CV of MOHIUDDIN AHMED
(980)-267-0371 | sohel.buet.cse.07@gmail.com | mahmed27@uncc.edu
Website | LinkedIn | GitHub | Google Scholar

Education

Doctor of Philosophy in Software and Information System [August 2016 - May 2023]
University of North Carolina at Charlotte, NC, USA

Bachelor of Science in Computer Science and Engineering [January 2008 - February 2013]
Bangladesh University of Engineering and Technology(BUET), Dhaka, Bangladesh

Dissertation Research & Projects

UNC Charlotte
NC, USA

AUTO-Hunter, Distributed Hierarchical Event Monitoring System for Attack Diagnosis through Active Investigation of Attacker Activities. [August 2020 - till date]

- Designed and implemented distributed hierarchical event monitoring system to reduce attack detection time, communication overhead and resource usages.
- Designed and developed low-level log collecting agents for windows system (ETW, event logs, syslog, NetFlow).
- Developed detectors to map low-level traces to MITRE ATT&CK technique and evidential reasoing framework which performs passive reasoning and active investigation on reported observables.
- *Development Languages/Tools:* Python, Java, RabbitMQ, ElasticSearch, Docker.

Critical Security Control (CSC) Validation, Automated extraction of threat action, observables, and development of key measurement indicators (KMI) and metrics for KMI of each CSC. [August 2018 - May 2020]

TTPDrill, Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources and mapping of threat actions to MITRE ATT&CK techniques. [January 2017 - July 2018]

- Extracted threat action from CTI reports using NLP and mapped the extracted threat actions to MITRE ATT&CK techniques and tactics using document similarity measures TF-IDF.
- *Development Language:* Java.

Publications

UNC Charlotte
NC, USA

- **Mohiuddin Ahmed**, Jinpeng Wei, Ehab Al-Shaer **(Recently Accepted)**. SCAHunter: Scalable Threat Hunting through Decentralized Hierarchical Monitoring Agent Architecture. (Computing 2023).
- **Mohiuddin Ahmed**, Jinpeng Wei, Yongge Wang and Ehab Al-Shaer. (2018). A Poisoning Attack Against Cryptocurrency Mining Pools. (CBT 2018).
- **Mohiuddin Ahmed**, Ehab Al-Shaer. (2019). Measures and metrics for the enforcement of critical security controls: a case study of boundary defense. (Poster presentation in HOTSOS 2019).
- Ghaith Husari, Ehab Al-Shaer, **Mohiuddin Ahmed**, Bill Chu, and Xi Niu. (2017). TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources. (ACSAC 2017).
- Rawan Al-Shaer, **Mohiuddin Ahmed**, Ehab Al-Shaer. (2018). Statistical Learning of APT TTP Chains from MITRE ATT&CK. (Poster presentation in ACSAC 2018).
- Mohammed Noraden Alsaleh, Jinpeng Wei, Ehab Al-Shaer and **Mohiuddin Ahmed**. (2018). gExtractor: Towards Automated Extraction of Malware Deception Parameters. (SSPREW-8, 2018).

Professional Skills

- **Programming Language:**
  – **Expert:** Python, Java, C++, C, Prolog; – **Working Knowledge:** R, Android, C#
- **Web Development and Scripting:** Shell Scripting, PHP, JavaScript, HTML5, SQL
- **Databases:** – **RDMS**: MySQL, Oracle SQL; – **NoSQL**: Elasticsearch
- **Frameworks:** Spring, Laravel, MODX CMS; • **Visualization Tools:** UML, Weka, Gephi
- **Version Control:** Git; • **Virtualization Tools:** VirtualBox, VMWare, Docker
- **Tools/Frameworks:** IDAPro, Sysmon, OllyDbg, Splunk, Scrum/Agile development
- **Machine Learning Libraries:** Standford CoreNLP, AllenNLP, NLTK, Scikit-learn, Keras
- **Cyber Security Research:** Cyber Threat Hunting, Malware Analysis, Mitre ATT&CK Framework, Critical Security Control, Bayesian Network, Uncertainty Reasoning

Professional Services

Teaching Assistant [August 2016 - April 2023]
Research Assistant, UNC Charlotte [August 2016 - July 2020]

- Developed distributed security analytics for distributed threat hunting and taught, designed, and prepared graduate courses.

Software Engineer, Security Lab(R&D) [March 2014 - December 2015]
Team Lead, Security Lab(R&D) [January 2016 - June 2016]
Kona Software Lab Ltd, Dhaka, Bangladesh which is a part of Kona I.

- Implemented dynamic libraries(.dll, .so, and .dylib) and different corresponding toolkits for PKI system and CA using Java and C++ that comply with PKCS#11, FIPS, KISA and PKCS#7.

Junior Software Engineer [March 2013 - February 2014]
Nascenia, Dhaka, Bangladesh.

- Integrated different betting API's in betting website using PHP and MODX CMS.

Professional Projects

PKI-Middleware, a PKCS#11 dynamic library developed for Windows, Linux, MAC and Android platform which complies KISA and FIPS standards. [May 2014 - December 2015]

- Implemented Multithreading and Multiprocessing, Smart Card Profile Initialization, key operation (RSA key, Secret key (DES3, AES, MAC, SEED) and Random Number Generation), and sign operation (Signature generation and verification, Symmetric and Asymmetric key encryption and decryption, MAC Generation and verification).
- *Development Language:* C++, JNI.

Custom CSP, *Cryptographic Service Provider* is a MSDN Compatible library that implements the Microsoft's CryptoAPI (CAPI). This CSP is used to enable NFC-based smart card authentication in Windows OS. [January 2016 - April 2016]

- *Development Language:* C++, Windows API.

CMS *(Cryptographic Message Syntax)*, a PKCS#7 based toolkit developed to support CA System during certificate Issue that supports all data types (*Signed, Enveloped, SignedAndEnveloped, data*) of PKCS#7 and their operations. [May 2015 - June 2015]

- *Development Language:* Java.

PKI-Middleware Wrapper is a Java wrapper to use PKCS#11 middleware library in Java Application. It reduces maintenance complexity of **JNI**, so that application developer don't have to write core C code to handle function call of PKCS#11 library. [January 2015 - March 2015]

- *Development Language:* Java.

Teaching Experiences

As a Teaching Assistant, I taught and assisted course instructors in following undergraduate and graduate courses to prepare course materials, assignments, quiz and exam questions, and conduct class when instructor is absent-

- **Intro to Info Security and Privacy** (ITIS3200)- An introductory overview of key issues and solutions for information security and privacy. Topics include: security concepts and mechanisms; security technologies; authentication mechanisms; mandatory and discretionary controls; basic cryptography and its applications; intrusion detection and prevention; information systems assurance; anonymity and privacy issues for information systems. [Fall 2016, Fall 2017, Fall 2019]
- **Principles of Info Security and Privacy** (ITIS6200, ITIS8200)- Topics include: security concepts and mechanisms; security technologies; authentication mechanisms; mandatory and discretionary controls; basic cryptography and its applications; intrusion detection and prevention; information systems assurance; anonymity and privacy issues for information systems. [Spring 2018, Fall 2018, Spring 2019, Spring 2021, Fall 2021]

UNC Charlotte
NC, USA

- **Knowledge Discovery in Database** (ITIS6162)- The entire knowledge discovery process is covered in this course. Topics include: setting up a problem, data prepossessing and warehousing, data mining in search for knowledge, knowledge evaluation, visualization and application in decision making. A broad range of systems, such as OLAP, LERS, DatalogicR+, C4.5, AQ15, Forty-Niner, CN2, QRAS, and discretization algorithms are covered. [Spring 2020]
- **Secure Programming and Penetration Testing** (ITIS4221, ITIS5221)- Techniques for web application penetration testing, secure software development techniques for network based applications. Automated approaches such as static code analysis and application scanning are also discussed. [Fall 2020]
- **Intro to Operating System and Networking** (ITSC3146)- Introduces the fundamentals of operating systems together with the basics of networking and communications. Topics include: processes, thread, scheduling, cache, memory management, file systems, inter-process communication, network architecture and protocols, HTTP, MAC, IP, TCP/UPD, and Internet routing. [Spring 2017]
- **Software Engineering** (ITSC3155)- An introduction to software engineering, which advances the study and application of engineering principles, methods, and techniques that can help us to improve the process of creating software as well as the resulting software products. The course covers fundamentals of software engineering, including: modern software process models; eliciting, specifying, and evaluating software system requirements; designing software systems to embody required quality attributes, including usability and security; an introduction to reusable software design solutions in the form of software architectural styles and design patterns; software system modeling, implementation, and deployment; and software quality assurance (measurement, inspection, testing). Project planning, working in teams, and using modern software development tools are also explored. [Spring 2017]

Research Advisor
Dr. Jinpeng Wei, Associate Professor
University of North Carolina at Charlotte, NC, USA
jwei8@uncc.edu | website