Shengye Wan

Email : swan@email.wm.edu

Personal Website

Mobile : +1-757-603-5379

Education

- **College of William and Mary** — Williamsburg, VA
  M.S. / Ph.D. Program, advised by Dr. Kun Sun (GPA: 3.85/4.00) — Aug. 2014 – Aug. 2020
  - **Ph.D. in Computer Science, Aug. 2014 – August 2020**:
    - **Dissertation**: Hardware-Assisted Security Mechanisms on ARM-Based Multi-Core Processors
  - **M.S. in Computer Science, Aug. 2014 – May 2016**:
    - **Thesis**: Protecting Web Contents Against Persistent Crawlers
- **Huazhong University of Science and Technology** — Wuhan, China
  B.Eng. in Software Engineering, advised by Dr. Zhongping Qin — Sept. 2010 – June 2014

Experience

- **Facebook, Inc.** — Menlo Park, CA
  Research Scientist — Oct. 2020 - Now
- **George Mason University** — Fairfax, VA
  Research Assistant Part-Time — Oct. 2019 - July 2020
  - [**Mobile Security**] **Securing In-Band Remote Control Channels on Untrusted Mobile Devices**:
    - Use TrustZone to provide a secure remote channel for the mobile device even when its rich OS is compromised
    - Propose the mechanism for deploying two isolated drivers on one shared NIC and protecting one driver with TrustZone
    - Language & tools: C, Python, iPerf
- **Facebook, Inc.** — Menlo Park, CA
  Software Engineer Intern, Product Security Team — July 2019 - Sept. 2019
  - **Enhancing Facebook Android Application Security**:
    - Android WebView related security issues finding and fixing
    - Language & tools: Java, IntelliJ IDEA
- **Baidu USA** — Sunnyvale, CA
  Security Research Intern — Jan. 2019 - July 2019
  - **Developing the Rust SDK for ARM TrustZone architecture**:
    - Provide the first complete Rust-safe GlobalPlatform APIs for developing TrustZone-based trusted applications
    - Open-source GitHub project: *rust-optee-trustzone-sdk*
    - Language & tools: Rust, C, OP-TEE OS
- **College of William and Mary** — Williamsburg, VA
  Research and Teaching Assistant — Jan. 2015 - Jan. 2019
  - [**Multi-Core Security**] **Scheduling TrustZone-Based Asynchronous Introspection on Multi-core Processors**:
    - Propose a technique for the untrusted OS to collect the running information of TrustZone-based software
    - Propose a rootkit with above technique to conduct a TOCTTOU attack on TrustZone-based asynchronous introspection
    - Propose an introspection mechanism in TrustZone to defeat the above rootkit
  - [**Network Security**] **Detection of Persistent Distributed Crawlers**:
    - Apply SVM-based machine learning detection with 6 proposed new features to detect persistent web-page crawlers
    - Language & tools: C, Python, PHP, LIBSVM, Scrapy, CodeIgnitor

Technical Skills

Programming Languages: (Proficient) C, Rust, Java, Python; (Familiar) ARM Assembly Language, C++, SQL
System, Frameworks and Tools: ARM TrustZone, Git, Linux Kernel, Android, LIBSVM, CodeIgnitor

Publications

S. Wan, M. Sun, K. Sun, N. Zhang, and X. He. RusTEE: Developing Memory-Safe ARM TrustZone Applications. To appear in Annual Computer Security Applications Conference (ACSAC), 2020.
J. Wang, K. Sun, L. Lei, **S. Wan**, Y. Wang, and J. Jing. Cache-in-the-Middle (CITM) Attacks : Manipulating Sensitive Data in Isolated Execution Environments. To appear in ACM Conference on Computer and Communications Security (CCS), 2020.
S. Wan, J. Sun, N. Zhang, K. Sun, and Q. Li. "SATIN: A Secure and Trustworthy Asynchronous Introspection on Multi-Core ARM Processors". In proceedings of IEEE DSN 2019 (received DSN 2019 Student Travel Award).
S. Wan, Y. Li, and K. Sun. "Protecting Web Contents against Persistent Distributed Crawlers". In Proceedings of IEEE ICC 2017.