Ayush RoyChowdhury, AI Security R&D

Austin, United States, (469) 994 8424, ayushrc0914@gmail.com

LINKS

Linkedin, Website

OBJECTIVE

Bachelor of Science in Electrical and Computer Engineer, graduated from UT Austin '24, with a focus on security and cloud automation. Researched into copilot and other rag-based systems security at Spark Lab, presented @ Defcon AI Village. Lead Convergent Forge to innovate and commercialize digital solutions for startups and non-profits. I am looking for full time work in Security, Software or AI research and development. Open to work at all locations, in-person or remote.

EXPERIENCE

Jan 2024 — Present

AI Security Research Assistant, Spark Lab

- Current work on RAG-based security, presented at DefCon 32 & ACE Conference!
  - confusedpilot.info - Confused Deputy Risks in Production Level Rag-Based Systems such as Copilot for M365
- Past work on Reinforcement learning-based detection of microarchitectural attacks, presented at ASPLOS '24 workshop & ACE Symposium!
  - ut-ldma.github.io - SoK (Systemization of Knowledge) on learning-based detection of microarchitectural attacks,

May 2024 — Aug 2024

Software Engineering Intern, Cox Automotive — Austin

- **AWS Research & Development**: Set up infrastructure for RAG-based systems with sparse retrieval in AWS. I researched performance improvements in routing vs. non-routing for OpenSearch clusters. Automated data refresh using Lambda.
- **Side Project**: Developed a secure backend-for-frontend to track dealership activity.
- **Hackathon**: Built a copilot tool to assess Rally epics, features, and stories for sprint planning, focusing on clarity and completeness.

Jun 2023 — Aug 2023

Cloud IoT R&D Intern, Trend Micro — Austin

- Worked at Trend Micro R&D team to automate the software delivery and bug fix pipeline for Security Management System using AWS IoT and middleware.
- Used OpenAI API to create a bug resolution system that leverages AI to suggest bug fixes based on code, testing and Jira context.

Jun 2022 — Aug 2022

Cloud Automation R&D Intern, Trend Micro — Austin

- Proposed and implemented a cloud feature that would automate client's network appliance management in Trend Micro's Cloud One service.
- Implemented an app to invoke a Lambda with KMS integration for network security filters offered to network appliances by Trend Micro's Cloud One service.

Jun 2021 — Aug 2021

Technical Product Intern, wakaNINE — Austin

- Developed a geo-location software to supplement wakaNINE's Delivery and Digital Marketing Team with a growth hacking initiative.
- Created a database used by Digital Marketing Team to tag, segment, and filter images for the Sales Team.

Feb 2021 — May 2021

Technical Product Extern, Chevron — Austin

- Roadmapped a scalable and working Industrial IoT solution for asset management with cloud and network security integration around existing subsea oil and gas infrastructure.
- Using market research, financing, and technology to create a cost and energy-effective solution that saved Chevron around $12 million for maintenance.
- Extended Battery Lifetime to 5 years and Asset Lifetime to 25 years.
- Part of the Practicuum Program at UT Austin

Jun 2020 — Oct 2020

Research and Development Intern, Blackswan Cybersecurity, LLC — Farmer's Branch

- Malware Analysis automation scripts that analyzed malware using Ghidra and performed static, dynamic, and memory analysis.
- Threat Analysis of phishing attacks by simulating similar variables seen in the nearby geo-location.

Sep 2018 — Aug 2020

Researcher, UNT CyberForensics Department

Denton

- Conceptualized and developed a patented skimmer detector for Cyber Defense Labs
- Helped in designing the algorithm and program for a Skimmer Database to help law enforcement predict the likelihood of skimmers in a neighborhood.
- Dark Web Open Source Intelligence Tool/Crime Map using web-scraping and machine learning to create a database.
- Tone Analysis Machine to mine social media for intelligence and sentiment using Natural Language Processing integration.

EDUCATION

2020 — 2024

B.S. Electrical and Computer Engineering, UT Austin

- Cumulative GPA: 3.59/4.0, Business Minor
- TA, SI Lead Intro to Embedded Systems - Fall 2024, TA for Foundations of Finance - 2023
- Director at Convergent Forge - 2023-2024
  - Helped create and manage digital products with Startups and Non-profits addressing stakeholder needs while aligned with their strategy and goals
  - Lead 4-7 teams of software engineers, product managers, and UI/UX designers with road mapping, building, delivering, and commercializing digital products for Startups and Non-profits
- Technical Product Manager at Convergent Forge - 2022-2023
- Engineer at Convergent - 2020-2022

SKILLS

ARM Assembly, C/C++, Java, React, Python, Go, R

AWS, Docker, Kubernetes, microk8s

Arduino, Raspberry Pi, Nordic nrf5

VMWare, VirtualBox, Kali Linux, Ghidra, Matlab, Solidworks

Tensorflow, PyTorch, Flask, Firebase, Django, SQL, OpenAI

FEATURED PROJECTS [ALL PROJECT CAN BE FOUND ON MY GITHUB ABOVE]

Feb 2023 — Dec 2023

GSTAgri

Austin

- ,Full Stack Engineer and Product Manager
- Capstone project focusing on Edge AI and IoT and leverages the ST150M, a Globalstar satellite modem, to create an asset monitoring and management system that predicts crop risk.
- Reducing overall data usage and cost by implementing Edge AI to alert clients based on metrics set by subject matter experts.

Jul 2023 — Aug 2023

Butterfly

Austin

- Provided Jira, Gherkin, and Code context, Butterfly is a web application with OpenAI integration to interact with Jira to create an informative user story and resolve quick bug fixes.

Aug 2022 — May 2023

Meals on Wheels Delivery App

Austin

- A delivery application similar to DoorDash made using React, Flask, Django, Python, SQL and Salesforce for Meals on Wheels volunteers who deliver meals to the elderly.

Aug 2023 — Sep 2023

RSA & AES-128 Implementation and DPA

Austin

- Implement RSA and AES-128 (Counter-Mode) in C using basic arithmetic functions
- Implemented a Differential Power Analysis attack by analyzing power traces from hardware and using Pearson Correlation to guess the encryption key.

Feb 2022 — May 2022

Web Application Security

Austin

- Netmapping to categorize IP addresses
- Packet tracing to identify important handshakes and packet information with different websites
- Syn Flood Attack using scapy on implemented Server-Client in C
- Deployed a website using Docker and Kubernetes, ran administration using microk8s
- Applied Command Injection, PHP Injection, SQL Injection, and CSP Bypass Attack
- Applied Forkbomb Attack