Sarvottam Kumar Modi

Email: sarvottamkumar2000@gmail.com
LinkedIn: c0d3nh4ck

Education

- **Indian Institute of Technology Kharagpur** Kharagpur, India
  Bachelor of Technology - Chemical Engineering; GPA: 8.60 *July 2018 - May 2022*
  Courses: *Cryptography & Network Security, Hardware Security, Programming & Data Structures, Deep Learning, Machine Intelligence & Expert Systems*

Skills Summary

- **Languages** Python, Assembly Language, C/C++, Bash
- **Frameworks** Intel Pin, DynamoRIO, Angr, TensorFlow, Keras, WinAppDbg
- **Tools** IDA Pro & IDAPython, WinDbg, WinAFL, AFLPlusPlus, GDB, Ghidra, QEMU
- **Areas** Reverse Engineering, Fuzzing, Dynamic Binary Instrumentation, Exploit Dev, Firmware Analysis
- **Platforms** Linux, Windows, AWS

Experience

- **Zscaler**
  Security Researcher I *Sep 2023 - Ongoing*
  - **Reverse Engineered** the DWG file parsing functionality within **Microsoft Visio**, involving **restructuring vftables** and **analyzing COM components**. Conducted detailed analysis of DWG file parsing, identifying critical functions validating CRC checksums
  - Developed and optimized a **harness for Microsoft Visio**, incorporating exception handling and COM components discovered through reverse engineering. **Conducted crash triage and in-depth analysis** of identified issues through fuzzing, **reporting findings to MSRC**
  - Developed a tool using **DynamoRIO** to generate **contextual information** and **code coverage for each basic block** executed within a DLL, enhancing reverse engineering efforts
  - Explored development of tools for a **snapshot-fuzzing framework**, including an API hooking tool for **analyzing heap allocation tracing performance** and **a foundational debugger**, with plans for future evolution into an instrumentation and automated execution engine
- **Zscaler**
  Associate Security Researcher *Jun 2022 - Aug 2023*
  - Developed **IDAPython scripts** to meticulously analyze coverage log files and identify potentially vulnerable functions
  - Developed a **File-Format fuzzing** framework which includes development of a **parser** for an undocumented raw-image file format e.g. CR2, and a custom **mutator** for it
  - **Reverse-engineered** intricate functions and proprietary structures of **Commercial-Off-The-Shelf software** involved in parsing image and Word document file formats **to develop specialized fuzzing harnesses**
  - Experimented with capturing **code coverage** information using the **Intel Pin** DBI framework to measure its performance
  - **Configured a highly efficient WinAFL fuzzing environment**, optimizing performance through RAM Disk utilization and parallelization across CPU cores on an ESXI server
  - Conducted **extensive literature review** and **experimentation** based on numerous blogs and research papers on file-format fuzzing, like FormatFuzzer, Jackalope and Peach Fuzzer
- **Secure Embedded Architecture Laboratory, IIT Kharagpur**
  Undergraduate Researcher *Dec 2021 - May 2022*
  - Developed a strong foundation in cache side-channel attacks (**Prime+Probe, Flush+Reload, Evict+Reload**) through extensive study of research papers and conference presentations
  - Developed an automation for **data collection on cache miss/hits timing across x86 instruction sets** on Intel CPUs for profiling the instructions
  - Applied machine learning (**GMM, KNN**) and template analysis (**LSQ**) techniques to identify exploitable micro-architectural patterns and assess potential side-channel attacks [GitHub Repo]
  - Conducted in-depth literature review on **micro-op cache** side-channel attacks on key papers like **UC-Check, I See Dead µops,** and **Osiris**
  - Implemented and **validated the UC-Check paper** on target systems, demonstrating practical expertise in micro-architectural analysis and verification
- **Digital Security Research Center, Technology Innovation Institute** Remote
  Security Engineer (Part-time) *Aug 2021 - Nov 2021*
  - **Fuzz testing** of various open-source libraries, parsers and programs with **AFLPlusPlus** and different sanitizers
  - Knowledge gathering on various components of **QEMU emulation** and emulation based fuzzing
  - Tested and worked with various **symbolic and taint analyis** tools like Angr, Kirenenko, Triton, etc.

- **Digital Security Research Center, Technology Innovation Institute** Remote
  Security Engineer Intern (Full-time) *May 2021 - Jul 2021*
  - Developed and optimized a tool to automatically prove a vulnerability as a **PoC** for a vulnerable program
  - **Firmware Analysis** of embedded / IoT devices and their binaries using binwalk, firmwalker, ghidra and other toolkits
  - **Partial Emulation** of various firmwares from IoT devices using ARM-X, Qiling, and QEMU
- **Complex Networks Research Group, IIT Kharagpur** Remote
  Research Intern *Apr 2020 - Jul 2020*
  - **Data mining** of **90,000+** tweets and its related information from tweet IDs in the Replab Dataset using Twitter API
  - **Exploratory Data Analysis** of tweets like N-gram exploration, WordCloud, and Named Entity Recognition
  - **Sentiment Analysis** of tweets using the libraries - Afinn, Textblob, and NLTK's Vader Sentiment Analyzer
  - **Topic Modelling** using Genism's LDA module and determining the number of topics and its distribution over tweets
  - **Brand Popularity** of entities from tweets using cosine similarity and number of retweets and likes [GitHub Repo]

Coursework Information

- **OpenSecurityTraning2**
  - Reversing C++ Binaries, C-Family Software Implementation Vulnerabilities, OS Internals, Intermediate and Beginner WinDbg, x86-64 Reset Vector: coreboot, x86_64 Assembly
- **Coursera**
  - Hacking and Patching, Web Application Security Testing with OWASP ZAP
- **Pluralsight**
  - The Essentials of COM, Malware Analysis Fundamentals
- **Others**
  - Advanced Deep Learning (Keras), AWS Cloud Practitioner Essentials, Networking Fundamentals

Projects

- **WebADB**
  A Web Application *GitHub*
  - Created a web-based ADB tool using the WebUSB API, eliminating the need for drivers or software installation. It allows users to execute ADB commands directly in the browser, uninstall bloatware apps using a ReactJS search bar, and will soon feature a built-in XTERM shell for seamless ADB shell access.

Honors and Awards

- Secured Gold in Network Security Hackathon in the prestigious 9th Inter IIT Tech Meet - Mar 2021
- Qualified in RMO (Regional Mathematics Olympiad) 2016 with a state rank of 6 conducted by HBCSE
- Qualified in NTSE (National Talent Search Examination) 2016 stage-1 with a state rank of 42 conducted by NCERT

Extra Curricular Activities

- Part of the Gold winning Inter-Hall Illumination Team of Radhakridhnan Hall of Residence for the year 2019-20
- Volunteered in the cleanliness drive in IIT campus on the occasion of 150th birth anniversary of Mahatma Gandhi
- Attended training and workshop on Disaster Managemen t Programme for both natural and industrial disasters