Md Mazharul Islam

Contact Information

Cell No. (+1) 980 210 0371
11006 Diploma Dr Apt A Charlotte NC, 28262
Email: msilam7@uncc.edu

Website: rakeb.github.io
GitHub: github.com/rakeb
Linkedin : in/rakebmazharul
StackOverflow: /users/1743849

Research Interest ◇ Cyber Deception ◇ Moving Target Defense ◇ Autonomous Cyberdefense ◇ Email Spear-phishing Detection ◇ Reinforcement Learning ◇ Sequential Decision Making under Uncertainty

Education

- **Ph.D.** in **Software and Information Systems**, [August, 2016 - Present]
  University of North Carolina at Charlotte, NC, USA
- **B.Sc.** in **Computer Science and Engineering**, [February, 2008 - February, 2013]
  Bangladesh University of Engineering and Technology, Dhaka, Bangladesh

Publication

1. **Islam, Md Mazharul**, E. Al-Shaer and M. A. Basit-Ur-Rahim. "Email address mutation for proactive deterrence against lateral spear-phishing attacks", International Conference on Security and Privacy in Communication Systems, 2020.
2. **Islam, Md Mazharul**, and Ehab Al-Shaer. "Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception." 2020 IEEE Secure Development (SecDev). IEEE, 2020.
3. **Islam, Md Mazharul**, Qi Duan, and Ehab Al-Shaer. "Specification-driven Moving Target Defense Synthesis." Proceedings of the 6th ACM Workshop on Moving Target Defense. 2019.
4. **Islam, Md Mazharul**, et al. "CLIPS/ActiveSDN for automated and safe cybersecurity course-of-actions orchestration." Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security. 2019.
5. Dalton, Adam, **Islam, Md Mazharul**, et al. "Active Defense Against Social Engineering: The Case for Human Language Technology." Proceedings for the First International Workshop on Social Threats in Online Conversations: Understanding and Management. 2020.
6. Duan, Q., Al-Shaer, E., **Islam, Md Mazharul**, & Jafarian, H. (2018, May). Conceal: A strategy composition for resilient cyber deception-framework, metrics and deployment. In 2018 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE.
7. Ahmed, A. R., **Islam, Md Mazharul**, & Rahman, M. S. (2012, December). On Acyclic Colorings of Graphs. In 2012 15th International Conference on Computer and Information Technology (ICCIT) (pp. 95-100). IEEE.

Under review

1. **Islam, Md Mazharul**, Dutta, A., & Al-Shaer, E. Autonomous Cyber Deception Planning Using Partially Oversavable Markov Decision Process.
2. **Islam, Md Mazharul**, Ehsan, A., & Al-Shaer, E. Multi-layer Email Headers Analytics to Defend Against Email Spear-phishing Attacks.
3. **Islam, Md Mazharul**, & Rahman, Sazzadur. Cryptographic Code Vulnerability Detection in StackOverflow.
4. Dutta, Ashutosh., **Islam, Md Mazharul**, Duan, Q., & Al-Shaer, E. Adaptive Multi-strategy Cyber Deception against Reconnaissance Attacks.

Technical Skills

- **Programming Language:** Python, Java, C, C++
- **System Orchestration:** Docker, Kubernetes, AWS, Git, Gradle
- **Web Development:** Django, JavaScript, HTML5, MySQL, Shell Scripting
- **Cybersecurity Expertise:** MITRE ATT&CK framework, Malware analysis, FIPS, NIST, PKCS, KISA
- **Others Expertise:** SDN, OpenDaylight, OpenFlow, SMT, Z3, MDP, POMDP, OpenSSL, Gephi

Projects

◇ **Chimera: Autonomous Cyber Deception Planer** Funded by ONR

Chimera is an autonomous orchestrator to design a deception environment in order to detect and deceive advanced persistent threats such as Ransomware, Information Stelar, RAT. Due to the uncertainty and dynamic nature of the attackers, I use Partially Observable Markov Decision Processes (POMDP) to observe adversary techniques based on MITRE ATT&CK framework and reinforcement learning to learn from the environment to choose the optimal deception actions.

Tools/languages: MITRE ATT&CK, IDS, POMDP, Python, C++

◇ **ActiveSDN** [code-activesdn] [code-activesdn-middleware] Funded by ARO

An open programming environment that enables developing and prototyping advanced active cyber defense mechanisms (such as IP or route mutation, honey network creation) rapidly and safely on Software Defined Networking (SDN). ActiveSDN also provides a language for security policy specification.

Tools/languages: OpenDaylight, OpenFlow, SDN, Java, Python, Git, VMware

◇ **Email Mutation** [code] Funded by DARPA

Sender Email address Mutation is a novel protocol to detect the lateral spear-phishing attack in which an adversary sends phishing emails to a victim from a legitimate but compromised email account. The protocol works with any mail service providers such as Gmail, Apple iCloud, and mail clients, such as mail.gogole.com, Outlook, Thunderbird, etc.

Tools/languages: SMTP, IMAP, Django, Python, Java, Chrome Extension, Git

◇ **Panacea: Email Header Analytics** [code] Funded by DARPA

Panacea is a multi-layer system to defend against email borne threats such as spamming, spoofing, and spear-phishing attacks. In Panacea, we use different techniques, including Machine Learning, NLP, real time active investigation such as evaluating domain reputation to detect such threats.

Tools/languages: Scikit-learn, Django, Python, C++, Git, Docker, Kubernetes

◇ **FIPS Certification for KONA N41M0 Smart Card**

I developed and documented the Demonstration Applet to achieve Security Requirements for Cryptographic Modules FIPS 140-2. The secure module KONA N41M0 certified by FIPS on November 25, 2015 (certificate no. 2476 and 2478).

Tools/languages: JavaCard, JAVA, specs: FIPS-140, VISA, MasterCard, Discover, PKI

◇ **AMEX, JCB and Discover Payment Applet**

As a team-lead, I designed the architecture of AMEX, JCB, and Discover Payment applications. I developed the critical crypto modules such as application cryptogram generation, cardholder verification, secure massaging, etc.

Tools/languages: JavaCard, Java, specs: Amex, JCB, Discover and PCKS

◇ **KonaPay**

I was a Scrum Master and team lead of the project *KonaPay* which is a payment solution compliant with EMV, VISA and MasterCard Payment Specifications.

Tools/languages: Java, specs: EMV, PKCS

◇ **Beauty900**

It's a complete eCommerence website developed using Magento framework. My part was implementing the Face Mapping module.

Tools/languages: Magento, PHP, MySQL

Professional Experience

- **Research Assistant**, CyberDNA, **SIS Department** [August, 2016 - Present]
  UNC Charlotte, NC, USA.
- **Team Lead**, Applet Team, **Security Lab** (R&D dept.) [August, 2015 - July, 2016]
  KONA Software Lab Ltd, Dhaka, Bangladesh.
- **Software Engineer**, Cloud Platform Team, **Payment Lab** [February, 2014 - July, 2015]
  KONA Software Lab Ltd, Dhaka, Bangladesh.
- **Software Engineer**, Nazdaq Technologies, Dhaka, Bangladesh. [February, 2013 - November, 2013]