Himanshu Sheoran

himanshu_sheoran@yahoo.com
Security Software Engineer — deut-erium.github.io
GCP Security and Privacy — deut-erium
Google — himanshu-sheoran

Education

Indian Institute of technology Bombay 2017-2021
Bachelor of Technology in Computer Science and Engineering
With Honors

Professional Experience

Software Engineer - Google Cloud security *October 2023 - Present*
Confidential Compute VM *Pune*

- Working on providing encryption-in-use on Google cloud with Intel TDX on Emerald Rapids
- Leaded cryptography category in Google CTF 2024, designed and implemented 3 cryptography challenges

VMware - Member of Technical Staff 2 *July 2021 - October 2023*
CarbonBlack Windows Sensor *Pune*

- **CIS Benchmarking**
  - Conceptualized and implemented compliance management module for automated scalable hardening and remediation of security configurations across various windows OSes and profiles based on **OVAL** rules
  - Designed efficient formats for CIS Benchmarks running **10000 times** faster than CIS -CAT pro
- **CarbonBlack XDR**
  - Aided kernel integration of LastLine IDS engine and solidified with extensive kernel mode tests
  - Developed an **usermode** pcap replay tool for windows independent of any kernel mode packet capture libraries
- **Cloud Workload Protection**
  - Worked with **VDI** to implement automatic sensor re-registration for cloned VMs on Azure
  - Worked on developing sensor installation scripts using launch scripts on **GCP and Azure**
- **Team Development**
  - Organized an internal Capture the Flag event for enhancing internal security practices at Pune office
  - Automated development machine setup cutting manual setup time worth **2 days** of work to **2 hours**

Project Sekai - International CTF Team *May 2022 - Present*

- Current overall world rank **6** in CTF competitions 2023 by winning **8** CTF competitions
- Designed and authored cryptography challenges in **SekaiCTF 2022** and **SekaiCTF 2023**

Cybersecurity Club IITB - Manager *May 2020 - May 2021*

- Spearheaded a team of 10 people for planning and organising sessions, talks and **CTF** contests
- Developed and maintaining active wiki and blog site about cybersecurity with **1000s** of daily visitors worldwide
- Organized intra institute two-day **Capture The Flag** competitions with active participation of 250 people

BOSCH - Research Intern *May 2019 - July 2019*

- Developed a retrofit prototype for automatic and optimal gear-shifting mechanism for Derailleur geared bicycles
- Developed **Smart Shift** mobile application for managing the configuration of the embedded system via Bluetooth

Awards & Achievements

- **Silver** Medal in 10^{th} International Olympiad in Cryptography NSUCRYPTO *(2023)*
- **Gold** Medal in 9^{th} International Olympiad in Cryptography NSUCRYPTO with **highest score** *(2022)*
- **Gold** Medal in 8^{th} International Olympiad in Cryptography NSUCRYPTO with **highest score** *(2021)*
- **Gold** Medal in 7^{th} International Olympiad in Cryptography NSUCRYPTO *(2020)*
- Secured All India Rank **59** in JEE Advanced among 200,000 students in India *(2017)*
- Secured All India Rank **368** in JEE Main among 1.2 million students across India *(2017)*
- Secured All India Rank **194** in Kishore Vaigyanik Protsahan Yojana *(2017)*
- Amongst **350** students selected for INPhO and amongst national **top 1** percentile in NSEP *(2016)*
- Amongst **350** students selected for INChO and amongst national **top 1** percentile in NSEC *(2016)*

Projects

RNGeesus

- Implemented new approaches for state and seed recovery of commonly used Pseudo Random Number Generators - Mersenne Twisters, LFSRs and Truncated Linear Congruential Generators using SMT modelling
- Analyzed flaws in seed initialization phase of most commonly used general purpose PRNGs - Mersenne Twisters to recover 19937 bit state and initial seed using 32 bits of output on a single core machine under **2 minutes**

Automated Cryptanalysis

- Implemented state of the art library for automated linear and differential cryptanalysis for SPN ciphers
- Successfully cracked variants of ciphers as big as 128 bit and as deep as 10 rounds in **10 minutes**

Secure Script Execution Server

- Developed a concurrent script execution server with client, ensuring signed script execution for enhanced security.
- Successfully implemented a custom messaging protocol and digital signature verification in **C** with **OpenSSL**.
- Ensured code reliability through rigorous unit testing, validating functionalities and enhancing project stability.

Pyfractal

- Developed an easy to use, fully documented **Python Library** for generating brainfilling fractal curves
- Integrated intuitive **GUI** using **Tkinter** enabling understanding of fractals without mathematical background
- Packaged ready to use, **open-sourced**, multi-platform binaries for out-of-the-box working software

Blogs

- **Personal Blog** - Covering my technical interests and wanderings and problems created by me
- **CTF Competition Writeups** - Containg all the writeups I created for CTF challenges in years 2020-2022
- **Cybersecurity Club IITB wiki** - Covering wiki pages for learning cybersecurity

Talks

- **6th Indian SAT+SMT Winter School** - RNGeesus - State and seed recovery for RNGs using SMT solvers

Technical Skills

Programming	Python, C, C++, bash, Powershell, SageMath, java, lisp
Development Tools	Git, Subversion, GitHub, Gitlab, VIM, tmux, Docker, Jekyll, AWS, Azure, ESX
Security Tools	Ghidra, Wireshark, IDA, gdb, windbg, Sysinternal suite, Z3, pwntools

Last Updated *July 21st, 2024*