移动代理系统安全体系结构研究

Research on Security Architecture of Mobile Agent System

陈 良 高成敏 （广东警官学院 计算机系 广州 510232）

摘要：本文对移动代理系统作了简要介绍。阐述了由于其移动性而引发的安全问题和安全需求。介绍了移动代理系统安全技术及其体系结构研究现状，对它们的优缺点进行了分析。

关键词：移动代理 安全 移动代理系统 安全体系结构

1 移动代理简介

移动代理（MA）是分布式计算四种设计范式 Client Server（CS），Remote Evaluation（REV），Code on Demond（CoD），MobileAgent（MA）中的一种[2]。

移动代理作为独立的计算程序，代表用户自主地在异构网络上按照一定的规程迁移，寻找合适的计算资源、信息资源或软件资源，并在资源所在的主机或网络上使用资源，完成特定的任务。

移动代理系统由移动代理（MA）和移动代理环境（MAE）两个部分组成[3]。如图1所示，MAE 是一个分布在网络各种计算设备上的软件系统，它也被称为移动代理服务器或移动代理平台. 它一般建立在操作系统之上，为 MA 提供运行的环境. MA 则是只能存活在 MAE 中的软件实体. MA 的移动便是从一个 MAE 移动到另一个 MAE。

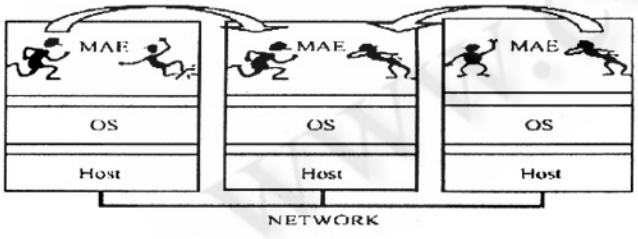

图 1 移动代理系统示意图（卡通人表示 MA）

移动代理的灵活性和高效率使得它有重大的应用价值，它的应用范围包括：电子商务、个人软件助理、分布式信息检索、电信网络服务、监视和通告、信息发布、移动设备计算、网络管理、并行任务求解、工作流管理和协作、动态网络等[3]。

2 移动代理安全问题及安全需求

2.1 移动代理的安全问题

移动代理具有许多独特的优点，但是，其严重的安全问题阻碍在现实商业应用中的大规模使用。移动性引发了以下安全问题：

通信安全性 Agent 在执行过程中，产生的数据交换包括运行结果、控制命令、参数传递等，在开放的网络环境中广泛地存在被窃取与破坏威胁，可以发生在 Agent 与 Agent、Agent 与主机、Agent 与用户之间。

主机安全性 主机（资源服务器）易受恶意 Agent 或其它主机攻击，首先表现为数据被窃取与破坏，如资源注册器破坏与参数窃取、数据资源被冒名者窃取；资源服务器抵赖和否认服务；一个恶意 Agant 大量复制自身，最终消耗掉该主机资源，导致无法为其它 Agent 服务；恶意 Agent 对 MAE 或主机的操作系统攻击等。

Agent 自身安全性 Agent 本身重要参数与数据受威胁，如用户标识、属性参数、代码等被窃取与破坏，发生恶意 Agent 冒名和 Agent 本身失去原性以至于变质，受到攻击可以来自于恶意 Agent 或来自于主机与其它非法用户。

2.2 通信的安全需求

完整性 在开放的网络环境中检测发生在 Agent 与 Agent、Agent 与主机、Agent 与用户之间通信的内容被破坏或篡改。

保密性 在开放的网络环境中防止发生在 Agent

与 Agent、Agent 与主机、Agent 与用户之间通信的内容被窃取泄露。

2.3 主机安全需求

资源的访问控制 保证主机资源(计算、存储、网络等)访问处于主机的控制之下。

MAE 与 OS 的可用性 保证 Agent 不对 MAE 和 OS 系统造成破坏。

2.4 移动代理安全需求

不同类型的移动代理具有不同的安全需求。对于发送到网络上的移动代理,下面三个重要的安全需求是保护方案应该部分或全部遵循的基本需求[4][5]。

完整性。保护方案应该保护移动代理以避免非授权的修改,并完全保持它的完整性。保护方案应该拥有防止代理相关信息或代理通信被修改以及一旦任何修改发生后进行检测的机制。

可审计性。保护方案应该允许对发生在代理上的动作进行一记帐以达到抗抵赖的目的。例如,如果上面的安全需求被主机侵犯,保护方案应该有记录所有恶意行为的机制。这作为事后记录来跟踪和识别任何恶意当事人。

保密性。保护方案应该保护移动代理免受窃听。窃听在许多场合都可能发生,最明显的一个是针对移动代理的内容,包括可执行代码、数据、以及状态。入侵者分析代理以得到决策逻辑信息、途中的信息、以及执行流信息。窃听也可能针对代理之间及代理与平台之间的通信。因为该需求主要关心私人数据,有时也称为数据隐私,或代理隐私。

3 安全技术解决方案

保护方案主要有两种意义:预防和检测。预防是使用一些机制使攻击难以发生。与预防相比,检测是事后的调查分析,它使用一些机制来检测在移动代理上完成的任何异常操作。预防试图根除攻击尝试,而检测试图威慑攻击尝试。

3.1 安全模型

移动代理系统本身是一个开放的系统,MAE 可能要接受不信任的移动代理,移动代理也可能到不信任的 MAE 中去执行,因此,必须要有安全措施。移动代理的安全模型描述如何保证代理的完整性,防止代理携带的数据泄露,代理和服务器的相互认证,代理的授权和服务器资源存取控制策略等。认证,代理的授权和服务器资源存取控制策略等。

3.2 主机的保护机制

沙箱模型 移动代理在一个称为"沙箱"的受限环境里运行。远程主机可以在沙箱里运行不被信任的代码,而不用担心有安全问题。这个方法应用在 jdk1.0 中。沙箱的主要缺点是在这种受限环境里运行的应用程序不太有用,因为它们的操作受到限制。

代码签名 代码的所有者对代码进行数字签名以确保代码的鉴别和完整性。Jdk1.1 采用了这个模型,引入了所谓的签名 applet。当接收到有效签名的 applet,java 虚拟机把 applet 当成可信任代码执行,授权它访问 java 所有的资源。没有正确签名的则跟 jdk1.0 一样在沙箱里运行。

访问控制。为了限制攻击的影响,一个方法是进行更复杂的访问控制。这可以看成是单一的沙箱策略改进为更小的应用特定的策略。jdk 1.2 采用了这个方法,允许定义更细粒度的安全策略。与沙箱模型和代码签名相比,访问控制模型在两方面都达到了最佳:移动代理的行动可以限制为只针对特定的资源,同时模型允许写出和运行真正有用的软件。但由于它是在运行时动态执行的,访问模式的实施需要付出性能上的代价。

代码验证。代码验证通过给定安全策略来分析移动代理的结构或行为,从而提供了代码语义的进一步保证。沙箱模型已经使用了一些初步的程序检查,包括静态的和动态的,如确保指令的操作数类型正确等。主机保护的一个新的方法是移动代理的静态类型检查,然后代码运行时就不需要昂贵的运行时检查。在这个领域令人鼓舞的进展包括 Proof – Carrying Code。在 Proof – Carrying Code 里,远程主机在同意运行代码前首先要求证明代码遵守它的安全策略。代码所有者发送程序和相应的证明,使用一系列公理和重写规则。收到代码后,主机可以在证明导引下检查程序。这可以看成是某种形式的程序类型检查,因为证明是从中直接导出的。与构造证明相比,检查证明是相对比较简单的,因此这个技术不会导致执行环境大的负担。但是,证明可能很大,证明的自动生成仍然是一个有待解决的问题。

3.3 移动代理的保护方案

移动代理的现有保护方案:被动方案和主动方

案[6]。

(1) 基于检测的安全性措施。通过对运行环境进行检测来判断其是否安全,以及通过对移动代理的运行结果作检测来判断其是否受到了攻击。

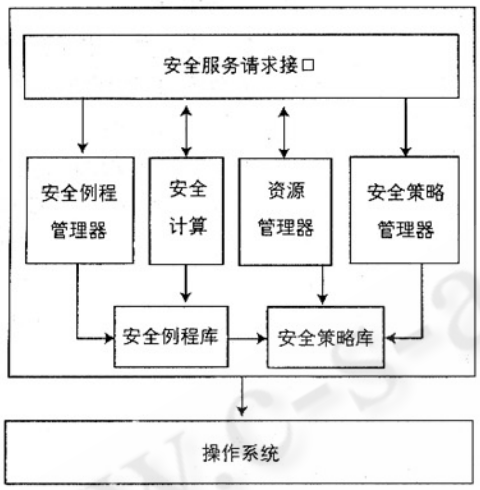

图 2　安全体系结构图

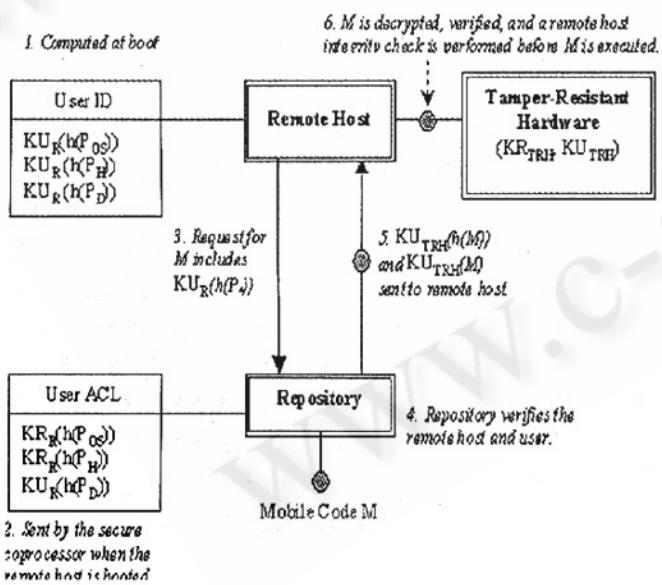

图 3　基于防篡改硬件的移动代理系统安全体系结构

不让移动代理到不被信任的运行环境中去执行任务 一个移动代理要前往某台主机时,首先判断该主机是否值得信赖。如是,则出发,反之放弃。问题是很难预先知道哪个主机值得信赖。一个解决办法是:建立一个封闭式的运行环境,禁止不被信赖的主机加入这个运行环境,从而,在这个运行环境中,每一台主机均是可以信赖的。Intranet 可以说是这一方面的典型应用。

在移动代理中加入一个状态评价函数 移动代理将根据状态评价函数的运算结果决定下一步的行动,但该函数也是由运行环境执行的,所以运算结果的可靠性仍然值得怀疑。

(2) 主动的保护措施。基于检测的方式是被动的。它只能检测到主机对移动代理的攻击,并不能真正保护移动代理免受破坏,不能保证移动代理在不信任的运行环境中安全运行。虽然要让移动代理在不信任的站点上绝对安全,没有一点问题是很难或者是根本无法解决的问题,但部分解决方案还是存在的。

加密函数。在移动代理中,并不是所有的代码和数据都是隐私,人们可能只对保护其中的关键数据和算法感兴趣,因此,只要保护移动代理中部分关键数据和算法即可。如对某个计算函数进行加密,使攻击者无法了解函数的内部逻辑。

共享秘密和互锁。由两个和两个以上的移动代理来共同完成一项任务,每个移动代理保持部分秘密,只有当它们达成一项协议后才可最终完成任务。

为每一台主机配置可信赖且能抵御攻击的硬件 抵御攻击的概念通常应用于一个明确的硬件模块,该模块负责一项特殊任务,外部环境只能通过一个完全受该模块控制的接口干预模块内任务的执行。

4　安全体系结构分析

一个基于 Java 的 Mobile Agent 安全体系结构模型[7],如图 2 所示。但该安全体系结构并不能提供对移动代理本身的安全保护。

一种基于硬件的安全体系结构模型,不但可以提供对移动代理主机的保护,同时可以提供对移动代理的安全保护,如图 3 所示。但其缺点是移动代理系统必须安装防篡改硬件。

(下转第 40 页)

(上接第 36 页)

5 结论

本文首先简要介绍了移动代理系统的优点及应用领域,在此基础上针对移动代理系统的安全问题和安全需求系统地进行了分析,并对当前相应的安全技术解决方案及其安全体系结构研究现状进行了分类和综述,对它们的优缺点进行了简要分析。

参考文献

1 Dale, J. A mobile agent architecture for distributed information management [Ph. D. Thesis]. Southampton: University of Southampton, 1997. 65 ~ 98.

2 Alfonso Fuggetta, Member, IEEE, Gian Pietro Picco, Member, IEEE, and Giovanni Vigna, Member, IEEE, Understanding Code Mobility, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 24, NO. 5, MAY 1998.

3 朱森良、邱瑜,移动代理系统综述,计算机研究与发展,第 38 卷 第 1 期,2001。

4 W Jansen, T Karygiannis. Mobile agent security. NIST Special Publication 800 – 19, NIST, 2000.

5 William M Farmer, Joshua D Guttman, Vipin Swarup. Security for mobile agents: issues and requirements. Baltimore (ed.), Proceedings of the 19th National Information Systems Security Conference, pp 591 – 597, 1996.

6 王汝传、徐小龙、郑晓燕、孙知信,移动代理安全机制模型的研究,计算机学报,第 25 卷 ,第 12 期,2002. 12。

7 王济勇、温 涛、李春光、汪大为、魏海平、林 涛,一个基于 Java 的 Mobile Agent 安全体系结构模型,计算机工程与应用,2000. 10。