XIAOGUANG WANG

✉ xgwang9@uic.edu · ☏ +1(540)998-2666 · ⚮ https://xiaoguang.wang

RESEARCH INTERESTS

Systems and Software Security, Operating Systems (Virtualization, ISA-Heterogeneous Systems), Compiler.

PROFESSIONAL EXPERIENCE

Assistant Professor, University of Illinois Chicago, Chicago, IL — Aug. 2023 - Now

Research Assistant Professor, Virginia Tech, Blacksburg, VA — July. 2021 - Aug.2023

Postdoc Associate, Virginia Tech, Blacksburg, VA — Jun. 2018 - Jun. 2021
- Secure Popcorn Linux, sponsored by U.S. Office of Naval Research (ONR). (`http://popcornlinux.org`)
- *Advisor*: Prof. Binoy Ravindran

Senior Software Engineer, Huawei Cloud BU, Xi'an, China — Jun. 2017 – Jun. 2018
- Heterogeneous cloud computing product design, OpenStack development (making the GPU/FGPA cloud instances publicly available).

Research Intern, Samsung Research China (SRC), Xi'an, China — Nov. 2016 – Feb. 2017
- Topic: Bare-metal operating systems migration with on-demand virtualization.

EDUCATION

Ph.D. in Computer Science, Xi'an Jiaotong University, China — 2010 – 2017
- *Thesis:* Enhancing System Software Security in Cloud Environment
- *Advisor*: Prof. Yong Qi

Visiting Ph.D. student at Florida State University, Tallahassee, U.S. — 2013 – 2015
- *Research topics:* System security; Operating system; Virtualization; Compiler.
- *Advisor*: Prof. Zhi Wang

B.Eng. in Software Engineering, Northwestern Polytechnic University, China — 2006 – 2010
- *Thesis:* Design and implementation of a Guest OS communication module with nested page tables. (Outstanding Undergraduate Thesis, NWPU)

SELECTED PUBLICATIONS

(Underline indicates students (co-)advised by me; * indicates equal contributions)
- **sMVX: Multi-Variant Execution on Selected Code Paths**
  SengMing Yeoh, Xiaoguang Wang, Jae-Won Jang, and Binoy Ravindran.
  25th ACM/IFIP International Middleware Conference (Middleware'24), December 2–6, 2024, Hong Kong, Hong Kong.
- **Dapper: A Lightweight and Extensible Framework for Live Program State Rewriting**
  Abhishek Bapat*, Jaidev Shastri*, Xiaoguang Wang*, Abilesh Sundarasamy, and Binoy Ravindran.
  44th IEEE International Conference on Distributed Computing Systems (ICDCS 2024), July 23-26, 2024, Jersey City, New Jersey, USA.
- **DynaCut: A Framework for Dynamic and Adaptive Program Customization**
  Abhijit Mahurkar*, Xiaoguang Wang*, Hang Zhang, and Binoy Ravindran.
  24th ACM/IFIP International Middleware Conference (Middleware'23), December 11-15, 2023, Bologna, Italy.
- **Understanding the Security of Linux eBPF Subsystem**
  Mohamed Husain, Xiaoguang Wang and Binoy Ravindran.
  14th ACM SIGOPS Asia-Pacific Workshop on Systems (APSys 2023), August 24-25, 2023, Seoul, South Korea

- Rave: **A Modular and Extensible Framework for Program State Re-Randomization**
  Chris Blackburn, Xiaoguang Wang and Binoy Ravindran.
  9th ACM Workshop on Moving Target Defense (MTD), Collocated with the ACM Conference on Computer and Communications Security (CCS), Los Angeles, USA, November 7, 2022.
- **Transparent, Cross-ISA Enclave Offloading**
  Xiaoguang Wang, Carlos Bilbao and Binoy Ravindran.
  5th Workshop on System Software for Trusted Execution (SysTEX 2022), Collocated with ASPLOS 2022 Lausanne, Switzerland, March 1st, 2022.
- **Dynamic and Secure Memory Transformation in Userspace**
  Robert Lyerly, Xiaoguang Wang, and Binoy Ravindran.
  The 25th European Symposium on Research in Computer Security (ESORICS 2020), Guildford, United Kingdom, September 14-18, 2020.
- **A Framework for Software Diversification with ISA Heterogeneity**
  Xiaoguang Wang, SengMing Yeoh, Robert Lyerly, Pierre Olivier, Sang-Hoon Kim, and Binoy Ravindran.
  The 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020), Donostia / San Sebastian, Spain, October 14-16, 2020.
- **Secure and Efficient In-process Monitor (and Library) Protection with Intel MPK**
  Xiaoguang Wang, SengMing Yeoh, Pierre Olivier, and Binoy Ravindran.
  The 13th European Workshop on Systems Security (EuroSec), co-located with EuroSys 2020, Heraklion, Crete, Greece, April 27, 2020.
- **Design and Implementation of SecPod, A Framework for Virtualization-based Security Systems**
  Xiaoguang Wang, Yong Qi, Zhi Wang, Yue Chen, Yajin Zhou.
  IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 16, No. 1, 2019.
- **Secure the Commodity Applications Against Address Exposure Attacks**
  Xiaoguang Wang, Yong Qi.
  The 22nd IEEE Symposium on Computers and Communications (ISCC'17), pp. 450-456. IEEE, 2017.
- **SecretSafe: A Lightweight Approach Against Heap Buffer Over-read Attack**
  Xiaoguang Wang, Yong Qi, Chi Zhang, Saiyu Qi, Peijian Wang.
  IEEE 41th Computer Software and Application Conference (COMPSAC'17), pp. 628-636. IEEE, 2017.
- **SecPod: A Framework for Virtualization-based Security Systems**
  Xiaoguang Wang, Yue Chen, Zhi Wang, Yong Qi, Yajin Zhou.
  Proceedings of the 2015 USENIX Annual Technical Conference (USENIX ATC '15).
- **AppSec: A Safe Execution Environment for Security Sensitive Applications**
  Jianbao Ren, Yong Qi, Yuehua Dai, Xiaoguang Wang, Yi Shi.
  Proceedings of the 11th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE). ACM, 2015.
- **ARMlock: Hardware-based Fault Isolation for ARM**
  Yajin Zhou, Xiaoguang Wang, Yue Chen, Zhi Wang.
  Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, 2014.
- **A lightweight VMM on many cores for high-performance computing**
  Yuehua Dai, Yong Qi, Jianbao Ren, Yi Shi, Xiaoguang Wang, and Yu Xuan.
  In ACM SIGPLAN/SIGOPS Internation Conference on Virtual Execution Environment (VEE), pp. 111-120. ACM, 2013.

Google scholar page: `https://scholar.google.com/citations?user=Sy-oJuIAAAAJ&hl=en`

Research Projects

Toward Automatic and Sound Memory Safety Bug Repair   Sep. 2024 - Sep. 2025
- CAHSI-Google Institutional Research Program.
- Role: PI ($80,000; UIC portion: $45,000)

CNS Core: Small: Rethinking Runtime Software Security Hardening in the Context of Hybrid Instruction Set Architecture   Oct. 2021 - Sep. 2024
- US National Science Foundation (NSF).

- Role: Co-PI ($500,000, 50% credit; UIC portion: $69,999)

Popcorn Linux Optimizations: Support for C/POSIX/Glibc, Secure Containers, and Advanced
Security Mechanisms   Aug 1, 2022 - July 31, 2023
- Office of Naval Research (ONR).
- Role: Co-PI ($250,000, 30% credit)

Secure Popcorn Linux   Jun. 2018 - Dec. 2021
- US Office of Naval Research (ONR).
- Role: Lead researcher (system design, software development, and paper writing).

Teaching

- UIC CS 594: Special Topics: Linux Kernel Programming (Spring'24)
- UIC CS 487: Building Secure Computer Systems (Fall'23, Fall'24)

Professional Activities

Students Mentoring:

- Ali Abir Shuvro (Ph.D. student, Aug. 2024 - Now)
- Robert Hernandez (MS student, Oct. 2024 - Now)
- Lily Leith (MS student, Nov. 2024 - Now)
- Himanshu Dongre (Undergrad, May 2024 - Now)
- Arushi Pandey (Undergrad, May 2024 - Now)

Students Mentored:

- Jae-Won Jang (Ph.D. student, Sep. 2021 - May. 2024, Northrop Grumman, MD)
- Filippo Giovanni, Del Nero (MS Thesis, Jan 2024 - May 2024, Politecnico di Milano)
- Simone Mannarino (MS Thesis, Jan 2024 - May 2024, Politecnico di Milano)
- Jaidev Shastri (Ph.D. student, Sep. 2021 - Oct. 2023, Virginia Tech)
- Abilesh Sundarasamy (MEng -> MS Thesis, May. 2022 - Dec. 2023, NVIDIA, CA)
- Mohamed Husain (MEng -> MS Thesis, Sep. 2021 - June 2023, Qualcomm, Austin, TX)
- Abhishek Bapat (MEng -> MS Thesis, May. 2021 - Dec. 2022, Zoox, CA)
- Carlos Bilbao (MS Thesis, Sep 2020 - Dec. 2021, AMD, Austin, TX)
- Abhijit Mahurkar (MEng -> MS Thesis, May. 2020 - Aug. 2021, Analog Devices, Boston, MA)
- Chris Blackburn (MS Thesis, Sep. 2020 - Jul. 2021, Lockheed Martin, Arlington, VA)
- Rob Lyerly (Ph.D. student, Oct. 2018 - May 2019, Facebook/Meta, Boston, MA)
- SengMing Yeoh (MEng -> MS Thesis, Sep. 2018 - Dec. 2020, Amazon AWS, Arlington, VA)

Guest Associate Editor:

- Frontiers in Computer Science (Computer Security Section), 2022 - 2024

Journal Reviewer:

- Future Generation Computer Systems (Elsevier), 2024; IEEE Transactions on Computers, 2023; Frontiers of Computer Science (Springer), 2022; Computing (Springer), 2021; Personal and Ubiquitous Computing (Springer), 2019.

Conference Program Committee Member:

- Artifact Evaluation Committee: USENIX Security 2022, ACM SOSP 2021, USENIX OSDI 2021, ACM SOSP 2019;
- ACM EuroSys 2023 (shadow PC); ACM EuroSys 2022 (shadow PC); IEEE S&P 2021 (shadow PC); IEEE WISA 2019

External Reviewer:

- ACM ASPLOS 2025; ACM SYSTOR 2020; IEEE MASCOTS 2019.

Invited Talks

Transparent, Cross-ISA Enclave Offloading

- SysTEX 2022, Collocated with ASPLOS 2022 Lausanne, Switzerland (remote presentation)

A Framework for Software Diversification with ISA Heterogeneity

- RAID 2020, Donostia/San Sebastian, Spain (online, remote presentation)

Secure Popcorn Linux

- Office of Naval Research (ONR) TPCP 2019 (PI meeting), Boston, MA, USA

Secure the Commodity Applications Against Address Exposure Attacks

- IEEE ISCC 2017, Heraklion, Crete, Greece

SecretSafe: A Lightweight Approach Against Heap Buffer Over-read Attack

- IEEE COMPSAC 2017, Turin, Italy

SecPod: A Framework for Virtualization-based Security Systems

- USENIX ATC 2015, Santa Clara, CA, US.

Transparent Security-Sensitive Process Protection via VMM-Based Process Shadowing

- IEEE COMPSAC Workshop 2013, Kyoto, Japan (remote presentation)

Awards

- NSF CNS Core Grant	Jul. 2021
- USENIX Annual Technical Conference (USENIX ATC 2015) Student travel grant	Jul. 2015
- Department of Computer Science, Florida State University, CS Expo, Best poster award.	Dec. 2013
- Excellent graduate student award at XJTU	Oct. 2012, Oct. 2016
- Outstanding Undergraduate Thesis, NWPU	May. 2010