ACCESS CONTROL

KTH Applied Information Security Lab

Presented by:
MALEEHA AFZAL:
REGISTRATION NO 00344
BESE3-(B)

Department of Computing, School of Electrical Engineering and Computer Sciences, NUST – Islamabad

Threats to computer systems.

Threats to confidential data and information
Threats to privacy of users.
Attacks on critical information and system resources.
Malwares (viruses, worms and Trojan horses)
Spywares.
Identity theft.
Unauthorized access.
Spam.
Denial of service attacks.
Account hijacks.

KTH Applied Information Security Lab

WAYS TO PROVIDE SECURITY:

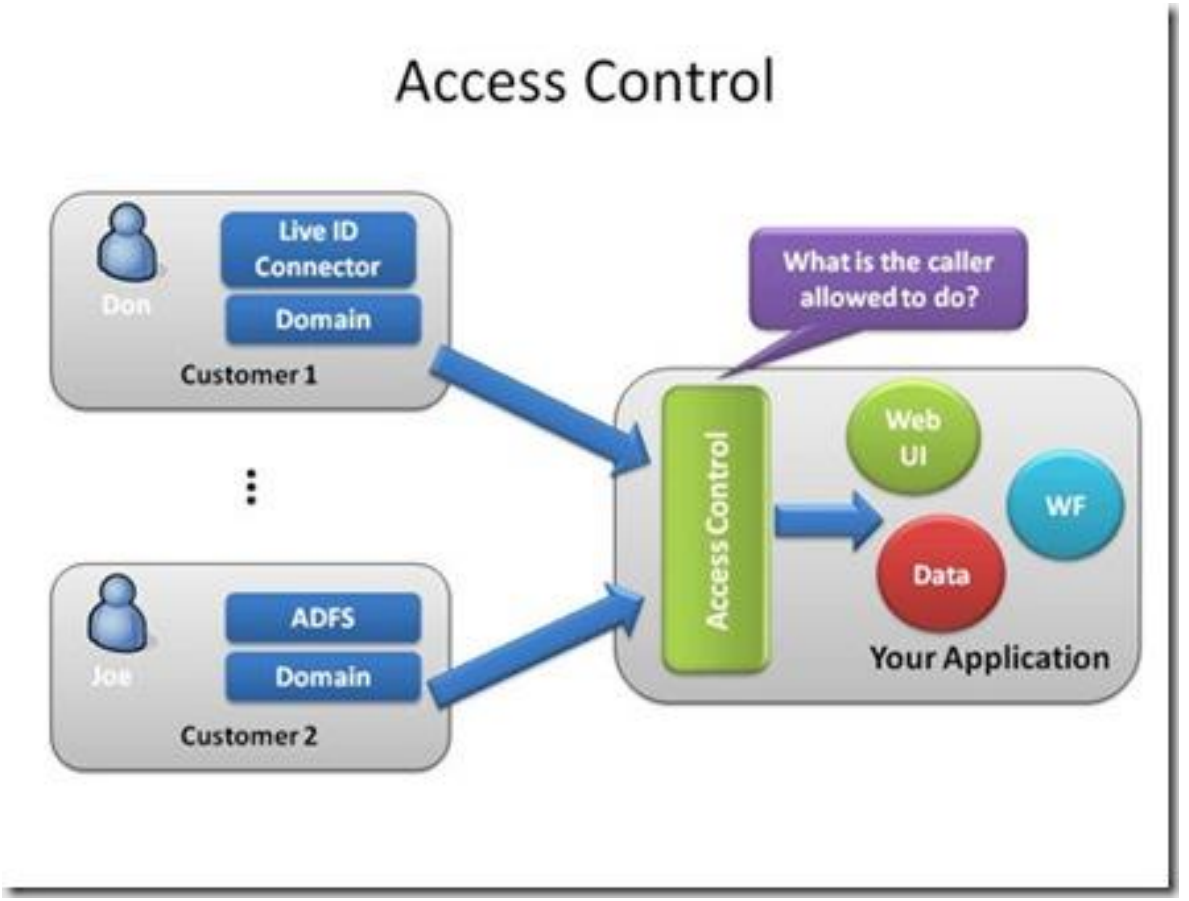
Many mechanisms for enhancing security and protecting one's own information:

Cryptography (encrypting important information).
Authorization (access control).

ACCESS CONTROL:

What is access control?

- The most fundamental security mechanism in use in computer systems.
- Access control is about who can access what.
- Preventing unauthorized access.
- Control on users privileges on resources data, and system.
- Ensures that only authorized accesses can take place.
- Capable of providing security for users accessing applications in a different security domain.



KTH Applied Information Security Lab

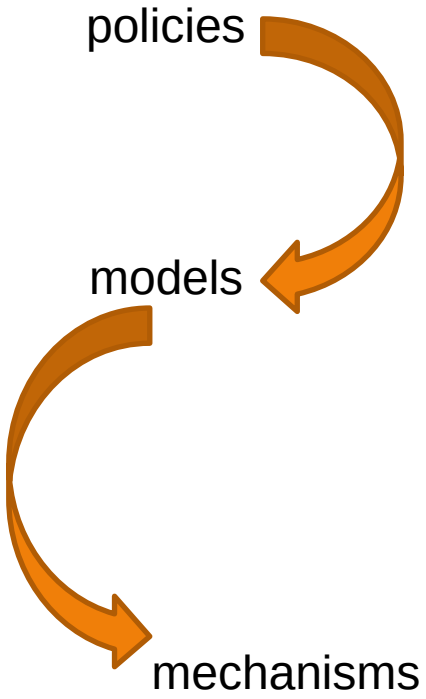
Department of Computing, School of Electrical Engineering and Computer Sciences, NUST – Islamabad

Access control procedure consists of following concepts.

Subject- who requests for an operation on object.(e.g., process, computer, human user, etc.)

Operation- is performed on objects(e.g., read, write, execute, delete, search, etc.)

Object- what has to be accessed. (system resources data etc.)



Access control policies

set of rules that define the permissions according to which access control is managed.

Access control models

- A formal representation and a working model of any security policy.
- The policies are organized/ formalized according to some access control model.

Access control mechanisms.

defines the low level (software and hardware) functions that implement the controls imposed by the policy and formally stated in the model.

KTH Applied Information Security Lab

Access Control policies:

There are three broad term types of policies.

Discretionary (DAC) (authorization-based) policies control access based on the identity of the requestor and on access rules stating what requestors are (or are not) allowed to do.

Mandatory (MAC) policies control access based on mandated regulations determined by a central authority.

Role-based (RBAC) policies control access depending on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles

Discretionary policies (DAC)

Basic idea:

- Users are given privileges on access based on their identity.
- Called discretionary as users can be given the ability of passing on their privileges to other users,
- where granting and revocation of privileges is regulated by an administrative policy.

Models:

access matrix model

	File 1	File 2	File 3	Program 1
Ann	own read write	read write		execute
Bob	read		read write	
Carl		read		execute read

In the access matrix model, the state of the system is defined by a triple (S,O,A)

The matrix can be stored either by rows or by columns

Access Control List (ACL)

The matrix is stored by column. Each object is associated with a list indicating all the subjects and the accesses they can perform on that object.

Capability lists

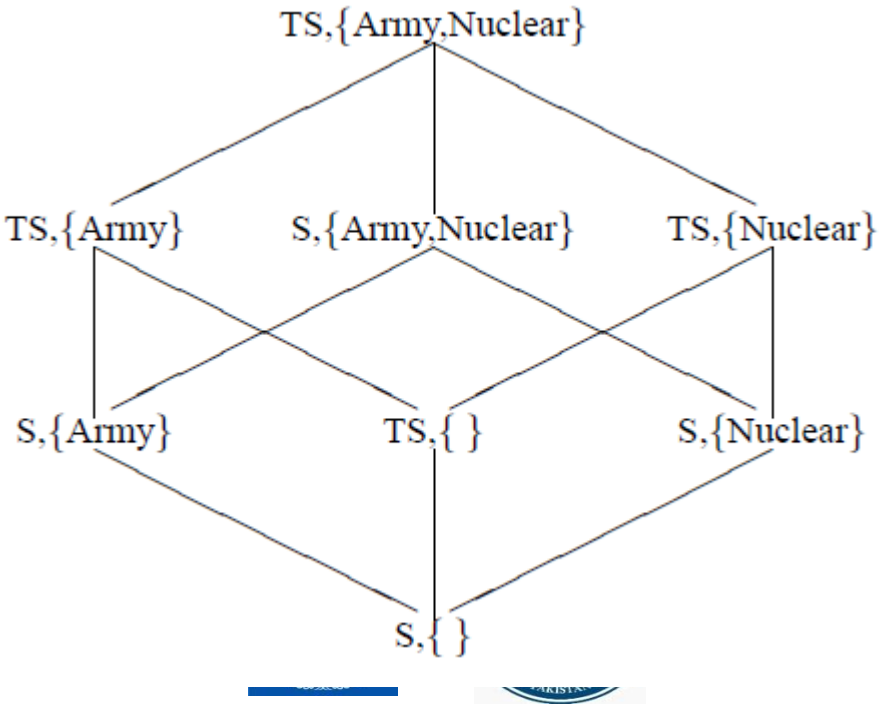
The matrix is stored by row. Each user has an associated list, called capability list, indicating , the accesses that the user is allowed to perform on objects

Mandatory policies (MAC)

- The decisions on whom to allow access are taken by some central authority.
- Users do not have the rights to pass on privileges like they have in Discretionary policies .
- No user is able to settle its own permission.
- The administrator defines the usage and access policy, which cannot be modified or changed by users

Models:

lattice based model:



In multilevel mandatory policies, an access class is assigned to each object and subject.
Mandatory access controls are based on security labels associated with each data item and each user.
A label on a data item is called **a security classification**, while a label on a user is called a **security clearance**.
an access class is defined as consisting of two components: a security level and a set of categories.

Security levels:

Top Secret (TS), Secret (S), Confidential (C), and Unclassified (U),

Secrecy based mandatory policies:
Focus on Prevention of improper disclosure of confidential information.

- No read up: A subject (i.e., a running program) with label X can read an object (i.e., a data item) with label Y only if X dominates Y.
- No write down: A subject with label X can write an object with label Y only if Y dominates X.

prevents information to flow from high level subjects/objects to subjects/objects at lower (or incomparable) levels

Integrity based mandatory policies:
Focus on prevention of improper modification of information or processes.

- No read down .
- No write up.

prevents information stored in low objects (and therefore less reliable) to flow to higher, objects

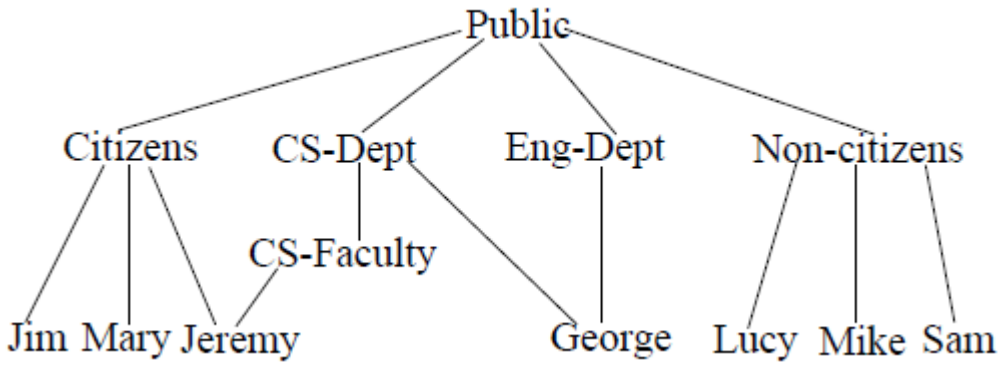
Limitations of mandatory policies.

- Do not guarantee complete secrecy of the information.
- Remain vulnerable to covert channels.
- Covert channels are channels that are not intended for normal communication, but still can be exploited to infer information.

Conditions:

system-dependent conditions
(like the **time or location of access**. For instance, a condition can be associated with the bank-clerks' authorization to access accounts, restricting its application only from machines within the bank building and in working hours).
content-dependent conditions

User groups:



Open and closed policies:

Closed policy: (positive) authorizations specify permissions for an access
Open policy: (negative) authorizations specify denials for an access.

Possible issues:

- Incompleteness
- conflicts

Methods to achieve Completeness:

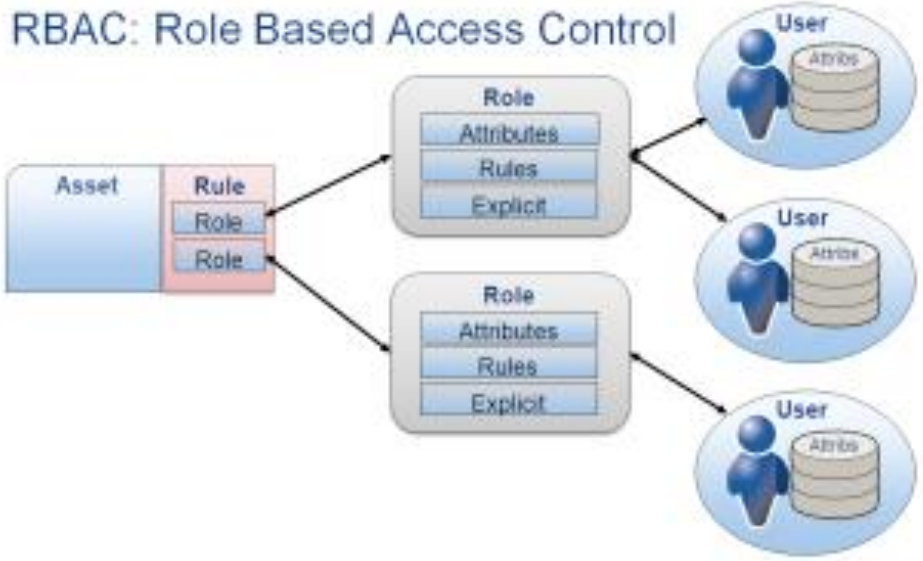
Male sure that access will always be either granted or denied. One of the two possibilities always exist by default.

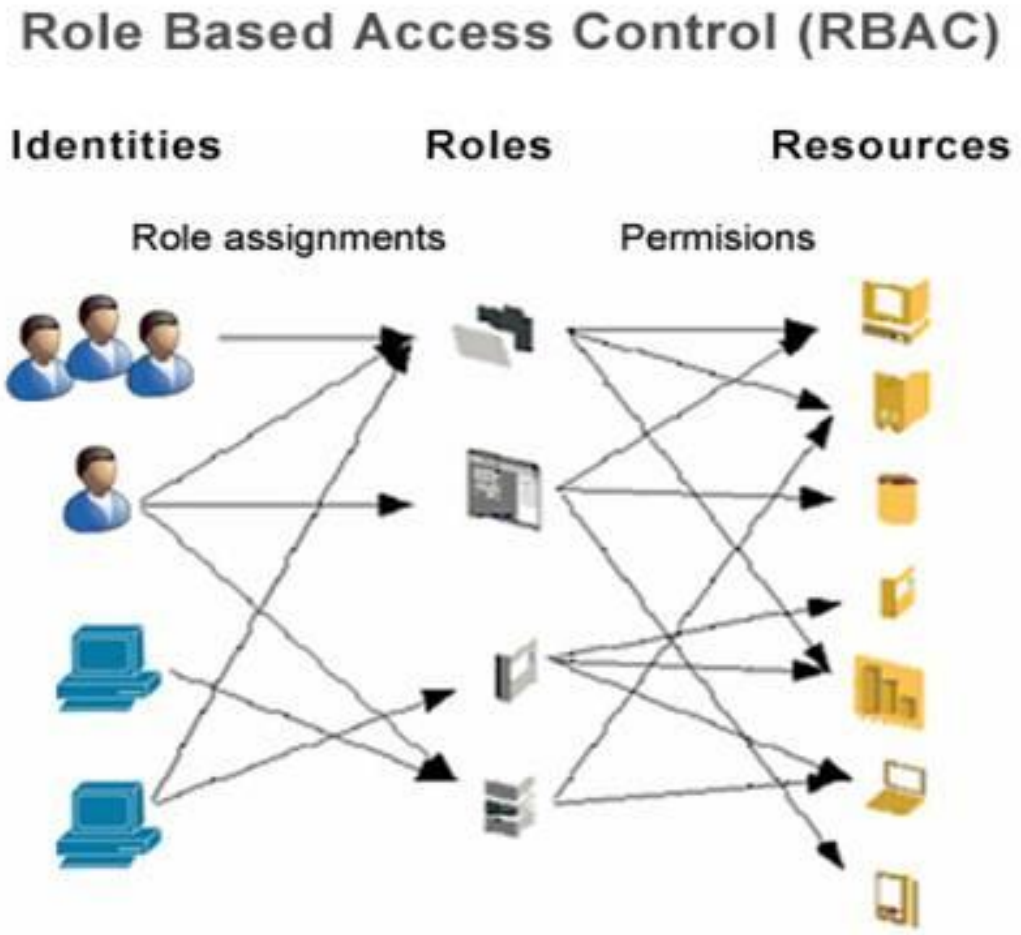
Methods for Conflict resolution:

Denials-take-precedence
Most-specific-takes-precedence
Most-specific-along-a-path-takes-precedence
Strong/weak
Priority level
Positional
Grantor-dependent
Time-dependent

Role-Based Access Control Policies: (RBAC)

- an alternative to traditional discretionary (DAC) and mandatory access control (MAC) policies.
- For access control purposes it is much more important to know the role of user in an organization rather than his identity.
- Users have roles.
- Users are assigned to roles.
- Each user role has specific authorizations

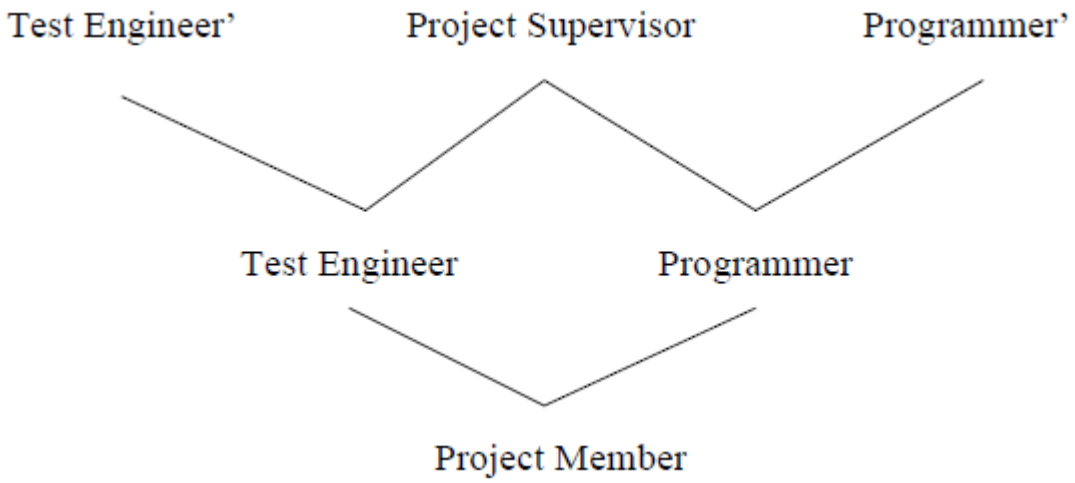




KTH Applied Information Security Lab

ting, School of Electrical Engineering and
Sciences, NUST – Islamabad

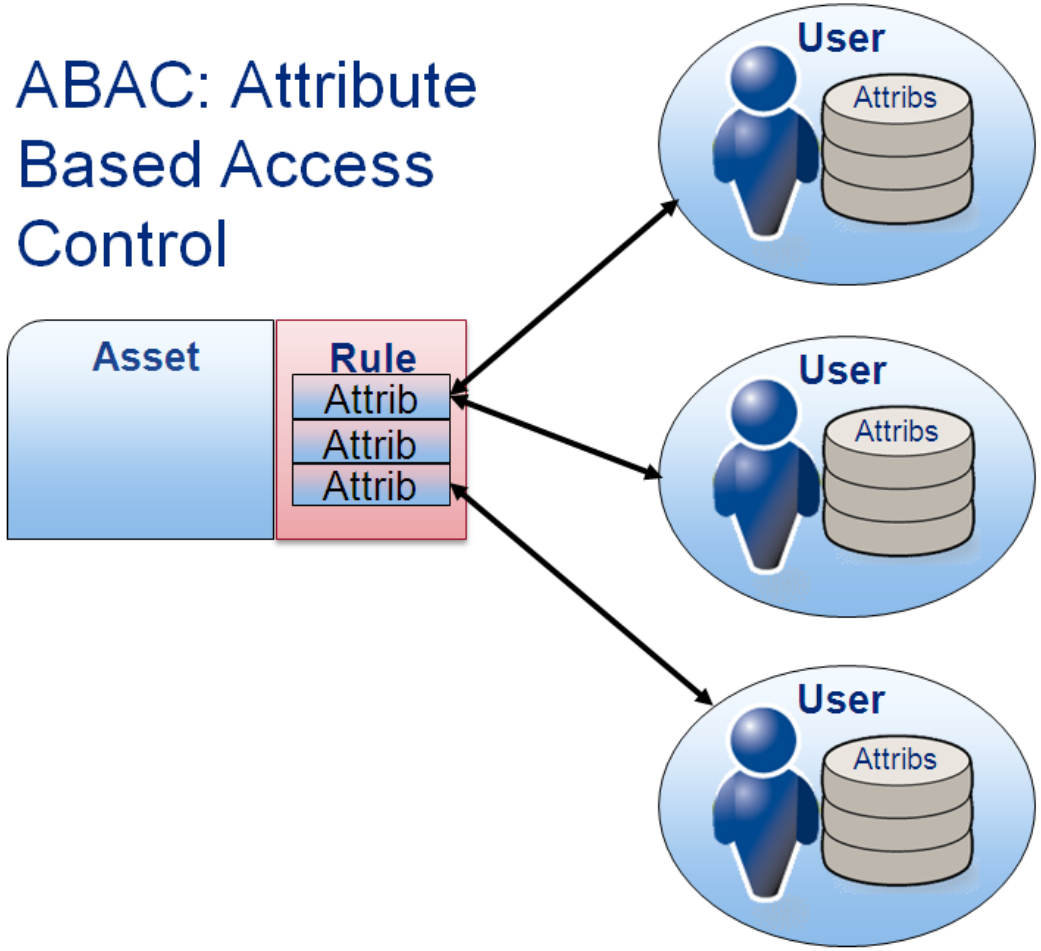
Role hierarchy:



KTH Applied Information Security Lab

Attribute based Access Control: (ABAC)

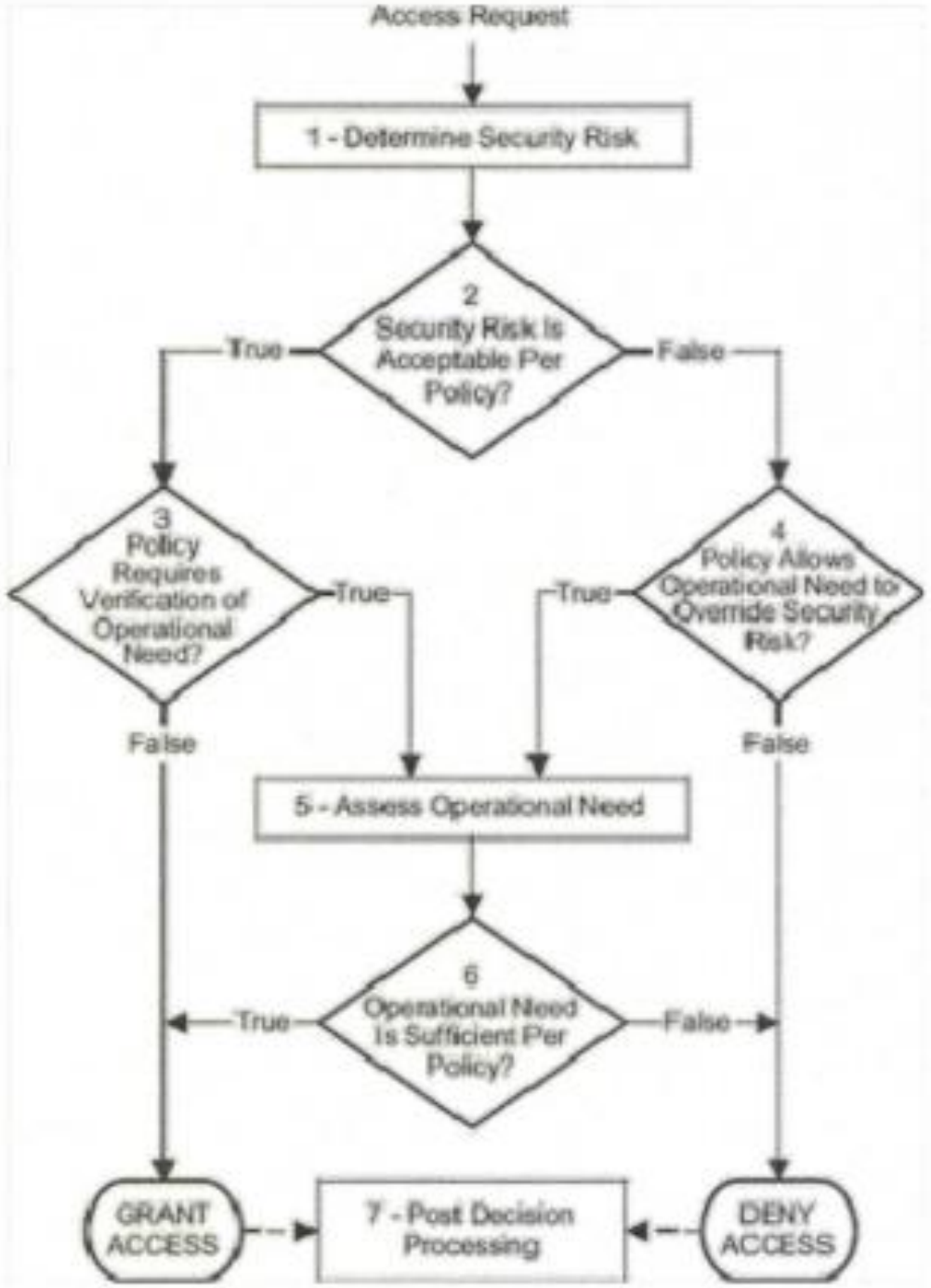
- Access control decisions are made based on a set of attributes, associated with the requester or the environment.
- The requester provides a set of attributes that will be used to determine whether the access will be allowed.
- Once the requester provides these attributes, they are checked against the permissible attributes and a decision will be made depending on the rules for access.



KTH Applied Information Security Lab

Department of Computing, School of Electrical Engineering and Computer Sciences, NUST – Islamabad

Risk Adaptive Access Control: (RAdAC)



KTH Applied Information Security Lab

Department of
Co

Context aware Access Control

Concerns with traditional access control:

- Rigidity.
- the impracticality of its deployment in networks with large numbers of diverse users and devices.
- Constantly changing security needs and nature of applications on cloud.

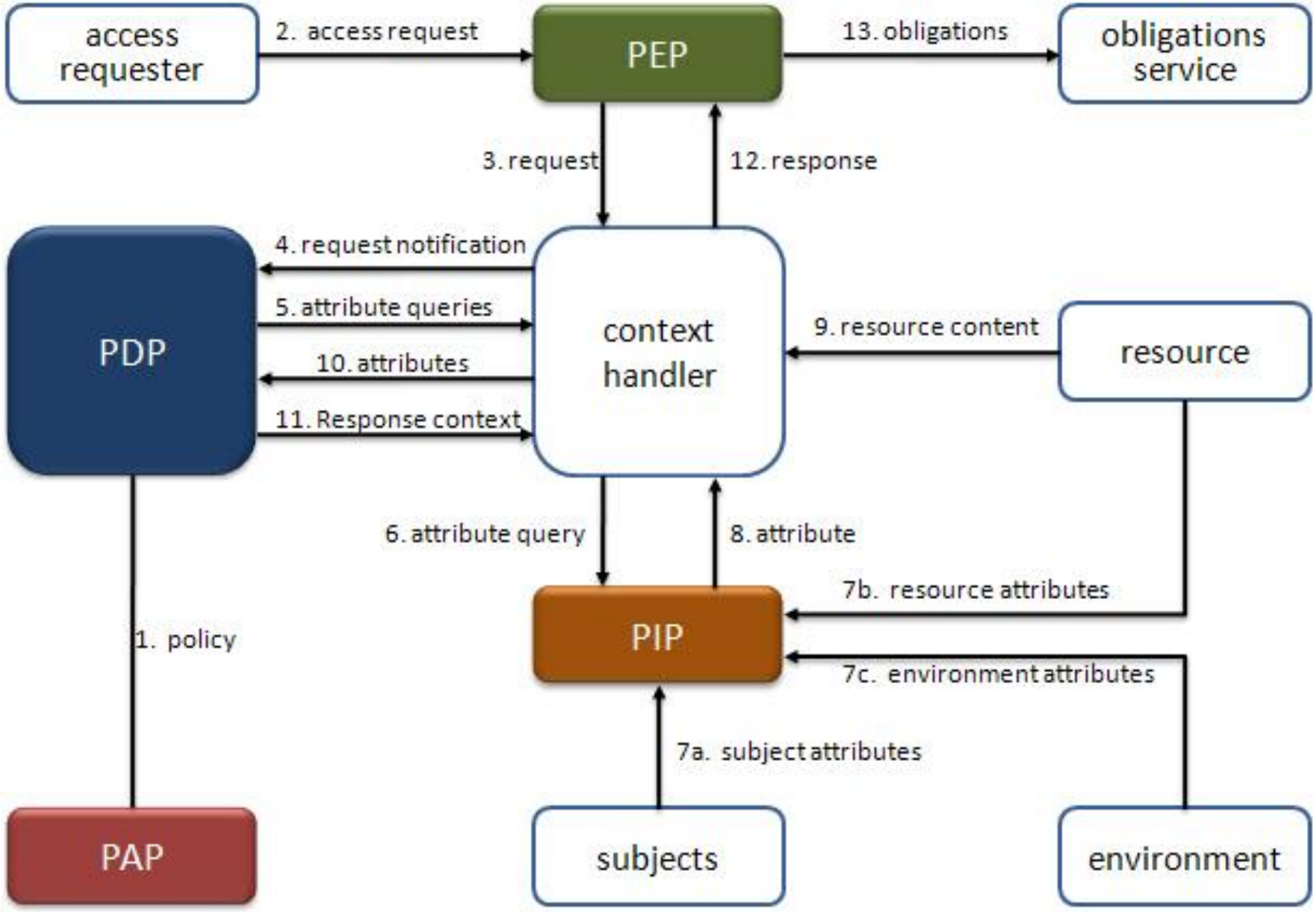
Basic idea

Context-aware access control mechanism dynamically grants and adapts permissions to users according to current context.

Context information

includes environment of the user such as:

- Location
- Time that the user accesses the resource.
- system information such as CPU usage.
- network bandwidth.



KTH Applied Information Security Lab

Thank you.

KTH Applied Information Security Lab

Department of Computing, School of Electrical Engineering and Computer Sciences, NUST – Islamabad