# Harshvardhan Patel

Computer Science and Engineering
UG 4th Year - Indian Institute of Technology (IIT) Bhilai

EMAIL: harshvardhanp@iitbhilai.ac.in

MOB. NO. +91-8097442119

| EDUCATION | UNIVERSITY | INSTITUTE | YEAR | CGPA |
|---|---|---|---|---|
| Undergraduate | IIT Bhilai | IIT Bhilai | Expected: May 2020 | 8.55 / 10 |

## INTERNSHIPS

**ROBERT BOSCH ENGINEERING AND BUSINESS SOLUTIONS, BANGALORE, IN** May 2019 – July 2019

INTERN – SECURITY AND PENETRATION TESTING (ESY-1) DEPARTMENT

- Created a framework using Bash, Bazel and Python scripts to produce minimal (in size) and source-code secure Docker images for various applications developed by the department.
- The framework built application specific base images from scratch, using Bazel scripts, packaging only the app's runtime dependencies – eliminating the bloat faced in OS specific images
- Wrote a recursive dependency parser in Python to automatically generate a complete dependency list of an application from the list of its high level dependencies
- Imported packages from snapshot.debian.org using Python and Bazel scripts
- Enforced source-code security by Cythonizing the Python source code of the applications within and enforced access control schemes on those container images
- Achieved up to **85 per cent size reduction** in Final Docker images

**MAX SECURE SOFTWARE, PUNE, IN** May 2018 – July 2018

SOFTWARE DEVELOPMENT INTERN – WINDOWS ANTIVIRUS DEPARTMENT

- Worked primarily on static malware detection in Windows environment.:
- Created a Proof of Concept (PoC) in Python for binary malware classification using Random Forests. Achieved a high classification accuracy and F2 score by engineering just over 30 statically extracted features.
- Ported the PoC to Windows Visual C++. Wrote functions for static feature-extraction, Wrote Windows (Dynamic Linked Libraries) DLLs linking the ML backend with the antivirus
- Integrated the setup into the Antivirus and **deployed into production**
- Towards the end of the internship, created a Python PoC for malicious Android APK detection based on features derived from Android manifest and Dalvik Executable (.dex) files

## PROJECTS

### E-WALLET APPLICATION | JAVA | ANDROID

- Developed the client side (Android application) of an E-wallet payment system
- Designed custom protocols for Peer to Peer (P2P) transactions and Peer to Vendor (P2V) transactions based on offline verification of QR codes that served as acknowledgement tokens
- Implemented basic functionalities like login, session management, transaction requests, QR code generation, offline QR code verification, secret storing and cryptographic primitives.

### BREAKING CAPTCHA USING MACHINE LEARNING | OPENCV | PYTHON | BASH

- Generated Text CAPTCHAs (a 4-charater combination of digits and alphabets disturbed by arbitrary orientation, noise-curves & noise-dots) as a .png file using PyCaptcha library.
- Performed image processing (morphological transformations) followed by image segmentation. Performed a comparative analysis of performance between multiple classifiers trained to recognize individual characters.

### 3-D SURROUNDING SCANNER | JAVA | PROCESSING 3.0 | ARDUINO

- Used an SD webcam and a red linear laser, mounted atop a rotating arm – powered by a stepper motor, to scan the surrounding objects through an angle of 180 degrees.
- Plotted the data points, collected from the video frames, in 3D space using the angle feedback from the stepper motor via the Arduino serial monitor

## RESEARCH EXPERIENCE

**SECURE BOOT FOR EMBEDDED DEVICES |** IOT | RASP PI | ARM TEE Fall 2019 (In Progress)

SUPERVISOR: DR. DHIMAN SAHA, ASSISTANT PROFESSOR, DEPT. EECS, IIT BHILAI

- Studying the ARM Trusted Execution Environment (TEE) implementation – TrustZone, for Linux-based embedded devices
- Designing a secure boot and trusted firmware update framework for ARM-based Linux embedded devices used as Edge Gateways in an IoT Network.
- Working on integrating a Trusted Platform Module – Optiga Trust X, with Raspberry Pi for providing a hardware root of trust to the framework

**DENOISING ADVERSARIAL MALWARE SAMPLES |** PYTHON | KERAS Fall 2019 (In Progress)

SUPERVISOR: DR. SK SUBIDH ALI, ASSISTANT PROFESSOR, DEPT. EECS, IIT BHILAI

- Using a GAN to generate adversarial Windows PE malware examples as an input to an arrangement of denoising autoencoders which aims to de-noise the perturbations introduced
- Primarily focussed on introducing perturbations to non-categorical features such as section entropies, section names etc. against a pre-trained black-box detector
- Achieved a high evasion rate by successfully generating synthetic section and overlay entropies

## TECHNICAL SKILLS AND INTERESTS

- INTERESTS: Machine Learning | Cybersecurity | Cloud Computing
- PROFICIENT LANGUAGES: C | C++ | Python | FAMILIAR WITH: Java | JavaScript | Bash
- APIS: OpenCV | scikit-learn | TensorFlow | Keras
- PLATFORMS: Linux | Windows | EMBEDDED SYSTEMS: Arduino | Raspberry Pi
- SOFTWARE SKILLS: Docker | Git | Bazel | LATEX | Android Studio | Wireshark | Metasploit

## KEY COURSES UNDERTAKEN

- Machine Learning†, Computer System Security†, Cryptography†
- OS, Data Structures and Algorithms, Computer Architecture, Principles of Programming Languages, Networks
- Adversarial Machine Learning†*, Electronic Payment Systems†*, Cryptographic Protocols†*

†GRADUATE-LEVEL COURSE TAKEN AS ELECTIVE | *TAKEN IN THE 2019-2020 FALL SEMESTER

## ACHIEVEMENTS

- ICPC (INTERNATIONAL COLLEGIATE PROGRAMMING CONTEST) 2019 ONLINE ROUND, INDIA – Team Name: PreciS10n | Rank: 225 out of 3700 teams (An ICPC team consist of 3 members from the same institution)
- ACM-ICPC 2018 ASIA GWALIOR-PUNE REGIONALS, INDIA – Team Name: TLERush | Rank: 69 out of 115 qualified teams
- ACM-ICPC 2018 ONLINE CONTEST, INDIA – Team Name: TLERush | Rank: 171 out of 3000 teams
- Qualified for Round 1 of GOOGLE CODE JAM **2018, 2019**
- ALL INDIA RANK **5755** in Joint Entrance Examination (JEE) Advanced 2016 among 150,000 candidates
- ALL INDIA RANK **3107** in Join Entrance Examination (JEE) Mains 2016 among 1.2 million candidates

## EXTRA-CURRICULAR

- GOOGLE DEVELOPER STUDENT CLUB (DSC) IIT BHILAI | Core Member, ML | Instructor at DSC ML boot camps and teaching seminars | 2019-20
- DEBATING SOCIETY | Core Member | Speaker, 3rd Inter-IIT Parliamentary Debate Competition'18 | 2018-20
- NEWS AND MEDIA BODY | Founder & Convener | 2017-18 | DANCE CLUB | Founder & Convener | 2016-17
- STUDENT MENTORSHIP BLOG – POLARIS, 2017 | Editor-in-chief and Moderator | 2017
- NATIONAL SERVICE SCHEME (NSS) IIT BHILAI | Taught at primary schools in villages as part of the NSS teaching cell | 2017-20