Semester Projects

CIS700 (Malware Analysis)

Kris Micinski, Fall 2021

- Instead of three projects, I have chosen to do a semester project
- Realistically, I expect about 4-5 (parts of) weeks of sustained effort to build and demo something cool.

Requirements

- Your course project must have a **goal**, a **motivation**, and a plan for **evaluation**
    - Should be something significant and new, but not necessarily novel research (e.g., you can demo an interesting exploit you develop)

- Project proposals due October 15

Example Topics

- Using the angr symbolic executor to discover a known vulnerability and thoughtfully explaining how it could be used to build a real exploit (you show exploit working)

- Writing a binary analysis tool (e.g., based on BAP) to find interesting ROP chains (e.g., the kinds from today's class)

- Demoing a novel exploit (or a significantly novel presentation of a known exploit you did in a different way) of significant challenge (i.e., not just against a program with an obvious exploit).

- In your project: assume all "real" protection mechanisms (ASLR, … but not necessarily CFI)

Presentations / Writing

- You must use LaTeX to write a 4-to-6-page paper on your project. It should have at least an introduction, related work (however brief), and evaluation section.

- You will prepare a 15-20 minute presentation/demo.

Proposals

- Due October 15
- Write a paragraph or two about what you will be doing.
- State **goal**, **motivation** (who cares/why do you care?), and **evaluation** (how will you evaluate your project? How will you know when you're done?)
- I reserve the right to make you do more or reject your proposal if it seems too trivial, etc…