

## Qiang Zeng, Assistant Professor

Department of Computer Science and Engineering  
University of South Carolina  
Columbia, SC 29208

zeng1@cse.sc.edu  
<https://cse.sc.edu/~zeng1/>  
Phone: (803) 576-6821

### RESEARCH INTERESTS

My main research interest is Computer Systems Security, with a focus on Cyber-Physical Systems, Internet of Things, and Mobile Computing. I am also interested in Adversarial Machine Learning.

### EDUCATION

Ph.D., Computer Science & Engineering, Penn State University	2009 – 2014
M.E., Computer Science & Engineering, Beihang University	2005 – 2008
B.E., Computer Science & Engineering, Beihang University	2001 – 2005

### RESEARCH EXPERIENCE

<b>University of South Carolina</b> , Assistant Professor Conduct research and teaching in the CSE department.	2018 –
<b>Temple University</b> , Assistant Professor Conducted research and teaching in the CIS department.	2015 – 2018
<b>Cyber Security Lab, Penn State University</b> , Research Assistant Finished multiple research projects on security. Published in PLDI'11, NDSS'12, and DSN'15.	2009 – 2014
<b>NEC Laboratories America</b> , Research Intern Improved the technique below in order to work with dynamic class loading. Published in CGO'14.	01/2013 – 04/2013
<b>NEC Laboratories America</b> , Research Intern Built the first scalable calling context encoding technique. One patent was awarded.	05/2012 – 08/2012
<b>IBM Thomas J. Watson Research Center</b> , Research Intern Invented the first safe query executor for multi-party distributed databases. Published in TKDE.	05/2011 – 08/2011

### GRANTS

TOTAL: \$3.1 MILLION, MY SHARE: \$1.5 MILLION

- **NSF**, “*CAREER: Towards Secure and Usable IoT Authentication Under Constraints.*” **Single PI**, total: \$546,667. 2022-2027.
- **NSF**, “*Collaborative Research: CNS Core: Medium: Towards Understanding and Handling Problems Due to Coexistence of Multiple IoT Platforms.*” **PI (lead)**, total: \$600,000, my share: \$300,000. 2021-2024.
- **NSF**, “*CCRI: Medium: Collaborative Research: Hardware-in-the-Loop and Remotely-Accessible/Configurable/Programmable Internet of Things (IoT) Testbeds.*” **PI**, total: \$1.5M, my share: \$450,000. 2020-2023.
- **NSF**, “*SaTC: CORE: Small: Collaborative: Enabling Precise and Automated Insecurity Analysis of Middleware on Mobile Platforms.*” **PI (lead)**, total: \$492K, my share: \$166,666. 2018-2021.
- University of South Carolina, “*Towards Remote Program Analysis of Internet-of-Things (IoT) Applications.*” **Single PI**, \$14,880. 2021–2022.

## PUBLICATIONS

### REFEREED JOURNAL PAPERS

- [1] Donghai Tian, **Qiang Zeng**, Dinghao Wu, Peng Liu, and Changzhen Hu. “Semi-synchronized Non-blocking Concurrent Kernel Cruising.” *Transactions on Cloud Computing (TCC)*, 2020.
- [2] **Qiang Zeng**, Lannan Luo, Zhiyun Qian, Xiaojiang Du, Zhoujun Li, Chin-Tser Huang, and Csilla Farkas. “Resilient User-Side Android Application Repackaging and Tampering Detection Using Cryptographically Obfuscated Logic Bombs.” *Transactions on Dependable and Secure Computing (TDSC)*, 2019.
- [3] Lannan Luo, **Qiang Zeng**,\* Chen Cao, Kai Chen, Jian Liu, Limin Liu, Neng Gao, Min Yang, Xinyu Xing, and Peng Liu (\*Corresponding author). “Tainting-Assisted and Context-Migrated Symbolic Execution of Android Framework for Vulnerability Discovery and Exploit Generation.” *IEEE Transactions on Mobile Computing (TMC)*, 2019.
- [4] Rixin Xu, **Qiang Zeng**,\* Liehuang Zhu, Haotian Chi, X. Du, and M. Guizani (\*Corresponding author). “Privacy Leakage in Smart Homes and Its Mitigation: IFTTT as a Case Study.” *IEEE ACCESS*, 2019.
- [5] **Qiang Zeng**, Mingyi Zhao, Peng Liu, Poonam Yadav, Seraphin Calo, and Jorge Lobo. “Enforcement of Autonomous Authorizations in Collaborative Distributed Query Evaluation.” *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 2014.

### REFEREED CONFERENCE PAPERS

- [6] Haotian Chi, Chenglong Fu, **Qiang Zeng**, and Xiaojiang Du. “[Title Hidden Due to Embargo].” In *Proceedings of the 43rd IEEE Symposium on Security and Privacy (Oakland)*, 2022. [Acceptance rate: 54/357=**15.1%**]
- [7] Lannan Luo, **Qiang Zeng**, Bokai Yang, Fei Zuo, Junzhe Wang. “Westworld: Fuzzing-Assisted Remote Dynamic Symbolic Execution of Smart Apps on IoT Cloud Platforms.” In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2021. [Acceptance rate = 24%]
- [8] Haotian Chi, **Qiang Zeng**, Xiaojiang Du, and Lannan Luo. “PFirewall: Semantics-Aware Customizable Data Flow Control for Smart Home Privacy Protection.” In *Proceedings of the 28th Annual Network and Distributed System Security Symposium (NDSS)*, 2021. [Acceptance rate: 87/573=**15.2%**]
- [9] Chenglong Fu, **Qiang Zeng**, and Xiaojiang Du. “HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes.” In *Proceedings of the 30th USENIX Security Symposium (USENIX Security)*, 2021. [Acceptance rate: 248/1319=**18.8%**]
- [10] Fei Zuo and **Qiang Zeng**. “Exploiting the Sensitivity of  $L_2$  Adversarial Examples to Erase-and-Restore.” In *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, 2021. [Acceptance rate: 29/157 = **18.5%** in Round One]
- [11] Xuanyu Liu, **Qiang Zeng**, Xiaojiang Du, Siva Likitha Valluru, Chenglong Fu, Xiao Fu, and Bin Luo. “SniffMislead: Non-Intrusive Privacy Protection Against Wireless Packet Sniffers in Smart Homes.” In *Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2021. [Acceptance rate: 37/166=**22.3%**]
- [12] Xiaopeng Li, **Qiang Zeng**,\* Lannan Luo, and Tongbo Luo (\*Corresponding author). “T2Pair: Secure and Usable Pairing for Heterogeneous IoT Devices.” In *Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS)*, 2020. [Acceptance rate: 121/715=**16.9%**]
- [13] Haotian Chi, **Qiang Zeng**, Xiaojiang Du, and Jiaping Yu. “Cross-App Interference Threats in Smart Homes: Categorization, Detection and Handling.” In *Proceedings of the 50th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2020. [Acceptance rate: 48/291=**16.5%**]

- [14] Xuening Xu, Xiaojiang Du, and **Qiang Zeng**. “Attacking Graph-Based Classification without Changing Existing Connections.” In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2020 [Acceptance rate: 70/302=**23.2%**]
- [15] Yipeng Zhang, Zhonghao Sun, Liqun Yang, Zhoujun Li, **Qiang Zeng**, Yueying He, and Xiaoming Zhang. “All Your PLCs Belong to Me: ICS Ransomware Is Realistic.” In *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020.
- [16] Xiaopeng Li, Fengyao Yan, Fei Zuo, **Qiang Zeng**, and Lannan Luo. “Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices.” In *Proceedings of the 25th Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2019. [Acceptance rate: 30/186 = **16.1%**; Winter Round]
- [17] Fei Zuo, Bokai Yang, Xiaopeng Li, Lannan Luo, and **Qiang Zeng**. “Exploiting the Inherent Limitation of  $L_0$  Adversarial Examples.” In *Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2019. [Acceptance rate: 37/166 = **22.3%**]
- [18] **Qiang Zeng**, Jianhai Su, Chenglong Fu, Golam Kayas, Lannan Luo, Xiaojiang Du, Chiu C. Tan, and Jie Wu. “A Multiversion Programming Inspired Approach to Detecting Audio Adversarial Examples.” In *Proceedings of the 49th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2019. [Acceptance rate: 54/252 = **21.4%**]
- [19] **Qiang Zeng**, Golam Kayas, Emil Mohammed, Lannan Luo, Xiaojiang Du, and Junghwan Rhee. “HeapTherapy+: Efficient Handling of (Almost) All Heap Vulnerabilities Using Targeted Calling-Context Encoding.” In *Proceedings of the 49th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2019. [Acceptance rate: 54/252 = **21.4%**]
- [20] Fei Zuo, Xiaopeng Li, Patrick Young, Lannan Luo, **Qiang Zeng**, and Zhexin Zhe. “Neural Machine Translation Inspired Binary Code Similarity Comparison beyond Function Pairs.” In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, 2019. [Acceptance rate = 89/521 = **17.1%**]
- [21] **Qiang Zeng**, Lannan Luo, Zhiyun Qian, Xiaojiang Du, and Zhoujun Li. “Resilient Decentralized Android Application Repackaging Detection.” In *Proceedings of IEEE/ACM International Symposium on Code Generation and Optimization (CGO)*, 2018. [Acceptance rate: 30/105 = 28.6%]
- [22] Haotian Chi, Longfei Wu, Xiaojiang Du, **Qiang Zeng**, and Paul Ratazzi. “e-SAFE: secure, efficient and forensics-enabled access to implantable medical devices.” In *IEEE Conference on Communications and Network Security (CNS)*, 2018. [Acceptance rate: 51/181 = 28.2%]
- [23] Rixin Xu, **Qiang Zeng**, Liehuang Zhu, Haotian Chi, Xiaojiang Du, and Mohsen Guizani. “Privacy Leakage in Smart Homes and Its Mitigation: IFTTT as a Case Study.” In *IEEE 37th International Performance Computing and Communications Conference (IPCCC)*, 2018. [Acceptance rate: 60/228=26.3%]
- [24] Lannan Luo, \* **Qiang Zeng**,\* Chen Cao, Kai Chen, Jian Liu, Limin Liu, Neng Gao, Min Yang, Xinyu Xing, and Peng Liu (\* co-first authors). “System Service Call-oriented Symbolic Execution of Android Framework with Applications to Vulnerability Discovery and Exploit Generation.” In *Proceedings of the 15th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2017. [Acceptance rate: 34/188 = **17.8%**]
- [25] Mingyue Liang, Zhoujun Li, **Qiang Zeng**, and Zhejun Fang. “Deobfuscation of Virtualization-obfuscated Code through Symbolic Execution and Compilation Optimization.” In *19th International Conference on Information and Communications Security (ICICS)*, 2017.
- [26] Lannan Luo and **Qiang Zeng**. “SolMiner: Mining Distinct Solutions in Programs.” In *the 38th International Conference on Software Engineering, SEET track (ICSE-SEET)*, 2016.
- [27] **Qiang Zeng**,\* Mingyi Zhao,\* and Peng Liu (\* co-first authors). “HeapTherapy: An Efficient End-to-end Solution Against Heap Buffer Overflows.” In *Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2015. [Acceptance rate: 50/229 = **21.8%**]

- [28] Jun Wang, Mingyi Zhao, **Qiang Zeng**, Dinghao Wu, and Peng Liu. “Risk Assessment of Buffer ‘Heartbleed’ Over-read Vulnerabilities.” (Practical Experience Report). In *Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2015. [Acceptance rate:  $50/229 = 21.8\%$ ]
- [29] **Qiang Zeng**, Junghwan Rhee, Hui Zhang, Nipun Arora, Guofei Jiang, and Peng Liu. “DeltaPath: Precise and Scalable Calling Context Encoding.” In *Proceedings of the International Symposium on Code Generation and Optimization (CGO)*, 2014. [Acceptance rate:  $29/100 = 29.0\%$ ]
- [30] **Qiang Zeng**, Jorge Lobo, Peng Liu, Seraphin Calo, and Poonam Yadav. “Safe Query Processing for Pairwise Authorizations in Coalition Networks.” In *Annual Conference of International Technology Alliance*, 2012.
- [31] Donghai Tian, **Qiang Zeng**, Dinghao Wu, Peng Liu, and Changzhen Hu. “Kruiser: Semi-synchronized Non-blocking Concurrent Kernel Heap Buffer Overflow Monitoring.” In *Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS)*, 2012. [Acceptance rate:  $46/258 = 17.8\%$ ]
- [32] **Qiang Zeng**, Dinghao Wu, and Peng Liu. “Cruiser: Concurrent Heap Buffer Overflow Monitoring Using Lock-free Data Structures.” In *Proceedings of the 32nd ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI)*, 2011. [Acceptance rate:  $55/236 = 23.3\%$ ]

#### REFEREED WORKSHOP PAPERS

- [33] Kimberly Redmond, Lannan Luo, and **Qiang Zeng**. “A Cross-Architecture Instruction Embedding Model for Natural Language Processing-Inspired Binary Code Analysis.” In *NDSS Workshop on Binary Analysis Research (BAR)*, 2019.
- [34] **Qiang Zeng**, Jianhai Su, Chenglong Fu, Golam Kayas, and Lannan Luo. “A Multiversion Programming Inspired Approach to Detecting Audio Adversarial Examples.” In *AAAI Workshop on Artificial Intelligence for Cyber Security (AICS)*, 2019.

#### BOOK CHAPTERS

- [35] Dinghao Wu, Peng Liu, **Qiang Zeng**, and Donghai Tian. “Software Cruising: A New Technology for Building Concurrent Software Monitor.” *Book chapter*, in *Secure Cloud Computing, Advances in Information Security Series*, Sushil Jajodia, Krishna Kant, Pierangela Samarati, Anoop Singhal, Vipin Swarup, and Cliff Wang (eds.), pages 303–324. Springer, 2014.

#### TECHNICAL REPORTS

- [36] Ravshanbek Norboev, Zakia Hossain, **Qiang Zeng**, and Lannan Luo. “On the Robustness of Stochastic Stealthy Network against Android App Repackaging.” Technical Report, 2017.
- [37] **Qiang Zeng**, Zhi Xin, Dinghao Wu, Peng Liu, and Bing Mao. “Tailored Application-specific System Call Tables.” Technical Report. 2014.

#### POSTERS

- [38] **Qiang Zeng**, Mingyi Zhao, and Peng Liu. “Targeted Therapy for Program Bugs.” In *35th IEEE Symposium on Security and Privacy (Oakland), Poster Session*, 2014.
- [39] Mingyue Liang, Zhoujun Li, **Qiang Zeng**, and Zhejun Fang. “Deobfuscation of Virtualization-based Obfuscated Binary.” In *26th Usenix Security Symposium, Poster Session*, 2017.

#### INVENTIONS AND PATENTS

- [40] Junghwan Rhee, Hui Zhang, Nipun Arora, Geoff Jiang, and **Qiang Zeng**. “Guarding a Monitoring Scope and Interpreting Partial Control Flow Context.” Publication No.: US9471461 B2, awarded 2016.
- [41] **Qiang Zeng**, Baosong Shan, Hua Miao, and Wei Li. “A Distributed System for Large-scale Real-time Streaming Transmission.” Publication No.: CN-101123526-B, awarded 2010.

- [42] Hua Miao, Baosong Shan, **Qiang Zeng**, Xianglong Liu, and Wei Li, “A Sliding Window Based Method for Rapid FGS Bandwidth Allocation.” Publication No.: CN-100579226-B, awarded 2010.

### **SCHOLARLY SERVICE**

- TPC member for USENIX Security, 2022
- TPC member for NDSS, 2022
- TPC member for DSN, 2022
- TPC member for USENIX Security, 2021
- TPC member for NDSS, 2021
- TPC member for the 18th International Conference on Security and Crypto (SECRYPT), 2021
- TPC member for AsiaCCS, 2020
- TPC member for GLOBECOM, 2020
- TPC member for IEEE Wireless Communications and Networking Conference (WCNC), 2020
- TPC member for the 17th International Conference on Security and Crypto (SECRYPT), 2020
- TPC member for IEEE International Conference on Multimedia and Expo (ICME), 2020
- TPC member for the 16th International Conference on Security and Crypto (SECRYPT), 2019
- TPC member for IEEE International Conference on Multimedia and Expo (ICME), 2019
- TPC member for 16th IEEE International Conference on Mobile Ad hoc and Smart Systems (IEEE MASS), 2019
- TPC member for 15th IEEE International Conference on Mobile Ad hoc and Smart Systems (IEEE MASS), 2018
- TPC member for the IEEE Conference on Communications and Network Security (CNS), 2018
- TPC member for the 36th IEEE International Conference on Consumer Electronics (ICCE), 2018
- Reviewer for IEEE Transactions on Dependable and Secure Computing
- Reviewer for IEEE Transactions on Information Forensics and Security
- Reviewer for IEEE Transactions on Parallel and Distributed Systems
- Reviewer for Concurrency and Computation: Practice and Experience
- Reviewer for ACM Transactions on Internet Technology
- Reviewer for IEEE Networking Letters
- Reviewer for Empirical Software Engineering

### **DEPARTMENTAL & UNIVERSITY SERVICE**

- Graduate Committee in the CSE department at UofSC, 2018–Present
- Hosted the CIS@Temple University Weekly Tea Social Events, 2016–2018 academic years
- IS&T Undergraduate Committee, Temple University, 2016–2017 academic year
- Tenure-track Junior Faculty Search Committee, CIS@Temple University, 2015–2016 academic year
- CS Undergraduate Committee, Temple University, 2015–2016 academic year
- PSM Cyber Security Master Program Committee, Temple University, 2015–2016 academic year

## SOFTWARE & DATASET RELEASE

- Code, datasets, and models for ERASE-AND-RESTORE (AsiaCCS’21) are publicly available at <https://github.com/quz105/Erase-and-Restore>
- Code, datasets, and models for MVP-EARS (DSN’19) are publicly available at <https://github.com/quz105/MVP-audio-AE-detector>
- Code, datasets, and models for AEPECKER (RAID’19) are publicly available at <https://github.com/fzuo/AEPecker>
- Code, datasets, and models for INNEREYE (NDSS’19) are publicly available at <https://nmt4binaries.github.io>
- Code for CENTAUR (MobiSys’17) is publicly available at <https://github.com/Android-Framework-Symbolic-Executor/Centaur>.
- Code for CRUISER (PLDI’11) is publicly available at <http://cruiser-psu.googlecode.com>.

## TEACHING

Table 1: Complete list of anonymous student evaluation scores. (Temple university did not have *instructor scores*. I did not have teaching tasks in Spring 2016 and Fall 2020. The data in Fall 2018 was mishandled by the university and is thus not included.)

Semester	Course	Course (Depart. Avg.)	Instructor (Depart. Avg.)
Teaching at Temple University			
Fall 2015	CIS5512: Operating Systems	4.3 (4.0)	N/A
Fall 2016	CIS5512: Operating Systems	4.2 (4.0)	N/A
Spring 2017	CIS4360: Secure Computer Systems	4.5 (4.0)	N/A
Fall 2017	CIS5512: Operating Systems	4.0 (4.0)	N/A
Spring 2018	CIS3207: Operating Systems	4.6 (4.0)	N/A
Teaching at University of South Carolina			
Spring 2019	CSCE790: Computer Systems Security	4.78 (4.12)	4.89 (4.32)
Fall 2019	CSCE311: Operating Systems	4.00 (4.19)	4.32 (4.42)
Spring 2020	CSCE791: Seminar	4.37 (4.04)	4.53 (4.20)
Spring 2020	CSCE790: Computer Systems Security	4.90 (4.04)	5.00 (4.20)
Spring 2021	CSCE311: Operating Systems	4.44 (4.14)	4.50 (4.34)

## MENTORSHIP/STUDENT SUPERVISION

- Undergraduate Research Assistants (incomplete list)
  - Patrick Young, May 2017–May 2018 (we co-authored a paper published in NDSS’19)
  - Emil Mohammed, May 2017–May 2018 (we co-authored a paper published in DSN’19)
  - Ravshanbek Norboev, May 2017–July 2017 (REU summer program)
  - Zakia Hossain, May 2017–August 2017 (2017 Frances Velay Fellowship)
- PhD Students
  - Fei Zuo, 2017–2021 (passed the dissertation defense in August 2021)
  - Chuxiong Wu, 2019–Present
  - Junzhe Wang (co-advised), 2020–Present
  - Likitha Valluru, 2020–Present
  - Jonathan Sharp, 2020–Present
  - Ying Meng, 2021–Present