各模块及函数的调用关系,并进一步优化模糊测试的效率,希望能够在不依托已知漏洞的情况下实现更大范围的自适应模糊测试方法.

References:

[1] Wang WX, Zhang J, Chang Q, Gu ZJ. Research on the security problem of cloud computing virtualization platform. Netinfo Security, 2016,2016(9):163−168 (in Chinese with English abstract).

[2] Gong Y, Li C, Wu W. Research on the security technology in virtualization. Netinfo Security, 2016,2016(9):73−78 (in Chinese with English abstract).

[3] Ma W, Han Z, Cheng Y. Research on multi-level management mechanism in trusted cloud computing. Netinfo Security, 2015, 2015(7):20−25 (in Chinese with English abstract).

[4] Shan GD, Dai YX, Wang H. Study on computer vulnerability taxonomy. Computer Engineering, 2002,28(10):3−6 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-3428.2002.10.002]

[5] Chen YC, Chen GQ, Chen ZM, Wan N. A binary code analysis of vulnerability scanning method for SDN smart grid. Netinfo Security, 2016,2016(7):35−39 (in Chinese with English abstract).

[6] Wu SZ, Guo T, Dong GW, Wang JJ. Software vulnerability analyses: A road map. Journal of Tsinghua University (Science and Technology), 2012,52(10):1309−1319 (in Chinese with English abstract).

[7] Li ZJ, Zhang JX, Liao XK, Ma JX. Survey of software vulnerability detection techniques. Chinese Journal of Computers, 2015, 38(4):717−732 (in Chinese with English abstract).

[8] Guo X, Wang P. Technique of cooperative reverse reasoning in related path static analysis. Ruan Jian Xue Bao/Journal of Software, 2015,26(1):1−13 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4658.htm [doi: 10.13328/j.cnki.jos.004658]

[9] Gan ST, Qin XJ, Chen ZN, Wang LZ. Software vulnerability code clone detection method based on characteristic metrics. Ruan Jian Xue Bao/Journal of Software, 2015,26(2):348−363 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4786.htm [doi: 10.13328/j.cnki.jos.004786]

[10] Ganapathy V, Jha S, Chandler D, Melski D, Vitek D. Buffer overrun detection using linear programming and static analysis. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: Academic Press, 2003. 345−354. [doi: 10.1145/948109.948155]

[11] Zhang DH, Liu DG, Wang WH, Lei J, Kung D, Csallner C. Testing C programs for vulnerability using trace-based symbolic execution and satisfiability analysis. In: Proc. of the Int'l Conf. on Dependable Systems and Networks (DSN 2010). New York: IEEE Computer Society, 2010. 321−338.

[12] Wang WG, Zeng QK, Sun H. Dynamic symbolic execution method oriented to critical operation. Ruan Jian Xue Bao/Journal of Software, 2016,27(5):1230−1245 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5027.htm [doi: 10.13328/j.cnki.jos.005027]

[13] Cui ZQ, Wang LZ, Li XD. Target-Directed concolic testing. Chinese Journal of Computers, 2011,34(6):953−964 (in Chinese with English abstract).

[14] Li X, Zhou Y, Li MC, Chen YJ, Xu GQ, Wang LZ, Li XD. Automatically validating static memory leak warnings for C/C++ programs. Ruan Jian Xue Bao/Journal of Software, 2017,28(4):827−844 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5189.htm [doi: 10.13328/j.cnki.jos.005189]

[15] Sun H, Li HP, Zeng QK. Statically detect and run-time check integer-based vulnerabilities with information flow. Ruan Jian Xue Bao/Journal of Software, 2013,24(12):2767−2781 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4385.htm [doi: 10.3724/SP.J.1001.2013.04385]

[16] Zou Q, Wu M, Hu WW, Zhang LB. An instrument-analysis framework for adaptive prefetch optimization in JVM. Ruan Jian Xue Bao/Journal of Software, 2008,19(7):1581−1589 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/1581.htm [doi: 10.3724/SP.J.1001.2008.01581]

[17] Ma JX, Li ZJ, Zhang T, Shen D, Zhang ZK. Taint analysis method based on offline indices of instruction trace. Ruan Jian Xue Bao/Journal of Software, 2017,28(9):2388−2401 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5179.htm [doi: 10.13328/j.cnki.jos.005179]

[18] Yang Z, Yin LH, Duan MY, Wu JY, Jin SY, Guo L. Generalized taint propagation model for access control in operation systems. Ruan Jian Xue Bao/Journal of Software, 2012,23(6):1602−1619 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4083.htm [doi: 10.3724/SP.J.1001.2012.04083]

[19] Sang KC, Woo M, Brumley D. Program-Adaptive mutational fuzzing. In: Proc. of the Security and Privacy. New York: IEEE Computer Society, 2015. 725−741. [doi: 10.1109/SP.2015.50]

[20] Ma JX, Zhang T, Li ZJ, Zhang JX. Improved fuzzy analysis methods. Journal of Tsinghua University (Science and Technology), 2016,56(5):478−483 (in Chinese with English abstract).

[21] Godefroid P, Kiezun A, Levin MY. Grammar-Based whitebox fuzzing. In: Proc. of the ACM Sigplan Conf. on Programming Language Design and Implementation. New York: Academic Press, 2008. 206−215. [doi: 10.1145/1375581.1375607]

[22] Li WM, Yu JQ, Ai SB. PyFuzzer: Automatic in-memory fuzz testing method. Journal on Commnications, 2013,34(Z2):64−68 (in Chinese with English abstract).

[23] Ouyang YJ, Wei Q, Wang QX, Yin ZX. Intelligent fuzzing based on exception distribution steering. Journal of Electronics & Information Technology, 2015,37(1):143−149 (in Chinese with English abstract).

[24] Huang L, Feng DG, Lian YF, Chen K, Zhang YJ, Liu YL. Method of DDoS countermeasure selection based on multi-attribute decision making. Ruan Jian Xue Bao/Journal of Software, 2015,26(7):1742−1756 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4673.htm [doi: 10.13328/j.cnki.jos.004673]

[25] Wang L, Yang XJ, Wang J, Luo Y. Automatedly checking function execution context of kernel programs in operation systems. Ruan Jian Xue Bao/Journal of Software, 2007,18(4):1056−1067 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1056.htm [doi: 10.1360/jos181056]

[26] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2011,22(1): 71−83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[27] Lin C, Su WB, Meng K, Liu Q, Liu WD. Cloud computing security: Architecture, mechanism and modeling. Chinese Journal of Computers, 2013,36(9):1765−1784 (in Chinese with English abstract).

[28] Zhang YQ, Wang XF, Liu XF, Liu L. Survey on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2016,27(6): 1328−1348 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5004.htm [doi: 10.13328/j.cnki.jos.005004]

[29] Zhu M, Tu BB, Meng D. The security research of virtualization software stack. Chinese Journal of Computers, 2017,40(2):481−504 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2017.00481]

[30] Elhage NV. A KVM Guest→Host privilege, escalation exploits. In: Proc. of the BlackHat USA. New York: IEEE Computer Society, 2011. 1−12.

[31] Wang G, Estrada ZJ, Pham C, Kalbarczyk Z. Hypervisor introspection: A technique for evading passive virtual machine monitoring. In: Proc. of the 2016 Usenix Security Symp. Boca Raton: CRC Press, 2016. 207−225.

[32] Panuccio A, Bicego M, Murino V. A Hidden Markov Model-Based Approach to Sequential Data Clustering Structural, Syntactic, and Statistical Pattern Recognition. Vol.1, Berlin, Heidelberg: Springer-Verlag, 2002. 734−743. [doi: 10.1007/3-540-70659-3_77]

[33] Rabiner LR. A tutorial on hidden Markov models and selected applications on speech recognition. Readings in Speech Recognition, 1990,77(2):267−296.

附中文参考文献:

[1] 王文旭,张健,常青,顾兆军.云计算虚拟化平台安全问题研究.信息网络安全,2016,2016(9):163−168.

[2] 宫月,李超,吴薇.虚拟化安全技术研究.信息网络安全,2016,2016(9):73−78.

[3] 马威,韩臻,成阳.可信云计算中的多级管理机制研究.信息网络安全,2015,2015(7):20−25.

[4] 单国栋,戴英侠,王航.计算机漏洞分类研究.计算机工程,2002,28(10):3−6. [doi: 10.3969/j.issn.1000-3428.2002.10.002]

[5] 陈颖聪,陈广清,陈智明,万能.面向智能电网 SDN 的二进制代码分析漏洞扫描方法研究.信息网络安全,2016,2016(7):35−39.

[6] 吴世忠,郭涛,董国伟,王嘉捷.软件漏洞分析技术进展.清华大学学报自然科学版,2012,52(10):1309−1319.

[7] 李舟军,张俊贤,廖湘科,马金鑫.软件安全漏洞检测技术.计算机学报,2015,38(4):717−732.

[8] 郭曦,王盼.相关路径静态分析中协同式逆向推理方法.软件学报,2015,26(1):1−13. http://www.jos.org.cn/1000-9825/4658.htm [doi: 10.13328/j.cnki.jos.004658]

[9] 甘水滔,秦晓军,陈左宁,王林章.一种基于特征矩阵的软件脆弱性代码克隆检测方法.软件学报,2015,26(2):348−363. http://www.jos.org.cn/1000-9825/4786.htm [doi: 10.13328/j.cnki.jos.004786]

[12] 王伟光,曾庆凯,孙浩.面向危险操作的动态符号执行方法.软件学报,2016,27(5):1230−1245. http://www.jos.org.cn/1000-9825/5027.htm [doi: 10.13328/j.cnki.jos.005027]

[13] 崔展齐,王林章,李宣东.一种目标制导的混合执行测试方法.计算机学报,2011,34(6):953−964. [doi: 10.3724/SP.J.1016.2011.00953]

[14] 李筱,周严,李孟宸,陈园军,Xu GQ,王林章,李宣东.C/C++程序静态内存泄漏警报自动确认方法.软件学报,2017,28(4):827−844. http://www.jos.org.cn/1000-9825/5189.htm [doi: 10.13328/j.cnki.jos.005189]

[15] 孙浩,李会朋,曾庆凯.基于信息流的整数漏洞插装和验证.软件学报,2013,24(12):2767−2781. http://www.jos.org.cn/1000-9825/4385.htm [doi: 10.3724/SP.J.1001.2013.04385]

[16] 邹琼,伍鸣,胡伟武,章隆兵.基于插桩分析的 Java 虚拟机自适应预取优化框架.软件学报,2008,19(7):1581−1589. http://www.jos.org.cn/1000-9825/19/1581.htm [doi: 10.3724/SP.J.1001.2008.01581]

[17] 马金鑫,李舟军,张涛,沈东,章张锴.基于执行踪迹离线索引的污点分析方法.软件学报,2017,28(9):2388−2401. http://www.jos.org.cn/1000-9825/5179.htm [doi: 10.13328/j.cnki.jos.005179]

[18] 杨智,殷丽华,段洣毅,吴金宇,金舒原,郭莉.基于广义污点传播模型的操作系统访问控制.软件学报,2012,23(6):1602−1619. http://www.jos.org.cn/1000-9825/4083.htm [doi: 10.3724/SP.J.1001.2012.04083]

[20] 马金鑫,张涛,李舟军,张江霄.Fuzzing 过程中的若干优化方法.清华大学学报(自然科学版),2016,56(5):478−483.

[22] 李伟明,于俊清,艾少波.PyFuzzer:自动化高效内存模糊测试方法.通信学报,2013,34(Z2):64−68.

[23] 欧阳永基,魏强,王清贤,尹中旭.基于异常分布导向的智能 Fuzzing 方法.电子与信息学报,2015,37(1):143−149.

[24] 黄亮,冯登国,连一峰,陈恺,张颖君,刘玉岭.一种基于多属性决策的 DDoS 防护措施遴选方法.软件学报,2015,26(7):1742−1756. http://www.jos.org.cn/1000-9825/4673.htm [doi: 10.13328/j.cnki.jos.004673]

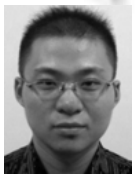
[25] 汪黎,杨学军,王戟,罗宇.操作系统内核程序函数执行上下文的自动检验.软件学报,2007,18(4):1056−1067. http://www.jos.org.cn/1000-9825/18/1056.htm [doi: 10.1360/jos181056]

[26] 冯登国,张敏,张妍,徐震.云计算安全研究.软件学报,2011,22(1):71−83. http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[27] 林闯,苏文博,孟坤,刘渠,刘卫东.云计算安全:架构、机制与模型评价.计算机学报,2013,36(9):1765−1784.

[28] 张玉清,王晓菲,刘雪峰,刘玲.云计算环境安全综述.软件学报,2016,27(6):1328−1348. http://www.jos.org.cn/1000-9825/5004.htm [doi: 10.13328/j.cnki.jos.005004]

[29] 朱民,涂碧波,孟丹.虚拟化软件栈安全研究.计算机学报,2017,40(2):481−504. [doi: 10.11897/SP.J.1016.2017.00481]



沙乐天(1985－),男,江苏南京人,博士,讲师,CCF 专业会员,主要研究领域为软件安全,漏洞挖掘,物联网攻防.

喻辉(1972－),男,工程师,主要研究领域为网络安全,漏洞挖掘.

肖甫(1980－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为物联网,传感网.

王汝传(1943－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为物联网.

杨红柯(1983－),男,工程师,主要研究领域为网络安全,漏洞挖掘.