Research and Skills Summary

For MS CS Graduate Application (Fall 2022)

Harshvardhan Patel (Firmware Developer - Atonarp)
BTech Computer Science and Engineering (2016-2020)

Research Interests

1. Systems Security
    a. Operating system (Linux) Security
    b. Linux Containers and Cloud Security
    c. Embedded systems security (Micro-architectural attacks)
2. Machine Learning and Cybersecurity
    a. Machine Learning for Malware Detection
    b. Adversarial attacks on ML-based Malware Classifiers
    c. Adversarial Machine Learning
    d. Privacy Preserving Machine Learning
3. Network Security

Experience in Research Interests

1. Application of Machine Learning for Windows PE Malware Detection
   a. Summer Internship (2018) with Max Secure Software - Antivirus Company
   b. Curated a list of 30 features which can be statically extracted from Windows PE file
   c. Evaluated Multiple Ensemble-learning-based classifiers to obtain lowest false-positive score (positive - Malware detected). Prototyping in Python and SciKit Learn
   d. Ported the best performing model to C++ for integration into Max Secure's Production Malware Scanner (Wrote Feature Extractor module in C++, used a High performance Library with C++ APIs)
2. Adversarial Attacks on ML based Malware Detection Engines
   a. Term Paper for Fall 2019 University Elective Course Adversarial Machine Learning
   b. Evaluated a Reinforcement Learning based adversarial attack proposed in an academic paper
   c. Wrote a term paper augmenting the methodology with additional PE features and code examples

Experience in Research Interests

- Trusted Platform Module (TPM 2.0) based Secure Boot, Device Fingerprinting, Remote Attestation
  a. Research Project with Prof. Dhiman Saha under the de.ci.phe.red Lab towards Indigenous 5G Test Bed Project
  b. Studied TPM 2.0 Key Management, Key Hierarchies and NV Ram Storage concepts
  c. Used TPM 2.0 SDK to program an Infineon TPM Chip to act a Root of Trust for Verified Boot
  d. Leveraged TPM 2.0 PCR Extension and TPM PCR Quote signing for communicating boot time firmware measurements (SHA256) over a simple challenge response protocol
  e. Used Raspberry Pi 4, Custom soft-spi driver for gpio-spi emulation and U-Boot to achieve verified boot and measured boot
- Operating Systems Security (Embedded Linux)
  - Working Full time as a Firmware developer at Atonarp
  - Responsible for implementing firmware security measures - High Assurance Boot (HAB), Linux OS Hardening (Linux Devops), Flash storage encryption and Hardware accelerate cryptographic operations (openssl hardware offloading)