

Yueqi Chen

Department of Computer Science
The University of Colorado Boulder
Email: yueqi.chen@colorado.edu
Homepage: <http://yueqichen.org/>
Twitter: https://twitter.com/Lewis_Chen

RESEARCH INTERESTS

In general, my research are is **system and software security**. I focus on revolutionizing **exploitation** techniques, programming **weird machine**, and using outcomes of these research to design **protections** in a quantitative approach for infrastructure cyber-systems (e.g., Operating Systems, Cryptography Libraries, and Satellite Systems). I am very happy that our works have received wide recognition in both academia and industry.

EDUCATION

- **Ph.D in Information Sciences, Pennsylvania State University**, State College, PA, USA (Aug 2017 - June 2022)
Advisor: Xinyu Xing
- **B.S. in Computer Science and Technology, Nanjing University**, Nanjing, China (Sept 2013 - June 2017)

EXPERIENCES

- **University of Colorado Boulder**, Boulder, USA (Aug 2022 - Present)
Assistant Professor
- **Northwestern University**, Evanston, USA (Jan 2022 - June 2022)
Visiting Scholar
Advisor: Xinyu Xing
- **Pennsylvania State University**, State College, USA (Aug 2017 - June 2022)
Research Assistant
Advisor: Xinyu Xing
- **IBM Watson**, Yorktown Heights, USA (May 2021 - Aug 2021)
Research Intern: worked on on-demand protection for kernel
Mentor: Michael Le, Dan Williams
- **Baidu X-Lab**, Sunnyvale, USA (May 2019 - Aug 2019)
Research Intern: worked on cache timing attack detection
Mentor: Peng Li, Shengjian Guo, Yueqiang Cheng
- **JD.com Silicon Valley R&D Center**, Mountain View, USA (May 2018 - Aug 2018)
Research Intern: worked on ARM ETM assisted kernel protection
Mentor: Yueh-Hsun Lin

HONORS & AWARDS

- Pwn2Own 2022, winner, Vancouver, Canada, May. 2022
- The 7th place in DEFCON 29 CTF (Team Nu1L), Las Vegas, USA, Aug. 2021
- **IBM PhD Fellowship Award, 2020**
- BlackHat USA, Student Scholarship, 2021
- IST Graduate Student Travel Grant Award, 2020
- BlackHat USA, Student Scholarship, 2020
- IST Graduate Student Travel Grant Award, 2019
- The 28th USENIX Security Symposium, Student Travel Grant Award, 2019
- FUZE is awarded one of the ten technical events of JD.COM, 2018
- The 16th place in DEFCON 26 CTF (Team r3kapig), Las Vegas, USA, Aug. 2018
- BlackHat USA, Student Scholarship, 2018
- The 39th IEEE Symposium on Security and Privacy, Student Travel Grant Award, 2018
- The 5th place in NSA codebreaker Challenge, Nov.2017

TALKS & LECTURES

- **Towards Exploitability Assessment for Linux Kernel Vulnerabilities**
Vrije Universiteit Amsterdam, Amsterdam, Netherlands, Nov. 2019
University of Oxford, Oxford, UK, Nov. 2019
- **Vulnerability Exploitability Assessment and Mitigation Design Defects in Linux Kernel**
CLK 2019, Hangzhou, China, Oct. 2019

PUBLICATIONS

1. CLExtract: Recovering Highly Corrupted DVB/GSE Satellite Stream with Contrastive Learning
M. Lin, M. Cheng, D. Luo, Y. Chen
Workshop on the Security of Space and Satellite Systems (SpaceSec) 2023
2. **Playing for K-Heaps: Empirical Evaluation of Kernel Heap Exploitation Robustness Techniques**
Y. Chen*, K. Zeng*, H. Cho, X. Xing, A. Doupé, T. Bao, and Y. Shoshitaishvili
USENIX Security Symposium (Security) 2022
* indicates equal contribution
3. **An In-depth Analysis of Duplicated Linux Kernel Bug Reports**
D. Mu, Y. Wu, Y. Chen, Z. Lin, C. Yu, X. Xing, and G. Wang
Network and Distributed System Security Symposium (NDSS) 2022
4. **GREBE: Facilitating Security Assessment for Linux Kernel Bugs**
Z. Lin, Y. Chen, D. Mu, C. Yu, Y. Wu, X. Xing, and K. Li
IEEE Symposium on Security and Privacy (SP) 2022

5. **A Systematic Study of Elastic Objects in Kernel Exploitation**
Y. Chen, Z. Lin, and X. Xing
ACM Conference on Computer and Communication Security (CCS) 2020
6. **Exposing Cache Timing Side-channel Leaks through Out-of-order Symbolic Execution**
Y. Chen*, S. Guo*, J. Yu, M. Wu, Z. Zuo, P. Li, and Y. Cheng
Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA) 2020
* indicates equal contribution
7. **SpecuSym: Speculative Symbolic Execution for Cache Timing Leak Detection**
Y. Chen*, S. Guo*, P. Li, Y. Cheng, H. Wang, M. Wu, and Z. Zuo
International Conference on Software Engineering (ICSE) 2020
* indicates equal contribution
8. **SLAKE: Facilitating Slab Manipulation for Exploiting Vulnerabilities in the Linux Kernel**
Y. Chen, and X. Xing
ACM Conference on Computer and Communication Security (CCS) 2019
9. **Towards the Detection of Inconsistencies in Public Security Vulnerability Reports**
Y. Dong, W. Guo, Y. Chen, X. Xing, Y. Zhang, and G. Wang
USENIX Security Symposium (Security) 2019
10. **RENN: Efficient Reverse Execution with Neural-Network Alias Analysis**
D. Mu, W. Guo, A. Cuevas, Y. Chen, J. Gai, X. Xing, and B. Mao
International Conference on Automated Software Engineering (ASE) 2019
11. **KEPLER: Facilitating Control-flow Hijacking Primitive Evaluation for Linux Kernel Vulnerabilities**
W. Wu, Y. Chen, X. Xing, and W. Zou
USENIX Security Symposium (Security) 2019
12. **FUZE: Towards Facilitating Exploit Generation for Kernel Use-After-Free Vulnerabilities**
W. Wu, Y. Chen, J. Xu, X. Xing, W. Zou, and X. Gong
USENIX Security Symposium (Security) 2018

OTHER PUBLICATIONS

13. **HotBPF++: A More Powerful Memory Protection for the Linux Kernel**
Z. Wang, Yueqi Chen
Linux Security Summit North America 2023
14. **Comp4Exp: A Compiler Framework for Exploit Generation**
Y. Chen, Z. Lin, K. Huang, X. Xing, T. Jaeger, and S. Jha
IEEE Symposium on Security and Privacy (SP) to be submitted to 2023
15. **HOTBPF: On-demand Kernel Object Isolation**
Y. Chen, Z. Lin, X. Xing, M. Le, D. Williams, and H. T. Jamjoon
USENIX Security Symposium (Security) in submission 2022

16. **Linux Kernel Hardening: The Good, The Bad, The Ugly**
Y. Chen, Z. Lin, D. Mu, X. Xing
USENIX Security Symposium (Security) in submission 2022
17. **HotBPF - An On-demand and On-the-fly Memory Protection for the Linux Kernel**
Y. Chen, Z. Lin
Linux Security Summit Europe 2022
18. **A General Approach to Bypassing Many Kernel Protections and Its Mitigation**
Y. Chen, Z. Lin, and X. Xing
BlackHat Asia 2021
19. **Your Trash Kernel Bug, My Precious 0-day**
Z. Lin, Y. Chen, X. Xing, and K. Li
BlackHat Europe 2021
20. **Finding Multiple Bug Effects for More Precise Exploitability Estimation**
Z. Lin, and Y. Chen
Linux Security Summit North America 2021
21. **Bypassing Many Kernel Protections Using Elastic Objects**
Y. Chen, Z. Lin, and X. Xing
Linux Security Summit Europe 2020
22. **Facilitate Linux Kernel Exploitation Step by Step**
Y. Chen
BlueHat IL 2020
23. **Hands Off and Putting SLAB/SLUB Feng Shui in a Blackbox**
Y. Chen, X. Xing, and J. Su
Black Hat Europe 2019

OPEN SOURCE CONTRIBUTION

- **w2l**: Transfer a limited overwriting to sensitive data leaking. Lead author.
<https://github.com/chenyueqi/w2l>
- **SLAKE**: Discover sensitive object and automate layout manipulation. Lead author.
<https://github.com/chenyueqi/SLAKE>
- **afl-pt**: Intel PT assisted AFL. Contributor
<https://github.com/junxzm1990/afl-pt>
- **KEPLER**: Code gadgets analysis and chaining tool. Contributor.
<https://github.com/ww9210/kepler-cfhp>
- **FUZE**: Primitive exploration and analysis tool. Contributor.
https://github.com/ww9210/Linux_kernel_exploits
- **Symo3**: Cache timing attack detection tool. Lead author.
<https://github.com/chenyueqi/symo3>

- **VIEM**: Vulnerability report analysis tool. Contributor.
https://github.com/pinkymm/inconsistency_detection
- **RENN**: Deep-learning assisted alias analysis. Contributor.
<https://github.com/mudongliang/RENN>
- **HotBPF**: On-demand protection for Linux kernel. Lead author.
<https://github.com/chenyueqi/hotBPF>

TEACHING

- **At CU Boulder**
Fall 2022: CSCI 7000-007 Advanced System Security, Instructor
- **At Penn State**
Fall 2019 : Cyber Analysis Studio (CYBER 362), Teaching Assistant
Spring 2019 : Information Security Management (IST 456), Teaching Assistant
Fall 2018 : Overview of Information Security (SRA 221), Teaching Assistant

COMMUNITY SERVICES

- **Session Chair**
IEEE Symposium on Security and Privacy (S&P), 2022
 - **Reviewer**
International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2023
IEEE Transactions on Dependable and Secure Computing, 2023
International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2022
IEEE Transactions on Dependable and Secure Computing, 2022
IEEE Symposium on Security and Privacy (S&P) Poster, 2022
ACM Transactions on Privacy and Security, 2021
 - **Shadow PC**
IEEE Symposium on Security and Privacy (S&P), 2021
 - **External reviewer**
IEEE Symposium on Security and Privacy (S&P), 2023
IEEE Symposium on Security and Privacy (S&P), 2022
USENIX Security, 2021
USENIX Security, 2020
ACM Conference on Computer and Communication Security (CCS), 2020
Annual Computer Security Applications Conference (ACSAC), 2020
ACM Conference on Computer and Communication Security (CCS), 2019
European Symposium on Research on Computer Security (ESORICS), 2019
Annual Computer Security Applications Conference (ACSAC), 2019
Information Security Conference (ISC), 2019
ACM Asia Conference on Information, Computer and Communication Security (ASIACCS), 2018
IEEE Conference on Communications and Network Security (CNS), 2019
-

Yueqi Chen

Last update: March 27, 2023