Examination 1
Computer and Network Security
18 October, 1995

Instructions:

- Do not start the examination until instructed to do so.
- **Graduate Students:** Answer question 1 and any two (2) other questions.
- **Undergraduate Students:** Answer any three (3) questions below.
- Start the answer to a new question on a new piece of paper (that is, no more than one answer per page).
- Be sure to include your name on your answer sheets.
- This test is closed book, but you may use one 8.5 by 11 inch sheet of notes.
- You have 50 minutes to complete this examination.

1. (a) Describe the Access Control Matrix model and how the ACM is used.
   (b) List all important categories of objects the ACM should have and give for each category a reasonable set of privileges.
   (c) Show how, by giving appropriate labels to the security domains and object types, and by providing an appropriate set of privileges, Bell-LaPadula MAC can be modeled using the ACM.
2. (a) Describe ACLs and how they work. What is needed to provide security using ACLs?
   (b) Describe C-lists and how they work. What is needed to provide security using C-lists?
   (c) Compare ACLs and C-lists - what are their relative strengths and weaknesses?
   (d) In what way does Unix combine both ACLs and C-lists? How is this useful?
3. (a) What are the three primary types of objectives of a security policy?
   (b) How do these relate to hardware?
   (c) How do these relate to software?
   (d) How do these relate to data?
4. (a) Describe and relate system access security and data access security.
   (b) What hardware mechanisms are often used to enforce protection on computers, and how are they used?
   (c) What is the reference monitor and how is it used?
   (d) What is containment, and how is it enforced in practice?
5. (a) Distinguish MAC and DAC.
   (b) How can DAC be incorporated into the ACL implementation of the ACM model? Be specific, and give examples.
   (c) How can DAC be incorporated into the C-list implementation of the ACM model? Be specific, and give examples.
   (d) Given K levels $1, 2, ..., K$, and universal category set S, what are system high and system low labels for security? Integrity?