Anand Mudgerikar

3685 De Soto Drive, West Lafayette, IN | 765-714-2796
amudgeri@purdue.edu | Website | Linkedin | Google Scholar

Research Interest

My research interests lie in Information Security, Cryptography, Computer Networks and Machine Learning. My research aim is to combine machine learning techniques, like reinforcement learning, with security techniques like intrusion detection to achieve stronger protection of computer systems and networks, while at the same time optimizing network functionality requirements, such as QoS in SDN enabled networks.

Education

Purdue University — West Lafayette, IN
PhD in Computer Science, Advisor: Elisa Bertino — *Jan 2016 – Present*

Purdue University — West Lafayette, IN
Masters in Information Security (CERIAS) — *Jan 2015 – May 2016*

DA-IICT — Gandhinagar, India
Bachelor of Technology in Information and Communication Technology — *Aug. 2009 – May 2013*

Experience

Graduate Research Assistant — Jan 2016 – Present
Purdue University, Advisor: Dr. Elisa Bertino — *West Lafayette, IN*

- Research projects on machine-learning techniques for security and safety of IoT device systems and for security of Computer Networks.
  - Developed a constrained reinforcement learning framework for optimizing user QoS requirements and network functionalities in IoT and SDN environments **(Jarvis, ICDCS 2020)**.
  - Developed a novel approach for optimizing RL based distributed analytics in coalition environments using GAN based domain adaptation developed as part of the **IBM DAIS Project**.
  - Developed a self-adapting, knowledge-driven expert Intrusion Detection System able to detect attacks in real time across a wide range of IoT systems **(Kalis, ICDCS 2017)**.
  - Developed a whitelist-based anomaly detection technique tailored towards IoT devices in order to detect DDoS attacks **(Heimdall IEEE IoT Journal 2017)**.
- Research projects on techniques for protection against cryptographic ransomware.
  - Designed a Systematic Approach for Cryptographic Ransomware Detection using anomaly detection, decoys and hooking techniques in Windows systems **(RW-Guard, RAID 2020)**.
- Research projects on hardware-accelerated cryptographic authentication
  - Developed a new suite of cryptographic mechanisms **(MILCOMM 2015)** as part of my **masters thesis**, employing hardware-acceleration using GPUs to ensure secure and reliable operation in IoVs(Internet of Vehicles) .
  - Provisional Patent filled by Purdue University: **Hardware Accelerated Priority Based Message Authentication for Vehicular Networks** .

Security Research Intern — May 2017 – Dec 2018
HPE Labs, Advisor: Dr. Puneet Sharma — *Palo Alto, CA*

- **E-Spion: Host based Intrusion Detection for IoT Devices (Asia CCS 2019)**
  - Developed a system level anomaly based Intrusion Detection system on the edge which profiles IoT device behaviors.
  - Patent filled by HPE: **Detecting attacks on computing devices, US20190238567A1**
- **Dito IoT HoneyPot (HPE TechCon 2017)**
  - Developed a high interaction 'best effort' honey pot system which replicates IoT devices on the network.
  - Runners up in HPE internship projects fair 2017.

Security Architecture Intern — May 2016 – Aug 2016
IBM Research, Advisor: Dr. Ashish Kundu — *Yorktown Heights, NY*

- Worked on designing the Single sign-on (SSO) security architecture for the educational platform of IBM Watson.

Research Associate July 2013 – Nov 2014
TIFAC, DST Govt. of India *New Delhi, India*

- Conducted a research study to analyze the security threats in 3rd party applications and responsible for ensuring network security to prevent any unauthorized access.
- Worked on improving the IPSec standard by incorporating secure Multicast functionality using multi-party key computation.

Graduate Teaching Assistant Jan 2016 – Dec 2016
Purdue University *West Lafayette, IN*

- Worked as a teaching assistant for courses CS240: Programming in C and CS381: Introduction to Analysis of Algorithms.

Publications

Mudgerikar A. and Bertino E., **Jarvis: Moving towards a smarter IoT using RL**, ICDCS 2020
Mudgerikar A., Sharma P. and Bertino E., **Edge based Intrusion Detection for the Internet Of Things**, ACM Transactions on Management Information Systems, 'Special Issue on Analytics for Cybersecurity and Privacy', 2020.
Mudgerikar A., Sharma P. and Bertino E., **E-Spion: System Level Intrusion Detection for the Internet Of Things**, AsiaCCS 2019.
Mehnaz S., **Mudgerikar A.** and Bertino E., **RWGuard: An Approach for Detection and Recovery of Cryptographic RansomWare**, RAID 2018, pp. 114-136.
Midi D., **Mudgerikar A.**, Rullo N. and Bertino E., **Kalis - A System for Knowledge-driven Adaptable Intrusion Detection for the Internet of Things**, ICDCS 2017
Yavuz A., **Mudgerikar A.**, Singla A., I. Papapanagiotou and Bertino E.,**Real-Time Digital Signatures for Time-Critical Networks** IEEE Transactions on Information Forensics and Security 2017
Midi D., Habibi J., **Mudgerikar A.** and Bertino E., **Heimdall: Mitigating the Internet of Insecure Things**, IEEE Internet of Things Journal 2017
Singla A., **Mudgerikar A.**, Papapanagiotou I. and Yavuz A., **HAA: Hardware-Accelerated Authentication for Internet of Things in Mission Critical Vehicular Networks**, MILCOMM 2015
Mudgerikar A. and Das M.L., **Secure multicast using IPsec and multi-party key computation**, Int. J. Internet Technology and Secured Transactions, Inderscience Publications, Vol. 5, No. 2, pp.149-162.

Patents

Patent Disclosure, **Detecting attacks on computing devices** , US20190238567A1 Patent Disclosure, **Hardware Accelerated Priority Based Message Authentication for Vehicular Networks**, OTC:2015-PAPA-67164

Technical Skills

Languages: C++, C, Java, Python, PHP, SQL, JavaScript, Android Development, CUDA.
Security: Network Intrusion Detection, Malware Analysis, Cryptography
Tools: Wireshark, Nmap, OpenVAS, Nessus, MetaSploit, Ollydgb, Kali Linux, Android Reverse Engineering.
Machine Learning: Reinforcement Learning, System Modelling
Tools: OpenAI gym, NumPy, Pandas, Tensorflow, Scikit-learn, Keras
General: OpenFlow, openSSL, ns2, SmartThings, IFTTT, Vim, Git, VirtualBox, Django Framework, MATLAB, MySQL, Latex.

Interests

Brazilian Jiu Jitsu, Table Tennis, Soccer, Cricket, Dota 2
College Representative (DA-IICT), IN-CTF and member of B01lers CTF Group, Purdue.
Captain of College Table Tennis Team, DA-IICT, India (2009-2013)
Coordinator of BattleDrome, LAN Gaming event in DA-IICT's Techno-Cultural festival, India