Personal Statement

I am applying for the PhD candidate to conduct research in the field of cybersecurity. To be more specific, I want to be dedicated to improving the safety and security of cyber-physical system (CPS) via threat modeling and anomaly detection techniques. Different from Internet systems, CPSs are integrations of networking, computing systems and actual facilities that monitor and control entities in the physical environment. This means it will be ineffective to simply apply the cybersecurity research outputs for the Internet system to CPS. Taking the railway as an example, attackers targeting such critical infrastructure will never stop at stealing passenger information or blackmailing computers like they usually do against Internet systems, but will try to disrupt the normal service process of the system to further cause severe safety accidents, such as derailment and train collision. This kind of advanced attack indicates that the consideration of combining safety and security is an inevitable research trend of CPS.

The reason why I am a good fit for pursuing research in this area is that I know both safety and security. When I was an undergraduate, I learned some courses about railway system since my university is prestigious in the rail transit field. Safety, as the most significant attribute of railway, is protected by many mechanisms and constraints. For example, a typical one is the "fail safe" principal, which ensures the system to stay in a safe state even if failure occurs. However, when I became a master student and got involved in the world of cybersecurity, I came to realize that these safety protections could be bypassed or breached once the system was under cyberattack, as they were not designed with security in mind.

To answer how could security affect safety and how much role will the protections play in this process, I've written an academic paper[1] as the first author to propose an integrated framework for exploring the intersecting part of safety and security, namely Process-Oriented and Coalescent Analysis (POCA). Different from the traditional "object-oriented" methods that directly start with system components, POCA mainly focuses on the specific working process of the object, which is "process-oriented". I've applied POCA in a service scenario of railway signal system to testify its competence of answering the 2 questions above. In terms of weakness identification, existing safety mechanisms could indeed eliminate several weaknesses in the service process. In terms of analysis results, threat scenarios designed by POCA describe how security threats can cause safety accidents by exploiting weaknesses to disrupt the service process.

At the theoretical level, threats can be captured by the aforementioned threat modeling methodology; at the practical level, threats can be identified by anomaly detection techniques. Although mature anomaly detection tools can accurately detect vulnerabilities, viruses and abnormal behaviors, they are incompetent to show the correlation between anomalies. However, the particularity of CPS will create a very tricky situation: if an attack chain is realized by an abnormal combination of normal operations, you will not find any abnormalities by detecting each operation, but only after correlating these together can you recognize that this is an attack behavior. To cope with such challenge, the knowledge graph (KG), with its competence of describing knowledge and modeling the relationship between entities, is considered to have great research value in the field of anomaly detection.

---

[1] Submitted to “International Journal of Critical Infrastructure Protection” on August, 2022. Currently it is under review.

While working on this project[2] as the principal investigator, I've built a basic KG based on ArangoDB for the railway signal system. There are two advantages of utilizing KG under my circumstance. First, it realizes a combination of theory and practice. It not only consists of knowledge data (BRON[3]), environment data (assets and topology) and behavior data (system logs), but also effectively integrates the aforementioned threat modeling outputs as the cyber threat intelligence (CTI). Second, it endows subsequent development the explainable attribute. It can be the foundation to develop model-based AI techniques for explainable representing, analysing and reasoning about the security and safety of CPS.

In the process of making the above progress, I also realized problems (future challenges) on both individual work of mine and general progress of a specific field. On the one hand, my current progress is rudimentary. The three years of master's degree is limited, since I spent most of my first year in class. Meanwhile, I am a pathfinder in this field in our laboratory, which means I have to research from scratch. As a result, I can only complete the construction of the underlying architecture of my research topic, but have no more time for the further research on the upper application. On the other hand, the emerging technique--KG requires further research as well. In the early stage, people's research on the application of KG in the cybersecurity field mainly focused on the construction of reasonable and effective graphs. In recent years, the emergence of some commonly recognized graph models symbolizes the end of this stage. At present, how to utilize KG to solve practical problems (e.g., attack path analysis, attack prediction) under different situations has become the research hotspot.

In summary, my goals as a PhD candidate are to research novel AI techniques and algorithms in order to overcome the limits of current methods for CPS. To cope with the continuously evolving attack technology, the security research should become interdisciplinary, such as to integrate the security with safety. I believe, in the future, both attack and defense will be more advanced and intelligent, and I am excited to contribute to this field of research.

---

[2] Applied basic research project of science & technology department of Sichuan Province [grant 21YYJC3147]. Detailed information can be found at https://jayzheng98.github.io/projects/project2.

[3] Security knowledge from MITRE ATT&CK, CAPEC, CWE, CVE, MITRE Engage and MITRE D3FEND are linked together in a graph called BRON (https://github.com/ALFA-group/BRON) by researchers from MIT.