Pritam Dash

2366 Main Mall, Vancouver, BC V6T 1Z4, Canada • **E-mail:** pdash@ece.ubc.ca

RESEARCH INTEREST

Reliable and Secure Systems, Machine Learning, Autonomous Systems.

EDUCATION

PhD in Electrical and Computer Engineering Sep 2020 – Present	University of British Columbia, Canada Advisor: Dr. Karthik Pattabiraman
MASc in Electrical and Computer Engineering Sep 2018 – Aug 2020	University of British Columbia, Canada Advisor : Dr. Karthik Pattabiraman
MS in Software Engineering (BS+MS Integrated Program) Jul 2011-May 2016	Vellore Institute of Technology, India

AWARDS AND HONORS

- Exemplary talk mention at Usenix Enigma'2022 link
- Best paper award at IEEE/IFIP DSN'2021 (flagship venue in the field of Dependable Computing research).
- Master's thesis featured in SERENE-RISC as top ten cybersecurity development in Canada – 2020.
- The University of British Columbia Four Year Fellowship (4YF) for doctoral studies – 2020. Given to the top 10 students in each incoming class of graduate students.
- President's Academic Excellence Award (UBC) – 2020, 2021, 2022.
- Conference travel grants ACSAC'19, DSN'19, Enigma'22.
- DAAD Working Internship in Science and Engineering Fellowship – 2015.
- Indian Academy of Sciences Research Fellowship – 2014, 2015 (~120 students selected across India).

RESEARCH EXPERIENCE

Research Intern at Oracle Labs, Vancouver, Canada **Jul 2022 – Dec 2022**

Research Area: AI for Software Development

- Designed a novel pre-training approach for BERT Model for improved understanding of semantic details in source code. This improves BERT model's zero-shot performance in downstream code automation tasks.

Research Assistant at the University of British Columbia, Vancouver, Canada **Sept 2018 – Present**

Secure and Reliable Autonomous Systems (research featured in News, EurekaAlert, TechXplore, GlobalNews)

- Proposed methods to detect and recover (operate safely despite the malicious intervention) autonomous vehicles from sensor spoofing attacks using feed-forward control and data-driven modeling.
- Highlighted vulnerabilities in state-of-the-art model-based attack detection techniques that can be exploited to launch new types of (stealthy) attacks against robotic aerial and ground vehicles.
- Highlighted vulnerabilities in swarm control algorithms that can be exploited to disrupt drone swarms via GPS spoofing. Proposed a fuzzer that discovers such vulnerabilities and helps secure drone swarms.

Machine Learning Security

- Proposed methods to detect and mitigate physically realizable adversarial attacks (patch attacks) against image classification models. This allows the models to predict robust outputs despite malicious inputs.

Side-channel leaks to Active Attacks in Cyber-Physical Systems (CPS)

- Demonstrated the limitations of end-to-end encryption protocols in CPS (e.g., water treatment plants, electric grids), and proposed side channel attacks that'd compromise components of the CPS.

Research Engineer at (IAIK) Graz University of Technology, Austria **Jan 2017 – Aug 2018**

Research areas: Applied Cryptography, End-to-End Confidentiality, Privacy.
Involved in CREDENTIAL EU Horizon 2020 Project. Key contributions are as follows:

- Designed a crypto framework for end-to-end confidentiality (IAIK-JCE extension) in federated identity management cloud services. This approach is used by three services providers in Germany and Italy.
- Lead the technical aspects of 'Liaisons and Standardization' activities of the CREDENTIAL project which resulted in developing as new cryptographic and privacy-preserving catalogue for making transparent quality assessment of cloud services. This is used by EuroCloud StarAudit.

Research Intern at Institute for Infocomm Research (I2R) – A*STAR, Singapore **Jan – Jun 2016**

- Developed game-based techniques for cyber security training and awareness.

Research Intern at Fraunhofer SIT, Darmstadt, Germany **Jun – Jul 2015**

- Investigated impact of code changes on security assurance cases of software.

SELECTED PUBLICATIONS

Talks **Pritam Dash**, "*Detection is not Enough: Attack Resilience for Safe and Robust Autonomous Robotic Vehicles*", Usenix Enigma 2022. Talk (Exemplary talk mention link).

Conferences Zitao Chen, **Pritam Dash**, Karthik Pattabiraman, "Jujutsu: A Two-stage Defense against Adversarial Patch Attacks on Deep Neural Networks", AsiaCCS 2023. Preprint arXiv.

Pritam Dash, Guanpeng Li, Zitao Chen, Mehdi Karimibiuki, Karthik Pattabiraman, "*PID-Piper: Recovering Robotic Vehicles from Physical Attacks*", IEEE/IFIP Dependable Systems and Networks (DSN) 2021. Acceptance Rate 16.4%.
Best paper award (1 out of ~300 submissions) Talk

Pritam Dash, Mehdi Karimibiuki, and Karthik Pattabiraman, "*Out of Control: Stealthy Attacks on Robotic Vehicles Protected by Control-Based Techniques*", ACM ACSAC 2019. Acceptance Rate 22.6%. Work featured in EurekaAlert, TechXplore, GlobalNews.

Demo/ Poster Yingao Yao, **Pritam Dash**, Karthik Pattabiraman, "*May the Swarm Be with You: Sensor Spoofing Attacks Against Drone Swarms*". ACM CCS 2022

Pritam Dash, and Karthik Pattabiraman, "*Demo: Recovering Autonomous Robotic Vehicles from Physical Attacks*". AutoSec @NDSS 2022.

Pritam Dash, Mehdi Karimibiuki, and Karthik Pattabiraman, "*Demo: Impact of Stealthy Attacks on Robotic Vehicle missions*". AutoSec @NDSS 2021.

Preprint (In submission) **Pritam Dash**, Guanpeng Li, Mehdi Karimi, Karthik Pattabiraman, "Replay-based Recovery for Autonomous Robotic Vehicles from Sensor Deception Attacks", preprint arXIV

PROFESSIONAL SERVICES

Conferences Reviewed papers at DSN'22, DSN'21, DSN'20, ISSRE'22, ISSRE'21, and QRS'19.

Mentorship Co-supervised a master student and undergraduate student at UBC (2021-2022).
Supervised summer research student at IAIK, TU Graz (Summer 2018)

Advisory Member of Advisory Board, EuroCloud StarAudit Certification Programme.

Date: March 1, 2023
Place: Vancouver, Canada

Pritam Dash