QINKUN BAO

1195 Bordeaux Dr, Sunnyvale, CA 94089
(+1)814-954-9223 ⋄ qinkunbao@gmail.com

EXPERIENCE

Baidu USA, Sunnyvale, CA *July 2021 - now*
Senior Security Researcher, Baidu X-Lab
Delivered: https://p4cleanroom.com (A confidential cloud service for hosting computational biology algorithms as SaaS services on the Azure confidential cloud.)

Baidu USA, Sunnyvale, CA *May 2020 - March 2021*
Research Intern, Baidu X-Lab

EPFL, Lausanne, Switzerland *February 2019 - July 2019*
Visiting Ph.D. student, VLSC lab
(Host: Dinghao Wu and Jim Larus)

Microsoft Research, Redmond, WA *May 2018 - August 2018*
Research Intern, Security and Cryptography group
(Mentor: Greg Zaverucha)

EDUCATION

The Pennsylvania State University Ph.D., Information Sciences and Technology, 2021
Ph.D. Dissertation: *Precise and Scalable Side-Channel Analysis.* (Advisor: Dinghao Wu)

University of Science and Technology of China B.E., Information Security, 2016

CURRENT PROJECTS

Apache Teaclave
Apache Teaclave (incubating) is an open source universal secure computing platform, making computation on privacy-sensitive data safe and simple. I am a **committer** of this project.
`https://teaclave.apache.org/`
`https://teaclave.apache.org/contributors/#committers`

SGXRay
SGXRay is an automated reasoning tool based on the SMACK verifier that detects SGX enclave bugs rooting from violations of trusted boundaries. After the analysis, it either finds an invalid pointer handling inside an SGX software stack such as deferencing unchecked pointer inside an enclave, invalid memory deallocation, and TOCTOU bugs, or prove the absense of such bugs up to a user-specified loop and recursion bound.
`https://github.com/baiduxlab/sgxray`

Side-channel Vulnerabilities Quantification
Develop side-channel quantification techniques that can automatically detect and quantify each address-based side-channel vulnerability. We evaluate the tool with real-world crypto and media libraries and find several severe leakages.
`https://github.com/s3team/Abacus`

Phoenix Binary Analysis Framework
Phoenix is a tiny binary analysis framework that supports X86 ELF. It provides components including dynamic symbolic execution engine, static symbolic reasoning, and internal abstract syntax tree (AST)

representations. Phoenix abandons the IR layer and works on native X86 instructions to achieve the ultimate performance. Phoenix is written in C++11 and also provides Python binding.

SECURITY VULNERABILITIES

I found security vulnerabilities in mainstream confidential computing frameworks.
Open Enclave:
CVE-2020-15224
Google Asylo:
CVE-2020-8904, CVE-2020-8905, CVE-2020-8935, CVE-2020-8936, CVE-2020-8937, CVE-2020-8938, CVE-2020-8939, CVE-2020-8940, CVE-2020-8941, CVE-2020-8942, CVE-2020-8943, CVE-2020-8944, CVE-2021-22548, CVE-2021-22549, CVE-2021-22550
I am also acknowledged by The Confidential Consortium Framework developers by reporting security bugs.

TECHNICAL SKILLS

- Strong system coding skills (C++, Rust, Python).
- Rich experience in Open-Source Software (OSS) technologies (Apache Committer).
- Knowledge with networking protocols and basic cryptography.

TEACHING

Instructor for IST 543, Software Security, Spring 2020
TA for IST 456, Information Security Management, Fall 2018

ACADEMIC SERVICE

Review for the 43rd International Conference on Software Engineering (ICSE 2021).
Review for the International Conference on Secure Knowledge Management (SKM 2021).
Review for the 29th IEEE International Conference on Software Quality, Reliability, and Security (QRS 2019).
Review for the 15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2019).

INVITED TALKS

"Automated Vulnerability Finding in SGX Enclave Application." Blackhat USA, Las Vegas, NV, 2021.
"Abacus: Precise Side-Channel Analysis" ICSE 2021, Virtual (originally Madrid, Spain), 2021.
"A Journey On Discovering Vulnerabilities And Exploiting SGX Enclave Frameworks?" ZeroCon Conference, Virtual (originally South Korea), April, 2020.
"How can untrusted data leads to R/W your secrets inside the Enclave?" Baidu Xlab, Sunnyvale, CA, August 8, 2020.
"Abacus: Precise Side-channel Analysis." EPFL, Switzerland, 2019.
"Identifying Crypto Primitives in Malware Samples." Microsoft Research, Redmond, WA, August, 2018.

PUBLICATIONS

(Three papers are under review from top-tier security and software engineering conferences.)

Qinkun Bao, Zihao Wang, Xiaoting Li, James Larus, Dinghao Wu, "Abacus: Precise Side-Channel Analysis", In *Proceedings of the 43rd International Conference on Software Engineering (ICSE 2021)*, Madrid, Spain, 2021.

Qinkun Bao, Zihao Wang, James Larus, Dinghao Wu, "Abacus: A Tool for Precise Side-Channel Analysis", In *Proceedings of the 43rd International Conference on Software Engineering: Companion (ICSE-Companion 2021)*, Madrid, Spain, 2021.

Shixiong Jing, **Qinkun Bao**, Pei Wang, Xulong Tang, Dinghao Wu, "Characterizing AI Model Inference Applications Running in SGX Environment", In *Proceedings of the 15th International Conference on Networking, Architecture, and Storage (NAS 2021)*.

Yufei Jiang, **Qinkun Bao**, Xiao Liu, Dinghao Wu, "RedDroid: Android Application Redundancy Customization based on Static Analysis", in *Proceedings of the 29th IEEE International Symposium on Software Reliability Engineering (ISSRE 2018)*, Memphis, TN, October 15-18, 2018.

Pei Wang, **Qinkun Bao**, Li Wang, Shuai Wang, Zhaofeng Chen, Tao Wei, Dinghao Wu, "Software Protection On-The-Go: An Empirical Study on Mobile App Obfuscation", in *Proceedings of 40th International Conference on Software Engineering (ICSE 2018)*, Gothenburg, Sweden, May 27-June 3, 2018.

Shengru Li, Kai Han, Nirwan Ansari, **Qinkun Bao**, Daoyun Hu, Junjie Liu, Shui Yu, Zuqing Zhu, "Improving SDN Scalability with Protocol-Oblivious Source Routing: A System-Level Study", *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 275-288, March 2018.

Shuai Wang, Wenhao Wang, **Qinkun Bao**, Pei Wang, Xiaofeng Wang, Dinghao Wu, "Binary Code Retrofitting and Hardening Using SGX", in *Proceedings of the 2017 workshop on Forming an Ecosystem Around Software Transformation (FEAST17)*, co-located with CCS 2017, Dallas, USA, November 3, 2017.

Shilin Zhu, Siyao Meng, **Qinkun Bao**, Xiaoliang Chen, and Zuqing Zhu, "Availability-Aware Service Provisioning in EONs: How Efficient will FIPP-p-Cycles be?", in *Proceedings of IEEE/OSA Optical Fiber Communication Conference (OFC)*, paper W2A.51, March 2016.

Xiaoliang Chen, Fan Ji, Shilin Zhu, **Qinkun Bao**, and Zuqing Zhu, "Availability-Aware Service Provisioning in SD-EON based Inter-Datacenter Networks", *Photonic Network Communications (Springer)*, vol. 31, no. 3, pp. 543-549, June 2016.