An Attribute Based Framework for Risk-Adaptive Access Control Models

Ravi Sandhu
Executive Director and Endowed Professor
August 2011

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu

Joint work with Savith Kandala and Venkata Bhamidipati

RAdAC Concepts

- Access to resources are automatically (or semi-automatically) granted based on:
  - Purpose for the access request,
  - Security risk, and
  - Situational Factors

- Motivating Example: Displaying a classified document…

Outline

- Benefits of Abstract Models
- Core Characteristics of RAdAC
- Components of RAdAC Model
- Mapping RAdAC to UCON
- Extending UCON Principles to RAdAC and Modified UCON Model

Benefits of Abstract Models

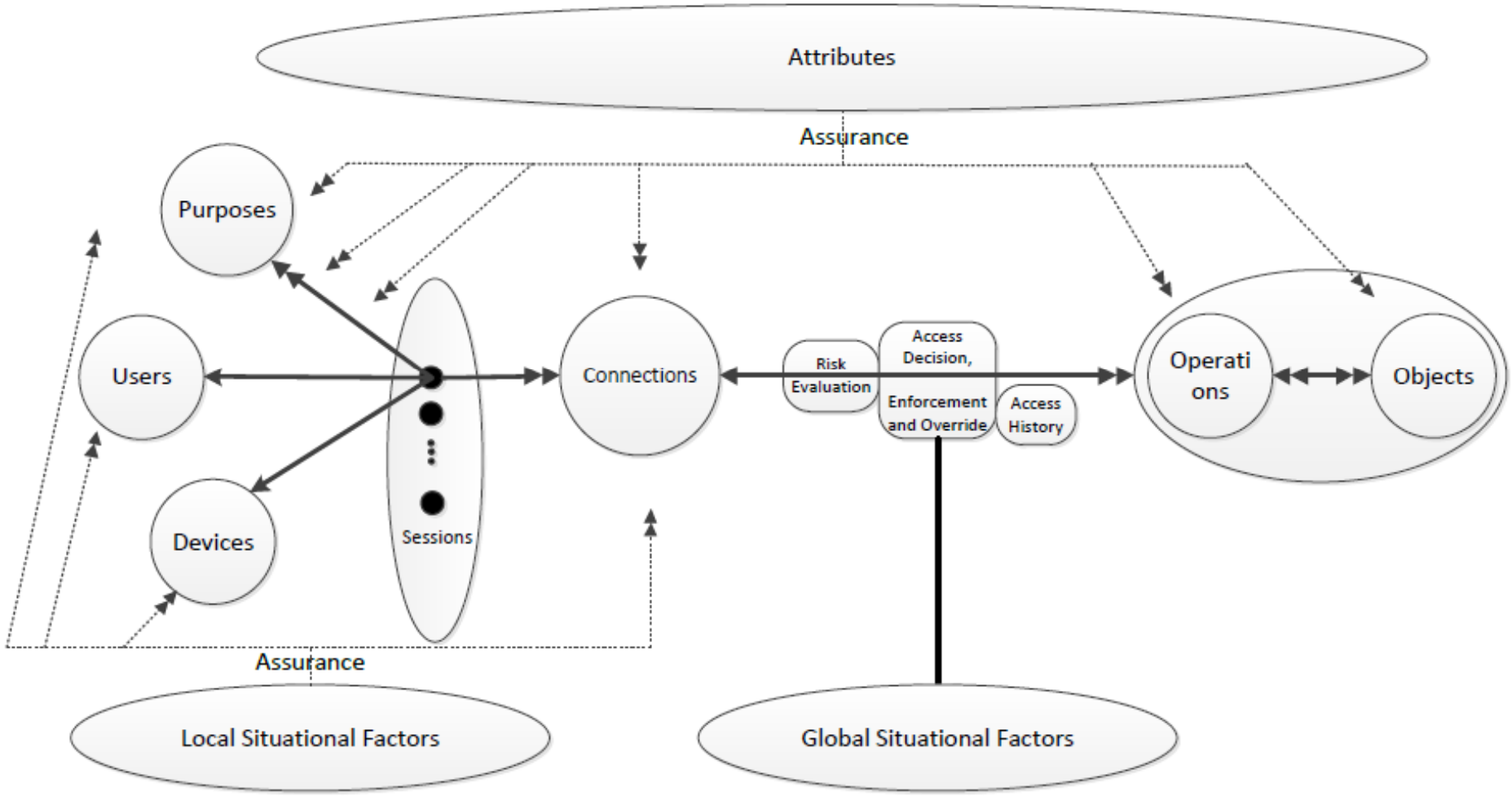
- Proposed at the Policy Layer
- Do not lay out enforcement and implementation details
- Successful practice – DAC, MAC and RBAC
- Provides a formal and structural foundation

Core Characteristics of RAdAC

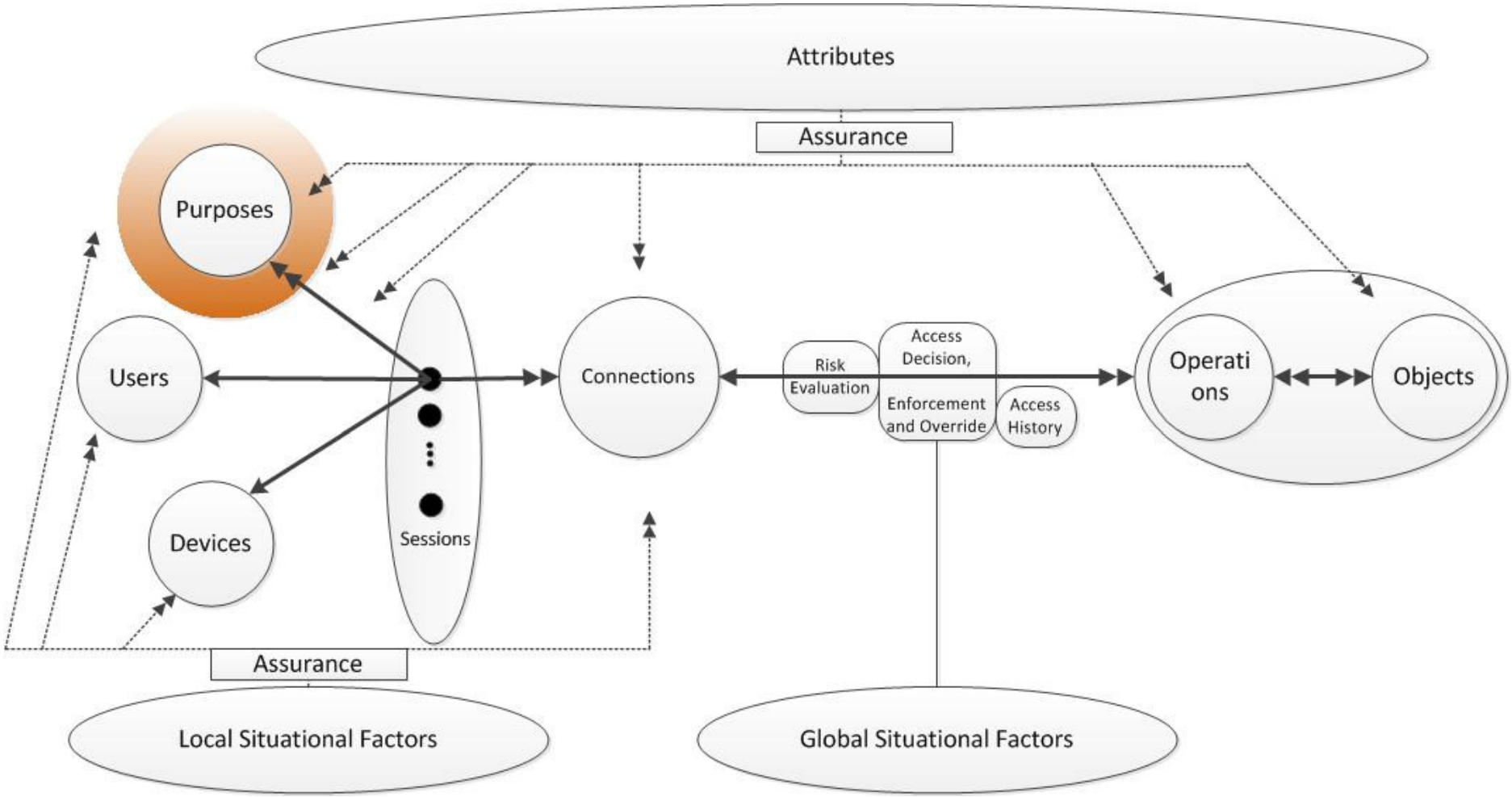
Reference – Robert McGraw, NIST Privilege Management Workshop, 2009

- Operational Need
- Security Risk
- Situational Factors
- Heuristics
- Adaptable Access Control Policies

RAdAC Model


Attributes
Assurance
Purposes
Users
Devices
Sessions
Connections
Risk Evaluation
Access Decision, Enforcement and Override
Access History
Operations
Objects
Assurance
Local Situational Factors
Global Situational Factors

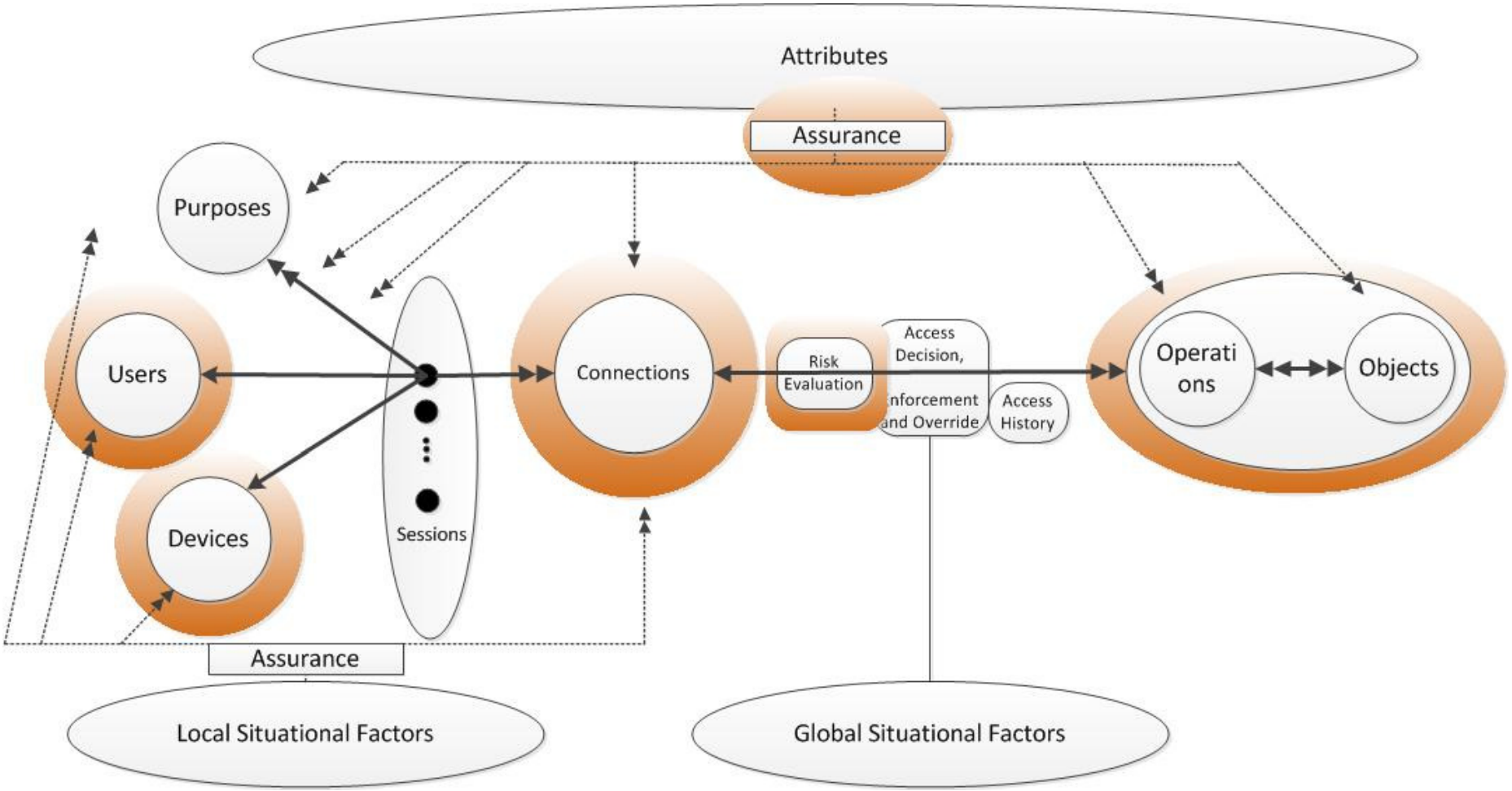
Operational Need / Purpose



Operational Need / Purpose

- Purpose (Operational Need)
  - The reason for the user's access request
  - Can manifest as:
    - A user's membership in a role
    - An authority is attesting to a user's need to access the object
  - Examples: Health Care – Emergency treatment
    Energy – Impending power emergency
    Banking – Consent to access acct info.

Security Risk

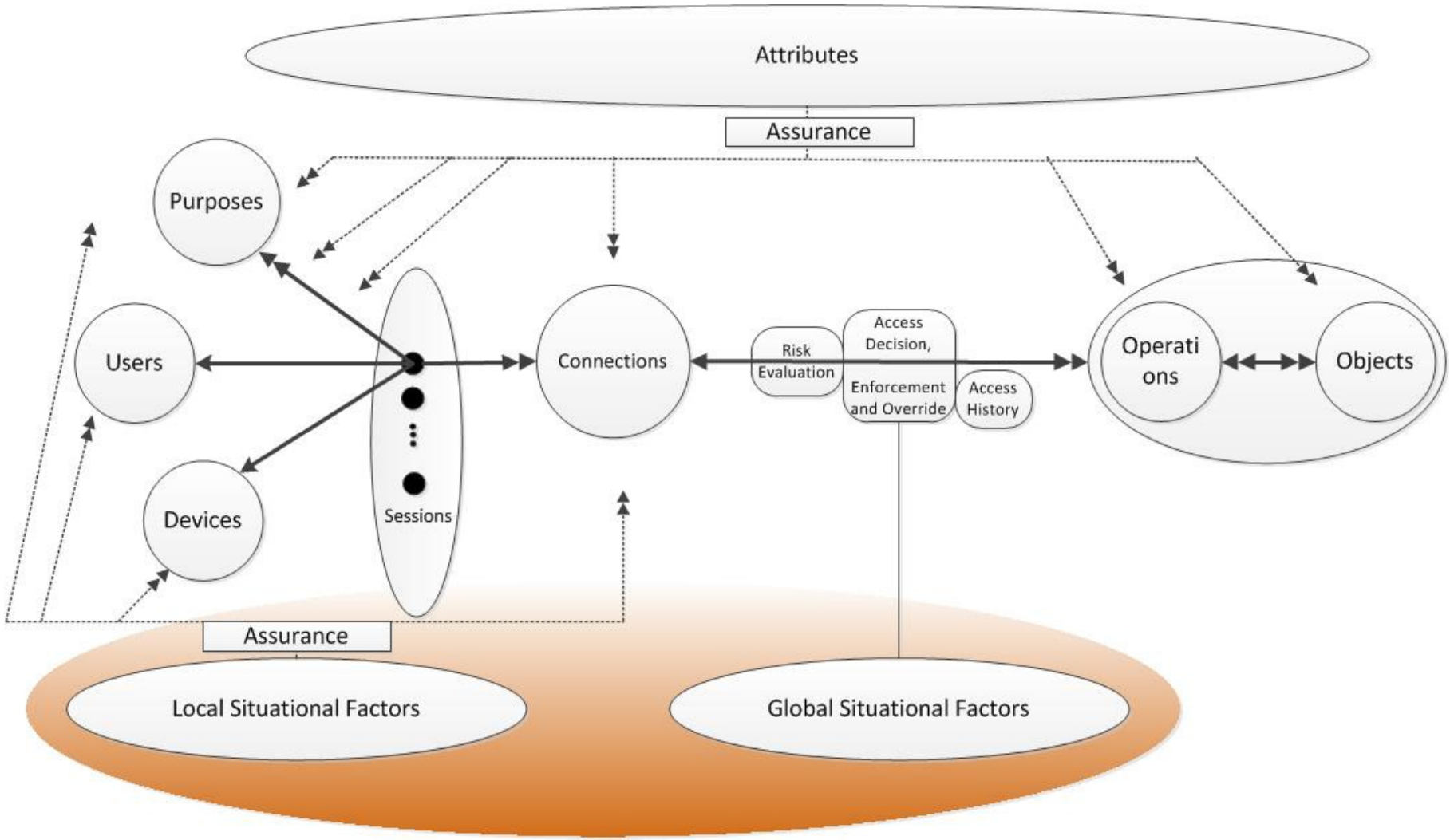


Security Risk

- Users
- Devices
- Objects
- Operations
- Connections
- Attribute Providers and Level of Assurance

- Security risk evaluation be based on risk associated with each of these components, as well as a composite risk.

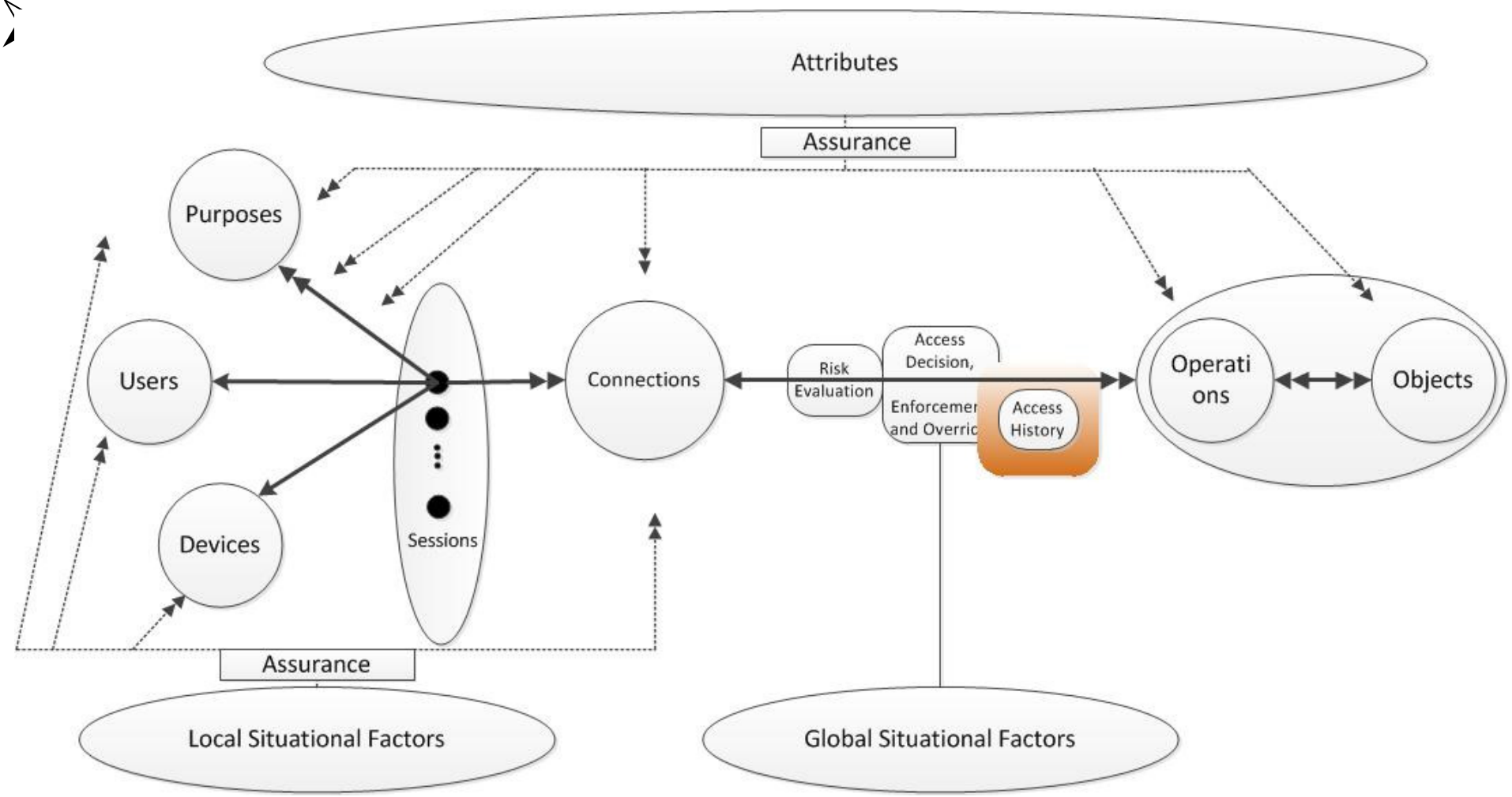
Situational Factors



Situational Factors

- Environmental or system oriented decision factors
- Global Situational Factors
  - Example : National terrorist threat level, Enterprise under cyber attack
- Local Situational Factors
  - Example: location, current local time for accessible time period (e.g., business hours), current location for accessible location checking (e.g., area code, connection origination point)

Access History

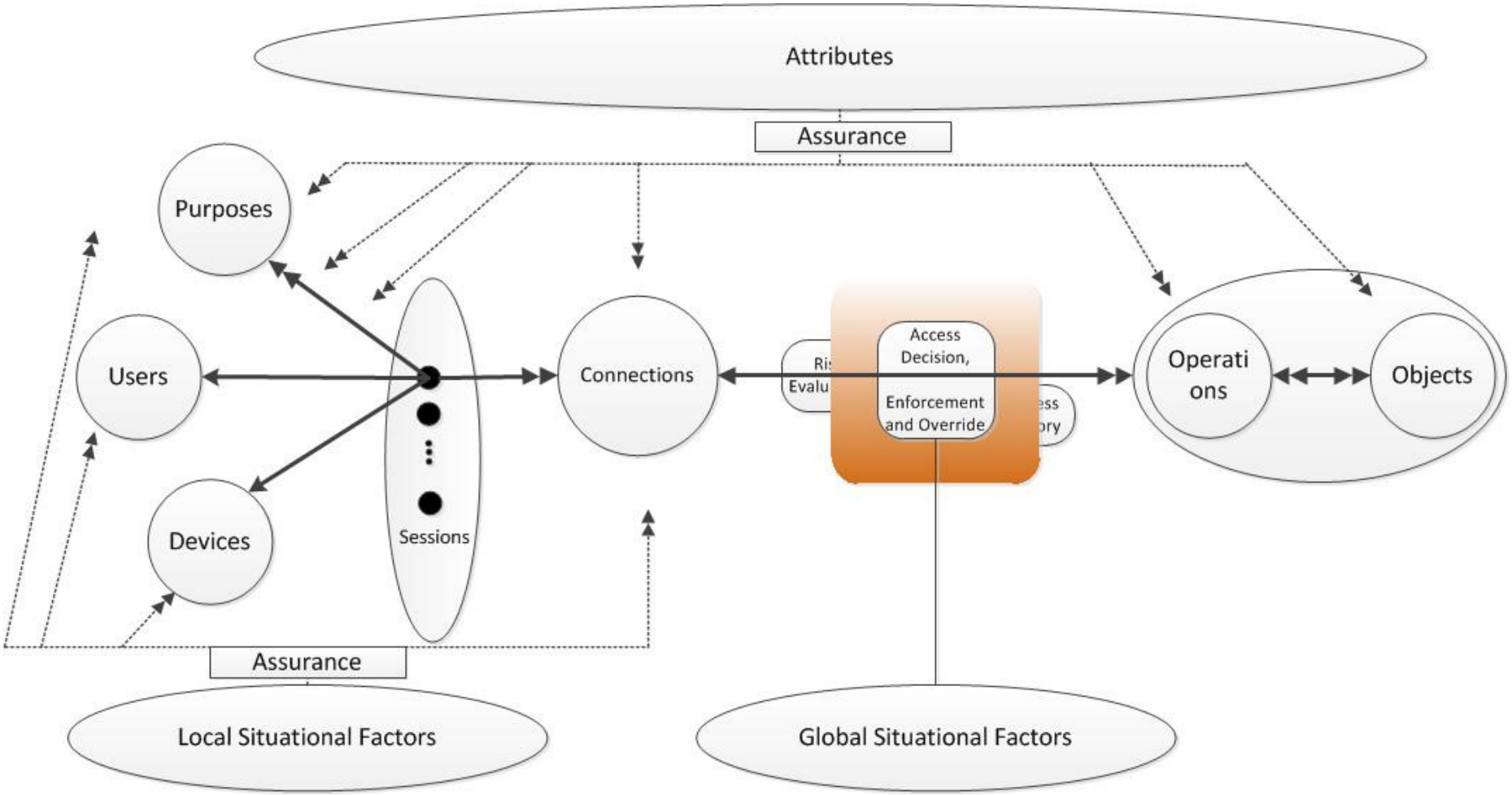


Access History

- Access History
  - Provides two functions
    - updates the object access history repository with the attributes in the access request and the access control decision
    - provides input for future access decisions

- Heuristics can be used to
  - Fine-tune access control policies
  - Improve future access decisions
  - Inputs the access decisions

Adaptable Access Control Policies

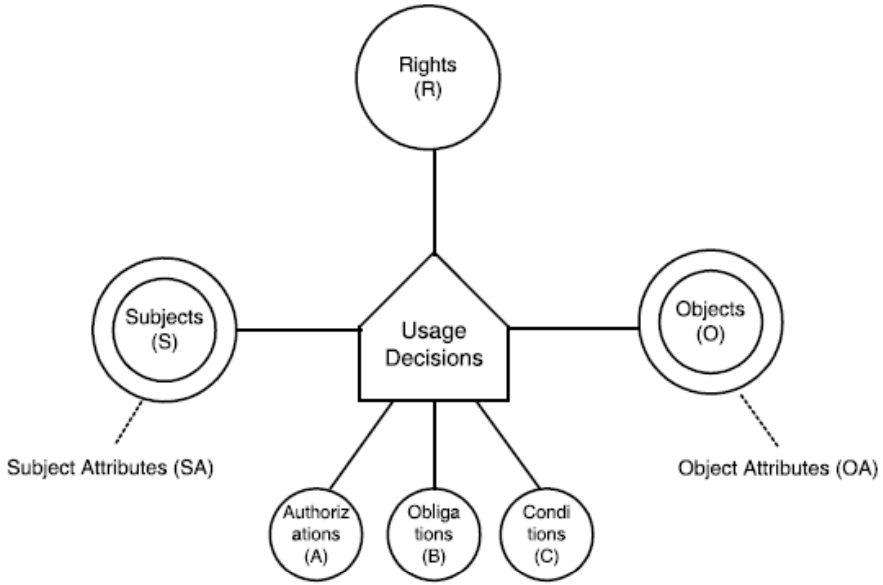


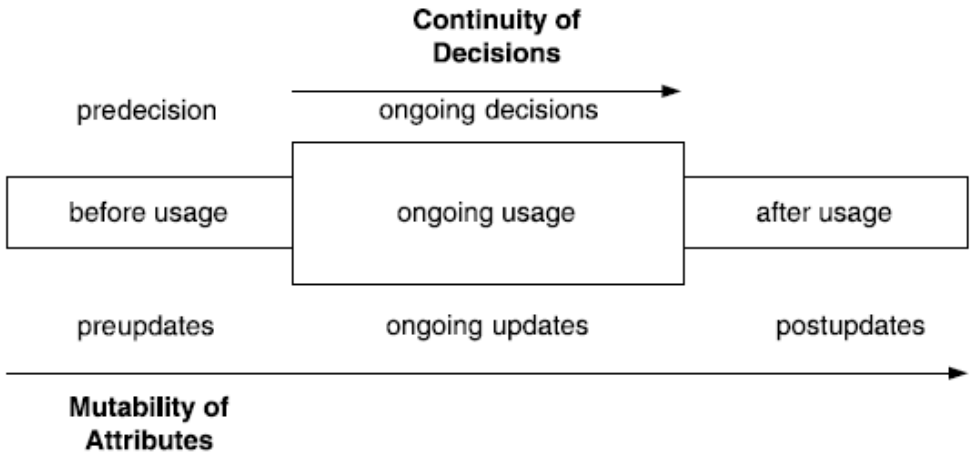
Adaptable Access Control Policies

- Adaptable access control policies can be defined based on all the components

- Overrides
  - Automatic
  - Semi-Automatic
  - Manual

UCON Model

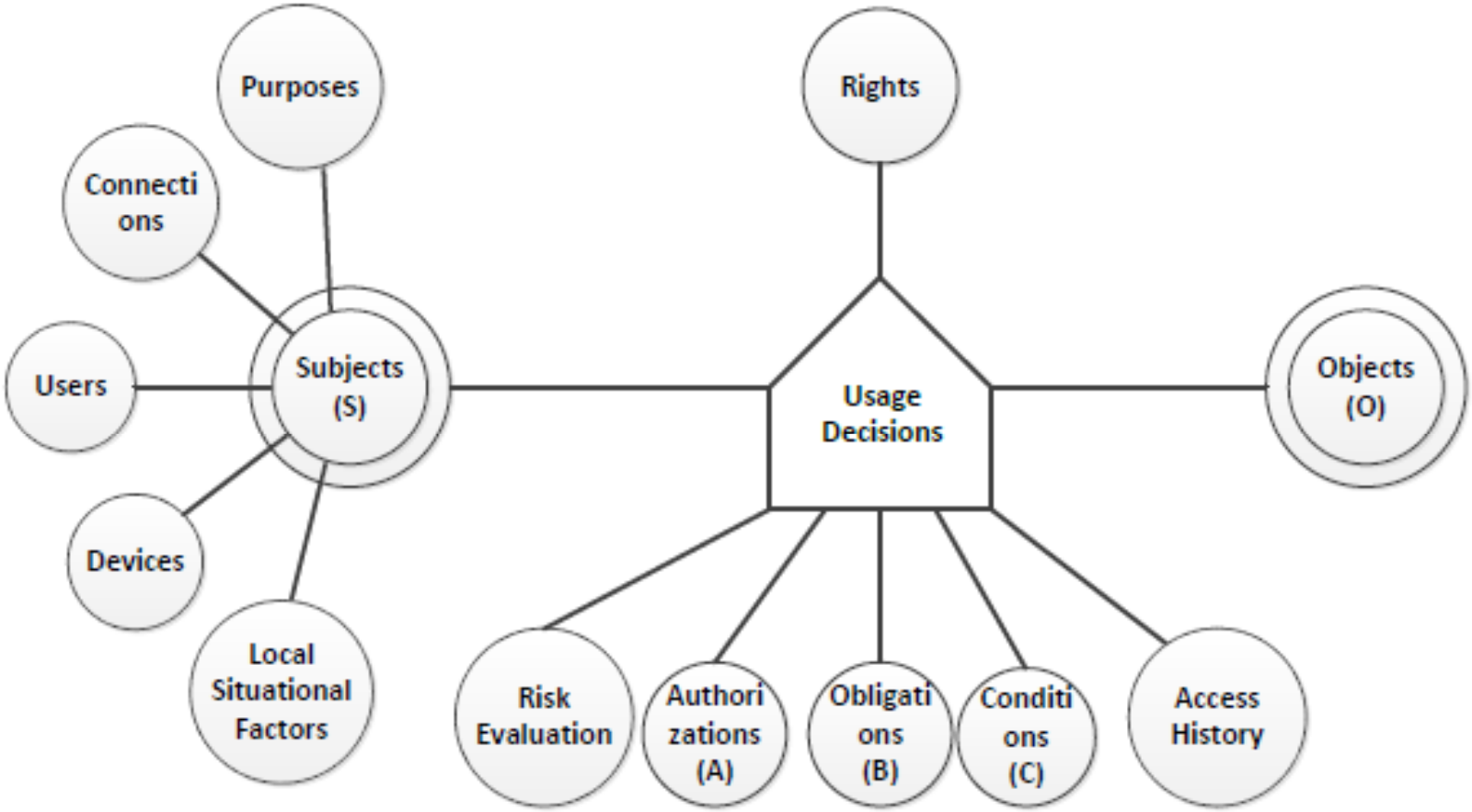

Rights
(R)
Subjects
(S)
Usage
Decisions
Objects
(O)
Subject Attributes (SA)
Object Attributes (OA)
Authoriz
ations
(A)
Obliga
tions
(B)
Condi
tions
(C)


Continuity of
Decisions
predecision
ongoing decisions
before usage
ongoing usage
after usage
preupdates
ongoing updates
postupdates
Mutability of
Attributes

Mapping RAdAC to UCON

- Key missing features
  - Subject definition
  - Access History
  - Risk Evaluation
- Extending UCON Principles to RAdAC

Modified UCON Model



Conclusion and Future Work

- Purely focused on the abstract models
- The modified UCON model with the decomposed subject definition and the added functions of access history and risk evaluation is most suitable for modeling and implementing the RAdAC concept.
- Future Work:
  - Enforcement and implementation
  - Defining architecture, protocols and mechanisms for the proposed RAdAC model