Adil Ahmad

School of Computing and Augmented Intelligence (SCAI)
Arizona State University
699 S Mill Ave, Tempe, AZ, 85281

Office: BYENG 372
Email: adil.ahmad@asu.edu
Homepage: adil-ahmad.net

Professional Experience

Arizona State University, Tempe, AZ ..... Aug 2022 – Current

School of Computing and Augmented Intelligence (SCAI)

Assistant Professor

Microsoft Research, Redmond, WA ..... May 2021 – Aug 2021

Summer Research Intern

Worked with Marcus Peinado and Sangho Lee

Microsoft Research, Redmond, WA ..... May 2019 – Aug 2019

Summer Research Intern

Worked with Marcus Peinado and Sangho Lee

NEC Labs, Princeton, NJ ..... May 2018 – Aug 2018

Summer Research Intern

Worked with Chung Hwan Kim

Research Summary

My interests broadly lie within the research domains of **computer security**, **systems**, and **architecture**. Currently, I investigate **safely storing sensitive data in remote machines** by leveraging hardware data protection features and securing critical machine software. In particular, I design software systems that leverage existing hardware features (e.g., Intel SGX) to protect data in remote machines. For attacks that existing hardware cannot efficiently prevent, I develop new hardware extensions to implement efficient data protection. Finally, I complement hardware data protection by securing machines against software vulnerabilities, eliminating many machine compromises that leak sensitive data in the first place.

Education

Purdue University, West Lafayette, IN, U.S.A ..... Aug 2016 - Aug 2022

Ph.D. in Computer Science

Thesis Advisors: Pedro Fonseca and Byoungyoung Lee

Lahore University of Management Sciences (LUMS), Lahore, Pakistan ..... May 2016

B.S. in Computer Science

Thesis Advisor: Ihsan Ayyub Qazi

Murray State University, Murray, KY, U.S.A ..... Spring 2015

Exchange Student

Publications

Conferences

[1] **Hardlog: Practical and effective system audit**.
Adil Ahmad, Sangho Lee, and Marcus Peinado.
IEEE Symposium on Security and Privacy (S&P), 2022.

[2] **Chancel: Efficient multi-client isolation under adversarial programs**.
Adil Ahmad, Juhee Kim, Jaebaek Seo, Insik Shin, Pedro Fonseca, and Byoungyoung Lee.
ISOC Network and Distributed System Security Symposium (NDSS), 2021.

[3] **Kard: Lightweight data race detection with per-thread memory protection**.
Adil Ahmad, Sangho Lee, Pedro Fonseca, and Byoungyoung Lee.
ACM International Conference on Architectural Support for Programming Languages (ASPLOS), 2021.

[4] **Shard: Fine-grained kernel specialization with context-aware hardening**.
Muhammad Abubakar, Adil Ahmad, Pedro Fonseca, and Dongyna Xu.
USENIX Security Symposium (Security), 2021.

[5] **Blackmirror: Preventing wallhacks in 3d online fps games**.
Seounghyun Park, Adil Ahmad, and Byoungyoung Lee.
ACM Conference on Computer and Communications Security (CCS), 2020.

[6] **Trustore: Side-channel resistant storage for sgx using intel hybrid cpu-fpga**.
Hyunyoung Oh, Adil Ahmad, Seounghyun Park, Byoungyoung Lee, and Yunheung Park.
ACM Conference on Computer and Communications Security (CCS), 2020.

[7] **A tale of two trees: One writes, and other reads. optimized oblivious accesses to large-scale blockchains**.
Duc V. Le, Lizzy Tengana Hurtado, Adil Ahmad, Mohsen Minaei, Byoungyoung Lee, and Aniket Kate.
Privacy Enhancing Technologies Symposium (PETS), 2020.

[8] **Obfuscuro: A commodity obfuscation engine on intel sgx**.
Adil Ahmad*, Byunggill Joe*, Yuan Xiao, Yinqian Zhang, Insik Shin, and Byoungyoung Lee.
ISOC Network and Distributed System Security Symposium (NDSS), 2019.

[9] **Obliviate: A data oblivious filesystem for intel sgx**.
Adil Ahmad, Kyungtae Kim, Muhammad Ihsanulhaq Sarfaraz, and Byoungyoung Lee.
ISOC Network and Distributed System Security Symposium (NDSS), 2018.

[10] **Detecting and defending against compelled certificate attacks using origin-bound captchas**.
Adil Ahmad, Faizan Ahmad, Lei Wei, Vinod Yegneswaran, and Fareed Zaffar.
EAI Conference on Security and Privacy in Communication Networks (SecureComm), 2018.

(* means equal contribution)

Teaching

Trusted Computing in Clouds (CSE 598), Arizona State University, Fall 2022

Advanced Operating Systems (CS 50300), Purdue University, Fall 2017

Intro to Programming (CS 18000), Purdue University, Fall 2016

Data Structures (CS 35000), Lahore University of Management Sciences, Fall 2015

Intro to Programming (CS 20000), Lahore University of Management Sciences, Fall 2015

Talks

Operating Systems Preview

ACM/USENIX Operating Systems Design and Implementation (OSDI), Jul. 2021

Chancel: Efficient Multi-client Isolation under Adversarial Programs

Microsoft Research Security Mini-Workshop, Jul. 2021

ISOC Network and Distributed Systems Security (NDSS), Feb. 2021

Kard: Lightweight Data Race Detection with Per-thread Memory Protection

ACM International Conference on Architectural Support for Programming Languages (ASPLOS), Apr. 2021

Side-Channel Security

Intel Tech Talk, Mar. 2021

Side-Channel Secure Storage for Enclaves

Microsoft Research Cryptography Colloquium, Nov. 2020

Obfuscuro: A Commodity Obfuscation Engine for Intel SGX

ISOC Network and Distributed System Security Symposium (NDSS), Feb. 2019

Obliviate: A Data Oblivious File System for Intel SGX

ISOC Network and Distributed System Security Symposium (NDSS), Feb. 2018

CERIAS Security Seminar, Feb. 2018

Professional Activity

Session Chair

IEEE Symposium on Security and Privacy (S&P), 2022

Shadow Program Committee

ACM European Conference on Computer Systems (EuroSys), 2020

Research Mentor

ACM International Conference on Architectural Support for Programming Languages (ASPLOS), 2021

ACM Symposium on Operating Systems Principles (SOSP), 2021

Honors and Awards

Purdue's nominee for the Google Ph.D. Fellowship, 2020

1 out of 100 recipient of Global UGRAD exchange scholarship (worth USD 15000)

Recipient of a LUMS undergraduate academic scholarship (2012 - 2016)

Relevant Coursework

Discrete Mathematics, Probability and Statistics, Linear Algebra

Data Structures and Algorithms, Operating Systems, Systems Security

Computer Networks, Databases, Software Security, Network Security