1
Introdução

Nos últimos anos, a computação distribuída vem se expandindo das redes locais das organizações para um cenário maior, alcançando e englobando grupos de instituições com interesses em comum e dispostas a uma interação mais ativa.

Esse crescente interesse de integração e colaboração, principalmente de ensino e pesquisa, tem levado grupos como o MACE da Internet2 e TF-AACE (*Task Force on Authentication and Authorisation Coordination for Europe*), dentre outros, a pesquisarem e proporem meios para promover e garantir a segurança nessa colaboração multi-organizacional. Entretanto, o envolvimento de tipos variados de serviços, recursos e requisitos torna essa tarefa complicada.

Uma das questões principais em segurança é o controle de acesso a diferentes recursos. O primeiro passo para determinar as permissões de uso dos recursos recai sobre a identificação do usuário. As abordagens comuns são replicar o cadastro dos usuários nas instituições e compartilhar identidades entre grupos de usuários. Ambas apresentam deficiências, seja pelo esforço em manter o cadastro atualizado ou pela imprecisão na identificação do requisitante externo. Além disso, em se tratando de um cenário envolvendo diferentes organizações, políticas de privacidade interferem nesse processo de identificação, limitando a quantidade de informações disponíveis sobre o usuário remoto.

A próxima etapa é a extração dos direitos efetivos para cada identidade que requisita acesso. O controle de acesso baseado em papéis vem se destacando pela sua flexibilidade e simplicidade. Estudos indicaram que a atribuição das permissões a papéis [21, 25] desempenhados pelos indivíduos, de um modo geral, se mostra mais vantajosa para a manutenção; o relacionamento de direitos com papéis e papéis com indivíduos se torna mais compreensível e simples de ser mantido.

Neste trabalho propomos uma arquitetura que utiliza o conceito de papéis para a autenticação e controle de acesso interinstitucional. Estuda-

mos sistemas que abordam a segurança entre diferentes domínios, analisando suas características positivas e negativas, para elaborar a proposta. A arquitetura se baseia em uma relação de confiança firmada entre as organizações, possibilitando aos usuários se autenticarem em suas instituições e acessarem recursos em outros domínios. Isso é realizado através de um bilhete digital emitido pela organização de origem do usuário, que atesta o papel por ele desempenhado. As demais instituições utilizam esse bilhete e o papel para estabelecer os direitos.

O conceito de remeter os usuários para autenticação em suas organizações de origens vem do Shibboleth [4, 32], que visa promover a segurança no domínio web, cujo modelo serviu como base para a proposta. No entanto, a nossa arquitetura tem por objetivo generalizar esse conceito para que o mesmo possa ser utilizado em outros domínios, cobrindo outras formas de interação entre as instituições.

Apesar de estarmos tratando classes de usuários através dos papéis, o que reduz número de identidades a serem controladas, num contexto com diversas organizações, esse número ainda pode ser alto. Analisaremos uma extensão ao modelo tradicional de controle de acesso baseado em papéis, que introduz um segundo nível de mapeamento, ligando papéis externos à organização com papéis definidos localmente. Cada instituição define e atribui permissões a um conjunto interno de papéis e relaciona os papéis externos com algum papel desse conjunto. O objetivo é reduzir o esforço de gerência dos direitos, simplificando a inclusão ou exclusão de novas organizações, e seus papéis, no ambiente de colaboração.

O capítulo 2 apresenta as tecnologias que abordam a questão de autenticação inter-domínios e controle de acesso. No capítulo 3, descrevemos os elementos de nossa proposta para autenticação e controle de acesso interinstitucional. A seguir, o capítulo 4 descreve dois estudos de caso empregando essa proposta. O primeiro caso cobre o serviço de diretórios LDAP, que foi o motivante para o desenvolvimento deste trabalho. O segundo aborda o serviço de transferência de arquivos FTP. Finalmente, no capítulo 5 apresentamos as conclusões finais e trabalhos futuros.