Extensões ao Modelo RBAC de Restrições para suportar Obrigações do $UCON_{ABC}$

Edemilson da Silva, Altair Santin, Edgard Jamhour e Carlos Maziero (PUCPR)

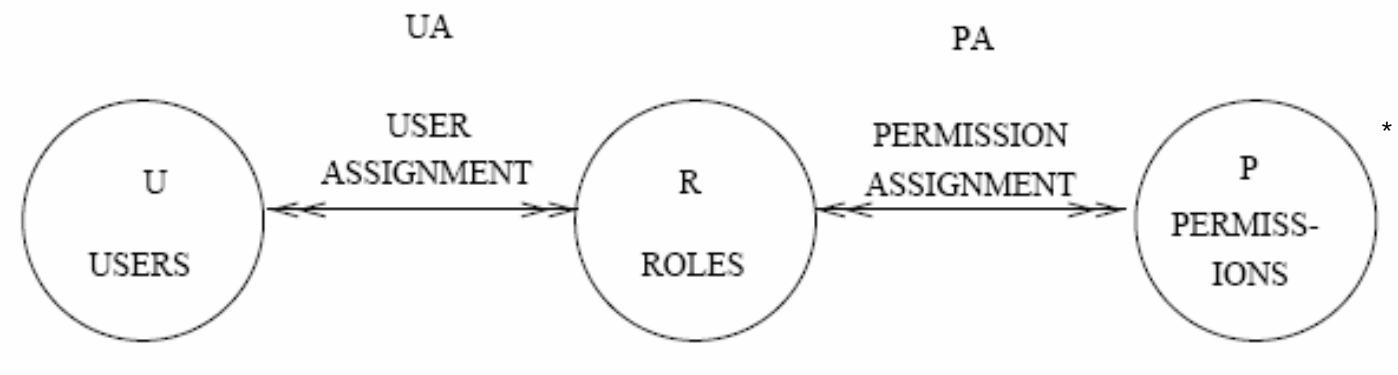
Emir Toktar (Paris VI)

Roteiro

- Introdução
- Modelo de restrições RBAC
- Modelo de Restrições $UCON_{ABC}$
- Motivação
- Proposta
- Conclusão

Introdução

- *Role Based Access Controle* é um modelo de **controle de acesso**



- ANSI INCITS 359-2004 (http://csrc.nist.gov/rbac/)

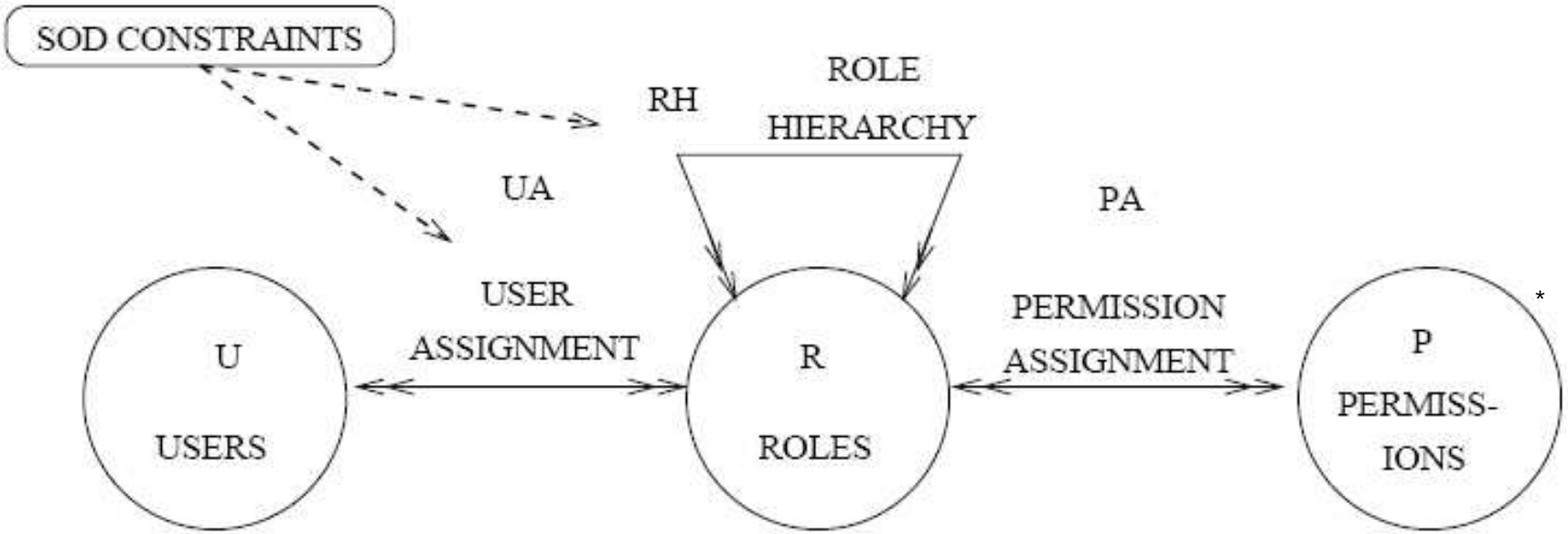
*Sandhu, R., Ferraiolo, D., Kuhn, R. The NIST Model for Role-Based Access Control: Towards A Unified Standard, ACM WRBAC. 2000.

Modelo de restrições NIST RBAC (modelo de consenso)

- *Separation of Duty* (estática/dinâmica)
  - Evita fraudes e danos acidentais
  - Divide as tarefas em subtarefas executadas sequencialmente
- Principio do mínimo privilégio
- Cardinalidade
  - Define o número máximo de papéis que um usuário pode ativar numa sessão

Restrições do modelo de Consenso

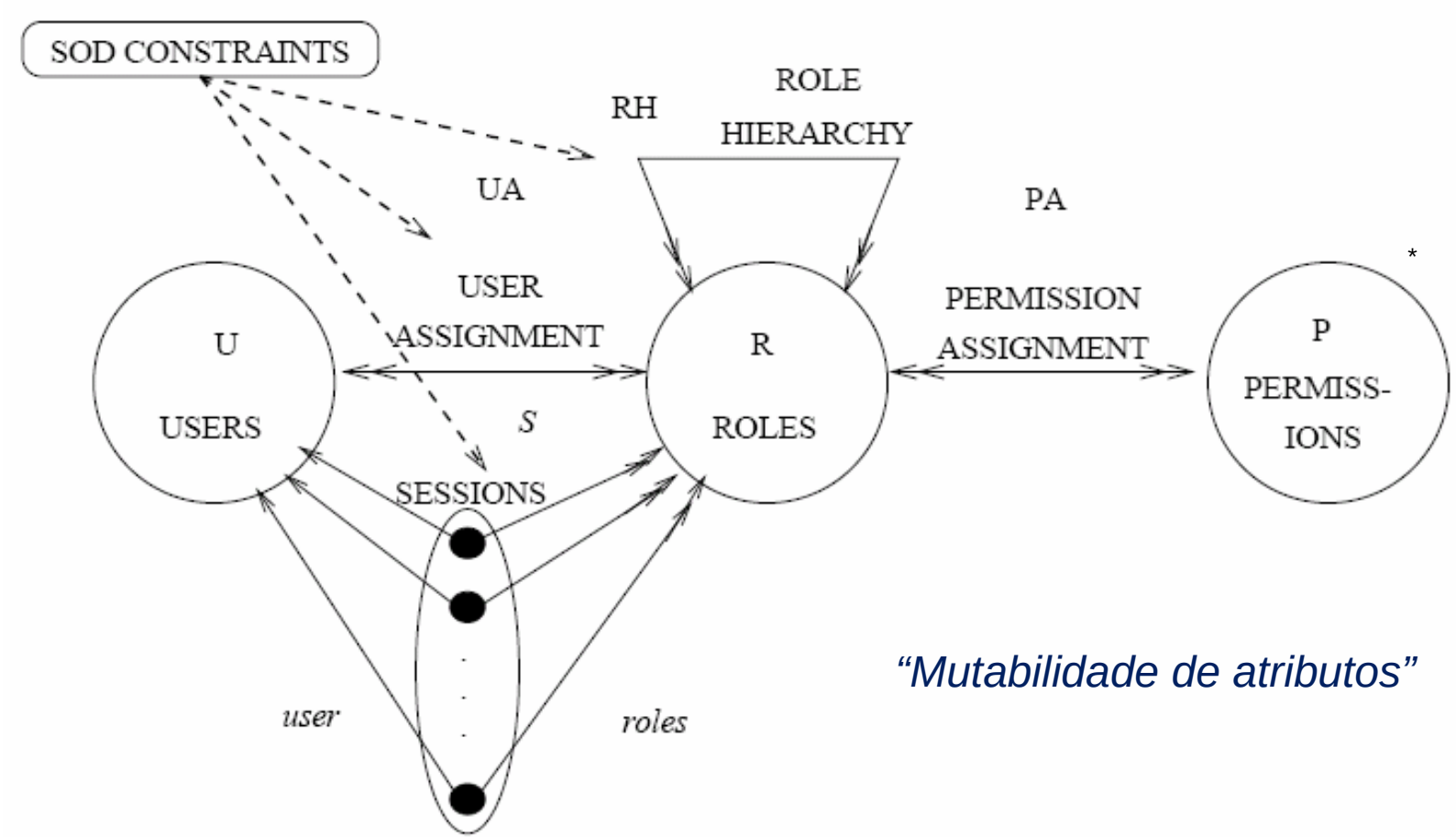
- *Separation of Duty (SoD)* - estática



*Sandhu, R., Ferraiolo, D., Kuhn, R. The NIST Model for Role-Based Access Control: Towards A Unified Standard, ACM WRBAC. 2000.

Restrições do modelo de Consenso

- *Separation of Duty (SoD)* - dinâmica



"Mutabilidade de atributos"

*Sandhu, R., Ferraiolo, D., Kuhn, R. The NIST Model for Role-Based Access Control: Towards A Unified Standard, ACM WRBAC. 2000.

Modelo de restrições do $UCON_{ABC}$

- UCON é um modelo de **Controle de uso**
- Restrições de:
  - **A**utorização, *o**B**ligation* (obrigações), **C**ondições:
    - Pré (*pre*),
    - Durante (*on* - *ongoing*) e
      - *Mutabilidade de atributos e princípio da continuidade*
    - Pós (*post*)

Motivação

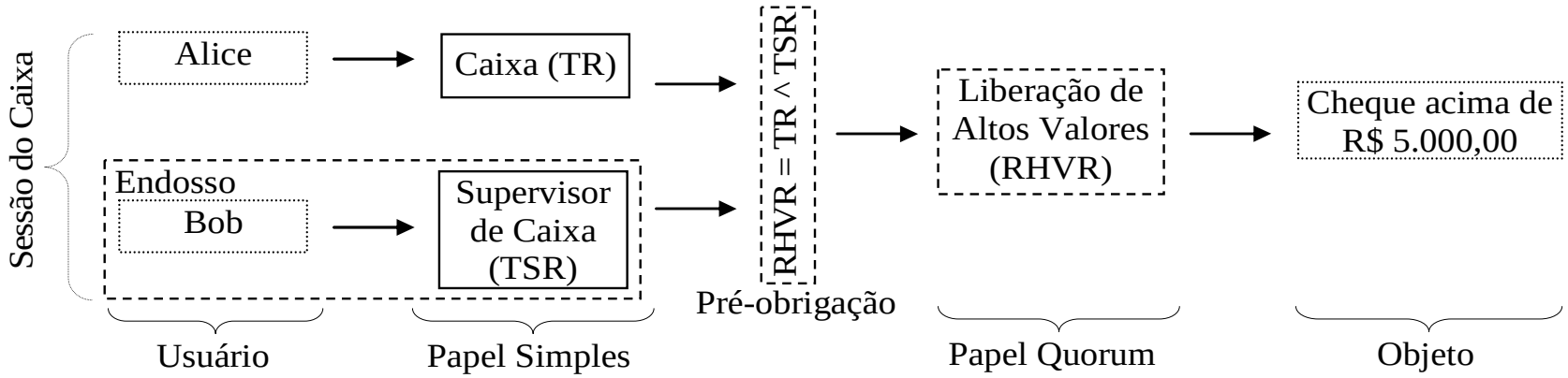
- Há atividades que:
  - não podem ser separadas e executadas em seqüência
  - não podem ser executadas por um único papel/principal ou necessitam de endosso
- Exemplo: abertura de porta de um cofre de banco (exigência da presença do tesoureiro e do contador, um de cada lado da porta)

Proposta

- 2 tipos de papeis:
  - simples e
  - quorum
- Controle de uso do papel quorum
  - *Pre-oBligation* ⇨ define os papeis simples necessários para a ativação do papel quorum
- Mutabilidade de atributo e princípio da continuidade
  - *On-oBligation* ⇨ define as condições para manutenção do papel quorum ativo. Exemplo: papeis simples adicionais, expiração do tempo de uso, revalidação de credenciais

Proposta

- Na sessão:
  - Usuário deve ter papel quorum associado a si
  - Um conjunto pré-definido de **papéis simples endossam** a ativação de um **papel quorum**
- Exemplo



Cenário

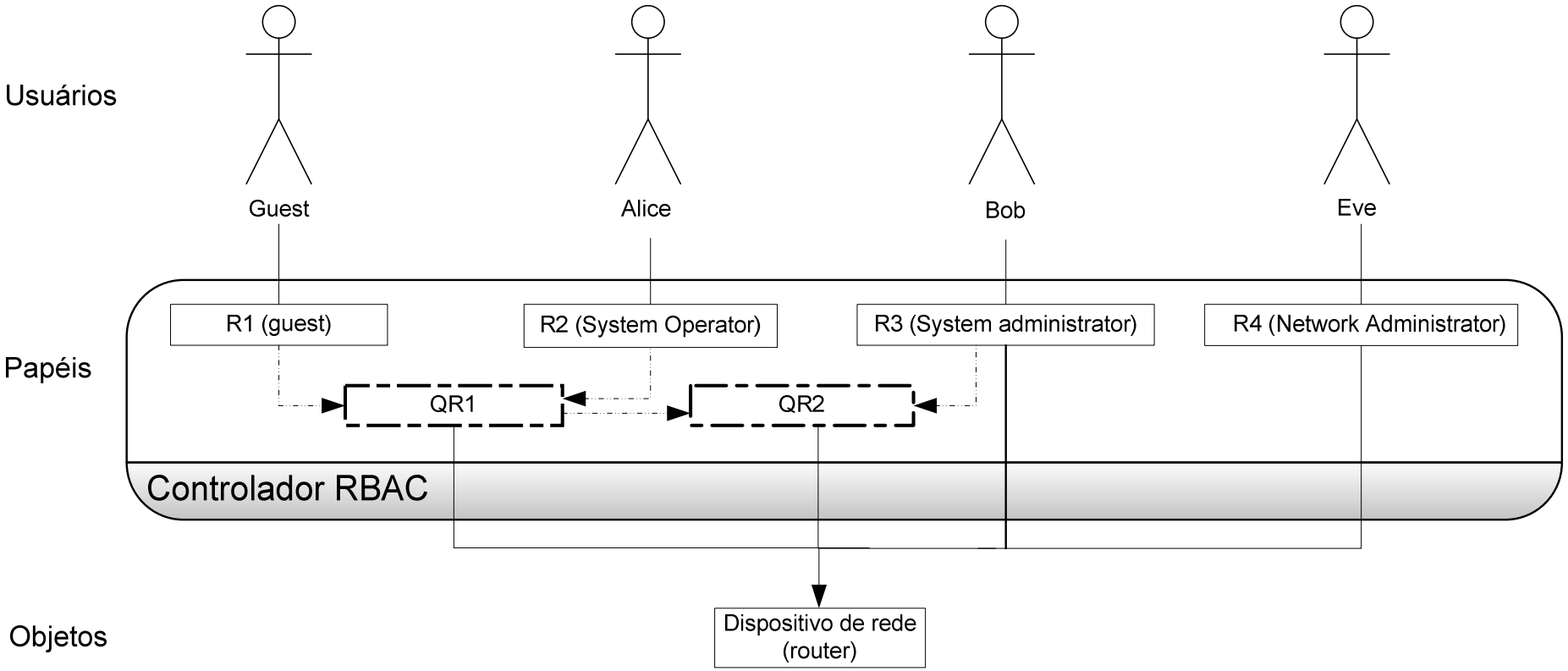
- Assumindo que administrador de rede está ausente e o roteador de acesso a Internet está em estado de falha.
- Considerando que há os seguintes papéis definidos no sistema:

Papel	***Descrição das principais atribuições do papel***
R1	**Guest:** Papel com direitos de acesso muito restritos de uso do sistema
R2	**System Operator:** Papel com direitos restritos de administração do sistema
R3	**System Administrator:** Papel com direitos irrestritos de administração dos recursos do sistema
R4	**Network Administrator:** Papel com direitos irrestritos de administração dos recursos de rede
QR1	**Papel (quorum)** com direitos de **visualização de configurações e efetivação de testes** de equipamentos
QR2	**Papel (quorum)** com **direitos irrestritos de administração** do sistema

Cenário

- Funcionário do fornecedor do equipamento é enviado para resolver o problema do roteador
- A política de segurança da empresa só permite que o usuário guest seja utilizado por terceiros

Cenário


Usuários
Guest
Alice
Bob
Eve
Papéis
R1 (guest)
R2 (System Operator)
R3 (System administrator)
R4 (Network Administrator)
QR1
QR2
Controlador RBAC
Objetos
Dispositivo de rede
(router)

Implementação

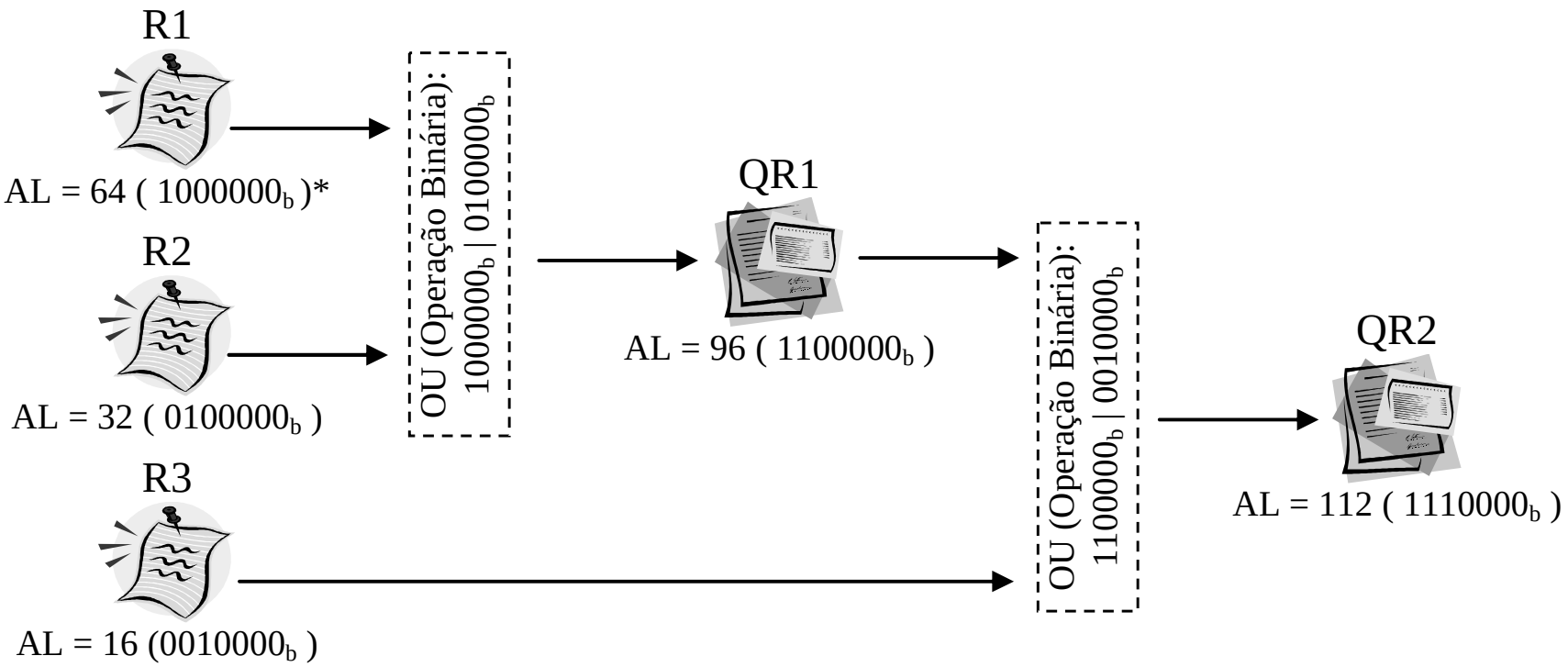
- Baseada no *framework* RBAC/Web do NIST
- Adicionou-se *Access Level* (AL) a cada papel

$$AL = \sum_{x=0}^{(n-1),k=0,1} 0^{k} \cdot 2^{x}$$

;onde *k* pode ser: *k*= 0 (default) ou k = 1 (se o papel simples com AL = 2^x é requerido para o endosso).

- ALs não hierárquicos (sistema escalável)
- Definição inequívoca de políticas
- Detalhes da extensão da API (no artigo)
- Login baseado no esquema usuário/senha

Exemplo de definição deAL



* Y_b representa Y no sistema binário

Conclusão

- Proposta preserva *SoD* (modelo de Consenso)
- Suporte a quorum de papéis não suportado pelo modelo de restrições do RBAC original, pré/on-obrigações so $UCON_{ABC}$
- Não oferece risco de segurança porque quem ativa o papel quorum é o controlador RBAC

Conclusões

- Protótipo mostrou uma prova de conceito
- Quando o acesso não for permitido usuário fica sabendo de que direitos precisa, e não apenas recebe um *deny* como resposta
- Pretende mudar o esquema usuário/senha para aceitar credenciais

Perguntas

- edemilson@ppgia.pucpr.br
- santin@ppgia.pucpr.br
- jamhour@ppgia.pucpr.br
- maziero@ppgia.pucpr.br
- emir.toktar@etu.upmc.fr