CBIS'2002 - VIII CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE – Natal, RN
Anais do VII Congresso Brasileiro de Informática em Saúde, 2002

MACA: Uma Ferramenta de Autorização e Controle de Acesso para o Prontuário Eletrônico de Pacientes

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

[1,2] Instituto do Coração – Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo
[1] Escola Politécnica da Universidade de São Paulo
[1] Departamento de Informática - Universidade Federal da Paraíba

Resumo – Conceber modelos adequados para autorização e controle de acesso para o prontuário eletrônico de pacientes (PEP) é indispensável para o uso em larga escala do PEP em grandes instituições de saúde. Este trabalho apresenta o MACA (***M****iddleware* para **A**utorização e **C**ontrole de **A**cesso), uma ferramenta que implementa um modelo de autorização contextual para o Controle de Acesso Baseado em Papéis (CABP). O CABP regula o acesso dos usuários aos recursos computacionais com base nos papéis que eles desempenham numa organização. Uma autorização contextual usa informações ambientais disponíveis durante o acesso, como o relacionamento usuário/paciente, para decidir se um usuário tem o direito de acessar um recurso do PEP. A arquitetura de software onde o MACA está implementado utiliza o protocolo LDAP (*Lightweight Directory Access Protocol*), a linguagem de programação Java, o serviço de segurança CORBA e o serviço de decisão para acesso a recursos (RAD – *Facility*) do CORBA/OMG. A adoção destes padrões para processamento aberto e distribuído permite que os componentes heterogêneos do PEP utilizem os serviços de autenticação de usuário e autorização de acesso de modo unificado e consistente, independentemente de plataforma.

Palavras-chave: prontuário eletrônico de pacientes, autorização e controle de acesso, segurança.

Abstract – Designing proper models for authorization and access control for the electronic patient record (EPR) is essential to wide scale use of the EPR in large health organizations. This work presents MACA (**M**iddleware for **A**uthorization and **A**ccess **C**ontrol), a tool that implements a contextual role-based access control (RBAC) authorization model. RBAC regulates user's access to computers resources based on their organizational roles. A contextual authorization uses environmental information available at access-request time, like user/patient relationship, in order to decide whether a user has the right to access an EPR resource. The software architecture where MACA is implemented uses 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, heterogeneous EPR components can request user authentication and access authorization services in a unified and consistent fashion across multiple platforms.

Keywords: electronic patient records, authorization and access control, security.

Introdução

Conceber modelos adequados para autorização e controle de acesso para o prontuário eletrônico de pacientes (PEP) é indispensável para o uso em larga escala do PEP em grandes instituições de saúde [1]-[4]. Entretanto, duas questões principais devem ser consideradas na concepção da política de autorização e durante o controle de acesso.

A primeira é que o controle de acesso ao PEP, em nenhuma circunstância, deve prejudicar o atendimento ao paciente por negar acesso legítimo às informações e serviços requisitados pelo pessoal médico. Fora desse 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 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. Por exemplo, é indesejável impor uma política de autorização excessivamente restritiva, que impeça um médico, numa emergência, de acessar o prontuário de um paciente gravemente doente [5]. Tampouco é desejável estabelecer uma política demasiadamente permissiva, facilitando a violação da privacidade do paciente. É necessário dispor de meios adequados para uma definição precisa de políticas de autorização para o PEP, onde o acesso é concedido ou negado no momento exato, de acordo com a necessidade e o direito do usuário, levando em conta informações contextuais ou circunstanciais.

A segunda questão refere-se a como administrar uma política de autorização e a como 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. Em geral, estes segmentos são sistemas legados e têm seus próprios mecanismos para controle de acesso implementados de forma estanque. Uma solução adequada para integração dos segmentos do PEP é a adoção de um serviço de *middleware* padronizado, tal como o CORBA *Healthcare Domain Task Force* [6]-[8]. Logo, 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, é um requisito básico.

Este trabalho apresenta o MACA (***M****iddleware*

para **A**utorização e **C**ontrole de **A**cesso), uma ferramenta que implementa um modelo de autorização contextual para o controle de acesso baseado em papéis, visando atender as questões postas anteriormente. O uso de contextos permite a definição de regras de autorização baseadas em fatores dinâmicos, existentes no momento em que uma solicitação de acesso é realizada [9]. A arquitetura de software que suporta esta implementação baseia-se em padrões de processamento aberto e distribuído a fim de alcançar interoperabilidade e portabilidade para segurança. O MACA usa o serviço de diretórios LDAP [10] como uma base de informações de gerência de segurança (BIGS), o serviço de segurança CORBA (SSC) [11] e o serviço de decisão para acesso a recursos (RAD – *Facility*) [12] como soluções de *middleware* para autenticação de usuários e decisão de autorização de acesso, respectivamente.

O MACA vem sendo desenvolvido no Instituto do Coração (InCor) - HC.FMUSP, como uma solução para incrementar a segurança de acesso para o prontuário eletrônico de pacientes [13] e está em uso rotineiro.

O Modelo de Autorização do MACA

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 [14], 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 (login e senha) ou com cartões de identificação, certificados digitais ou dados biométricos.

O MACA implementa um modelo de autorização contextual [9] para o controle de acesso baseado em papéis (CABP) definido pelo NIST (*National Institute of Standards and Technology*) [15]. O CABP tem características que atendem aos requisitos de controle de acesso do PEP, sendo uma recomendação do HIPAA (*Health Insurance Portability and Accountability Act of 1996*) para regular o acesso às informações clínicas de pacientes [16].

Controle de Acesso Baseado em Papéis

O CABP 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 [15]. Neste caso, autorizações não são associadas diretamente a usuários, mas sim a papéis, de acordo com as atribuições pertinentes. Papéis são associados a usuários segundo as funções que eles exercem. Por exemplo, se um usuário é um médico e tem o cargo de diretor clínico, ele terá os papéis *Médico* e *Diretor Clínico* associados. Consequentemente, seus direitos de acesso ao PEP são os definidos para estes papéis, de acordo com a necessidade de saber/fazer inerente a autoridade e responsabilidade de cada papel.

Ademais, o CABP favorece a administração da política de acesso, pois permite colocá-la na perspectiva e um modelo organizacional [17]. Usuários podem facilmente ser remanejados de um papel para outro e novas autorizações podem ser concedidas para papéis, refletindo as necessidades da organização. Como privilégios não são concedidos diretamente para usuários, mas a papéis, a rotatividade de pessoal tem um baixo impacto na administração da política de autorização, que é realizada de forma unificada através de papéis administrativos. Neste caso, os procedimentos para remoção de privilégios, ou bloqueio de contas de acesso ao PEP, quando o vínculo de um usuário com a organização se encerra, podem ser feitos com facilidade. Isto é particularmente útil em hospitais escola, onde o número de usuários do PEP com vínculo temporário não é desprezível.

Autorizações Contextuais

O modelo de autorização implementado pelo MACA [9] estende o CABP proposto pelo NIST com a inclusão de regras contextuais às autorizações. Tais regras permitem estabelecer políticas de acesso com base em variáveis ambientais que denotam informações sobre usuário corrente, data/hora e local do acesso, etc. Novas variáveis podem ser livremente programadas e incorporadas para especificação de políticas de autorização mais complexas. Autorizações contextuais permitem a definição de políticas de acesso mais precisas, flexíveis, com baixa granularidade, onde o acesso é concedido ou negado no momento exato, de acordo com a necessidade do usuário.

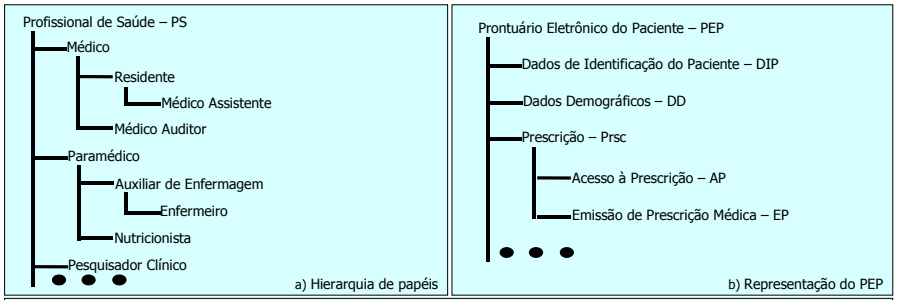
A inclusão de regras contextuais nas autorizações atende a um requisito recomendado pelo HIPAA [16] para o controle de acesso em aplicações na área de saúde, mas que não é contemplado no modelo de referência do NIST.

Exemplo

Esta seção apresenta um exemplo didático com as características de utilização do modelo de autorização do MACA. A Figura 1 *b)* ilustra uma representação parcial de um PEP, onde uma política de autorização de acesso deve ser aplicada. Os recursos do PEP são estruturados numa estrutura de árvore e cada deles tem um privilégio de acesso particular. Os recursos *PEP*, *DIP*, *DD*, *Prsc* e *AP* denotam objetos com privilégio de acesso "consulta". *PEP* representa um objeto onde usuários podem pesquisar pelo prontuário de uma pessoa específica. *DIP* mostra dados que podem identificar diretamente

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

o paciente, enquanto *DD* mostra dados demográficos anônimos. *Prsc* apresenta a lista de cabeçalhos de prescrições médicas. *AP* permite a visualização da prescrição de um paciente específico. *EP* representa a ação de emitir uma prescrição e tem privilégio de acesso "execução". Uma característica do CABP é a capacidade em representar os recursos abstratamente, independente de sua forma concreta.



PS: <PS, PEP, +, consulta, fraca>; <PS, DIP, +, consulta, fraca>; <PS, DD, +, consulta, fraca>; <PS, Prsc, +, consulta, fraca>; <PS, AP, -, consulta, fraca>; <PS, EP, -, execução, fraca>.

Médico: <Médico, AP, +, consulta, fraca>

Residente: <Residente, EP, **exp-abs**(umCodPac) { umCodPac **in** pacCtx.patientes_internados | netCtx.peer_dns **in** secCtx.dominios_emergencia | netCtx.peer_dns **in** secCtx.dominios_ambulatório }, execução, forte>.

Médico Assistente: ...

Médico Auditor: <Médico Auditor, EP, -, execução, forte>; <Médico Auditor, AP, **exp-abs**(umCodPac) { pacCtx.plano_saude(umCodPac) **in** userCtx.convenios }, consulta, fraca>.

Paramédico: <Paramédico, AP, **exp-abs**(umCodPac) { umCodPac **in** pacCtx.patientes_internados & paramedicCtx.esta_no_turno_de_trabalho(dtCtx.data_hora, userCtx.matricula) }, consulta, fraca>.

Auxiliar de Enfermagem: ...

Enfermeiro: ...

Nutricionista: ...

Pesquisador Clínico: <Pesquisador Clínico, DIP, -, consulta, fraca>; < Pesquisador Clínico, AP, +, consulta, fraca>.

c) Autorizações

Figura 1 – Exemplo de aplicação do modelo de autorização do MACA.

Papéis Hierárquicos

No MACA, papéis são dispostos numa hierarquia estruturada como uma árvore invertida. Isto facilita a gerência da política de autorização pelo compartilhamento de autorizações comuns entre os papéis. Por exemplo, na Figura 1 *a)*, autorizações comuns a maioria dos papéis são associadas ao papel *PS*, que denota um profissional genérico da área de saúde. Todo papel descendente de *PS* herda tais autorizações, podendo redefini-las ou adicionar novas autorizações.

Autorizações positivas (+) e negativas (-) são um recurso adicional que também facilita a gerência da hierarquia. Quando o acesso é proibido (permitido) para a maioria dos papéis descendentes, então uma autorização negativa (positiva) deve ser usada no papel ascendente. No exemplo da Figura 1 *c)*, uma minoria dos papéis descendentes de *PS* têm o direito de visualizar prescrições. Logo, a autorização <PS, AP, -, consulta, fraca> é associada a *PS* e apenas os casos de exceção são redefinidos como autorizações positivas nos papéis (*Médico* e *Pesquisador Clínico*) onde esta operação é permitida. Outra vantagem em usar autorizações negativas é que proibições de acesso podem ser estabelecidas explicitamente.

Aplicação de Autorizações Contextuais

A definição de uma política de acesso usando apenas autorizações positivas e negativas, de forma estática, não atende às necessidades de controle de acesso para o PEP. Atributos do usuário, data/hora e local de acesso, relacionamento usuário/paciente, status do paciente, robustez da autenticação do usuário e segurança da conexão são alguns dos fatores que merecem atenção na definição de regras de autorização de acesso para o PEP [2], [4], [16].

Por exemplo, um usuário com papel *Médico Auditor* (Figura 1 *c)*) deveria acessar apenas as prescrições dos pacientes dos convênios que ele representa. Usando somente autorizações positivas e negativas, ou o acesso é concedido a todas as prescrições, ou ele é negado para todas elas. Empregando contextos, uma autorização será positiva ou negativa dependendo do resultado da avaliação de uma expressão lógica, denominada *regra de autorização*, no momento da solicitação de acesso. Logo, é possível definir uma política de acesso mais exata para visualização de prescrições por parte dos médicos auditores. Na regra estabelecida para o recurso *AP*, no papel *Médico Auditor*, `umCodPac` é um parâmetro da regra passado durante a solicitação de autorização e identifica o paciente relacionado com a prescrição a ser visualizada. `pacCtx.plano_saude` é uma função contextual que retorna a identificação do plano de saúde do paciente denotado por `umCodPac`. `userCtx.convenios` é um contexto que denota o conjunto das identificações dos convênios para os quais o médico auditor trabalha. De acordo com esta regra, o acesso é concedido somente quando um médico auditor tenta visualizar as prescrições de pacientes dos planos que ele representa.

As demais regras na Figura 1 *c)* especificam que residentes e seus descendentes só podem prescrever para pacientes internados, ou para aqueles em atendimento na emergência ou no ambulatório; e que os paramédicos e seus descendentes somente podem visualizar prescrições de pacientes internados quando estiverem em seu turno de trabalho.

Autorizações Fortes, Fracas e Conflitos de Interesse

Autorizações fortes são usadas para políticas de acesso estritas, que não podem ser revogadas. No exemplo da Figura 1 *c)*, a regra de autorização para o papel *Residente* prescrever é forte e não pode ser redefinida por seus descendentes. Já o papel *Médico Auditor* e seus eventuais descendentes não po

dem, em nenhuma circunstância, efetuar prescrições. Logo, nos casos em que um mesmo usuário possua ambos os papéis associados, haverá um conflito sempre que a regra da autorização do papel *Residente* conceder o acesso, pois a regra do papel *Médico Auditor* nega este acesso. A política adotada para resolver conflitos fortes como este é negar o acesso. Isto porque autorizações fortes devem ser usadas para proteger recursos críticos, que envolvam conflitos de interesses. Neste caso, é indesejável que um mesmo usuário possa efetuar prescrições e ao mesmo tempo auditá-las.

Autorizações fracas são usadas para definir políticas que podem ser revogadas. Esta característica confere flexibilidade na especificação das políticas de acesso, pois permite que uma autorização seja redefinida em papéis descendentes. Ademais, quando da ocorrência de conflitos entre autorizações fracas, prevalecerá aquela autorização que concede o acesso. Neste caso, o conflito não sinaliza um conflito de interesses real, mas apenas necessidades acesso distintas para papéis diferentes.

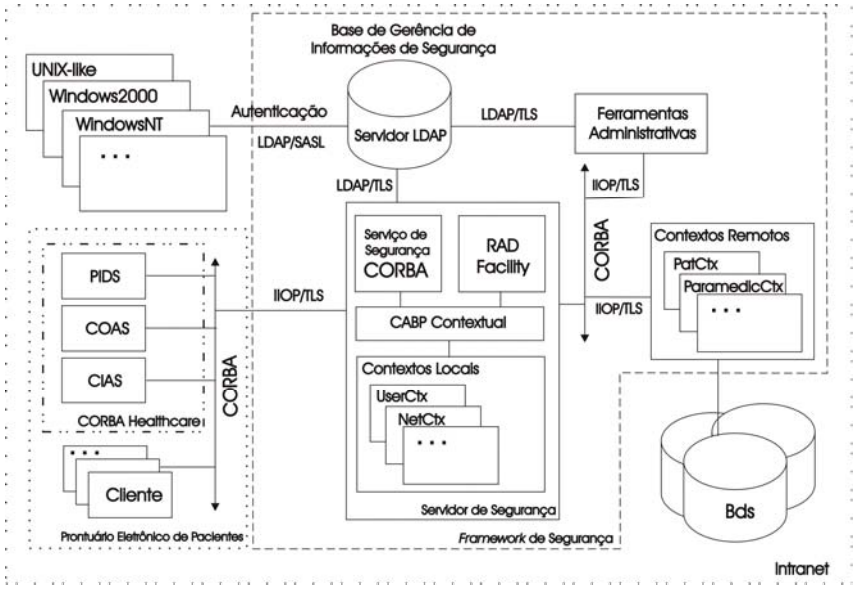


Figura 2 – Esquema da Arquitetura de Implementação.

Arquitetura de Implementação

A arquitetura onde os componentes do MACA foram implementados é apresentada na Figura 2. É um modelo cliente-servidor multicamada com os seguintes componentes principais: um servidor LDAP, encarregado de manter a base de gerência de informações de segurança (BIGS); um servidor de segurança, encarregado de oferecer serviços de autenticação de usuário, de decisão de acesso à recursos, dentre outros; e, finalmente, as aplicações clientes do PEP que requisitam estes serviços de segurança. A adoção de padrões de processamento aberto e distribuído foi um importante requisito para alcançar interoperabilidade e portabilidade dos serviços de segurança.

Prontuário Eletrônico de Pacientes

No contexto do MACA, o PEP é um sistema distribuído composto por aplicações heterogêneas [1]. Os serviços padrão PIDS [6], COAS [7] e CIAS [8] do CORBA *Healthcare Domain Task Force* são a infra-estrutura de *middleware* para acessar informações de pacientes a partir de fontes heterogêneas e, em muitos casos, legadas. Esta infra-estrutura é usada como base para construção de aplicações voltadas aos usuários finais, tais como sistema para visualização de imagem médicas integrado com informações clínicas, sistema de prescrição médica, sistema de emissão de laudos, etc.

Outra característica do CORBA *Healthcare* é que ele pode ser usado para integrar os segmentos do PEP entre instituições. Entretanto, vale ressaltar que o CORBA *Healthcare* somente oferece serviços de leitura para informações clínicas. Na prática, há a necessidade de se construir ou usar objetos CORBA customizados para alimentar dados do paciente nos bancos de dados do PEP. Estes objetos podem ser novas aplicações desenvolvidas em servidores de aplicação, como o *Enterprise JavaBeans*, ou ser um envoltório CORBA (*wrapper*) de um sistema legado. Em outros casos, os segmentos do PEP são aplicações legadas independentes. A despeito disto, é desejável impor a autenticação do usuário e uma política de autorização e controle de acesso unificadas para estes segmentos, sejam eles objetos CORBA ou não.

Os segmentos do PEP são protegidos pela *intranet* da instituição que os mantém. Isto é, a *intranet* limita o acesso a segmentos selecionados do PEP (e. g., serviços do CORBA *Healthcare*) apenas para terceiros confiáveis (e. g., outros hospitais, pacientes, etc.) através de conexões seguras (uma rede privada virtual, por exemplo). Contudo, tanto dos acessos externos, quanto os internos, são regulados pela política de segurança armazenada na BIGS e estabelecida pela instituição mantenedora dos segmentos do PEP.

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 [10]. Por ser hierárquico e flexível, o LDAP é capaz de representar naturalmente as hierarquias de papéis e de recursos do modelo de auto

rização. 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.).

Todo acesso à BIGS é realizado através do protocolo LDAP sobre TLS (*Transport Layer Security*) para assegurar confidencialidade e integridade na comunicação. Adicionalmente, TLS pode assegurar autenticação mútua entre clientes LDAP e o servidor LDAP. Ademais, a autenticação via sistemas operacionais e gerenciadores de bancos de dados mais comuns podem ser efetuadas com segurança junto ao servidor LDAP através do protocolo SASL [18]. Esta solução viabiliza a autenticação unificada de usuários numa organização, independente de sistema operacional ou aplicação, uma recomendação para segurança de acesso para o PEP [4], [16].

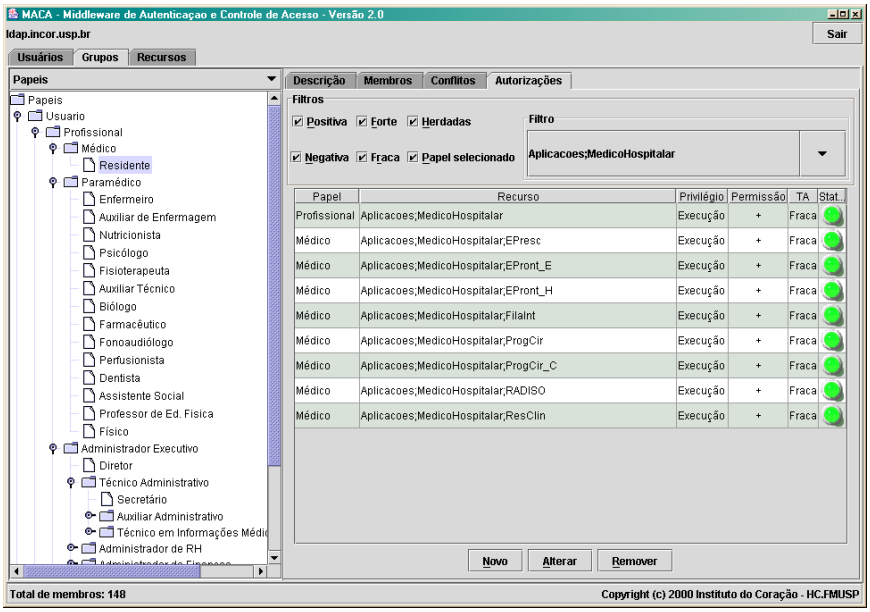


Figura 3 – Módulo administrativo do MACA para gerência de autorizações.

A administração da política de segurança é realizada na BIGS via ferramentas administrativas e apenas por usuários privilegiados através de interações seguras e com autenticação e controle de acesso adequados. O servidor LDAP deve ser protegido fisicamente e todos os acessos não locais devem ser desabilitados. A localização unificada das políticas de segurança facilita a administração, mas introduz uma sobrecarga adicional, visto que todos os clientes LDAP usam um único servidor. Ademais, um servidor central introduz um único ponto de falha e abre oportunidades de ataques para colocá-lo fora de serviço. Como LDAP é um serviço de diretório distribuído e a maioria das implementações disponíveis têm mecanismo de réplica automático, é viável construir um servidor logicamente centralizado e tolerante a falhas, embora fisicamente distribuído e redundante.

Servidor de Segurança

Cabe ao servidor de segurança (Figura 2) oferecer autenticação, autorização e controle de acesso às aplicações clientes, dentre outros serviços de segurança. O RAD – *Facility* [12] 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 de autorização do MACA, pois prevê o tratamento dos fatores dinâmicos que influenciam a lógica de autorização e possibilita a combinação de diferentes políticas de controle de acesso. O Serviço de Segurança CORBA oferece interface padrão para autenticação de usuários e faz o controle de acesso transparente para as operações definidas nos objetos CORBA. O módulo "CABP Contextual" implementa o modelo de autorização do MACA, sendo utilizado como política de autorização de acesso pelo SSC e pelo RAD – *Facility*. Todas as interações entre os objetos CORBA clientes e o servidor de segurança ocorrem via IIOP (*Internet Inter-ORB Protocol*) sobre TLS.

Software Implementado

O MACA foi implementado no InCor com a linguagem de programação Java e inclui as ferramentas administrativas, o módulo "CABP Contextual", bem como as implementações dos contextos. As ferramentas administrativas permitem gerenciar a política de acesso ao PEP armazenada na BIGS. Permitem a um administrador criar, atualizar e remover usuários, papéis, recursos e autorizações. A Figura 3 ilustra o módulo administrativo do MACA que gerencia autorizações. O módulo "CABP Contextual" implementa o serviço de autenticação de usuários com *login* e senha, o gerenciador de sessões de usuários e o serviço de autorização de acesso. Ainda provê um interpretador para regras de autorização contextual. Contextos locais são implementados em Java e compartilham o mesmo espaço de endereçamento do módulo "CABP Contextual". Contextos remotos são acessados por clientes Java/CORBA via IIOP sobre TLS. Contextos são bibliotecas dinâmicas carregadas em tempo de execução através do mecanismo de extensão de Java.

Discussão e Conclusão

Atualmente o MACA está em uso rotineiro no InCor. O processo adotado para sua implantação baseou-se nas seguintes etapas: definição dos papéis desempenhados na instituição; cadastramento dos usuários e atribuição dos respectivos papéis; criação

das autorizações para as aplicações que compõe PEP. Cerca de 1400 perfis de usuários estão armazenados no servidor LDAP e 56 papéis configurados. Cada usuário pode associar-se a no máximo quatro papéis. Vinte sistemas legados implementados no ambiente de programação Magic [19], tal como o "Sistema de Prescrição Médica", foram modificados para incluir os serviços de autenticação de usuário e de autorização de acesso do MACA.

O desenvolvimento do MACA buscou atender as necessidades de controle de acesso do PEP encontradas em grandes instituições de saúde, como o InCor. O modelo de autorização implementado busca aumentar a privacidade do paciente e a segurança de acesso aos seus dados. A integração de regras contextuais às autorizações do CABP confere mais flexibilidade e poder de expressividade na especificação da política de acesso ao PEP. O controle de acesso pode ser efetuado de forma mais precisa, no momento exato, de acordo com o direito e a necessidade do usuário, mas sem custos gerenciais excessivos. Isto porque lógicas de controle de acesso mais complexas, tradicionalmente embutidas nas aplicações protegidas, podem agora ficar isoladas destas aplicações, embora mantendo o contexto necessário para conceder ou não uma autorização. Assim, mudanças na lógica de autorização não implicam em mudanças nas aplicações.

Finalmente, a arquitetura em que o MACA está implementado é baseada em padrões de processamento aberto e distribuído. Assim, os segmentos do PEP podem utilizar os serviços de autenticação de usuário e autorização de acesso independente de plataforma, mas com uma administração unificada da política de acesso.

Referências

[1] E. Smith e J. H. P. Eloff, "Security in Health-Care Information Systems – Current Trends", *Int. J. Med. Inf.*, vol. 54, pp. 39-54, Apr. 1999.

[2] K. Beznosov, "Requirements for Access Control: US Health-care Domain", *Proc. 3rd ACM Workshop on Role-based Access*, 1998, pp. 43.

[3] S. Kaihara, "Realisation of the Computerised Patient Record: Relevance and Unsolved Problems", *Int. J. Med. Inf.*, vol. 49, pp. 1-8, Mar. 1998.

[4] National Academy of Sciences, *For the Record: Protecting Electronic Health Information*. Washington, DC: National Academy Press, 1997, pp. 93-94.

[5] T. C. Rindefleisch, "Privacy, Information Technology, and Health Care", *Commun. ACM*, vol. 40, pp. 93-100, Aug. 1997.

[6] OMG – Object Management Group. (2001) Person Identification Service, v. 1.1. [Online] Available: http://www.omg.org/cgi-bin/doc?formal/2001-04-04

[7] OMG – Object Management Group. (2001) Clinical Observation Access Services, v. 1.0. [Online] Available: http://www.omg.org/cgi-bin/doc?formal/2001-04-06

[8] OMG – Object Management Group. (2001) Clinical Image Access Services FTF Final Report. [Online] Available: http://www.omg.org/cgi-bin/doc?dtc/2001-10-02

[9] G. H. M. B. Motta e S. S. Furuie, "Um Modelo de Autorização Contextual para o Controle de Acesso Baseado em Papéis", *Anais 20º Simp. Bras. Redes de Comp.: II Workshop Bras. Seg. de Sist. Comp.*, 2002, pp. 136-143.

[10] W. Yeong, T. Howes e S. Kille. (1995, March) Lightweight Directory Access Protocol (LDAP). Internet Engineering Task Force – IETF. [Online]. Available: http://www.ietf.org/rfc/rfc1777.txt

[11] OMG – Object Management Group. (2001) CORBA Security Service Specification. [Online] Available: http://www.omg.org/cgi-bin/doc?formal/01-03-08

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

[13] S. Furuie, M. Rebelo, M. Gutierrez, R. Moreno, F. Nardon, G. Motta, J. Figueiredo, N. Bertozzo e V. Fiales, "Prontuário Eletrônico em Ambiente Distribuído e Heterogêneo: a Experiência do InCor", *Anais do CBIS'2002 – VIII Congresso Brasileiro de Informática em Saúde*, 2002.

[14] R. S. Sandhu and P. Samarati, "Access Control: Principles and Practice", *IEEE Commun. Mag.*, vol. 32, pp. 40-48, Sep. 1994.

[15] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn e R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control", *ACM Trans. Info. Syst. Security*, vol. 4, pp. 224-274, Aug. 2001.

[16] Department of Health and Human Services, "Security and Electronic Signature Standards", *Federal Register*, vol. 63, pp.43241-43280, Aug. 1998.

[17] S. Oh e S. Park, "Enterprise Model as a Basis of Administration on Role-Based Access Control", *Proc. 3rd Int. Symp. Coop. Database Syst. Adv. App.*, 2001, pp. 150-158.

[18] J. Myers. (1997, October) Simple Authentication and Security Layer (SASL). Internet Engineering Task Force – IETF. [Online]. Available: http://www.ietf.org/rfc/rfc2222.txt

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

Contato

Gustavo H. M. B. Motta
Unidade de P&D, Serviço de Informática do Instituto do Coração - HC.FMUSP.
Fone: 11 3069 5545
e-mail: gustavo.motta@incor.usp.br