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**: Introduction to Computer Systems, Secure Software Development, Software Reverse Engineering.

BITS Pilani University, *B.E. in Electronics Engineering* *Aug 2018 – May 2022*
- **Coursework**: Machine Learning, Network programming, Data Structures & Algorithms, 2 Research Publications.
- **Extra-curricular**: Long Distance Running, Hockey Team, Non-profit Teacher, and Punjab Cultural Association

Work Experience

Amazon Seattle, WA
Security Engineering Intern *May 2023 – Aug 2023*
- Analyzing **infrastructure of third-party applications** before allowing access to privileged customer data.
- Creating an information flow pipeline and **prioritization-scoring system** to identify, prioritize, and report assessment status of third-party (3P) application reviews.
- Setting up **AWS cloud automated identification/reporting** use of non-reviewed applications being used.

Samsung Bangalore, IN
Network and Systems Intern *July 2021 – Jan 2022*
- Worked on **ML-based log analysis** for **system fault detection** and post-mortem **root cause analysis**
- Designed and implemented an **anomaly detection** system to monitor system background information and take pre-emptive action before hard failure. Achieved 80% detection capability.
- **Saved service teams 20 hrs/week** in maintenance cost and helped comply with system assurance goals.

BITS Pilani Research Pilani, IN
Research Assistant: Internet of Things (IoT) Assurance *Jan 2021 – May 2021*
- Designed and implemented **network IDS for IoT** to overcome few design flaws of existing IDS. IDS can detect 22 attacks with help of 3 ML based modules using **Random Forest, ANN, Decision Tree, and XGBoost**
- Central Module attack detection F1 score: **94.41%**. Edge modules attack detection F1 score: **99.98%** & **99.87%**

BITS Pilani Research Pilani, IN
Research Assistant: Software Defined Networks (SDN) Assurance *Aug 2021 – Jan 2022*
- Surveyed and analyzed methods used to **detect and mitigate** Denial-of-Service (**DoS**) and Distributed Denial-of-Service attack vectors at **Data Plane** level in Software Defined Networks (SDN) using **P4 language**.
- Identified **limitations of P4** for defensive software dev. E.g. no support for loops, complex numerical functions.

Skills

- **Forte**: Systems, Networking, Software Security, Machine Learning, Deep Learning, Network Security, Server Design, Network Programming, Data Analysis, Automation.
- **Languages**: C, C++, Python, MATLAB, LaTeX, HTML, Assembly language, SQL, Dafny.
- **Tools**: VScode, Jupyter, MobSF, WireShark, Tensorflow, Metasploit, Scikit-Learn, Git, GitHub, Snort, IDA, Ghidra.

Projects

- **Concurrent TFTP Servers**: A TFTP single process server to handle multiple clients using **listen** call on multiple FDs (Speed - **25 Mbps**). Second, A TFTP **multi process server** to spawn 1 child server/client (Speed - **50 Mbps**).
- **Simple Hadoop Server**: Replicated a simple of **Google File Storage** by creating client, data server and meta-data server. Client uploads files in chunks and **distributed data servers** stores 3 copies of each chunk to ensure **availability** in case of a server crash.
- **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.