Amir Sabzi

github.com/amir-sabzi
Mobile:+1(236)5135283 | Email: sabzi@cs.ubc.ca

Research Interests

Differential Privacy, Network and Systems Security, Systems for Machine Learning

Education

M.Sc. in Computer Science Sep. 2021 – Sep. 2023
University of British Columbia Vancouver, Canada
- Advisors: Aastha Mehta, Mathias Lécuyer
- Thesis: A differentially private network traffic shaping framework
- GPA: 91/100

B.Eng. in Electrical Engineering Sep. 2016 – Feb. 2021
B.Sc. in Computer Science (minor) Tehran, Iran
Sharif University of Technology
- GPA: 18.43/20.00

Publications

1. **NetShaper: A Differentially Private Network Side-Channel Mitigation System**, USENIX Security '24.
   Amir Sabzi, Rut Vora, Swati Goswami, Margo Seltzer, Mathias Lécuyer, Aastha Mehta
2. **Macchiato: Importing Cache Side Channels to SDNs**, ANCS 2021, (**Best Paper**)
   Amir Sabzi, Liron Schiff, Kashyap Thimmaraju, Andreas Blenk, Stefan Schmid

Research Experiences

Research Staff Member Oct. 2023 – Present
University of British Columbia
- **Improving Differentially Private Machine Learning.**

Graduate Research Assistant Sep. 2021 – Sep. 2023
University of British Columbia
- **Mitigating network side channels with differential privacy.**
- Supervisors: Prof. Aastha Mehta and Prof. Mathias Lécuyer

Research Intern Jun. 2020 – Aug. 2021
University of Vienna
- **Security analysis of programmable networks.**
- Supervisor: Prof. Stefan Schmid

Undergraduate Research Assistant Jan. 2019 – Feb. 2020
Cloud-Native Telecommunication Networks office
- **Enabling GTP-U protocol in a cloud-native software-defined network.**
- Supervisors: Prof. Babak Khalaj and Dr. Azad Ravanshid

Teaching Assistance Experiences

University of British Columbia

Topics in Security and Privacy (Graduate), 2021, Instructor: Prof. Mehta

Introudction to Computer Networking, 2023, Instructors: Prof. Hutchinson and Prof. Mehta

Sharif University of Technology

Software-Defined Mobile Networks (Graduate), 2020, Instructor: Dr. Ravanshid.

Data structures & Algorithm design, 2020, Instructor: Prof. Salehkaleybar.

Communication Data Networks (3 times), 2019-2020, Instructor: Prof. Pakravan.

Communications Systems, 2019, Instructor: Prof. Babak Khalaj.

Signals and Systems, 2019, Instructor: Prof. Babak Khalaj.

Skills

Programming Languages: Python (JAX, PyTorch), C/C++, P4, MATLAB, MIPS/X86-Assembly
Tools: Open vSwitch, NS-3, mininet, Git, Docker
Languages: Farsi, English

Relevant Projects

Improving Differentially Private Machine Learning

- Developing a generator to generate a synthetic dataset using the differentially private gradients from a classifier trained with DP-SGD.
- Using synthetic data to enhance the model's utility.

Differentially Private Traffic Shaping in TEE

- Designing an isolated Differentially Private traffic shaping module using ARM TrustZone.
- Reducing the trusted computing base compared to existing solutions.

Verification of Deep Neural Networks with Projectagons

- Studying different methods for the verification of deep neural networks and their advantages and disadvantages.
- Presenting the new idea of applying projectagons to deep neural network verification.
- Implementing the projectagon-based verification concept and offering a proof of concept to showcase its feasibility and comparing its precision with existing methods.

Security Analysis of Web

- Implementing various cyberattacks, such as Control Hijacking, web application vulnerability analysis (XSS and SQL injection), and a Man-In-The-Middle attack via Diffie-Hellman key exchange vulnerabilities with arp poisoning.

Kernel Programming

- Developing a packet-sniffing kernel module with user-defined filters, a dedicated file system for packet logging, and additional modules for concurrency management.

Selected Courses

Computer Systems and Networks

Advanced Data Networks
Blockchain Technology
Introduction to Formal Verification
Distributed Systems
Advanced Operating Systems
Kernel Programming

Machine Learning and Optimization

Stochastic Processes
Convex Optimization
Statistics and Applications
Introduction to Machine Learning
Causal Machine Learning
Learning to Move (Reinforcement Learning)

Honors and Awards

Ranked 16th among 162: EE Department, Sharif University of Technology, 2020

Fellowship, Iran National Elites Foundation, 2018

Ranked in the top 0.2% among 250,000 students taking part in Iran National University Entrance Exam, 2016.