Descentralização e Autonomia para Administração de Políticas de Acesso no MACA: Um Modelo de Autorização Contextual para o Controle de Acesso Baseado em Papéis

Gustavo H. M. B. Motta[1], Sérgio S. Furuie[2]

[1]Departamento de Informática – Universidade Federal da Paraíba (UFPB)

[2] Instituto do Coração – HC FM.USP/Escola Politécnica da USP

gustavo.motta@di.ufpb.br, sergio.furuie@incor.usp.br

Abstract. *Role-based access control (RBAC) is a NIST standard that establishes a generalized solution for the access control problem in information systems (IS). This work presents and discusses how to use MACA (contextual authorization model) to administer access control policies for RBAC in large organizations. MACA supports decentralized and autonomous policies as well centralized ones or a mix of both.*

Resumo. *O controle de acesso baseado em papéis (CABP) é um padrão do NIST que apresenta um enfoque generalizado para o problema do controle de acesso em sistemas de informação (SI). Este trabalho descreve e discute a utilização do MACA (Modelo de Autorização ContextuAl) para administração de políticas de acesso para CABP em grandes organizações. O MACA suporta desde as políticas descentralizadas e autônomas, até as políticas centralizadas, ou um misto das duas.*

1. Introdução

O controle de acesso baseado em papéis (CABP) [Ferraiolo et al. 2001] é um padrão do NIST (*National Institute of Standards and Technology*) que apresenta um enfoque generalizado para o problema do controle de acesso em sistemas de informação (SI). O CABP regula o acesso dos usuários aos objetos protegidos com base nos papéis que eles exercem numa organização. Os papéis denotam funções que descrevem a autoridade e a responsabilidade concedidas aos usuários. As autorizações para acessar objetos não são associadas diretamente a usuários, mas para papéis, de acordo com as atribuições pertinentes. O CABP é uma solução adequada para atender as demandas de controle de acesso existentes em organizações de grande porte, que se destacam por possuírem processos de negócio complexos, operados por numerosos profissionais, com diferentes papéis, abrangendo transversalmente diversos SI.

A administração estritamente centralizada de políticas de acesso para o CABP apresenta problemas. A possibilidade de concentração de poderes num único indivíduo pode acarretar abusos de autoridade, fraudes ou conflitos de interesses. Por outro lado, o número de papéis pode alcançar valores da ordem de centenas ou de milhares e o número de usuários pode variar, desde dezenas de milhares, até centenas de milhares. Isto inviabiliza na prática o gerenciamento dos papéis, dos usuários e de seus relacionamentos por uma equipe centralizada de administradores da política de acesso. É necessário descentralizar a autoridade e a responsabilidade administrativas por múltiplos usuários para viabilizar a gerência e também para evitar a existência do "superusuário".

Este trabalho descreve e discute a utilização do MACA (Modelo de Autorização ContextuAl) [Motta 2003] para administração descentralizada e autônoma de políticas de acesso para CABP. O MACA é um modelo de autorização contextual que estende o modelo de referência para o CABP do NIST. As autorizações contextuais usam regras

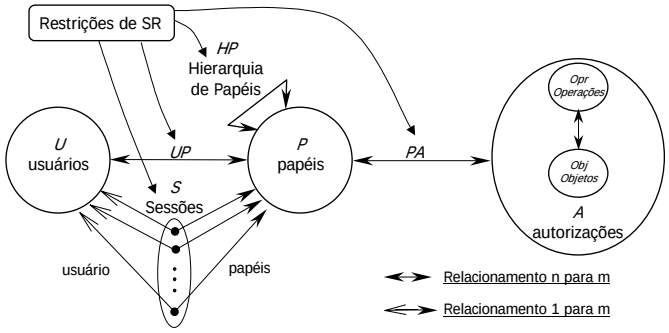

Figura 1. Esquema do modelo de referência para CABP do NIST

baseadas em informações oriundas do ambiente das organizações para decidir se um usuário tem permissão para executar uma determinada operação num objeto. A idéia é usar o próprio modelo de CABP do MACA para definir políticas de acesso às funções administrativas do CABP, como a criação e manutenção de contas de usuários, de papéis e seus relacionamentos. A implementação do MACA está disponível como software livre (licença GNU GPL) em http://maca.sourceforge.net/.

O restante do trabalho está organizado da seguinte forma. A seção 2 introduz o modelo para CABP do NIST, com destaque para suas funções administrativas. A seção 3 analisa aspectos da autonomia e da descentralização da administração de políticas de acesso para o CABP nas organizações. A seção 4 mostra a implementação de tais políticas usando o MACA. A seção 5 discute as contribuições do MACA para administração de políticas de acesso para o CABP e sua relação com trabalhos afins. Por fim, a seção 6 traz a conclusão do trabalho.

2. O CABP do NIST e as Funções Administrativas

O padrão NIST para CABP (Figura 1) possui quatro conjuntos de entidades principais: *U* (usuários), *P* (papéis), *A* (autorizações) e *S* (sessões). Especifica que uma autorização é um relacionamento *n* para *m* entre os recursos protegidos (objetos) e respectivas formas de acesso (operações). Estas entidades possuem os seguintes relacionamentos: usuário-papel *UP*; papel-autorização *PA*; hierarquia de papéis *HP* e sessões. As relações *UP* e *PA* especificam associações *n* para *m* entre usuários e papéis; e entre papéis e autorizações, respectivamente. *HP* define hierarquias de papéis para representar as linhas de autoridade e responsabilidade de uma organização. Uma sessão se relaciona com um único usuário por vez, mas permite que ele assuma (ative) múltiplos papéis simultaneamente.

Aos relacionamentos do padrão, podem-se estabelecer restrições de separação de responsabilidades (SR) para minimizar as chances de fraude ou dano acidental pela demasiada concentração de poder numa única pessoa. A SR distribui para vários usuários a responsabilidade e a autoridade para realizar uma tarefa suscetível de fraudes ou mau uso, de modo que um indivíduo não seja poderoso o suficiente para efetuá-la sem um conluio [Ferraiolo et al. 2001]. A SR é definida através de papéis mutuamente exclusivos, tanto na relação *UP*, quanto na relação *PA*. Em *UP*, dois ou mais papéis mutuamente exclusivos não podem ter usuários em comum associados. Já em *PA*, define-se a separação de responsabilidades proibindo-se a associação de uma mesma autorização a papéis mutuamente exclusivos.

O padrão para CABP especifica funções administrativas para a criação e a manutenção (ler, alterar, excluir) das entidades (*e. g.*, usuários, papéis, autorizações, obje-

tos e operações) e dos respectivos relacionamentos (*e. g.*, usuário-papel e papel-autorização) existentes em implementações do CABP. A Figura 3 (b) ilustra as funcionalidades administrativas básicas do CABP, onde uma variedade de políticas de acesso pode ser configurada. O objeto *CABP FA* representa uma ferramenta administrativa para o CABP que permite criar, ler, alterar ou excluir contas de usuários, papéis, autorizações, objetos e operações, bem como vincular (desvincular) usuários e autorizações para (de) papéis nas relações usuário-papel e papel-autorização, respectivamente. A operação *criarNovaSenha* atribui sigilosamente uma nova senha para um usuário.

3. Descentralização e Autonomia na Administração de Políticas de Acesso

Os poderes disponíveis nas funções administrativas do *CABP FA* (Figura 3 (b)) podem acarretar abusos, fraudes ou conflitos de interesses quando concentrados num único indivíduo. É necessário descentralizar a autoridade e a responsabilidade administrativas por múltiplas pessoas para evitar a existência de "superusuários". Ademais, o considerável número de usuários e papéis nas grandes organizações demandam mais autonomia para os administradores, a fim de viabilizar a gerência da política de acesso. Porém, a distribuição do poder para um grande número de administradores não pode se ocorrer às custas de uma autonomia ilimitada. O desafio é descentralizar os detalhes operacionais da administração do CABP, mas sem perder o controle unificado das políticas administrativas. Segundo [Sandhu et al. 1999], existe uma tensão entre o desejo de escalabilidade obtido com a descentralização e a manutenção de um controle firme das políticas.

Uma organização poderia optar por centralizar a execução das funções administrativas para criação e manutenção de papéis, de objetos e operações, e de autorizações, assim como a vinculação (desvinculação) de autorizações para (de) papéis. Porém, as unidades constitutivas da organização (*e. g.*, Figura 2) teriam a autonomia para criar e manter seus próprios usuários, podendo vinculá-los (desvinculá-los) aos (dos) papéis existentes. Por exemplo, os administradores do Serviço de Hemodinâmica só teriam permissão para gerenciar as contas dos usuários associados ao serviço, não podendo manipular contas de usuários de outras unidades. Por sua vez, um administrador de divisão teria autonomia para gerenciar contas de usuários associados diretamente à divisão, assim como, dos usuários associados aos serviços a ela subordinados. Do mesmo modo, um administrador de instituto poderia gerenciar as contas de qualquer usuário subordinado ao instituto. Já um administrador da organização (Hospital de Clínicas) poderia gerenciar as contas de qualquer usuário da organização. Tal política estabeleceria uma hierarquia de acesso, cuja abrangência é limitada pela estrutura organizacional.

A descentralização e a autonomia administrativas também podem ser estendidas para o gerenciamento das autorizações (autorizações, objetos, operações e respectivos relacionamentos), tomando por base a estrutura organizacional, como no exemplo anterior. Entretanto, como em geral os sistemas (objetos e operações) da organização (*e. g.*, os componentes do Prontuário Eletrônico do Paciente) permeiam todas as unidades organizacionais, o mais razoável é distribuir o poder de gerência das autorizações para os responsáveis (proprietários) pelos sistemas. De modo similar, a criação e a manutenção de papéis pode ser desconcentrada e autônoma, mas limitada pela estrutura hierárquica da organização. Por exemplo, um administrador de papéis do Serviço de Hemodinâmica poderia criar ou manter papéis, desde que fossem descendentes do papel *Hemodinamicista*.

Em suma, as organizações podem requerer desde políticas administrativas amplamente descentralizadas e autônomas, até políticas totalmente centralizadas. Porém, em geral, demandam políticas mistas, limitadas, descentralizando e dando autonomia

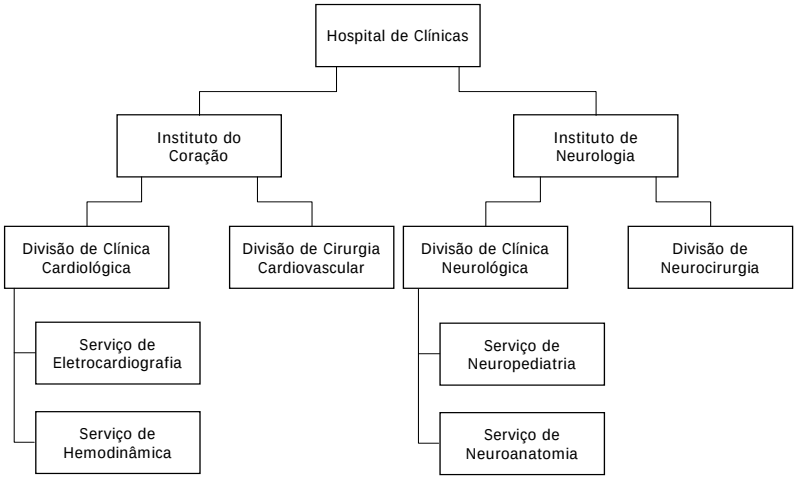

Figura 2. Organograma parcial da estrutura hierárquica de um hospital.

para executar parte das funções administrativas, mas mantendo concentrados os poderes para execução de outras funções.

4. Administração de uma Política de Acesso para o CABP Usando o MACA

A execução de políticas administrativas descentralizadas e autônomas, com grande número de usuários, papéis e administradores, justifica a utilização do CABP do MACA para controlar o acesso às funções administrativas do CABP. O objetivo é utilizar papéis administrativos para controlar e distribuir a autoridade e a responsabilidade na realização das funções administrativas do CABP numa organização.

A Figura 3 exemplifica a utilização do MACA para definir uma política administrativa para o CABP num hospital, cujo organograma é o ilustrado na Figura 2. Os papéis administrativos (Figura 3 (a)) para os usuários do *CABP FA* estão divididos em três categorias principais: *Administrador de Usuário*, *Administrador de Papel* e *Administrador de Autorização*. A política administrativa do hospital determina a centralização da administração de papéis e de autorizações nos papéis *Administrador de Papel* e *Administrador de Autorização*, respectivamente. Os administradores de papéis podem gerenciar papéis sem restrições, conforme estabelecem respectivas autorizações positivas (+) na Figura 3 (c). Já um administrador de autorizações pode gerenciar autorizações, objetos e operações, e vincular (desvincular) autorizações a (de) papéis (v. autorizações associadas na Figura 3 (c)). A administração de papéis e de autorizações, portanto, não depende da estrutura organizacional do hospital.

Porém, a política administrativa determina a distribuição do poder de gerenciar as contas de usuários por diferentes papéis e a sua descentralização de acordo com as unidades organizacionais do hospital. As políticas configuradas para cada um dos papéis na Figura 3 (c) são descritas a seguir:

- **Administrador de Usuário**: pode ler a conta e ver os papéis de qualquer usuário do hospital, independente de unidade organizacional onde está lotado;
- **Administrador de Help Desk**: único papel com o poder de definir uma nova senha para usuários do hospital;
- **Administrador de Contas**: pode alterar ou excluir contas de usuários, desde que os usuários sejam lotados numa unidade organizacional igual ou subordinada a unidade organizacional onde o administrador está lotado. Porém, um administrador de contas está impedido de alterar ou excluir a própria conta (ver regra na Figura 3 (c)). O parâmetro `atributos`, na regra da autorização para alterar, denota a lista

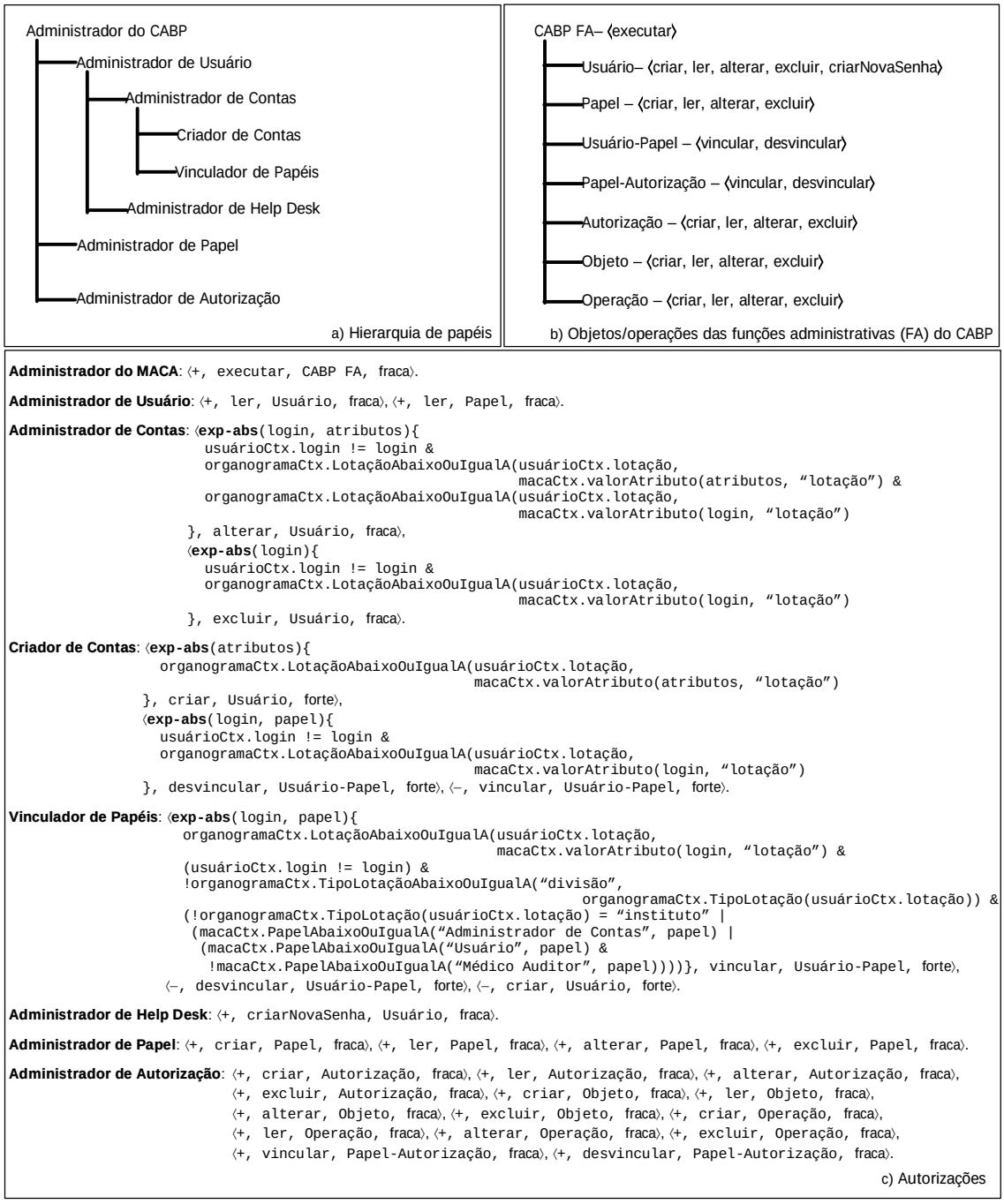

Figura 3. Exemplo da uma política administrativa usando o MACA. (a) hierarquia dos papéis administrativos. (b) Representação das funções administrativas do CABP. (c) Autorizações contextuais associadas a cada papel. As autorizações do tipo forte estabelecem políticas estritas, que não podem ser revogadas, enquanto as autorizações fracas são permissivas e podem ser revogadas.

dos novos valores dos atributos a serem armazenados na conta do usuário. O parâmetro `login` traz a identificação única da conta a ser alterada ou excluída. A função `LotaçãoAbaixoOuIgualA`, do contexto `organogramaCtx`, retorna `true` se a unidade organizacional passada como seu segundo argumento for igual ou subordinada à unidade organizacional passada como primeiro argumento. A variável `lotação`, do contexto `usuárioCtx`, retorna a identificação da unidade organizacional onde o administrador de contas é lotado. A função contextual `ValorAtributo`, do contexto

`macaCtx`, recupera o valor de um atributo específico (segundo argumento – "`lotação`") da lista de valores de atributos passada como primeiro argumento. Quando o login do usuário é passado como primeiro argumento, então a função `ValorAtributo` retorna o valor do atributo especificado que está armazenado na conta do usuário. Note-se, portanto, na regra da primeira autorização, que a alteração só é permitida se a lotação existente na conta do usuário e a nova lotação são iguais ou subordinadas a lotação do administrador. Isto é, um administrador de contas do Instituto do Coração pode transferir a lotação de um usuário do Serviço de Hemodinâmica para a Divisão de Cirurgia Cardiovascular, mas não para o Serviço de Neuropediatria, por exemplo;

- **Criador de Contas**: pode criar a conta de um usuário ou desvincular seus papéis, desde que o usuário seja lotado numa unidade organizacional igual ou subordinada a unidade organizacional onde o administrador está lotado. Entretanto, está impedido de desvincular os próprios papéis. A última autorização (negativa) proíbe que ele vincule papéis para usuários, ou seja, ele não pode conceder poderes;
- **Vinculador de Papéis**: pode vincular papéis para um usuário, desde que o usuário seja lotado numa unidade organizacional igual ou subordinada a unidade organizacional onde o administrador está lotado e a conjunção das seguintes condições seja satisfeita: 1) ele não pode atribuir papéis para si mesmo; 2) a unidade organizacional de lotação do administrador não pode ter um tipo igual ou subordinando ao tipo *divisão*; 3) se a unidade organizacional (lotação) do administrador for do tipo *instituto*, então o papel a ser atribuído deve ser igual ou descendente do papel *Administrador de Contas* ou deve ser igual ou descendente do papel *Usuário*, excluindo-se o papel *Médico Auditor* e seus descendentes (não mostrados). O parâmetro `papel` na regra da primeira autorização denota o identificador do papel a ser vinculado ao usuário identificado por `login`. A função `TipoLotaçãoAbaixoOuIgualA`, do contexto `organogramaCtx`, retorna `true` se o tipo de unidade organizacional passado como seu segundo argumento for igual ou subordinado ao tipo passado como primeiro argumento. A função `TipoLotação`, do contexto `organogramaCtx`, retorna o tipo da unidade organizacional passada como parâmetro. A função `PapelAbaixoOuIgualA`, do contexto `macaCtx`, retorna `true` se o papel passado como seu segundo argumento for igual ou descendente do papel passado como primeiro argumento.

A política especificada na Figura 3 (c) descentraliza a gerência de contas de usuários porque permite que administradores setoriais (nos serviços ou divisões) realizem as funções administrativas operacionais nas contas de seus próprios usuários, porém de maneira limitada. Por exemplo, um criador de contas do Serviço de Hemodinâmica, pode criar, alterar ou excluir a conta de um usuário do serviço. Porém, uma função de maior responsabilidade, que atribui poderes mediante a vinculação de papéis, só é permitida para um vinculador de papéis do Instituto do Coração. Acresça-se que o vinculador de papéis pode conceder o poder de gerenciar contas para outros usuários do instituto pela atribuição de papéis descendentes (ou iguais) ao papel *Administrador de Contas*. No entanto, está proibido de atribuir os papéis *Administrador de Help Desk* ou *Médico Auditor*. Apenas vinculadores de papéis lotados diretamente no Hospital de Clínicas podem fazê-lo, e para qualquer usuário da organização.

Independente da descentralização baseada numa estrutura organizacional, a política da Figura 3 (c) distribui o poder de gerenciar contas por diferentes papéis, com destaque à separação de responsabilidades existente entre os papéis *Criador de Contas* e *Vinculador de Papéis*. A SR do MACA estabelece o seguinte: 1) quem cria contas e desvincula papéis de usuários (*Criador de Contas*) está terminante e incondicionalmen-

te proibido de vincular papéis (autorização forte e negativa irrevogável), isto é, não pode conceder poderes; 2) quem pode vincular papéis (*Vinculador de Papéis*) está terminante e incondicionalmente proibido de criar contas e de desvincular papéis de usuários (autorizações fortes e negativas irrevogáveis). A intenção é impedir que um mesmo indivíduo concentre os poderes para criar contas de usuários e para vincular e desvincular papéis. Conseqüentemente, evita-se que um administrador malicioso possa, de forma isolada, criar fraudulentamente a conta de um usuário "fantasma" para conceder-lhe poderes com a vinculação de papéis. Mesmo existindo um administrador vinculado aos papéis *Criador de Contas* e *Vinculador de Papéis*, o MACA assegura que ele não poderá criar contas, vincular e desvincular papéis, evitando-se assim que ele cometa fraudes dessa forma.

Observa-se, na política ilustrada, que o poder do administrador depende do papel que ele exerce e da unidade organizacional onde ele está lotado: quanto mais específico o papel na hierarquia (*e. g.*, *Criador de Contas* e *Vinculador de Papéis*) e mais abrangente a unidade organizacional (*e. g.*, Hospital de Clínicas), maior será o poder. É importante notar que o uso das autorizações contextuais do MACA permitiu separar a abrangência da autoridade administrativa das unidades organizacionais sobre os usuários, dos papéis a que esses estão vinculados. Não se precisou criar, por exemplo, os papéis "Criador de Contas de Serviço" ou "Criador de Contas de Instituto", tampouco o papel "Criador de Contas do Instituto do Coração". Ou seja, a hierarquia de papéis e a estrutura organizacional são ortogonais: a modificação de um não implica na alteração do outro e vice-versa.

5. Discussão

O que o MACA traz de inovador é a capacidade de executar diversas políticas administrativas para o CABP com a criação de contextos e a configuração de regras de autorização apropriadas. Ou seja, as possíveis políticas administrativas com o MACA não estão definidas *a priori*, tampouco estão embutidas no próprio modelo. Com isso, as características mais relevantes dos principais modelos administrativos recentemente propostos para o CABP podem ser suportadas.

É o caso dos modelos administrativos para o CABP baseados em hierarquias organizacionais propostos por [Kern et al. 2003; Oh & Sandhu 2002; Perwaiz & Sommerville 2001]. Eles se caracterizam por separar a autoridade administrativa –das unidades de uma estrutura organizacional– dos papéis aos quais usuários ou objetos estão associados. A independência entre a estrutura organizacional e a hierarquia de papéis resolveu um dos maiores problemas encontrados no modelo seminal para administração do CABP, o ARBAC97 [Sandhu et al. 1999], que é o forte acoplamento entre a autoridade administrativa e as associações de usuários e objetos (via autorizações) com papéis [Kern et al. 2003; Oh & Sandhu, 2002]. A existência do contexto `organogramaCtx` com as funções de escopo (*e. g.*, `LotaçãoAbaixoOuIgualA`) e a definição das regras de autorização permitiram ao MACA distribuir privilégios administrativos de acordo com a pertinência de um usuário a uma unidade de uma estrutura hierárquica, mas com independência da hierarquia de papéis. Outros contextos e regras habilitariam o MACA a utilizar estruturas organizacionais distintas para determinar a autoridade administrativa sobre usuários e objetos. Por exemplo, os membros do projeto de uma organização, possivelmente pertencente a papéis e a unidades organizacionais distintas, poderiam ter privilégios administrativos apenas sobre as autorizações associadas aos objetos desenvolvidos pelo projeto. Já a abrangência da autoridade sobre usuários e seus

volvidos pelo projeto. Já a abrangência da autoridade sobre usuários e seus relacionamentos seria determinada pelo organograma organizacional.

O MACA também pode ser configurado para suportar a gerência da hierarquia de papéis com base em *escopos administrativos*, um conceito introduzido por [Crampton & Loizou 2002]. Um escopo administrativo define um subconjunto de papéis hierarquicamente relacionados sobre os quais um papel administrativo tem autoridade. Por exemplo, poderia-se especificar que um papel administrativo somente gerenciaria os papéis que fossem exclusivamente descendentes de um outro papel. Os escopos administrativos podem ser definidos no MACA com regras utilizando as funções de escopo sobre papéis (*e. g.*, `PapelAbaixoOuIgualA`, `PapelAcimaOuIgualA`), além de outras definições disponíveis no contexto `macaCtx`.

6. Conclusão

Este trabalho descreveu e discutiu a utilização do MACA para administrar políticas de acesso no CABP, solução amplamente aceita para controle de acesso a SI em grandes organizações. O MACA pode ser configurado para combinar diferentes políticas administrativas a fim de atender demandas comuns às organizações, bem como suas idiossincrasias. Suporta desde as políticas descentralizadas e autônomas, até as políticas centralizadas, ou um misto das duas. Ademais, a separação entre a abrangência da autoridade administrativa das unidades organizacionais sobre os usuários, dos papéis a que esses estão vinculados, permitida pelo MACA, confere mais flexibilidade para definição e evolução de políticas administrativas porque uma mesma hierarquia de papéis (administrativos) pode ser utilizada em instituições com diferentes estruturas organizacionais.

Referências

Crampton, J. and Loizou, G. (2002) “Administrative scope and role hierarchy operations”. In: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, p. 145-154.

Ferraiolo, D. F.; Sandhu, R.; Gavrila, S.; Kuhn, D. R. and Chandramouli, R. (2001) “Proposed NIST standard for role-based access control.” ACM Transactions on Information and System Security, v. 4, n. 3, p. 224-274.

Kern, A.; Schaad, A. and Moffett, J. (2003) “An administration concept for the enterprise role-based access control model”. In: Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies, p. 3-11.

Motta, G. H. M. B. (2003) Um modelo de autorização contextual para o controle de acesso ao prontuário eletrônico do paciente em ambientes abertos e distribuídos. Tese (Doutorado) – Escola Politécnica, Universidade de São Paulo, São Paulo, 212 p.

Oh, S. and Sandhu, R. (2002) “A model for role administration using organization structure”. In: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, p. 155-168.

Perwaiz, N. and Sommerville, I. (2001) “Structured management of role-permission relationships”. In: Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, p. 163-169.

Sandhu, R. S.; Bhamidipati, V. and Munawer, Q. (1999) “The ARBAC97 model for role-based administration of roles”. ACM Transactions on Information and System Security, v. 2, p. 105-135.