Sutanu Kumar Ghosh

Graduate Research Assistant, University of Illinois Chicago

✉ sghosh34@uic.edu ☎ 312-792-9189 Chicago, Illinois

I'm a Ph.D. student with a cybersecurity background actively working on host-based attack detection and attack correlation. I'm primarily interested in real-life problems in the domains of Advanced and Persistent Threats (APT) based attack detection, attack correlation, and threat intelligence platforms. I'm seeking an internship position that matches my skills and knowledge.

Education

PhD in Computer Science, *University of Illinois Chicago* Aug 2018 – present | Chicago, USA

- Research in attack detection and attack correlation frameworks.
- SOC Operator knowledge-based attack correlation.
- Threat intelligence platforms analysis.

Bachelor's in Computer Science & Engineering, 2014 – 2017 | Kolkata, India
Maulana Abul Kalam Azad University of Technology

- Thesis: Classification of medical image anomalies based on k-means and c-means clustering
- Courses: Object Oriented Programming, Compilers, Computer Networks, Discrete Maths, Operating Systems

Publications

OSTINATO: Cross-host Attack Correlation through Attack Activity Similarity Detection, *ICISS 2022*
Sutanu Kumar Ghosh, Kiavash Satvat, Rigel Gjomemo, V.N.Venkatakrishnan

Projects

SOC Operator knowledge based attack correlation, *Research paper under progress*

- Integrating SOC operator knowledge into the alarms raised by the underlying monitoring systems to prioritize efficient incident response.

Ostinato: Cross-host attack correlation, *Research paper*

- Developed a robust cross-platform framework that performs attack correlation that leverages a unique intuition about APT attack groups and subsequently performs a correlation between cross-host attacks through a novel graph comparison algorithm.

Skills

Languages ●●●●○
C++, Python, Custom Domain Language, Scripting, Java, Git, SQL

Technical ●●●●●
Understanding of vulnerability-scanning tools (Metasploit, Nmap, and others) and Threat Intelligence Platforms, ATT&CK, CALDERA.

Professional Experience

Graduate Research Assistant, SISL Lab, *University of Illinois Chicago* Jan 2019 – present | Chicago, USA

- Working as RA in the SISL Lab of the Computer Science department.
- Research in attack detection, and attack correlation.

Awards

Best Paper Award: OSTINATO, Dec 2022
18th International Conference on Information Systems Security (ICISS) 2022.