Ruizhe Wang

🌐 https://ruizhe-w.github.io ✉ ruizhe.wang@uwaterloo.ca Ⓖ Google Scholar

EDUCATION

University of Waterloo
Ph.D. in Computer Sciences *Sep. 2024 – Aug. 2028*
- **Supervisor**: Meng Xu, N. Asokan

University of Waterloo
M.Math in Computer Sciences *Sep. 2022 – Aug. 2024*
- **Supervisor**: Meng Xu, N. Asokan

University of Wisconsin-Madison
B.S. in Computer Sciences (honor) and Mathematics; GPA: 4.0/4.0 *Sep. 2019 – Dec. 2021*
- **Advisor**: Earlence Fernandes

Beijing Institute of Technology
The Internet of Things Engineering (honor); GPA: 91.5/100 (1/31) *Sep. 2017 – June 2019*

RESEARCH EXPERIENCES

Graduate Research Assistant, University of Waterloo *Sep. 2022 – Present*
- Conduct research about system security

Visiting Scholar, Max Planck Institute for Software Systems *May 2022 – Sep. 2022*
- Conduct research about human factor security under the supervision of Dr. Elissa M. Redmiles.

Research Assistant, UW-Madison Security and Privacy *Nov. 2019 – Dec. 2021*
- Conduct research about the Cyber-Physical System (CPS) Security.

Software Development Engineer Intern, Amazon *May 2020 – Aug. 2020*
- Co-Implemented a serverless application to increase Amazon package delivery efficiency by automatically providing rescue plans for delayed packages using Typescript and Java.
- Deployed the application on AWS and created four RESTful APIs using Google Guice and AWS CDK
- Fully tested the service with Mockito and JUnit and created AWS Metrics dashboards and thresholds that can automatically fire alarms.

Artifact Evaluation PC, ACM MobiSys *2023*

External Reviewer, IEEE Internet of Things Journal (IoT-J) *2021*

PUBLICATIONS

Ruizhe Wang, Roberta De Viti, Aarushi Dubey, and Elissa M. Redmiles. The role of privacy guarantees in voluntary donation of private health data for altruistic goals. In *Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2026.

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

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

Ruizhe Wang, Angelica Goetzen, Elissa M. Redmiles, Savvas Zannettou, and Oshrat Ayalon. Likes and fragments: Examining perceptions of time spent on tiktok. *arXiv preprint*, 2023.

Yunang Chen, Amrita Roy Chowdhury, **Ruizhe Wang**, Andrei Sabelfeld, Rahul Chatterjee, and Earlence Fernandes. Data privacy in trigger-action iot systems. *IEEE Symposium on Security and Privacy (Oakland)*, 2021.

Yuzhe Ma, Jon Sharp, **Ruizhe Wang**, Earlence Fernandes, and Xiaojin Zhu. Sequential attacks on kalman filter-based forward collision warning systems. *The Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI)*, 2020.

SELECTED RESEARCH PROJECTS

Semantic-Based Typing System   *Sep. 2024 – Present*
○ Co-proposed a semantic-based typing system for development assistance and bug-finding.

User Perception on Privacy Enhancement Technologies   *May 2022 – Aug. 2025*
○ Conducted a vignette survey to assess U.S. participants' willingness to donate medical data for research, examining the impact of four PETs: data expiration, anonymization, purpose restriction, and access control.
○ Highlight the limited effect of presenting PETs and show the potential of audit transparency on user perceptions.

Use-After-Free Targeted Secure Memory Allocator   *Sep. 2022 – Aug. 2024*
○ Co-proposed a "type"-based memory allocation scheme that segregated objects allocated through different call sites or call stacks to restrict type confusion.
○ Co-developed an entropy-based memory allocator that detects failed attack attempts and limits the reuse of dangling pointers, thereby preventing attackers from repeatedly launching entropy-reducing attacks.

Data Privacy in Trigger-Action Platforms   *Sep. 2019 – Apr. 2020*
○ Co-Proposed a protocol in Trigger-Action Platforms (TAPs) using Garbled Circuits that can avoid leaking sensitive information when the trigger or the platform is compromised.
○ Evaluated the efficiency of the new protocol on the rules of popular commercial TAPS (IFTTT & Zapier) using Python Flask. Showed that more than 90% of the top-500 frequency rules are supported while the latency and throughput reduced less than 60%.

HONORS & AWARDS

Honors

2025	**WiM Mentorship Award**, University of Waterloo	*Waterloo, ON*
2024	**WiM Mentorship Award**, University of Waterloo	*Waterloo, ON*
2024 - 26	**Government of Ontario - Canada Foundation for Innovation - Bell Emergis Scholarship**, University of Waterloo	*Waterloo, ON*
2024	**Graduate Conference Funding**, University of Waterloo	*Waterloo, ON*
2023	**CISPA Travel Grant**, CISPA Helmholtz Center for Information Security	*Germany*
2022 - 24	**David R. Cheriton Scholarship**, University of Waterloo	*Waterloo, ON*
2020	**Honorable Mention**, Computing Research Association (CRA) Outstanding Undergraduate Researcher Award	*Madison, WI*
2020	**DeWitt Scholarship**, UW-Madison	*Madison, WI*
All Sems.	**Deans List**, College of L&S, UW-Madison	*Madison, WI*
2018	**First-Class Academic Excellence Scholarship(10%)**, BIT	*Beijing, China*

Contest Awards

2021	**4th Place (4/90)**, ACM ICPC NCNA Regional Contest	*Madison, WI*
2018	**3rd Place (3/369)**, Freshman Programming Contest at BIT	*Beijing, China*
2017	**2nd Prize (10%)**, Lssec Techall BIT Programming Contest	*Beijing, China*

OTHER EXPERIENCES

Valedictorian Selection Committee, Faculty of Math   *2025*

Executive Member, Computer Science Graduate Student Association   *2024 – Present*

Technical Consultant, Tech Clinic   *2020 – 2021*

Volunteer Instructor, Charity Primary School   *2019*