥用和信息泄露等漏洞.《基于宿主权限的移动广告漏洞攻击技术》提出了一种基于宿主权限的移动广告漏洞攻击方法,该方法能够在广告主、广告平台和移动应用均可信的前提下,通过广告网络发起中间人攻击,可得到很好的攻击效果.《基于动态行为分析的网页木马检测方法》提出了一种结合了动态分析与机器学习的网页木马检测方法,可实现对混淆网页木马的有效检测.

本专题主要面向软件安全漏洞检测领域,突出反映我国网络空间安全学者在该领域的最新研究进展.在此,我们特别要感谢《软件学报》编委会、中国计算机学会系统软件专委会和软件工程专委会对本专题工作的指导、支持和帮助,感谢编辑部各位老师所付出的辛勤努力,感谢评审专家严谨、细致、及时的评审工作,感谢向本专题积极投稿的所有作者,希望本专题有助于促进系统软件、软件工程、网络空间安全及相关领域人员在软件安全漏洞检测方面的研究与实践工作.

王林章 (1973－),男,江苏建湖人,博士,南京大学计算机科学与技术系教授,中国计算机学会系统软件专委会秘书长,CCF 杰出会员.主要研究领域为软件测试,模型驱动软件测试与验证,软件系统安全测试.已发表学术论文 50 多篇,曾获 OOPSLA 2013 最佳论文奖.

陈恺(1982－),男,博士,中国科学院信息工程研究所研究员,中国科学院大学教授,入选国家“万人计划”青年拔尖人才,北京市“科技新星”,中国计算机学会系统软件专委会委员,中国保密协会隐私保护专委会委员,CCF 专业会员.主要研究领域为软件与系统安全,在 S&P、USENIX Security、CCS、ICSE 等发表论文 70 余篇,获 ISSRE 2016 最佳论文奖.



王戟 (1969－),男,博士,国防科技大学教授,博士生导师,中国计算机学会软件工程专委会副主任,形式化方法专委会副主任,CCF 高级会员.主要研究领域为高可信软件工程,分布与并行计算程序设计.2007 年获国家杰出青年科学基金资助,2009 年入选教育部长江学者奖励计划特聘教授.