

## Preliminary Exam for System Security and Software Security

Claim: This doc is adapted from CUPLV Group's Instruction (<https://plv.colorado.edu/bec/pl-prelim/pl-prelim.pdf>)

### Potential Committee Members

Yueqi Chen  
Dirk Grunwald  
Sangtae Ha  
Gowtham Kaki  
Eric Keller  
Tamara Lehman  
Shivakant Mishra  
Eric Wustrow

### Overview

The purpose of the system security and software security preliminary exam is to provide students the opportunity to demonstrate mastery of the fundamentals of security while gaining depth in a specific sub-area of research. The exam is for students who have identified, in consultation with their advisor, a sub-area of security as a potential area for their dissertation work. Overall, the goal of the exam is for students to demonstrate that they are ready for Ph.D.-level research within the chosen field of study.

### Format

The exam will include two parts: (1) a 45-minute presentation of papers in a chosen area of research, and (2) an implementation project.

The student will work with the committee to select an exam date.

### Student Preparation

The exam committee will consist of at least three faculty members to serve on a student's preliminary exam committee. The advisor, in consultation with the student, will invite the additional faculty members. The committee will advise each student about the compilation of his or her individual "prelim" bibliographies. Each committee member will advise on papers from his or her area of expertise.

**At least two months** before the exam, students are expected to begin compiling a bibliography that includes breadth in system security and software security and depth in the chosen sub-area.

This exercise is intended to encourage students to think about the kind of research they want to be and what texts will most inform their work.

The implementation project will supplement the reading and demonstrate technical competency in the implementation skills needed to perform research in the chosen area. The project details should be coordinated with the exam committee months in advance.

### **Literature Critique in the Area of Research**

Once the papers for the literature critique have been chosen, the student will have four weeks to read these papers and prepare a 45-minute talk about them. It is expected that the student will follow references in the papers, as appropriate, to give a thorough critique.

The committee will evaluate the talk based on (a) the extent to which the exam taker was able to understand these papers and extract the key ideas in the papers; (b) the extent to which the exam taker was able to identify the strengths and weaknesses of the papers; and © the extent to which the exam taker was able to communicate the information in a clear but succinct manner.

### **Implementation Project**

The implementation project will allow the student to demonstrate mastery of the implementation skills needed to perform research in the chosen sub-area (e.g., reverse engineering, vulnerability analysis and exploitation, and hardware features for protection design).

The committee will evaluate the project based on (a) whether the project demonstrates the ability to prototype security analysis tools and (b) the extent to which the student was able to explain the architecture of the system in a clear and concise manner.