LIANG Zhenkai

Interesting in Being, Meaningful in Doing.

NUS School of Computing
13 Computing Drive
Computing 1, #03-16
Singapore, 117417

Email: liangzk@nus.edu.sg
Phone: (+65) 6516 1226
Fax: (+65) 6779 4580
Web: http://www.comp.nus.edu.sg/~liangzk

EDUCATION

Ph.D. in Computer Science, *December 2006*
Department of Computer Science, Stony Brook University, USA.

B.S. in Economics, *July 1999*
China Center for Economic Research, Peking University, China.

B.S. with Honor in Computer Science, *July 1999*
Department of Computer Science and Technology, Peking University, China.

PROFESSIONAL EXPERIENCE

Associate Professor, *January 2014 – Present*
Department of Computer Science, National University of Singapore, Singapore.

Co-Lead Principal Investigator, *October 2015 – Present*
National Cybersecurity R&D Laboratory, Singapore.

Assistant Dean (Graduate Studies), *July 2013 – June 2016*
School of Computing, National University of Singapore, Singapore.

Assistant Professor, *June 2008 – December 2013*
Department of Computer Science, National University of Singapore, Singapore.

Postdoctoral Researcher, *August 2006 – May 2008*
CyLab, Carnegie Mellon University, USA.

Research Assistant, *June 2002 – July 2006*,
Department of Computer Science, Stony Brook University, USA.

Teaching Assistant, *August 2001 – May 2002*,
Department of Computer Science, Stony Brook University, USA.

Software Engineer, *July 1999 – July 2001*,
Beijing Huatech Network Co. Ltd., China.

RESEARCH INTERESTS

Computer system security and software security, security of AI and other emerging systems, cyber security experimentation and analysis, system provenance analysis, trusted execution environments, economics/finance/policy aspects of cyber security, such as prevention of online scam, financial modeling of cyber crime, and cyber insurance.

PUBLICATIONS

Conference and Workshop

1. *"Kernel Auditing using Augmented Reference Behavior Analysis and Virtualized Selective Tracing."* Chuqi Zhang, Spencer Faith, Feras Al-Qassas, Theodorus Wensan Februanto, Zhenkai Liang, and Adil Ahmad. In *the 47th IEEE Symposium on Security and Privacy (S&P)*, May 2026.
2. *"PromoGuardian: Detecting Promotion Abuse Fraud with Multi-Relation Fused Graph Neural Networks."* Shaofei Li, Xiao Han, Ziqi Zhang, Zhenkai Liang, Yao Guo, Xiangqun Chen, Ding Li, Shuli Gao, and Minyao Hua. In *the 47th IEEE Symposium on Security and Privacy (S&P)*, May 2026.
3. *"RSafe: Incentivizing proactive reasoning to build robust and adaptive LLM safeguards."* Jingnan Zheng, Xiangtian Ji, Yijun Lu, Chenhang Cui, Weixiang Zhao, Gelei Deng, Zhenkai Liang, An Zhang, and Tat-Seng Chua. In *the 39th Annual Conference on Neural Information Processing Systems (NeurIPS)*, December 2025.
4. *"Improving LLM-based Log Parsing by Learning from Errors in Reasoning Traces."* Jialai Wang, Juncheng Lu, Jie Yang, Junjie Wang, Zeyu Gao, Chao Zhang, Zhenkai Liang, and Ee-Chien Chang. In *the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, November 2025.
5. *"Propagation-Based Vulnerability Impact Assessment for Software Supply Chains."* Bonan Ruan, Zhiwei Lin, Jiahao Liu, Chuqi Zhang, Kaihang Ji, and Zhenkai Liang. In *the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, November 2025.
6. *"ZendDiff: Differential Testing of PHP Interpreter."* Yuancheng Jiang, Jianing Wang, Qiange Liu, Yeqi Fu, Jian Mao, Roland H. C. Yap, and Zhenkai Liang. In *the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, November 2025.
7. *"PsyScam: A Benchmark for Psychological Techniques in Real-World Scams."* Shang Ma, Tianyi Ma, Jiahao Liu, Wei Song, Zhenkai Liang, Xusheng Xiao, and Yanfang Ye. In *the 2025 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, November 2025.
8. *"TAPPecker: TAP Logic Inference and Violation Detection in Heterogeneous Smart Home Systems."* Qixiao Lin, Jian Mao, Ziwen Liu, and Zhenkai Liang. In *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, October 2025.
9. *"TANS: A Chess-Inspired Notation System for Strategy Analysis of Tennis Games."* Yuexi Song, Chuanfei Li, Hao Cao, Ling Wu, Huanhuan Zheng, and Zhenkai Liang. In *the 2nd International Sports Analytics Conference and Exhibition (ISACE)*, September 2025.
   - **Distinguished Paper Award.**
10. *"Signals and Symptoms: ICS Attack Dataset from Railway Cyber Range."* Anis Yusof, Yuancheng Liu, Niklaus Kang, Choon Meng Seah, and Zhenkai Liang and Ee-Chien Chang. In *the 11th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems*, September 2025.

11. *"Evaluating Disassembly Errors With Only Binaries."* Lambang Akbar, Yuancheng Jiang, Roland Yap, Zhenkai Liang, and Zhuohao Liu. In *the 20th ACM ASIA Conference on Computer and Communications Security (AsiaCCS)*, August 2025.
12. *"Fuzzing the PHP Interpreter via Dataflow Fusion."* Yuancheng Jiang, Chuqi Zhang, Bonan Ruan, Jiahao Liu, Manuel Rigger, Roland H. C. Yap, and Zhenkai Liang. In *the 34th USENIX Security Symposium*, August 2025.
    - **Distinguished Paper Award.**
13. *"Your Scale Factors are My Weapon: Targeted Bit-Flip Attacks on Vision Transformers via Scale Factor Manipulation.."* Jialai Wang, Yuxiao Wu, Weiye Xu, Yating Huang, Chao Zhang, Zongpeng Li, Mingwei Xu, and Zhenkai Liang. In *the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2025.
14. *"Fork State-Aware Differential Fuzzing for Blockchain Consensus Implementations."* Wonhoi Kim, Hocheol Nam, Muoi Tran, Amin Jalilov, Zhenkai Liang, Sang Kil Cha, and Min Suk Kang. In *International Conference on Software Engineering (ICSE)*, May 2025.
15. *"Erebor: A Drop-In Sandbox Solution for Private Data Processing in Untrusted Confidential Virtual Machines."* Chuqi Zhang, Rahul Priolkar, Yuancheng Jiang, Yuan Xiao, Mona Vij, Zhenkai Liang, and Adil Ahmad. In *European Conference on Computer Systems (EuroSys)*, March 2025.
16. *"*SCRUTINIZER*: Towards Secure Forensics on Compromised TrustZone."* Yiming Zhang, Fengwei Zhang, Xiapu Luo, Rui Hou, Xuhua Ding, Zhenkai Liang, Shoumeng Yan, Tao Wei, and Zhengyu He. In *the Network and Distributed System Security Symposium (NDSS)*, February 2025.
17. *"UI-CTX: Understanding UI Behaviors with Code Contexts for Mobile Applications."* Jiawei Li, Jiahao Liu, Jian Mao, Jun Zeng and Zhenkai Liang. In *the Network and Distributed System Security Symposium (NDSS)*, February 2025.
18. *"ProvGuard: Detecting SDN Control Policy Manipulation via Contextual Semantics of Provenance Graphs."* Ziwen Liu, Jian Mao, Jun Zeng, Jiawei Li, Qixiao Lin, Jiahao Liu, Jianwei Zhuge and Zhenkai Liang. In *the Network and Distributed System Security Symposium (NDSS)*, February 2025.
19. *"From Observations to Insights: Constructing Effective Cyberattack Provenance with PROVCON."* Anis Yusof, Shaofei Li, Arshdeep Singh Kawatra, Ding Li, and Ee-Chien Chang and Zhenkai Liang. In *Workshop on SOC Operations and Construction (WOSOC) 2025*, February 2025.
20. *"VulZoo: A Comprehensive Vulnerability Intelligence Dataset (Tool Demonstration Track)."* Bonan Ruan, Jiahao Liu, Weibo Zhao, and Zhenkai Liang. In *the 39th IEEE/ACM International Conference on Automated Software Engineering, Tool Demonstrations (ASE Demo)*, October 2024.
21. *"MaskDroid: Robust Android Malware Detection with Masked Graph Representations."* Jingnan Zheng, Jiahao Liu, An Zhang, Jun Zeng, Ziqi Yang, Zhenkai Liang, and Tat-Seng Chua. In *the 39th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, October 2024.

22. *"The HitchHiker's Guide to High-Assurance System Observability Protection with Efficient Permission Switches."* Chuqi Zhang, Jun Zeng, Yiming Zhang, Adil Ahmad, Fengwei Zhang, Hai Jin, and Zhenkai Liang. In *the 31st ACM Conference on Computer and Communications Security (CCS)*, September 2024.

23. *"KernJC: Automated Vulnerable Environment Generation for Linux Kernel Vulnerabilities."* Bonan Ruan, Jiahao Liu, Chuqi Zhang, and Zhenkai Liang. In *the 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, September 2024.
    - **Best Practical Paper Award.**

24. *"CrypTody: Cryptographic Misuse Analysis of IoT Firmware via Data-flow Reasoning."* Jianing Wang, Shanqing Guo, Wenrui Diao, Yue Liu, Haixin Duan, Yichen Liu, and Zhenkai Liang. In *the 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, September 2024.

25. *"UIHash: Detecting Similar Android UIs through Grid-Based Visual Appearance Representation."* Jiawei Li, Jian Mao, Jun Zeng, Qixiao Lin, Shaowen Feng, and Zhenkai Liang. In *USENIX Security Symposium*, August, 2024.

26. *"Detecting Logic Bugs in Graph Database Management Systems via Injective and Surjective Graph Query Transformation."* Yuancheng Jiang, Jiahao Liu, Jinsheng Ba, Roland Yap, Zhenkai Liang, and Manuel Rigger. In *the 46th International Conference on Software Engineering (ICSE)*, April 2024.

27. *"Evaluating Disassembly Ground Truth Through Dynamic Tracing."* Lambang Akbar, Yuancheng Jiang, Roland Yap, Zhenkai Liang, and Zhuohao Liu. In *the Workshop on Binary Analysis Research co-located with NDSS Symposium (BAR)*, February 2024.

28. *"Securing Web Inputs Using Parallel Session Attachments."* Ziqi Yang, Ruite Xu, Qixiao Lin, Shikun Wu, Jian Mao, and Zhenkai Liang. In *International Conference on Security and Privacy in Communication Networks (SecureComm)*, October 2023.

29. *"Learning Graph-based Code Representations for Source-level Functional Similarity Detection."* Jiahao Liu, Jun Zeng, Xiang Wang, and Zhenkai Liang. In *the 45th IEEE/ACM International Conference on Software Engineering (ICSE)*, May 2023.

30. *"PalanTír: Optimizing Attack Provenance with Hardware-enhanced System Observability."* Jun Zeng, Chuqi Zhang, and Zhenkai Liang. In *the 29th ACM Conference on Computer and Communications Security (CCS)*, November 2022.

31. *"Extensible Virtual Call Integrity."* Yuancheng Jiang, Gregory J. Duck, Roland Yap, Zhenkai Liang, and Pinghai Yuan. In *the 27th European Symposium on Research in Computer Security (ESORICS)*, September 2022.

32. *"AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports."* Zhenyuan Li, Jun Zeng, Yan Chen, and Zhenkai Liang. In *the 27th European Symposium on Research in Computer Security (ESORICS)*, September 2022.

33. *"TeLL: Log Level Suggestions via Modeling Multi-level Code Block Information."* Jiahao Liu, Jun Zeng, Xiang Wang, Kaihang Ji, and Zhenkai Liang. In *the*

31st ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), July 2022.

34. *"FreeWill: Automatically Diagnosing Use-after-free Bugs via Reference Miscounting Detection on Binaries."* Liang He, Hong Hu, Purui Su, Yan Cai, and Zhenkai Liang. In *USENIX Security Symposium*, July 2022.
35. *"FlowMatrix: GPU-Assisted Information-Flow Analysis through Matrix-Based Representation."* Kaihang Ji, Jun Zeng, Yuancheng Jiang, Zhenkai Liang, Zheng Leong Chua, Prateek Saxena, and Abhik Roychoudhury. In *USENIX Security Symposium*, July 2022.
36. *"RecIPE: Revisiting the Evaluation of Memory Error Defenses."* Yuancheng Jiang, Roland Yap, Zhenkai Liang, and Hubert Rosier. In *the 17th ACM ASIA Conference on Computer and Communications Security (AsiaCCS)*, June 2022.
37. "SHADEWATCHER*: Recommendation-guided Cyber Threat Analysis using System Audit Records."* Jun Zeng, Xiang Wang, Jiahao Liu, Yinfang Chen, Zhenkai Liang, Tat-Seng Chua, and Zheng Leong Chua. In *IEEE Symposium on Security and Privacy (S&P)*, May 2022.
38. *"Identifying privacy weaknesses from multi-party trigger-action integration platforms."* Kulani Mahadewa, Yanjun Zhang, Guangdong Bai, Lei Bu, Zhiqiang Zuo, Dileepa Fernando, Zhenkai Liang, and Jin Song Dong. In *International Symposium on Software Testing and Analysis (ISSTA)*, July 2021.
39. *"WATSON: Abstracting Behaviors from Audit Logs via Aggregation of Contextual Semantics."* Jun Zeng, Zheng Leong Chua, Yinfang Chen, Kaihang Ji, Zhenkai Liang, and Jian Mao. In *the Network and Distributed System Security Symposium (NDSS)*, February 2021.
40. *"Robust P2P Primitives Using SGX Enclaves."* Yaoqi Jia, Shruti Tople, Tarik Moataz, Deli Gong, Prateek Saxena, Zhenkai Liang. In *the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, October 2020.
41. *"Neural Network Inversion in Adversarial Setting via Background Knowledge Alignment."* Ziqi Yang, Jiyi Zhang, Ee-Chien Chang, Zhenkai Liang. In *the 26th ACM Conference on Computer and Communications Security (CCS)*, November 2019.
42. *"LightSense: A Novel Side Channel for Zero-permission Mobile User Tracking."* Quanqi Ye, Yan Zhang, Guangdong Bai, Naipeng Dong, Zhenkai Liang, Jin Song Dong, Haoyu Wang. In *22nd Information Security Conference (ISC)*, September 2019.
43. *"Detecting Android Side Channel Probing Attacks Based on System States."* Qixiao Lin, Jian Mao, Futian Shi, Shishi Zhu, Zhenkai Liang. In *the 14th International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, June 2019.
    - **Best Paper Award.**
44. *"One Engine To Serve 'em All: Inferring Taint Rules Without Architectural Semantics."* Zheng Leong Chua, Yanhao Wang, Teodora Baluta, Prateek Saxena, Zhenkai Liang, Purui Su. In *the 21st Network and Distributed System Security*

Symposium (NDSS), February 2019.
- **Distinguished Paper Award Honorable Mentions.**

45. *"Fuzzing Program Logic Deeply Hidden in Binary Program Stages."* Yanhao Wang, Zheng Leong Chua, Yuwei Liu, Purui Su, and Zhenkai Liang. In *the 26th IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, February 2019.
46. *"HOMESCAN: Scrutinizing Implementations of Smart Home Integrations."* Kulani Tharaka Mahadewa, Kailong Wang, Guangdong Bai, Ling Shi, Jin Song Dong, and Zhenkai Liang. In *the 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*, December 2018.
47. *"Automated Identification of Sensitive Data via Flexible User Requirements."* Ziqi Yang, and Zhenkai Liang. In *International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2018.
48. *"DTaint: Detecting the Taint-Style Vulnerability in Embedded Device Firmware."* Kai Cheng, Qiang Li, Lei Wang, Qian Chen, Yaowen Zheng, Limin Sun, Zhenkai Liang. In *the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 2018.
49. *"Robust Detection of Android UI Similarity."* Jian Mao, Jingdong Bian, Hanjun Ma, Yaoqi Jia, Zhenkai Liang, and Xuxian Jiang. In *IEEE International Conference on Communications (ICC)*, May 2018.
50. *"A Novel Graph-based Mechanism for Identifying Traffic Vulnerabilities in Smart Home IoT."* Yizhen Jia, Yinhao Xiao, Jiguo Yu, Xiuzhen Cheng, Zhenkai Liang, Zhiguo Wan. In *IEEE Conference on Computer Communications (INFOCOM)*, April 2018.
51. *"Automatically Assessing Crashes From Heap Overflows."* Liang He, Yan Cai, Hong Hu, Purui Su, Zhenkai Liang, Yi Yang, Huafeng Huang, Jia Yan, Xiangkun Jia, and Dengguo Feng. In *the 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE)*, November 2017.
52. *"Detecting Phishing Websites via Aggregation Analysis of Page Layouts."* Jian Mao, Jingdong Bian, Wenqian Tian, Shishi Zhu, Tao Wei, Aili Li, and Zhenkai Liang. In *International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, October 2017.
53. *"Enabling practical experimentation in cyber-security training."* Jian Mao, Zheng Leong Chua, and Zhenkai Liang. In *International Conference on Dependable Systems and Communications (DSC)*, August 2017.
54. *"Privilege Leakage and Information Stealing through the Android Task Mechanism."* Yinhao Xiao, Guangdong Bai, Jian Mao, Zhenkai Liang, and Wei Cheng. In *International Conference on Pervasive and Ubiquitous Computing Adjunct (PAC)*, August 2017.
55. *"Neural Nets Can Learn Function Type Signatures From Binaries."* Zheng Leong Chua, Shiqi Shen, Prateek Saxena, and Zhenkai Liang. In *the 26th USENIX Security Symposium*, August 2017.
56. *"Phishing Website Detection Based on Effective CSS Features of Web Pages."* Jian Mao, Wenqian Tian, Pei Li, Tao Wei, and Zhenkai Liang. In *the 12th*

International Conference on Wireless Algorithms, Systems, and Applications (WASA), June 2017.

57. *"The Web/Local Boundary Is Fuzzy: A Security Study of Chrome's Process-based Sandboxing."* Yaoqi Jia, Zheng Leong Chua, Hong Hu, Shuo Chen, Prateek Saxena, and Zhenkai Liang. In *the 23rd ACM Conference on Computer and Communications Security (CCS)*, October 2016. (Acceptance rate: 16.5%)
58. *"A Function-Level Behavior Model for Anomalous Behavior Detection in Hybrid Mobile Applications."* Jian Mao, Ruilong Wang, Yue Chen, Yinhao Xiao, Yaoqi Jia, and Zhenkai Liang. In *International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, October 2016.
59. *"Toward Exposing Timing-based Probing Attacks in Web Applications."* Jian Mao, Yue Chen, Futian Shi, Yaoqi Jia, and Zhenkai Liang. In *the 11th International Conference on Wireless Algorithms, Systems, and Applications (WASA'16)*, August 2016.
60. *"Anonymity in Peer-assisted CDNs: Inference Attacks and Mitigation."* Yaoqi Jia, Guangdong Bai, Prateek Saxena, and Zhenkai Liang. In *the 16th Privacy Enhancing Technologies Symposium (PETS)*, July 2016. (Acceptance rate: 26.98%)
61. *"Data-Oriented Programming: On the Expressiveness of Non-Control Data Attacks."* Hong Hu, Shweta Shinde, Sendroiu Adrian, Zheng Leong Chua, Prateek Saxena, and Zhenkai Liang. In *the 2016 IEEE Symposium on Security and Privacy*, May 2016.
62. *"Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software."* Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena. In *the 20th European Symposium on Research in Computer Security (ESORICS)*, September 2015.
63. *"Web-to-Application Injection Attacks on Android: Characterization and Detection."* Behnaz Hassanshahi, Yaoqi Jia, Roland H. C. Yap, Prateek Saxena, and Zhenkai Liang. In *European Symposium on Research in Computer Security 2015 (ESORICS)*, September 2015.
64. *"Automatic Generation of Data-Oriented Exploits."* Hong Hu, Zheng Leong Chua, Sendroiu Adrian, Prateek Saxena, and Zhenkai Liang. In *the 24th USENIX Security Symposium*, August 2015.
65. *"You Can't Be Me: Enabling Trusted Paths & User Sub-Origins in Web Browsers."* Enrico Budianto, Yaoqi Jia, Xinshu Dong, Prateek Saxena, and Zhenkai Liang. In *the 17th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, September 2014.
66. *"SQLR: Grammar-guided Validation of SQL Injection Sanitizers."* Sai Sathyanarayan, Dawei Qi, Zhenkai Liang, and Abhik Roychoudhury. In *the 19th International Conference on Engineering of Complex Computer Systems (ICECCS)*, August 2014. (Short paper)
67. *"Understanding Complex Binary Loading Behaviors."* Ting Dai, Mingwei Zhang, Roland Yap, and Zhenkai Liang. In *the 19th International Conference on Engineering of Complex Computer Systems (ICECCS)*, August 2014.

68. *"DroidVault: A Trusted Data Vault for Android Devices."* Xiaolei Li, Hong Hu, Guangdong Bai, Yaoqi Jia, Zhenkai Liang, and Prateek Saxena. In *the 19th International Conference on Engineering of Complex Computer Systems (ICECCS)*, August 2014.
    - **Best Paper Award.**
69. *"A Light-weight Software Environment for Confining Android Malware."*. Xiaolei Li, Guangdong Bai, Benjamin Thian, Zhenkai Liang, and Heng Yin. In *International Workshop on Trustworthy Computing*, June 2014.
70. *"I Know Where You've Been: Geo-Inference Attacks via the Browser Cache."* Yaoqi Jia, Xinshu Dong, Zhenkai Liang, and Prateek Saxena. In *Web 2.0 Security & Privacy Workshop (W2SP)*, May 2014.
    - **Best Paper Award.**
71. *"A Usage-Pattern Perspective for Privacy Ranking of Android Apps."* Xiaolei Li, Xinshu Dong, and Zhenkai Liang. In *the 2014 International Conference on Intelligent Science and Systems (ICISS)*, December 2014.
72. *"TrustFound: Towards a Formal Foundation for Model Checking Trusted Computing Platforms"*. Guangdong Bai, Jianan Hao, Jianliang Wu, Yang Liu, Zhenkai Liang, and Andrew Martin. In *the 19th International Symposium on Formal Methods (FM)*, May 2014.
73. *"AirBag: Boosting Smartphone Resistance to Malware Infection"*. Chiachih Wu, Yajin Zhou, Kunal Patel, Zhenkai Liang, and Xuxian Jiang. In *the 21st Annual Network & Distributed System Security Symposium (NDSS)*, February 2014. (Acceptance rate: 18.6%)
74. *"Rating Web Pages Using Page-Transition Evidence."* Jian Mao, Xinshu Dong, Pei Li, Tao Wei, and Zhenkai Liang. In *the 15th International Conference on Information and Communications Security (ICICS)*, December 2013. (Short paper)
75. *"Protecting Sensitive Web Content from Client-side Vulnerabilities with* CRYPTONS." Xinshu Dong, Zhaofeng Chen, Hossein Siadati, Shruti Tople, Prateek Saxena, and Zhenkai Liang. In *the 14th ACM Conference on Computer and Communications Security (CCS)*, November 2013. (Acceptance rate: 19.8%)
76. *"BaitAlarm: Detecting Phishing Sites Using Similarity in Fundamental Visual Features."* Jian Mao, Kun Li, Pei Li, Tao Wei, and Zhenkai Liang. In *the International Workshop on Secure Cloud Computing*, September 2013.
77. *"A Quantitative Evaluation of Privilege Separation in Web Browser Designs."* Xinshu Dong, Hong Hu, Prateek Saxena, and Zhenkai Liang. In *the 18th European Symposium on Research in Computer Security (ESORICS)*, September 2013. (Acceptance rate: 17.8%)
78. *"A Comprehensive Client-side Behavior Model for Diagnosing Attacks in Ajax Applications."* Xinshu Dong, Kailas Patil, Jian Mao, and Zhenkai Liang. In *the 18th International Conference on Engineering of Complex Computer Systems (ICECCS)*, July 2013. (Acceptance rate: 26.3%)
79. *"A Software Environment for Confining Malicious Android Applications via Resource Virtualization."* Xiaolei Li, Guangdong Bai, Zhenkai Liang, and Heng

Yin. In *the 18th International Conference on Engineering of Complex Computer Systems (ICECCS)*, July 2013. (Short paper)

80. *"Enforcing System-Wide Control Flow Integrity for Exploit Detection and Diagnosis."* Aravind Prakash, Heng Yin, and Zhenkai Liang. In *the 8th ACM Symposium on Information, Computer and Communications Security (AsiaCCS)*, May 2013. (Acceptance rate: 28.7%)

81. *"Detecting and Preventing ActiveX API-Misuse Vulnerabilities in Internet Explorer."* Ting Dai, Sai Sathyanarayan, Roland Yap, and Zhenkai Liang. In *the 14th International Conference on Information and Communications Security (ICICS)*, December 2012. (Short paper)

82. *"An Empirical Study of Dangerous Behaviors in Firefox Extensions."* Jiangang Wang, Xiaohong Li, Xuhui Liu, Xinshu Dong, Junjie Wang, Zhenkai Liang, and Zhiyong Feng. In *the 15th Information Security Conference (ISC)*, September 2012. (Acceptance rate: 31.9%)

83. *"Codejail: Application-transparent Isolation of Libraries with Tight Program Interactions."* Yongzheng Wu, Sai Sathyanarayan, Roland Yap, and Zhenkai Liang. In *the 17th European Symposium on Research in Computer Security (ESORICS)*, September 2012. (Acceptance rate: 20.2%)

84. *"Tracking the Trackers: Fast and Scalable Dynamic Analysis of Web Content for Privacy Violations."* Minh Tran, Xinshu Dong, Zhenkai Liang, and Xuxian Jiang. In *the 10th International Conference on Applied Cryptography and Network Security (ACNS)*, June 2012. (Acceptance rate: 17.2%)

85. *"A Framework to Eliminate Backdoors from Response Computable Authentication."* Shuaifu Dai, Tao Wei, Chao Zhang, Tielei Wang, Yu Ding, Zhenkai Liang, and Wei Zou. In *the 2012 IEEE Symposium on Security and Privacy*, May 2012. (Acceptance rate: 13.0%)

86. *"Identifying and Analyzing Pointer Misuses for Sophisticated Memory-corruption Exploit Diagnosis."* Mingwei Zhang, Aravind Prakash, Xiaolei Li, Zhenkai Liang, and Heng Yin. In *the 19th Annual Network & Distributed System Security Symposium (NDSS)*, February 2012. (Acceptance rate: 17.8%)

87. *"AdSentry: Comprehensive and Flexible Confinement of JavaScript-based Advertisements."* Xinshu Dong, Minh Tran, Zhenkai Liang, and Xuxian Jiang. In *the 27th Annual Computer Security Applications Conference (ACSAC)*, December 2011. (Acceptance rate: 20%)

88. *"Towards Fine-Grained Access Control in JavaScript Contexts."* Kailas Patil, Xinshu Dong, Xiaolei Li, Zhenkai Liang, and Xuxian Jiang. In *the 31st IEEE International Conference on Distributed Computing Systems (ICDCS)*, June 2011. (Acceptance rate: 15.4%)

89. *"Jump-Oriented Programming: A New Class of Code-Reuse Attack."* Tyler Bletsch, Xuxian Jiang, Vince Freeh, and Zhenkai Liang. In *the 6th ACM Symposium on Information, Computer and Communications Security (AsiaCCS)*, March 2011. (Acceptance rate: 16.1%)

90. *"Heap Taichi: Exploiting Memory Allocation Granularity In Heap-spraying Attacks."* Yu Ding, Tao Wei, Tielei Wang, Zhenkai Liang, and Wei Zou. In *the*

25st Annual Computer Security Applications Conference (ACSAC), December 2010. (Acceptance rate: 16.3%)

91. *"Golden Implementation Driven Software Debugging."* Ansuman Banerjee, Abhik Roychoudhury, Johannes A. Harlie, and Zhenkai Liang. In *ACM SIGSOFT 18th International Symposium on Foundations of Software Engineering (FSE)*, November 2010. (Acceptance rate: 20%)
92. *"Test Generation to Expose Changes in Evolving Programs."* Dawei Qi, Abhik Roychoudhury, and Zhenkai Liang. In *the 25th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, September 2010. (Acceptance rate: 18%)
93. *"Transparent Protection of Commodity OS Kernels using Hardware Virtualization."* Michael Grace, Zhi Wang, Deepa Srinivasan, Jinku Li, Xuxian Jiang, Zhenkai Liang, and Siarhei Liakh. In *the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm)*, September 2010. (Acceptance rate: 25%)
94. *"Towards Generating High Coverage Vulnerability-Based Signatures with Protocol-Level Constraint-Guided Exploration."* Juan Caballero, Zhenkai Liang, Pongsin Poosankam, and Dawn Song. In *the 12th International Symposium on Recent Advances in Intrusion Detection (RAID)*, September 2009. (Acceptance rate: 28.3%)
95. *"DARWIN: An Approach for Debugging Evolving Programs."* Dawei Qi, Abhik Roychoudhury, Zhenkai Liang, and Kapil Vaswani. In *the ESEC and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE)*, August 2009. (Acceptance rate: 14.7%)
    - **ACM SIGSOFT Distinguished Paper Award.**
96. *"BitBlaze: A New Approach to Computer Security via Binary Analysis."* Dawn Song, David Brumley, Heng Yin, Juan Caballero, Ivan Jager, Min Gyung Kang, Zhenkai Liang, James Newsome, Pongsin Poosankam, and Prateek Saxena. (Invited keynote paper.) In *the 4th International Conference on Information Systems Security (ICISS)*, December 2008. (Acceptance rate: 18%)
97. *"Expanding Malware Defense by Securing Software Installations."* Weiqing Sun, R. Sekar, Zhenkai Liang, and V.N. Venkatakrishnan. In *the 5th Conference on Detection of Intrusions, Malware and Vulnerability Analysis (DIMVA)*, July 2008. (Acceptance rate: 31%)
98. *"AGIS: Automatic Generation of Infection Signatures."* Zhuowei Li, Xiaofeng Wang, Zhenkai Liang, and Michael K. Reiter. In *the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 2008. (Acceptance Rate: 25%)
99. *"HookFinder: Identifying and Understanding Malware Hooking Behaviors."* Heng Yin, Zhenkai Liang, and Dawn Song. In *the 15th Annual Network and Distributed System Security Symposium (NDSS)*, February 2008. (Acceptance rate: 17.8%)
100. *"Polyglot: Automatic Extraction of Protocol Message Format using Dynamic Binary Analysis."* Juan Caballero, Heng Yin, Zhenkai Liang, and Dawn Song.

In *the 14th ACM Conference on Computer and Communications Security (CCS)*, October 2007. (Acceptance rate: 18%)

101. *"Towards Automatic Discovery of Deviations in Binary Implementations with Applications to Error Detection and Fingerprint Generation."* David Brumley, Juan Caballero, Zhenkai Liang, James Newsome, and Dawn Song. In *the 16th USENIX Security Symposium*, August 2007. (Acceptance rate: 12.3%)
    - **Best Paper Award.**
102. "Automatic Generation of Buffer Overflow Attack Signatures: An Approach Based on Program Behavior Models." Zhenkai Liang and R. Sekar. In *the 21st Annual Computer Security Applications Conference (ACSAC)*, December 2005. (Acceptance rate: 19.6%)
103. *"Fast and Automated Generation of Attack Signatures: A Basis for Building Self-Protecting Servers."* Zhenkai Liang and R. Sekar. In *the 12th ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance rate: 15.2%)
104. *"Automatic Synthesis of Filters to Discard Buffer Overflow Attacks: A Step Towards Realizing Self-Healing Systems."* Zhenkai Liang, R. Sekar, and Daniel C. DuVarney. In *the USENIX Annual Technical Conference*, April 2005. (Short Paper.)
105. *"One-way Isolation: An Effective Approach for Realizing Safe Execution Environments."* Weiqing Sun, Zhenkai Liang, R. Sekar, and V. N. Venkatakrishnan. In *the 12th Annual Network and Distributed System Security Symposium (NDSS)*, February 2005. (Acceptance rate: 13%)
106. *"Isolated Program Execution: An Application Transparent Approach for Executing Untrusted Programs."* Zhenkai Liang, V. N. Venkatakrishnan, and R. Sekar. In *the 19th Annual Computer Security Applications Conference (ACSAC)*, December 2003. (Acceptance rate: 30%)
    - **Outstanding Paper Award.**
107. *"An Approach for Secure Software Installation."* V. N. Venkatakrishnan, R. Sekar, S. Tsipa, T. Kamat, and Z. Liang. In *the 16th Large Installation System Administration Conference (LISA)*, November 2002.

Journal

1. *"I Know Your Social Network Accounts: A Novel Attack Architecture for Device-identity Association."* Yinhao Xiao, Yizhen Jia, Xiuzhen Cheng, Shengling Wang, Jian Mao, and Zhenkai Liang. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Volume 20, Issue 2, February 2023.
2. *"Semantic-fuzzing-based Empirical Analysis of Voice Assistant Systems of Asian Symbol Languages."* Jian Mao, Ziwen Liu, Qixiao Lin, and Zhenkai Liang. In *IEEE Internet of Things Journal*, Volume 9, Issue 12, September 2022.
3. *"Scrutinizing Implementations of Smart Home Integrations."* Kulani Mahadewa, Kailong Wang, Guangdong Bai, Ling Shi, Yan Liu, Jin Song Dong, and Zhenkai Liang. In *IEEE Transactions on Software Engineering (TSE)*, Volume 47, Issue 12, December 2021.

4. *"Asia's Surging Interest in Binary Analysis."* Sang Kil Cha, and Zhenkai Liang. In *Communications of the ACM*, Volume 63, Issue 4, March 2020.
5. *"Phishing Page Detection via Learning Classifiers from Page Layout Feature."* Jian Mao, Jingdong Bian, Wenqian Tian, Shishi Zhu, Tao Wei, Aili Li, and Zhenkai Liang. In *EURASIP Journal on Wireless Communications and Networking (EURASIP JWCN)*, Volume 2019, February 2019.
6. *"I Can See Your Brain: Investigating Home-Use Electroencephalography System Security."* Yinhao Xiao, Yizhen Jia, Xiuzhen Cheng, Jiguo Yu, Zhenkai Liang, and Zhi Tian. In *IEEE Internet of Things Journal (IoT-J)*, Volume 6, Issue 4, February 2019.
7. *"Automated Identification of Sensitive Data from Implicit User Specification."* Ziqi Yang, and Zhenkai Liang. In *Cybersecurity*, Volume 1, Issue 1, December 2018.
8. *"Detecting Malicious Behaviors in JavaScript Applications."* Jian Mao, Jingdong Bian, Ruilong Wang, Yue Chen, Yinhao Xiao, and Zhenkai Liang. In *IEEE Access*, Volume 6, January 2018.
9. *"SplitPass: A Mutually Distrusting Two-Party Password Manager."* Yutao Liu, Dong Du, Yubin Xia, Haibo Chen, Binyu Zang, and Zhenkai Liang. In *Journal of Computer Science and Technology (JCST)*, Volume 33, Issue 1, January 2018.
10. *"Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity."* Jian Mao, Jingdong Bian, Wenqian Tian, Pei Li, Tao Wei, and Zhenkai Liang. In *IEEE Access*, Volume 5, August 2017.
11. *"RoppDroid: Robust Permission Re-delegation Prevention in Android Inter-component Communication."* Ting Dai, Xiaolei Li, Bhanaz Hassanshahi, Roland Yap, and Zhenkai Liang. In *Computer & Security*, Volume 68, July 2017.
12. *"Monet: A User-Oriented Behavior-Based Malware Variants Detection System for Android."* Mingshen Sun, Xiaolei Li, John C.S. Lui, Richard T. Ma, and Zhenkai Liang. In *IEEE Transactions on Information Forensics and Security (TIFS)*, Volume 12, Issue 5, May 2017.
13. *"Toward Exposing Timing-Based Probing Attacks in Web Applications."* Jian Mao, Yue Chen, Futian Shi, Yaoqi Jia, and Zhenkai Liang. In *Sensors*, Volume 27, Issue 1, February 2017.
14. *"Man-in-the-browser-cache: Persisting HTTPS Attacks via Browser Cache Poisoning."* Yaoqi Jia, Yue Chen, Xinshu Dong, Prateek Saxena, Jian Mao, and Zhenkai Liang. In *Computer & Security*, Volume 55, November 2016.
15. *"A Framework for Practical Dynamic Software Updating."* Gang Chen, Hai Jin, Deqing Zou, Zhenkai Liang, Bing Bing Zhou, and Hao Wang. In *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, Volume 27, Issue 4, April 2016.
16. *"Automatic Permission Inference for Hybrid Mobile Apps."* Jian Mao, Hanjun Ma, Yue Chen, Yaoqi Jia, and Zhenkai Liang. In *Journal of High Speed Networks*, Volume 22, Issue 1, February 2016.
17. *"Tool, Technique, and Tao in Computer Security Education."* Zhenkai Liang and Jian Mao. In *IEEE Reliability Newsletter Special Issues*, August 2015.

18. *"I Know Where You've Been: Geo-Inference Attacks via the Browser Cache."* Yaoqi Jia, Xinshu Dong, Zhenkai Liang, and Prateek Saxena. In *IEEE Internet Computing*, Volume 19, Issue 01, January/February, 2015.
19. *"SafeStack: Automatically Patching Stack-based Buffer Overflow Vulnerabilities."* Gang Chen, Hai Jin, Deqing Zou, Bing Bing Zhou, Zhenkai Liang, Weide Zheng, and Xuanhua Shi. To appear in *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Volume 10, Issue 06, November/December 2013.
20. *"DARWIN: An Approach for Debugging Evolving Programs."* Dawei Qi, Abhik Roychoudhury, Zhenkai Liang, and Kapil Vaswani. In *ACM Transactions on Software Engineering and Methodology (TOSEM)*, Volume 21, Issue 3, June 2012.
21. *"Alcatraz: An Isolated Environment for Experimenting with Untrusted Software."* Zhenkai Liang, Weiqing Sun, R.Sekar, and V.N. Venkatakrishnan. In *ACM Transactions on Information and System Security (TISSEC)*, Volume 12, Issue 3, January 2009.

Book Chapter

1. *"Automatically Identifying Trigger-based Behavior in Malware."* David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Pongsin Poosankam, Dawn Song, and Heng Yin. In *Botnet Analysis and Defense*, vol. 36 of Advances in Information Security Series, Wenke Lee, Cliff Wang, and David Dagon (editors), pp. 65-88, Springer, 2008.

HONORS AND AWARDS

Research Awards:

1. **Distinguished Paper Award**, *the 34th USENIX Security Symposium*, 2025.
2. **Distinguished Paper Award**, *the 2nd International Sports Analytics Conference and Exhibition (ISACE)*, 2025.
3. **Best Practical Paper Award**, *the 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2024.
4. **Distinguished Paper Award Honorable Mentions**, *the 21st Network and Distributed System Security Symposium (NDSS)*, 2019.
5. **Best Paper Award**, *the 14th International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, 2019.
6. **Best Paper Award**, *the 19th International Conference on Engineering of Complex Computer Systems (ICECCS)*, 2014.
7. **Best Paper Award**, *Web 2.0 Security & Privacy Workshop (W2SP)*, 2014.
8. **ACM SIGSOFT Distinguished Paper Award**, *the ESEC and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE)*, 2009.
9. **NUS Young Investigator Award**, *National University of Singapore*, 2009.
10. **Best Paper Award**, *the 16th USENIX Security Symposium*, 2007.
11. **Outstanding Paper Award**, *the 19th Annual Computer Security Applications Conference (ACSAC)*, 2003.

Education Awards:

1. **Faculty Teaching Excellence Award**, *NUS School of Computing*, Academic Year 2024/2025.
2. **Faculty Teaching Excellence Award**, *NUS School of Computing*, Academic Year 2021/2022.
3. **Faculty Teaching Excellence Honour Roll**, *NUS School of Computing*, Academic Year 2014/2015.
4. **Annual Teaching Excellence Award**, *National University of Singapore*, Academic Year 2013/2014.
5. **Faculty Teaching Excellence Award**, *NUS School of Computing*, Academic Year 2013/2014.
6. **Annual Teaching Excellence Award**, *National University of Singapore*, Academic Year 2012/2013.
7. **Faculty Teaching Excellence Award**, *NUS School of Computing*, Academic Year 2012/2013.

PROFESSIONAL SERVICES

- Steering Committee Member, *ACM Computer and Communications Security (CCS)*, 2025 – Present.
- Track (sub-conference) Chair, *Software Security Track, the 29th ACM Con- ference on Computer and Communications Security (CCS)*, 2022.
- Steering Group Member, *Network and Distributed System Security Symposium (NDSS)*, 2019 – 2024.
- Program Co-Chair, *the 14th ACM ASIA Conference on Computer and Communications Security (AsiaCCS)*, 2019.
- Associate Editor, *IEEE Transactions on Dependable and Secure Computing (TDSC)*, June 2014 - October 2018.
- Member of Editorial Board, *International Journal of Security and Networks*, July 2012 - February 2015.
- Program Co-Chair, *the 4th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2014.
- Student Travel Grant Co-Chair, *ACM Conference on Computer and Communications Security (CCS)*, 2012.
- Selected Technical Program Committee Member
  - *Network and Distributed System Security Symposium (NDSS)*, 2013 - 2021.
  - *ACM Conference on Computer and Communications Security (CCS)*, 2014 - 2016, 2018 - 2019, 2022, 2024.
  - *USENIX Security Symposium*, 2014, 2017.
  - *International World Wide Web Conference (WWW)*, 2011, 2014, 2015, 2019, 2021.
  - *ACM Symposium on Information, Computer and Communications Security (AsiaCCS)*, 2013, 2014, 2015, 2017, 2019, 2025.