Gaoning Pan

Github: github.com/hustdebug   **Email** : pgn@zju.edu.cn   **Mobile** : +86-153-0655-0528

EDUCATION

- **Zhejiang University**   Hangzhou, China
  PhD student in Cyberspace Security; Supervised by Prof. Chunming Wu and Prof. Shouling Ji   *Sept. 2018 – Present*

- **Huazhong University of Science and Technology**   Wuhan, China
  *Bachelor in Telecommunications Engineering; **ranking: 1/182***   *Sept. 2014 – June. 2018*

SKILLS

- **Programming**: Python, C/C++

- **Research Interests**: System and Software Security, Fuzzing, Virtualization Security

ACADEMIC PUBLICATIONS

- **Gaoning Pan**, Xingwei Lin, Xuhong Zhang, Yongkang Jia, Shouling Ji, Chunming Wu, Xinlei Ying, Jiashui Wang, and Yanjun Wu. **V-SHUTTLE: Scalable and Semantics-Aware Hypervisor Virtual Device Fuzzing**. ACM Conference on Computer and Communications Security (CCS), 2021. Best Paper Award

- **Gaoning Pan**, Yongkang Jia, Qiuhao Li, Xiao Lei, Xuhong Zhang, Qinying Wang, Chenyang Lyu, Xiang Chen, Chunming Wu, Shouling Ji, Yuan Tian. **V-Sounder: Efficient Instruction-Agnostic Virtual CPU Fuzzing via VM State Injection**. IEEE Transacations on Software Enginerring (TSE). (Under review)

- **Gaoning Pan**, Yiming Tao, Chunming Wu. **Virtual Machine Exploitation Based on Cross Domain Attack**. ACM Transacations on Software Enginerring and Methodology (TOSEM). (Under review)

- Chenyang Lyu, Jiacheng Xu, Shouling Ji, Xuhong Zhang, Qinying Wang, Binbin Zhao, **Gaoning Pan**, Wei Cao, Peng Chen, and Raheem Beyah. **MINER: A Hybrid Data-Driven Approach for REST API Fuzzing**. USENIX Security Symposium 2023.

- Xiang Ling, Lingfei Wu, Saizhuo Wang, **Gaoning Pan**, Tengfei Ma, Fangli Xu, AleX Liu, Chunming Wu, Shouling Ji. **Deep Graph Matching and Searching for Semantic Code Retrieval**. ACM Transactions on Knowledge Discovery from Data (TKDD), 2021.

- Boyang Zhou, **Gaoning Pan**, Chunming Wu, Kai Zhu, Wei Ruan. **Multi-Variant Network Address Hopping to Defend Stealthy Crossfire Attack**. Science China Information Sciences, 2020.

- Shuangxi Chen, **Gaoning Pan**, Chunming Wu, Xinyue Jiang. **Research on Executive Control Strategy of Mimic Web Defense Gateway**. IEEE International Symposium on Networks, Computers and Communications (ISNCC), 2019.

INDUSTRIAL CONFERENCES

- **Gaoning Pan**, Xingwei Lin, Xinlei Ying, Jiashui Wang. **Scavenger: Misuse Error Handling. Leading To QEMU/KVM Escape**. Black Hat Asia 2021.

- Yongkang Jia, Xiao Lei, Yiming Tao, **Gaoning Pan**, Chunming Wu. **Timekiller: Leveraging Asynchronous Clock to Escape from QEMU/KVM**. HITBSecConf 2023

- Qiuhao Li, **Gaoning Pan**, Hui he, Chunming Wu. **Hunting and Exploiting Recursive MMIO Flaws in QEMU/KVM**. Black Hat Asia 2022.

- Qiuhao Li, **Gaoning Pan**, Hui he, Chunming Wu. **Matryoshka Trap: Recursive MMIO Flaws Lead to VM Escape**. CanSecWest 2022.

Work Experience

- **Zhejiang University AAA Team**   Top international CTF team
- **Ant Security Light-year Lab**   Research on Virtual Device Fuzzing   1/5
- **State Grid Zhejiang Corporation**   Key application research and development projects   2/7
- **Wuhan National Optoelectronics Laboratory**   Multimode reliable transmission project   3/8

Honors And Awards

- 2022, **Pwnie Awards**, Most Innovative Research Nomination Award
- 2022, PhD National Scholarship, Zhejiang University
- 2022, Outstanding Graduate, Zhejiang University
- 2021, **Best Paper Award** of ACM CCS 2021
- 2019, International First Place of HITCON-quals 2019
- 2018, X-NUCA National University Cybersecurity Competition, Ranked 2nd
- 2019, **DEFCON final**, Ranked 4th
- 2019, Codegate-quals, Ranked 5th
- 2018, Undergraduate National Scholarship, Huazhong University of Science and Technology
- 2018, Outstanding Graduate, Huazhong University of Science and Technology
- 2017, Second Prize of Robomasters National College Robot Competition