Meng Xu

Assistant Professor

meng.xu.cs@uwaterloo.ca
https://cs.uwaterloo.ca/~m285xu/
DC 2639, 200 University Ave W, Waterloo, ON, N2L 3G1

Research Interests

My research focuses on **system and software security**, with an emphasis on

- secure-by-design languages (*e.g.*, Rust, Move)
- automated security analysis (*e.g.*, fuzz testing, symbolic execution), and
- runtime defense techniques (*e.g.*, moving target defense, secure hardware).

My research has been applied to identify and address security and privacy issues in *system*, *web*, *mobile*, *IoT*, and *smart contract* applications.

Academic Experience

Assistant Professor, Cheriton School of Computer Science — *Sep 2021 – Present*
University of Waterloo — Waterloo, ON, Canada

Research Scientist, Move Developer Platform Team, — *Sep 2020 – Sep 2021*
Facebook / Novi — Menlo Park, CA, United States

Research Intern, Security, Privacy, and Cryptography Group — *May 2018 - Aug 2018*
Microsoft Research (Advisor: Dr. Marcus Peinado) — Redmond, WA, United States

Research Intern, Infer Team, — *Jan 2018 - Apr 2018*
Facebook — Menlo Park, CA, United States

Visiting Scholar, — *May 2017 - Aug 2017*
CISPA (Advisor: Prof. Michael Backes) — Saarbrücken, Germany

Education

Georgia Institute of Technology, — *Aug 2014 – Jul 2020*
Ph.D., Computer Science (Advisor: Prof. Taesoo Kim) — Atlanta, GA, United States

Nanyang Technological University, — *Aug 2010 – May 2014*
B.Engineering., Computer Science, *First Class Honor* — Singapore
B.Business., Business Administration, *First Class Honor*

PhD Thesis

Finding Race Conditions in Kernels: the Symbolic Way and the Fuzzy Way

The scale and pervasiveness of concurrent software pose challenges for security researchers: race conditions are more prevalent than ever, and the growing software complexity keeps exacerbating the situation — expanding the arms race between security practitioners and attackers beyond memory errors. As a consequence, we need a new generation of bug hunting tools that not only scale well with increasingly larger codebases but also catch up with the growing importance of race conditions.

In this thesis, two complementary race detection frameworks for OS kernels are presented: multi-dimensional fuzz testing and symbolic checking. Fuzz testing turns bug finding into a probabilistic search, but current practices restrict themselves to one dimension only (sequential executions). This thesis illustrates how to explore the concurrency dimension and extend the bug scope beyond memory errors to the broad spectrum of concurrency bugs. On the other hand, conventional symbolic executors face challenges when applied to OS kernels, such as path explosions due to branching and loops. They also lack a systematic way of modeling and tracking constraints in

the concurrency dimension (e.g., to enforce a particular schedule for thread interleavings) The gap can be partially filled with novel techniques for symbolic execution in this thesis.

Publications

Be Careful of What You Embed: Demystifying OLE Vulnerabilities
Yunpeng Tian, Feng Dong, Haoyi Liu, Meng Xu, Zhiniang Peng, Zesen Ye, Shenghui Li, Xiapu Luo, Haoyu Wang
In *Proceedings of the 2025 Annual Network and Distributed System Security Symposium (NDSS)*, February, 2025

SeMalloc: Semantics-Informed Memory Allocator
Ruizhe Wang, Meng Xu, N. Asokan
In *Proceedings of the 2024 ACM Conference on Computer and Communications Security (CCS)*, October, 2024

BliMe Linter
Hossam ElAtali, Xiaohe Duan, Hans Liljestrand, Meng Xu, N. Asokan
In *Proceedings of the 2024 IEEE Secure Development Conference (SecDev)*, October, 2024

SerdeSniffer: Enhancing Java Deserialization Vulnerability Detection with Function Summaries
Xinrong Liu, He Wang, Meng Xu, Yuqing Zhang
In *Proceedings of the 2024 European Symposium on Research in Computer Security (ESORICS)*, September, 2024

uBOX: A Lightweight and Hardware-assisted Sandbox for Multicore Embedded Systems
Xia Zhou, Yujie Bu, Meng Xu, Yajin Zhou, Lei Wu
In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, September, 2024

CO3: Concolic Co-execution for Firmware
Changming Liu, Alejandro Mera, Engin Kirda, Meng Xu, Long Lu
In *Proceedings of the 2024 USENIX Security Symposium (SEC)*, August, 2024

S2malloc: Statistically Secure Allocator for Use-After-Free Protection And More
Ruizhe Wang, Meng Xu, N. Asokan
In *Proceedings of the 2024 Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, July, 2024

AddressWatcher: Sanitizer-Based Localization of Memory Leak Fixes
Aniruddhan Murali, Mahmoud Alfadel, Mei Nagappan, Meng Xu, Chengnian Sun
In *Transactions on Software Engineering (TSE)*, July, 2024

Monarch: A Fuzzing Framework for Distributed File Systems
Tao Lyu, Liyi Zhang, Zhiyao Feng, Yueyang Pan, Meng Xu, Mathias Payer, Sanidhya Kashyap
In *Proceedings of the 2024 USENIX Annual Technical Conference (ATC)*, July, 2024

Research Report: Not All Move Specifications Are Created Equal
Meng Xu
In *Proceedings of the 2024 Workshop on Language-Theoretic Security (LangSec)*, May, 2024

Securing Aptos Framework with Formal Verification
Junkil Park, Teng Zhang, Wolfgang Grieskamp, Meng Xu, Gerardo Di Giacomo, Kundu Chen, Yi Lu, Robert Chen
In *Proceedings of the 2024 International Workshop on Formal Methods for Blockchains (FMBC)*, April, 2024

FuzzSlice: Pruning False Positives in Static Analysis Warnings through Function-Level Fuzzing
Aniruddhan Murali, Noble Mathews, Mahmoud Alfadel, Mei Nagappan, Meng Xu
In *Proceedings of the 2024 International Conference on Software Engineering (ICSE)*, April, 2024

Sense: Enhancing Microarchitectural Awareness for TEEs via Subscription-Based Notification
Fan Sang, Jaehyuk Lee, Xiaokuan Zhang, Meng Xu, Scott Constable, Yuan Xiao, Michael Steiner, Mona Vij, Taesoo Kim
In *Proceedings of the 2024 Annual Network and Distributed System Security Symposium (NDSS)*, February, 2024

Finding Specification Blind Spots via Fuzz Testing
Ru Ji, Meng Xu
In *Proceedings of the 2023 IEEE Symposium on Security and Privacy (Oakland)*, May, 2023

Fast and Reliable Formal Verification of Smart Contracts with the Move Prover
David Dill, Wolfgang Grieskamp, Junkil Park, Shaz Qadeer, Meng Xu, Emma Zhong
In *Proceedings of the 2022 International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, April, 2022
*** EAPLS Best Paper Award**
*** SCP Best Tool Paper Nomination**

Finding Bugs in File Systems with an Extensible Fuzzing Framework
Seulbae Kim, Meng Xu, Sanidhya Kashyap, Jungyeon Yoon, Wen Xu, Taesoo Kim
In *ACM Transactions on Storage (ToS)*, May, 2020

Krace: Data Race Fuzzing for Kernel File Systems
Meng Xu, Sanidhya Kashyap, Hanqing Zhao, Taesoo Kim
In *Proceedings of the 2020 IEEE Symposium on Security and Privacy (Oakland)*, May, 2020

Finding Semantic Bugs in File Systems with an Extensible Fuzzing Framework
Seulbae Kim, Meng Xu, Sanidhya Kashyap, Jungyeon Yoon, Wen Xu, Taesoo Kim
In *Proceedings of the 2019 ACM Symposium on Operating Systems Principles (SOSP)*, October, 2019

Dominance as a New Trusted Computing Primitive for the Internet of Things
Meng Xu, Manuel Huber, Zhichuang Sun, Paul England, Marcus Peinado, Sangho Lee, Andrey Marochko, Dennis Mattoon, Rob Spiger, Stefan Thom
In *Proceedings of the 2019 IEEE Symposium on Security and Privacy (Oakland)*, May, 2019

Stopping Memory Disclosures via Diversification and Replicated Execution
Kangjie Lu, Meng Xu, Chengyu Song, Taesoo Kim, Wenke Lee
In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, October, 2018

QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing
Insu Yun, Sangho Lee, Meng Xu, Yeongjin Jang, Taesoo Kim
In *Proceedings of the 2018 USENIX Security Symposium (SEC)*, August, 2018
*** USENIX Security Best Paper Award**

Precise and Scalable Detection of Double-Fetch Bugs in OS Kernels
Meng Xu, Chenxiong Qian, Kangjie Lu, Michael Backes, Taesoo Kim
In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (Oakland)*, May, 2018

Prevention of Cross-update Privacy Leaks on Android
Beumjin Cho, Sangho Lee, Meng Xu, Sangwoo Ji, Taesoo Kim, Jong Kim
In *Computer Science and Information Systems (ComSIS)*, January, 2018

Checking Open-Source License Violation and 1-day Security Risk at Large Scale
Ruian Duan, Ashish Bijlani, Meng Xu, Taesoo Kim, Wenke Lee
In *Proceedings of the 2017 ACM Conference on Computer and Communications Security (CCS)*, October, 2017

PlatPal: Detecting Malicious Documents with Platform Diversity
Meng Xu, Taesoo Kim
In *Proceedings of the 2017 USENIX Security Symposium (SEC)*, August, 2017

Bunshin: Compositing Security Mechanisms through Diversification
Meng Xu, Kangjie Lu, Taesoo Kim, Wenke Lee
In *Proceedings of the None USENIX Annual Technical Conference (ATC)*, July, 2017

Toward Engineering a Secure Android Ecosystem: A Survey of Existing Techniques
Meng Xu, Chengyu Song, Yang ji, Ming-Wei Shih, Kangjie Lu, Cong Zheng, Ruian Duan, Yeongjin Jang, Byoungyoung Lee, Chenxiong Qian, Sangho Lee, Taesoo Kim
In *ACM Computing Surveys (CSUR)*, August, 2016

UCognito: Private Browsing without Tears
Meng Xu, Yeongjin Jang, Xinyu Xing, Taesoo Kim, Wenke Lee
In *Proceedings of the 2015 ACM Conference on Computer and Communications Security (CCS)*, October, 2015

Teaching Experience

Course Instructor, Software and Systems Security (CS 489/698), *Spring 2023*
University of Waterloo

Course Instructor, Computer Security and Privacy (CS 458/658), *Winter 2023*
University of Waterloo

Course Instructor, Software Security Seminar (CS 858), *Fall 2022*
University of Waterloo

Course Instructor, Computer Security and Privacy (CS 458/658), *Winter 2022*
University of Waterloo

Teaching Assistant, Information Security Lab (CS 6265), *Fall 2015*
Georgia Institute of Technology
Instructor: Prof. Taesoo Kim

Teaching Assistant, Introduction to Information Security (CS 6035), *Spring 2019*
Georgia Institute of Technology
Instructor: Prof. Wenke Lee

Funding

BlackBerry Research Grant (BlackBerry)
CAD $200,000 [50% share] *2023*

CPI + AI Seed Grant (University of Waterloo)
CAD $20,000 [50% share] *2023*

Unrestricted Research Gift (Meta / Novi)
USD $50,000 [100% share] *2022*

Amazon Research Award (Amazon)

USD $60,000 [100% share] *2022*

NGI Assure (NLnet Foundation)
Euro €34,319 [50% share] *2022*

Discovery Grant (NSERC)
CAD $170,000 [100% share] *2022*

Discovery Launch Supplement (NSERC),
CAD $12,500 [100% share] *2022*

Start-up Grant (University of Waterloo)
CAD $120,000 [100% share] *2021*

Professional Service

PC Member
The Network and Distributed System Security Symposium (NDSS) *2024*
International Symposium on Research in Attacks, Intrusions and Defenses (RAID) *2023*
IEEE Conference on Dependable and Secure Computing (DSC) *2022*
ACM Conference on Computer and Communications Security (CCS) *2018*

Shadow PC Member
IEEE Symposium on Security and Privacy (Oakland) *2018*
European Conference on Computer Systems (EuroSys) *2018*

External Reviewer
Network and Distributed System Security Symposium (NDSS) *2018, 2019, 2020*
IEEE Symposium on Security and Privacy (Oakland) *2019*
ACM Conference on Computer and Communications Security (CCS) *2015, 2017, 2019*
USENIX Security Symposium (Security) *2015, 2018*
USENIX Annual Technocal Conference (ATC) *2017, 2018*
IEEE International Conference on Distributed Computing Systems (ICDCS) *2017*

Journal Reviewer
IEEE Transactions on Dependable and Secure Computing (TDSC) *2020*
Computers & Security *2016*

Invited Talks

Finding Race Conditions in Kernels: the Symbolic Way and the Fuzzy Way
University of Waterloo *Jan 2020*
University of Santa Barbara *Feb 2020*
Purdue University *Feb 2020*
Simon Fraser University *Feb 2020*
CISPA, Saarland University *Feb 2020*
Microsoft Research, Redmond *Mar 2020*
Rutgers University *Mar 2020*
ETH Zurich *Mar 2020*
National University of Singapore *Apr 2020*

Precise and Scalable Detection of Double-Fetch Bugs in Kernels
Facebook *Apr 2018*
Baidu USA *Apr 2018*
Microsoft Research *Jul 2018*
Internet Security Conference *Sep 2018*
Chinese Academy of Sciences *Sep 2018*

Purdue University, CERIAS Security Seminar *Oct 2018*

Security through Multi-Layer Diversity
CISPA, Saarland University *Jun 2017*

UCognito: Private Browsing without Tears
Ionic Security *Apr 2016*
Georgia Tech, Cybersecurity Lecture Series *Sep 2015*

Open Source Contributions

Linux kernel: for patching double-fetch bugs in drivers, filesystems, and scheduler.
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git

FreeBSD kernel: for patching double-fetch bugs in networking stack.
https://svnweb.freebsd.org

Facebook Infer: for scaling it to the whole Facebook codebase.
https://github.com/facebook/infer

Hydra: an extensible fuzzing framework for finding semantic bugs in file systems.
https://github.com/sslab-gatech/hydra

Deadline: a precise and scalable double-fetch detector written as an LLVM pass.
https://github.com/sslab-gatech/deadline

PlatPal: a malicious PDF detector based on platform diversity.
https://github.com/sslab-gatech/platpal

Bunshin: an efficient N-version execution engine with multi-threading support.
https://github.com/sslab-gatech/bunshin

UCognito: an universal implementation of private browsing mode for browsers and more.
https://github.com/sslab-gatech/ucognito

Playcrawl: a GooglePlay app crawler with supporting for crawling old app versions
https://github.com/sslab-gatech/playcrawl

Awards & Scholarships

EAPLS Best Paper Award *2022*
USENIX Security Distinguished Paper Award *2018*
Atlanta Startup Battle 1st Place *2018*
Georgia Tech IISP Cybersecurity Demo Day Winner *2018*
Georgia Tech IISP Cybersecurity Demo Day Finalist *2016*
Singapore MOE Scholarship for Undergraduate Studies *2010 – 2014*

References

Dr. Taesoo Kim (advisor)
Catherine M. and James E. Allchin Early Career Associated Professor, +1 404-385-2934
School of Computer Science, taesoo@gatech.edu
Georgia Institute of Technology https://taesoo.gtisc.gatech.edu

Dr. Wenke Lee
Professor and John P. Imlay Jr. Chair, +1 404-385-2879
School of Computer Science, wenke@cc.gatech.edu

Georgia Institute of Technology http://wenke.gtisc.gatech.edu

Dr. Michael Backes
Professor, Chair of Information Security & Cryptography, +49 (0)681-302-3249
Computer Science Department, backes@cs.uni-saarland.de
Saarland University https://www.infsec.cs.uni-saarland.de/~backes/

Dr. Marcus Peinado
Architect, +1 206-349-1619
Security, Privacy, and Cryptography Group, marcuspe@microsoft.com
Microsoft Research https://www.microsoft.com/en-us/research/people/marcuspe/