Yueqi Chen

Department of Computer Science
The University of Colorado Boulder
Email: yueqi.chen@colorado.edu
Homepage: http://cusecurity.cs.colorado.edu/yueqichen/

RESEARCH INTERESTS

In general, my research interest is **system and software security** and centers around **weird machine** concept. I desire to understand weird machine, especially for cyber infrastructures (e.g., Operating Systems, Cryptography Libraries, and Satellite Systems), by developing new exploitation techniques to program weird machine and building protections to anti-program weird machine. I am very happy that our works have received wide recognition in both academia and industry.

HONORS & AWARDS

- CSAW 2022 Applied Research Competition Best Paper Finalist, 2023
- CSAW 2022 Applied Research Competition Best Paper Finalist, 2022
- 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

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. **PET: Prevent Discovered Errors from Being Triggered in the Linux Kernel**
   Z. Wang, ***Y. Chen***, Q. Zeng
   USENIX Security Symposium ***(Security)*** *2023*

3. **Mitigating Security Risks in Linux with KLAUS: A Method for Evaluating Patch Correctness**
   Y. Wu, Z, Lin, ***Y. Chen***, D. Le, D, Mu, and X. Xing
   USENIX Security Symposium ***(Security)*** *2023*

4. **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

5. **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*

6. **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*

7. **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*

8. **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

9. **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

10. **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*

11. **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*

12. **RENN: Efficient Reverse Execution with Neural-Network Alias Analysis**
    D. Mu, W. Guo, A. Cuevas, ***Y. Chen***, J. Gai, X. Xing, and B. Mao
    I*nternational Conference on Automated Software Engineering* ***(ASE)*** *2019*

13. **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*

14. **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

15. **Kill Latest MPU-based Protections in Just One Shot: Targeting All Commodity RTOSes**
    M. Lin, Z. Wang, J. Wang, C. Lin, M, Shen, ***Y. Chen***
    BlackHat USA 2023

16. **An End-to-End Tool Decoding Highly Corrupted Satellite Stream from Eavesdropping**
    M. Lin, *M. Chen, X. Zheng, D. Luo*, ***Y. Chen***
    BlackHat USA 2023

17. **HotBPF++: A More Powerful Memory Protection for the Linux Kernel**
    Z. Wang, Y. Chen
    Linux Security Summit North America 2023

18. **HotBPF - An On-demand and On-the-fly Memory Protection for the Linux Kernel**
    Y. Chen, Z. Lin
    Linux Security Summit Europe 2022

19. **A General Approach to Bypassing Many Kernel Protections and Its Mitigation**
    Y. Chen, Z. Lin, and X. Xing
    BlackHat Asia 2021

20. **Your Trash Kernel Bug, My Precious 0-day**
    Z. Lin, ***Y. Chen***, X. Xing, and K. Li
    BlackHat Europe 2021

21. **Finding Multiple Bug Effects for More Precise Exploitability Estimation**
    Z. Lin, and ***Y. Chen***
    Linux Security Summit North America 2021

22. **Bypassing Many Kernel Protections Using Elastic Objects**
    Y. Chen, Z. Lin, and X. Xing
    Linux Security Summit Europe 2020

23. **Facilitate Linux Kernel Exploitation Step by Step**
    Y. Chen
    BlueHat IL 2020

24. **Hands Off and Putting SLAB/SLUB Feng Shui in a Blackbox**
    Y. Chen, X. Xing, and J. Su
    Black Hat Europe 2019

TEACHING

- **At CU Boulder**

  Fall 2023: CSCI 5523 / ECEN5033 Modern Offense and Defense in Cyberspace, Instructor

  Spring 2023: CSCI 7000 / ECEN5033 Modern Offense and Defense in Cyberspace, Instructor

  Fall 2022: CSCI 7000 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

- **In Boulder**

  CU Cyber Club, Faculty Advisor

  Computer Engineering Track Faculty Search Committee, Member

  Graduate Committee, Member

  Course Support Committee, Member

- **Panelist**

  National Science Foundation SaTC Program, 2023

- **Session/Donation/Track Chair**

  IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), 2024

  IEEE Symposium on Security and Privacy (S&P), 2024

  IEEE Symposium on Security and Privacy (S&P), 2022

- **Reviewer**

  Workshop on the Security of Space and Satellite Systems (SpaceSec), 2024

  ACM Conference on Computer and Communication Security (CCS), 2023

  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

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

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

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

Yueqi Chen

Last update: Jan 02, 2024