**Direction 1: Trace-based Exploit Detection**

**In this final project, you will be exploring trace-based exploit detection in binary programs. We will provide you two binaries, each with an exploitable vulnerability. Specifically, the first binary has a *buffer overflow* vulnerability, and the second one *use-after-free* vulnerability. You ONLY need to work on one of them.**

**// When the input is less than or equal to 10 chars, the binary returns properly**

**$ buffer\_overflow “AABBCCDDEE”**

**// When the input is larger than 10 chars, the buffer overflow occurs**

**$ buffer\_overflow “AABBCCDDEEFF”**

**// When you provide true to the binary, the vulnerability will be triggered**

**$ use\_after\_free true**

**// When you provide false to the binary, the vulnerability will NOT be triggered**

**$ use\_after\_free false**

**Task Description:You are tasked to analyze the execution trace of the chosen binary using techniques taught in class or any other techniques you find helpful. You goal is to identify the vulnerability through the execution trace.**

**Obtaining Execution Trace of a Binary Program: You can obtain the execution trace of a binary program using many tools. Here, we provide detailed instructions on how to obtain such execution trace using *peekaboo*,** <https://github.com/melynx/peekaboo>**, a tool based on DynamoRIO. Please refer to the Tutorials and Documentation in this link (**<https://dynamorio.org/>**) to familiarize yourself with DynamoRIO.**

**You can obtain the execution trace of a program called binary\_name using the following command:**

**$** *DynamoRIO-PATH*/bin64/drrun -c libpeekaboo\_dr.so -- binary\_name

**After generating the trace, you can use the readtrace program to inspect the generated trace. Please refer to this link (**<https://github.com/melynx/peekaboo>**) on how to interpret the generated trace.**

**$ readtrace -h**

**Submission: You are required to write a report on your analysis.**

**Q&A: For any specific question, just write it down in this document.**

1. **Can we use GDB to debug the binary? Or only using peekaboo?**