ASHISH HOODA

https://pages.cs.wisc.edu/~hooda

EDUCATION

University of Wisconsin-Madison, Madison, WI — Aug 2019 - Present
Doctoral Student, Computer Science

Indian Institute of Technology, Delhi, India — July 2014 - May 2018
B.E. in Electrical Engineering (*Minor in Computer Science*)

INTERESTS

Security & Privacy, Computer Vision, Large Language Models, Graph Learning

PUBLICATIONS

* : CO FIRST AUTHORS

PRP: Propagating Universal Perturbations to Attack LLM Guard-Rails
Ashish Hooda*, Neal Mangaokar*, Jihye Choi, Shreyas Chandrashekaran, Kassem Fawaz, Somesh Jha, Atul Prakash
Preprint *[Paper]*

Do Large Code Models Understand Programming Concepts? A Black-box Approach
Ashish Hooda, Mihai Christodorescu, Miltos Allamanis, Aaron Wilson, Kassem Fawaz, Somesh Jha
Preprint *[Paper]*

D4: Detection of Adversarial Diffusion Deepfakes Using Disjoint Ensembles
Ashish Hooda*, Neal Mangaokar*, Ryan Feng, Kassem Fawaz, Somesh Jha, Atul Prakash
WACV 2024 (*IEEE/CVF Winter Conference on Applications of Computer Vision*) *[Paper]*

Experimental Analyses of Physical Surveillance Risks in Client-Side Content Scanning
Ashish Hooda, Andrey Labunets, Tadayoshi Kohno, Earlence Fernandes
NDSS 2024 (*Network and Distributed System Security Symposium*) *[Paper]*

Theoretically Principled Trade-off for Stateful Defenses against Query-Based Black-Box Attacks
Ashish Hooda*, Neal Mangaokar*, Ryan Feng*, Kassem Fawaz, Somesh Jha, Atul Prakash
ICML 2023 (*2nd AdvML Frontiers Workshop*) *[Paper]*

Stateful Defenses for Machine Learning Models Are Not Yet Secure Against Black-box Attacks
Ashish Hooda*, Neal Mangaokar*, Ryan Feng*, Kassem Fawaz, Somesh Jha, Atul Prakash
CCS 2023 *(ACM Conference on Computer and Communications Security)* *[Paper]*

SkillFence: A Systems Approach to Mitigating Voice-Based Confusion Attacks
Ashish Hooda, Matthew Wallace, Kushal Jhunjhunwalla, Earlence Fernandes, Kassem Fawaz
IMWUT 2022 (*ACM Interactive, Mobile, Wearable and Ubiquitous Technologies*) *[Paper]*

Invisible Perturbations: Physical Adv Examples Exploiting the Rolling Shutter Effect
Ashish Hooda*, Athena Sayles*, Mohit Gupta, Rahul Chatterjee, Earlence Fernandes
CVPR 2021 (*Conference on Computer Vision and Pattern Recognition*) *[Paper]*

WORK EXPERIENCE

Research Intern @ Google Research — Jul 2023 - Nov 2023
Supervisor: Mihai Christodorescu, Miltos Allamanis
Internship with the Android Security and Learning for Code teams. Worked on evaluating program semantics understanding of Large Language Models for Code.

Open Source Contributor @ Langroid — May 2023 - Present
Working on Langroid : a Multi-Agent Framework for developing LLM Applications.

Applied Scientist Intern @ Amazon AWS Research — Jun 2022 - Sep 2022
Supervisor: Ali Torkamani
Developed an efficient Graph Neural Network training framework that scales to billion node scale graphs. Utilized residual quantization to reduce codebook size without sacrificing precision. Demonstrated memory and compute efficiency on the largest Open Graph Benchmark dataset - ogbn-papers100M.

Software Engineer @ Microsoft India R&D — Jun 2018 - Jul 2019
Worked on Omnichannel Engagement Hub in the Dynamics CRM team; Created a Microsoft Azure Service-Fabric based service for configuring presence of a user. Proposed and Implemented a probabilistic distribution model for agent assignment with real-time feedback.

INVITED TALKS

Do Code LLMs understand program semantics? *Google Learning for Code Team*, Nov 2023

Do Stateful Defenses Work Against Black-Box Attacks? *Google AI Red Team*, Oct 2023

Deepfake Detection Against Adaptive Attackers *Google AI Red Team*, Aug 2023

TECHNICAL

Languages: Python, Java, C++, C, MATLAB

Frameworks/Libraries: PyTorch, Tensorflow, Apache Spark, Deep Graph Library

SERVICE

- Reviewer: ICML 2024
- Reviewer: Workshop on Understanding of Foundation Models (ME-FoMo), ICLR 2023, 2024
- Artifact Evaluation Committee Member: USENIX Security Symposium '22
- External Reviewer: USENIX Security Symposium
- External Reviewer: IEEE Symposium on Security and Privacy (IEEE S&P)
- External Reviewer: IEEE SaTML
- Mentor at Individualized Cybersecurity Research Mentoring (iMentor) Workshop 2023

AWARDS & ACHIEVEMENTS

- Accepted for NDSS Travel Grant 2024.
- Accepted to WACV Doctoral Consortium 2024.
- Runner up in CS Research Symposium, 2022 (UW Madison).
- Qualified for regionals at ACM International Collegiate Programming Contest (ICPC), 2017.
- Runner-up at Microsoft CODE-FUN-DO Hackathon, 2015.
- Secured **All India Rank 4** in Central Board of Secondary Education (CBSE) Board Examination given by over 2 million students.
- Secured **All India Rank 17** in Joint Entrance Exam (JEE) given by over 1 million students.
- Selected for Special Class Railway Apprentice (SCRA) (Top 100 out of over 0.1 million applicants).
- Awarded the Junior Science Talent Search Examination (JSTSE) Scholarship.