MACA: uma solução para autenticação de usuários e autorização de acesso em ambientes abertos e distribuídos

Gustavo H. M. B. Motta

Departamento de Informática – Universidade Federal da Paraíba – Brasil
e-mail: gustavo.motta@di.ufpb.br

1. O problema

Os recentes avanços nas áreas de comunicação e computação viabilizam, técnica e economicamente, a disponibilidade em larga escala de uma variedade de informações e de serviços computacionais, independente do local e do momento do acesso. A despeito dos inegáveis benefícios que traz, tal disponibilidade acarreta problemas em situações onde restringir o acesso é imperativo para resguardar a privacidade de indivíduos e organizações. É o que ocorre em aplicações corporativas emergentes, como as baseadas em tecnologias *web*, envolvendo negócios nos setores público e privado.

Aplicações corporativas emergentes são sistemas distribuídos que, muitas vezes, integram aplicações legadas, acessando bancos de dados distintos em plataformas heterogêneas. Demandam um controle de acesso com granularidade fina a informações e serviços para um grande número de usuários exercendo funções corporativas com diferentes privilégios, abrangendo múltiplas unidades organizacionais simultaneamente. Em geral, tais aplicações têm mecanismos próprios de autenticação de usuário e de controle de acesso implementados de forma estanque, com privilégios de acesso ligados diretamente a identidade de usuários ou a grupos. Problemas típicos decorrentes desse enfoque incluem:

- Custo elevado para administrar a concessão/revogação de autorizações de acesso para usuários que precisam acessar múltiplas aplicações corporativas no exercício de suas funções;
- Maior risco de usuários manterem/acumularem autorizações de acesso indevidas motivado pela dificuldade em remover privilégios de usuários que mudam de função ou que são desligados da corporação, seja funcionário, prestador de serviços, consultor ou outro vínculo temporário;
- Necessidade de conhecimentos técnicos, em geral, sem relação com o vocabulário da cultura organizacional, para concessão/revogação de privilégios a usuários. Conseqüentemente, essa tarefa passa à esfera do *staff* da área de TI (tecnologia da informação), quando deveria ser exercido por alguém da área de recursos humanos ou de uma área fim na corporação, com conhecimento efetivo das funções a serem exercidas pelos usuários;
- Dificuldade de impor a autenticação de usuários e políticas de acesso corporativas de forma unificada e coerente, independente de aplicações e plataformas. Como resultado, um usuário tem diversas contas em múltiplas aplicações, exigindo a memorização de numerosos *logins* e senhas.;
- Surgimento de situações de conflitos de interesses por ações "sensíveis" realizadas por um mesmo usuário. Por exemplo, um mesmo indivíduo pode, num sistema, solicitar um pagamento e em outro, considerar a solicitação válida, ordenando que se pague. É necessário, portanto, unificar políticas de acesso entre aplicações visando estabelecer políticas coerentes no âmbito das corporações, inclusive contemplando a separação de responsabilidades para evitar situações com a descrita anteriormente.

Por fim, a implementação isolada de mecanismos de autenticação e de autorização de acesso em aplicações corporativas dificulta assegurar/vefiricar a validade das políticas de segurança em vigor. Ademais, por propiciar maior risco de fraudes, erros, ataques e outras violações de segurança, é imperativo que as organizações busquem soluções para diminuir as chances de ocorrência desses problemas.

2. A solução do MACA

A meta do MACA (***M**iddleware* de **A**utenticação e **C**ontrole de **A**cesso) é prover os serviços de autenticação de usuário e de autorização de acesso para aplicações legadas ou em desenvolvimento, independente de plataforma e de linguagem de programação, através de uma API padronizada.

O MACA implementa um modelo de autorização contextual que estende o modelo de referência para o controle de acesso baseado em papéis proposto pelo NIST (*National Institute of Standards and Technology*) dos EUA. O CABP regula o acesso dos usuários aos recursos protegidos 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. As autorizações não são associadas diretamente a usuários, mas sim a papéis, de acordo com as atribuições pertinentes. Papéis é que são associados a usuários, segundo as funções que eles exercem.

Por exemplo, num hospital, se um usuário é um médico e tem o cargo de diretor clínico, ele terá os papéis *Médico* e *Diretor Clínico* associados. Conseqüentemente, seus direitos de acesso são os definidos para estes papéis, de acordo com a necessidade

de saber/fazer inerente a autoridade e responsabilidade de cada papel.

Uma autorização contextual permite ou proíbe o acesso com base na avaliação de *regra de autorização* durante uma tentativa de acesso. Regras são definidas em termos de variáveis ou funções ambientais disponíveis em contextos que denotam informações relevantes para implementar políticas de acesso específicas. Por exemplo, num hospital, pode-se definir uma autorização contextual definindo a seguinte política: *médicos só podem prescrever terapias para pacientes internados ou em atendimento na emergência*.

A arquitetura de software do MACA baseia-se em padrões de processamento aberto e distribuído a fim de alcançar interoperabilidade e portabilidade. Adota o serviço de diretórios LDAP como uma base de gerência de informações de segurança; o CORBA *Security Service* para autenticação e o serviço de decisão para acesso a recursos (RAD – *Facility*), do CORBA *horizontal facilities*, como soluções de *middleware* para autenticação de usuários e solicitação de autorizações de acesso, respectivamente, por parte das aplicações clientes. É uma solução escalável que viabiliza a administração da política de acesso de modo unificado e coerente, a partir de diferentes sistemas, em plataformas e linguagens de programação distintas, e de forma padronizada. Está também prevista a disponibilidade destes serviços através de *Web Services* a fim de aumentar a interoperabilidade da solução.

2.1. Principais vantagens

- As autorizações contextuais concedem ao MACA flexibilidade e poder expressivo para estabelecer políticas de acesso para as aplicações corporativas e de gestão de políticas administrativas para o CABP que se adaptam à diversidade ambiental e cultural das organizações;
- Suporta o princípio do privilégio mínimo, pelo qual, um usuário só tem os privilégios necessários para desempenhar suas funções, evitando-se assim que ele possa efetuar ações desnecessárias ou potencialmente danosas e que são autorizadas apenas como um efeito colateral;
- Permite configurar o conceito da "separação de responsabilidades" (SR), cuja meta é reduzir as chances de fraude ou dano acidental decorrentes da demasiada concentração de poder numa única pessoa. A SR distribui para vários usuários a responsabilidade e a autoridade para realizar uma tarefa suscetível de fraudes ou mau uso, de modo que um indivíduo não seja poderoso o suficiente para efetuá-la sem um conluio. A SR é usada para prevenir que um usuário realize ações em que há conflito de interesses e também pode se usada para **evitar a existência de "super usuários"**;
- Coloca a administração da política de acesso na perspectiva dos modelos organizacionais e não em função de plataformas tecnológicas específicas, possibilitando a redução direta e indireta dos custos administrativos e a imposição coerente da política nos diversos sistemas organizacionais;
- Implementa o conceito de *login* unitário para usuários, independente de plataforma ou aplicação. A partir de um único ponto de controle, pode-se criar/bloquear/remover contas de usuários (incluindo contas de *e-mail*) e conceder/remover privilégios utilizando-se o vocabulário da cultura organizacional.

3. Uso Industrial do MACA

O MACA, atualmente na versão 3.2, está em uso rotineiro e estável no Instituto do Coração do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo (InCor) desde o início de 2001, num esquema de funcionamento 24 × 7, sendo acessado por aproximadamente 1000 estações de trabalho. Os serviços de autenticação e autorização vêm sendo usados em missão crítica para controlar o acesso ao prontuário eletrônico do paciente (PEP) da instituição, composto por cerca de 40 aplicações, distribuídas e implementadas em plataformas heterogêneas, que incluem os sistemas operacionais LINUX (Suse), Windows e as linguagens de programação Oracle/Forms, Java, Java/JSP, Delphi e Magic. Cerca de 2200 usuários têm acesso controlado ao PEP, com diferentes privilégios, dependendo dos papéis associados, dentre os 66 papéis disponíveis.

O InCor é um centro de referência em cardiologia, com mais 20 anos de experiência desenvolvimento de sistemas de informação hospitalar e conta com cerca de 600 leitos, 2.600 funcionários e 300 profissionais temporários (residentes ou estagiários) que realizam por mês, aproximadamente, 300 cirurgias, 11.600 procedimentos de diagnóstico por imagem e 100.000 exames laboratoriais, dentre outras atividades.

4. Licenciamento do MACA

A implementação do MACA está disponível como software livre sob licença GNU GPL no sítio http://*maca.sourceforge.net/*. Possui manuais para instalação e configuração e tutoriais de utilização. Entretanto, a utilização em ambientes corporativos mais complexos requer um processo sistemático de análise de requisitos para implementação de políticas de acesso, considerando o ambiente a cultura das organizações.