Nikkolas Irwin
CS 450
Homework 3

1. Suppose H(m) is a collision-resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x' with x ≠ x', we have H(x) ≠ H(x')? Explain your answer.

   ANS:

   It is NOT true. There are an arbitrary number of n-bit inputs which map to the same output. The number of inputs is arbitrary and variable-length while the number of outputs is 2^n and fixed-length. Since there are multiple inputs that map into the same output (hash-value) the function is NOT one-to-one, and the statement is false.

2. Please compare discretionary access control and role-based access control and explain the advantage of role-based access control.

ANS:

Attributes of Discretionary Access Control (DAC)

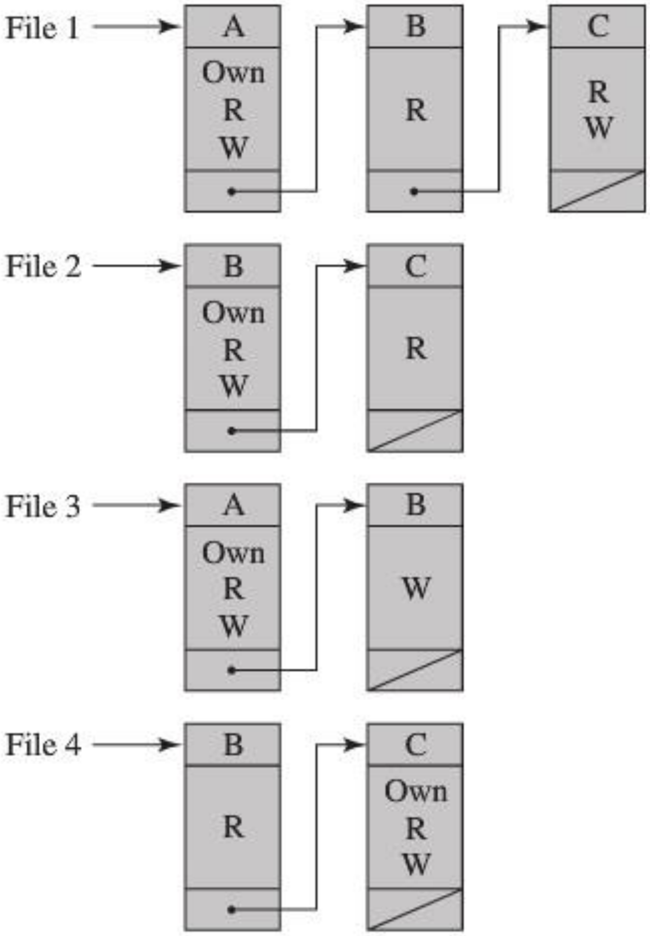
- **An entity may be granted access rights that permit the entity, by its own volition, to enable another entity to access some resource.**
- **DAC uses an access matrix where one dimension consists of identified subjects that may attempt data access to the resources. The other dimension lists the objects that may be accessed.**
- **Identified subjects can be individual users, user groups, terminals, network equipment, hosts, or applications (in addition to users).**
- **Objects may be individual data fields at the greatest level of detail, records, files, or even an entire database.**
- **Each entry in the matrix indicates the access rights of a subject to a unique object.**
- **Decomposition of the access matrix by columns yields access controls lists while decomposition by rows yields capability tickets.**

Attributes of Role-Based Access Control (RBAC)

- **While DAC defines the access rights of individual users and groups of users, RBAC is based on the roles that users assume in a system rather than the user's identity.**
- **RBAC defines a role as a job function within an organization and assigns rights to roles instead of individual users.**
- **Users are assigned to roles either statically or dynamically.**
- **The relationship of users to roles is many-to-many.**
- **RBAC effectively follows the principle of least privilege.**
- **RBAC contains (in a base model): users, roles, permissions, and sessions.**

The advantage of a RBAC model over a DAC model is that the RBAC model provides an easier system for managing users. Since RBAC uses roles for granting access to resources, users can be centrally administered based on the role(s) they are assigned. An additional advantage of RBAC are that at the system level you need elevated privileges to modify a RBAC database while at the user level you can still apply DAC.

3. For the discretionary access control model, an access control matrix can either be decomposed by columns or rows. Given the ACL below, please write down the original access control matrix.



ANS: (Access Matrix)

		OBJECTS			
SUBJECTS		**File 1**	**File 2**	**File 3**	**File 4**
	User A	Own, Read, Write		Own, Read, Write	
	User B	Read	Own, Read, Write	Write	Read
	User C	Read, Write	Read		Own, Read, Write