Zecheng He

+1 (609) 933-1447 • zechengh@princeton.edu • www.princeton.edu/∼zechengh
Princeton University, Princeton, NJ, 08540, USA

Education

Princeton University 2015.9-2021.9
Ph.D., Electrical and Computer Engineering
Advisor: Prof. Ruby B. Lee
Dissertation Topic: Security Meets Deep Learning
Research Area: Multi-modal ML, AI Security, Privacy

Princeton University 2015.9-2017.9
M.A., Electrical and Computer Engineering
GPA: 3.92/4.00

University of Science and Technology of China (USTC) 2011.9-2015.6
B.E., Electronic Information Engineering
GPA: 4.00/4.3, rank 1/281

Work Experience

Research Scientist, Facebook 2021.9-present

Research Intern, Google 2020.5-2020.8
Deep Dialogue Team
Multi-modal Embedding for Semantic UI Understanding

Software Engineer Intern, Facebook 2019.5-2019.8
Business Integrity Core ML
Policy-violation Ads Detection with Weighted Model Training

Research Intern, SRI International 2017.6-2017.9
Center for Vision Technologies
Sequential Anomaly Detection in Controller Systems

Selected Research Experience

Multi-modal UI Understanding through User Actions [AAAI'21]
Advisor: Prof.Ruby Lee, Dr.Jindong Chen (Google Research)

- Proposed the first multi-modal pre-trained feature representation for semantic UI understanding.
- Implemented and migrated the model training process to TPUs and achieved 8x speed-up.
- Evaluated the model on five types of downstream tasks, and achieved up to 15.5% increase in accuracy.
- Compared to other embedding approaches and showed the supreme of our approach.

Sensitive-Sample Fingerprinting for Deep Neural Networks [CVPR'19]
Advisor: Prof.Ruby Lee, Prof.Tianwei Zhang (Nanyang Technological University)

- Developed sensitive-sample fingerprinting, a low-cost approach for cloud customers to self-served verify the integrity of the black-box DNN models in the cloud.
- Performed an evaluation of the proposed defense mechanism against four types of DNN integrity attacks in five application domains.
- Evaluated and compared to other fingerprinting approaches to show the supreme of our approach.
- Achieved high detection accuracy (>99%) with low-cost (<5 black-box accesses).

Modeling and Evaluating Microarchitectural Attacks [HPCA'21, MICRO'17]
Advisor: Prof.Ruby Lee

- Developed graph models to understand and reason about the speculative executions attacks, e.g., Spectre, Meltdown and Foreshadow. The proposed model covers all existing speculative execution attacks and defenses.

- Investigated the novel probabilistic information flow graph (PIFG) model for cache side-channel attacks.
- Demonstrated new defense stretagies against the speculative execution attacks from the model.
- Evaluated secure caches' resilience against side-channel attacks through PIFGs.

Model Inversion Attacks against Collaborative Inference Systems **[ACSAC'19, IoTJ'20]**
Advisor: Prof.Ruby Lee, Prof.Tianwei Zhang (Nanyang Technological University)

- Presented the first line of privacy attacks against users' sensitive data in edge-cloud collaborative inference systems.
- Demonstrated three types of attacks (whitebox, blackbox and query-free) to reverse users' inference data.
- Tested the proposed attacks and designed defenses against them.
- Implemented the defenses and revealed the security-usability tradeoff in collaborative inference systems.

Sequential Anomaly Detection with Enhanced Deep Learning **[TrustCom'19]**
Advisor: Prof.Ruby Lee, Dr.Sek Chai (SRI International)

- Developed a new system for industrial controllers anomaly detection, based on deep sequential models and hardware performance counters (HPCs).
- Demonstrated statistical tests to enhance the performance of sequential learning models for anomaly detection.
- Achieved fast (<250ms) and accurate (>99%) detection with an FPGA accelerator.
- Extended the sequential anomaly detection approach to a broader scope of systems, e.g., smartphone impostor detection and cloud side-channel detection.

Publications

Peer-reviewed Publications

1. **Zecheng He**, Srinivas Sunkara, Xiaoxue Zang, Ying Xu, Lijuan Liu, Nevan Wichers, Gabriel Schubiner, Ruby Lee, and Jindong Chen, "ActionBert: Leveraging User Actions for Semantic Understanding of User Interfaces", AAAI Conference on Artificial Intelligence (AAAI), 2021
2. **Zecheng He**, Guangyuan Hu, and Ruby Lee, "New Models for Understanding and Reasoning About Speculative Execution Attacks", IEEE International Symposium on High-Performance Computer Architecture (HPCA), 2021
3. Guangyuan Hu, **Zecheng He**, and Ruby Lee, "Smartphone Impostor Detection with Behavioral Data Privacy and Minimalist Hardware Support", TinyML Symposium, 2021, **Best Paper Award**
4. Qingsong Yao, **Zecheng He**, Yi Lin, Kai Ma, Yefeng Zheng, and S. Kevin Zhou, "A Hierarchical Feature Constraint to Camouflage Medical Adversarial Attacks", International Conference on Medical Image Computing and Computer-Assisted Intervention (MICCAI), 2021
5. Guangyuan Hu, **Zecheng He**, and Ruby Lee, "SoK: Hardware Defenses Against Speculative Execution Attacks", IEEE International Symposium on Secure and Private Execution Environment Design (SEED), 2021
6. **Zecheng He**, Tianwei Zhang, and Ruby Lee, "Attacking and Protecting Data Privacy in Edge-Cloud Collaborative Inference Systems", IEEE Internet of Things Journal (IEEE IoTJ), 2020
7. Qingsong Yao, **Zecheng He**, Hu Han, and S. Kevin Zhou, "Miss the Point: Targeted Adversarial Attack on Multiple Landmark Detection", International Conference on Medical Image Computing and Computer-Assisted Intervention (MICCAI), 2020
8. **Zecheng He**, Tianwei Zhang, and Ruby Lee, "Sensitive-Sample Fingerprinting of Deep Neural Networks", IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2019
9. **Zecheng He**, Tianwei Zhang, and Ruby Lee, "Model Inversion Attack against Collaborative Inference", Annual Computer Security Applications Conference (ACSAC), 2019

10. **Zecheng He**, Aswin Raghavan, Guangyuan Hu, Sek Chai, and Ruby Lee, "Power-Grid Controller Anomaly Detection with Enhanced Temporal Deep Learning", IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2019
11. **Zecheng He**, and Ruby Lee, "How Secure is Your Cache against Side-channel Attacks?", IEEE/ACM International Symposium on Microarchitecture (MICRO), 2017
12. **Zecheng He**, Ketan Tang, and Lu Fang, "Cross-scale Image Restoration under High Density Salt-and-pepper Noise", 24th IEEE International Conference on Image Processing (ICIP), 2017
13. **Zecheng He**, Tianwei Zhang, and Ruby Lee, "Machine Learning Based DDoS Attack Detection From Source Side in Cloud", IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 2017

In Submission

1. **Zecheng He**, and Ruby Lee, "CloudShield: Real-time Anomaly Detection in the Cloud", arXiv preprint arXiv:2108.08977

Techinical Report

1. Guangyuan Hu, **Zecheng He**, and Ruby Lee, "Smartphone Impostor Detection with Built-in Sensors and Deep Learning", arXiv:2002.03914, 2020
2. Tianwei Zhang, **Zecheng He**, and Ruby Lee, "Privacy-preserving Machine Learning through Data Obfuscation", arXiv preprint arXiv:1807.01860, 2018
3. **Zecheng He**, Tianwei Zhang, and Ruby Lee, "VerIDeep: Verifying Integrity of Deep Neural Networks through Sensitive-Sample Fingerprinting", arXiv preprint arXiv:1808.03277, 2018
4. **Zecheng He**, and Ruby Lee, "Cache Side Channel Attacks on Intel SGX", Princeton University Technical Report CE-L2017-001, 2017
5. **Zecheng He**, and Ruby Lee, "Security Verification of Resilience to Cache Side-channel Attacks", SRC Report, 2016

Patent

1. Sek Chai, **Zecheng He**, Aswin Raghavan, and Ruby Lee, "Anomalous Behavior Detection in Processor Based Systems", U.S. Patent Application No. 16/410,675
2. Srinivas Sunkara, Xiaoxue Zang, Ying Xu, Lijuan Liu, Nevan Wichers, Gabriel Schubiner, Jindong Chen, Abhinav Rastogi, Blaise Aguera-Arcas, and **Zecheng He** "Machine-Learned Models for User Interface Prediction, Generation, and Interaction Understanding", U.S. Patent Application No. 17/335,596

Selected Awards

Best Paper Award, TinyML Symposium	2021
Gordon Y.S. Wu Fellowship, Princeton University	2015-2020
1^{st} place, Siemens FutureMakers Challenge	2018
Outstanding Graduates, USTC	2015
Guo Moruo Scholarship (top 1%), USTC	2014
National Scholarship of China	2013

Invited Talks

"New models for understanding and reasoning about speculative execution attacks", University of Illinois at Urbana-Champaign (UIUC)	2021.8
"Security meets deep learning in the cloud", University of Nottingham	2021.4
"Security meets deep learning", Indiana University Purdue University Indianapolis	2021.4
"Security meets deep learning", University of Calgary	2021.3
"Security meets deep learning in the cloud", Google Research	2020.12

"Sensitive-Sample Fingerprinting of Deep Neural Networks", Princeton AI Seminar 2020.10
"Security meets deep learning", Futurewei Technologies 2020.9
"Security meets deep learning", Princeton AI Seminar 2019.4
"How secure is your cache against side-channel attacks?", SRC Techcon 2018.9
"Security in deep learning", Z^2AI 2018.8
"Deep learning based zero-day controller-hijacking attack detection in power-grid systems", Siemens FutureMakers Challenge 2018.8
"Security meets deep learning", SRI International 2017.6
"Modeling and Evaluating Cache Resilience Against Side-channel Attacks", Princeton Research Day 2017.5
"Security Verification of Resilience to Cache Side-Channel Attacks", SRC T3S 2016.9

Professional Services

Reviewer for IEEE Transactions on Instrumentation and Measurement (TIM) 2020, 2021
Reviewer for Journal of Information Security and Applications (JISA) 2019, 2020, 2021
Reviewer for IEEE Access 2019, 2020
Reviewer for IEEE Signal Processing Letters (SPL) 2019
Reviewer for Computers and Security 2018
PC member for Securware conference 2020, 2021
PC member for CYBER conference 2021
Session chair for session 4, CSCloud conference 2017

Teaching Experience

Architectures for Secure Computers and Smartphones (ELE472), Princeton University Fall'20
Introduction to Computing: Programming Autonomous Vehicles (ELE115), Princeton University Spring'20
Smartphone Security and Architecture (ELE470), Princeton University Fall'17
Signals and Systems, USTC Spring'15
The C Language Programing, USTC Fall'14

Programming Languages and Platforms

Python, C, Lua, Java, SQL, Matlab, X86/MIPS Assembly, Verilog, Tensorflow, Pytorch, Keras