Arslan Khan

Website: https://arslan8.github.io/
Email: arslankhan52@gmail.com

Research Interests

My research interests lie in the general area of systems and security. In particular, I am interested in embedded systems security, operating systems and trusted/confidential computing.

Education

Purdue University — West Lafayette, USA
Ph.D. in Computer Science, Advisors: Dongyan Xu and Dave Jing Tian — 2018–2023

University of Engineering and Technology — Lahore, Pakistan
B.S. in Electrical Engineering — 2011–2015

- Thesis: "Design and Implementation of Data Handling Unit for Microsatellites"

Experience

FRIENDS Lab and PURSEC Lab
Postdoctoral Researcher — 2023-Current

- Exploring different approaches for making robust Confidential/Trusted Computing Infrastructure and secure embedded systems.

FRIENDS Lab and PURSEC Lab
Graduate Research Assistant — 2018-2023

- Exploring different approaches for making robust Confidential/Trusted Computing Infrastructure and secure embedded systems.

Qualcomm
Interim Engineering Intern - Secure Software Group (SSG) — Summer 2022, 2023

- Worked on enhancing Qualcomm's Trusted Execution Environment solutions, such as Qualcomm Trusted Execution Environment (QTEE) and Trust Management Engine (TME)

Siemens (Formerly Mentor Graphics)
Senior Software Engineer - Virtualization and Kernel Team — 2015-2018

- Worked on the design and development of Nucleus Hypervisor and Nucleus RTOS Kernel 4.0.
- Worked on integration of Global Platform (GP) API for Nucleus Hypervisor for ARM TrustZone-enabled devices.
- Worked on the paravirtualization of different guest OS, such as Embedded Linux, including design and implementation of different virtual devices, such as the virtio network device.
- Worked on various architecture and platform ports for Nucleus Hypervisor and Nucleus RTOS.

Al-Khwarizmi Institute of Computer Science (KICS)
Intern - RF Lab — Summer 2014

- Fabrication and programming of motor driver cards and motherboards for Heliostats.

Publications

[KXT23a] **Arslan Khan**, Dongyan Xu, and Dave Jing Tian. "EC: Embedded Systems Compartmentalization via Intra-Kernel Isolation". In: *2023 IEEE Symposium on Security and Privacy (S&P)*. 2023.

[KXT23b] **Arslan Khan**, Dongyan Xu, and Dave Jing Tian. "Low-Cost Privilege Separation with Compile Time Compartmentalization for Embedded Systems". In: *2023 IEEE Symposium on Security and Privacy (S&P)*. 2023.

[Kha+23] **Arslan Khan**, Muqi Zou, Kyungtae Kim, Dongyan Xu, Antonio Bianchi, and Dave Jing Tian. "Fuzzing SGX Enclaves via Host Program Mutations". In: *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. 2023.

[Kha+21a] **Arslan Khan**, Joseph I. Choi, Dave Jing Tian, Tyler Ward, Kevin R. B. Butler, Patrick Traynor, John M. Shea, and Tan F. Wong. "Privacy-Preserving Localization using Enclaves". In: *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. **Best Presentation Award**. 2021, pp. 0269–0278.

[Kha+21b] **Arslan Khan**, Hyungsub Kim, Byoungyoung Lee, Dongyan Xu, Antonio Bianchi, and Dave Jing Tian. "M2MON: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles." In: *USENIX Security Symposium*. 2021, pp. 285–302.

Under Submission:

1. "D-Helix: A Decompiler Testing Framework using Symbolic Differentiation" Muqi Zou, **Arslan Khan**, Ruoyu Wu, Antonio Bianchi, Dave Jing Tian. USENIX Security 2024

2. "DnD2: Decompiling Deep Neural Networks (DNN) from embedded firmware using dynamic analysis" Ruoyu Wu, **Arslan Khan**, Muqi Zou, Dave Jing Tian, Antonio Bianchi USENIX Security 2024

3. "SAIN: State-Aware Invariants to Mitigate ICS Invariants Attack Insensitivity" Syed Ghazanfar Abbas, Muslum Ozgur, Abdulellah Abdulaziz M Alsaheel, **Arslan Khan**, Berkay Celik, Dongyan Xu USENIX Security 2024

Scholarships and Awards

- MVP for CyberTruck 2023 CTF (Robert Bosch Team) 2023
- Outstanding Service to the Department of Computer Science, Purdue University 2023
- Andrews Fellowship, Purdue University Graduate School. 2018–2020
- Role Model, Focal Review at Siemens. 2016

Professional Services

- Artifact Evaluation Committee (AEC): USENIX Security 2022, EuroSys 2023, CCS 2024
- External Reviewer:
  - USENIX Security 2023-24
  - IEEE S&P 2021
  - NDSS 2021, 2024

Engagement, Diversity, and Outreach Activities

- Lead Graduate Student - PURSEC Lab 2020–Current
  Organized the security reading group at Purdue and research logistics for PURSEC.
- President - Computer Science Graduate Student Association 2022–Current
  Organized different activities for the graduate student association
- Ombudsperson - Computer Science Department Fall 2018 - Current
  Part of the Ombuds Services program at Purdue Graduate School
- Diversity Coordinator
  Part of the Diversity Task Force at Purdue CS
- Faculty Search Committee Representative
  Part of the faculty search/recruitment process at Purdue CS.