**Introduction of Machine Learning Security**

**Project Title**

Student Name in Chinese (Student ID)

**Introduction**

Mention the aim and overview of your concept and justification. Provide a concise explanation of your idea and the reasoning behind it. Briefly outline the approach you will employ to accomplish your objective. Mention any new thought. (Suggested length: 3-4 lines)

**Method**

Mention the procedure how to generate the attack (from the given information to the required output). Describe any proposed method if applicable. Flowchart and figure are welcome for illustration, but NO program code is allowed. (Suggested length: 8-15 lines)

**Experiment**

**Settings**

Describe the experimental settings, for example, the preparation of training and test sets, explain how fairness is ensured (e.g. independent runs), mention how to determine appropriate parameters for each machine learning method, what platform you used, etc. (Suggested length: < 7 lines)

**Results and Discussion**

Evaluate the performance of your attack in terms of the cost, concealment, and damage. Tables and figures are welcome but No programming code should be included. (Suggested length: 10-12 lines)

**Conclusion**

Summary this report less than 5 statements. (Suggested length: < 3 lines)