Xinyang Ge

Microsoft Research
One Microsoft Way
Redmond, WA 98052

Phone: +1 (425) 707-2680
Email: xing@microsoft.com
Homepage: http://aka.ms/xing

Education

- **Ph.D., Computer Science and Engineering** 2012.08 – 2016.08
  The Pennsylvania State University, University Park
  Advisor: Dr. Trent Jaeger
- **B.Eng., Software Engineering** 2008.09 – 2012.06
  Nanjing University

Professional Experience

Senior Researcher, **Microsoft Research**, Redmond, WA 2016.09 – Present

- REPT: Developed a tool that enables reverse debugging for production failures reported back to Microsoft by combining efficient online hardware tracing with novel offline binary analysis.

Research Assisant, **The Pennsylvania State University**, University Park, PA 2012.08 – 2016.08

- GRIFFIN: Implemented a hardware-assisted control-flow integrity enforcement mechanism for unmodified program binaries using Intel Processor Trace.
- KCFI: Developed a system to retrofit operating system kernels for fine-grained control-flow integrity.
- SPROBES: Designed an ARM TrustZone-based system that enforces the kernel code integrity for commodity operating systems.

Research Intern, **Microsoft Research**, Redmond, WA 2015.05 – 2015.08

- Prototyped the support of Intel Processor Trace on Windows to enable tracing arbitrary applications.

Research Intern, **Microsoft Research**, Redmond, WA 2014.05 – 2014.08

- Prototyped a whitebox fuzzing service on Azure for finding security critical bugs in Windows applications (a.k.a., Microsoft Security Risk Detection).

Technical Intern, **eBay**, Shanghai, China 2011.08 – 2012.05

- Developed a search engine specialized for SQL queries for enabling database administrators to find and reuse high-quality queries from each other.

Undergraduate Assistant, **Nanjing University**, Nanjing, China 2011.02 – 2011.06

- fryy: Developed a tiny operating system running on commodity hardware for educational purpose.

Publications

1. Weidong Cui, **Xinyang Ge***, Baris Kasikci, Ben Niu, Upamanyu Sharma, Ruoyu Wang, and Insu Yun. REPT: Reverse Debugging of Failures in Deployed Software. In *Proceedings of the 13th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, October, 2018. **Jay Lepreau Best Paper Award**. (* authors listed in alphabetic order)

2. Le Guan, Peng Liu, Xinyu Xing, **Xinyang Ge**, Shengzhi Zhang, Meng Yu, and Trent Jaeger. Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2018.
3. Baris Kasikci, Weidong Cui, **Xinyang Ge**, and Ben Niu. Lazy Diagnosis of In-Production Concurrency Bugs. In *Proceedings of the 26th Symposium on Operating Systems Principles (SOSP)*, October, 2017.
4. Le Guan, Peng Liu, Xinyu Xing, **Xinyang Ge**, Shengzhi Zhang, Meng Yu, and Trent Jaeger. TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone. In *Proceedings of the 15th International Conference on Mobile Systems, Applications and Services (MobiSys)*, June, 2017.
5. **Xinyang Ge**, Weidong Cui, and Trent Jaeger. GRIFFIN: Guarding Control Flows Using Intel Processor Trace. In *Proceedings of the 22nd ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, April, 2017.
6. **Xinyang Ge**, Mathias Payer, and Trent Jaeger. An Evil Copy: How the Loader Betrays You. In *Proceedings of the 21st Network and Distributed System Security Symposium (NDSS)*, February, 2017.
7. Yuqiong Sun, Giuseppe Petracca, **Xinyang Ge**, and Trent Jaeger. Pileus: Protecting User Resources from Vulnerable Cloud Services. In *Proceedings of the 32nd Annual Computer Security Applications Conference (ACSAC)*, December, 2016.
8. **Xinyang Ge**, Nirupama Talele, Mathias Payer, and Trent Jaeger. Fine-Grained Control-Flow Integrity for Kernel Software. In *Proceedings of the 1st IEEE European Symposium on Security and Privacy (Euro S&P)*, March, 2016.
9. Hayawardh Vijayakumar, **Xinyang Ge**, Mathias Payer, and Trent Jaeger. JIGSAW: Protecting Resource Access by Inferring Programmer Expectations. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security)*, August, 2014.
10. Hayawardh Vijayakumar, **Xinyang Ge**, and Trent Jaeger. Policy Models to Protect Resource Retrieval. In *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies (SACMAT)*, June, 2014.
11. **Xinyang Ge**, Hayawardh Vijayakumar, and Trent Jaeger. SPROBES: Enforcing Kernel Code Integrity on the TrustZone Architecture. In *Proceedings of the 3rd IEEE Mobile Security Technologies Workshop (MoST)*, May, 2014.
12. **Xinyang Ge**, Jia Liu, Qi Qi, and Zhenyu Chen. A New Prediction Approach Based on Linear Regression for Collaborative Filtering. In *Proceedings of the 8th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, June, 2011.

Professional Services

- **PC Member**, ACM Conference on Computer and Communications Security (CCS), 2019.
- **PC Member**, ACM Conference on Computer and Communications Security (CCS), 2018.
- **PC Member**, IEEE Conference on Dependable and Secure Computing (DSC), 2018.
- **Reviewer**, IEEE Transaction on Dependable and Secure Computing (TDSC), 2018.
- **Reviewer**, ACM Transaction on Privacy and Security (TOPS), 2018.
- **PC Member**, ACM Conference on Computer and Communications Security (CCS), 2017.
- **PC Member**, IEEE Conference on Dependable and Secure Computing (DSC), 2017.