

基于 SOMA 实现 SARBA 的解决方案^{*}

王 婵, 罗源明

(中山大学信息科学与技术学院, 广东 广州 510275)

摘 要: 移动代理安全性问题的解决是移动代理系统广泛推广应用的关键。提出了一个基于 CORBAsecurity 的安全 Agent 请求代理体系结构 (SARBA), 并论述了如何在 SOMA 移动代理系统的基础上实现 SARBA 体系结构, 这对解决移动代理跨域互操作的安全问题会有一定的作用。

关键词: 移动代理; 安全; CORBAsecurity; 安全 Agent 请求代理体系结构 (SARBA); Secure and Open Mobile Agent
中图分类号: TP393.01 **文献标识码:** A **文章编号:** 0529-6579 (2003) S2-0110-03

移动代理跨域互操作的安全问题是推广移动代理系统应用的关键, 它包括以下两点: (1) 关于移动代理的迁移认证, 目前大多数移动代理系统如美国提出的 Concordia^[1]、Ajanta^[2] 等都只能做到单域认证, 日本 IBM 提出的 Aglet^[3] 遵循 OMG 提出的 MASIF^[4] 规范, 可以做到代理在两个域之间的迁移认证; (2) 在资源访问控制方面, 访问控制列表 (如 Concordia^[1]) 这种方法比较传统而且难以管理, 而基于 proxy 的访问控制 (如 Ajanta^[2]、Aglet^[3]) 虽然安全性比较高, 但缺乏灵活性, 而且实现起来比较繁琐。OMG 就对象安全问题提出了 CORBAsecurity 的解决方案, 它通过各种安全机制建立了一个良好的安全控制模型。

本文提出了一个基于 CORBAsecurity 的安全 Agent 请求代理体系结构 SARBA (Secure Agent Request Broker Architecture)^[5], 并给出了在 SOMA^[6] 移动代理系统的基础上 SARBA 的一个实现方案。

1 安全 Agent 请求代理体系结构

在 CORBA 安全对象模型的基础上, 本文扩展 ORB 构建了适应移动代理跨域互操作的 ARB, 提出了基于这个 ARB 的 SARBA 分层安全体系结构 (如图 1 所示), 它描述了代理从发起者系统 (Initiator Server) 迁入目的系统 (Target Server) 所经历三个分层:

(1) 传输层: 该层处理通信方面问题, 以及提供代理迁移的通道。

(2) ARB: 这是 SARBA 的核心, 包括 ARB

Core、ARB 接口、ARB 安全服务以及策略接口。本文的扩展工作包括: 增加了 ClassLoader、ProtectionDomain 接口以提供初步授权服务, 扩展了原有的提供授权服务的 AccessDecision 接口, 并增加了各种安全策略接口。这样, ARB 就向上层提供了三个 ARB 安全服务: 安全迁移服务、初步授权服务和授权服务。

(3) 应用层: 含 MAFAgentSystem 接口, 域服务器还含 MAFFinder 接口。

本文通过调用 ARB 提供的接口实现了以下两个安全控制服务:

(1) 代理迁移认证的安全控制服务: 对代理在三个域之间的跨域迁移认证问题提出一个解决方案, 涉及 SARBA 的传输层、ARB 的安全迁移服务以及应用层的两个 MAF 接口。

(2) 资源访问控制的安全控制服务: 较好地实现了资源的访问控制, 达到安全性与灵活性的平衡。这个安全控制服务是通过调用 ARB 的初步授权服务与授权服务来实现的。

2 基于 SOMA 实现 SARBA 的一个解决方案

本文提出的实现 SARBA 的一个解决方案是通过在一个基于 CORBA 的移动代理系统中设计一个部件, 在部件中完成对 ORB 接口的扩展, 然后由这个部件提供的新接口与 ORB 原有的接口构成 ARB 的接口。我们选择意大利的 Bologna 大学推出的 SOMA 移动代理系统作为实现 SARBA 的基础。

* 收稿日期: 2003-06-13

基金项目: 广州市科技局重点攻关资助项目 (01-018-425115)

作者简介: 王婵 (1978 年生), 女, 硕士研究生; 通讯联系人: 罗源明; E-mail: wang-chen@sina.com

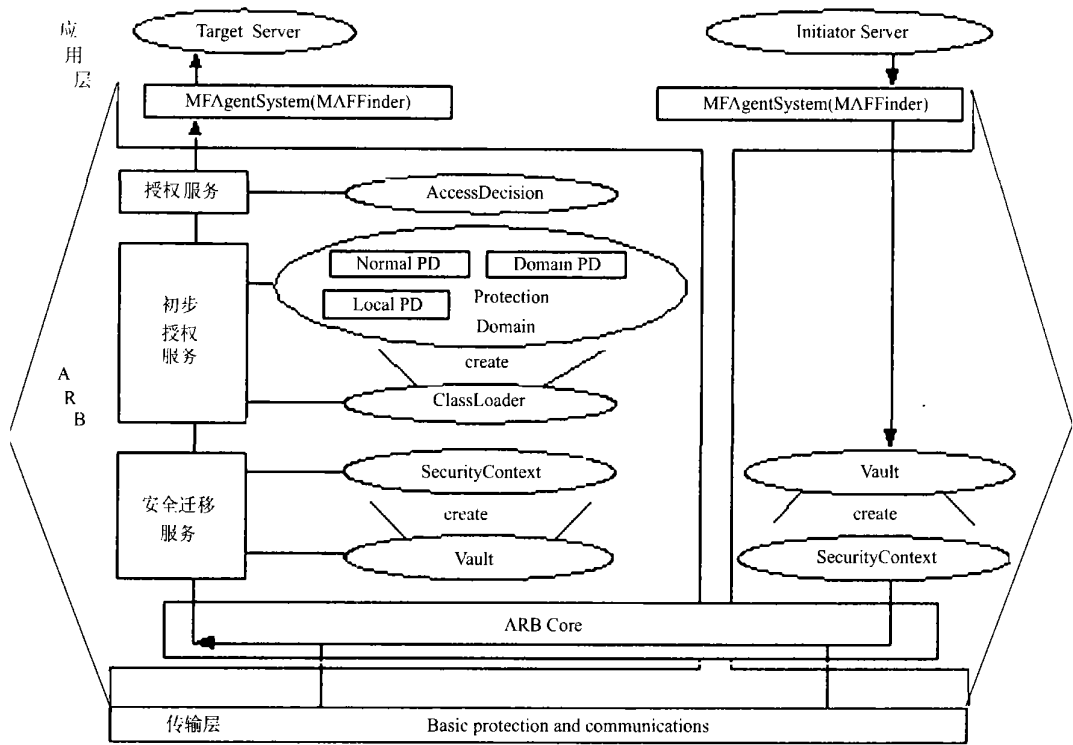


图 1 SARBA 分层安全体系结构
Fig. 1 Hierarchical secure architecture of SARBA

2.1 SOMA 移动代理系统概要

SOMA 是一个基于 CORBA 的移动代理系统，它用 Java 语言实现，提供了一个可测量的、动态的、开放的、安全的移动代理框架。基于 SOMA 的服务目前已在各个领域得到应用，如网络、系统和 服务管理、分布式信息检索、多媒体播放等。SOMA 主要解决移动代理的两个问题：互操作与安全。一方面，SOMA 融合 CORBA 实现了三个域之间互操作的定位^[7]。另一方面，在安全性能上，SOMA 设计了一个 Multiple Hops protocol 来代替传统的 TTP solution 来保护代理的完整性^[6]，并使用这个协议开发了一个电子商务的原型系统。

2.2 在 SOMA 的基础上具体实现 SARBA

SOMA 将 MASIF 规范与 COABA 紧密结合起来，使用 ORB 实现了 MASIF 规范，并且在 SOMA.CfMAF 软件包内提供了相应的类和一些公用函数。

本文使用 VisiBroker ORB for Java，用 Java 语言实现。CORBA 的安全服务规范及其 IDL 见 CORBA Security Services 1.8 Specification (CSS 1.8)^[8]。Java 的 IDL 见 <http://java.sun.com/products/jdk/idl>。SOMA 移动代理系统的源码和开发工具包可以在网站 <http://www.fia.deis.unibo.it/Software/SOMA>^[6] 上获取到，本文使用的是目前最新的版本 SOMA 30beta。

SARBA 的实现框架如图 2 所示。

我们在 SOMA 的基础上新增加一个软件包 ARB'，在 ARB' 中完成对 ORB 接口的安全服务方面的扩展。然后，由这个 ARB' 提供的新接口与 ORB 原有的接口构成 ARB 的接口。最后，我们调用这个 ARB 提供的接口，实现 MASIF 规范中定义的 MAFFinder 接口与 MFAgentSystem 接口，以及代理迁移认证服务与资源访问控制服务两个安全控制服务。下面给出 ARB' IDL 的部分接口定义：module ARB' {

```
interface ClassLoader {
CORBA::Object init protection domain (
in Security::SecAttribute GroupId ); };
interface AccessDecision {
boolean access allowed (
in Security::SecAttribute agent source,
in Security::DelegationState delegation state,
in Object target,
in CORBA::Identifier operation name ); };
interface PDPolicy: AccessPolicy { .....};
interface ADPolicy: AccessPolicy { .....};
interface ProtectionDomain { .....};
interface Current: SecurityLevel1; Current { .....}; };
```

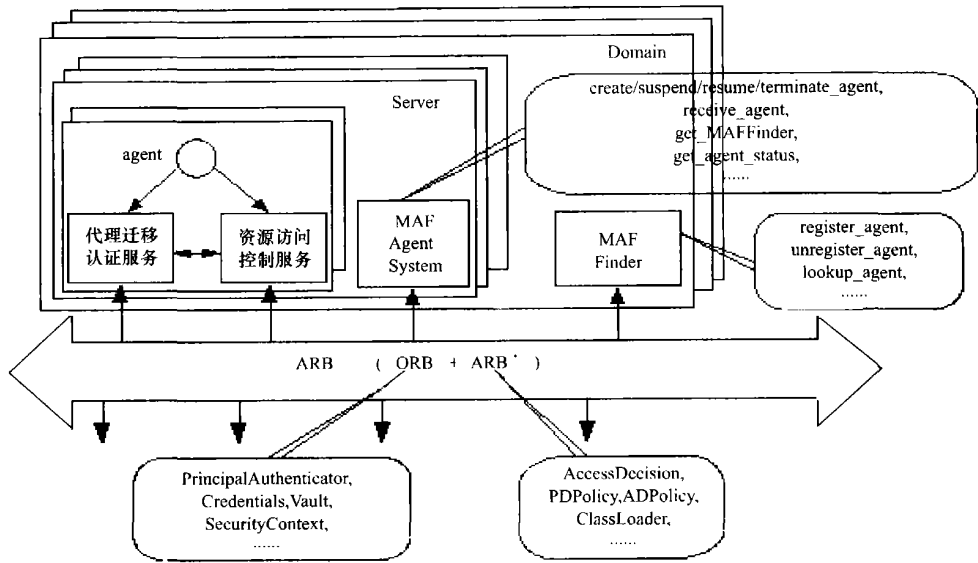


图 2 SARBA 的实现框架

Fig. 2 Implementation frame of SARBA

3 结 论

本文所论述的 SARBA 的实现方案为解决移动代理安全性问题提供了一种途径，我们的工作包括以下几点：

- (1) 扩展 ORB 构建了 ARB，给出了基于这个 ARB 的 SARBA 分层安全体系结构。
- (2) 通过 SARBA 对资源访问控制与代理，对三个域之间的跨域迁移认证问题提出了一个解决方案。
- (3) 深入研究了 SOMA 移动代理系统，在它的基础上提出了 SARBA 的一个实现方案，设计了 ARB' 的 IDL 以及编写了大部分的 Java 代码。

关于移动代理跨域互操作的安全问题涉及面很广，还有许多问题可作进一步的研究。

参考文献：

[1] WALSH T, PACIOREK N, WONG D. Security and reliability in Concordia-sup TM [J]. Proc 31st Annual Hawaii

International Conference on System Sciences, IEEE, 1998; 44—53.

[2] ARNIK N M, TRIPATHI A R. A security architecture for mobile agents in Ajanta, <http://www.cs.umn.edu/Ajanta>.
[3] IBM Research, Aglets, <http://www.trl.ibm.com/aglets/index-e.htm>.
[4] OMG, MASIF Revision, <http://www.omg.org/docs/orbos/1998-03-09.pdf>.
[5] 王婵, 罗源明. 移动代理跨域互操作的安全研究 // 全国计算机新技术与计算机继续教育论文集 Cj . 2003.
[6] Bologna University, Italy. SOMA. <http://www.lia.deis.unibo.it/Software/SOMA>
[7] WILHELM U G, STAAMANN S M. Levente Buttyan. A pessimistic approach to trust in mobile agent platforms[J]. IEEE Internet Computing, 2000; 40—48.
[8] OMG. CORBA Security Services 1.8 Specification(CSS1.8), <http://www.omg.org/technology/documents/formal/security-service.htm>, Mar 2002

A Solution Scheme of Implementing Secure Agent Request Broker Architecture Based on SOMA

WANG Chan, LUO Yuan ming

(Information Science and Technology College, Sun Yat sen University, Guangzhou 510275, China)

Abstract: Security in mobile agent is very important to apply mobile agent system widely. This paper presents a CORBAscurity based SARBA (Secure Agent Request Broker Architecture) and introduces how to implement it based on SOMA (Secure and Open Mobile Agent) mobile agent system. It can prevent or solve some security problems in multi-hop interoperation between mobile agent systems.

Key words: mobile agent; security; CORBAscurity; SARBA; SOMA