Mohiuddin Ahmed | Portfolio | GitHub | LinkedIn | Google Scholar

Charlotte, North Carolina, USA; Email: sohel.buet.cse.07@gmail.com; Phone: +1 980-267-0371

Education

- **Doctor of Philosophy** in Software and Information System, UNC Charlotte, NC, USA. [August 2016 - August 2023]
- **Bachelor of Science** in Computer Science and Engineering [January 2008 - February 2013]
  - ◇ Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh.

Professional Skills

- **Languages and Frameworks:**
  - ◇ **Expert:** Python, Java, C++, C, Prolog, Shell Scripting, SQL, Java Spring, JavaScript, MySQL, Oracle SQL, Elasticsearch, RabbitMQ, OpenSSL, Standford CoreNLP, AllenNLP, NLTK, Scikit-learn, Keras, Machine Learning, TCP/IP, OSI Model, MITRE ATT&CK Framework, CIS Critical Security Control, Cyber Threat Hunting.
  - ◇ **Working Knowledge:** R, C#, Microsoft .NET, PHP, Laravel, TensorFlow, Terraform, Ansible, Chef, Kubernetes.
- **Tools and Platforms:**
  - ◇ **Expert:** IDAPro, OllyDbg, Docker, Gradle, CMake, VirtualBox, VMWare, Git, Scrum/Agile, Windows, Linux, Mac.
  - ◇ **Exposure:** AWS, Azure, Weka, Gephi, Maven, Splunk, UML, Android.

Professional Experiences

- **Graduate Assistant**, UNC Charlotte, NC, USA. [August 2016 - May 2023]
  - ◇ Developed distributed hierarchical event monitoring system to detect attacks based on attack technique description (static and behavioral features) provided by the MITRE ATT&CK framework, and taught graduate courses on cybersecurity.
- **Team Lead, Security Lab**, Kona Software Lab Ltd, Dhaka, Bangladesh. [January 2016 - June 2016]
- **Software Engineer, Security Lab**, Kona Software Lab Ltd, Dhaka, Bangladesh. [March 2014 - December 2015]
  - ◇ Implemented dynamic libraries (.dll, .so, and .dylib) and different corresponding PKI system and CA toolkits using Java and C++ that comply with PKCS#11, FIPS, KISA, and PKCS#7.
- **Junior Software Engineer**, Nascenia, Dhaka, Bangladesh. [March 2013 - February 2014]
  - ◇ 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. Implemented multi-threading and multiprocessing, smart card profile initialization, asymmetric (RSA, ECA) and symmetric (DES3, AES, MAC, SEED) key operation (encryption, decryption, key generation, and Signature generation and verification). *Development Language:* C++, JNI, OpenSSL. [May 2014 - December 2015]
- **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. *Development Language:* C++, Windows API, OpenSSL. [January 2016 - April 2016]
- **CMS**, *Cryptographic Message Syntax* is a PKCS#7 based toolkit developed to support CA System during certificate Issuance that supports all data types (*Signed, Enveloped, SignedAndEnveloped, data*) of PKCS#7 and their operations. *Development Language:* Java. [May 2015 - June 2015]
- **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 libraries. *Development Language:* Java. [January 2015 - March 2015]

Dissertation Research Projects

- **Scalable-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 usage. Developed low-level log collecting agents for Windows system (ETW, event logs). Developed detectors to map low-level traces to MITRE ATT&CK technique and evidential reasoning framework which performs passive reasoning and active investigation on reported observables. *Development Languages/Tools:* Python, Java, RabbitMQ, ElasticSearch, Docker.
- **TTPHunter**, 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

- **Mohiuddin Ahmed**, Jinpeng Wei, Ehab Al-Shaer. 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).
- Mohammed Noraden Alsaleh, Jinpeng Wei, Ehab Al-Shaer and **Mohiuddin Ahmed**. (2018). gExtractor: Towards Automated Extraction of Malware Deception Parameters. (SSPREW-8, 2018).