

Identity & Authorization in access control

- Identification
- Authentication
- Authorization
- Access control

Identification

- Assigning of an an entity ACCOUNTABLE for subsequent ACTIONS.
- Accountable entity CAN be a person.
- Accountable entity can ALSO be an organization or even a community or nation.
- Accountable entity can ALSO be a 'Non Person Entity' (NPE).
 - Computer
 - Router
 - Program
 - Process

Authentication

- A MEANS for allowing a right of usage of an access control relevant property to be established :
 - Identity (example: passport)
 - Role (example: uniform)
 - Privilege (example: car key)
 - Label (example: gender)
 - Etc
- An access control relevant property is any property from what either accountability or authority flows.

Authorization

- The EXPLICIT assignment of privileges on the basis of access control relevant properties.

Access Control

- The usage of a combination of one or more of the concepts identification, authentication and authorization in order to determine if a request should be honored.
 - NBAC
 - LBAC
 - ZBAC

NBAC

- Authentication based.
 - Identity based access control
 - Role based access control
- Authentication of subject credentials.
- Authorization flows from subject credentials.
- Commonly used with Access Control List technology.
- Alternatively delegation on authentication can be used.
- Dominant form of access control in dominant operating systems (Windows, Linux, OS-X).

ZBAC

- AuthoriZation based.
- Authentication of authorization token only.
- Authorisation based on EXPLICIT usage of authorization token.
- Well known implementation: Object references in memory safe object oriented programming languages.

LBAC

- Label based
- Authorization based on combination of object and subject labels.
- Used as base for multi level security (BLP/BIBA).
- Well known implementation : SELinux, label based security module for Linux.