ZHENXIAO QI

+1-951-421-9319 • zhenxiao020@gmail.com • https://github.com/enlighten5

SUMMARY

Zhenxiao Qi is a fifth-year Ph.D. candidate. His research focuses on advancing binary analysis and threat detection. He developed various binary analysis techniques (e.g., dynamic taint analysis, concolic execution, memory snapshot analysis, etc) to solve security problems, including vulnerability detection, kernel rootkit detection, memory forensics, etc.

EDUCATION

University of California, Riverside Aug. 2018 - Present
Degree expected: Ph.D. in Computer Science
University of California, Riverside
Master of Science, Computer Science
University of California, Riverside Aug. 2017 – Jun. 2018
Exchange student, Computer Science
Xidian University Aug. 2014 – Jun. 2018
Bachelor of Engineering, Information Security

PROFESSIONAL EXPERIENCE

Research Intern @ Google Cloud, Sunnyvale, CA Jun 2022 – Sep. 2022
- Detection of malicious activities and intrusion threats on Google Cloud Platform VMs.
- Developed an efficient algorithm for locating kernel memory region in large memory snapshots.

Software Engineer Intern @ Deepbits, Riverside, CA Oct. 2021 – Jun. 2022
- Developed kernel rootkit and threat detection services for cloud VM protection.
- Developed agent-less dynamic analysis for Docker container.
- Developed memory forensics for analyzing VM memory snapshots.

Research Intern @ Google Cloud, Remote Jun. 2021 – Sep. 2021
- Developed a logic inference-based profile generation for kernel memory analysis on Google Cloud VMs.
- Enable memory analysis on unsupported cloud VMs due to lack of matching kernel profiles.

Graduate student researcher @ UCR Jun. 2018 – Present

PUBLICATIONS

[NDSS'22] Zhenxiao Qi, Yu Qu, Heng Yin, LOGICMEM: Automatic Profile Generation for Binary-only Memory Forensics via Logic Inference, to appear in the Network and Distributed System Security Symposium, February 2022.
[NDSS'21] Zhenxiao Qi, Qian Feng, Yueqiang Cheng, Mengjia Yan, Peng Li, Heng Yin, and Tao Wei, SpecTaint:SpecTaint: Speculative Taint Analysis for Discovering Spectre Gadgets, to appear in the Network and Distributed System Security Symposium, February 2021
[RAID'19] Ali Davanian, **Zhenxiao Qi**, Yu Qu, and Heng Yin, DECAF++: Elastic Whole-System Dynamic Taint Analysis, in the 22nd International Symposium on Research in Attacks, Intrusions and Defenses, September 2019

RESEARCH PROJECTS

Enhancing Memory Analysis: An Efficient Algorithm for Locating Kernel Memory
Google Cloud, Mentor: Mithun Iyer
- Kernel code hash matching is one effective method to detect malicious code running in the kernel.
- To generate hashes of kernel code, the first step is to locate the kernel memory region.
- Sequentially scanning the memory snapshot to locate kernel memory is inefficient as the kernel can be placed anywhere due to KASLR and the memory snapshot can be large.

- Developed an efficient method that walks the kernel page table and filters out user-level pages based on PTE flags.
- Reduced the searching time from minutes to 1 second.

Agent-less dynamic container monitoring
Deepbits, Mentor: Xunchao Hu

- Developed a runtime container monitor approach without running an agent inside the container.
- Automatically collect activities of running processes inside the container, such as network connection, opened files, process credentials and permissions, etc.
- Performed large-scale analysis of existing docker images hosted on DockerHub.

Memory snapshot analysis for kernel rootkit and threat detection
Deepbits, Mentor: Xunchao Hu

- Developed an API-based service for memory snapshot analysis.
- Developed a differential testing approach to detecting hidden kernel rootkits and threats.

Binary-only profile generation for kernel integrity analysis on Google Cloud VMs
Google Cloud, Mentor: Mahesh Pisal

- Worked with the Virtual Machine Threat Detection team to improve the coverage of kernel threat detection.
- Around 20% VMs are not supported due to the lack of kernel profiles.
- Integrated the research prototype LOGICMEM to enable the analysis on uncovered VMs.

LogicMEM: A Logic Inference Approach to Automate Profile Generation for Binary-only Memory Forensics
UCR, Advisor: Heng Yin

- Existing profile generation approaches require access to the target system to obtain debug symbols, which is not feasible when only the memory snapshot is available
- LOGICMEM is the first binary-only profile generation approach to profile generation.
- Widely tested on a range of Linux kernel distributions and showed high precision and recall.

SpecTaint: Speculative Taint Analysis for Discovering Spectre Gadgets
UCR, Advisor: Heng Yin

- A novel Spectre gadget detection approach by enabling dynamic taint analysis on simulated speculative execution paths
- The evaluation results show significantly improved precision and recall with reasonable efficiency.
- Detected 11 new Spectre gadgets from real-world programs such as Brotli and Caffee.

SKILLS & OTHER

Languages: C/C++, Python, Rust, Go, Logic Programming.
Program analysis: FL/AFL++, Angr, DECAF, QSYM, SymSan, SymCC, SymQEMU.
Developer Tools: Git, Docker, TravisCI, Google Cloud Platform, VS Code, Visual Studio, PyCharm, IntelliJ.

PROFESSIONAL SERVICES

Reviewer: Cybersecurity, Computers and Security, Journal of Cyber Security Technology.
Sub-reviewer: SENIX Security'21, DIMVA'19.
Artifact evaluation: ACSAC '18 and ACSAC '19.

HONORS & AWARDS

- Outstanding Teaching Assistance in CSE Department 2019-2020
- Dean's Distinguished Fellowship, UC, Riverside 2018-2019
- Outstanding Student Scholarship, Xidian University 2014-2017