Reetwik Das

reetwik12@gmail.com @reetwik12 reetwik-das reetwik12

Education

2020 – present **MS + Ph.D., Department of Computer Science & Engineering, IIT Madras**.

2014 – 2018 **B.Tech. Department of Computer Science & Engineering, NIT Goa**.

Research Interests

Securing AI/ML models against adversarial attacks, Hardware Security,

Projects

Reverse Engineering ANN — A black-box attack that uses Fault injections on ANN models, and observes the change in model output to extract the model parameters.

Fault resistant ANNs — Countermeasures to protect the ANN models deployed on embedded devices from fault injection attacks.

Confusion Neurons — Countermeasures preventing an adversary to extract a trained DNN model under white-box access.

Ph.D. Forum

1 R. Das, N. Singh, and C. Rebeiro, "Metrics for evaluating fault injection attacks on artificial neural networks," *IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 2021.

Work Experience

Feb 2024 – Aug 2024 **Research Intern, Robert Bosch GmbH, Renningen, Germany.** Developing countermeasures preventing an adversary to extract trained DNN models under white-box access.

July 2018 – Aug 2020 **Consultant (INFOSEC), Microsoft IGD, Hyderabad.** Threat modelling, security code review and penetration testing of applications developed by Microsoft IGD.

May 2017 – July 2017 **Research Intern, National Institute of Technology Karnataka, Surathkal.** Dialect based classification of speech recognition using random forest classifier.

Jan 2021 – Nov 2023 **Teaching Assistant, IIT Madras.** Secure Processor Micro-architecture (July-Nov 2024), (July-Nov 2022) | Paradigms of Programming (July-Nov 2023) | Secure System Engineering (Jan-May 2023), (Jan-May 2022) | Operating Systems (July-Nov 2021) | Introduction to programming (Jan-May 2021)

Skills

Coding — C/C++, Python, Julia

Tools and Frameworks — Docker, Scrapy, Tensorflow, LaTeX.

Achievements

2023 **Star TA (Teaching Assistant) Award**, CSE Department, IIT Madras, for Secure Processor Microarchitecture course.

2022 **Best Learner Award**, Poster Day, CSE Department, IIT Madras, for answering the maximum number of MCQs correctly in the posters presented.

2019 **Super Rookie Award**, Apps Domain, Microsoft IGD, for identifying critical security bugs present in a developed application.

People's Choice Award, Machathon, Microsoft, for the prototype of a solution developed in a 2-day Hackathon.

Extracurricular activities

2022 Organized esCTF, a nationwide embedded security CTF competition in IIT Madras.

2022-2023 Represented Pampa hostel in Inter hostel sports events in Chess and Table tennis.

2017-2018 Campus ambassador of Inter NIT competitive coding event, Codathon.

2017 Represented NIT Goa in ACM ICPC, Regionals.

Organized technical and cultural fests of NIT Goa.

References

Prof. Chester Rebeiro (Ph.D. Advisor)
Associate Professor,
Department of Computer Science & Engineering
Indian Institute of Technology Madras, Chennai, India
Email: chester@cse.iitm.ac.in
Web: http://www.cse.iitm.ac.in/~chester/