

Xi Tan

Cyber building A-120J
University of Colorado Colorado Springs
Colorado Springs, CO, 80918

E-mail: xtan4@uccs.edu
Homepage: mintancy.github.io

EDUCATION

<i>Ph.D.</i> , Computer Science and Engineering, University at Buffalo, Buffalo, NY, USA	2024
<i>M.S.</i> , Computer Technology, Institute of Information Engineering, UCAS, Beijing, China	2019
<i>B.S.</i> , Computer Science and Technology, Jilin University, Changchun, China	2016

PROFESSIONAL EXPERIENCE

<i>Assistant Professor, SUNRISE Lab, University of Colorado Colorado Springs</i>	<i>August 2024 – Present</i>
• Research Topics: Systems and Software Security	
<i>Graduate Research Assistant, Cacti Lab, University at Buffalo</i>	<i>August 2020 – June 2024</i>
• Systematically analyzing the security of ARM Cortex-M-based embedded systems; enforcing control-flow integrity on embedded systems; discovering new attack surfaces on Cortex-M architecture.	
<i>Course Instructor, Department of Computer Science and Engineering, University at Buffalo</i>	<i>Fall 2023</i>
• Taught CSE 565 Computer Security, a core graduate-level course.	
<i>Graduate Research Assistant, Cacti Lab, Rochester Institute of Technology</i>	<i>August 2019 – August 2020</i>
• Built background on ARM Cortex-M architecture and compartmentalization approaches.	
<i>Graduate Research Assistant, Institute of Information Engineering</i>	<i>August 2016 – June 2019</i>
• Virtual machine introspection based malware detection.	

PUBLICATIONS (* co-first author)

1. Zheyuan Ma, Gaoxiang Liu, Alex Eastman, Kai Kaufman, Md Armanuzzaman, **Xi Tan**, Katherine Jesse, Robert Walls, and Ziming Zhao. “We just did not have that on the embedded system: Insights and Challenges for Securing Microcontroller Systems from the Embedded CTF Competitions”. *Accepted at ACM Conference on Computer and Communications Security (CCS) 2025*.
2. Zheyuan Ma*, **Xi Tan***, Lukasz Ziarek, Ning Zhang, Shambhu Upadhyaya, Hongxin Hu, and Ziming Zhao. “Exploring and Mitigating Cross-state Control-flow Hijacking Attacks on ARM Cortex-M TrustZone”. *IEEE Transactions on Information Forensics and Security Search form Search (TIFS) 2025*.
3. **Xi Tan**, Zheyuan Ma, Sandro Pinto, Le Guan, Ning Zhang, Jun Xu, Zhiqiang Lin, Hongxin Hu, and Ziming Zhao. “SoK: Where’s the up?! A Comprehensive (bottom-up) Study on the Security of Arm Cortex-M Systems”. *USENIX WOOT conference on offensive technologies (WOOT), 2024*. [code link].
4. Ziming Zhao, Md Armanuzzaman, **Xi Tan**, and Zheyuan Ma. “Trusted Execution Environments in Embedded and IoT Systems: A CactiLab Perspective.” *Symposium on Secure and Private Execution Environment Design (SEED), 2024*.
5. Yujie Wang, Cailani Lemieux Mack, **Xi Tan**, Ning Zhang, Ziming Zhao, Sanjoy Baruah, and Bryan C. Ward, InsectACIDE: Debugger-Based Holistic Asynchronous CFI for Embedded System, *IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2024*. H5-index: 25.

6. **Xi Tan**, Sagar Mohan, Md Armanuzzaman, Zheyuan Ma, Gaoxiang Liu, Alex Eastman, Hongxin Hu, and Ziming Zhao. “The Canary is Dead: On the Effectiveness of Stack Canaries on Microcontroller-based Systems”. *ACM/SIGAPP Symposium On Applied Computing (SAC) 2024*. H5-index: 37.
7. **Xi Tan** and Ziming Zhao. “SHERLOC: Secure and Holistic Control-Flow Violation Detection on Embedded Systems”. *ACM Conference on Computer and Communications Security (CCS) 2023*. Acceptance rate: $234/1222 = 19.16\%$. [code link]. H5-index: 90.
8. Zheyuan Ma, **Xi Tan**, Lukasz Ziarek, Ning Zhang, Hongxin Hu, and Ziming Zhao. “Return-to-Non-Secure Vulnerabilities on ARM Cortex-M TrustZone: Attack and Defense”. *ACM/IEEE Design Automation Conference (DAC) 2023*. Acceptance rate: $263/1156 = 22.7\%$. [code link]. H5-index: 56.
9. Dissertation. **Xi Tan**. Control-Flow Security for Microcontroller-Based Systems. State University of New York at Buffalo, 2024
10. Patent. Bibo Tu, **Xi Tan**, and Kun Zhang. “Methods and System for Detecting Malware Behavior of Virtual Machine”. *Beijing: CN109597675A, 2019-04-09*.

PRESENTATIONS

- Research talk at US CYBER COMMAND Tech Talk on the topic: “A Landscape of Security in Embedded Systems” Spring 2025
- Research talk at USENIX WOOT on the topic: “SoK: Where’s the up?! A Comprehensive (bottom-up) Study on the Security of ARM Cortex-M Systems” 2024
- Poster presentation @ *Great Lake Security Day (GLSD)* Spring 2023
 - A Peak of the Security Landscape of Cortex-M Based Systems.
- Poster presentation @ *Great Lake Security Day (GLSD)* Winter 2021
 - Practical Control-Flow Integrity Enforcement on IoT Devices.
- Invited Talk @ *UB CSE 501 course*: Security landscape on embedded systems. Fall 2022
- Invited Talk @ *UB CSE 501 course*: Embedded Capture the Flag (eCTF). Fall 2021
- Research-in-progress presentation at Secure Knowledge Management (SKM) conference. Fall 2021

TEACHING

- CS 5220 Computer Communication. Graduate level. Fall 2024/2025
- CS 4910 Intro to Computer Security. Undergraduate level. Spring 2025
- CS 2160 Comp Organization and Assembly Language. Undergraduate level. Spring 2025

MENTORSHIP

- At UCCS:
 - Aryan Padiyal (PhD student) Spring 2025 - present
Project: Enhancing memory safety on embedded systems
 - Mentored eCTF competition 2025 Spring 2025
- At UB:
 - Sagar Mohan (master’s, now PhD student at NEU) 2024 - Spring 2025
Project: Efficient shadow stack on embedded systems
 - Zheyuan Ma (PhD student) 2023 - 2024
Project: Attack and defense on Cortex-M based embedded systems
 - Junzhe Li (undergraduate, now master’s student at CMU) 2023
Project: Enhancing control-flow integrity on embedded systems

PROFESSIONAL SERVICES

- *Leading service:* Lead the UCCS Hacking Training every other Friday. Fall 2025 - present
- *Committee Member:*
 - UCCS PhD Cybersecurity program. 2024 - present
 - UCCS Colorado Cybersecurity Scholarship Summer 2025
 - UCCS College of Engineering and Applied Sciences Scholarship Spring 2025
 - USENIX Security Artifact Evaluation 2022, 2023
- *Conferences Review:* USENIX Annual Technical Conference (USENIX ATC'2024), IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom 2024, 2025), ACM Internet Measurement Conference (IMC 2026)
- *Journals Review:* Information Systems Frontiers (2022), Organizational Cybersecurity Journal Practice, Process and People (2025), ACM Transactions on Cyber-Physical Systems (TCPS 2024), IEEE Transactions on Dependable and Secure Computing (TDSC 2024, 2025)
- *Volunteer:*
 - Served as a mentor for CyberTruck Challenge event Jun. 2025
 - NSF Panels Review 2024
 - Attended VehicleSec workshop co-located with NDSS as a volunteer Feb. 2023