CPRE 538X Reverse Engineering and Security Testing
Dr. Thomas Daniels
206 Nuclear Engineering Laboratory
Iowa State University

Covers security testing and reverse engineering of hardware and software. Reverse engineering is covered as an element of defining the behavior of the system and also as a tool for developing test cases for security flaws.

Students will perform two larger projects and several reviews of academic papers in the area.

Objectives: Students will be able to:
- Apply a variety of testing and reverse engineering techniques in systems
- Choose techniques based on their goals or limitations of the system's environment
- Evaluate the results of their tests

Topic List (Potential Projects/Homeworks are in Parentheses)

1. Types of Testing and Reverse Engineering (Written Homework on concepts and terminology.)
   a. Testing
      i. Performance
      ii. Error Testing
      iii. Security
   b. Reverse Engineering
      i. Goals
      ii. H/W
      iii. S/W
   c. Testing and Reverse Engineering Methodologies
      i. Black/White Box Testing
      ii. Flaw-Hypothesis Methodology
      iii. Others...

2. System Definition: (Pick a system(s) and have students define and document the following subtopics for each.)
   a. System Boundary
      i. Physical Device
      ii. Process
      iii. Multi-process
      iv. Distributed
   b. System Interfaces
      i. Input/Output
   c. Behavior Specification
      i. Known Good
ii. Known Bad
iii. Formal methodologies
d. System History
   i. Past flaws
   ii. Ancestral codebase/hardware
3. Reverse Engineering (Given some malware/or other s/w system, students decompile using IDA Pro and answer questions about it. Also use system call traces, etc.)
4. Flaw Hypotheses and Common weaknesses (Given a system, Develop a set of flaw hypotheses and justifications for them. Relate them to the CWE.)
5. Developing Security Tests and Evaluating Results (Develop tests and run them against the system.)
6. Reporting and Evaluating Results (Final report on the results of the tests from above, and what can be generalized about the results. Also, recommend remediations or precautions for the system.)