Xi Tan

Cybersecueirty Center
University of Colorado Colorado Springs
Colorado Springs, CO, 80918

E-mail: xtan4@uccs.edu
Homepage: mintancy.github.io/team/xitan.html
Ph: (719)-255-3492

EDUCATION

Ph.D, Computer Science and Engineering — University at Buffalo, Buffalo, NY, USA
- Advisor: Zimng Zhao — August 2020 - June 2024

Ph.D Student, Computer and Information Sciences — Rochester Institute of Technology, NY, USA
- Advisor: Ziming Zhao — August 2019 - August 2020

M.S., Computer Technology — Institute of Information Engineering, CAS, Beijing, China
- Advisor: Bibo Tu — August 2016 - June 2019

B.S., Computer Science and Technology — Jilin University, Changchun, China — June 2016

PROFESSIONAL EXPERIENCE

Assistant Professor, University of Colorado Colorado Springs — August 2024 – Present
- Research interests: Systems and Software Security

Graduate Research Assistant, Cacti Lab, University at Buffalo — August 2020 – June 2024
- Systematically analyzing the security of Arm Cortex-M-based embedded systems; enhancing memory safety on embedded systems; discovering new attack surfaces on Cortex-M architecture.

Course Instructor, Department of Computer Science and Engineering, University at Buffalo — Fall 2023
- Taught CSE 565 Computer Security, a core graduate course with an enrollment of 58 students.

Graduate Research Assistant, Cacti Lab, Rochester Institute of Technology — August 2019 – August 2020
- Built background on Arm Cortex-M architecture and compartmentalization approaches.

Graduate Research Assistant, Institute of Information Engineering — 2016 – 2019
- Virtual machine introspection based malware detection.

PUBLICATIONS

1. **Xi Tan**, Zheyuan Ma, Sandro Pinto, Le Guan, Ning Zhang, Jun Xu, Zhiqiang Lin, Hongxin Hu, Ziming Zhao. "Where's the" up"?! A Comprehensive (bottom-up) Study on the Security of Arm Cortex-M Systems". *USENIX WOOT Conference on Offensive Technologies, 2024.* [*code link*]
2. Ziming Zhao, Md Armanuzzaman, **Xi Tan**, and Zheyuan Ma. "Trusted Execution Environments in Embedded and IoT Systems: A CactiLab Perspective". *IEEE International Symposium on Secure and Private Execution Environment Design (SEED), 2024.*
3. 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". *EEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2024.*
4. **Xi Tan**, Sagar Mohan, Md Armanuzzaman, Zheyuan Ma, Gaoxiang Liu, Alex Eastman, Hongxin Hu, and Ziming Zhao. "Is the Canary Dead? On the Effectiveness of Stack Canaries on Microcontroller-based Systems". *ACM/SIGAPP Symposium On Applied Computing (SAC) 2024.*
5. **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*]

6. 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*]
7. Wenlin Yang, **Xi Tan**, Junchen Guo, Shuo Wang. "The Vulnerability Analysis and Security Enhancement of Docker". *Information Security and Technology 4, 2016.*

PATENT

1. Bibo Tu, **Xi Tan**, Kun Zhang. "Methods and System for Detecting Malware Behavior of Virtual Machine". *Beijing: CN109597675A, 2019-04-09.*

SELECTED AWARDS AND HONORS

- Won the 2nd place at Russell L. Agrusa CSE Student Innovation Competition @ UB 2023.12
- MITRE eCTF, team member of Cacti @ UB 2023
  - Ranked 4 among 60 teams. Developed a secure key fob system for car door locks, safeguarding against unauthorized access, replay attacks, and key fob duplication. [*code link*]
- MITRE eCTF, team captain of Cacti @ UB 2022
  - Ranked 5 among 28 teams. Designed a secure firmware update and bootloader for an avionic device, safeguarding intellectual property and mission secrets against untrusted environments and supply-chain threats like hardware trojans. [*code link*]
- MITRE eCTF, team captain of Cacti @ UB 2021
  - Ranked 9 at final among 20+ teams in MITRE eCTF. Best write-up award. Designed a secure communication system for an unmanned aerial vehicle (UAV) package delivery, safeguarding against unauthorized network access and disruptions. [*code link*]
- MITRE eCTF, team member of Cacti @ UB 2020
  - Ranked 6 at final among 20+ teams. Developed a secure audio digital rights management (DRM) module for a Digilent Cora Z7 multimedia player, ensuring protection against piracy, region restrictions, and cloned device production. [*code link*]
- Merit student at Institute of Information Engineering, Chinese Academy of Sciences 2017

TRAVEL GRANTS

- 2024 Travel Grants at WOOT 2024 (Aug. 12-13, Philadelphia)
- 2023 Grants at DAC Young Fellow program 2023 (Jul. 9-13, San Francisco)
- 2023 Travel grants at NDSS VehicleSec workshop 2023 (Feb. 27, San Diego).
- 2021 Travel Grants at CCS iMentor 2021 (Nov. 14-19, virtual)
- 2021 Travel grants at NDSS 2021 (Feb. 21-25, virtual).
- 2020 Travel grants at USENIX Security 2020 (Aug. 12-14, virtual).
- 2020 Travel grants at CODASPY CyberW 2020 (Mar. 18, virtual).

PROFESSIONAL SERVICES

- *PC Member*: IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom), USENIX Annual Technical Conference (USENIX ATC), ACM Transactions on Cyber-Physical Systems 2024
- *Student Advising and Mentoring*: Junzhe Li (undergraduate), Sagar Mohan (master) 2023
- *Artifact Evaluation Committee Member, USENIX Security* 2022 – 2023
- *Young Fellows Program Participant, DAC* Jul. 2023
- *Student Volunteer, VehicleSec, NDSS Workshop* Feb. 2023
- *CTF Training, University at Buffalo/Rochester Institute of Technology* 2019 – 2022
- *External Reviewer*: IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom), IEEE Conference on Communications and Network Security (CNS), Redesign Industrial Control Systems with Security (RICSS), IEEE Latin America Transactions, IEEE International Conference on Application-specific Systems, Architectures, and Processors (ASAP), ACM Conference on Data and Application Security and Privacy (CODASPY), IEEE Acess.

PRESENTATIONS

- 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
- **Presentation**: Research-in-progress presentation at SKM. Fall 2021

INTERESTS

calligraphy, drawings, novels, poets, and tech blogs