**Xinyang Ge**

|  |  |  |
| --- | --- | --- |
| The Pennsylvania State University | Phone: | (814) 880-8813 |
| Department of Computer Science and Engineering | Email: | aegiryy@gmail.com |
| 344 IST Building, University Park, PA 16802 | Homepage: | http://www.cse.psu.edu/~xxg113 |

Education

|  |  |
| --- | --- |
| **Ph.D., Computer Science and Engineering**  The Pennsylvania State University, University Park  *Advisor: Dr. Trent Jaeger* | 2012.8 – 2016.8 |
| **B.Eng., Software Engineering**  Nanjing University | 2008.8 – 2012.6 |

Professional Experiences

|  |  |
| --- | --- |
| **Penn State**, University Park, PA  Research Assistant, Advisor: Trent Jaeger | 2012.8 – 2016.8 |
| BINTRAN: a static binary rewriting tool that can arbitrarily insert or modify instructions within an ELF object, based on which, we instrumented the MINIX microkernel to implement the fine-grained control-flow integrity.  SPROBES: a TrustZone-based instrumentation mechanism that can transparently break on any normal world instruction from the secure world, using which, we enforced the kernel code integrity for Linux.  STING+: an in-vivo dynamic testing framework that can intercept all ongoing system calls with the capability to modify their arguments and return values at runtime, based on which, we developed a system to detect unsafe resource access in various programs (e.g., Apache). | |
| **Microsoft Research**, Redmond, WA  Research Intern, Mentor: Weidong Cui | 2015.5 – 2015.8 |
| Developed a prototype system for supporting Intel Processor Trace on Windows, enabling efficiently tracing multithreaded applications and recovering the exact control flows afterwards. | |
| **Microsoft Research**, Redmond, WA  Research Intern, Mentor: David Molnar | 2014.5 – 2014.8 |
| Developed an Azure cloud testing service that runs SAGE, a whitebox fuzzer employing symbolic execution to find defects as fast as possible by maximizing the code coverage, for resource-efficient large-scale fuzz testing of Windows applications (e.g., Microsoft Office). | |
| **eBay Inc.**, Shanghai, China  Technical Intern, Mentor: Eddy Cai | 2011.8 – 2012.5 |
| Developed a specialized search engine for historical SQL queries to help new database administrators find reusable queries. | |
| **Nanjing University**, Nanjing, China  Teaching Assistant, Instructor: Jidong Ge | 2011.2 – 2011.6 |
| fryy: a small operating system kernel designed from scratch for illustrating how OS functions (e.g., task management, file system, etc.) are implemented on real hardwares (x86). | |
| **State Key Laboratory for Novel Software Technology**, Nanjing, China  Research Intern, Advisor: Zhenyu Chen | 2011.8 – 2012.5 |
| Implemented an experimental recommender system and proposed a prediction approach based on regression for improving the quality of recommendation. | |

Honors & Awards

|  |  |
| --- | --- |
| Student Grant, USENIX OSDI | 2014.10 |
| Student Grant, USENIX Security | 2013.8 |
| Excellent Graduate Student, Nanjing University | 2012.6 |
| Award for Best Teaching Aids, Nanjing University | 2011.9 |
| Kwang-Hua Scholarship, Kwang-Hua Education Foundation | 2010.0 |

Skills

|  |
| --- |
| Programming Languages: C, Assembly, Python |
| Operating Systems: Linux, Windows, FreeBSD, MINIX |
| Misc: Intel Processor Trace, ARM TrustZone, Binary Analysis |

Publications

1. **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 (EuroS&P)*, March, 2016.
2. 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.
3. 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.
4. **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.
5. **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.