# Homework 4

**Due Date:** December 7, 2000 **160 Points**

1. (*30 points*) Alice can read and write the file *x*, can read the file *y*, and can execute the file *z*. Bob can read *x*, can read and write *y*, and cannot access *z*.
   a. Please write a set of access control lists for this situation, and say what each Several capability-based systems have been list is associated with.
   b. Please write a set of capability lists for this situation, and say what each list is associated with.
2. (*30 points*) Consider how a system with capabilities as its access control mechanism could deal with Trojan horses.
   a. In general, do capabilities offer more or less protection against Trojan horses than do access control lists? Justify your answer in light of the theoretical equivalence of ACLs and C-Lists.
   b. Consider now the inheritance properties of new processes. If the creator controls which capabilities the created process is given initially, how could the creator limit the damage that a Trojan horse could do?
   c. Can capabilities protect against all Trojan horses? Either show that they can, or describe a Trojan horse process that C-Lists cannot protect against.
3. (*30 points*) Consider Multics procedure *p* and data segment *d*. Procedure *p* is executing and needs to access segment *d*. Segment *d*'s access bracket is (5, 6). Assume that *d*'s access control list gives *p* full (read, write, append, and execute) rights to *d*. In which ring(s) must *p* execute for the following to happen?
   a. *p* can read, write, and append to *d*?
   b. *p* can read *d* but not write to or append to *d*?
   c. *p* cannot access *q*?
4. (*10 points*) Prove that the set of all subsets of a given set *S* (called the *power set* of *S*) forms a lattice under the relation "subset" ($\subseteq$).
5. (*30 points*) Given the security levels TOPSECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, say what type of access (read, write, or both) is allowed in the following situations. Assume discretionary access controls allow anyone access unless otherwise specified.
   a. Paul, cleared for (TOPSECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
   b. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).
   c. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
   d. Sammi, cleared for (TOPSECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).
   e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).
6. (*30 points*) A computer system provides protection using the Biba policy. How would a virus spread if:
   a. the virus were placed on the system at system low (the compartment which all other compartments dominate)?
   b. the virus were placed on the system at system high (the compartment which dominates all compartments)?