[48] Heintze N, Riecke JG. The SLam calculus: Programming with secrecy and integrity. In: Proc. of the 25th ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. ACM Press, 1998. 365−377. [doi: 10.1145/268946.268976]

[49] Myers AC. JFlow: Practical mostly-static information flow control. In: Proc. of the 26th ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. ACM Press, 1999. 228−241. [doi: 10.1145/292540.292561]

[50] Banerjee A, Naumann DA. Secure information flow and pointer confinement in a Java-like language. In: Proc. of the IEEE Computer Security Foundations Workshop. New York: IEEE, 2002. 253−267.

[51] Sabelfeld A, Sands D. A per model of secure information flow in sequential programs. Higher-Order and Symbolic Computation, 2001,14(1):59−91. [doi: 10.1023/A:1011553200337]

[52] Smith G, Volpano D. Secure information flow in a multi-threaded imperative language. In: Proc. of the 25th ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. San Francisco: ACM Press, 1998. 355−364.

[53] Zdancewic S, Zheng L, Nystrom N, Myers AC. Untrusted hosts and confidentiality: Secure program partitioning. ACM SIGOPS Operating Systems Review, 2001,35(5):1−14. [doi: 10.1145/502059.502036]

[54] Volpano D, Smith G. Eliminating covert flows with minimum typings. In: Proc. of the 10th IEEE Computer Security Foundations Workshop. IEEE, 1997. 156−168. [doi: 10.1109/CSFW.1997.596807]

[55] Agat J. Transforming out timing leaks. In: Proc. of the 27th ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. ACM Press, 2000. 40−53. [doi: 10.1145/325694.325702]

[56] Volpano D, Smith G. Probabilistic noninterference in a concurrent language. In: Proc. of the11th IEEE Computer Security Foundations Workshop. New York: IEEE, 1998. 34−43.

[57] Ørbæk P, Palsberg J. Trust in the λ-calculus. Journal of Functional Programming, 1997,7(06):557−591. [doi: 10.1017/S0956796897002906]

[58] Dam M, Giambiagi P. Confidentiality for mobile code: The case of a simple payment protocol. In: Proc. of the 13th IEEE Computer Security Foundations Workshop (CSFW-13). IEEE, 2000. 233−244. [doi: 10.1109/CSFW.2000.856940]

[59] Volpano D, Smith G. Verifying secrets and relative secrecy. In: Proc. of the 27th ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages. ACM Press, 2000. 268−276. [doi: 10.1145/325694.325729]

[60] Clark D, Hunt S, Malacaria P. Quantitative analysis of the leakage of confidential data. Electronic Notes in Theoretical Computer Science, 2002,59(3):238−251. [doi: 10.1016/S1571-0661(04)00290-7]

[61] Wang TL. Research on binary-executable-oriented software vulnerability detection [Ph.D. Thesis]. Beijing: Peking University, 2011 (in Chinese).

[62] 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]

[63] Kemerlis VP, Portokalidis G, Jee K, Keromytis AD. Libdft: Practical dynamic data flow tracking for commodity systems. ACM SIGPLAN Notices, 2012,47(7):121−132. [doi: 10.1145/2365864.2151042]

[64] Luk CK, Cohn R, Muth R, Klauser A, Lowney G, Hazelwood K. Pin: Building customized program analysis tools with dynamic instrumentation. ACM Sigplan Notices, 2005,40(6):190−200. [doi: 10.1145/1064978.1065034]

[65] Brumley D, Jager I, Avgerinos T, Schwartz EJ. BAP: A binary analysis platform. In: Proc. of the Computer Aided Verification. Berlin, Heidelberg: Springer-Verlag, 2011. 463−469. [doi: 10.1007/978-3-642-22110-1_37]

[66] Song D, Brumley D, Yin H, Caballero J, Jager I, Kang MG, Saxena P. BitBlaze: A new approach to computer security via binary analysis. In: Proc. of the Information Systems Security. Berlin, Heidelberg: Springer-Verlag, 2008. 1−25. [doi: 10.1007/978-3-540-89862-7_1]

[67] Kang MG, McCamant S, Poosankam P, Jager I, Kang MG, Saxena P. DTA++: Dynamic taint analysis with targeted control-flow propagation. In: Proc. of the NDSS. San Diego: Internet Society, 2011. 223−231.

[68] Clause J, Li W, Orso A. Dytan: A generic dynamic taint analysis framework. In: Proc. of the 2007 Int'l Symp. on Software Testing and Analysis. Portland: ACM, Press, 2007. 196−206. [doi: 10.1145/1273463.1273490]

[69] Qin F, Wang C, Li Z, Zhou Y, Wu Y. Lift: A low-overhead practical information flow tracking system for detecting security attacks. In: Proc. of the 39th Annual IEEE/ACM Int'l Symp. on Microarchitecture. Orlando: IEEE, 2006. 135−148. [doi: 10.1109/MICRO.2006.29]

[70] Wang C, Hu S, Kim HS. Stardbt: An efficient multi-platform dynamic binary translation system. In: Proc. of the Advances in Computer Systems Architecture. Berlin, Heidelberg: Springer-Verlag, 2007. 4−15. [doi: 10.1007/978-3-540-74309-5_3]

[71] Newsome J, Song D. Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software. Network & Distributed System Security Symp., 2005,29(5):720−724.

[72] Nethercote N, Seward J. Valgrind: A framework for heavyweight dynamic binary instrumentation. ACM Sigplan Notices, 2007, 42(6):89−100. [doi: 10.1145/1273442.1250746]

[73] Schultz D, Liskov B. IFDB: Decentralized information flow control for databases. In: Proc. of the 8th ACM European Conf. on Computer Systems. ACM Press, 2013. 43−56. [doi: 10.1145/2465351.2465357]

[74] Cheng W, Ports DRK, Schultz DA. Abstractions for usable information flow control in Aeolus. In: Proc. of the USENIX Annual Technical Conf. Berkeley: USENIX, 2012. 139−151.

[75] Davis B, Chen H. DBTaint: Cross-Application information flow tracking via databases. Proc. of the WebApps, 2010,22(8):2−10.

[76] Huang YW, Yu F, Hang C. Securing Web application code by static analysis and runtime protection. In: Proc. of the 13th Int'l Conf. on World Wide Web. ACM Press, 2004. 40−52. [doi: 10.1145/988672.988679]

[77] Chlipala A, Impredicative LLC. Static checking of dynamically-varying security policies in database-backed applications. In: Proc. of the OSDI. Berkeley: USENIX, 2010. 105−118.

[78] Corcoran BJ, Swamy N, Hicks M. Cross-Tier, label-based security enforcement for Web applications. In: Proc. of the 2009 ACM SIGMOD Int'l Conf. on Management of Data. ACM Press, 2009. 269−282. [doi: 10.1145/1559845.1559875]

[79] Yoshihama S, Yoshizawa T, Watanabe Y. Dynamic information flow control architecture for Web applications. In: Proc. of the Computer Security (ESORICS 2007). Berlin, Heidelberg: Springer-Verlag, 2007. 267−282. [doi: 10.1007/978-3-540-74835-9_18]

[80] Schoepe D, Hedin D, Sabelfeld A. SeLINQ: Tracking information across application-database boundaries. ACM SIGPLAN Notices, 2014,49(9):25−38. [doi: 10.1145/2692915.2628151]

[81] Garvey CE, Papaccio PN. Multilevel data store design. In: Proc. of the AIAA/ASIS/DODCI 2nd Aerospace Computer Security Conf. San Diego: Internet Society, 1986. 58−64.

[82] Garvey C, Wu A. ASDViews [relational databases]. In: Proc. of the '88 IEEE Symp. on Security and Privacy. IEEE, 1988. 85−95. [doi: 10.1109/SECPRI.1988.8100]

[83] Denning DE, Lunt TF, Schell RR. The SeaView security model. In: Proc. of the '88 IEEE Symp. on Security and Privacy. IEEE, 1988. 218−233. [doi: 10.1109/SECPRI.1988.8114]

[84] Dwyer P, Onuegbe E, Stachour P, Thuraisingham B. Query processing in LDV: A secure database system. In: Proc. of the 4th IEEE Aerospace Computer Security Applications Conf. IEEE, 1988. 118−124. [doi: 10.1109/ACSAC.1988.113426]

[85] McDermott JP, Jajodia S, Sandhu RS. A single-level scheduler for the replicated architecture for multilevel-secure databases. In: Proc. of the 7th Annual Computer Security Applications Conf. IEEE, 1991. 2−11. [doi: 10.1109/CSAC.1991.213023]

[86] ORACLE7 Server Application Developer's Guide. Oracle Corporation, 1992.

[87] Hasan M, O'Connor JP, Pryzby G. Trusted distributed rubix. Trusted Distributed Rubix, 1996,23(1):172−191.

[88] Hunt GC, Larus JR. Singularity: Rethinking the software stack. ACM SIGOPS Operating Systems Review, 2007,41(2):37−49. [doi: 10.1145/1243418.1243424]

[89] Vogt P, Nentwich F, Jovanovic N. Cross site scripting prevention with dynamic data tainting and static analysis. In: Proc. of the NDSS. San Diego: Internet Society, 2007. 76−82.

[90] Chugh R, Meister JA, Jhala R, Lerner S. Staged information flow for JavaScript. ACM SIGPLAN Notices, 2009,44(6):50−62. [doi: 10.1145/1543135.1542483]

[91] Li Z, Zhang K, Wang XF. Mash-If: Practical information-flow control within client-side mashups. In: Proc. of the 2010 IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN). IEEE, 2010. 251−260. [doi: 10.1109/DSN.2010.5544312]

[92] De Groef W, Devriese D, Nikiforakis N. FlowFox: A Web browser with flexible and precise information flow control. In: Proc. of the 2012 ACM Conf. on Computer and Communications Security. ACM Press, 2012. 748−759. [doi: 10.1145/2382196.2382275]

[93] Austin TH, Flanagan C. Multiple facets for dynamic information flow. ACM SIGPLAN Notices, 2012,47(1):165−178. [doi: 10.1145/2103621.2103677]

[94] Hedin D, Sabelfeld A. Information-Flow security for a core of JavaScript. In: Proc. of the 25th IEEE Computer Security Foundations Symp. (CSF). IEEE, 2012. 3−18. [doi: 10.1109/CSF.2012.19]

[95] Just S, Cleary A, Shirley B. Information flow analysis for javascript. In: Proc. of the 1st ACM SIGPLAN Int'l Workshop on Programming Language and Systems Technologies for Internet Clients. ACM Press, 2011. 9−18. [doi: 10.1145/2093328.2093331]

[96] Bichhawat A, Rajani V, Garg D. Information flow control in WebKit's JavaScript bytecode. In: Proc. of the Principles of Security and Trust. Berlin, Heidelberg: Springer-Verlag, 2014. 159−178. [doi: 10.1007/978-3-642-54792-8_9]

[97] Chinis G, Pratikakis P, Ioannidis S, Athanasopoulos E. Practical information flow for legacy Web applications. In: Proc. of the 8th Workshop on Implementation, Compilation, Optimization of Object-Oriented Languages, Programs and Systems. ACM Press, 2013. 17−28. [doi: 10.1145/2491404.2491410]

[98] Pappas V, Kemerlis VP, Zavou A, Polychronakis M, Keromytis AD. CloudFence: Data flow tracking as a cloud service. In: Proc. of the Research in Attacks, Intrusions, and Defenses. Berlin, Heidelberg: Springer-Verlag, 2013. 411−431. [doi: 10.1007/978-3-642-41284-4_21]

[99] Xie X, Ray I, Adaikkalavan R, Gamble R. Information flow control for stream processing in clouds. In: Proc. of the 18th ACM Symp. on Access Control Models and Technologies. ACM Press, 2013. 89−100. [doi: 10.1145/2462410.2463205]

[100] Priebe C, Muthukumaran D, O'Keeffe D, Eyers D, Shand B, Kapitza R, Pietzuch P. CloudSafetyNet: Detecting data leakage between cloud tenants. In: Proc. of the 6th Edition of the ACM Workshop on Cloud Computing Security. ACM Press, 2014. 117−128. [doi: 10.1145/2664168.2664174]

[101] Mundada Y, Ramachandran A, Feamster N. Silverline: Data and network isolation for cloud services. Proc. of HotCloud, 2011, 23(3):342−356.

[102] Pasquier TFJM, Bacon J, Eyers D. FlowK: Information flow control for the cloud. In: Proc. of the 6th IEEE Int'l Conf. on Cloud Computing Technology and Science (CloudCom). IEEE, 2014. 70−77. [doi: 10.1109/CloudCom.2014.11]

[103] Pasquier TFJM, Bacon J, Shand B. FlowR: Aspect oriented programming for information flow control in ruby. In: Proc. of the 13th Int'l Conf. on Modularity. ACM Press, 2014. 37−48. [doi: 10.1145/2577080.2577090]

[104] Ganjali A, Lie D. Auditing cloud management using information flow tracking. In: Proc. of the 7th ACM Workshop on Scalable Trusted Computing. ACM Press, 2012. 79−84. [doi: 10.1145/2382536.2382549]

[105] Bacon J, Eyers D, Pasquier TF, Singh J, Papagiannis I, Pietzuch P. Information flow control for secure cloud computing. IEEE Trans. on Network and Service Management, 2014,11(1):76−89. [doi: 10.1109/TNSM.2013.122313.130423]

[106] Yang Z, Yang M. Leakminer: Detect information leakage on android with static taint analysis. In: Proc. of the 3rd World Congress on Software Engineering (WCSE). IEEE, 2012. 101−104. [doi: 10.1109/WCSE.2012.26]

[107] Mann C, Starostin A. A framework for static detection of privacy leaks in android applications. In: Proc. of the 27th Annual ACM Symp. on Applied Computing. Sierre: ACM Press, 2012. 1457−1462. [doi: 10.1145/2245276.2232009]

[108] Gibler C, Crussell J, Erickson J, Chen H. Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale. In: Proc. of the Trust and Trustworthy Computing. Berlin, Heidelberg: Springer-Verlag, 2012. 291−307. [doi: 10.1007/978-3-642-30921-2_17]

[109] Xiao X, Tillmann N, Fahndrich M. User-Aware privacy control via extended static-information-flow analysis. In: Proc. of the 27th IEEE/ACM Int'l Conf. on Automated Software Engineering. Palo Alto: ACM Press, 2012. 80−89. [doi: 10.1145/2351676.2351689]

[110] Xu R, Saïdi H, Anderson R. Aurasium: Practical policy enforcement for android applications. In: Proc. of the 21st USENIX Security Symp. Bellevue: USENIX, 2012. 32−44.

[111] Fritz C, Arzt S, Rasthofer S, Bartel A, Klein J, McDaniel P. Highly precise taint analysis for android application. EC SPRIDE Technical Report, TUD-CS-2013-0113, 2013. http://www.bodden.de/pubs/TUD-CS-2013-0113.pdf

[112] Enck W, Gilbert P, Chun BG, Chun BG, Cox LP, Sheth AN. TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In: Proc. of the OSDI. Berkeley: USENIX Association, 2010. 255−270.

[113] Yan LK, Yin H. Droidscope: Seamlessly reconstructing the OS and Dalvik semantic views for dynamic Android malware analysis. In: Proc. of the 21st USENIX Security Symp. Bellevue: USENIX, 2012. 135−146.

[114] Gilbert P, Chun BG, Cox L. Automating privacy testing of smartphone applications. Technical Report, CS-2011-02, Duke University, 2011.

[115] Akoush S, Carata L, Sohan R. Mrlazy: Lazy runtime label propagation for mapreduce. In: Proc. of the 6th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 2014). USENIX Association, 2014. 332−345.

[116] Pasquier TFJM, Singh J, Bacon J. Managing big data with information flow control. SIGARCH Computer Architecture News, 2014, 14(9):721−731.

[117] Singh J, Pasquier TFJM, Bacon J. Securing tags to control information flows within the Internet of Things. In: Proc. of the 2015 Int'l Conf. on Recent Advances in Internet of Things (RIoT). IEEE, 2015. 1−6. [doi: 10.1109/RIOT.2015.7104903]

[118] Portokalidis G, Homburg P, Anagnostakis K. Paranoid android: Versatile protection for smartphones. In: Proc. of the 26th Annual Computer Security Applications Conf. ACM Press, 2010. 347−356. [doi: 10.1145/1920261.1920313]

[119] Chen S, Kozuch M, Strigkos T, Falsafi B, Gibbons PB, Mowry TC, Vlachos E. Flexible hardware acceleration for instruction-grain program monitoring. ACM SIGARCH Computer Architecture News, 2008,36(3):377−388. [doi: 10.1145/1394608.1382153]

[120] Ruwase O, Gibbons PB, Mowry TC, Ramachandran V, Chen S, Kozuch M, Ryan M. Parallelizing dynamic information flow tracking. In: Proc. of the 20th Annual Symp. on Parallelism in Algorithms and Architectures. ACM Press, 2008. 35−45. [doi: 10.1145/1378533.1378538]

[121] Chow J, Garfinkel T, Chen PM. Decoupling dynamic program analysis from execution in virtual environments. In: Proc. of the USENIX 2008 Annual Technical Conf. on Annual Technical Conf. Berkeley: USENIX Association, 2008. 1−14.

[122] Jee K, Kemerlis VP, Keromytis AD. ShadowReplica: Efficient parallelization of dynamic data flow tracking. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security. ACM Press, 2013. 235−246. [doi: 10.1145/2508859.2516704]

[123] Jee K, Portokalidis G, Kemerlis VP, Ghosh S, August DI, Keromytis AD. A general approach for efficiently accelerating software-based dynamic data flow tracking on commodity hardware. In: Proc. of the 19th NDSS. San Diego: Internet Society, 2012. 324−335.

[124] Chang W, Streiff B, Lin C. Efficient and extensible security enforcement using dynamic data flow analysis. In: Proc. of the 15th ACM Conf. on Computer and Communications Security. Alexandria: ACM Press, 2008. 39−50. [doi: 10.1145/1455770.1455778]

[125] Portokalidis G, Bos H. Eudaemon: Involuntary and on-demand emulation against zero-day exploits. In: Proc. of the 2008 EuroSys. 2008. 287−299. [doi: 10.1145/1352592.1352622]

[126] Saxena P, Sekar R, Puranik V. Efficient fine-grained binary instrumentation with applications to taint-tracking. In: Proc. of the 6th CGO. ACM Press, 2008. 74−83. [doi: 10.1145/1356058.1356069]

[127] Kim HC, Keromytis AD. On the deployment of dynamic taint analysis for application communities. IEICE Trans. on Information & Systems, 2009,92(3):548−551.

附中文参考文献:

[12] 姚剑波.基于句法分析的安全信息流[博士学位论文].贵州:贵州大学,2006.

[20] 赵保华,陈波,陆超.概率信息流安全属性分析.计算机学报,2006,29(8):1447−145.

[21] 李超,殷丽华,郭云川.基于 ptSPA 的概率时间信息流安全属性分析.计算机研究与发展,2011,48(8):1370−1380.

[39] 单智勇,石文昌.STBAC:一种新的操作系统访问控制模型.计算机研究与发展,2008,45(5):758−764.

[40] 杨智,殷丽华,段淼毅,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]

[61] 王铁磊.面向二进制程序的漏洞挖掘关键技术研究[博士学位论文].北京:北京大学,2011.

[62] 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]

吴泽智(1990－),男,湖南长沙人,博士生,主要研究领域为网络与信息安全,信息流控制.

杨智(1975－),男,博士,副教授,主要研究领域为操作系统安全,信息流控制,云计算安全.

陈性元(1963－),男,博士,教授,博士生导师,主要研究领域为网络与信息安全.

杜学绘(1968－),女,博士,教授,博士生导师,主要研究领域为信息系统多级安全,云计算安全.