GERÊNCIA DE SEGURANÇA OSI
INTERFACE DE CONTROLE DE ACESSO

Alexandre Moraes Ramos[1]
Elizabeth Specialski[2]

Universidade Federal de Santa Catarina
Curso de Pós-Graduação em Ciência da Computação
Caixa Postal 476 - Campus Universitário - 88040-900 - Florianópolis - SC
Tel (048) 2319738 - Telex (048) 2240 UFSC BR - Fax (048) 2319770

RESUMO

Este artigo apresenta uma Interface de Controle de Acesso para o Modelo de Gerenciamento OSI. É destinada às autoridades de segurança e visa auxiliar a implementação de serviços de controle de acesso em sistemas de gerência. A interface interage com um ambiente de gerenciamento através da troca de informações com as Entidades de Aplicação de Gerenciamento de Sistema (SMAEs) dos processos de aplicação para autorizar as associações e as operações de gerenciamento. A interface é baseada na Função de Controle de Acesso [ISO 10164-9].

ABSTRACT

This works describes an Access Control Interface to the OSI Management Model. It is dedicated to the security authority in management system and intends to help the implementation control access service in systems management. The interface with the management environment occurs exchanging information with the System Management Application Entities (SMAEs) of Application Processes for authorize management associations and operations. The interface is based on Access Control Function [ISO 10164-9].

[1] **Mestre em Ciência da Computação - UFSC (moraes@inf.ufsc.br)**
[2] **Mestre em Ciência da computação - UFRGS (beth@inf.ufsc.br)**

1. INTRODUÇÃO

Uma rede de computadores pode ser definida como um conjunto de equipamentos autônomos e interligados com a finalidade de compartilhamento de recursos lógicos e físicos. Este compartilhamento é alcançado graças à facilidade para a troca de informações possibilitada pela interoperabilidade entre os sistemas residentes nos equipamentos interconectados.

O alcance da interoperabilidade só é possível se forem utilizadas interfaces comuns entre os sistemas comunicantes. Neste sentido, o Modelo de Referência para Interconexão de Sistemas Abertos (RM-OSI) [ISO 7498] da Organização Internacional para Padronização (ISO) oferece um conjunto de normas que solucionam os problemas de integração e limitação entre as diferentes interfaces de comunicação.

As redes de computadores, como quaisquer sistemas de computação, estão sujeitas a problemas de quebra de segurança. Às vezes, até mais do que os sistemas de computação simples, devido ao seu ambiente de operação ser mais complexo e vulnerável. Os problemas surgem do fato das redes compartilharem vários recursos; operarem com sistemas complexos e diferentes; crescerem constantemente dificultando definir os limites da rede; terem muitos pontos passíveis de acesso; necessitarem de privacidade, integridade e autenticação; além de terem todos os problemas comuns aos sistemas de computação.

A fim de proteger as redes de computadores, a ISO definiu um Modelo de Segurança OSI que é composto por serviços e mecanismos [ISO 7498-2], além de funções de gerenciamento [ISO 10164-7,8,9] específicos para a área de segurança. Os serviços e mecanismos de segurança tratam exclusivamente da segurança e proteção da comunicação entre sistemas abertos. A utilização destes serviços e mecanismos em um determinado sistema aberto é definido pela Política de Segurança de acordo com as necessidades particulares de cada sistema. As funções de gerenciamento de segurança dão suporte às atividades dos sistemas de gerência e são responsáveis pelo sucesso da política de segurança adotada e também por garantirem o aperfeiçoamento da proteção da rede.

Entretanto, os sistemas de gerenciamento manipulam informações extremamente sensíveis e importantes para o perfeito funcionamento da rede. Um usuário, ao manipular um sistema qualquer, jamais teria acesso a informações tão sensíveis quanto as disponíveis em um sistema de gerência. Um sistema de gerência controla objetos gerenciados, que nada mais são do que os recursos reais de uma rede, executa operações sobre estes, gera relatórios estatísticos, alarmes, auditorias, etc. Apesar de conter funções exclusivas que cuidam da segurança da rede, a gerência acrescenta mais vulnerabilidades às já existentes, tornando a rede mais insegura [LUC93].

Dentro deste contexto, os sistemas de gerenciamento necessitam de prevenção contra acessos não autorizados. Usuários sem permissão não devem manipular informações de gerência, fazer uso ou mesmo divulgá-las indevidamente a fim de não prejudicarem o funcionamento da rede indiretamente através dos sistemas de gerência.

2. FUNÇÃO DE CONTROLE DE ACESSO

O serviço de controle de acesso em sistemas de gerenciamento OSI são implementados através da Função de Controle de Acesso [ISO 10164-9]. Esta função tem como objetivo avaliar e autorizar os pedidos de acesso aos objetos gerenciados armazenados na Base de Informações de Gerenciamento (MIB), baseada em mecanismos de segurança, de acordo com a política de controle de acesso definida para a rede.

A política de controle de acesso para recursos de gerenciamento deve identificar quais são as informações de gerenciamento que devem ter o acesso controlado, identificar quem pode manipulá-las e sob que condições, e identificar quais são as regras que controlam o acesso a estas informações de gerenciamento.

Existem dois tipos de controle de acesso nos casos específicos de gerenciamento OSI:

- para associação de aplicações de gerência, que visa garantir que iniciadores sem permissão não estabeleçam associações de gerência;
- para operações de gerência, que visa garantir que essas operações sejam feitas pelas entidades autorizadas, mas sob restrições relativas a horário, tipo de operação, recurso e informações envolvidas.

A Função de controle de acesso, que tem seu modelo básico apresentado na Figura 1, é composta pelas funções:

- *Access Control Enforcement Function* (AEF);
- *Access Control Decision Function* (ADF).

A função AEF é responsável por receber o pedido de acesso, feito por um usuário, chamado de iniciador, selecionar os parâmetros de controle de acesso do pedido e repassá-los à função ADF. A função ADF é responsável por receber os parâmetros de controle de acesso da função AEF e decidir se o pedido de acesso é válido ou não.

Para validar um pedido de acesso, a função ADF compara os parâmetros recebidos do pedido com as regras da política de controle de acesso. Se o pedido estiver de acordo com as regras, ele é validado pela função ADF. Caso contrário, o pedido é rejeitado. Uma vez tomada a decisão, a função ADF repassa o resultado para a função AEF. Se a decisão for negativa, a função ADF também entrega à função AEF as instruções de rejeição, que podem ser, por exemplo, só uma resposta negativa ou, até mesmo, uma instrução para abortar a conexão.

Na prática, é muito difícil distinguir o gerenciamento de segurança dos próprios mecanismos de segurança visto que , algumas vezes, o gerenciamento de segurança é implementado através dos próprios mecanismos de segurança (ver Função de Controle de Acesso [ISO 10164-9]).

Existem vários tipos de mecanismos de controle de acesso, vão desde os mais simples até os mais complexos, variando de acordo com as características e necessidades do ambiente que requer o controle. Fica a cargo da autoridade responsável, por especificar uma política de acesso para um sistema de gerenciamento, definir as autorizações, ou seja, as

concessões de direitos aos usuários de gerência (quem pode fazer o que e para que). A natureza dos mecanismos de autorização é que distingue as várias políticas de controle de acesso.

Figura 1 - Modelo Básico da Função de Controle de Acesso

3. POLÍTICAS DE CONTROLE DE ACESSO

As políticas de controle de acesso para sistemas de gerenciamento definem quais os recursos de gerência que necessitam de proteção. Estes recursos são associados a um objeto específico para controle de acesso, chamado de objeto *target*. Um objeto *target* contém atributos para representar as informações e regras de controle de acesso a serem aplicadas ao recurso de gerenciamento a que está associado o objeto *target*. Faz parte da definição de uma política de controle de acesso para recursos de gerenciamento a especificação dos objetos *target*.

As políticas de controle de acesso variam de acordo com os mecanismos de segurança adotados (listas de controle de acesso, diretórios, senhas, rótulos, ...). Segundo [FOR94], existem vários tipos de políticas e podem ser divididas em: *Individual-based Policy*; *Group-based Policy*; *Role-based Policy*; *Multi-level Policy* e *Modelo Militar*.

Individual-based e *Group-based* fornecem, aos usuários, particulares tipos de acesso aos recursos e deixam a cargo destes usuários o controle de novos acessos.

As políticas *Multi-level* e *Modelo Militar* são impostas pela autoridade do domínio de segurança e não podem ser evitadas pelos usuários.

Combinando características desses dois grupos, a política Role-based é, ao mesmo tempo, imposta pela autoridade de segurança e fornece particulares tipos de acesso.

Em geral, estas políticas podem ser combinadas e adotadas de acordo com as necessidades e benefícios identificados pela autoridade de segurança. Em seguida, serão apresentadas características básicas dessas políticas de segurança, que podem ser encontrados com mais detalhes em [FOR94] e [PFL89] tais como:

Individual-based: é definida em termos dos objetos sujeitos ao controle de acesso (objetos *target*), através de uma lista que contém uma entrada para cada usuário identificando o que o usuário pode fazer sobre um objeto. Pode ser implementada, conforme a Figura 2 através do mecanismo de lista de controle de acesso que é descrito em [PFL89].

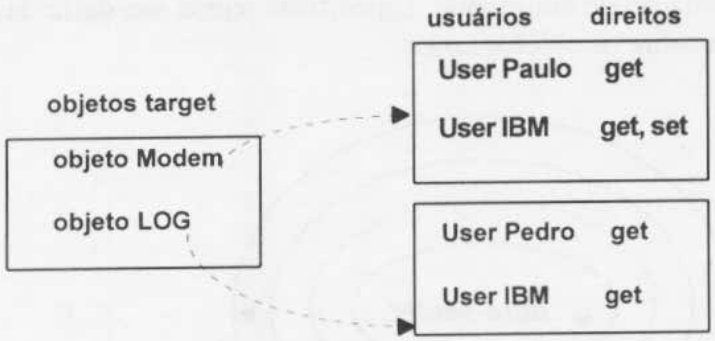


Figura 2 - Lista de Controle de Acesso

Group-based: a vários usuários são garantidos direitos sobre um determinado objeto *target*. Múltiplos usuários são agrupados e referenciados por um identificador comum. Como exemplo, na lista de controle de acesso da Figura 2, vários usuários poderiam formar o grupo *IBM*. Uma vantagem é que a troca de membros entre grupos não afeta os direitos de acesso associados aos grupos. Estas características tendem a tornar esta política mais fácil e eficiente quanto a implementação de políticas do tipo *individual-based*.

Role-based: É um tipo de política que pode ser considerada como uma variação de *group-based*. Identifica os grupos com níveis de privilégios, onde um grupo tem maior significância que o outro (hierarquia de privilégios).

A diferença está na modelagem das regras de autorização, ou seja, cria grupos com níveis de operações distintas. Como exemplo, as operações de gerenciamento mais simples (ex: *get* e *set*) podem ser associadas a grupos com menor prioridade e as operações mais importantes (ex: *create* e *delete*) são associadas a grupos com prioridade mais elevada, como exemplo:

- grupo: gerente de rede - autorização: *create, delete, action, set e get*;
- grupo: técnico de rede - autorização: *action, set e get*;
- grupo: operador de rede - autorização: *set e get*.

Segundo [FOR94], este tipo de política é muito poderosa. Primeiro, é definida de forma simples, onde é facilmente compreendida por pessoas com pouco conhecimento técnico. E segundo, porque é facilmente expressa através de uma matriz de controle de acesso, ou pela política de *group-based*.

O ponto crítico para utilização desta política é justamente na modelagem dos grupos associados às regras. A modelagem deve ser capaz de fornecer a granularidade de segurança requerida pelo sistema de gerência.

Multi-level: é um tipo de política onde a autoridade classifica hierarquicamente os objetos *target*, sob seu domínio de segurança, com níveis de sensiblidade dentro de uma hierarquia de níveis como na Figura 3. Os usuários são, também, classificados com níveis da hierarquia adotada, chamados de *clearence*.

Entre o nível de *clearence* do usuário e o nível de sensibilidade do objeto *target* é estabelecida uma relação de autoridade. Específicas regras são definidas para garantir o direito de escrita e leitura sobre os objetos *target*.

Figura 3 - Níveis de Sensibilidade

A regra para leitura, conhecida como *Simple Security Condition,* estipula que um usuário com um dado nível de *clearence* só pode executar uma operação de leitura sobre um objeto com o mesmo ou menor nível de sensibilidade.

A regra para escrita, conhecida como **-property*, estipula que um usuário com um dado nível de *clearence* somente executa operações de escrita sobre um objeto com o mesmo ou maior nível de sensibilidade. A razão para esta regra é prevenir um usuário de um nível superior transferir dados, através da escrita, para um usuário de nível inferior.

Modelo Militar: é uma variação da política *Multi-level,* utilizada pelas forças armadas. Além do nível de sensibilidade, os objetos *target* são classificados em áreas de utilização chamadas domínios. Estas áreas de utilização são usadas para garantir a necessidade de acesso somente a quem, realmente, precisa e deve utilizar os recursos de gerência.

A classificação dos recursos de gerência é dada pela combinação de {*nível, domínio*}. O usuário para ter acesso às informações dos recursos de gerenciamento, ou seja: aos objetos *target*, tem que ter autorização (*clearence*). A autorização do usuário também é expressa pela combinação de {*nível, domínio*}.

O usuário só poderá acessar um recurso de gerenciamento, se o seu nível de *clearence* for compatível com o nível de sensibilidade do objeto *target* associado ao recurso e se seu domínio contiver o domínio do objeto.

Figura 4 - Modelo Militar

Conforme a Figura 4, encontram-se como exemplos de domínio *agente de contabilização, agente de falhas e agente de segurança*. Um objeto *target* é relacionado a um nível e a um ou mais domínios de acordo com a área de utilização a que está associado:

ex: objeto *target* {*nível, domínio*}:

- arquivo de log {*secreto, agente de contabilização*};
- função de teste {*secreto, agente de falhas*};
- relatório de alarmes {*sem restrição, agente de falhas, agente de segurança*};
- arquivo de senhas {*ultra-secreto, agente de segurança*}.

Como um outro exemplo, supõe-se um objeto *target* classificado como {*secreto, segurança/falhas*} só pode ser acessado por usuários com nível de *clearence* {*ultra-secreto, agente de segurança ou agente de falhas*} ou {*secreto, agente de falhas ou agente de segurança*}, mas o acesso não é permitido para usuários com uma *clearence* {*ultra-secreto, agente contabilização*}.

Tendo a autoridade de segurança identificado e definido a política ou a combinação de políticas que irão suprir as necessidades de segurança do domínio sob sua responsabilidade, o próximo passo é definir os *objetos target* que permitirão a colocação em prática das políticas estabelecidas.

4. INTERFACE DE CONTROLE DE ACESSO

A ***Interface de Controle de Acesso*** é destinada às autoridades de segurança. Visa auxiliar a implementação de políticas de controle de acesso em sistemas de gerenciamento OSI. A *interface* permite à autoridade de segurança estipular as regras de autorização de seu domínio de segurança, oferecendo-lhe mecanismos de segurança que possibilitam a implementação das políticas de acesso: *Individual-based, Group-based; Role-based; Multi-level;* e *Modelo Militar.*

A *interface* tem como principais objetivos:

- controlar o acesso à MIB;
- controlar o estabelecimento de associações;
- facilitar a definição de objetos target;

- fornecer uma ferramenta amigável que permita à autoridade de segurança implementar e administrar as regras de autorização definidas por uma política de segurança;
- fornecer uma base de regras para as autorizações definidas.

O modelo proposto para a Interface de Controle de Acesso é composto por três elementos conforme ilustrado na Figura 5:

- um Sistema de Definição de Autorização (SDA);
- um Sistema de Controle de Autorização (SCA);
- uma Base de Dados de Autorização (BDA).

O sistema SDA é um sistema interno e independente do padrão OSI. É composto por métodos comuns que permitem a manipulação da base BDA (inclusão, alteração, exclusão e consulta). O sistema SCA implementa a funcionalidade das funções de controle de acesso AEF e ADF do modelo de gerência OSI [ISO 10164-9]. A base BDA é formada pelos objetos de controle de acesso modelados através de mecanismos de segurança que permitem a implementação das políticas de acesso.

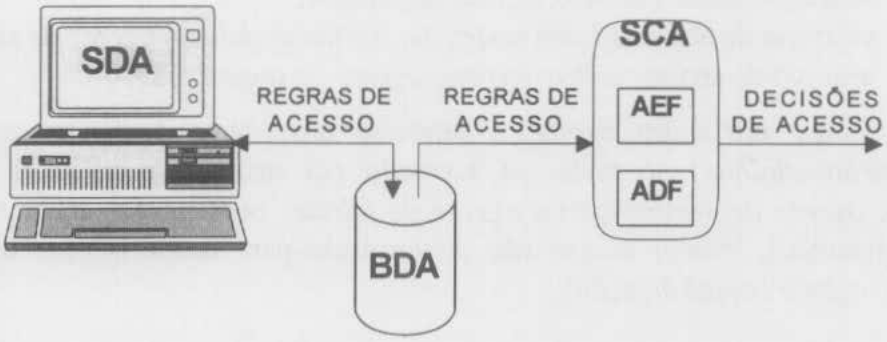


Figura 5 - Modelo Genérico da Interface de Controle de Acesso

A Interface de Controle de Acesso interage com um ambiente de gerenciamento através da troca de informações com a Entidade de Aplicação de Gerenciamento de Sistemas (SMAE) de um processo de aplicação, a fim de validar os pedidos de associação e de operações de gerenciamento (ver Figura 6).

O primeiro passo para funcionamento da *interface*, ocorre a nível conceitual, onde a autoridade de segurança de um sistema de gerência define a política de segurança a ser adotada e, consequentemente, as regras de autorização do sistema. A partir daí, a autoridade pode, através do sistema SDA, alimentar e administrar a base BDA com as regras definidas. Estas regras são modeladas através das listas de regras que compõem a base BDA.

Uma vez que as regras estão modeladas e introduzidas na base BDA, o sistema SCA pode entrar em operação. Toda vez que o processo de aplicação (PA) local for requisitado para estabelecer uma associação de gerência ou para realizar uma operação de gerenciamento, este processo invoca o sistema SCA para inferir sobre a base BDA e decidir se o pedido é valido ou não.

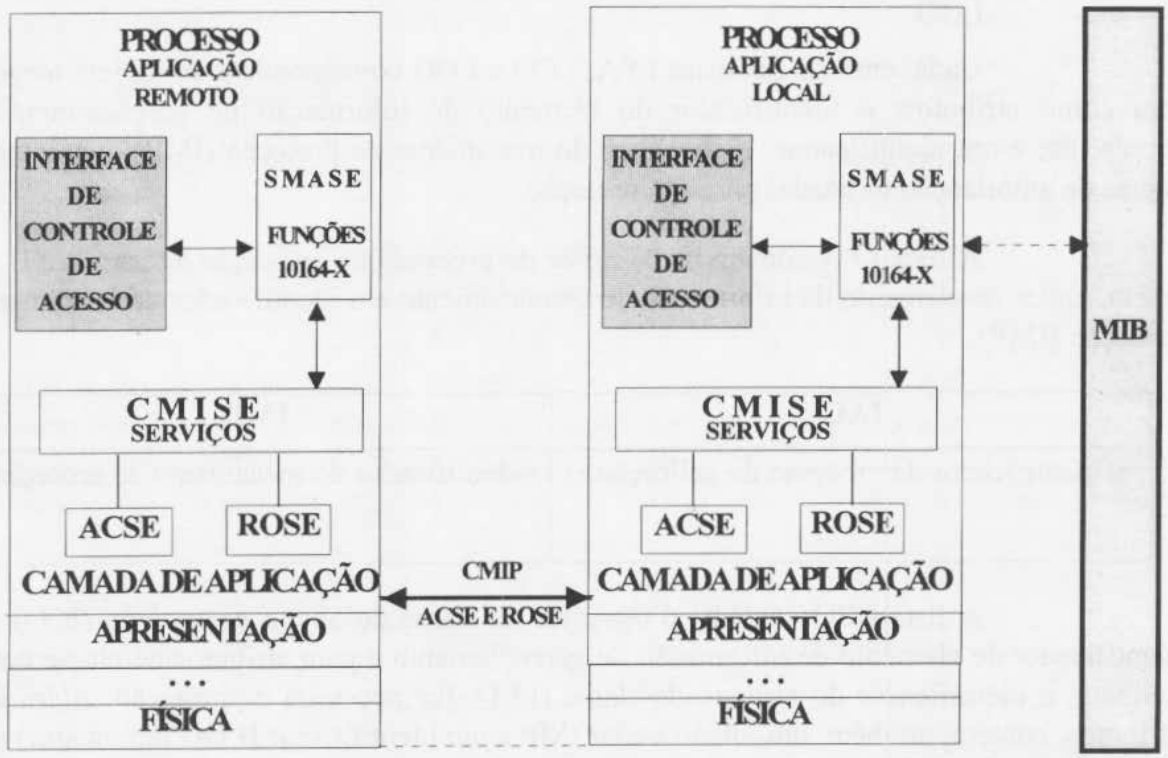


Figura 6 - Localização da Interface de Controle de Acesso

4.1 BASE DE DADOS DE AUTORIZAÇÃO

A Base de Dados de Autorização (BDA) é formada pelo conjunto de objetos *target* que representam os elementos de informação de gerenciamento que necessitam de proteção de acesso. Como o serviço de controle de acesso é requerido a nível de associação e a nível de operação de gerenciamento, a Interface de Controle de Acesso permite a criação de objetos *target* para processos de aplicação, classes de objetos gerenciados, atributos de classes de objetos gerenciados e instâncias de classes de objetos gerenciados.

Os objetos *target* ficam armazenados em listas específicas:

- Lista para Processos de Aplicação (LPA): contém os objetos *target* que representam os processos de aplicação que necessitam de controle de acesso a nível de associação de gerenciamento;
- Lista para Classes de Objetos Gerenciados (LCO): contém os objetos *target* que representam as classes de objetos gerenciados e atributos de classe de objetos gerenciados que necessitam de proteção a nível de operação de gerenciamento. Esta lista tem associada as regras globais de proteção de todas as instâncias da classe;
- Lista para Objetos Gerenciados (LOG): contém as instâncias de classe que necessitam de proteção. Esta lista é opcional e é vinculada a lista LCO. Se uma particular instância de uma classe da lista LCO necessitar de regras de proteção

específicas (Item Rules), será incluída através de um objeto *target* na lista LOG.

Cada entrada das listas LPA, LCO e LOG corresponde a um objeto *target* que tem como atributos: o identificador do elemento de informação de gerenciamento que representa; e um identificador (apontador) do mecanismo de proteção (IMP) que contém as regras de autorização utilizadas para sua proteção.

A lista LPA contém o descritor de processo de aplicação agente (IAG) como identificador de elemento de informação de gerenciamento e o identificador do mecanismo de proteção (IMP).

IAG	IMP
< identificador de processo de aplicação>	<identificador do mecanismo de proteção>

A lista LCO contém o descritor da classe de objeto gerenciado (ICO) como identificador de elemento de informação de gerenciamento e para atributos de classe contém, também, o identificador do atributo de classe (IAT) que necessita de proteção. Além destes atributos, contém, também, um identificador IMP e um identificador ILOG (apontador) para a lista opcional LOG.

ICO	IAT	IMP	ILOG
<identificador da classe do objeto>	<identificador do atributo da classe>	<identificador do mecanismo de proteção>	<identificador da lista opcional LOG>

A lista opcional LOG contém o descritor do objeto gerenciado IOG como identificador do elemento de informação de gerenciamento, ou seja, a instância da classe que necessita de regras específicas, e um identificador IMP que aponta para o mecanismo de acesso utilizado para proteger a instância.

IOG	IMP
<identificador de objeto gerenciado>	<identificador do mecanismo de proteção>

Se o objeto *target* fizer parte do domínio de segurança das políticas *Individual-based*, *Group-based* ou *Role-based* terá associado como mecanismo de proteção uma lista de controle de acesso (LCA). Este mecanismo permite a implementação destas políticas.

As listas LCA contém a identificação dos usuários (IdI) autorizados a manipular o elemento de informação de gerenciamento que objeto *target*, ao qual está associado, representa e contém, também, as informações de contexto (IC), ou seja, as

condições que a operação deve satizfazer para poder ser realizada (hora do dia, dia da semana, ...).

IdI	IC
<identificador de usuário>	< hora do dia, dias da semana, ...>

Caso o objeto *target* faça parte do domínio de segurança Multi-level ou Modelo Militar terá associado o mecanismo de rótulo. Os rótulos contém o nível de sensibilidade (NS) da informação e as informações de contexto (IC). No Modelo Militar, o rótulo contém, além destes atributos, o domínio (DOM) ao qual está vinculado o elemento de informação de gerenciamento que o objeto *target* representa.

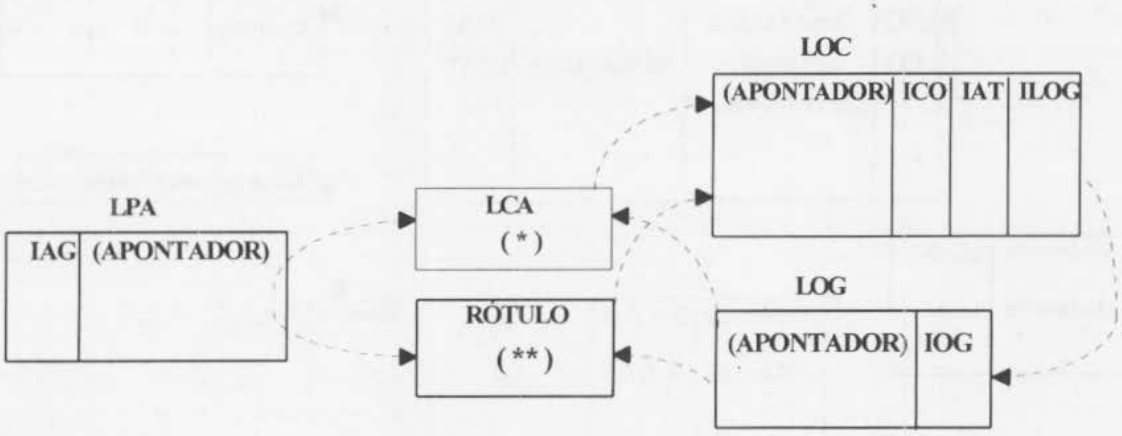
NS	IC
<identificador do nível de sensibilidade>	<hora do dia, dias da semana, ... >

Rótulo Multilevel

NS	DOM	IC
<identificador do nível de sensibilidade>	<domíno>	<hora do dia, dias da semana, ... >

Rótulo Modelo Militar

As listas LPA, LCO, LOG, LCA e o rótulo fazem parte dos mecanismos de segurança utilizados pela Interface de Controle de Acesso para implementar políticas de controle de acesso. Estes mecanismos encontram-se armazenados na base BDA e expressam as regras de autorização utilizadas pelo Sistema de Controle de Autorização (SCA) para definir se um pedido de acesso é válido ou não. O modelo genérico da base BDA é apresentado na Figura 7.



(*) - implementa políticas Individual-based, Group-based e Role-based

(**) - implementa políticas Multi-level e Modelo Militar

Figura 7 - Modelo Genérico da base BDA

Como exemplo de lista LPA, que contém objetos *target* para processos de aplicação, observe a Figura 8.

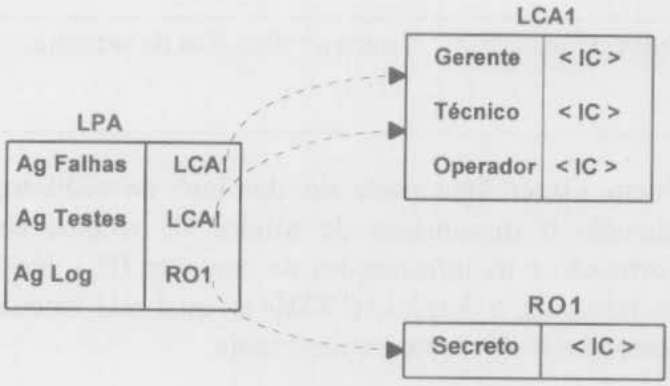


Figura 8 - Exemplo da lista LPA na base BDA

A Figura 9 apresenta um exemplo do relacionamento das listas LCO e LOG na base BDA.

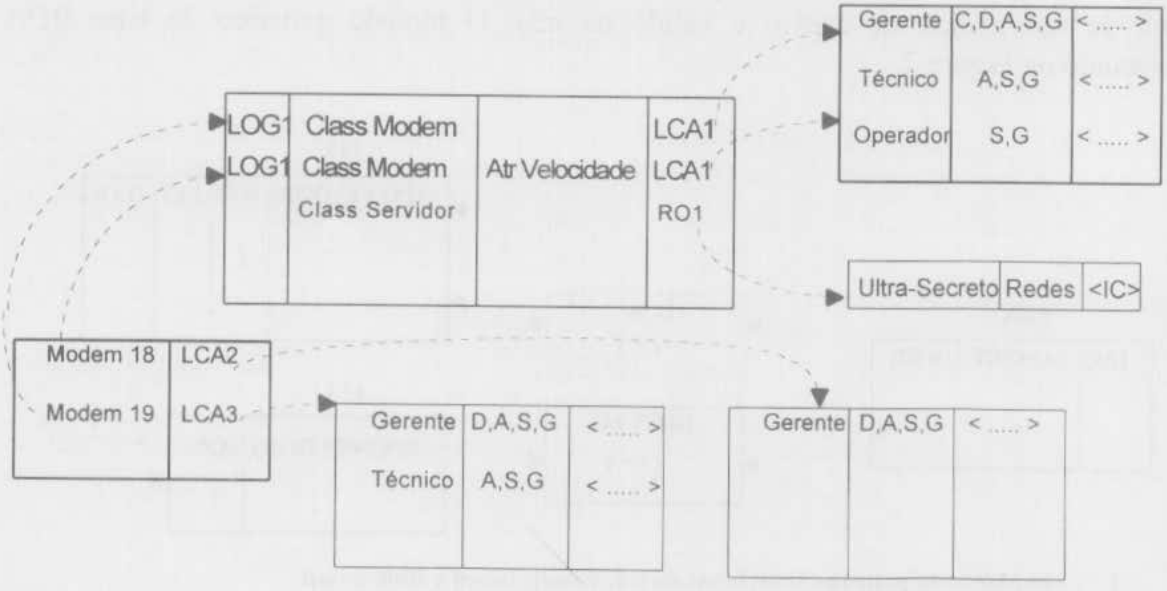


Figura 9 - Relacionamento das listas LCO e LOG na base BDA

4.2 SISTEMA DE CONTROLE DE AUTORIZAÇÃO (SCA)

O Sistema de Controle de Autorização (SCA) tem a funcionalidade de controle de acesso baseada na Função de Controle de Acesso [ISO 10164-9] e é composto pelas funções:

- *Access Control Enforcement Function* (AEF);
- *Access Control Decision Function* (ADF).

As funções AEF e ADF trabalham em conjunto com as listas LPA, LCO, LOG, LCA e o rótulo a fim de proteger os recursos de rede manipulados por um sistema de gerência. Não permitem que entidades desautorizadas estabeleçam associações e controlam as operações de gerenciamento sobre os objetos gerenciados, armazenados na MIB.

O sistema SCA, através da função ADF, trabalha como um motor de inferências que age sobre a Base de Definição de Autorização (BDA), usando uma estratégia de encadeamento para frente, onde decide se o pedido de acesso é permitido ou não.Estratégia de encadeamento para frente baseia-se em regras que codificam sobre como responder a certas configurações de entrada [RIC93].

A função AEF recebe os pedidos para estabelecimento de associação e para operações de gerenciamento. Seleciona os parâmetros importantes para o controle de acesso (identificador do iniciador; identificador da classe do objeto; identificador do objeto gerenciado; identificação do atributo da classe; operação de gerenciamento; hora; endereço; etc) e repassa-os para a função ADF. A função ADF é responsável por receber os parâmetros da função AEF e decidir se o pedido é valido ou não. Para isto, ele compara os parâmetros recebidos com as regras de autorização armazenadas na base BDA.

As inferências feitas pela função ADF, para decidir se um pedido de acesso é válido ou não, obedecem a seguinte ordem de precedência:

- para as asssociações de gerência, aplicam-se as regras contidas nos mecanismos de acesso (lista LCA ou rótulo) associados aos processos de aplicação integrantes da lista LPA. Caso o processo de aplicação, solicitado para associação, não esteja contido na lista LPA, a associação é, por *default*, permitida.
- para as operações de gerência, as regras aplicadas para decisão de acesso seguem os seguintes critérios:

1) Se um pedido de acesso é feito para um objeto que não se encontra na lista LCO, o acesso a este objeto é permitido;
2) Se um pedido de acesso é feito para um objeto que se encontra na lista LCO, deve-se fazer as seguintes considerações para decidir se o acesso a este objeto *target* é válido ou não:

a) Se existir lista opcional LOG associada a classe deste objeto, e a instância requerida deste objeto fizer parte desta lista opcional LOG, aplicam-se as regras contidas no mecanismo de acesso (lista LCA ou rótulo) associado à instância deste objeto gerenciado da lista opcional LOG;

b) Se existir lista opcional LOG associada a classe deste objeto, e a instância requerida deste objeto não fizer parte desta lista opcional LOG, então aplicam-se as regras contidas no mecanismo de acesso (lista LCA ou rótulo) associado à classe do objeto gerenciado que se encontra na lista LCO.

Em outras palavras, quando a função AEF fornece os parâmetros, a função ADF faz referência às informações na base BDA e aplica as técnicas de encadeamento para frente [LEV88] [RIC93]. Esta técnica é descrita através de um conjunto de condições e consequências que nada mais são do que um sistema de regras do tipo *se / então*.

De acordo com o modelo da Função de Controle de Acesso [ISO 10164-9], a função ADF após negar um pedido de acesso, deve enviar, também, à função AEF, instruções de prosseguimento à negação, como por exemplo, enviar uma resposta negativa, ignorar o pedido de acesso ou simplesmente abortar a conexão.

4.3 SISTEMA DE DEFINIÇÃO DE AUTORIZAÇÃO (SDA)

O Sistema de Definição de Autorização (SDA) é uma ferramenta de apoio às autoridades de segurança. Permite que as regras de autorização de um sistema de gerência sejam definidas de forma automática, dentro de um ambiente simples e amigável.

O sistema SDA implementa serviços específicos para a manipulação dos mecanismos de segurança da Base de Dados de Autorização (BDA). É através do sistema SDA que a autoridade consegue administrar as regras de autorização armazenadas em forma de listas e rótulos na base BDA.

A modelagem da política de autorização, ou seja a definição de quem pode fazer o que, com quem, e quando, deve ser feita fora do escopo da Interface de Controle de Acesso, pois não é especificada pelo padrão OSI. Cabe à autoridade de segurança modelar suas necessidades da melhor maneira possível, a fim de obter o nível de segurança requerido para o seu sistema de gerência.

A autoridade de segurança define qual ou quais são as políticas de segurança adotadas em seu domínio, ou seja define a política a ser empregada nos agentes e nos objetos gerenciados que formam o domínio, estipulando as regras de associação e de operação de gerenciamento. Estas regras são armazenadas na base BDA através do sistema SDA.

O ambiente do sistema SDA oferece, ao administrador de segurança, as políticas de acesso descritas no item 3: *Individual-based* (Inb); *Group-based* (Grb); *Role-based* (Rob); *Multi-level* (Mls); *e Modelo Militar* (Mms) (ver Figura 10, n.1). Após selecionar a política a ser empregada, a autoridade de segurança escolhe qual a função que se deseja executar sobre a base BDA (*incluir, excluir, alterar e consultar*) (ver Figura 10, n.2).

Uma vez escolhida a política a ser adotada e a função a ser executada, o próximo passo é definir o domínio a ser manipulado (ver Figura 10, n.3). Para isto, informa-se o domínio de gerenciamento ao qual as regras de autorização ficarão vinculadas. Para finalizar o processo de configuração do ambiente de definição de autorizações, a autoridade de segurança escolhe qual tipo de acesso ele quer administrar: controle de acesso para

associação (LPA) ou controle de acesso para operações de gerenciamento (LCO e LOG) (ver Figura 10, n.4).

Depois da configuração do ambiente de autorização, a autoridade de segurança interage diretamente com o ambiente particular de cada política. Todos os ambientes particulares de cada política dividem-se em definições para as Listas de Processo Agente (LPA) e Listas de Classes e Atributos de Objetos Gerenciados (LCO). Cada ambiente destes, permite criar objetos para controle de acesso do domínio de gerenciamento ao qual estão vinculadas. Para isto, deve-se informar os parâmetros básicos necessários para a definição de um objeto *target* nestas listas (ex: identificador de agente; identificador de nível de sensibilidade; informações de contexto para a lista LPA da política *Multi-level.*

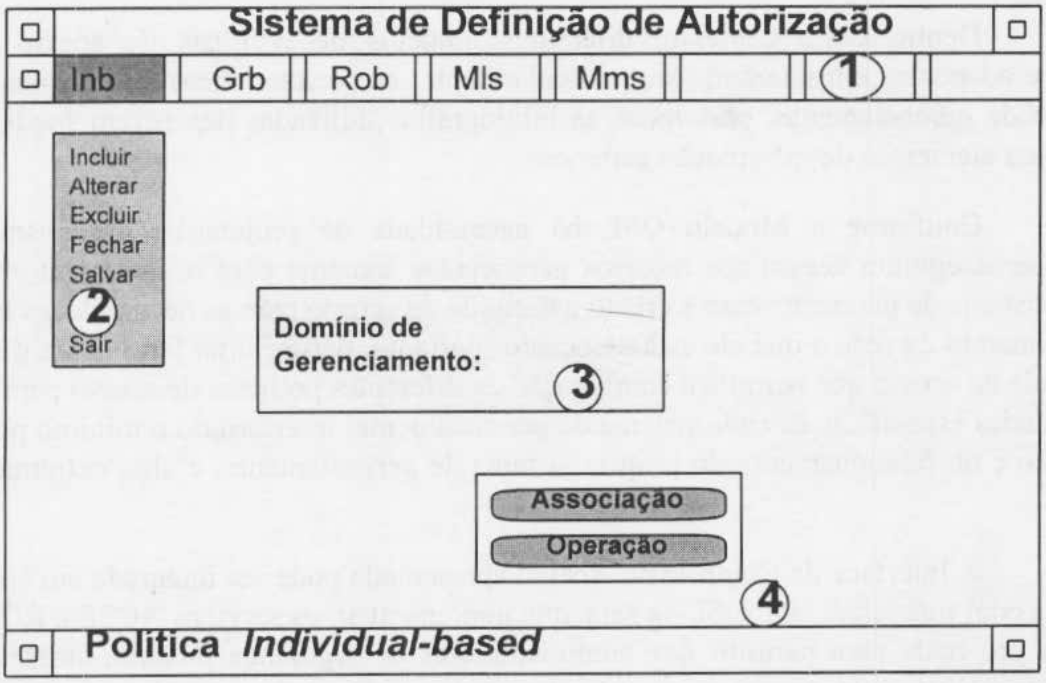


Figura 10 - Ambiente do sistema SDA

5. INTEGRAÇÃO DA INTERFACE À PLATAFORMA DE SUPORTE A GERÊNCIA DA REDE LOCAL UFSC

A Interface de Controle de Acesso faz parte do Projeto de Especificação e Implementação de uma plataforma de gerenciamento com funcionalidade OSI [THI93] que está sendo desenvolvido pelo Grupo de Redes de Computadores da Universidade Federal de Santa Catarina (UFSC).

A plataforma de gerenciamento é proposta para redes heterogêneas considerando, para tal, as normas da ISO através do Modelo de Referência OSI. Consiste de um suporte para o desenvolvimento de sistemas de gerência e não para implementação de um sistema de gerenciamento OSI especificamente.

A Interface de Controle de Acesso, por sua vez, consiste de ferramentas de suporte para implementação do serviço de controle de acesso para sistemas de gerência com funcionalidade OSI.

6. CONCLUSÕES

Este trabalho concentra-se no estudo dos aspectos relacionados com a Gerência de Segurança OSI e, em especial, com a Função de Controle de Acesso [ISO 1064-9] que implementa o serviço de controle de acesso para as informações de gerência armazenadas na MIB. A Função de Controle de Acesso requer que uma política de acesso seja definida para os elementos de informação de gerenciamento que necessitam de proteção.

Dentro deste contexto, diferentes modelos de políticas de acesso foram estudadas e adaptadas considerando-se, particularmente, as características dos elementos de informação de gerenciamento, pois todas as bibliografias utilizadas descrevem modelos de políticas para elementos de informação genéricos.

Conforme o Modelo OSI, há necessidade de projetar-se mecanismos de controle que assegurem acesso aos recursos gerenciados somente para usuários autorizados. Mas cada sistema de gerenciamento é criado e definido de acordo com as necessidades básicas de gerenciamento da rede a que ele está associado. Portanto, definir uma ferramenta genérica para controle de acesso que permita a combinação de diferentes políticas de acesso para suprir as necessidades específicas de cada sistema de gerenciamento, interferindo o mínimo possível na definição e no funcionamento do próprio sistema de gerenciamento, é algo extremamente complexo.

A Interface de Controle de Acesso apresentada pode ser integrada em sistemas de gerência com funcionalidade OSI, ou seja, que implementem os serviços ACSE e ROSE. A mesma foi projetada para permitir que administradores de segurança possam, através dela, implementar políticas de acesso para os recursos de gerência de uma forma amigável e transparente. Porém sua utilização requer, primeiramente, que a autoridade de segurança identifique, em seu sistema de gerenciamento, quais são as reais ameaças e contra as quais é necessário e vantajoso adotar-se medidas de proteção.

7. BIBLIOGRAFIA

[BRI93] BRISA, Gerenciamento de Redes: *Uma Abordagem de Sistemas Abertos*, Makron Books, São Paulo, 1993.

[FOR94] FORD, W., *Computer Communications Security: Principles, Standards Protocols and Techniques*, Prentice-Hall, New Jersey, 1994.

[ISO 7498] ISO/IEC - Information Processing Systems - Open Systems Interconnection - *Basic Reference Model*, Outubro, 1984.

[ISO 7498-2] ISO 7498-2 - Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: *Security Architecture*, Fevereiro, 1989.

[ISO 7498-4] ISO/IEC 7498-4 - Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 4: *Management Framework*, Novembro, 1989.

[ISO 10164-7] ISO/IEC DIS 10164-7 - Information Technology - Open Systems Interconnection - Systems of Management - Part 7: *Security Alarm Reporting Function*, Março, 1991.

[ISO 10164-8] ISO/IEC DIS 10164-8 - Information Technology - Open Systems Interconnection - Systems of Management - Part 8: *Security Audit Trail Function*, Novembro, 1990.

[ISO 10164-9] ISO/IEC CD 10164-9 - Information Technology - Open Systems Interconnection - Systems of Management - Part 9: *Objects and Attributes for Access Control*, Outubro, 1991.

[LEV88] LEVINE, R. I. et alli, *Inteligência Artificial e Sistemas Especialistas: Aplicações e Exemplos*, McGraw-Hill, São Paulo, 1988.

[LUC93] DE LUCCA, J. E., *Arquitetura para Segurança em Gerência de Redes*, Trabalho Individual - CPGCC UFSC, Santa Catarina, Dezembro, 1994.

[PFL89] PFLEEGER, C.P., *Security in Computing*, Prentice-Hall, New Jersey, 1989.

[RAM94] RAMOS, A. M., *Interface de Controle de Acesso para o Modelo de Gerenciamento OSI*, Dissertação de Mestrado - CPGCC UFSC, Santa Catarina, Agosto, 1994.

[RIC93] RICH, E. e KNIGHT, K., *Inteligência Artificial*, Makron Books, São Paulo, 1993.

[SOU92] DE SOUSA, R. T., *Arquitetura de Segurança e Gerência de Segurança no Modelo OSI*, Anais do 2. Congresso 3. Demonstração de Interoperabilidade de Sistemas Abertos (OSI 92), São Paulo, 1992.

[THI93] THIRY, M., *Definição de uma Plataforma de Gerenciamento para a Rede Local UFSC*, Dissertação Mestrado - CPGCC UFSC, Santa Catarina, Dezembro, 1993.