Defesa de mestrado

Um serviço de autorização Java EE baseado
em certificados de atributos X.509

Stefan Neusatz Guilhen

Introdução

- **Segurança:** autenticação, autorização, proteção dos dados
- **Plataforma Java EE:**
 - JAAS, JSSE, RBAC
 - Modelo de gerenciamento de privilégios restrito
 - Ausência de autoridade de privilégios
- **Padrão X.509:**
 - Certificados de atributos X.509
 - Modelo de gerenciamento flexível
 - Garantias de integridade e origem
 - Favorecimento à distribuição

Trabalhos relacionados

- **Akenti**: gerenciamento distribuído de políticas de controle de acesso
- Autenticação exclusivamente por CCPs
- Certificados de atributos proprietários

Trabalhos relacionados

- **PERMIS**: controle de acesso baseado em papéis
- Autenticação flexível
- Autorização baseada em certificados de atributos X.509
 - Atributo não padronizado para papéis
 - Certificados armazenados em serviços de diretório LDAP
 - Gerador de certificados depende de código proprietário

Trabalhos relacionados

- **SESAME**: autorização baseada em certificados com tempo de validade restrito
- Autenticação por *Kerberos* ou CCPs
 - Tíquete gerado a cada autenticação
- Privilege Attribute Server
 - Troca tíquetes por certificados contendo papéis
 - Atribui certificados diretamente ao usuário

Trabalhos relacionados

- **CORBASec**: arquitetura de segurança não intrusiva.
- Definição do serviço por interfaces
- PrincipalAuthenticator:
 - Abstração mecanismo de autenticação
 - Associa identidades ao SecurityCurrent
- AccessControlInterceptor
 - Controle de acesso no cliente e no servidor
- SecureInvocationInterceptor
 - Proteção da camada de transporte

Infra-estrutura de gerenciamento de privilégios

- Evolução da infra-estrutura de chaves públicas X.509
 - Atributos e privilégios separados do CCP
- Certificados de atributos
 - Tempo de vida independente da chave pública
 - Gerenciados por autoridades específicas
- Flexível quanto à autenticação
 - Integração com os CCPs
 - Outros mecanismos

Certificado de atributos X.509

- RFC 3281

```
AttributeCertificate ::= SEQUENCE {  
    acinfo          AttributeCertificateInfo,  
    signatureAlgorithm AlgorithmIdentifier,  
    signatureValue   BIT STRING  
}
```

```
AttributeCertificateInfo ::= SEQUENCE {  
    holder          Holder,  
    issuer          AttCertIssuer,  
    serialNumber    CertificateSerialNumber,  
    attrCertValidityPeriod AttCertValidityPeriod,  
    attributes      SEQUENCE OF Attribute,  
    extensions      Extensions OPTIONAL  
}
```


Implementação: infra-estrutura de segurança do JBoss 4

- Visão geral

Implementação: infra-estrutura de segurança do JBoss 4

- Processo de autenticação

Implementação: infra-estrutura de segurança do JBoss 4

- Processo de autorização

Implementação: infra-estrutura de segurança do JBoss 4

- Módulos JAAS autenticam e obtém os papéis dos usuários
 - UsersRolesLoginModule (arquivos)
 - DatabaseServerLoginModule (banco de dados)
 - LdapLoginModule (serviço de diretórios)
 - BaseCertLoginModule (autenticação via CCP)
- Configurações em conjunto
 - Módulos que apenas autenticam
 - Módulos que apenas obtém papéis

Implementação: visão geral

- Gerador de certificados de atributos X.509
 - Escassez de ferramentas
- Extensão da infra-estrutura do JBoss
 - Implementação dos modelos *pull* e *push*
- Verificadores de revogação
 - Verificação por *OCSP* e *CRL*
- Mapeamento de papéis
- Estudo comparativo de desempenho

Implementação: ACGenerator

- Arcabouço para geração de certificados de atributos X.509 e CRLs

Implementação: modelo Pull

- X509ACPullLoginModule

Implementação: modelo Pull

- Diagrama de colaboração

Implementação: modelo Push

- Somente para componentes *EJB*
- Primeira etapa: passagem dos certificados

Implementação: modelo Push

- Diagrama de classes

Implementação: modelo Push

- Diagrama de colaboração
- Autenticação: feita por outro módulo

Implementação: revogação de certificados

- Revogadores: *Chain of Responsibility*
 - OCSPRevocationHandler: protocolo *OCSP*
 - CRLRevocationHandler: listas de certificados revogados

Implementação: revogação de certificados

- Diagrama de colaboração

Implementação: mapeamento de papéis

- Especificados em arquivo XML

Resultados experimentais

- Ambiente de testes
 - Rede local *Fast Ethernet*
 - Computadores Intel Centrino 2GHz, 2Gb RAM
 - SO Fedora Core 7
 - Serviços distribuídos
 - Testes de desempenho com cliente local e remoto
 - Carga inicial: 1000 usuários, com média de 3 papéis cada
 - Estudo comparativo com módulos do JBoss
 - Aplicação de testes: componente EJB2

Resultados experimentais

- Distribuição dos serviços envolvidos

Resultados experimentais: *cache* habilitado

(a) Durações médias das chamadas ao *EJB* de testes.

		UsersRoles	DatabaseServer	Ldap	X509ACPull	X509ACPush
Chamadas Locais	Média	0,344	0,339	0,343	0,342	0,375
	Desvio Padrão	0,636	0,360	0,411	0,570	0,492
	Mínimo	0,309	0,302	0,307	0,307	0,340
	Máximo	64,972	25,332	25,329	72,025	37,576
	I.C. (95%)	[0,335; 0,353]	[0,334; 0,344]	[0,337; 0,349]	[0,334; 0,350]	[0,368; 0,382]
Chamadas Remotas	Média	0,935	0,961	0,942	0,951	1,038
	Desvio Padrão	1,518	0,452	0,367	0,463	0,391
	Mínimo	0,555	0,577	0,592	0,576	0,668
	Máximo	206,056	28,446	26,862	35,148	33,162
	I.C. (95%)	[0,914; 0,956]	[0,955; 0,967]	[0,937; 0,947]	[0,945; 0,957]	[1,033; 1,043]

(b) Durações das chamadas com *cache* de segurança habilitado. Todos os tempos são expressos em milissegundos.

Resultados experimentais: *cache* desabilitado

(a) Durações médias das chamadas ao *EJB* de testes.

		UsersRoles	DatabaseServer	Ldap	X509ACPull	X509ACPush
Chamadas Locais	Média	3,091	2,039	1,585	9,788	8,909
	Desvio Padrão	1,616	1,680	1,813	3,638	2,887
	Mínimo	2,963	1,926	1,395	9,510	8,613
	Máximo	217,279	217,472	221,072	307,641	272,759
	I.C. (95%)	[3,069; 3,113]	[2,016; 2,062]	[1,560; 1,610]	[9,738; 9,838]	[8,869; 8,949]
Chamadas Remotas	Média	3,761	2,660	2,174	10,411	9,529
	Desvio Padrão	1,568	1,666	1,674	3,381	2,982
	Mínimo	3,223	2,291	1,685	9,916	8,928
	Máximo	210,028	219,944	220,529	298,631	278,490
	I.C. (95%)	[3,739; 3,783]	[2,637; 2,683]	[2,151; 2,197]	[10,364; 10,458]	[9,488; 9,570]

(b) Durações das chamadas com cache de segurança desabilitado. Todos os tempos são expressos em milisegundos.

Resultados experimentais: impacto da validação

(a) Sobrecarga imposta pelo uso do verificador padrão no modelo *pull*.

(b) Sobrecarga imposta pelo uso do verificador padrão no modelo *push*.

		X509ACPull + EmptyVerifier	X509ACPull + DefaultVerifier	X509ACPush + EmptyVerifier	X509ACPush + DefaultVerifier
Chamadas Locais	Média	1,454	9,788	0,830	8,909
	Desvio Padrão	2,726	3,638	1,683	2,887
	Mínimo	1,331	9,510	0,764	8,613
	Máximo	294,494	307,641	215,834	272,759
	I.C. (95%)	[1,416; 1,492]	[9,738; 9,838]	[0,807; 0,853]	[8,869; 8,949]
Chamadas Remotas	Média	1,991	10,411	1,485	9,529
	Desvio Padrão	2,566	3,381	1,592	2,982
	Mínimo	1,557	9,916	1,165	8,928
	Máximo	264,976	298,631	213,902	278,490
	I.C. (95%)	[1,955; 2,027]	[10,364; 10,458]	[1,463; 1,507]	[9,488; 9,570]

(c) Durações das chamadas com diferentes configurações do verificador utilizado. Todos os tempos são expressos em milissegundos.

Resultados experimentais: mapeamento de papéis

(a) Sobrecarga imposta pelo uso do mecanismo de mapeamento no modelo *pull*.

(b) Sobrecarga imposta pelo uso do mecanismo de mapeamento no modelo *push*.

		X509ACPull	X509ACPull + Role Mapping	X509ACPush	X509ACPush + Role Mapping
Chamadas Locais	Média	9,788	9,827	8,909	9,035
	Desvio Padrão	3,638	4,087	2,887	2,902
	Mínimo	9,510	9,587	8,613	8,728
	Máximo	307,641	312,370	272,759	273,044
	I.C. (95%)	[9,738; 9,838]	[9,770; 9,884]	[8,869; 8,949]	[8,995; 9,075]
Chamadas Remotas	Média	10,411	10,465	9,529	9,828
	Desvio Padrão	3,381	3,842	2,982	2,845
	Mínimo	9,916	9,970	8,928	9,305
	Máximo	298,631	303,609	278,490	271,979
	I.C. (95%)	[10,364; 10,458]	[10,412; 10,518]	[9,488; 9,570]	[9,789; 9,867]

(c) Durações das chamadas. Todos os tempos são expressos em milisegundos.

Resultados experimentais: verificador de revogação OCSP

(a) Sobrecarga imposta pelo uso do verificador de revogação OCSP no modelo *pull*.

(b) Sobrecarga imposta pelo uso do verificador de revogação OCSP no modelo *push*.

		X509ACPull	X509ACPull + OCSPHandler	X509ACPush	X509ACPush + OCSPHandler
Chamadas Locais	Média	9,788	22,905	8,909	22,001
	Desvio Padrão	3,638	5,208	2,887	4,181
	Mínimo	9,510	22,286	8,613	21,323
	Máximo	307,641	325,216	272,759	282,508
	I.C. (95%)	[9,738; 9,838]	[22,833; 22,977]	[8,869; 8,949]	[21,943; 22,059]
Chamadas Remotas	Média	10,411	23,407	9,529	23,125
	Desvio Padrão	3,381	5,160	2,982	4,426
	Mínimo	9,916	22,655	8,928	22,324
	Máximo	298,631	333,730	278,490	289,126
	I.C. (95%)	[10,364; 10,458]	[23,335; 23,479]	[9,488; 9,570]	[23,064; 23,186]

(c) Durações das chamadas. Todos os tempos são expressos em milissegundos.

Resultados experimentais: verificador de revogação CRL

(a) Duração média das chamadas com o verificador de revogação CRL no modelo *pull*.

		X509ACPull+ CRLRevocationHandler				
		1 Entrada	250 Entradas	500 Entradas	1000 Entradas	2000 Entradas
Chamadas Locais	Média	18,199	23,619	28,918	39,519	67,467
	Desvio Padrão	4,725	5,404	6,240	8,056	12,872
	Mínimo	17,865	23,273	28,514	38,976	61,064
	Máximo	323,941	333,201	352,832	376,917	452,710
	I.C. (95%)	[18,134; 18,264]	[23,544; 23,694]	[28,832; 29,004]	[39,407; 39,631]	[67,289; 67,645]
Chamadas Remotas	Média	18,878	24,281	29,536	40,103	67,139
	Desvio Padrão	4,603	5,341	6,203	7,962	12,033
	Mínimo	18,305	23,738	28,991	39,384	60,554
	Máximo	311,672	343,433	306,998	366,861	460,032
	I.C. (95%)	[18,814; 18,942]	[24,207; 24,355]	[29,450; 29,622]	[39,993; 40,213]	[66,972; 67,305]

(b) Durações das chamadas. Todos os tempos são expressos em milissegundos.

Resultados experimentais: avaliação

- Alto custo de validação dos certificados
- Identificação de melhorias:
 - OCSP: múltiplos certificados
 - CRL: uso de cache
- Em produção: uso de cache
 - Preservação de recursos
 - Uso viável dos certificados de atributos

Considerações Finais: contribuições

- Integração da IGP à plataforma Java EE
 - Flexibilidade de gerenciamento de privilégios
 - Suporte aos modelos *pull* e *push*
 - Segurança das informações dos certificados
- Estudo comparativo de desempenho
 - Avaliação da solução desenvolvida
 - Identificação de custos associados aos certificados
- Artigo aceito em conferência nacional – SBSeg
- Inclusão do código em definitivo ao JBoss

Considerações Finais: trabalhos futuros

- Suporte ao modelo push por HTTP
- Aprimoramento dos verificadores de revogação
- Testes de interoperabilidade
- Disponibilização do serviço para outras aplicações
 - Uso fora do ambiente Java EE
 - Esforço em progresso
- Artigo em conferência internacional