Pengfei Sun

✉ *pengfei.sun@rutgers.edu*
pengfeisun.com

Research Interests

My research focuses on software and systems security, including reverse engineering, malware analysis, memory forensics, Mobile/IoT embedded system security, bot detection, anomaly detection, AI-assisted security, virtualization and cloud security.

Appointment

05/2019-Present **Senior Research Scientist**, *Shape Security*, Mountain View, CA, USA..

Education

2013-05/2019 **Ph.D. Electrical and Computer Engineering**, *Rutgers University*, New Brunswick, NJ, USA. (1st year@University of Miami).
Advisor: Saman Zonouz. Thesis: "Exploring Semantic Reverse Engineering for Software Binary Protection."

2009–2012 **M.S. Electrical and Computer Engineering**, *Peking University*, Beijing, China.
Advisor: Qingni Shen. Thesis: "AppGuard: Application Secure Execution Environment on Untrusted Operating System."

2011–2012 **Visiting Graduate Student**, *Singapore Management University*, Singapore, Singapore.

2005–2009 **B.S. Mathematics and Applied Mathematics**, *North China University of Technology*, Beijing, China.

Publications

Pengfei Sun, Luis Garcia and Saman Zonouz. Automated Mobile/IoT Firmware Vulnerability Assessment based on Deep Learning. *ACSAC*, 2019, submitted.

Pengfei Sun, Luis Garcia and Saman Zonouz. Towards Robust Semantic Reverse Engineering of Control System Binaries. *Poster session, the 28th USENIX Security Symposium (Usenix Security'19)*, 2019.

Pengfei Sun, Luis Garcia and Saman Zonouz. Tell Me More Than Just Assembly! Reversing Cyber-physical Execution Semantics of Embedded IoT Controller Software Binaries. *The 49th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2019.

Mingbo Zhang, Luis Garcia, **Pengfei Sun**, Xiruo Liu and Saman Zonouz. Dynamic Memory Protection via Intel SGX-Supported Heap Allocation. *The 16th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC)*, 2018.

Devendra Shellar, **Pengfei Sun**, Saurabh Amin and Saman Zonouz. Compromising Security of Economic Dispatch in Power System Operations. *The 47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017.

Gabriel SallesLoustau, Luis Garcia, **Pengfei Sun**, Maryam Mehri and Saman Zonouz. Power Grid Safety Control via FineGrained MultiPersona Programmable Logic Controllers. *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2017.

Sriharsha Etigowni, Mehmet Cintuglu, Maryam Kazerooni, Shamina Hossain, **Pengfei Sun**, Katherine Davis, Osama Mohammed and Saman Zonouz. Cyber-Air-Gapped Detection of Controller Attacks through Physical Interdependencies. *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2017.

Pengfei Sun, Rui Han, Mingbo Zhang and Saman Zonouz. Trace-Free Memory Data Structure Forensics via Past Inference and Future Speculations. *Annual Computer Security Applications Conference (ACSAC)*, December 2016.

Pengfei Sun, Rui Han, and Saman Zonouz. Post-Intrusion Memory Forensics Analysis. *Poster session, the 37th IEEE Symposium on Security and Privacy (S&P)*, May 2016.

Henry Senyondo, **Pengfei Sun**, Robin Berthier, and Saman Zonouz. PLCloud: Comprehensive Power Grid PLC Security Monitoring with Zero Safety Disruption. *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, November 2015.

Ying Chen, Qingni Shen, **Pengfei Sun**, Yangwei Li, Zhong Chen, and Sihan Qing. Reliable Migration Module in Trusted Cloud based on Security Level: Design and Implementation. *In proceedings of the International Workshop of the 26th IEEE International Parallel and Distributed Processing Symposium (IPDPS'12)*, May 2012.

Yangwei Li, Qingni Shen, Cong Zhang, **Pengfei Sun**, Ying Chen, and Sihan Qing. A Covert Channel Using Core Alternation. *The 26th IEEE International Conference on Advanced Information Networking and Applications (AINA'12)*, March 2011.

Qingni Shen, Xin Yang, Xi Yu, **Pengfei Sun**, Yahui Yang, and Zhonghai Wu. Towards Data Isolation & Collaboration in Storage Cloud. *In proceedings of the 2011 IEEE Asia-Pacific Services Computing Conference (APSCC'11)* December 2011.

Pengfei Sun, Qingni Shen, Ying Chen, Zhonghai Wu, Cong Zhang, Anbang Ruan, and Liang Gu. LBMS: Load Balancing based on Multilateral Security In Cloud. *Poster session, The 18th ACM Conference on Computer and Communications Security (CCS'11)*, October 2011.

Pengfei Sun, Qingni Shen, Liang Gu, Yangwei Li, Sihan Qing, and Zhong Chen. Multilateral Security Architecture for Virtualization Platform in Multi-tenancy Cloud Environment. *In proceedings of the 13th IEEE Joint International Computer Science and Information Technology Conference (JICSIT'11)*, August 2011.

Patent

Qingni Shen, **Pengfei Sun**, Yangwei Li, and He Wei. A Method and System for Solving Multilateral Conflict on Virtualization Platform. *Under Chinese Patent Registration No. ZL CN201110228801.X*, April 2014.

Awards and Honors

- **IEEE/IFIP DSN Full Travel Award**, 2019.
- **Rutgers University ECE Academic Achievement Award**, 2019.
- **Rutgers University ECE PhD Research Excellence Award**, 2016.
- **Annual Computer Security Applications Conference Student Full Travel Award**, 2016.
- **The IEEE Symposium on Security and Privacy Student Full Travel Award**, 2016.
- **TCIPG Summer School Scholarship**, 2015.
- **University of Miami Graduate Fellowship**, 2013.
- **Peking University Outstanding Thesis Award**, 2012.
- **The ACM CCS 2011 Student Full Travel Award**, 2011.

Public Speaking

- **Towards Robust Semantic Reverse Engineering of Control System Binaries.**, Usenix Security (August 2019).
- **Tell Me More Than Just Assembly! ReversingCyber-physical Execution Semantics of Embedded IoT Controller Software Binaries.**, DSN (June 2019).
- **Trace-Free Memory Data Structure Forensics via Past Inference and Future Speculations**, ACSAC (December 2016).
- **Reviver: Trace-Free Memory Data Forensics Through Speculative Symbolic Execution**, TCIPG Summer School (June 2015).
- **Reliable Migration Module in Trusted Cloud based on Security Level: Design and Implementation**, IEEE IPDPS'12 Workshop (May 2012).

- **LBMS: Load Balancing based on Multilateral Security In Cloud**, ACM CCS'11 Poster Session (October 2011).

Research Experience

05/2019-Present **Senior Research Scientist**, *Shape Security, Mountain View, CA*.
Work on fraud detection and bot detection. Design and implement automated anomaly detection system.

05/2013-05/2019 **Research Assistant, 4N6 Cyber Security and Forensics Research Group**, *Rutgers University*.
Focus on semantic reverse engineering by program analysis and machine learning approach. Designed a framework [**Mismo**] to automatically analyze embedded system binaries to extract semantic information about the control algorithms that they implement. Based on the framework, I found one bug in one control algorithm of Linux kernel. I also designed and implemented a system [**ReViver**] to extract data structures semantic information from live memory without source code, debug symbol information and past execution traces. The system integrated static analysis and dynamic midway symbolic execution to retrieve data structures and all fields with high accuracy by experimenting on all CoreUtils applications and five popular large applications.

06/2018-10/2018 **Tech Lead**, *Sekurity, New York, NY*.
Working on Homeland Security DHS SBIR project as tech lead. Building binary vulnerability detection and exploration framework based on deep learning and dynamic analysis. Focus on mobile (Android/IOS) and IoT binaries vulnerability.

06/2017-08/2017 **Research Intern**, *Fujitsu Laboratories of America, Sunnyvale, CA*.
Designed one system which can mitigate Use-After-Free exploitation by preventing the freeing of memory chunks if references are found. Integrated static and dynamic analysis to do live pointer analysis to find live references for each memory object in any execution time. What's more, evaluated several current binary rewriting technologies based on DARPA CGC data set and did further exploration for reassembly symbolization recognition.

06/2016-08/2016 **Research Scientist Intern**, *GrammaTech, Ithaca, New York*.
Focus on autonomic computing system, and creating automated regression tests for system reasoning performance metrics. Producing test and evaluating different instrumentation scenarios. Contributing to the integration of system reason system and the design and evalutation of dynamic instrument selection.

10/2011-05/2012 **Research Assistant, School of Information Systems**, *Singapore Management University*.
Designed and implemented a system that provides a secure isolated execution environment for applications and ensures the privacy of data and application execution integrity in runtime based on Tiny VMM, since current commodity operating systems are rather big and not sufficiently reliable and secure [**AppGuard**].

09/2010-09/2011 **Team Leader, Virtualization & Cloud Security Group**, *Peking University*.
Designed and built a new secure load balancing architecture. When a host (physical machine) reaches peak-load, make sure that tenants' VMs automatically migrate to a host with the most appropriate security configurations by index and negotiation, instead of migrating to a host which is vulnerable to potential attacks, such as side channels[**LBMS**]. Developed Covert Channels using Core-Alternation, a prototype that can be able to create a core-alternative channel and communicates data in confidence [**CCCA**]. Worked with other team members to design and develop a prototype for data isolation and sharing among different organizations in cloud storage environment.

Professional Services

- **IEEE ISTAS 2019**, Program Committee.
- **IEEE S&P 2018**, Student Program Committee.
- **ICIMP 2018, 2019**, Program Committee.
- **IEEE JETCAS 2018**, Journal Reviewer.
- **IEEE Transactions on Industrial Informatics**, Journal Reviewer.
- **International Journal of Production Research**, Journal Reviewer.
- **Usenix WOOT 2016**, External Reviewer.

Teaching

Spring 2010 **Teaching Assistant, Operating System Security**, *Peking University*.
Designed and graded assignments and taught labs for graduate-level-course.

Spring 2010 **Teaching Assistant, Network Attack and Defense**, *Peking University*.
Designed and graded assignments.