ICS Threat Intelligence

Project Description: The goal of this project is to build a threat intelligence framework that focuses on multistage advanced persistent threats (APTs) industrial control systems (ICS). The first phase of the project focuses on forensics, or attack story reconstruction. Given that a multistage ICS APT attack has occurred, we want to reconstruct the attack story, detailing what happened in each step. During this internship, the intern will be exposed to several domains of research. They will know how industrial control systems work, what multistage advanced persistent threats are and how to build them, identify forensic information sources, work with large language models, and reinforcement learning ML.

Project Type: Research

Internship Batch:

- **Batch 1:** May 11 to July 10, suitable for Education City students, i.e., CMUQ, TAMUQ and HBKU students
- **Batch 2:** May 25 to July 24, suitable for QU university students

Duties/Activities:

- Researching and constructing ICS APT attacks
- Identifying information sources such as logs and network traffic
- Building an ML model to distinguish benign activities from malicious ones
- Building an ML model to correlate malicious activity in various ICS components and attack stages

Required Skills:

- Familiarity with large language models, next token prediction, and sentiment analysis
- Familiarity with systems engineering
- Familiarity with regex
- Familiarity with information security concepts
- Ability to write simple malicious programs and scripts
- Familiarity with reinforcement learning is a plus

Preferred Intern Academic Level: Senior

Learning Opportunities:

- Learning how to replicate APT attack campaigns on testbed from researching attack reports
- Learning how industrial control systems work
- Learning how to use ML for forensics

Expected Team Size: *2*

Mentors

Name: Dr. Khaled Serag Alsharif email: kseragalsharif@hbku.edu.qa