

Bruno Oliveira Silvestre

**Autenticação e Controle de
Acesso Interinstitucional**

DISSERTAÇÃO DE MESTRADO

DEPARTAMENTO DE INFORMÁTICA

Programa de Pós-graduação em
Pós-graduação em Informática

Rio de Janeiro
Março de 2005

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO



Bruno Oliveira Silvestre

**Autenticação e Controle de Acesso
Interinstitucional**

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Pós-graduação em Informática do Departamento de Informática da PUC-Rio

Orientador: Prof. Noemi Rodriguez

Rio de Janeiro
Março de 2005



Bruno Oliveira Silvestre

**Autenticação e Controle de Acesso
Interinstitucional**

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Pós-graduação em Informática do Departamento de Informática do Centro Técnico Científico da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Noemi Rodriguez

Orientador

Departamento de Informática — PUC-Rio

Prof. Guido Lemos de Souza Filho

UFPB

Prof. Renato Fontoura de Gusmão Cerqueira

PUC-Rio

Prof. Sérgio Colcher

PUC-Rio

Prof. José Eugenio Leal

Coordenador Setorial do Centro Técnico Científico —

PUC-Rio

Rio de Janeiro, 21 de Março de 2005

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador.

Bruno Oliveira Silvestre

Bacharel em Ciência da Computação pela Universidade Federal do Espírito Santo.

Técnico em Processamento de Dados pela Escola Técnica Federal do Espírito Santo.

Ficha Catalográfica

Silvestre, Bruno Oliveira

Autenticação e Controle de Acesso Interinstitucional/ Bruno Oliveira Silvestre; orientador: Noemi Rodriguez. — Rio de Janeiro : PUC–Rio, Departamento de Informática, 2005.

v., 56 f: il. ; 30 cm

1. Dissertação (mestrado) - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática.

Inclui referências bibliográficas.

1. Informática – Teses. 2. Autenticação. 3. Controle de acesso. 4. Segurança. 5. Controle de acesso baseado em papéis. 6. Autenticação interinstitucional. I. Rodriguez, Noemi. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

CDD: 004

Agradecimentos

Agradeço aos meu pais e meus irmãos por todo o apoio dado. Mesmo distante, a presença de espírito deles foi motivante para a conclusão de mais esta etapa da minha vida.

À Profa. Noemi Rodriguez por ter sido mais que uma orientadora de mestrado, me ajudando não só no desenvolvimento deste trabalho mas também em decisões difíceis da minha vida.

À CAPES pela bolsa de fomento concedida, sem a qual nada disso seria possível.

Aos meus amigos de classe e de república pelos momentos de descontração e pelo enriquecimento cultural.

Resumo

Silvestre, Bruno Oliveira; Rodriguez, Noemi. **Autenticação e Controle de Acesso Interinstitucional**. Rio de Janeiro, 2005. 56p. Dissertação de Mestrado — Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

O uso de computação distribuída vem expandindo seu escopo, saindo de aplicações em redes locais para aplicações envolvendo diversas instituições. Em termos de segurança, essa expansão introduz desafios em identificar usuários oriundos das diferentes organizações e definir seus direitos de acesso a determinado recurso.

Abordagens comuns adotam a replicação do cadastro dos usuários pelas diversas instituições ou o compartilhamento de uma mesma identidade por um conjunto de usuários. Entretanto, essas estratégias apresentam deficiências, demandando, por exemplo, maior esforço de gerência por parte dos administradores e até esbarrando em políticas de privacidade.

Neste trabalho propomos uma arquitetura que utiliza o conceito de papéis para a autenticação e o controle de acesso entre diferentes instituições. Baseado em uma relação de confiança entre as organizações, a arquitetura permite que os usuários sejam autenticados nas instituições onde estão afiliados e utiliza o papel por eles desempenhados para controlar o acesso aos recursos disponibilizados pelas demais organizações.

Palavras-chave

Autenticação; Controle de Acesso; Segurança; Controle de Acesso Baseado em Papéis; Autenticação Interinstitucional

Abstract

Silvestre, Bruno Oliveira; Rodriguez, Noemi. **Interinstitutional Access: Authentication and Access Control**. Rio de Janeiro, 2005. 56p. MSc. Dissertation — Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Distributed computing has been expanding its scope from local area network applications to wide-area applications, involving different organizations. This expansion implies in several new security challenges, such as the identification of users originating from different organizations and the definition of their access rights.

Common approaches involve replicating user data in several institutions or sharing identities among sets of users. However, these approaches have several limitations, such as the increased management effort of administrators or problems with privacy policies.

This work proposes a framework for inter-institutional authentication. The framework is based on the concepts of RBAC (role-based access control) and of trust between organizations.

Keywords

Authentication; Access Control; Security; Role Base Access Control, Inter-institutional Authentication

Conteúdo

1	Introdução	10
2	Tecnologias Relacionadas	12
2.1	Kerberos	12
2.2	Shibboleth	15
2.3	Globus	18
2.4	Controle de Acesso Baseado em Papéis	20
3	Proposta	24
3.1	Autenticação	25
3.2	Direitos de Acesso	27
3.3	Privacidade e Auditoria	29
3.4	Flexibilidade da Arquitetura	29
4	Estudos de Caso	31
4.1	LDAP	31
4.2	FTP – File Transport Protocol	41
5	Conclusão	46
A	Aplicação de Busca de Informações sobre Vídeos	52

Lista de Figuras

2.1	Autenticação via Kerberos.	13
2.2	Componentes da arquitetura do Shibboleth.	16
2.3	Uso do certificado <i>proxy</i> na solicitação de serviço.	19
2.4	Modelo CABP ₀	21
3.1	Arquitetura proposta.	25
3.2	Mapeamento entre papéis externos e locais.	28
4.1	Exemplo da definição de um atributo e de uma classe de objeto.	33
4.2	Exemplo de uma entrada LDAP.	33
4.3	Exemplo de uma estrutura do diretório LDAP.	34
4.4	Aplicação de busca sobre informações.	36
4.5	Protocolo de autenticação através do bilhete.	39
4.6	Exemplo dos atributos <i>saslAuthzTo</i> e <i>saslAuthzFrom</i> .	40
4.7	Esquema utilizado no mapeamento de papéis.	41
4.8	Arquitetura para o FTP.	42
4.9	Definição do atributo e classe de objeto para o LDAP.	43
4.10	Autenticação no serviço FTP.	44
A.1	Aplicação para recuperação de informações sobre vídeos	52
A.2	Serviço WAYF provido pelo Shibboleth.	53
A.3	Janela de autenticação do usuário.	54
A.4	Interface para a realização da busca.	55
A.5	Resultado de um busca.	55
A.6	Informações detalhadas sobre o vídeo.	56

[...] Em outros momentos, como agora, quando a estática patentemente carecia de regularidade, ela recordava o famoso axioma de Shannon sobre a teoria da informação: a mensagem codificada de maneira mais eficiente era indistinguível do ruído se o receptor não dispusesse, de antemão, da chave para a decodificação.

[...]

“O tempo necessário para se praticar a física é um luxo”, ele disse a Ellie. “Há muitas pessoas que seriam capazes do mesmo se tivessem oportunidades. No entanto, se você tem de bater as ruas atrás de comida, não dispões de tempo suficiente para a física. Eu tenho a obrigação de melhorar as condições de vida dos jovens cientistas em meu país.”

Carl Sagan, *Contato*.