# 2023 Spring CNS Reading Critique #7

## Dos and Don'ts of Machine Learning in Computer Security

**R11921A16 何秉學**

## I. Summary

In this paper, they tried to point out some pitfalls of computer security paper that are associated with machine learning. Especially the paper in the last 10 years published at top-tier conferences. In addition, they identify 10 common pitfalls such as sampling bias problems, label inaccuracy, data snooping problems, spurious correlations, etc that are associated with the whole machine learning workflow, i.e. data collection and labeling, system design and learning, performance evaluation and deployment, and operation. They also provide some recommendations and some remedies and try to mitigate the threat. The top 3 pitfalls in their research are sampling bias, data snooping, and lab-only evaluation.

## II. Strength

The various pitfalls proposed in the article can actually be widely applied in various fields, not only limited to network security, but even biological sciences, horticultural fruit tree growth models, etc., you should pay attention to these issues The author not only asks questions, but also puts forward some possible mitigation solutions, and even gives suitable examples in the field of network security at the end, so that readers can understand how serious the harm will be after the superposition of various traps.

## III. Weakness

For those who do not pay attention to this field, they will half-understand the description of those pitfalls, especially when describing, they are not very good at giving examples or simply explaining the problems behind the cited papers, which makes it very difficult to read.

## IV. Reflection

I learned that the various pitfalls mentioned in the article may appear at each stage of introducing machine learning. Therefore, while doing relevant research, we must actively examine the data at each stage and evaluate the final results, to avoid hard work. The research done goes down the drain. In addition, this also reminds me of what my seniors mentioned before. Before introducing machine learning, we should think about the correctness, completeness, and availability of information, and then consider whether there is a simple way to use the model basis for the paper. Not everything has to be related to machine learning. After all, it can be processed more simply, which means that the calculation is more efficient, the energy consumption is lower, etc.

If I were the author, I would spend more space explaining the articles cited in each trap, their research titles, and their relationship with the trap, so that readers can better feel the seriousness of the harm.