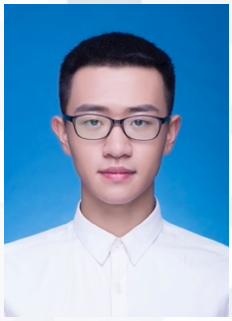
潘高宁

153-0655-0528 | pgn@zju.edu.cn

籍贯：浙江温州　　年龄：27



教育背景
Educational Experience

本科：华中科技大学	通信工程（排名 1/182）	2014/09 – 2018/06	本科生国家奖学金
博士：浙江大学	网络空间安全	2018/09 – 至今	博士生国家奖学金

个人技能
Personal Skills

编程技能：CCF 计算机职业资格认证 400 分（前 0.78%）　PAT 甲级 100 分（排名 1/1207）

研究方向：系统安全、模糊测试(Fuzzing)、虚拟化漏洞挖掘

学术著作
Academic Publications

1. **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). (CCF-A, **网络空间安全四大顶级会议, Best Paper Award，国内高校第二篇**)
2. **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). (CCF-A, Under review)
3. **Gaoning Pan**, Yiming Tao, Chunming Wu. Virtual Machine Exploitation Based on Cross Domain Attack. ACM Transacations on Software Enginerring and Methodology (TOSEM) (CCF-A, under review)
4. 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. (CCF-A, **网络空间安全四大顶级会议**)
5. 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. (CCF-B)
6. 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. (CCF-B)
7. 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. (EI 检索)

工业会议
Industrial conferences

1. **Gaoning Pan**, Xingwei Lin, Xinlei Ying, Jiashui Wang, Scavenger: Misuse Error Handling. Leading To QEMU/KVM Escape, Black Hat Asia 2021. **(国际最高黑客会议，该年国内唯一高校登上)**
2. Qiuhao Li, **Gaoning Pan**, Hui he, Chunming Wu, Hunting and Exploiting Recursive MMIO Flaws in QEMU/KVM, Black Hat Asia 2022. **(国际最高黑客会议，指导)**
3. Qiuhao Li, **Gaoning Pan**, Hui he, Chunming Wu, Matryoshka Trap: Recursive MMIO Flaws Lead to VM Escape, CanSecWest 2022. **(国际顶尖黑客会议，指导)**

科研经历
Project Experience

1. **Hypervisor 虚拟设备漏洞挖掘研究**：研究设计了轻量级语义感知的虚拟机漏洞挖掘工具 V-Shuttle，针对虚拟设备中 DMA 数据复杂嵌套的问题，构建了语义感知 DMA 重定向方法。本工具总计发现主流虚拟机中的 35 个未知漏洞，其中 17 个被国际漏洞社区授予了 CVE 编号。相关成果发表在了安全顶会 CCS 2021 上，并获得“**最佳论文奖**”,这是**中国团队历史上第二次以第一作者身份获得安全四大会议的 Best Paper 奖项**。同时这也是在蚂蚁安全光年实验室实习期间合作完成的工作，工具已在蚂蚁集团中得到了实际落地应用
2. **Hypervisor 虚拟 CPU 漏洞挖掘研究**： 研究基于退出状态注入的虚拟 CPU Fuzzing 方法，解决虚拟 CPU 场景下指令输入搜索空间爆炸的问题，从而提高 Fuzzing 效率。本工具总计发现 KVM 虚拟机中的 21 个未知漏洞，其中 5 个被国际漏洞社区授予了 CVE 编号
3. **Hypervisor 跨域攻击漏洞利用：**研究虚拟机场景下的跨域攻击，利用客户机内存来构造任意读写的原语，这是在在虚拟机场景下首次提出漏洞利用方法，相关成果发表在了黑客大会 Black Hat Asia 2021 上，并在“天府杯”原创漏洞演示赛完成 QEMU 0day 逃逸攻击

项目经历
Project Experience

浙江大学 AAA 战队	国内顶尖网络安全战队	
蚂蚁金服光年实验室	虚拟设备漏洞挖掘研究	1/5
国家电网浙江总公司	重点应用研发项目	2/7
武汉国家光电实验室	多模可靠传输项目	3/8

比赛经历
Project Experience

Pwnie Award（黑客奥斯卡）	最具创新性研究提名奖
Robomasters 全国大学生机器人大赛	全国二等奖
HITCON-quals 2019	全国第一名
D3^CTF 线上赛	全国第二名
X-NUCA 2018 全国高校网安联赛	全国第二名
第三届“强网杯”网络安全挑战赛	全国三等奖
数字经济云安全共测大赛	全国第三名
“西湖论剑”中国杭州网络安全技能大赛团队对抗赛	全国第三名
DEFCON-final 2019	全国第四名
Codegate 2019 国际黑客竞赛	国际第五名

社会贡献
Social Contributions

- 带领团队参与浙江省“护网 2021”网络安全应急演练活动，获得**浙江省公安厅**的高度认可
- 参与编著《网络安全国际学术研究进展》书籍