Pragya Sharma

pragyasharma@vt.edu pragyasharmaa.github.io

Education

Virginia Tech — Arlington, Virginia, USA — Jan 2021 - Present
Ph.D. in Computer Engineering — *GPA: 4.0*

Indian Institute of Technology Bombay — Mumbai, India — Jul 2013 - Jun 2018
B.Tech. & M.Tech. in Electrical Engineering — *GPA: 8.36/10.0*

Work Experience

Kryptowire Labs — McLean, Virginia, USA — May 2022 - Aug. 2022
Research & Development Intern

- Deployed the WAVE framework on a Kubernetes cluster and executed stress-testing experiments on WAVE persistent storage server to assess the scalability of the system in extensive deployment scenarios.
- Evaluated the performance of WAVE by analyzing metrics such as latency, CPU utilization, and storage size. Additionally, suggested alternative approaches for facilitating cross-domain interactions.

Cadence Design Systems — Pune, India — Jul. 2018 - Dec. 2020
Senior Design Engineer

- Worked extensively on development and optimization of IEEE 754 vector floating-point DSPs within the Tensilica family of MathX processors. Conducted comprehensive performance benchmarking of these DSPs using software examples compiled with both gcc and llvm C compilers.
- Contributed to the optimization and enhancement of Instruction Set Architecture (ISA) of Tensilica ConnX family DSP processors, focusing on achieving faster performance through the efficient utilization of VLIW slots. Additionally, benchmarked these cores in the context of communication and radar/lidar processing chains.
- Assisted in the development of the neural network (NN) library of the Tensilica HiFi4 DSP to enhance Automatic Speech Recognition (ASR) capabilities of voice-controlled digital assistants.

Research Interests and Publications

Interests: Network Security, 5G security, Blockchain, Adversarial Learning

1. **5G-WAVE: A Core Network Framework with Decentralized Authorization for Network Slices**
   P. Sharma*, T. Atalay, H. Gibbs, D. Stojadinovic, A. Stavrou and H. Wang
   IEEE INFOCOM 2024 - IEEE International Conference on Computer Communications [Accepted]

2. **Adaptive Flow-Level Scheduling for the IoT MAC**
   P. Sharma*, J. Nair and R. Singh
   COMSNETS 2020 - International Conference on COMmunication Systems & NETworkS

Projects

CASTLE: Cyber Agents for Security Testing and Learning Environments — Jul 2023 - Present

- Built an emulation environment consisting of Linux VMs, OpenVSwitch switches and SDN controllers to enable attack-defense plays for learning by red and blue agents.
- Working on creation of high-fidelity cyber digital twin of enterprise networks using knowledge graph modeling for network topology, to be leveraged as a multi-agent reinforcement learning environment for cyber-defense.

5G-WAVE: Integrating WAVE with 5G core for decentralized authorization — May 2022 - Jun 2023

- Designed and implemented a decentralized authorization framework for the 5G core service access among VNFs by utilizing WAVE to eliminate the security vulnerabilities caused by a central OAuth2.0 authorization server.
- Deployed the 5G-WAVE platform on a Kubernetes cluster with OpenAirInterface (OAI) entities as 5G VNFs. Modified the design to offload authorization among VNFs onto side-car proxies (SCPs) which enable service access by creation and verification of WAVE attestations.
- Measured time cost based performance of service operations in 5G-WAVE in network slice deployments to analyze latency overhead and scalability of the design with multiple slices.

Detecting Price Manipulation Vulnerabilities exploited by DeFi Flash Loans Dec 2023

- Performed a thorough research survey of DeFi attacks with a specific focus on flash loan attacks and existing price manipulation vulnerability detection methods.
- Implemented a price manipulation vulnerability detector using call graph construction and static taint analysis, resulting in a 30% improvement of accuracy over existing methods.

Feature-Fingerprinting of SSH Attacks and Countermeasures with Honeypots Apr 2022

- Deployed Cowrie honeypot to log brute-force SSH attacks on an isolated victim node. Performed an extensive analysis with feature extraction from publicly available datasets of Cowrie.
- Proposed a resource-draining mathematical computational challenge to the attacker as a countermeasure.

Anomaly Detection in Network Traffic using Reinforcement Learning Dec 2021

- Implemented a binary classifier to detect attack events in wireless network traffic using Deep Q-Learning
- Simulated an adversarial environment for a classifier agent with input data samples representing system states.

Exploring DNS Security - DNSSEC and DANE Dec 2021

- Implemented DNSSEC in a private DNS network using Docker. Established a chain-of-trust among root, top-level domain (TLD) and authoritative nameservers through DNSSEC key-signed zone records.
- Deployed DNSSEC-enabled resolvers to fetch DNSSEC and TLSA records from websites in the wild.

Exploring vulnerabilities in WPA2 Nov 2020

- Conducted penetration testing on Android smartphones to expose vulnerabilities in the WPA2 protocol, specifically Key Reinstallation Attack (KRACK), highlighting the risk of a MitM attacker decrypting packets.

Relevant Coursework

- **Security** - System and Software Security, Network Security, Fundamentals of Information Security
- **AI** - Reinforcement Learning, Fundamentals of Machine Learning
- **Others** - Blockchain Technologies, Markov Chains and Queuing Systems, Wireless and Mobile Communications

Technical Skills

- **Software/Packages** - Kubernetes, Docker, OpenVSwitch, GNS3, Vagrant, Gymnasium, Wireshark
- **Languages** - C, C++, Python, Bash

Leadership Experience

- **Campus Representative, Arlington** - Virginia Tech Graduate Student Assembly (VT-GSA) 2022
- **President, Washington DC Chapter** - IIT Bombay Heritage Foundation (IITB-HF) Jun 2022-Present
- **Web Nominee** - Hostel Affairs, IIT Bombay Apr 2015 - Mar 2016