Dr. LIANG Zhenkai

NUS School of Computing
13 Computing Drive
Computing 1, #03-27
Singapore, 117417

Email: liangzk@comp.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, *2006*,
Department of Computer Science, Stony Brook University, USA.

M.S. in Computer Science, *2004*,
Department of Computer Science, Stony Brook University, USA.

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

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

PROFESSIONAL EXPERIENCE

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

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

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

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

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

RESEARCH INTERESTS

Computer system security, browser and web security, operating systems, program analysis, software debugging and testing.

PUBLICATIONS

Book Chapters

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.

Journals

1. *"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)*, accepted in May 2013.

2. *"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.
3. *"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.

Peer-refereed Conferences

1. *"A Quantitative Evaluation of Privilege Separation in Web Browser Designs."* Xinshu Dong, Hong Hu, Prateek Saxena, and Zhenkai Liang. In *Proceedings of the 18th European Symposium on Research in Computer Security (ESORICS)*, September 2013. (Acceptance rate: 17.8%)
2. *"A Comprehensive Client-side Behavior Model for Diagnosing Attacks in Ajax Applications."* Xinshu Dong, Kailas Patil, Jian Mao, and Zhenkai Liang. In *Proceedings of the 18th International Conference on Engineering of Complex Computer Systems (ICECCS)*, July 2013. (Acceptance rate: 26.3%)
3. *"Enforcing System-Wide Control Flow Integrity for Exploit Detection and Diagnosis."* Aravind Prakash, Heng Yin, and Zhenkai Liang. In *Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, May 2013. (Acceptance rate: 28.7%)
4. *"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 *Proceedings of the 15th Information Security Conference (ISC)*, September 2012. (Acceptance rate: 31.9%)
5. *"Codejail: Application-transparent Isolation of Libraries with Tight Program Interactions."* Yongzheng Wu, Sai Sathyanarayan, Roland Yap, and Zhenkai Liang. In *Proceedings of the 17th European Symposium on Research in Computer Security (ESORICS)*, September 2012. (Acceptance rate: 20.2%)
6. *"Tracking the Trackers: Fast and Scalable Dynamic Analysis of Web Content for Privacy Violations."* Minh Tran, Xinshu Dong, Zhenkai Liang, and Xuxian Jiang. In *Proceedings of the 10th International Conference on Applied Cryptography and Network Security (ACNS)*, June 2012. (Acceptance rate: 17.2%)
7. *"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 *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, May 2012. (Acceptance rate: 13.0%)
8. *"Identifying and Analyzing Pointer Misuses for Sophisticated Memory-corruption Exploit Diagnosis."* Mingwei Zhang, Aravind Prakash, Xiaolei Li, Zhenkai Liang, and Heng Yin. In *Proceedings of the 19th Annual Network & Distributed System Security Symposium (NDSS)*, February 2012. (Acceptance rate: 17.8%)

9. *"AdSentry: Comprehensive and Flexible Confinement of JavaScript-based Advertisements."* Xinshu Dong, Minh Tran, Zhenkai Liang, and Xuxian Jiang. To appear in *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC)*, December 2011. (Acceptance rate: 20%)
10. *"Towards Fine-Grained Access Control in JavaScript Contexts."* Kailas Patil, Xinshu Dong, Xiaolei Li, Zhenkai Liang, and Xuxian Jiang. In *Proceedings of the 31st IEEE International Conference on Distributed Computing Systems (ICDCS)*, June 2011. (Acceptance rate: 15.4%)
11. *"Jump-Oriented Programming: A New Class of Code-Reuse Attack."* Tyler Bletsch, Xuxian Jiang, Vince Freeh, and Zhenkai Liang. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, March 2011. (Acceptance rate: 16.1%)
12. *"Heap Taichi: Exploiting Memory Allocation Granularity In Heap-spraying Attacks."* Yu Ding, Tao Wei, Tielei Wang, Zhenkai Liang, and Wei Zou. In *Proceedings of the 25st Annual Computer Security Applications Conference (ACSAC)*, December 2010. (Acceptance rate: 16.3%)
13. *"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%)
14. *"Test Generation to Expose Changes in Evolving Programs."* Dawei Qi, Abhik Roychoudhury, and Zhenkai Liang. In *Proceedings of the 25th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, September 2010. (Acceptance rate: 18%)
15. *"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 *Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm)*, September 2010. (Acceptance rate: 25%)
16. *"Towards Generating High Coverage Vulnerability-Based Signatures with Protocol-Level Constraint-Guided Exploration."* Juan Caballero, Zhenkai Liang, Pongsin Poosankam, and Dawn Song. In *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID)*, September 2009. (Acceptance rate: 28.3%)
17. *"DARWIN: An Approach for Debugging Evolving Programs."* Dawei Qi, Abhik Roychoudhury, Zhenkai Liang, and Kapil Vaswani. In *Proceedings of 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.**
18. *"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 *Proceedings of the 4th International Conference on Information Systems Security (ICISS)*, December 2008. (Acceptance rate: 18%)

19. *"Expanding Malware Defense by Securing Software Installations."* Weiqing Sun, R. Sekar, Zhenkai Liang, and V.N. Venkatakrishnan. In *Proceedings of the 5th Conference on Detection of Intrusions, Malware and Vulnerability Analysis (DIMVA)*, July 2008. (Acceptance rate: 31%)
20. *"AGIS: Automatic Generation of Infection Signatures."* Zhuowei Li, Xiaofeng Wang, Zhenkai Liang, and Michael K. Reiter. In *Proceedings of the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 2008. (Acceptance Rate: 25%)
21. *"HookFinder: Identifying and Understanding Malware Hooking Behaviors."* Heng Yin, Zhenkai Liang, and Dawn Song. In *Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS)*, February 2008. (Acceptance rate: 17.8%)
22. *"Polyglot: Automatic Extraction of Protocol Message Format using Dynamic Binary Analysis."* Juan Caballero, Heng Yin, Zhenkai Liang, and Dawn Song. In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS)*, October 2007. (Acceptance rate: 18%)
23. *"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 (*authors listed in alphabetical order*). In *Proceedings of the 16th USENIX Security Symposium*, August 2007. (Acceptance rate: 12.3%)

    - **Conference Best Paper Award.**
24. Zhenkai Liang and R. Sekar. "Automatic Generation of Buffer Overflow Attack Signatures: An Approach Based on Program Behavior Models." In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC)*, December 2005. (Acceptance rate: 19.6%)
25. *"Fast and Automated Generation of Attack Signatures: A Basis for Building Self-Protecting Servers."* Zhenkai Liang and R. Sekar. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance rate: 15.2%)
26. *"One-way Isolation: An Effective Approach for Realizing Safe Execution Environments."* Weiqing Sun, Zhenkai Liang, R. Sekar, and V.N. Venkatakrishnan. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS)*, February 2005. (Acceptance rate: 13%)
27. *"Isolated Program Execution: An Application Transparent Approach for Executing Untrusted Programs."* Zhenkai Liang, V.N. Venkatakrishnan, and R. Sekar. In *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC)*, December 2003. (Acceptance rate: 30%)

    - **Conference Outstanding Paper Award.**
28. *"An Approach for Secure Software Installation."* V.N. Venkatakrishnan, R. Sekar, S. Tsipa, T. Kamat, and Z. Liang. In *Proceedings of the 16th Large Installation System Administration Conference (LISA)*, November 2002.

Others

1. *"BaitAlarm: Detecting Phishing Sites Using Similarity in Fundamental Visual Features."* Jian Mao, Kun Li, Pei Li, Tao Wei, and Zhenkai Liang. In *Proceedings of the International Workshop on Secure Cloud Computing*, September 2013.
2. *"UserCSP: User Specified Content Security Policies." (Poster)* Kailas Patil, Tanvi Vyas, Frederik Braun, and Zhenkai Liang. In *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS)*, July 2013.
3. *"A Software Environment for Confining Malicious Android Applications via Resource Virtualization." (Short paper)* Xiaolei Li, Guangdong Bai, Zhenkai Liang, and Heng Yin. IN *Proceedings of the 18th International Conference on Engineering of Complex Computer Systems (ICECCS)*, July 2013.
4. *"ClickGuard: Preventing Click Event Hijacking in Broswers."* Kailas Patil, Xinshu Dong, and Zhenkai Liang. In *Proceedings of the 8th International Conference on Applied Cryptography and Network Security, Industry Track*, June 2010.
5. *"Automatic Synthesis of Filters to Discard Buffer Overflow Attacks: A Step Towards Realizing Self-Healing Systems." (Short paper)* Zhenkai Liang, R. Sekar, and Daniel C. DuVarney. In *Proceedings of the USENIX Annual Technical Conference*, April 2005.
6. *"Immunizing Servers from Buffer Overflow Attacks." (Extended Abstract)* Zhenkai Liang, R. Sekar, and Daniel C. DuVarney. In *Adaptive and Resilient Computing Security Workshop*, November 2004.

Technical Reports

1. *"An Entensible Security Framework in Web Broswers."* Xinshu dong, Kailas Patil, Xuhui Liu, Jian Mao, and Zhenkai Liang. TR-2012-001, Systems Security Group, School of Computing, National University of Singapore, Feburary 2012.
2. *"Towards Practical Automatic Generation of Multipath Vulnerability Signatures."* David Brumley, Zhenkai Liang, James Newsome, and Dawn Song. CMU-CS-07-150, School of Computer Science, Carnegie Mellon University, April 2007.
3. *"BitScope: Automatically Dissecting Malicious Binaries."* David Brumley, Cody Hartwig, Min Gyung Kang, Zhenkai Liang, James Newsome, Pongsin Poosankam, Dawn Song, and Heng Yin. CS-07-133, School of Computer Science, Carnegie Mellon University, March 2007.

RESEARCH GRANTS

- (PI) "Establishing Trusted Web Sessions on Untrusted User Devices." MOE AcRF Tier-2, S$383,452, April 2013 – March 2016.
- (PI) "Securing the Android Mobile Platform against Browser-based Attacks." NUS FRC, S$152,000, August 2011 – August 2014.
- (co-PI) "Analyzing the Security of Software in Binary Form." DRTech, S$371,000, April 2010 – April 2014.
- (PI) "A Framework for General Security Support in Web Browsers." NUS Young Investigator Award, S$477,050, February 2009 – August 2012.

- (co-PI) "Symbolic Taint Analysis." DRTech DIRP, S$397,290, January 2009 – July 2012.
- (PI) "Improving Security Incident Response by Automatic Vulnerability Diagnosis." NUS FRC, S$167,880, October 2008 – September 2011.

Selected Honors and Awards

- ACM SIGSOFT Distinguished Paper Award, 2009.
- NUS Young Investigator Award, National University of Singapore, 2009.
- Best Paper Award, *16th USENIX Security Symposium*, 2007.
- Outstanding Paper Award, *19th Annual Computer Security Applications Conference (ACSAC)*, 2003.

Selected Professional Services

- Member of Editorial Board, International Journal of Security and Networks.
- Student Travel Grant Co-Chair, ACM Conference on Computer and Communications Security (CCS), 2012.
- Program Committee Member
  - The Network and Distributed System Security Symposium (NDSS), 2013, 2014.
  - The International World Wide Web Conference (WWW), 2011.
  - The ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2013.
  - The International Conference on Applied Cryptography and Network Security (ACNS), 2012.
  - The International Conference on Information Privacy, Security, Risk and Trust (PASSAT), 2011, 2012.
  - The International Conference on Information Systems Security (ICISS), 2008, 2009, 2010, 2012.
  - The Information Security Conference (ISC), 2011, 2012.
  - The European Workshop on Systems Security (EuroSec), 2009, 2010, 2011.