Name: Richeng Jin

Hard Problem Area: Security Metrics and Models

Overall Research Goal(s):
What do you ultimately hope to show with your research? This section can involve some jargon, but try to relate these goals to your broad impact section. Start with the larger goal(s) and narrow the scope towards your specific study (and specific goals, below).

As information systems become ubiquitous, Intrusion Detection Systems (IDSs) have assumed increasing importance. Despite the abundance of intrusion detection algorithms developed so far, there is still no single detection algorithm that can catch all possible attacks. On the other hand, it is infeasible for practical IDSs to run all the detection algorithms simultaneously due to resource limitation, leaving potential opportunities for the adversary to explore. This resource scarcity problem becomes more severe when the system is in an ill state (e.g., partially compromised system state).

Enabling collaboration among multiple IDSs may be a viable way to mitigate this problem. Particularly, IDSs in the healthy state can share some of their idle computational resources to those in ill states, so as to improve their intrusion detection performance. Therefore, it is expected that collaboration among IDSs can lead to substantial performance gains.

The main goal of this work to design a smart collaboration protocol through which IDSs can not only maintain their own benefits but also help others efficiently, in the presence of intelligent intruders as well as dynamic system environments.

Broad Impact:
Why is your research important? This section should avoid any technical jargon and should be meaningful to the general public. Try to keep this down to five sentences. This should be hierarchical: the broad impact decomposed into more specific impacts that connect your overall research goals to your more specific goals.

Nowadays, information systems and digital devices are ubiquitous in our daily life. As a result, the importance of securing information systems and networks can never be over-emphasized. When adversaries invading our systems, IDSs will serve as a vital line of defense to protect our important information asset. Although substantial amount of research efforts have been devoted to developing various intrusion detection algorithms, we still observe continuing reported failures of IDSs, leading to great loss of information asset. In many situations, an IDS fails simply because of lacking required computational resources, especially when facing severe attacks. We plan to mitigate this problem by designing an effective collaboration scheme that allows IDSs with idle resources to help the IDSs under severe attacks. It is expected that, through employing our collaboration scheme, the overall intrusion detection performance can be improved and better security assurance of information systems can be achieved.
**Specific Research Goals:**
Lay out the steps you are going to take to achieve your overall research goal. You can get technical here.

Our objective in this work is to develop a two layer game theoretic approach to solve the multiple IDS configuration problem.

1. The first layer game is concerned with the interaction between each IDS and the corresponding attacker. Particularly, we plan to leverage the stochastic game theory framework since it is a natural mathematical tool to examine the interaction between two (or more) intelligent parties (e.g., the IDS and the attacker) as well as handle the underlying system dynamics (e.g., different states of the information system).

2. The second layer game is concerned with the interactions among multiple IDSs. When all IDSs and attackers obtain their optimal strategies from the first layer game, the IDSs will determine how to collaborate so as to maximize their overall detecting performance. We will first focus on the centralized scenario and then try to extend the study to a distributed setting.

3. We plan to explore some corresponding game-theoretic quantities, such as myopic reward and value-function, as metrics to facilitate the IDS collaboration scheme design.

4. We plan to determine the conditions under which there is significant, marginal, and no collaboration gain, respectively.

**Success Criteria:**
How will you determine whether you satisfied your specific and overall research goals?

Many metrics have been developed in literature to measure the performance of IDSs, such as detection rate, false alarm rate, processing time, traffic increase, etc. In this work, we will evaluate the proposed algorithms comprehensively through comparing their performance with that of existing ones without collaboration using these metrics. Furthermore, we will examine the proposed algorithms in various scenarios and identify the conditions under which substantial collaboration gain exists.

**Anticipated Difficulties, Limitations, and Criticisms:**
What will make the above specific research goals difficult to achieve? How do you plan on dealing with these difficulties if they arise?

The major difficulties may arise from the following aspects:

- In this work, we assume that all the IDSs are reliable. In practice, we should also deal with the free rider problem. One possible way is to introduce a metric to measure the trustworthiness of each IDS.
- The attackers are intelligent, which may be able to infer the configuration of the IDSs through the results of previous attacks and change their strategies accordingly.
- The system states are dynamic, which means the IDSs should learn their strategies under all the possible system states.
- When each IDS determines how to allocate its resource, we should avoid the case that all the IDSs allocate their redundant resources to one (or a few) ill IDS(s).
• How to realize the fairness among IDSs.
• In practice, we should consider the fact that some IDSs may be more important than the others. In this case, we may introduce a new metric to measure the importance of an IDS, which will play a role in the resource allocation scheme.