Jun Xu

WestGate Building E364
The Pennsylvania State University
University Park, PA 16802

814-880-9326
jxx13@ist.psu.edu
http://www.personal.psu.edu/jxx13

Research Interests

My research interests include **system security**, **software security**, and **software engineering**. The goal of my research is to secure computing systems by neutralizing the risk of vulnerabilities in the software stack. I specialize in vulnerability discovery, runtime protection, and vulnerability diagnosis. I also do research to mitigate the threats of malware.

Education

2013-Now **Ph.D Candidate** in **Cyber Security**
College of Information Sciences and Technology, The Pennsylvania State University
Thesis: Combining Heterogeneous Sources of Information to Analyze Software Crash
Adviser: Dr. Peng Liu

2009-2013 **B.A.Sc** in **Information Security**
Department of Information Security, University of Science and Technology of China
Graduated with Guo-Moruo Scholarship
Adviser: Dr. Nenghai Yu

Experiences

2013-Now **Graduate Research Assistant** *The Pennsylvania State University*
Adviser: Dr. Peng Liu & Dr. Xinyu Xing

Summer 2017 **Intern Research Assistant** *Samsung Research America*
Mentor: Ahmed Azab

Summer 2016 **Intern Research Assistant** *FireEye Lab*
Mentor: Jimmy Su

Summer 2015 **Intern Research Assistant** *FireEye Lab*
Mentor: Tao Wei & Jimmy Su

Spring 2013 **Intern Research Assistant** *The Pennsylvania State University*
Adviser: Dr. Peng Liu

Honors & Awards

2017 **Nominee by IST for Alumni Association Dissertation Award**, *The Pennsylvania State University*, 2017 (Under review).

2017 **RSA Security Scholarship**, *RSA Conference 2017*, U.S.A.

2016 **Student Travel Grant**, *CCS 2016*.

2013 **Outstanding Honor for National Undergraduates Innovative Project**, *China* (%5).

2013 **Guo-Moruo Scholarship**, *University of Science and Technology of China* (The first award established in a university in Mainland China).

Conference Publications

C-1 Huang, J., **Xu, J.**, Xing, X., Liu, P., *&* Qureshi, M. "FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware". In *Proceedings of 24th ACM Conference on Computer and Communications Security* (**CCS'17**), Dallas, USA, October 2017.

C-2 **Xu, J.**, Mu, D., Xing, X., Liu, P., Chen, P., *&* Mao, B. "POMP: Postmortem Program Analysis with Hardware-Enhanced Post-Crash Artifacts". In *Proceedings of 26th USENIX Security Symposium* (**USENIX Security'17**), Vancouver, Canada, August 2017.

C-3 Chen, P., **Xu, J.**, Hu, Z., Xing, X., Zhu, M., Mao, B, *&* Liu, P. "What You See is Not What You Get! Thwarting Just-in-Time ROP with Chameleon". In *Proceedings of 47th IEEE/IFIP International Conference on Dependable Systems and Networks* (**DSN'17**), Denver, USA, June 2017.

C-4 Deng, L., Liu, P., **Xu, J.**, Chen, P., *&* Zeng, Q. "Dancing with Wolves: Towards Practical Event-driven VM Monitoring". In *Proceedings of 13th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments* (**VEE'17**), Xian, China, April 2017.

C-5 **Xu, J.**, Mu, D., Chen, P., Wang, P., Xing, X., *&* Liu, P. "CREDAL: Towards Locating a Memory Corruption Vulnerability with Your Core Dump". In *Proceedings of 23nd ACM Conference on Computer and Communications Security* (**CCS'16**), Vienna, Austria, October 2016.

C-6 Guan, L., **Xu, J.**, Wang, S., Xing, X., Lin, L., Huang, H., Liu, P., *&* Lee, W. "From Physical to Cyber: Escalating Protection for Personalized Auto Insurance ". In *Proceedings of 14th ACM Conference on Embedded Networked Sensor Systems* (**Sensys'16**), Palo Alto, USA, December 2016.

C-7 Chen, P., **Xu, J.**, Xu, D., Lin, Z., *&* Liu, P. "A Practical Approach for Adaptive Data Structure Layout Randomization". In *Proceedings of 20th European Symposium on Research in Computer Security* (**ESORICS'15**), Vienna, Austria, September 2015.

C-8 Zhong, C., Zhao, M., Xiao, G., *&* **Xu, J.** (2013). "Leveraging "Visualization Functions" in Hypothesis-based Collaboration on Cyber Analysis". IEEE *Symposium on Visual Analytics Science and Technology* (short paper).

C-9 **Xu, J.**, Zhang, W., Yang, C., Xu, J., *&* Yu, N. (2012). "Two-Step-Ranking Secure Multi-Keyword Search Over Encrypted Cloud Data". In *Proceedings of International Conference on Cloud and Service Computing*. IEEE.

Workshop Publications

W-1 **Xu, J.**, Guo, P., Zhao, M., Erbacher, R. F., Zhu, M., *&* Liu, P. "Comparing Different Moving Target Defense Techniques". In *The First ACM Workshop on Moving Target Defense* (**MTD'14**), Tempe, USA, October 2014.

Other Publications

O-1 **Xu, J.**, Huang, J., Xing, X., Liu, P., *&* Qureshi, M. "FlashGuard: Hardware-Assisted Recovery Against Encryption Ransomware". In *RSA Conference 2017 Security Scholar Poster Exhibition* (**RSAC'17 Poster**), San Francisco, CA.

O-2 **Xu, J.**, Guo, P., Chen, B., Erbacher, R., Chen, P., *&* Liu, P. "Demo: A Symbolic N-Variant System". In *The Third ACM Workshop on Moving Target Defense* (**MTD'16 Demo**), Vienna, Austria, October 2016.

O-3 Chen, P., **Xu, J.**, Wang, J., *&* Liu, P. (2015, July). "Instantly Obsoleting the Address-code Associations: A New Principle for Defending Advanced Code Reuse Attack". http://arxiv.org/abs/1507.02786. arXiv Technical Report.

O-4 **Xu, J.**. "Table-Based SQL Injection Detection in WEB Service". *Bachelor Thesis*, University of Science and Technology of China, 2013.

Papers under Submission and Preparation

Authors are suppressed for anonymity (* *indicates a paper led by me*)

P-1 * "Reverse Execution". November 2017.

P-2 * "PTRIX: Enabling Efficient Hardware-Assisted Fuzzing for COTS Binary". November 2017.

P-3 * "SoK: An Empirical Study of Postmortem Program Analysis". December 2017.

P-4 "SEFuzz: Harnessing Efficiency of Fuzzing and Soundness of Symbolic Execution". December 2017.

P-5 "Rectifying Misleading Vulnerability Reports". January 2018.

P-6 "Automating Kernel Exploit Generation". January 2018.

Research

Vulnerability Discovery, Mitigation, and Diagnosis

2017 *Ptrix*, a fuzzer leverages Intel PT to achieve efficient and effective grey-box fuzzing.

2017 *SRACE*, a static analysis tool to find race condition bugs.

2017 *POMP*, a system that enhances a core dump with execution trace from Intel PT, performs reverse execution against the trace, and pinpoints the root cause of a software crash.

2016 *CREDAL*, a tool to analyze core dumps caused by memory corruption, locate the crash point, restore the stack trace, and narrow down code segments carrying vulnerabilities.

2015 *CHAMELEON*, a defense that implements adaptive address space layout randomization to defend against Just-in-Time Return Oriented Programming attacks.

2014 *SALADS*, a compiler plugin to achieve adaptive data structure layout randomization to mitigate memory corruption within data structures.

Malware Analysis and Defense

2016 *FlashGuard*, a recovery system that allows victims to restore files encrypted by ransomware.

2015 *DPACKER*, a kernel-level framework to dump malware instructions at run-time.

Impacts

Nov 2017 POMP is covered by International Forum for Security Research in Chinese (https://www.inforsec.org/wp/?p=2335).

Nov 2017 My research on discovering vulnerabilities on IoT devices is funded by JD.com with **$25,000**.

Oct 2017 Our fuzzers discovered many vulnerabilities that have lasted for long time in the wild (http://www.personal.psu.edu/jxx13/bug.html).

June 2017 We have open-sourced POMP and it has been forked by multiple research groups (https://github.com/junxzm1990/pomp).

June 2017 A proposal by Dr. Xinyu Xing based on my dissertation research has been funded by NSF for **$500,000** (Memory corruption driven postmortem program analysis).

Talks

June 2017 **What You See is Not What You Get! Thwarting Just-in-Time ROP with Chameleon**.
IEEE/IFIP DSN 2017, Denver, CO

Oct 2016 **Towards Locating a Memory Corruption Vulnerability with Your Core Dump**.
ACM CCS 2016, Vienna, Austria

Oct 2016 **A Symbolic N-Variant System**.
ACM MTD 2016, Vienna, Austria

August 2015 **Automated malware unpacking using dynamic analysis**.
FireEye Lab, Milpitas, CA

Oct 2014 **Comparing different moving target defense techniques**.
ACM MTD 2014, Tempe, AZ

Teaching Experiences

Spring 2017 Teaching Assistant, *The Pennsylvania State University*, SRA211: Introduction to Information Security
Instructor: Dr. Peng Liu

Fall 2016 Teaching Assistant, *The Pennsylvania State University*, SRA211: Introduction to Information Security
Instructor: Dr. Xinyu Xing

Mentoring Experiences

2016-Now Dongliang Mu, *The Pennsylvania State University*, Visiting Ph.D.
• Reverse Execution

2017 Wei Wu, *The Pennsylvania State University*, Visiting Ph.D.
• Automating Kernel Exploit Generation

2017 Yueqi Chen, *The Pennsylvania State University*, Ph.D.
• Rectifying Misleading Vulnerability Reports

2015-Now Alejandro Cuevas Villalba, *The Pennsylvania State University*, Undergraduate
• Quantification of Moving Target Defenses

Professional Services

TPC IEEE CNS 2018.

Reviewer IET Information Security 2017; IEEE TDSC 2017, 2016; ACM MTD 2016, 2015; IEEE TrustCom 2016; Financial Cryptography 2016; USENIX WOOT 2016.

References

Peng Liu, Professor
College of Information Sciences and Technology, The Pennsylvania State University
E330 Westgate Building, University Park, PA 16802
814-863-8641
pliu@ist.psu.edu

Trent Jaeger, Professor
School of Electrical Engineering and Computer Science, The Pennsylvania State University

W359 Westgate Building, University Park, PA 16802
814-865-1042
trj1@psu.edu

Xinyu Xing, Assistant Professor
College of Information Sciences and Technology, The Pennsylvania State University
E312 Westgate Building, University Park, PA 16802
814-863-0017
xxing@ist.psu.edu

Jian Huang, Assistant Professor
Department of Electronic and Computer Engineering, University of Illinois Urbana-Champaign
614-906-8989
jianh@illinois.edu

Jimmy Su, Head of JD.com Security Research Center, Ph.D.
JD.com Security Research Center
2900 Lakeside Dr Suite 230, Santa Clara, CA, 95054
925-385-8823
Jimmy.Su@jd.com