Esquema de Autorização para Redes de Larga Escala combinando os Modelos de Segurança Web, Java e CORBA

Carla Merkle Westphall, Joni da Silva Fraga e Lau Cheuk Lung
Laboratório de Controle e Microinformática - LCMI-DAS-UFSC
Campus Universitário - Trindade - Florianópolis - SC
Caixa Postal 476 - CEP 88040-900
e-mail: {merkle,fraga,lau}@lcmi.ufsc.br

Resumo - Este resumo apresenta um esquema de autorização para redes de larga escala, envolvendo modelos e ferramentas de programação representados pelo Web, Java e CORBA. O esquema de autorização é fundamentado em estruturas e conceitos introduzidos no Web, Java e CORBA, com relação a segurança. Um primeiro protótipo desse esquema é apresentado nesse texto, onde as soluções adotadas visando a sua concretização são discutidas. Esse esquema foi desenvolvido no sentido de facilitar a implementação de políticas de autorização nesses sistemas. A implementação visa políticas discricionárias e não discricionárias, mas, primeiramente, políticas discricionárias foram implementadas no protótipo. Os modelos de segurança adotados foram adaptados ao contexto definido no sentido de elaborar um esquema de autorização realizável e prático.

Palavras-Chave: Segurança, Políticas de autorização, Esquemas de autorização.

Nossa Proposição de Esquema de Autorização para Redes de Larga Escala

Novos paradigmas e ferramentas de programação distribuída têm surgido para suprir novas necessidades dos sistemas distribuídos de larga escala. Entre esses novos paradigmas e ferramentas estão, além dos códigos móveis, o próprio Web e o CORBA. Esquemas de autorização para esses tipos de sistemas envolvendo mobilidade de código, portanto, devem sofrer um processo de renovação e amadurecimento, o que fornece um amplo tema de pesquisa na área de segurança.

A linguagem Java popularizou o conceito de código móvel através dos seus *applets* executados a partir de *browsers* Web. O ambiente Web representa a estrutura mais simples para códigos móveis, disponibilizando toda uma rede mundial e possibilitando carga de códigos em qualquer ponto da rede. O modelo de programação distribuída Java/CORBA/Web está se tornando padrão *de facto* de programação na Internet [1].

O esquema de autorização proposto neste resumo é fundamentado em estruturas e conceitos introduzidos no Web, Java e CORBA, com relação a segurança. No nosso ponto de vista a implementação de um esquema de autorização em redes de larga escala possui dois níveis, um *nível global* e um *nível local*, a exemplo de sistemas como Delta-4 [2]. O esquema proposto (figura 1) define um servidor de autorização, formado por um *applet de autorização* e por *objetos de serviço CORBA*. O *applet* de autorização é responsável pela autenticação de um cliente e interage com um objeto de serviço CORBA, instalado no site do servidor Web. Essa interação ocorre para estabelecer as credenciais CORBA do cliente de forma que esse cliente possa ser carregado, na forma de um *applet* de aplicação. As chamadas executadas por esse *applet* de aplicação sobre um servidor remoto da aplicação estarão sujeitas a dois níveis de controle de acesso. No nível mais alto, um objeto de serviço CORBA é responsável pela validação de pedidos de acesso aos objetos persistentes, verificando os direitos segundo a política apropriada. A partir dessa verificação de alto nível são geradas *capabilities* que serão validadas nos servidores remotos, conforme o segundo nível de controle de acesso definido em nosso esquema. Para montar esses dois níveis de controle de acesso, utilizamos os dois níveis de interceptação definidos no modelo de segurança CORBA [5]. O objeto de serviço CORBA que implementa a política do sistema interage também com um serviço de nomes e com o servidor de arquivos para armazenar e recuperar todas as informações de controle sobre os recursos no sistema. O modelo CORBA de segurança define um bom *framework* para a realização desses controles e também da segurança das mensagens transmitidas no suporte de comunicação. Usando esse *framework*, além desses controles citados acima, implementamos

outros controles como os controles criptograficos necessários no esquema, também na forma de objetos CORBA de seviço.

Os núcleos de segurança e *Trusted Computing Bases* validam os acessos locais dos *applets* de aplicação. Para implementar essa base confiável que valida os acessos locais, usamos o modelo de segurança Java e seus procedimentos de controle de acesso. O modelo de segurança Java, na sua versão 1.2, possui arquivos de política que identificam quais operações podem ser realizadas pelos códigos carregados (*applets*). Além disso, conta com o gerente de segurança que realiza o controle de acesso baseado na política concretizada através dos domínios de proteção. No nível local, o que se pode dizer é que o esquema de autorização trata com aspectos de segurança de códigos móveis, já que os clientes são representados por *applets* Java. Nesse aspecto, o esquema proposto resolve alguns problemas de segurança de códigos móveis como proteção da máquina contra códigos móveis, usando procedimentos de autenticação bem como os próprios domínios de proteção do modelo de segurança Java.

Um primeiro protótipo do esquema proposto foi desenvolvido em nossos laboratórios. As implementações foram feitas usando as ferramentas OrbixWeb 3.0 da Iona, Netscape Communicator 4.5, JDK 1.2 da Sun e o SSLeay - versão free do protocolo SSL 3.0. Essa primeira experiência implementa políticas discricionárias, se limitando a uma única verificação de controle de acesso no lado do servidor de aplicação. Dentre os objetos implementados nesse protótipo, além dos objetos *Applet de aplicação* e *Servidor de aplicação*, temos os objetos de *Decisão de Acesso*, *Vault*, *Contexto de Segurança* e *Policy* que são objetos do modelo CORBA de segurança. O controle de acesso realizado no protótipo está baseado em um mecanismo de lista de acesso implementado no objeto *Policy*. Políticas não-discricionárias ou obrigatórias são objetivos futuros em nosso protótipo [3] [4].

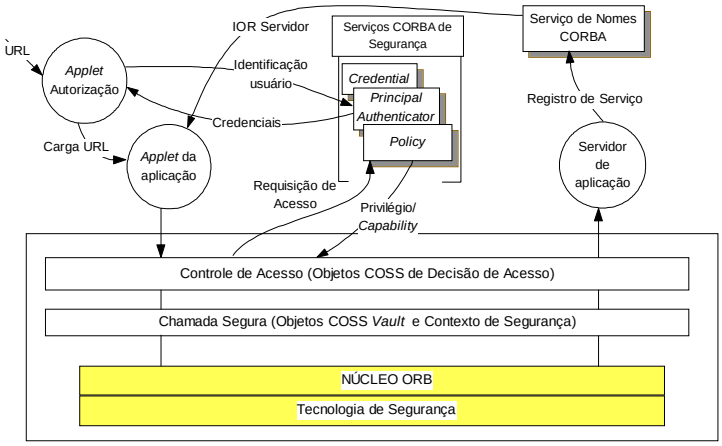

Figura 1 – Estrutura do Esquema de Autorização Java/CORBA/Web.

Referências Bibliográficas

[1] *Standards et Technologies, Normalisation – Java en route vers le standard ISO*, Le Monde Informatique, n. 743, 21 novembre 1997.

[2] Nicomette, Vincent. *La Protection dans les Systèmes à Objets Répartis*. PhD thesis, Institut National Polytechnique de Toulouse, 1996.

[3] Bell, D. E., Lapadula, L. J., *Secure computer systems: Mathematical foundations and model*. Tech. Rep. M74-244, MITRE Corp, October 1974.

[4] Sandhu, Ravi S., *Role-Based Access Control*. A. C. S., Vol. 46, Academic Press, 1998.

[5] Westphall, Carla Merkle. *Esquemas de Autorização para a Programação Distribuída combinando os Modelos de Segurança Java/CORBA/Web*. Exame de Qualificação de Doutorado, LCMI-DAS-UFSC, Agosto 1998, Certificado de Reg. n. 165.863, livro 277, folha 4 da Fundação Biblioteca Nacional, Rio de Janeiro.