





Mohammad Saidur Rahman


Ph.D. Student

 saidur.rahman@mail.rit.edu

 +1 (585) 284-4652

 rahmanmsaidur.com

 msrocean

 msrocean

 Rochester, NY, USA.

Education

Ph.D. in Computing & Information Sciences

August, 2018 - Present

Rochester Institute of Technology

Courses: Deep Learning for Vision, Sensor and SCADA Security, Cyberinfrastructure Foundations, Quantitative Foundations

CGPA: 3.95/4.00

MS in Computing Security

Rochester Institute of Technology

Courses: Penetration Testing, Network Security, Internet Security & Privacy, Cryptography & Authentication, Machine Learning
August, 2018 | **CGPA: 3.88/4.00**

Bachelor in Management Information Systems (MIS)

University of Dhaka

July 2016 | **CGPA: 3.74/4.00**

Skills

Programming: Python, C, MATLAB, C++ (basic), Java (basic), Bash

Machine Learning & Deep Learning : TensorFlow, Keras, PyTorch

Security Tools: CobaltStrike, Armitage, Metasploit-Framework, Nmap, Netcat, Cryptcat Socat, OpenVAS, Nessus, Snort

Networking: TCP, UDP, BGP, VLAN, Access Control, Firewalls, IDS, IPS

OS: Ubuntu, Kali Linux, CentOS, Red Hat Linux, Linux Mint, XUbuntu, Windows

Non-Technical: Leadership, Strategic Planning, Project Management, Negotiation, Team Work

Employment

Graduate Research Assistant

January 2017 - Present

Center for Cybersecurity, Rochester Institute of Technology

Research Area(s): Security & Privacy, Deep Learning, and Adversarial Machine Learning.

Graduate Teaching Assistant

Spring 2020, '19, & '18

Rochester Institute of Technology

Course CSEC-759.01: Deep Learning Security, Anonymity & Tor, Internet Security & Privacy.

Developed Simulations: i) Timing Analysis of Network Traffic, ii) Website Fingerprinting with Deep Learning, iii) LSTM for Attack Prediction, and iv) Fooling a CNN with Adversarial Examples.

Publications, Posters, & Tech Reports

arXiv

MS Rahman, M Imani, N Mathews, M Wright, "Mockingbird: Defending Against Deep-Learning-Based Website Fingerprinting Attacks with Adversarial Traces".

PETS 2020

MS Rahman, P Sirinam, N Mathews, KG Gangadhara, M Wright, "Tik-Tok: The Utility of Packet Timing in Website Fingerprinting Attacks".

ACM CCS 2019

P Sirinam, N Mathews, MS Rahman, M Wright, "Triplet Fingerprinting: More Practical and Portable Website Fingerprinting with N-shot Learning".

MS Rahman, N Mathews, and M Wright, "POSTER: Video Fingerprinting in Tor".

N Mathews, MS Rahman, and M Wright, "POSTER: Evaluating Security Metrics for Website Fingerprinting".

ACM CCS 2018

M Imani, MS Rahman, M Wright, "POSTER: Adversarial Traces for Website Fingerprinting Defense".

IEEE S&P 2018

MS Rahman, KG Gangadhara, P Sirinam, M Wright, "POSTER: Using Packet Timing in Website Fingerprinting".

P Sirinam, MS Rahman, KG Gangadhara, M Wright, "POSTER: Website Fingerprinting Attacks with Timing-based Features using Capsule Networks".

Awards & Grants

CCS 2019 Travel Grant

Travel grant received to attend ACM Conference on Computer and Communications Security (CCS) 2019.

Bronze Medal Winner

Category: Computations & Applications, 8th Annual Conference of the UPSTATE Chapters of the American Statistical Association.

Awards at Rochester Institute of Technology

- Winner at 3-Minute Thesis Presentation Competition 2018.

- Winner at Graduate Research Showcase 2017.

Certification

- **Mathematics for Machine Learning Specialization**

- **Deep Learning Specialization**

Coursera