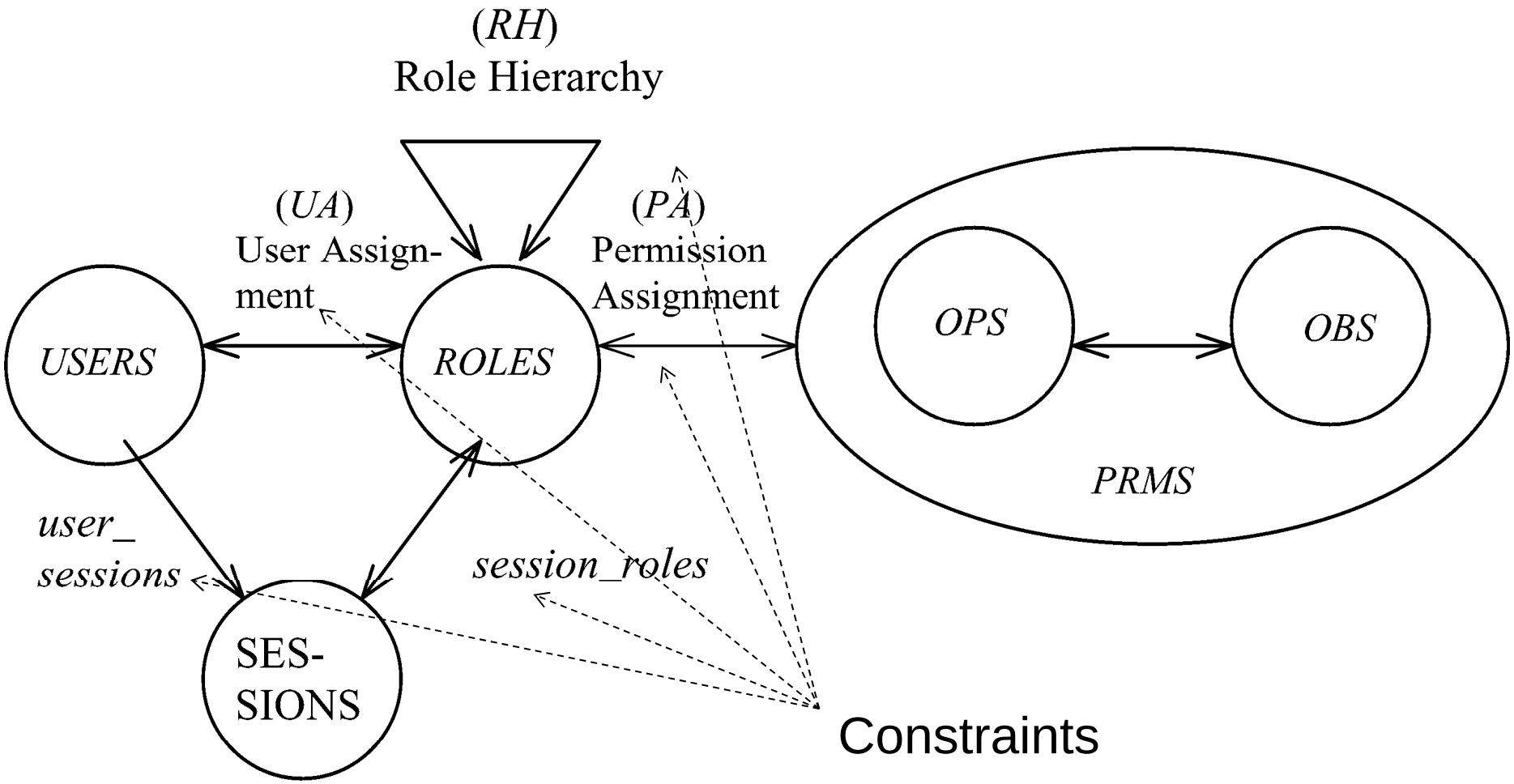
Risk-Aware RBAC Sessions

Khalid Zaman Bijon, Ram Krishnan and Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio

Dec 17, 2012
ICISS 2012
IIT Guwahati, Assam, India

RBAC Sessions



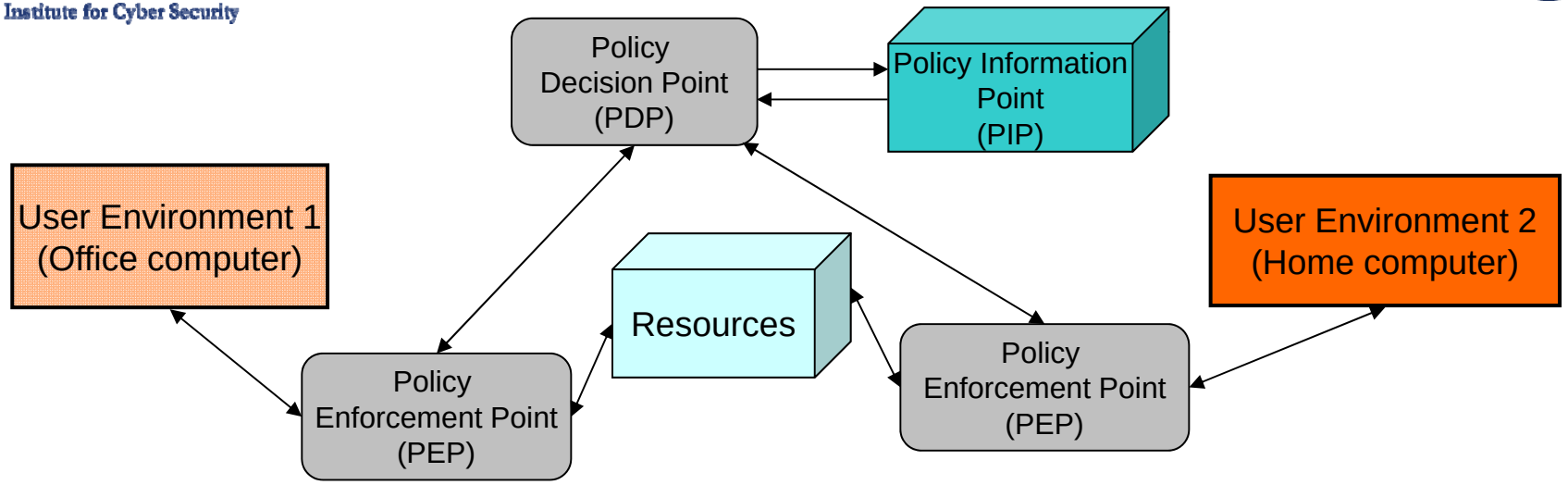
RBAC Sessions

- Motivation for Session in Classical RBAC
  - Least Privilege
  - Dynamic Separation of Duty
- A major risk mitigation feature in RBAC
- Functionalities:
  - Role Activation: Activate a role **(Increase the session's access capability)**
  - Role Deactivation: Deactivate a role **(Decrease the session's access capability)**

Concern:

1. User's complete discretion on activation and deactivation
2. No differentiation of sessions

Motivational Scenario



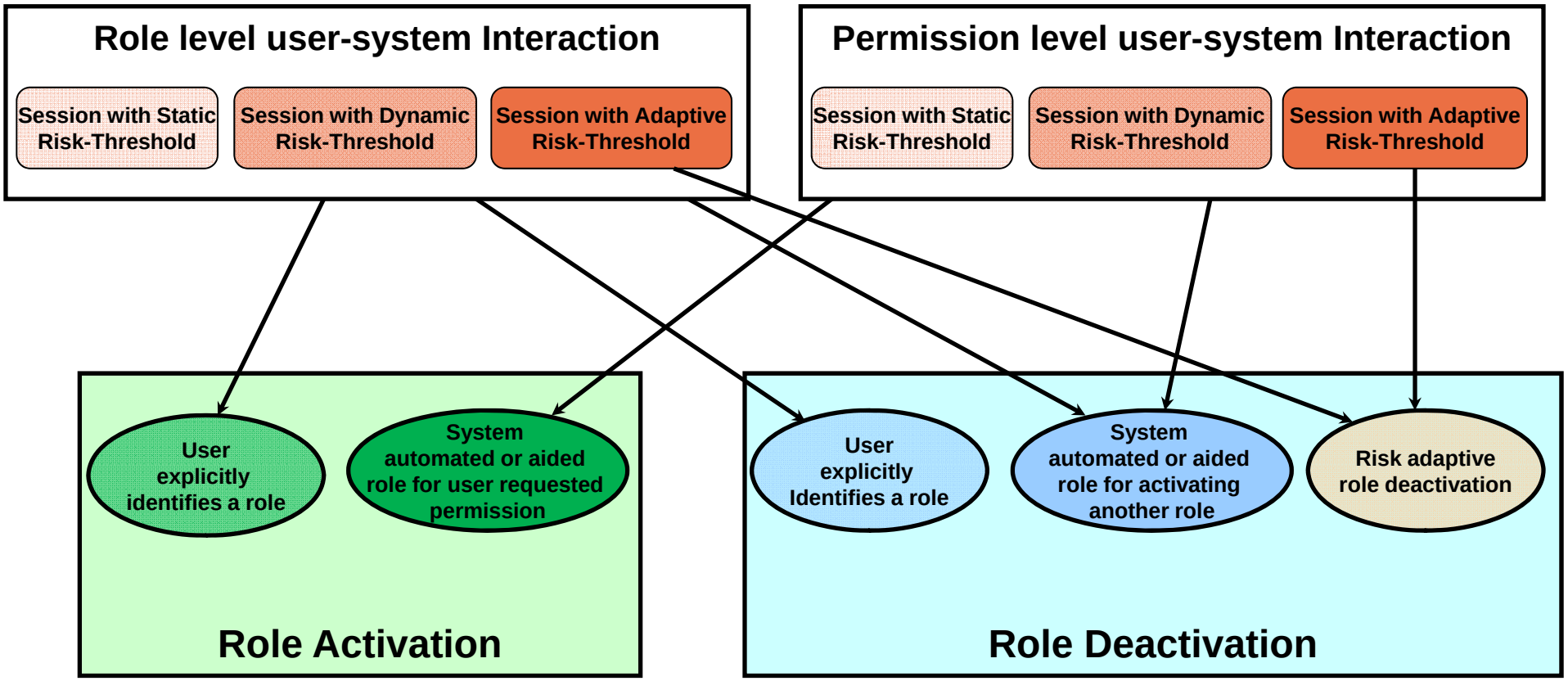
A simple PDP/PEP based Access Control Enforcement Model

- Environment 2 might be less secure than Environment 1
  - Thus, user sessions from them should not be equally secure
- A user session can also be compromised
  - E.g. by malware running in user's computer (environment)
- Attacker could completely impersonate the user in a compromised session
  - Activating all the roles assigned to the user **(role activation is entirely at user's discretion in every session)**

Mitigation Strategy

- A procedure to identify how risky a session is
  - risk-estimation of a session
- Limit session's access capability based on its estimated risk
  - a threshold on role activation based on estimated risk
  - session risk threshold vs combined risk of activated roles
- Reduce User's discretion on Role activation and deactivation
  - involve system to select a role to activate or deactivate

Overview


Role level user-system Interaction
Session with Static Risk-Threshold
Session with Dynamic Risk-Threshold
Session with Adaptive Risk-Threshold
Permission level user-system Interaction
Session with Static Risk-Threshold
Session with Dynamic Risk-Threshold
Session with Adaptive Risk-Threshold
User explicitly identifies a role
System automated or aided role for user requested permission
User explicitly Identifies a role
System automated or aided role for activating another role
Risk adaptive role deactivation
Role Activation
Role Deactivation

Risk-Aware RBAC Session Characteristics

- Risk-Aware RBAC sessions could be different types
  - when and how the risk-threshold is estimated
  - system and user properties that influences the calculation process
- Session with static risk-threshold (SSR)
  - statically calculated
  - does not change across session
  - properties that does not change frequently (e.g. credential, assigned role-set)
- Session with dynamic risk-threshold (SDR)
  - calculated before each user session
  - may vary across session
  - Some dynamic properties (e.g. time, place, currently activated roles)
- Session with adaptive risk-threshold (SAR)
  - calculated before each user session
  - may vary across and within a session
  - affected by certain user activities during a session
  - need system functionalities to stop certain activities (e.g. system automated role deactivation)

User Driven Role Activation

- A User can activate a role in a session iff
  - the role is assigned to the user
  - activation of a role does not cross the risk-threshold of the session
    - individual risk of the role below the risk-threshold and
    - combined risk of activated roles is below the risk-threshold

- Activation of a role might also lead to deactivate certain activated roles in a session
  - in order to satisfy session risk-threshold
  - system guided or system automated

- Two different user-system interactions for role activation
  - role level (simply request a role to activate)
  - permission level (request a permission to access and system will activate the role)

Role Activation Framework
(role level user-system interaction)

- Strict Activation
  - activates if risk-threshold is satisfied
  - no deactivation of already activated roles in session

- Activation with System Guided Deactivation
  - activates if risk-threshold is satisfied
  - if not, system suggests user to deactivate certain activated roles in order to lower session risk

- Activation with System Automated Deactivation
  - activates if risk-threshold is satisfied
  - if not, system automatically deactivates roles
  - need a specific role deactivation algorithm (e.g. LRU, heuristics)

Role Activation Framework
(permission level interaction)

- Permission level interaction process:
  - users simply try to access a permission in a session
  - system checks whether necessary role is activated in the session
  - if yes, allow the user access
  - otherwise, finds if there is a role for the permission
- In the presence of multiple roles with the permission
  - system displays roles and user selects one, or
  - automatic role selection by the system
- Automatic role selection
  - less risky role, role with minimum permission, etc.
- Three different role activation models
  - strict activation (no deactivation)
  - activation with system guided deactivation
  - activation with system automated deactivation

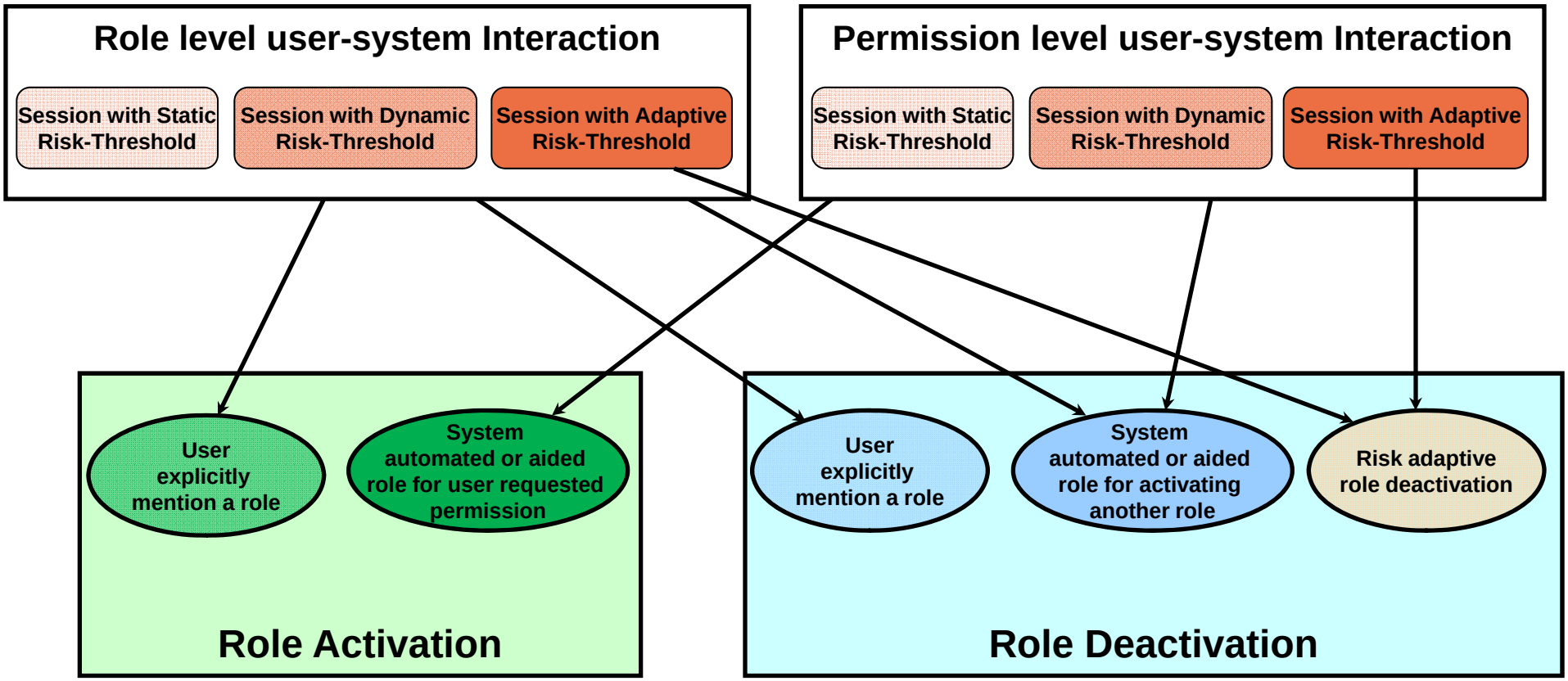
Risk-Adaptive Role Deactivation

- Risk-threshold varies during a session in SAR
  - might need continuous monitoring of a session activities
  - could be lowered by user's abnormal behavior or any detected malicious activities or other factors
  - further reduces the session's access capability

- Decrease of risk-threshold might cause deactivation of certain activated roles
  - roles that exceeds newly estimated threshold, roles that reduces the threshold, etc.

- System automated role deactivation function
  - called by the system each time risk-threshold change
  - automatically deactivates affected roles, or
  - forces user to deactivate certain roles (provides some choices on what roles to be deactivated)

Summary


Role level user-system Interaction
Session with Static Risk-Threshold
Session with Dynamic Risk-Threshold
Session with Adaptive Risk-Threshold
Permission level user-system Interaction
Session with Static Risk-Threshold
Session with Dynamic Risk-Threshold
Session with Adaptive Risk-Threshold
User explicitly mention a role
System automated or aided role for user requested permission
Role Activation
User explicitly mention a role
System automated or aided role for activating another role
Risk adaptive role deactivation
Role Deactivation

Formal Specification

- Formally enhance NIST Core RBAC model
  - for a session with dynamic risk threshold
  - develop functionalities for a permission level user-system interaction (present NIST RBAC only supports role level interaction)
- Three required information of a risk-aware session in NIST Core RBAC
  - **assigned risk :** a mapping of permission p to a positive real value, which gives the risk assigned to a permission.
  - **risk threshold :** a mapping of session s to a positive real number that gives the maximum risk the session could contain.
  - **present risk :** a mapping of session s to a positive real number that gives the present risk value of the session.
- Necessary functions
  - **AssignRisk**: assigns a risk value to a permission
  - **RoleRisk**: returns estimated risk of a role
  - **CreateSession**: user creates a session and system calculate risk-threshold for the session
  - **PerformTask**: user tries to perform a task that might cause a role activation
  - **CheckAccess**: called by PerformTask function, it checks if user is authorized for a permission
  - **AddActiveRole**: called by CheckAccess, tries to activate if there is a role for the requested permission
  - **Deactivation**: called by AddActiveRole to deactivate some already activated roles in order to activate a role for the requested permission