ymalhi@andrew.cmu.edu
(412) 499-4176
Pittsburgh, PA

Yuvraj Malhi

yuvraj-malhi.github.io
linkedin.com/in/yuvraj-malhi
github.com/yuvraj-malhi

Education

Carnegie Mellon University, *M.S. in Information Security* *Aug 2022 – Dec 2023*

- **Coursework**: Software Reverse Engineering, Secure Software Systems, Network Security, Mobile & IoT Security.
- **Extra-curricular**: Long Distance Running, Hockey Team, Non-profit Teacher, and Punjab Cultural Association

BITS Pilani University, *B.E. in Electronics Engineering* *Aug 2018 – May 2022*

Skills

- **Forte**: Network Security, Buffer Overflow, Malware Analysis, Reverse Engineering, Web Security, Software Security, ML Applications in Security, Intrusion Detection, Cryptography, Netowrking, Software Development, Linux.
- **Languages**: C, C++, Python, MATLAB, LaTeX, HTML, Assembly language, SQL, Java, Shell, Dafny.
- **Tools**: IDA, Ghidra, MobSF, Metasploit, WireShark, Tensorflow, Pytorch, Scikit-Learn Git, GitHub, Snort.

Work Experience

Amazon Seattle, WA
Security Engineering Intern *May 2023 – Aug 2023*

- **Analyzed security infrastructure** of third-party applications to avoid illegal data access and incident response.
- Created a **risk-scoring framework** for automation of third-party **application security** vulnerability assessments based on data confidentiality, **SSO** usage, **passive scanning**, and active penetration testing and red team reports.
- Set up AWS cloud architecture for automated identification of **un-authorized applications** being used.

Samsung Bangalore, IN
Network and Systems Intern *July 2021 – Jan 2022*

- Worked on ML-based log analysis for **system compromise/fault detection** and **root cause analysis**.
- Designed an **anomaly detection** system to monitor system background information and take pre-emptive action before hard failure. **Saved service teams 20 hrs/week** by automating 90% maintenance.

BITS Pilani Research Pilani, IN
Research Assistant: Mitigating DDoS Attacks in SDN Data Plane *Aug 2021 – Jan 2022*

- Surveyed and analyzed methods used to **detect and mitigate** Denial-of-Service (**DoS**) and Distributed Denial-of-Service (**DDoS**) attacks at **Data Plane** level in Software Defined Networks (SDN) using P4 language.
- Identified **limitations of P4** for attack detection/mitigation: no support for loops, complex numerical functions.

IIT Kanpur Kanpur, UP
Cybersecurity Intern *May 2021 – Aug 2021*

- Among **top 5** students from India selected in the **Intrusion Detection Team** of IIT's cybersecurity division.
- Surveyed and categorized **non-encrypted/encrypted traffic analysis** solutions by application or mechanism.

BITS Pilani Research Pilani, IN
Research Assistant: Machine Learning Intrusion Detection Systems for IoT *Jan 2021 – May 2021*

- Designed and implemented **network IDS for IoT** to overcome few design flaws of existing IDS. This design can detect **22 attacks** with help of **3 ML-based detectors** using Random Forest, ANN, Decision Tree, XGBoost.
- Central Module attack classification rate: **94.41%**. Edge modules attack detection rates: **99.98%** and **99.87%**.

Projects

- **Android Location Stealth**: A Kotlin-based Android application that finds device using — **WiFi Triangulation** (for API 19-25) with accuracy of **30 ft** and **IP GeoLocation** (for API 26-31) with accuracy of **200 ft - 2 mi**.
- **Mini-C-Dafny**: Created a type-safe language in Dafny, similar to C which respects **non-interference**, typedeness, security types, and **taint analysis**. Also prevents major attacks on cache, side channel, buffer overflow, control flow.
- **Ultra-fast URL Port Scanner**: Scans URL open ports up to **10X faster** than traditional scanners by using 100 child scanners **concurrently**. The scanner also **lists all IPv4 and IPv6 addresses** allotted to each URL.
- **Concurrent TFTP Servers**: A TFTP single process server to handle multiple clients using **listen** call on multiple FDs with speed **25 Mbps**. Second, A TFTP **multi process server** to spawn a child server per client with speed **50 Mbps**.