Himanshu Sheoran

Member of Technical Staff
R&D - CarbonBlack Cloud
VMware Inc.

✉ himanshu_sheoran@yahoo.com
deut-erium
in himanshu-sheoran

Research Interests

Cryptography, Cybersecurity and Formal Verification

Education

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

Professional Experience

VMware *July 2021 - Present*
CarbonBlack Windows Sensor | Mentor: Priya Heda *Pune*

- Working on implementing on-sensor compliance management module for automatic benchmarking and remediation of security configurations against all windows OSes and profiles, running **1000 times** faster than CISCAT pro
- Working on CarbonBlack Extended Detection and Response (**XDR**) solution for network based IDS
- Worked with Virtual Desktop Infrastructure to implement automatic sensor re-registration for cloned VMs
- Organized an internal Capture The Flag event for enhancing internal security training for Pune office.

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

- **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 *May 2019 - July 2019*
New Initiatives Lab | Mentor: Gunnar Godara *Bangalore*

- 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 embedded system via bluetooth

Research Experience

RNGeesus *Spring 2021*
Guide: Prof. Bernard Menezes *Course Project, IITB*

- 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 5 minutes
- Developed new approaches for state recovery of truncated LCGs for state recovery in $GF(2^n)$ where lattice reduction approaches fail due to non existence of modular inverses using far less outputs with no false positive solutions

Controller Synthesis *Spring 2021*

Guide: Prof. Ashutosh Gupta *RnD Project, IITB*

- Synthesising verifiable controller for a real-time system based on data-driven RL approaches and algorithmic SAT-SMT approaches to control a railway network modelled as timed-automata constraints over a set of specifications
- Utilized tools like DCvalid and UPPAAL to design and model networks of timed automata and verify solutions
- Studied approaches for determinization and minimaztion of timed automata specification given in duration calculus

ANF allSAT solver *Spring 2021*

Guide: Prof. VR Sule *Course Project, IITB*

- Implemented parallel all-SAT solver for finding all satisfying solutions of a sparse multivariate boolean polynomial
- Developed a parallel implementation of solver in SageMath solving for a complete set of orthogonal implicants of boolean functions appearing as factors of the boolean formula represented in Algebraic Normal Form

Automated Linear Cryptanalysis *Spring 2021*

Guide: Prof. Bernard Menezes *Course Project, IITB*

- Implemented automated linear cryptanalysis module for SPN ciphers by finding optimal linear biases for each s-box
- Capable of processing SPN networks of depth 6, p-box size 36 and 6 bit sboxes in less than **5 minutes**

Awards & Achievements

- **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)*
- Bagged **2nd** position in HCL HACK IITK 2021 Cybersecurity Hackathon *(2022)*
- Secured **Gold** medal in Saptang Netsec Challenge 9th Inter IIT Tech Meet *(2021)*
- Secured **2nd** position in Capture The Flag competition in 8th Inter IIT Tech Meet *(2019)*
- 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

Pyfractal | Self Project *Summer 2020*

- 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

Malware Detector-Classifier | Self Project *Summer 2020*

- **Developed** a malware detector cum classifier based on static analysis of program ensuring **zero risk** to host
- Processed **50GB** of malware and benign files to train high accuracy and f-score ML model for certain classification
- Engineered high importance features based on practical malware analysis for **low overhead** of computation

P2P BotNet Detector | Self Project *Summer 2020*

- Developed a network analysis tool for detection of **Peer-to-Peer** botnet infected hosts and traffic in network
- Analysed **47 Million** botnet and benign packets for anomaly based machine learning model used in detection
- Deduced network flows for transmission of botnet malware and further communications between infected hosts

Secure Personal Cloud | Course Project *Autumn 2018*

- Developed a web application and a command line linux client for a cloud based file system for multiple users
- Implemented full **client-side** encryption for web client using **SJCL** and linux client using **pyCryptodome**
- Implemented support for multiple simultaneous clients with automatic sync of files between client and server

SAT-Solver | Course Project *Spring 2018*

- Implemented **SAT** solver based on **DPLL** algorithm in functional programming paradigm in Racket
- Implemented recursive literal assignment and backtracing for finding satisfying assignment of formula in CNF

OSPF Protocol for Routers | Course Project *Spring 2019*

- Implemented Open Shortest Path First protocol in **VHDL** for building forwarding tables on routers
- Modified the standard OSPF protocol and packets to increase the efficiency of data transfer and processing

Art Generation with GAN | Course Project *Autumn 2019*

- Implemented Deep Convolutional Generative Adversarial Networks to generate art from art datasets
- Image dataset collected by scraping Google image art datasets and converted to 64X64 using bilinear interpolation

Shell File Server Client | Course Project *Spring 2019*

- Developed a shell-based file server using **Socket programming** capable of handling multiple concurrent clients
- Implemented user authentication and multiple sockets for a user enabling simultaneous parallel downloads

Regular Expression Parser | Course Project *Spring 2018*

- Implemented basic level string matcher Linux-CLI utility **egrep** using functional programming in **Racket**

Technical Skills

Programming	Python, C, C++, bash, SageMath, Racket, javascript, java
Development Tools	Git, GitHub, Docker, Jekyll, AWS, Azure, SVN
Security Tools	Ghidra, Wireshark, Nmap, Cutter, IDA, gdb, Z3, pwntools

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

Organized Competitions

- **SekaiCTF 2022 -** Preparing problems on Cryptography *(2022)*
- **Cryptohack.org -** Preparing challenges for upcoming module on Post Quantum Cryptography *(2022)*
- **Zh3r0 CTF V2** Prepared and deployed **7 challenges** on Cryptography and programming *(2021)*

Extracurriculars

- Amongst top **20** players at **cryptohack.org** completing **all** challenges and ranked **1st** in India *(2022)*
- Won **best writeup** award for crypto challenge Pythia in Google CTF 2021 *(2021)*
- Community moderator, contributor and amongst top **50** players at **cryptohack.org** *(2020)*
- Participation in **40+** international Capture The Flag events in 2020 and **25+** in 2021 *(2020)*
- Secured **First** position in Intra Department Badminton Tournament (Mens' Doubles) *(2018)*
- Secured **Third** position in XLR8, Remote Controlled bot making competition at IITB freshmen year *(2017)*
- Secured **Third** position in Potpurri Competition in Freshiezza, a college freshman competition *(2017)*