Xinyang Ge

Principal Researcher
Microsoft Research
Redmond, WA 98052

Phone: +1 (814) 880-8813
Email: aegiryy@gmail.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

Employment

- **Microsoft Research**, Redmond, WA
  - Principal Researcher 2020.09 – Present
  - Senior Researcher 2016.09 – 2020.08
- Research Assistant, **The Pennsylvania State University**, University Park, PA 2012.08 – 2016.08
- Research Intern, **Microsoft Research**, Redmond, WA 2015.05 – 2015.08
- Research Intern, **Microsoft Research**, Redmond, WA 2014.05 – 2014.08

Honors & Awards

- Jay Lepreau Best Paper Award, OSDI, 2018.

Major Projects

- Pagoda: Software piracy is a long-standing problem for the PC industry. Pagoda is a practical SGX-based anti-piracy solution for PC. It protects the plaintext of the application's code binary using Intel SGX without requiring developers to make any code change. Pagoda can smoothly run unmodified Windows games while hiding the executed machine instructions from a physical attacker.
- HyperFuzzer: Hypervisor security is crucial in the cloud era. HyperFuzzer is the first efficient hybrid fuzzer for the hypervisor. It mutates an entire VM against the hypervisor running on bare metal, and enables dynamic symbolic execution over only a control-flow trace recorded by Intel Processor Trace. HyperFuzzer can launch thousands of VMs per second and has found 12 critical bugs in Hyper-V (as of 5/14/2021), which saved tens of millions of dollars for Microsoft Azure.
- REPT: Crash dumps are hard to debug because it only captures a single moment when the crash happened. REPT is a reverse debugging system that allows developers to go back in time to better understand the conditions that lead up to the crash. REPT combines efficient hardware tracing with novel binary analysis to reconstruct the execution history from a crash dump. It is deployed on Windows 10 and awarded the best paper at OSDI'18 (demo).

Publications

1. Jiyong Yu, Xinyang Ge, Trent Jaeger, Chris Fletcher, and Weidong Cui. Pagoda: Towards Ending Software Piracy using Hardware Enclaves. In submission.

2. Xinyang Ge, Ben Niu, Robert Brotzman, Yaohui Chen, HyungSeok Han, Patrice Godefroid, and Weidong Cui. HyperFuzzer: An Efficient Hybrid Fuzzer for Virtual CPUs. In *Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS)*, November, 2021.

3. Xinyang Ge, Ben Niu, and Weidong Cui. Reverse Debugging of Kernel Failures in Deployed Systems. In *Proceedings of the 2020 USENIX Annual Technical Conference (ATC)*, July, 2020.

4. 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**.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

Patents

1. Xinyang Ge, Weidong Cui, Ben Niu, Tony Chen. "Protecting Commercial Off-the-Shelf Program Binaries From Piracy Using Hardware Enclaves". MS# 407929-US-NP.
2. Weidong Cui, Xinyang Ge, Baris Kasikci, Ben Niu, Ruoyu Wang, Insu Yun. "Reverse Debugging of Software Failures". US Patent Number 10,565,511.

Invited Talks

1. Hardware Tracing and Its Applications. Fudan University. February 14, 2019.

Students Advised

- Ph.D. Dissertation Committee
  - Ya Xiao, Virginia Tech, 2022 (expected).
- Microsoft Research Ph.D. Interns
  - Jiyong Yu (UIUC), Hsuan-Chi (Austin) Kuo (UIUC), 2020.
  - HyungSeok Han (KAIST), Robert Brotzman (PSU), Subarno Banerjee (UMich), 2019.
  - Bogdan Stoica (EPFL), Yaohui Chen (NEU), Hangchen Yu (UT Austin), 2018.
  - Ruoyu (Fish) Wang (UCSB), Insu Yun (GaTech), 2017.

Professional Services

- PC Member, The Network and Distributed System Security Symposium (NDSS), 2022.
- PC Member, The Network and Distributed System Security Symposium (NDSS), 2021.
- 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.
- PC Member, ACM Conference on Computer and Communications Security (CCS), 2017.
- PC Member, IEEE Conference on Dependable and Secure Computing (DSC), 2017.

Open-Source Contributions

- Bochs PC Emulator (https://bochs.sourceforge.io)
  - Add support for running Microsoft Hyper-V (r13783)
  - Fix an integer-overflow bug when restoring from a snapshot (r13786)
- WinAFL (https://github.com/googleprojectzero/winafl)
  - Enable fuzzing Hyper-V with custom mutations by adding new callbacks (commits)

Last updated: October 12, 2021