5
Conclusão

Neste trabalho apresentamos a proposta de uma arquitetura para a autenticação e o controle de acesso interinstitucional baseado no uso de papéis. Abordagens tradicionais de gerenciamento de usuários em multi-organizações empregam a replicação do cadastro dos usuários nos diversos domínios de acesso ou o compartilhamento de contas. O objetivo da arquitetura é contornar os problemas comumente causados por essas abordagens.

A adoção de um modelo centralizado em um cenário envolvendo diversas instituições na maioria dos casos se torna inviável. A nossa proposta de usar um bilhete assinado digitalmente para a autenticação, inspirado no Kerberos, distribui a responsabilidade do controle pelos membros da federação. Assim, cada organização fica responsável por verificar e atestar a validade de seus usuários. Essa mesma filosofia de dividir a responsabilidade sobre os usuários também é utilizada pelo Shibboleth, que agrupa as organizações em federações, e através da relação de confiança entre elas é possível realizar acessos a recursos de outras instituições.

A identificação dos usuários via papéis traz vantagens para a manutenção das permissões. O modelo de controle baseado em papéis do NIST agrupa os usuários em classes (papéis) e simplifica a atribuição dos direitos. Ao estendermos esse modelo adicionando mais um nível de mapeamento, entre papéis externos e internos, permitimos que papéis de diferentes organizações possam ser tratados da mesma forma, criando um conceito de equivalência entre eles. Assim, um administrador define e mantém os direitos de um conjunto pequeno de papéis internos e, então, estabelece uma relação entre os papéis externos e algum papel desse conjunto, propagando automaticamente as permissões.

Lidamos também com a questão de privacidade, que leva à escassez de informações para a validação do usuário, decorrente, por exemplo, de políticas institucionais. Por isso, a arquitetura evita o uso de identificadores pessoais tanto na autenticação quanto no controle de acesso.

Algumas das tecnologias estudadas que abordam a autenticação entre

domínios não fornecem componentes flexíveis que permitam o acoplamento com o ambiente já instalado nas organizações, forçando a utilização de mecanismos específicos para a identificação do usuário. O modelo proposto neste trabalho emprega pontos de flexibilização que as instituições adaptam de acordo com seus recursos disponíveis. Implementamos dois estudos de casos, um para o serviço FTP e outro para o serviço LDAP, que mostram como diferentes tecnologias podem ser utilizadas.

O objetivo também com o cenário do LDAP, era analisar o funcionamento do Shibboleth como mecanismo de autenticação. A primeira versão da aplicação web recebia as credenciais do usuário através de uma página de *login* e ficava responsável por contactar a instituição de origem para garantir a identidade do usuário. Essa abordagem requer que a aplicação seja confiável pois ela manipula diretamente as credenciais. O papel do Shibboleth é retirar essa exigência, fazendo com que toda interação entre usuário e organização de origem seja direta. Desse modo, a preocupação sobre a legitimidade da aplicação pode não ser tão grande, visto que ela irá manipular apenas os atributos disponibilizados via Shibboleth. E caso uma aplicação obtenha um bilhete indevidademente, o mecanismo de *leasing* 3.1 reduz o período em que ele pode ser usado.

No estudo de caso utilizando o serviço LDAP, a implementação do mecanismo de autenticação para suportar o bilhete foi feita de forma ortogonal, não havendo a necessidade de realizar alterações no servidor OpenLDAP. Entretando, no caso do FTP foram realizadas adptações na implementação servidor para que o mesmo pudesse interagir com a arquitetura. Um ponto a ser investigado é como fornecer meios para que as aplicações legadas possam utilizar a arquitetura sem a necessidade de sofrer alterações no seu código. Essa invertigação pode considerar o uso de um módulo ou uma biblioteca que faça a ponte entre as aplicações e a arquitetura.

Um cenário não explorado, mas no qual acreditamos ser interessante aplicar a arquitetura proposta, é o de grade computacional. A distribuição geográfica e multi-institucional que envolve o conceito de grade, juntamente com a necessidade de manter um controle sobre o uso dos recursos internos, se encaixam bem nos requisitos do modelo.

Em determinadas situações, principalmente envolvendo sistemas distribuídos, é importante dispor de um mecanismo de delegação, permitindo aos usuários repassar seus direitos, ou partes deles. Por exemplo, aplicações podem necessitar de acesso a recursos em nome do usuário – comum no ambiente de grade de computacional. Um tópico para trabalhos futuros é estudar os mecanismo de delegação já existentes, como o repasse de bilhe-

tes e TGTs do Kerberos ou o certificado *proxy* empregado pelo Globus, e analisar meios de incluir delegação na arquitetura, mantendo as características estabelecidas (simplicidade no controle de acesso, anonimato, auditoria, etc).