Md Sajidul Islam Sajid

sajidcsedu | website | msajid@towson.edu | ☎ +1.704.763.2809

Research Interest

My research interest focuses on **Cybersecurity** in the areas of **System Security**, **Cyber Deception**, and **Data Engineering for Security** with an emphasis on **Malware Analysis**. I aim to develop solutions that cope up with the ever-evolving threat landscape for detecting malware, understanding their capabilities with high precision and orchestrating systems to channel disinformation without compromising sensitive data and user experience.

Education

2017 - 2023	Ph.D in Computer and Information Systems University of North Carolina at Charlotte **Advisor:** Dr. Jinpeng Wei **Co-advisor:** Dr. Ehab Al-Shaer (Carnegie Mellon University)
2010 - 2014	B.Sc. in Computer Science and Engineering University of Dhaka

Work Experiences

Assistant Professor at Towson University Aug 2023 - Present

Courses: I am teaching COSC 439: Operating Systems and COSC 440: Operating Systems Security.

Research Assistant at UNC Charlotte Aug 2017 - July 2023

- Conducted research in the cybersecurity area with emphasis on malware analysis, data analytics and cyber deception.
- Led collaborative projects, mentored and guided the master's students working on these projects.
- Demonstrated yearly progress to the grant sponsors.

Teaching Assistant at UNC Charlotte Aug 2021 - May 2022

Courses: ITIS 6330/8330: Malware Analysis (Spring, 21; Spring 22) and ITIS 6200/8200: Principles of Information Security and Privacy (Fall, 22).

- Held office hours, graded assignments and exam papers.
- Assisted students with project ideation and taught different malware analysis tools to shape their final projects.
- Instructed classes in the absence of the primary instructor.

Security and Privacy Graduate Intern at IBM Research May 2022 - Aug 2022

- Developed a framework capable of detecting Grayware in the Microsoft Store.
- Performed experiments on 200 apps to confirm the prevalence of Grayware.
- Presented the research findings in a poster session and gave an exit talk on the framework.
- Submitted a patent for the framework.

Software Engineer at Kona Software Lab Ltd Dec 2014 - Aug 2017

- Developed highly interactive server-client-based payment solutions using Java, Spring and REST APIs.
- Wrote scripts to perform automated end-to-end functionality testing to ensure fast bugless product release.
- Analyzed failed cases on the production servers to fix bugs.
- Communicated and worked with multi-disciplinary teams of developers, QA engineers and operatives daily to integrate and test features.
- Managed a team of three members to write structured, efficient and manageable codes to perform automated E2E testing of several released products.

Software Engineering Associate at Accenture Oct 2014 - Dec 2014

- Developed middleware/enabling applications using Java, Oracle and integrated with different upstream and downstream nodes to provide customers-specific services and facilities.
- Performed user acceptance testing to ensure developed solutions met requirements.

Technical Skills

Language and Database	Python, Java, C/C++, PHP, MySQL, Oracle
Frameworks	Spring, Spring Boot, Codeignitor, django
Web Technologies	Servlets, JSP, JavaScript, Ajax, JQuery, HTML, CSS, REST APIs, Flask
Malware/Threat Analysis	Static and Dynamic Analysis, OllyDbg, IDA Pro, Ghirda, radare2, Cuckoo Sandbox, API Monitor, Wireshark, Snort, Yara, Suricata, Sysmon, PCAP Analysis
Cybersecurity Standards	NIST, MITRE Att&ck Framework, STIIX and MITRE MBC
Machine Learning	Neural Networks - ANN, RNN, CNN, XGBoost, Random Forest, kNN, SVM
Others	Maven, Gradle, Git, JIRA, Elasticsearch, Kibana, Logstash (ELK)

Research Projects

Malware behavior prediction using machine learning based classification Aug 2017 - Jan 2020

The goal of this project was to categorize malware based on their behavioral similarities using Machine Learning.

- Implemented autonomous agents capable of performing dynamic analysis utilizing symbolic execution and collecting malware execution traces (API calls).
- Categorized malware using Neural Networks where API calls and their parameters were used as the feature.

Malicious API sequence identification and mapping them to MITRE Apr 2020 - Dec 2021

The goal of this project was to extract Malicious Sub-graphs (MSGs) from the malware using dynamic malware analysis and map them to the MITRE TTPs. The mapped MSGs present how malware achieves a particular MITRE technique by calling a sequence of APIs.

- Performed dynamic malware analysis to understand implementation at the API (Win32) level.
- Implemented an algorithm to retrieve Malicious Sub-graphs (MSGs) from malware execution using data dependency.
- Created mapping between MSG to MITRE using text mining (NLP). MSDN API documentation, MITRE attack description and StackOverflow questions and answers were used as the text inputs.

Automated and conflict-free deceptive system orchestration Aug 2017 - Oct 2022

Part one: This project aimed to find system variables (deception parameters) that can be altered to deceive malware.

- Developed a symbolic execution-based dynamic malware analyzer to extract different system variables on which malware relies to achieve its goal.
- Formulated optimal deception parameter selection process based on feasibility, optimization and cost-effectiveness.
- Created the deception playbook consisting of HoneyThings (honey-registry, honey-files and fake configurations) for the optimal deception parameters.
- Integrated this project with our previously built classification model (to detect malware types) and orchestrated the deception environment by deploying relevant HoneyThings on demand.

Part two: This project aimed to address the limitations of the previous work, while the larger objective is to deceive malware in a conflict-free manner by modifying the API responses using API hooking.

- Integrated this project with our previously built MSG-to-MITRE mapping to identify malicious API sequences.
- Implemented detour hook functions with embedded deception actions to modify the API responses on the run-time.
- Applied assume-guarantee to ensure non-conflicting deception actions selection.

Grayware detection on MS Store by performing threat hunting on system events May 2022 - Present

The goal of this project is to develop a framework capable of detecting Grayware and explaining their infection chain.

- Designed and implemented a sandbox capable of running and collecting run-time traces of MS Store Apps.
- Building Cyber Threat Intelligence Ontology (CTIO) specifically for Grayware from existing CTI (MBC, MITRE) frameworks in an automated manner using text similarity (TF-IDF).
- Performing threat-hunting operations on the collected logs using the CTIO to confirm the prevalence of Grayware and their infection chains and capabilities.

Efficient backup creation to fight ransomware and deplete attackers' resources Oct 2022 - Present

This project aims to offer better file backups to tackle ransomware and abuse the communication channel between the malware and the C&C to deplete attackers' resources.

- Performing malware analysis to understand API sequences in ransomware and utilize API hooking to create optimal and effective system backups.
- Studying the key exchange mechanism to abuse the channel to deplete attackers' resources by providing fake keys.

Publications

[1] Sajid, M. S. I., Wei, J., Al-Shaer, E., Duan, Qi., Abdeen, B., & Khan, L. (2023, September) symbSODA: Configurable and Verifiable Orchestration Automation for Active Malware Deception. In ACM Transactions on Privacy and Security (TOPS)

[2] Sajid, M. S. I., Wei, J., Abdeen, B., Al-Shaer, E., Islam, M. M., Diong, W., & Khan, L. (2021, December). Soda: A system for cyber deception orchestration and automation. In Annual Computer Security Applications Conference (ACSAC)

[3] Sajid, M. S. I., Wei, J., Alam, M. R., Aghaei, E., & Al-Shaer, E. (2020, June). Dodgetron: Towards autonomous cyber deception using dynamic hybrid analysis of malware. In 2020 IEEE Conference on Communications and Network Security (CNS)

[4] Islam, M. M., Dutta, A., **Sajid, M. S. I.**, Al-Shaer, E., Wei, J., & Farhang, S. (2021, October). CHIMERA: Autonomous Planning and Orchestration for Malware Deception. In 2021 IEEE Conference on Communications and Network Security (CNS)

[5] Alam, M. M., **Sajid, M. S. I.**, Wang, W., & Wei, J. (2022, April). IoTMonitor: A Hidden Markov Model-based Security System to Identify Crucial Attack Nodes in Trigger-action IoT Platforms. In 2022 IEEE Wireless Communications and Networking Conference (WCNC)

[6] Sajid, M. S. I., Rahim, I. B., & Jahan, M. (2014). An Energy-Efficient Data Aggregation Tree Construction Algorithm for Wireless Sensor Networks. Int. Journal of Comp Networks and Wireless Comm. (IJCNWC)

[7] Sajid, M. S. I., Araujo, F., Taylor, T., Jang, J. Peeking into the Gray Area of MS Store: A Framework to Analyze Grayware in MS Store (Patent) - Under review

[8] Alam, M. R., Wei, J., **Sajid, M. S. I.**, Wang, Q. Attacking IoT Devices through the IoT Cloud Platforms: An Empirical Study (CODAYSPY, 23) - Under review

[9] Sajid, M. S. I., Wei, J., Al-Shaer, E. Understanding API sequences in ransomware to create effective and optimal system backups and deplete attackers' resources. - In progress.

Professional Services

Reviewer - (Publon Profile) 2020 - present

International World Wide Web Conference (2021, 2022, 2023), International Conference on Information and Communications Security (ICICS), IEEE INFOCOM - IEEE Conference on Computer Communications

REU Mentor - UNC Charlotte, NC, USA May 2019 - Aug 2019

Leadership Experiences

Treasurer - Ekush - Bangladeshi Student Organization at UNC Charlotte, NC, USA Dec 2018 - Oct 2019

Team Lead - Kona Software Lab Ltd, Dhaka, Bangladesh Jan 2017 - Aug 2017