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

- Thesis: "Securing resource-constrained devices using low-cost solutions."

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

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

Professional 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

- Added software fault isolation capabilities to GCC and tested the new extensions with Ardupilot to create an IO-level monitor.
- Worked on compiler frontend (clang) and LLVM to develop new language extensions for C language to achieve compile-time isolation. Additionally, ported Zephyr and FreeRTOS to the work with the new language extensions.
- Extended AFLplusplus to create a program mutation-based fuzzer. Additionally, developed a library OS to rehost Intel SGX enclaves on commodity machines, enabling Intel SGX enclave fuzzing on commodity machines.
- Explored hardware debug architecture to create a high-speed reference monitor for ARM M profile-based embedded systems. Additionally, formally verified the reference monitor using VeriFast.
- Reverse engineered hardware acceleration of various machine learning frameworks, such as Apache TVM, TensorFlow Lite, OpenVX, etc. to extract machine learning models used by accelerators on 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.

Teaching Experience.

Guest Lectures:

- **CS52700 (Software Security):** Gave lecture on Software Compartmentalization. (Class taught by Dr. Antonio Bianchi)
- **CS59200-TCC (Trusted and Confidential Computing):** Class lead, lead discussions for various topics. (Class taught by Dr. Dave (Jing) Tian)
- **CS 590 (IoT/CPS Security):** Gave guest lecture on Trusted and Confidential Computing (TCC). (Class taught by Dr. Berkay Celik)

Publications

[Zou+24] Muqi Zou, **Arslan Khan**, Ruoyu Wu, Han Gao, Antonio Bianchi, and Dave (Jing) Tian. "D-Helix: A Generic Decompiler Testing Framework Using Symbolic Differentiation". In: *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024.

[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+21] **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. "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
2. "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
- Program Committee Member:
  - IEEE/ACM Workshop on the Internet of Safe Things (2024).

Mentoring Experience.

Pursec Mentees:

Graduate Researchers:

- **Muqi Zou (PhD):** (PhD Purdue University)
  Project: Fuzzing SGX programs using program mutations
- **Arushi Arora (PhD):** (PhD Purdue University)
  Project: Securing TOR networks using trusted computing.
- **Syed Ghazanfar Abbas (PhD):** (PhD Purdue University)
  Project: Securing industrial control systems using compartmentalization and invariant enforcement.

Undergraduate Researchers:

- **Seunghyun Yeo (Victor) (SNU):**
  Project: Architecture-independent enclave Migration using Open Enclave.
- **Sai Raj Karra (Software Engineer at Apple):**
  Project: Fingerprinting Linux kernel using trusted execution.
- **Joseph Hsu (Computer Scientist at Air Force Research Lab):**
  Project: Dynamic firmware analysis using ARM Coresight.
- **Jack Xiang (Passion Fin):**
  Project: Fingerprinting Linux kernel using trusted execution.

Purdue CSGSA Mentees:

2022:

- **Li, Lixiang (PhD):** PhD Purdue University
- **Chen, Xuan (PhD):** PhD Purdue University

- **Sree Sai Ankit Rao Pittala (MS):** MS Purdue University
- **Devin Attila Ersoy (MS):** MS Purdue University (Interned at Signify)
- **Rucha Shrikant Deshpande(MS):** MS Purdue University
- **Terzoglou, Athina (PhD):** PhD Purdue University
- **Basile, Dante John Artas (PhD):** PhD Purdue University
- **Luo, Xinyu (PhD):** PhD Purdue University

2021:

- **Janani Vijayarajan (M.S):** Software Engineer, R&D at Axtria - Ingenious Insight
- **Natarajan, Abhiram (Phd):** EPSRC postdoctoral fellow at University of Warwick (Previously, postdoctoral fellow at the University of Colorado at Boulder)
- **Wu, Shuang (Phd):** Ph.D. candidate in Statistics at University of California, Los Angeles
- **Benjamin Bond (PhD):** Ph.D. Purdue University (Interned at Idaho National Lab)
- **William Lu (PhD):** PhD Purdue University (Interned at Google and Microsoft)

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 2022–2023
  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.

References:

1. **Dr. Dongyan Xu**	Professor	Purdue University, E-mail: `dxu@purdue.edu`
2. **Dr. Kevin R. Butler**	Professor	University of Florida, E-mail: `butler@ufl.edu`
3. **Dr. Dave (Jing) Tian**	Assistant Professor	Purdue University, E-mail: `daveti@purdue.edu`
4. **Dr. Antonio Bianchi**	Assistant Professor	Purdue University, E-mail: `antoniob@purdue.edu`
5. **Dr. Z. Berkay Celik**	Assistant Professor	Purdue University, E-mail: `zcelik@purdue.edu`