



Serviço de Segurança CORBA

André Dantas Vieira
Universidade Federal de Pernambuco
Centro de Informática
Seminário de Redes e Sistemas Distribuídos
2004.1



Roteiro

- ❖ Introdução
- ❖ Segurança em Objetos Distribuídos
- ❖ Segurança CORBA
- ❖ Serviços de Segurança CORBA
- ❖ Conclusão
- ❖ Referências



Introdução

- ❖ Segurança é um requerimento essencial em ambientes de objetos distribuídos
- ❖ Em 1996, a OMG libera o Serviço de Segurança
- ❖ Framework de Segurança
 - ✓ Interno ao ORB
 - ✓ Transparência para o desenvolvedor
 - ✓ Padronização permite portabilidade de objetos provenientes ambientes distintos
 - ✓ Administradores devem ter conhecimentos das políticas de segurança



Segurança de Objetos Distribuídos

- ❖ Mais inseguro que ambientes Cliente/Servidor
- ❖ Objetos distribuídos:
 - ✓ Podem ser clientes e servidores
 - ✓ Interações não são totalmente perceptíveis
 - ✓ Interações menos previsíveis
 - ✓ Polimorfismo
 - ✓ Escalabilidade
 - ✓ Dinamismo
- ❖ Solução
 - ✓ Implementação interna no ORB



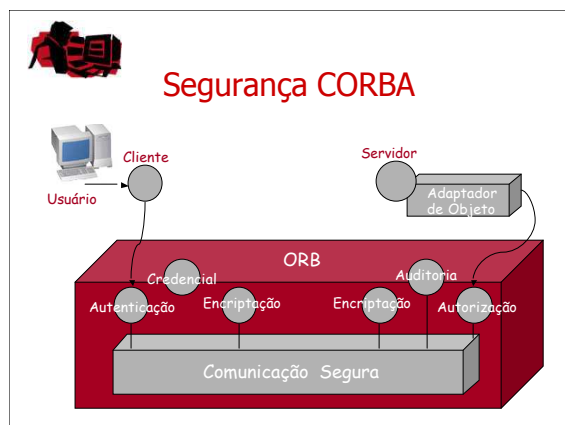
Segurança CORBA

- ❖ Maioria dos objetos não tem consciência das políticas de segurança e da implementação destas pelo ORB
- ❖ Especificação permite mudança de níveis de segurança



Segurança CORBA

- ❖ Serviços de Segurança
 - ✓ Autenticação
 - ✓ Delegação
 - ✓ Autorização
 - ✓ Auditoria
 - ✓ Não Repudição
 - ✓ Não Alteração
 - ✓ Domínios



Autenticação

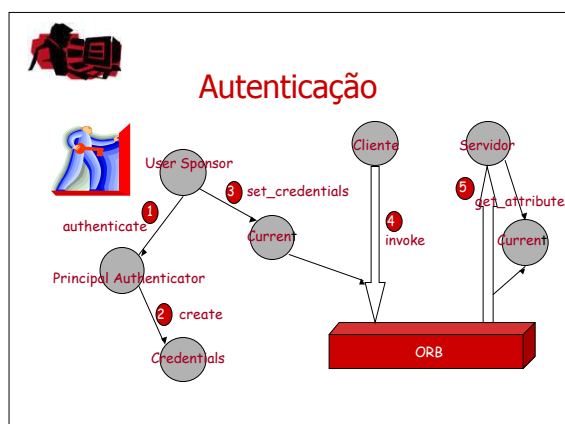
- ❖ Primeira ação ser tomada pelo cliente
- ❖ Cliente é chamado de Principal
 - ✓ Usuário ou Objeto autenticado pelo ORB
 - ✓ Possui Credenciais
- ❖ Credenciais
 - ✓ Id de autenticação
 - ✓ Classe
 - ✓ Privilégios

Autenticação

- ❖ Necessidade de uma única autenticação
 - ✓ Contexto de Segurança
- ❖ Contexto de Segurança
 - ✓ Controlado internamente pelo ORB
 - ✓ Transparência para o Principal
- ❖ Mecanismo de Autenticação
 - ✓ Kerberos
 - ✓ Chaves Pública
 - ✓ Smart cards

Autenticação

- ❖ Passos para Autenticação
 - ✓ Autenticar o Principal
 - ✓ Criar o objeto Credenciais
 - ✓ Associar a Credencial ao contexto de execução
 - ✓ Invocação de método seguro pelo Cliente
 - ✓ Servidor executa o método seguro

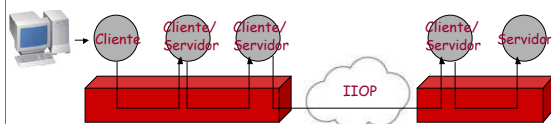


Delegação de Privilégios

- ❖ Necessária em sistemas de objetos distribuídos
 - ✓ Corrente de chamadas inter-objetos
 - ❖ Encadeamento de invocações
- ❖ Controle de acesso realizado em cada ponto da corrente
- ❖ Controle de Delegação
 - ✓ Explícito pelo cliente
 - ✓ Políticas de Delegação do ORB



Delegação de Privilégios



Delegação de Privilégios

- ❖ Esquemas de Delegação
 - ✓ Sem delegação
 - ✓ Delegação Simples
 - ✓ Delegação Composta
- ❖ Expiração de delegação
 - ✓ Temporal
 - ✓ Número máximo de invocações



Delegação de Privilégios

Sem Delegação



Delegação Simples



Delegação Composta



Autorização

- ❖ Granularidade no controle de acesso
 - ✓ Métodos
 - ✓ Objetos
 - ✓ Grupo de Objetos
- ❖ Trade-off
 - ✓ Overhead X Complexidade



Autorização

- ❖ Realizada nos objetos servidores
- ❖ Servidores usam ACLs para o controle de acesso
- ❖ Access Control List
 - ✓ Principals & Classes
 - ✓ Classes & Direitos
 - ✓ Direitos & Métodos



Autorização

- ❖ Controle de Acesso
 - ✓ Privilégios corrente do invocador
 - ✓ Qualquer controle aplicado a tais privilégios
 - ✓ Operação a ser invocada
 - ✓ Políticas de acesso no objeto alvo



Autorização

Principal	Classe
Fulano	Gerente
Sicrano	Funcionário
Beltrano	Cliente

Classe	Right
Gerente	get, set, create
Funcionário	get
Cliente	get, set

Right	Operação
get	get_address get_account_value get_credit_status
set	update_account update_credit write_check
create	transfer_account add_new_line_of_credit

Access Control Lists



Auditoria

- ❖ Monitoramento de eventos no ORB
- ❖ Peça no arsenal do administrador para detecção de intrusão
- ❖ Políticas de Auditoria
 - ✓ Eventos do sistema
 - ✓ Eventos da aplicação



Auditoria

- ❖ Possíveis eventos
 - ✓ Objeto ou tipo de objeto
 - ✓ Operação
 - ✓ Hora
 - ✓ Atributos do Principal
 - ✓ Sucesso ou falha em operações
- ❖ Políticas auxiliam o monitoramento de eventos necessários
 - ✓ Logs de auditoria podem crescer muito!!!



Não Repudição

- ❖ Evidência inquestionável da ocorrência de uma ação
 - ✓ Se uma invocação ocorreu realmente, e quem a realizou
- ❖ Bastante discutido em E-Commerce
- ❖ ORB provê:
 - ✓ Provas de envio
 - ✓ Provas de recebimento

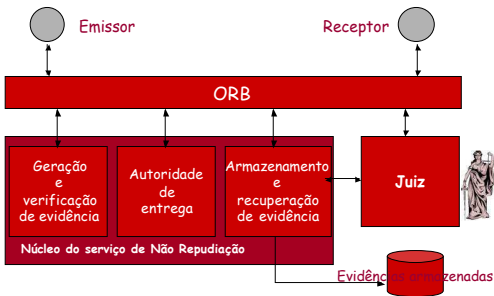


Não Repudição

- ❖ Framework de serviços:
 - ✓ Evidência de criação de mensagem
 - ✓ Evidência de recebimento de mensagem
 - ✓ Armazenamento de evidências
 - ✓ Juiz



Não Repudição





Não Alteração

- ❖ Mecanismos adotados pelo ORB
 - ✓ Encriptação
 - ✓ Checksum s criptografados
- ❖ Qualidade de proteção designada pelos mecanismos adotados
- ❖ Request e Response podem ter mecanismos diferentes



Não Alteração

- ❖ Especificação permite a adoção de mecanismos padrões da indústria
 - ✓ RSA
 - ✓ Kerberos
 - ✓ SSL

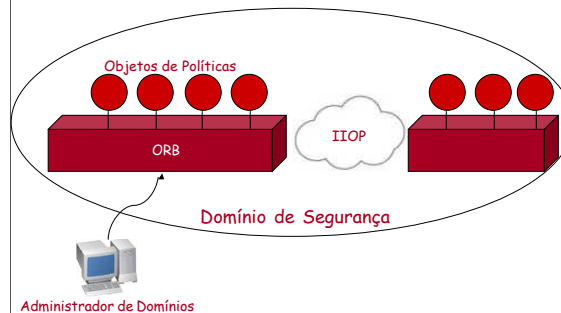


Domínios

- ❖ Definição
 - ✓ Conjuntos de objetos sujeitos a certas políticas de segurança, e administrados por uma autoridade
- ❖ Políticas são as regras e critérios que restringem as ações dos objetos
- ❖ Políticas são administradas pelo Administrador do domínio



Domínios



Domínios

- ❖ Tipos de domínios
 - ✓ Sub-Domínios
 - ✓ Domínios Confiáveis
- ❖ Interação entre Domínios
 - ✓ Interoperable Object Reference
 - ❖ Define a segurança e mecanismos utilizados pelo objeto
 - ✓ Transmissão de contexto nas mensagens do Inter Orb Object Protocol
- ❖ Objetos de domínios diferentes devem usar a mesma tecnologia de segurança



Conclusão

- ❖ Especificação de Segurança bastante ampla, abrangendo praticamente todos os serviços de segurança existentes
- ❖ Especificação bastante complexa, e muitas vezes abstrata demais
- ❖ Decisões de implementação por parte dos desenvolvedores são vitais para evitar o excesso de complexidade, e para prover um serviço de segurança confiável



Referências

- ❖ Instant CORBA – Robert Orfali, Dan Harkley, Jeri Edwards
- ❖ Security Service v1.8 - OMG



Serviço de Segurança CORBA

André Dantas Vieira
Universidade Federal de Pernambuco
Centro de Informática
Seminário de Redes e Sistemas Distribuídos
2004.1