Revista Brasileira de Engenharia Biomédica,
v. 17, n. 3, p. 141-150, set/dez 2001

ISSN 1517-3151

Artigo Original
recebido: 18/09/2001 e aceito em 03/12/2001

Um modelo de autorização e controle de acesso para o prontuário eletrônico de pacientes em ambientes abertos e distribuídos

An authorization and access control model for electronic patient record in open distributed environments

Gustavo H. M. B. Motta
Instituto do Coração
Hospital das Clínicas da Faculdade
de Medicina da Universidade de São Paulo
Escola Politécnica da Universidade de São Paulo
Departamento de Informática
Universidade Federal da Paraíba
Rua Alves Guimarães, 866 / aptº 22
05410-001 São Paulo - SP
Fones: [011] 3069 5545 / 3081 2645
e-mail: gustavo.motta@incor.usp.br

Sérgio S. Furuie
Instituto do Coração
Hospital das Clínicas da Faculdade
de Medicina da Universidade de São Paulo

Resumo
Conceber modelos para autorização e controle de acesso para prontuário eletrônico do paciente (PEP) é indispensável para viabilizar o uso em larga escala do PEP em grandes instituições de saúde. Este trabalho propõe um modelo de autorização adequado às exigências de controle de acesso ao PEP, buscando assegurar a privacidade do paciente e a segurança de acesso aos seus dados, mas flexível o suficiente para tratar casos de exceção com base em informações contextuais. O modelo permite regular o acesso dos usuário ao PEP com base nas funções (papéis) que estes exercem numa organização, estendendo e refinando o modelo de referência para controle de acesso baseado em papéis do tipo simétrico definido pelo NIST (*National Institute of Standards and Technology*). Suporta hierarquia de papéis com herança de autorizações; controle de acesso seletivo aos recursos do PEP; autorizações positivas e negativas; exceções estáticas e dinâmicas baseadas em contextos; separação de responsabilidades estática e dinâmica baseadas em conflitos fortes e fracos entre papéis. Uma arquitetura é proposta para implementar este modelo usando o serviço de diretório LDAP (*Lightweight Directory Access Protocol*), a linguagem de programação Java, e os padrões CORBA/OMG *CORBA Security Service* e *Resource Access Decision Facility*. Com estes padrões abertos e distribuídos, os componentes heterogêneos do PEP podem solicitar serviços de autorização de acesso de modo unificado e consistente a partir de múltiplas plataformas. O PEP na WEB do InCor foi selecionado como aplicação piloto para emprego deste modelo e hoje cerca de 780 usuários o acessa com diferentes privilégios, dependendo dos papéis associados a cada um deles. Desenvolvimentos futuros incluem a especificação de modelos contextuais para criação de autorizações dinâmicas para o PEP e a utilização de mecanismos mais robustos de autenticação do usuário.
Palavras-chave: Arquitetura aberta e distribuída, Autorização e controle de acesso, Prontuário eletrônico do paciente

Abstract
Designing proper models for authorization and access control for the electronic patient record (EPR) is essential to a wide scale use of the EPR in large health organizations. This work presents a suitable authorization model for the access control requirements of the EPR, capable to assure patient privacy and access security to his/her data, but flexible enough to grant access in exceptional cases. This model regulates users' access to EPR based on their

roles in an organization, extending and reifying the NIST (National Institute of Standards and Technology) symmetric reference model for role-based access control. It supports role-tree hierarchy with authorization inheritance; selective EPR resources access controls; positive and negative authorizations; static and dynamic contextual exceptions; static and dynamic separation of duty, based on weak and strong role conflicts. The access control aim is to limit the users activities according to the authorization model proposed. An architecture is proposed to implement this model using Lightweight Directory Access Protocol, Java programming language and the CORBA/OMG standards CORBA Security Service and Resource Access Decision Facility. With those open and distributed standards the heterogeneous EPR components can request access authorization services in a unified and consistent fashion across multiple platforms. The InCor's web EPR was selected as the pilot application to employ this model and today about 780 users have access to EPR via web with distinct privileges, which depends of their associated roles. Further developments include the specification of contextual models to create dynamic authorizations for the EPR and the use of a more robust user authentication mechanism.

***Keywords**: Access control and authorization, Electronic patient record, Open distributed architectures*

Extended Abstract

Introduction

Designing proper models for authorization and access control for the electronic patient record (EPR) is essential to a wide scale use of the EPR in large health organizations (Kaihara, 1998). This work presents a suitable authorization model for the access control requirements of the EPR, capable to assure patient privacy and access security to his/her data, but flexible enough to grant access in exceptional cases. An architecture was proposed to implement this model based on open and distributed standards, so that the heterogeneous EPR components can request access decision services in a unified and consistent fashion across multiple platforms and programming languages.

Authorization and Access Control Model: The proposed model regulates users' access to EPR based on their roles in an organization. This model extends and reifies the NIST (National Institute of Standards and Technology) symmetric reference model (Figure 1) for role-based access control (RBAC) (Sandhu et al., 2000). Each user has a set of related roles and each role is associated with a set of EPR resources authorization. Users are given permission to adopt roles during his/her sessions. It supports role-tree hierarchy with authorization inheritance; selective EPR resources access control; positive and negative authorizations; static and dynamic exceptions based on contexts, like patient/user relationship; static and dynamic separation of duty, based on weak and strong role conflicts. The access control aim is to limit the users activities according to the authorization model proposed. During authentication or immediately afterwards, the user activates an initial allowed role. Subsequent roles are activated automatically (based on user's needs and related EPR resource permissions) provided that those will not have strong conflicts with any user's roles already active. The access control algorithm has three main steps – strong authorization checking, dynamic authorization checking and weak authorization checking – that are specified in details by (Motta and Furuie, 2001).

Implementation Architecture

The proposed architecture is based on open and distributed standards, and it is established upon a three-tier client/server model (Figure 3). The first one is a data server, which holds a security management information base (SMIB). The SMIB stores security ERP profiles, such as access authorizations, roles, resources and users representations, authentication data, user-role and role-authorization relationships, among others. Those informations are stored using a directory service based on Lightweight Directory Access Protocol (LDAP) (Yeong et al., 1995), an open standard defined by IETF (Internet Engineering Task Force). The second one is a security server, which offers authentication and access control to client applications, amongst other security services, like auditing and non-repudiation. To overcome the EPR components heterogeneity and distribution, the CORBA Security Service (CSS) (OMG, 1998) and the CORBA resource access decision facility (RAD Facility) (OMG, 2000) was adopted. The user authentication uses a standard CSS interface and the access decision uses the RAD Facility standard interfaces. A Java language implementation of user authentication via login name and password and the implementation of the authorization and access control model proposed on this work were carried out. The third-tier is the client applications that interact with the CSS and RAD facility to get user authentication and access authorizations, respectively.

Discussion and Conclusion

Our solution aimed to satisfy the access control needs of InCor's EPR, composed of distributed and heterogeneous systems. The implementation of this solution took the following steps: user role definition; registering users and assigning their roles; and choice of a pilot application to employ the proposed model. The InCor's web EPR was selected as the pilot application and today about 780 users have access to EPR via web with distinct privileges, which depends on their associated roles. We are now defining access authorizations for two large legacy applications – "Procedure Record System" and "Medical Prescription System" – used by medical staff.

This work proposed a proper model for access authorization to the EPR aiming to assure patient privacy and security access to his/her data, but flexible enough to consider exceptional cases based on contextual information. An architecture was proposed to implement this model based on open and distributed standards. So, the EPR users can request authorization and access controls services in a platform independent manner, but with a unified access control and authorization policy management. Further developments include the specification of contextual models to create dynamic authorizations for the EPR, as well as more robust authentication in this architecture based on digital certificates and smart cards.

Introdução

Conceber modelos para autorização e controle de acesso adequados para prontuário eletrônico de paciente (PEP) é indispensável para viabilizar o uso em larga escala do PEP em grandes instituições de saúde (Kaihara, 1998). Entretanto, duas questões principais desafiam sua concepção e aplicação.

A primeira é que o controle de acesso ao PEP em nenhuma circunstância prejudique o atendimento ao paciente por negar acesso legítimo às informações e aos serviços requisitados pelo pessoal médico. No entanto, fora deste contexto, as informações do prontuário são sigilosas, exceto quando em atendimento à vontade do paciente ou a determinações legais. O problema é que não existe um modelo claro sobre a política de autorização e controle de acesso a ser adotada para o PEP, isto é, como determinar quem tem direito a acessar certas classes de informações, com quais privilégios e em quais condições. É indesejável impor um controle tão restrito que impeça um médico, em uma sala de emergência, acessar o prontuário de um paciente gravemente doente. Neste caso, a circunstância da emergência é considerada uma exceção, sobrepondo-se a restrições de acesso estabelecidas (NAS, 1997). Um modelo para autorização e controle de acesso ao PEP deve ser flexível o suficiente para suportar casos excepcionais, estabelecidos estática ou dinamicamente, levando em conta informações contextuais ou circunstanciais (Motta *et al.*, 2000).

A segunda questão refere-se a como administrar uma política de autorização e impor o controle de acesso ao PEP, visto que este é composto por segmentos que estão distribuídos em bases de dados distintas, acessadas por aplicações diversas, em plataformas heterogêneas. É necessária a adoção de uma arquitetura aberta e distribuída capaz de suportar a administração da política de autorização e o controle de acesso de modo unificado e consistente, a partir de diferentes sistemas, em plataformas e linguagens de programação distintas, mas de forma padronizada.

Este trabalho apresenta um modelo abrangente de autorização e controle de acesso para o PEP e propõe sua implementação numa arquitetura aberta e distribuída visando a atender às questões postas anteriormente. O modelo refina e estende o padrão de referência para controle de acesso baseado em papéis (CABP) do tipo simétrico (Sandhu *et al.*, 2000) estabelecido pelo NIST (*National Institute of Standards and Technology*) e sua implementação baseia-se numa arquitetura aberta e distribuída, uma necessidade para soluções de segurança em sistemas de informação em saúde segundo (Smith e Eloff, 1999).

Modelo de Autorização e Controle de Acesso

Autorizações estabelecem as permissões[1] de acesso que um sujeito[2] pode exercer em um determinado recurso computacional. O controle de acesso vai limitar as ações que um usuário legítimo de um sistema de computação realiza (Sandhu e Samarati, 1994), com base nas autorizações aplicáveis ao mesmo no momento do acesso. Exige a autenticação prévia do usuário, visando a estabelecer sua identidade para o sistema de segurança, tipicamente através de uma informação pessoal (nome para *login* e senha) ou com cartões de identificação, certificados digitais ou dados biométricos.

O modelo proposto permite regular o acesso dos usuários às informações do PEP com base nos papéis que eles exercem numa organização. Os papéis denotam funções que descrevem a autoridade e a responsabilidade concedidas a um usuário para o qual um papel foi associado (Sandhu *et al.*, 1996). Neste caso, autorizações não são associadas diretamente a usuários, mas sim a papéis, de acordo com as atribuições pertinentes. Por exemplo, aqueles usuários que são médicos têm o papel *Médico* associado e consequentemente são autorizados a executar, nos sistemas componentes do PEP, as ações necessárias ao exercício de suas funções. Já usuários no papel de *Auxiliar de Enfermagem* não têm autorização para exercer as mesmas funções de médico, mas sim aquelas necessárias à sua atividade. Em princípio, este modelo permite o acesso ao PEP de acordo com a necessidade inerente às atribuições de cada papel.

O Padrão NIST para Controle de Acesso Baseado em Papéis

O padrão NIST para CABP do tipo simétrico (Figura 1) possui quatro conjuntos de entidades: *U* (usuários), *P* (papéis), *A* (autorizações) e *S* (sessões). O padrão deixa em aberto a representação de usuários, papéis, autorizações e sessões, e a interpretação de autorizações, cabendo estas tarefas a implementações específicas. Estas entidades possuem os seguintes relacionamentos: usuário-papel *UP*; papel-autorização *PA*; hierarquia de papéis *HP* e sessões. As relações *UP* e *PA* especificam as associações entre usuários e papéis; e entre papéis e autorizações, respectivamente. A capacidade em se

[1] *Os termos direito de acesso, privilégio, permissão e autorização são usados neste texto indistintamente.*
[2] *Um sujeito pode ser um usuário humano ou algum agente autônomo que atua em benefício deste. Também é chamado de principal.*

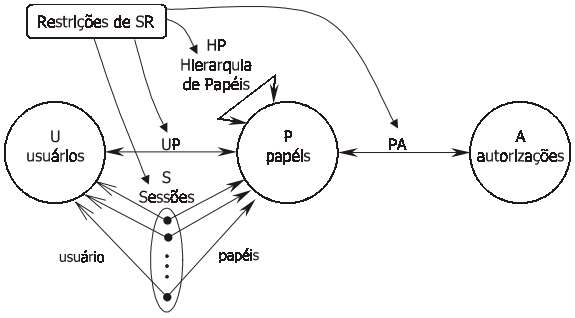

Figura 1. Padrão NIST de referência do CABP simétrico (Sandhu *et al.*, 2000) ***Figure 1.*** NIST standard for RBAC symmetric model (Sandhu *et al.*, 2000)

determinar de forma viável os relacionamentos *UP* e *PA* é que vai caracterizar o CABP simétrico. *HP* define uma relação de ordem parcial entre papéis (Sandhu *et al.*, 1996), dispondo-os em hierarquias a fim de melhor representar as linhas de autoridade e responsabilidade de uma organização. Uma sessão se relaciona com um único usuário por vez, mas requer que este possa assumir (ativar) múltiplos papéis simultaneamente, desde que estes papéis estejam associados a este usuário na relação *UP*. Por outro lado, um usuário pode ter várias sessões ao mesmo tempo.

Aos relacionamentos do padrão podem-se estabelecer restrições para minimizar as chances de fraude ou dano acidental pela demasiada concentração de poder numa única pessoa. Uma restrição típica é limitar o número máximo de papéis associados a um usuário. Outra é a *separação de responsabilidades* (SR), que distribui a responsabilidade e a autoridade para realização de uma ação por múltiplos usuários, de modo que uma única pessoa não seja poderosa o suficiente para efetuá-la sem um conluio. A SR é comumente definida através de papéis mutuamente exclusivos, tanto na relação *UP*, quanto na relação *PA*. Na relação *UP*, dois ou mais papéis que são mutuamente exclusivos não podem ter usuários em comum associados. Já na relação *PA*, a separação de responsabilidades é definida pela proibição de associar uma mesma autorização a papéis que são mutuamente exclusivos. A idéia é adotá-la para minimizar a possibilidade de um usuário assumir papéis onde ocorram conflitos de interesse. Quando a restrição é imposta no momento em que estas relações são estabelecidas, ela é denominada de separação de responsabilidades estática (SRE). A separação de responsabilidades dinâmica (SRD) ocorre quando potenciais conflitos de interesse são detectados no momento em que um usuário tenta ativar mais de um papel simultaneamente, independente das sessões que abriu. A SRD admite que um usuário possua vários papéis que são conflitantes entre si, desde que não sejam ativados simultaneamente.

Autorizações

O modelo proposto neste trabalho refina e estende o padrão NIST visto anteriormente. Aproveita as idéias de autorizações positivas e negativas e o suporte a exceções estáticas através de autorizações fortes e fracas do modelo de autorização de acesso para sistemas de gerenciadores de bancos de dados relacionais definido por (Bertino *et al.*, 1999). Entretanto, de modo distinto deste, baseia a política de autorização de acesso em papéis e não em grupos de usuários. Ademais, propõe a utilização de exceções dinâmicas influenciadas por fatores circunstanciais ou contextuais que acontecem no momento da solicitação da autorização de acesso. Por fim, o tipo de recurso protegido não se restringe a tabelas de banco de dados relacionais, podendo também ser objetos, métodos, programas, dentre outros.

Definição – Uma autorização de acesso é uma tupla <p, r, tp, priv, ta>, onde p é o papel para o qual o privilégio é estabelecido; r especifica o recurso para o qual o privilégio se aplica; tp especifica o tipo de privilégio, positivo (+) quando concedido e negativo (-) quando proibido; priv é o privilégio de acesso estabelecido e ta especifica se o tipo de autorização é forte ou fraca. Este modelo apresenta características que o torna adequado para o controle de acesso ao PEP, conforme descrito a seguir:

Hierarquia de Papéis – A hierarquia de papéis proposta neste modelo de CABP é restrita à estrutura de árvores invertidas, tal como definido por (Sandhu *et al.*, 2000). Este esquema facilita o compartilhamento de autorizações, pois aquelas concedidas para papéis mais genéricos estão naturalmente disponíveis nos papéis mais específicos descendentes destes. A Figura 2a ilustra a hierarquia de papéis parcial definida para o Instituto do Coração (InCor) e a Figura 2c mostra as autorizações atribuídas a cada papel. O papel *Residente* herda todas as autorizações de acesso definidas para os papéis *Médico* e *Usuário*, especificando apenas as suas próprias autorizações. Papéis podem ser vistos, portanto, como agrupamentos de autorizações.

Acesso Seletivo aos Recursos – O prontuário eletrônico de pacientes é segmentado, logo necessita-se especificar diferentes autorizações de acesso para suas diferentes partes. O modelo proposto represen-

ta hierarquicamente os recursos do PEP, conforme ilustrado na Figura 2b. Para cada parte dele, define-se uma ou mais autorizações, permitindo a seletividade do acesso. Cada segmento representa um tipo de recurso específico, com diferentes privilégios de acesso. Por exemplo, a Figura 2b descreve parcialmente a estrutura de páginas na WEB que dá acesso ao PEP no InCor. Os recursos PEP, IP, DM, Exm, Prsc, AP e AL são do tipo página na WEB e os privilégios possíveis de acesso são *consulta* e *autoria*. Os recursos EL e EP são do tipo procedimento, com privilégio de acesso *execução*. Um usuário que assuma o papel de *Médico* tem a autorização para executar estes procedimentos (Figura 2c) e portanto, pode emitir laudos e efetuar prescrições.

Autorizações Positivas e Negativas – Autorizações positivas especificam os acessos que são permitidos, enquanto autorizações negativas estabelecem aqueles que são negados. Quando o acesso é proibido para a maioria dos usuários, usa-se uma autorização negativa. Por exemplo, os acessos ao PEP e a IP são negados nas autorizações do papel *Usuário* (Figura 2c), visto que, usuários comuns não podem consultar o prontuário ou ter acesso à identificação do paciente. Por outro lado, um usuário com o perfil *Médico* tem aquela autorização positiva, uma vez que, em sua maioria, os médicos têm o direito de acessar o prontuário. Esta capacidade facilita a administração da política autorização.

Suporte Controlado a Exceções Estáticas e Dinâmicas – Uma exceção especifica que determinadas autorizações não são válidas em casos particulares (Bertino *et al.*, 1999). Exceções ocorrem estaticamente quando o tipo de privilégio (+ ou –) de uma autorização de um papel é modificado num papel descendente deste. Por exemplo, o papel *Paramédico* tem a autorização <Paramédico, AL, +, consulta, fraca>, entretanto uma exceção é estabelecida para o papel *Auxiliar de Enfermagem* com a autorização <Auxiliar de Enfermagem, AL, -, consulta, fraca>, que modifica o tipo de privilégio e nega o acesso. Outros papéis abaixo de *Paramédico*, que não especifiquem esta exceção, têm acesso aos laudos.

Exceções dinâmicas modificam o tipo de privilégio de uma autorização mediante uma circunstância ou contexto existente no momento em que o usuário exerce um conjunto específico de papéis numa sessão. Para tanto, produz-se dinamicamente uma outra autorização equivalente a esta, mas do tipo fraca e com tipo de privilégio oposto. Por exemplo, os papéis *Médico* e *Paramédico* não têm permissão de acesso à identificação do paciente, pois herdam a autorização <Usuário, IP, -, consulta, fraca> e não estabelecem nenhuma exceção estática. Entretanto, esta autorização negativa pode ser relaxada com a criação de uma autorização dinâmica equivalente positiva, associada aos papéis *Médico* e *Paramédico*, com base em fatores circunstanciais ou contextuais, descritos a seguir:

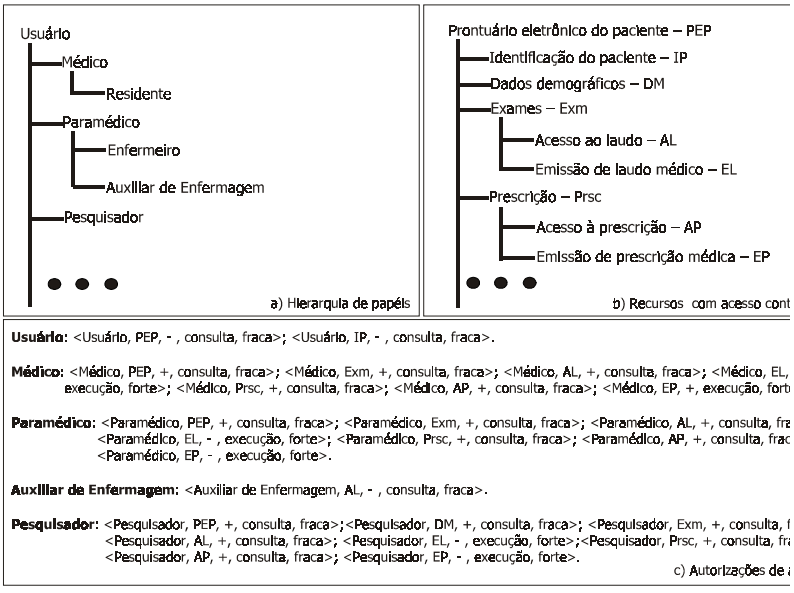

Figura 2. Exemplo de uso do modelo de autorização de acesso ao PEP. ***Figure 2.*** *An example of the access authorization model for the EPR*

- *A localização do usuário*: de acordo com o local onde o usuário acessa uma informação, autorizações positivas ou negativas podem ser relaxadas por meio de uma exceção gerada dinamicamente. Por exemplo, uma autorização dinâmica somente seria gerada, concedendo o acesso, quando este efetuasse-se em estações da sala de emergência ou do ambulatório;
- *Relacionamento usuário/paciente*: certos tipos de relacionamentos entre o usuário e o paciente não podem ser estabelecidos estaticamente, quando da definição dos papéis e seus privilégios. Só são possíveis de se determiná-los dinamicamente, no momento em que uma autorização de acesso é solicitada. Por exemplo, não é possível saber *a priori* os clientes de um plano de saúde, a fim de liberar, para o médico auditor, o acesso apenas aos PEPs dos pacientes deste plano. Por variar com o tempo, este relacionamento deve ser verificado no momento do acesso, para que uma autorização apropriada seja criada dinamicamente;
- *Data e hora do acesso*: o momento do acesso é um fator importante para negar ou conceder uma autorização. Para um médico exercendo o papel de *Residente*, o turno de trabalho determina janelas de tempo em que o acesso à identificação do paciente é permitida, por exemplo.

A fim de controlar o uso de exceções, para cada autorização concedida, + ou -, especifica-se se ela admite exceções ou não. As autorizações *fracas* admitem exceções, ao passo que, as *fortes*, não as admitem. Isto permite que se estabeleçam, desde as políticas mais restritas, até as mais permissivas, com a variação entre os dois extremos controlada pela especificação de autorizações fortes e fracas.

O modelo apresentado permite que exceções dinâmicas sejam criadas, mas não prescreve como serão especificadas e geradas, exceto que sejam fracas. A implementação de exceções dinâmicas dependerá da política de segurança que se pretende adotar e de condições locais impostas pelos sistemas legados que compõem o PEP.

Separação de Responsabilidades – É especificada neste modelo com base nos conflitos existentes entre as autorizações, mas de modo natural e não arbitrário. Isto porque as autorizações positivas e negativas sinalizam conflitos de interesse no acesso a um determinado recurso. Se para um papel, um acesso é autorizado para um recurso e, em outro papel, este mesmo acesso é desautorizado, então certamente haverá conflitos para um usuário exercendo ambos os papéis. Assim, os conflitos são deduzidos automaticamente segundo a autoridade e a responsabilidade estabelecidas para cada papel através das autorizações associadas.

O conflito entre autorizações ocorre estaticamente quando se estabelecem as associações entre autorizações e papéis e dinamicamente quando um usuário ativa, simultaneamente, papéis que possuem autorizações que são conflitantes entre si. As definições de cada tipo de conflito seguem abaixo:

- *Conflito estático*: duas autorizações $<p_1, r_1, tp_1, priv_1, ta_1>$ e $<p_2, r_2, tp_2, priv_2, ta_2>$ conflitam estaticamente se, e somente se, p_1 é ancestral de p_2 ou p_1 é descendente de p_2 ou $p_1 = p_2$ e $r_1 = r_2$ e $tp_1 \neq tp_2$ e $priv_1 = priv_2$ e $ta_1 = ta_2$. Por exemplo, se a autorização <Auxiliar de Enfermagem, EL, +, execução, forte> fosse definida, ela conflitaria com a autorização <Paramédico, EL, -, execução, forte>;
- *Conflito dinâmico*: duas autorizações $<p_1, r_1, tp_1, priv_1, ta_1>$ e $<p_2, r_2, tp_2, priv_2, ta_2>$ conflitam dinamicamente se, e somente se, para $p_1 \neq p_2$, p_1 é ativado simultaneamente com p_2 para um mesmo usuário e $r_1 = r_2$ e $tp_1 \neq tp_2$ e $priv_1 = priv_2$ e $ta_1 = ta_2$. Por exemplo, as autorizações <Médico, EL, +, execução, forte> e <Pesquisador, EL, -, execução, forte>, mesmo não conflitando estaticamente, podem conflitar dinamicamente, caso um mesmo usuário ative simultaneamente os papéis *Pesquisador* e *Médico*.

Quando o tipo de autorização é forte em autorizações conflitantes (dinâmica ou estática), o tipo de conflito é denominado de *conflito forte*. Caso contrário, o conflito é denominado *conflito fraco*. Dois ou mais papéis que possuam autorizações conflitantes entre si são denominados *papéis conflitantes*.

Neste modelo, a separação de responsabilidades estática não admite autorizações que estabeleçam conflitos estáticos fortes entre papéis, pois, numa mesma linha de responsabilidades na hierarquia, não pode haver contradição nas ações permitidas (ou proibidas) de modo absoluto (que não admitem exceções) através de uma autorização forte. Por outro lado, o conflito estático fraco é admitido em papéis distintos e a política de resolução dos conflitos dá-se da seguinte maneira:

1. Uma autorização fraca, negativa ou positiva, especificada num papel, prevalece sobre qualquer autorização fraca conflitante especificada em papéis ascendentes deste. Por exemplo, as autorizações <Auxiliar de Enfermagem, AL, -, consulta, fraca> e <Paramédico, AL, +, consulta, fraca>

conflitam, porém para um usuário assumindo o papel de *Auxiliar de Enfermagem*, a primeira autorização tem primazia sobre a segunda, definida para o papel *Paramédico*;

2. Caso o usuário simultaneamente ative mais de um papel de mesma linha hierárquica, prevalecerão as autorizações do papel mais específico. Por exemplo, na linha <*Usuário*, *Paramédico*, *Auxiliar de Enfermagem*>, a ativação simultânea dos papéis <*Usuário*, *Paramédico*, *Auxiliar de Enfermagem*>, ou <*Usuário*, *Paramédico*>, ou <*Paramédico*, *Auxiliar de Enfermagem*> equivale a ativação do papel *Auxiliar de Enfermagem*.

A separação de responsabilidades dinâmica proíbe a ocorrência de conflitos dinâmicos fortes. Um usuário pode possuir papéis que eventualmente estabeleçam conflitos dinâmicos fortes, porém é proibida a ativação simultânea destes papéis para ele, evitando-se a ocorrência dos conflitos. Por exemplo, é proibido a um usuário a ativação concomitante dos papéis *Médico* e *Pesquisador*, mesmo que ele tenha estes dois papéis associados. Isto porque ambos os papéis estabelecem conflitos dinâmicos fortes. No entanto, o usuário poderá assumir os papéis *Médico* ou *Pesquisador* isoladamente. Já os conflitos dinâmicos fracos são admitidos e política de resolução dá-se da seguinte maneira: havendo duas ou mais autorizações fracas conflitantes dinamicamente, prevalecerá aquela autorização que concede o acesso.

Controle de Acesso

O modelo de controle de acesso visa a possibilitar aos sujeitos o acesso aos recursos computacionais estritamente de acordo com o modelo de autorização especificado anteriormente. O usuário deverá, durante a autenticação, ou logo em seguida, selecionar um papel inicial para ativar, dentre aqueles associados para ele. Deste momento em diante, papéis subseqüentes poderão ser ativados automaticamente com base na necessidade do usuário utilizar um recurso, segundo as condições definidas a seguir:

Condições para Ativação de Papéis – Um usuário possui um conjunto de papéis ativos (P_A), um conjunto de papéis disponíveis (P_D) e o conjunto de papéis associados estaticamente (P_{AE}), obtido da relação *UP* (Figura 1). Antes de iniciar sua primeira sessão, o conjunto P_A é vazio e os conjuntos P_D e P_{AE} são iguais e correspondem aos papéis associados ao usuário. As seguintes assertivas devem prevalecer a qualquer momento (invariante do estado do sistema para um usuário):

· $P_A \cup P_D \subseteq P_{AE}$;

· $P_A \cap P_D = \varnothing$;

· $\forall p_a \in P_A$; $p_d \in P_D$, p_a não tem autorizações que conflitam fortemente com autorizações de p_d.

Após o início da primeira sessão, o conjunto P_A é inicializado com o papel inicial escolhido pelo usuário. A partir deste momento, o conjunto de papéis disponíveis para o usuário ativar (P_D) corresponderá aos papéis presentes em P_{AE}, com exceção daqueles que conflitem fortemente com algum papel ativo presente em P_A. Assim, não há a possibilidade do usuário ativar dois papéis que conflitam fortemente ao mesmo tempo. Estas condições vigoram independente das sessões abertas por usuário.

Por exemplo, um usuário com P_{AE} = {*Médico*, *Pesquisador*}, ativando inicialmente o papel de *Médico*, com P_A = {*Médico*}, não poderá simultaneamente ativar o papel *Pesquisador*, pois como estes dois papéis conflitam fortemente (Figura 2), o conjunto de papéis disponíveis, P_D, será necessariamente vazio, de acordo com as condições estabelecidas anteriormente. Para ativar o papel *Pesquisador*, deve-se desativar o papel *Médico*, de modo que P_A volte a ser vazio e P_D = {*Médico*, *Pesquisador*}. Assim, o usuário poderá assumir um novo papel inicial, no caso, *Pesquisador*.

Para um usuário com P_{AE} = {*Enfermeiro*, *Pesquisador*}, a ativação inicial do papel *Enfermeiro*, com P_A = {*Enfermeiro*}, permitirá ativação concomitante do papel *Pesquisador*, pois este é um papel disponível em P_D, visto que não conflita com nenhum papel ativo. De acordo com o modelo proposto, a ativação de um papel presente no conjunto P_D é automática, baseada na necessidade e na permissão do usuário ativar um determinado recurso. Por exemplo, o papel *Enfermeiro* não autoriza o acesso para o recurso *DM* (Dados Demográficos). Neste caso, uma solicitação de acesso a este recurso será concedida com a ativação automática do papel *Pesquisador*, que tem a autorização <Pesquisador, DM, +, consulta, fraca>. Ao final, o conjunto P_A = {*Enfermeiro*, *Pesquisador*} e o conjunto de papéis disponíveis P_D será vazio.

A ativação automática de papéis visa a facilitar para o usuário final a utilização do PEP. O acesso é concedido naturalmente, de acordo com as funções que exerce na organização. O modelo, porém, não exclui a possibilidade do usuário ativar explicitamente um papel. A conveniência de adotar tal estratégia vai depender da política de controle de acesso especificada.

Algoritmo de Controle de Acesso – Deve satisfazer as condições de ativação de papéis e o modelo de autorização expostos anteriormente. Autorizações

fortes têm prioridade sobre autorizações fracas e são absolutas, não admitindo exceções nem conflitos fortes em papéis ativados. Já as autorizações geradas dinamicamente para papéis ativos ou disponíveis, positivas ou negativas, sobrepõem-se a quaisquer autorizações estáticas fracas equivalentes estabelecidas. Três etapas básicas compõem o algoritmo – a verificação de autorizações fortes, a verificação de autorizações dinâmicas e finalmente a verificação de autorizações fracas – especificado em detalhes em (Motta e Furuie, 2001).

Arquitetura de Implementação

A arquitetura para implementação do modelo de autorização e controle de acesso ao PEP baseia-se num modelo cliente-servidor com três camadas (Figura 3). Compõe-se de um servidor de dados, responsável pelo armazenamento da base de informações de gerência de segurança (BIGS); de um servidor de segurança, com a incumbência de oferecer serviços de segurança, neste caso em particular, os serviços de autenticação de usuário e controle de acesso; e de aplicações clientes no terceiro nível, que solicitam estes serviços através de uma API (*Application Programming Interface*) padronizada. A adoção de padrões abertos foi um importante requisito para escolha das tecnologias de implementação dos componentes da arquitetura, descritos a seguir.

Base de Informações de Gerência de Segurança

A BIGS mantém os perfis de segurança para proteção do PEP, tais como, autorizações de acesso, papéis, representações dos recursos protegidos e dos usuários, dados para autenticação, relacionamentos usuários-papéis, papéis-autorizações, etc. Estas informações são armazenadas em um serviço de diretórios hierarquizado, cujo acesso e esquemas de descrição de dados são padronizados através do protocolo LDAP (Yeong *et al.*, 1995), definido pelo IETF. Por ser hierárquico e flexível, o LDAP é capaz de representar naturalmente as hierarquias de papéis e de recursos do modelo de autorização. Esquemas de dados padronizados preexistentes no LDAP são usados no armazenamento de informações sobre usuários (*login*, nome, senha, *e-mail*, etc.), papéis (nome, descrição, membros, etc.) e recursos (nome, descrição, localização, etc.). Embora conte com atributos predefinidos, o serviço de diretórios LDAP permite a definição de novos atributos, conforme o modelo que se deseja adotar. Como os atributos preexistentes não eram suficientes para representar o modelo de autorização proposto, novos esquemas foram criados com todos os atributos necessários para representá-lo.

Todo acesso à BIGS é realizado através do protocolo LDAP sobre SSL (*Secure Socket Layer*) e as autenticações via sistemas operacionais usam o padrão SASL

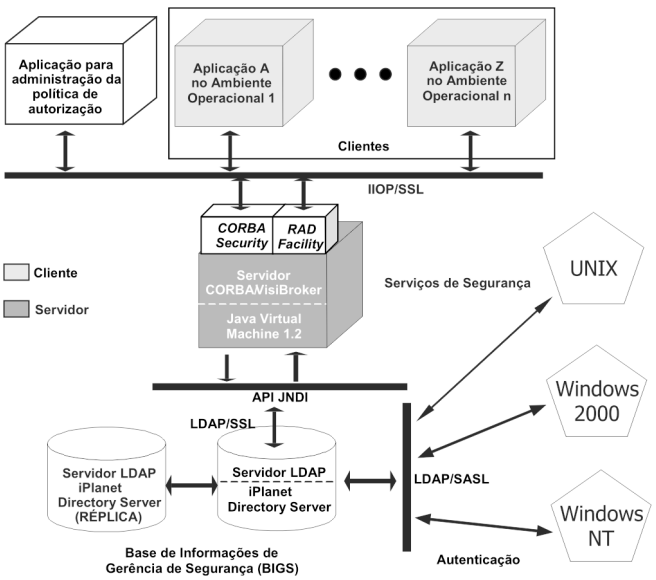

Figura 3. Esquema da arquitetura de implementação. ***Figure 3.*** *Implementation architecture scheme*

(Myers, 1997). Esta solução viabiliza a autenticação unificada de usuários numa organização, independente de sistema operacional ou aplicação, uma recomendação para controle de acesso ao PEP (Bakker *et al.*, 1998). Ademais, este servidor é física e logicamente protegido de acessos não autorizados, havendo apenas interações seguras de usuários autenticados. A administração da política de autorização e controle de acesso é unificada na BIGS, sendo realizada apenas por usuários privilegiados. Para assegurar a funcionalidade ininterrupta da BIGS, um mecanismo transparente de réplica automática deve ser assegurado.

Servidor de Segurança

Cabe ao servidor de segurança oferecer autenticação e controle de acesso às aplicações clientes, dentre outros serviços de segurança, tais como auditoria e não repudiação. Como o PEP compõe-se de aplicações heterogêneas, em geral legadas, é preciso oferecer estes serviços independente de plataforma e linguagem de programação. A solução foi adotar os padrões abertos para processamento distribuído *CORBA Security Service* (CSS) e o serviço de decisão para acesso a recursos (RAD – *Facility*) (OMG, 1998 e OMG, 2000). O RAD – *Facility* oferece interfaces padronizadas que permitem o controle de acesso detalhado, ao nível da aplicação, mas de uma forma em que a lógica do controle de acesso é separada da lógica da aplicação, com transparência em relação ao modelo de decisão efetivamente implementado. Este *framework* é adequado para suportar o modelo proposto neste trabalho, pois prevê o tratamento dos fatores dinâmicos que influenciam a lógica de autorização e possibilita a combinação de diferentes políticas de controle de acesso (Beznosov *et al.*, 1999). O CSS oferece interface padrão para autenticação de usuários, dentre outros serviços de segurança, como confidencialidade de comunicação e não repudiação. Uma implementação na linguagem de programação Java da interface de autenticação de usuário do CSS baseada no nome de *login* e senha e da interface de autorização de acesso do RAD – *Facility*, segundo o modelo proposto neste trabalho, foi por nós desenvolvida. Estas interfaces foram integradas no servidor CORBA/Visibroker, também implementado em Java, com o CSS ativado, com acesso através do protocolo padrão IIOP (*Internet Inter-Orb Protocol*) sobre SSL. O acesso ao servidor LDAP se faz através da API JNDI (*Java Naming Directory Interface*) empregando LDAP sobre SSL. O controle de sessão dos usuários conectados é também responsabilidade deste servidor.

Discussão e Conclusão

O desenvolvimento desta solução visou atender as necessidades de controle de acesso do PEP do InCor, composto por aplicações distribuídas e heterogêneas. O processo adotado para implantação da solução baseou-se nas seguinte etapas: definição dos papéis desempenhados na instituição; cadastramento dos usuários e atribuição dos respectivos papéis; seleção de uma aplicação piloto para emprego do modelo proposto. Foram definidos 30 papéis, com cada usuário podendo associar-se a no máximo quatro deles. O PEP na WEB (Tachinardi *et al.*, 1995) foi selecionado como aplicação piloto por possuir uma ampla variedade de usuários e por necessitar de um aprimoramento do seu controle de acesso a fim de viabilizar o seu acesso externo, e não apenas internamente, na *intranet* corporativa da instituição, como ocorre hoje. Um total de 780 usuários tem hoje acesso com diferentes privilégios ao PEP na WEB que oferece informações clínicas organizadas a partir de diferentes sistemas de informação hospitalar, incluindo exames e procedimentos realizados, imagens médicas, dados em tempo real de monitores beira de leito e documentos digitalizados do prontuário em papel.

No momento, está em andamento o projeto para definição das autorizações de acesso para as aplicações legadas "Sistema de Registro de Procedimentos" e "Sistema de Prescrição Médica", utilizadas por médicos e outros profissionais de saúde, desenvolvidos no ambiente de programação Magic (Magic Software Enterprises, 2000). A intenção é adaptar paulatinamente as aplicações existentes para este novo esquema de autenticação e de controle de acesso, bem como as que venham ser desenvolvidas, de modo que todo o PEP tenha o seu acesso controlado segundo uma política unificada e consistente.

Este trabalho propôs um modelo de autorização adequado para as exigências de controle de acesso ao prontuário eletrônico, buscando assegurar a privacidade do paciente e a segurança de acesso aos seus dados, mas flexível o suficiente para tratar casos de exceção com base em informações contextuais. Sem considerar as exceções, a execução de uma política de autorização para o PEP é de difícil implementação: ou se teria uma definição de privilégios permissiva, comprometendo a privacidade do paciente; ou ela seria por demais rígida, comprometendo o acesso às informações essenciais para um atendimento adequado. Ademais, a combinação do CABP com o modelo de autorização com exceções dinâmicas possibilita a implementação de uma política de acesso ao PEP es-

tritamente de acordo com a necessidade do usuário em acessar uma informação ou realizar uma ação para efetuar tarefas inerentes à sua função organizacional.

Apresentou ainda a implementação deste modelo numa arquitetura baseada em padrões abertos e distribuída, capaz de ser acessada pelos diversos segmentos em que o PEP se distribui, mas com uma administração unificada para política de autorização e controle de acesso. Tal arquitetura possibilita trabalhar com diferentes políticas de controle de acesso, oferecendo portanto, maior flexibilidade.

Está em andamento a especificação de modelos contextuais específicos para criação dinâmica de autorizações de acesso ao PEP, bem como ferramentas para sua administração. Também é pesquisada uma forma viável de implantar nesta arquitetura a autenticação robusta do usuário baseada em *smart cards* e em certificados digitais.

Referências

Bakker, A., Barber, B., Ishikawa, K., Takeda, H. and Yamamoto, K. (1998), "Overall Conclusions and Recommendations", *International Journal of Medical Informatics*, v. 49, n. 1, p. 135-137.

Bertino, E., Jajordia, S. and Samarati, P. (1999), "A Flexible Authorization Mechanism for Relational Data Management Systems", *ACM Transactions on Information Systems*, v. 17, n. 2, p. 101-140.

Beznosov, K., Deng, Y., Blakley, B., Burt, C. and Barkley, J. (1999) "A Resource Access Decision Service for CORBA-based Distributed Systems", *Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC '99)*, p. 310-319.

Kaihara, S. (1998), "Realisation of the Computerised Patient Record: Relevance and Unsolved Problems", *International Journal of Medical Informatics*, v. 49, n. 1, p. 1-8.

Magic Software Enterprises (2000), The Magic® Guide to Application Partitioning & Client/Server – Magic Enterprise Edition Version 8, Magic Software Enterprises Ltd.

Motta, G. H. M. B. e Furuie, S. S. (2001), *Controle de Acesso Baseado em Papéis para o Prontuário Eletrônico do Paciente em Ambientes Distribuídos e Abertos*, Relatório Técnico, Unidade de Pesquisa e Desenvolvimento, Instituto do Coração - HC.FMUSP, São Paulo, SP, julho.

Motta, G. H. M. B., Furuie, S. S., Nardon, F. B. e Gutierrez, M. A. (2000) "Considerações Sobre o Controle de Acesso ao Prontuário Eletrônico do Paciente", *Anais do CBIS´2000 – VII Congresso Brasileiro de Informática em Saúde*, São Paulo, SP, 14 a 18 de outubro.

Myers, J. *Simple Authentication and Security Layer – SASL* (1997), Internet Engineering Task Force – IETF, In: http://www.ietf.org/rfc/rfc2222.txt?number=2222.

NAS – National Academy of Sciences (1997), *For the Record: Protecting Electronic Health Information*, National Academy Press, Washington, DC, EUA.

OMG – Object Management Group (1998), *CORBA Security Service Specification*. In: http://www.omg.org/cgi-bin/doc?formal/98-12-17.

OMG – Object Management Group (2000) *Resource Access Decision Facility*. In: http://www.omg.org/cgi-bin/doc?dtc/00-08-06.

Sandhu, R. S. and Samarati, P. (1994), "Access Control: Principles and Practice", *IEEE Communications Magazine*, v. 32, n. 9, p. 40-48, setembro.

Sandhu, R. S., Coyne, E. J. and Youman, C. E. (1996), "Role-Based Access Control Models", *IEEE Computer*, v. 29, n. 2, p. 38-47, fevereiro.

Sandhu, R., Ferraiolo, D. and Kuhn, R. (2000), "The NIST Model for Role-Based Access Control: Towards a Unified Standard", *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*, Berlin, Alemanha, p. 47-63, outubro.

Smith, E. and Eloff, J. H. P. (1999), "Security in Health-Care Information Systems – Current Trends", *International Journal of Medical Informatics*, v. 54, n. 1, p. 39-54.

Tachinardi, U.; Furuie, S. S.; Bertozzo, N.; Moura, L.; Gutierrez, M. A. and Melo, C. P. (1995), "Hypermedia Patient Data Retrieval and Presentation Through WWW", *Proceedings of the 19th Symposium on Computer Applications in Medical Care*, p. 551-555.

Yeong, W., Howes, T. and Kille, S. (1995), *Lightweight Directory Access Protocol (LDAP)*. Internet Engineering Task Force – IETF, In: http://www.ietf.org/rfc/rfc1777.txt?number=1777.