Tutorial 5

Aim

To exemplify access control and its use in different areas

Questions

1. Authentication, authorisation and access control relate mainly to secrecy/confidentiality and integrity. What is the connection between them? Explain them and their relation on an everyday, not computing-related example.

   Authentication is the mechanism whereby systems may securely identify users' eligibility to use the system.
   Authentication systems provide answers to the questions:
   * Is the user really who he/she claims to be?
   Authorization is a permission (or denial) of the requested access type / level to a particular object by a particular authenticated user.
   Access control is the mechanism that determines if a particular authorisation can be issued or not, i.e. the requested operation can proceed or not.

   Access control is based on authentication and access control policies, and produces a positive or negative authorization, i.e. the operation is either allowed or denied.
   Examples
   - Entering a house
     - Authentication: having a key (proof by possession)
     - Authorisation: the key works with the lock
     - Access control: the door opens
   - Withdrawing money from an ATM
     - Authentication: having a card (proof by possession) and knowing the PIN (proof by knowledge)
     - Authorisation: the central computer instructs the ATM to dispense the money
     - Access control: money handed out

2. What are the basic differences between positive and negative access rights? Give examples for both from your everyday life.

   Positive (what a user can do): the usual way
   - Specify what is permitted

   Negative rights (what the user is not allowed to do): rarely used
   - Specify what is denied

3. Access control lists (ACLs) and capabilities

   Subject: active participant
   Object: passive entity
   ACL: List attached to an object, describes the subjects and their permissions on the object
   Capability list: List attached to a subject, describes the objects and permissions on them

   (a) File systems use access control lists for security and protection. Why is it more economical in this case than using capabilities?

   Usually there are fewer users than files in a system, so the lists are shorter. In fact, the lists are made even shorter by assigning privileges to groups of users, not to individuals.

   (b) Web servers can also use ACLs. Is it also more economical than capabilities? Are ACLs or capabilities more flexible in this case?

   It may or may not be more economical. In fact, capabilities in the form of well-protected cookies can be easier to implement. A more important point is flexibility, as the subjects may be described according to different characteristics: host (IP address, domain name), user agent, time etc

4. You have been asked to implement role-based access control in a
   (a) medical surgery
   (b) student result database system
   (c) library
   (d) classroom

   Would you use mandatory or discretionary access control? Explain it for each case. Define the roles and their access rights, and a plausible way of assigning those rights to roles. What constraints would you apply on roles and access rights, and why?

   Mandatory is stricter and safer when personal data is involved, as is the case in the examples.
   (a) Doctor: *rw* medical data, nurse: *r* medical data, *rw* admin data,
   (b) Student: *r* results, admin staff: *r* results *rw* personal data, teaching staff: *rw* results
   (c) Librarian: *rw* all patron records, patrons: *rw* own records
   (d) Teacher: *rw* all information, students: *r* material *rw* discussion forum