14500 Roadrunner Way
APT 314
San Antonio, TX 78249

Mir Mehedi A. Pritom

mirmehedi.pritom@utsa.edu
Mo: +1(706)-308-8671
LinkedIn: www.linkedin.com/in/mpritom
Webpage: webpages.uncc.edu/mpritom/

Education

Ph.D. Student in Computer Science — Jan 2019 - Present
University of Texas at San Antonio, TX, USA; **CGPA: 4.00**
Concentration: Cyber Security and Threat Intelligence

Master of Science in Information Technology — Aug 2015 - Dec 2018
University of North Carolina at Charlotte, NC, USA; **GPA: 3.70**
Concentration: Security and Privacy

Bachelor of Science in Computer Science & Engineering — Feb 2010 - Apr 2014
University of Dhaka, Bangladesh; **GPA: 3.64**

Professional Experience

Graduate Research Assistant — May 2019 - Present
Laboratory of Cybersecurity Dynamics (LCD)
University of Texas at San Antonio, TX, USA

- Working on projects in the direction of Cyber Threat Intelligence, Security Analytics, applying ML and Blockchains for Cybersecurity Management

Graduate Research Assistant — May 2016 - Aug 2016
Center for Cybersecurity Analytics and Automation (CCAA)
University of North Carolina at Charlotte, NC, USA

- **Predicting 0-day Malicious IP Addresses using Cyber Threat Intelligence:** Proposed new strategy for predicting maliciousness (i.e., hosting phishing website, malware attacks) of networks based on 'shared Hosting' and 'bad neighborhood' characteristics which can predict 88% of the zero-day malware instances missed by top 5 AVs and successfully block 68% of the phishing websites before reported in Phishtank.

Software Engineer — Sep 2014 - Aug 2015
Samsung Research & Development Institute Bangladesh, Dhaka

- Developed efficient and robust web-based mobile applications (games, utility apps) for Tizen Platform (JavaScript, HTML, CSS, C++)
- Learned agile software development, worked in full software development cycle

Graduate Teaching Assistant
Dept. of Software and Information Systems, UNC Charlotte, NC, USA
Dept. of Computer Science, UT San Antonio, TX, USA

- **Secure Software Development and Analysis** (CS 4683) at UTSA — Spring 2019
- **Cyber Operations** (CS 4673) at UTSA — Fall 2018
- **Secure Programming and Penetration Testing** (ITIS 4221/5221) at UNCC — Summer 2018
- **Network-Based Application Development** (ITIS 4166) UNCC — Spring 2018
- **IT Infrastructure II: Design and Practise** (ITIS 3110) at UNCC — Fall 2017
- **Intro to Security and Analytics** (ITIS 5260) at UNCC — Summer 2017
- **Introduction to Information Security and Privacy** (ITIS 3200) UNCC — Spring 2017
- **Advanced Network Security** (ITIS 6167/8167) at UNCC — Fall 2016
- Fall 2015

Technical Skills

- **Languages:** C/C++ (prior experience), Java (proficient), R (proficient), Python (proficient), JavaScript (prior experience), PHP (prior experience), MySQL (prior experience)
- **Tools and Environments:** RStudio, Visual Studio, IntelliJ IDEA, Eclipse, PyCharm, Anaconda, Fortify Static Code Analyzer, IBM SPSS, Xampp, Burp Suite, VBox, Vagrant, VMWare Workstation 12.0, Wireshark, Bro IDS/IPS, Git.
- Hands-on experience in Machine Learning and Deep Learning platform (**Scikit-Learn**, **Tensorflow, Keras**)
- Hands-on experience with Palo Alto Network's next-generation Firewalls and IDS.
- Good research practices, writing skills, and problem-solving capabilities.
- Good analytical knowledge for getting insights about security and other datasets.
- **OS:** Windows, Ubuntu, Macintosh.
- Others: Problem-solving in UVa Online Judge (http://uhunt.onlinejudge.org/id/618960)

Academic Project Highlights

- **Blockchain-based Cyber Security Management:** We are building an innovative Blockchain-based Cyber Security Management (B2CSM) system, which can automate the process for further investigating the effect of APTs on our systems based on the relevant historical data and characteristics of the APT received from the third party. We are studying a way to leverage Blockchain to ensure the integrity of the historical data as APTs try to manipulate those for hiding footprints.
- **Open-source Cyber Threat Intel (CTI) Feed Analysis:** CTI helps identify indicators of compromise (e.g., IPs, domains, hashes) before they can actively compromise different organizations. We collect CTI data from the open-source repository; we analyze existing feeds to measure their reputation using the 'Combine' (python based) tool. This reputation can further help us compare the feeds and reduce the search space while using these feeds in future research.
- **Predicting the 'cause' and 'factors' for leaving schools:** With R programming, we are extracting in-depth factors for predicting root-cause of the withdrawal of students from Cabarrus County "K-12 semi-structured dataset" using standard data mining techniques such as correlation analysis, linear regression analysis, categorical data analysis, pattern mining, classification (random forest, neural networks), and frequent pattern mining.
- **Static Analysis of Java Web App:** Finding and fixing SQL, persistent and nonpersistent XSS vulnerabilities from an existing Java-based web application that had database connections, login facilities, in-app commenting, and buying products with pen-testing and static analysis.

Leadership and Volunteering

- General Secretary, CCI Grad Students' Organization, UNC Charlotte (CCI-Grads) Oct 2017 - Oct 2018

- President, Bangladesh Student Organization at UNC Charlotte Mar 2018 - Dec 2018

Publications

[J1] **Mir Mehedi A Pritom**, Sujan Sarker, Md. Abdur Razzaque, Mohammad Mehedi Hassan, M. Anwar Hossain, Abdulhameed Alelaiwi, **"A Multiconstrained QoS Aware MAC Protocol for Cluster-Based Cognitive Radio Sensor Networks"**, International Journal of Distributed Sensor Networks (IJDSN) 2014.
[C1] Amirreza Niakanlahiji, **Mir Mehedi Pritom**, Bei-Tseng Chu and Ehab Al-Shaer, **"Predicting Zero-day Malicious IP Addresses"**, SafeConfig: Applying the Scientific Method to Active Cyber Defense Research workshop in ACM CCS 2017
[C2] **Mir Mehedi A Pritom**, Chuqin Li, Bill Chu, Xi Niu, **"A Study on Log Analysis Approaches Using Sandia Dataset",** Network Security Analytics and Automation Workshop in ICCCN 2017.
[C3] Md Nazmus Sakib Miazi, **Mir Mehedi A Pritom**, Mohamed Shehab, Bill Chu, Jinpeng Wei, **"The Design of Cyber Threat Hunting Games: A Case Study",** Network Security Analytics and Automation Workshop in ICCCN 2017.
[P1] **Mir Mehedi A Pritom**, Amirreza Niakanlahiji, Bill Chu, **"Proactive Connection Blocking Based on Cyber Threat Intelligence (CTI)"**, 17th Annual Graduate Research Symposium at UNC Charlotte, March 2017 **(Won 2nd place among Computer Science, Math and Engineering Posters)**