移动Agent系统 安全问题 计算机安全 (26)

计算机科学2000Vol.27№.10

程序代码

移动 Agent 系统的安全问题*)

Security Issues of Mobile Agent System

TP18 TP309

99-101

董红斌 石纯一

(哈尔滨师范大学计算机系 哈尔滨 150080) (清华大学计算机系 北京 100084)

Abstract This article introduces security issues related to mobile agent system and discusses some technical approaches to address the problem.

Keywords Mobile agent, Mobile agent system, Security

1 引言

近年来,移动 Agent 技术已成为计算机网络和分布式系统最具活力的发展方向。移动 Agent 是一段可自主执行的程序代码,可以通过网络从一台机器移动到另一台机器运行,可用来寻找合适的计算资源、信息资源和软件资源,处理或使用这些资源,代表用户完成特定的任务。移动 Agent 具有移动性、自主性、反应性、社会性和学习能力等基本性质。移动 Agent 技术分为两类:

·弱移动技术将移动代码发送到远程站点执行,或动态连接远程站点并进行信息检索。最重要的弱移动技术是 Java,常常是移动 Agent 系统选择的程序设计语言。然而,典型的 Java applet 只是有限意义上的移动:从一个 HTTP 服务器移动到客户机,执行,死亡。特殊情况下,从一个执行环境移动到另一个执行环境没有执行状态。

·强移动技术允许一个移动代码或程序段在不同执行环境间移动。这种情况下,执行程序或程序段暂停下来,它的代码和执行状态被发送到远程执行环境,例如,Telescript 和 Agent Tcl。

利用强移动技术建立移动 Agent 的分布计算环境是可能的,不象 Java applets 那样用户可以下载程序,这种 Agent 可以自主决定什么时间移动到哪里去,还可以将自己的执行状态通过网络移动。目前有些移动 Agent 系统是基于 Java 的,另一些系统是用其它语言设计的,这些移动 Agent 系统研究出于军事和民用两种目的。除了用于简单的信息搜索任务外,移动 Agent 还用于与商业相关的应用,如价格协商、合同签定、服务提供和无形物品等。计算机网络和分布系统是基于被动数据单元的交换,相反,主动网络的数据单元由移动 Agent 的数据单元替换,通过移动 Agent 指导网络处理数据和数据传输。当前,主动网络已成为计算机网络和分布系统领域研究的新方向,移动 Agent 系统在分布领域与主动网络具有同等重要研究意义。

移动 Agent 系统的应用和广泛传播改变着人类赖以生存的环境:过去,有中央计算机系统与终端长久连接运行;现在,以客户/服务器方式为用户工作站提供各种信息服务;将来,有移动 Agent 系统动态为任务 Agent 和网络服务提供支持。

从现在的客户/服务器计算环境到将来的移动 Agent 系统的转变是一个重大进步,这种转变依然存在着一些障碍,即移动 Agent 和其执行状态在执行环境中移动时的安全问题,这些问题已在计算机网络和分布式系统安全领域进行了较长时间的研究,Chess 指出移动 Agent 系统出现的安全问题是对计算机安全系统的设计和实现提出的新挑战[1],更准确地说,用以提供访问控制和通讯安全服务的程序和程序段的设计技术和机制应该满足移动性的要求。这就提出了移动 Agent 系统的安全问题,这涉及三个方面:(1)移动 Agent 之间通讯的安全保护;(2)保护执行环境免受潜在的恶意 Agent 的损害;(3)保护 Agent 免受潜在的恶意服务器和环境的攻击。移动 Agent 系统的安全性是急需解决但又难以解决的问题之一,它直接影响移动 Agent 系统的实用性,下面对上述问题进行讨论。

2 移动 Agent 通讯的安全保护

移动 Agent 系统中的 Agent 是分布的,因此安全通讯是重要的。移动 Agent 间通讯存在如下一些问题:

·不安全通讯通道 移动 Agent 能否确定地知道与它们交谈的 Agent 就是期望与之交谈的 Agent;在

*)本课题得到国家自然科学基金资助,董红斌 副教授,清华大学访问学者,研究方向为分布式人工智能,移动 Agent。石纯一 教授,研究方向为人工智能应用基础。

信息传输过程中 Agent 接收的信息是否可靠；Agent 通讯是否是秘密进行的，发送信息方是否否认发送了信息。在移动 Agent 系统中安全通讯可能受到恶意 Agent 的威胁，Agent 彼此间能够相互欺骗，监听第三方的谈话，修改传输的信息，拒绝履行承诺。

·不安全委托。Agent 按照自身的利益行动，在实际应用中我们应该知道 Agent 正在执行用户请求的委派，例如，在我们向 Agent 发出信息前，银行想知道 Agent 是否是我们委派的 Agent 在工作，除非一些安全委派机制是合适的，否则一个 Agent 可以永远假冒委派的 Agent。

为保证通讯安全要对所有信息提供通讯认证，对任何可能的安全危害进行检测，通讯应该是秘密进行的。文[9]中给出了一种基于"加密信道-权限控制"的 Agent 系统通讯安全性实现方法，为防止非法入侵者的危害，Agent 系统在安全加密信道上运行，并提供了多层次检查机制，以满足分布式的要求。提出基于 RSA 和 Rabin 算法的加密信道提供底层的签名和加密服务，并构造高层的权限控制机制 DSM。在 DSM 中提出一种混合的权限检查方案，Agent 凭借其身份类别可以访问一类缺省的 Agent 服务，以及利用 Agent ID 进行访问，这样可以保证系统的安全通讯。

3 执行环境的保护

容易引起人们注意的是移动 Agent 系统运行环境的安全性问题，如何保护执行环境免受潜在的恶意 Agent 的攻击?有许多移动 Agent 攻击网络环境的例子，如 Internet 蠕虫事件就说明了简单的复制技术对计算机网络和分布式系统造成的危害。移动 Agent 有许多潜在的表现形式，如 Trojan 木马、计算机病毒和网络蠕虫。理论上防止恶意 Agent 的出现是困难的，例如很难决定任意一个代码段是否包含 Trojan 木马。

通常有几种方法可以防止执行环境受到潜在的恶意 Agent 的损害：沙箱、数字"收缩-打包"和检验传输代码，这三种方法可单独使用或混合使用。

3.1 沙箱

保护执行环境免受潜在的恶意移动 Agent 攻击的有效手段是限制移动 Agent 的访问权限，移动 Agent 是在某种沙箱中运行，所造成的损害较小，例如，允许移动 Agent 在屏幕上绘制有趣的图画，但它不能访问局部文件系统或利用网络与其它站点连接。

Sun 系统是采用"沙箱"方法对 Java applets 进行分布的，Java applets 是在受到安全保护的 Java 虚拟机(JVM)上运行的。公共 JVM 浏览软件如 Netscape Navigator 和 Microsoft Internet Explore，它们不允许访问局部文件系统的 applets，可以通过网络下载程序，安全策略不允许建立 TCP 连接，"沙箱"方法对移动 Agent 是一个严格的限制，对应用来说这个限制也许是比较严厉的。

3.2 数字"收缩-打包"

保护一个执行环境的另一种方法是移动 Agent 的执行认证，这种方法称为数字"收缩-打包"的方法，虽然不能确定一个移动 Agent 是恶意的，但可以确定它申请的资源的可靠性，这种方法已在 Microsoft 的认证代码技术中应用。

"沙箱"和数字"收缩-打包"方法是两种不同的方法，可以融合为一种复杂的安全保护技术，这在 Sun 系统的新安全模型中得到验证[8]。

3.3 检验-传输代码

卡内基·梅隆大学提出了一种选择技术用以保护一个执行环境免受潜在的恶意移动 Agent 的攻击[7]，这种技术称为检验传输代码(PCC)，它可使计算机系统自动确定其它系统提供的 Agent 的安装和运行是安全的。PCC 的关键思想是代码设计者提供一个检验编码，检验编码遵守由代码使用者制定的一个安全策略。检验编码传输给使用者并快速有效地用于描述检验传输过程，PCC 和其相关技术的主要问题是需要了解代码使用者的安全弱点。

4 移动 Agent 的保护

在传统的计算机安全方面，执行环境对程序造成危害的问题很难引起人们的重视，这是因为执行环境和程序共同组成一个完整的部分。然而，移动 Agent 和执行环境是不同的两个部分，这就提出了如何保护 Agent 免受潜在的恶意服务器和环境的攻击的问题。

保护 Agent 免受潜在的恶意服务器的攻击不是一个移动 Agent 系统应有的特性，移动 Agent 往往不能在执行环境中得到有效保护，因为执行环境是移动 Agent 需要访问的地方，这意味着移动 Agent 对访问计算机的可靠性具有很强的要求。保护 Agent 免受恶意服务器的攻击的研究方法可分为下面几种：

·第一种方法设法绕过问题，即不让 Agent 访问不可靠服务器。这种方法的主要问题是很难掌握哪一个服务器是可靠的或不可靠的，另外，可靠性不是绝对的。

·第二种方法通过组织测量方法设法绕过问题，移动 Agent 不访问有较多访问者的服务器，只访问部分开放的服务器。

·第三种方法利用特殊的抗干扰硬件保证移动 Agent 的完整，这种方法要求在每台机器上使用特殊硬件，这是较苛刻的要求。

·第四种方法设法解决与移动 Agent 保护相关的问题，通过建立限制环境、在移动 Agent 和密码安全港之间建立协议，使潜在破坏者难以得手。

然而，这些方法大多不够理想，因为它们或者限制性强或者太不可靠。移动 Agent 保护的主要挑战是能

否对如下问题给出满意解：移动 Agent 能否保护自己免受恶意服务器的伤害？移动 Agent 能否隐藏它想完成的工作？移动 Agent 能否为一个文件进行远程签字而不暴露用户的密码？

目前解决保护移动 Agent 免受潜在恶意服务器和环境的危害的目标是预防和检测，有限制黑箱安全、加密检测对象和密码跟踪三种方法，前一种方法目标是预防，后两种方法目标是检测。

4.1 限制黑箱安全

基于黑箱保护的方法是由 Stuttgart 大学的 Hohl 提出的[3]，主要思想是从一个给定的 Agent 规范生成执行代码，如果在任何时间内 Agent 不会受到攻击且只有它的输入和输出行为能被观察到，则一个 Agent 被看作一个黑箱。然而，目前没有任何算法能够用来支持这种黑箱的安全，Hohl 又定义了黑箱保护的有效时间，黑箱保护特性与时间相关，为实现限制黑箱安全特性提出了几个转换算法，转换算法的任务是生成一个子 Agent，子 Agent 的代码和表示与源 Agent 不同，但输出相同的结果。

4.2 加密检测对象

文[2]基于密码和 Hash 函数给出了一个移动 Agent 系统的安全机制，利用一个公共密码系统和一个 Hash 函数编码和译码数据，提供认证和生成数据签字，利用加密技术和检测对象技术监视对 Agent 的任何非法操作。这种检测和调查机制使系统可有效地防止恶意服务器的攻击，容易发现潜在破坏者，此外，检测过程可阻止非确认移动 Agent 进入服务器。因此，移动 Agent 系统的安全机制能保证移动 Agent 在信息检索中的自由和安全。

4.3 密码跟踪

文[14]基于密码跟踪提出了一种检测移动 Agent 的代码、状态和控制流的系统开发机制，这种开发机制的目标是检测任何可能的对移动 Agent 的代码、状态和执行流的非法修改，基于邮件的数据分析，即分析一个 Agent 在运行过程中搜集的相关数据信息。

结束语 本文对移动 Agent 系统的安全问题进行了阐述，主要包含三方面的内容：(1)移动 Agent 之间通讯的安全保护；(2)如何保护执行环境免受潜在的恶意 Agent 的破坏；(3)如何保护 Agent 免受潜在的恶意服务器和环境的危害。移动 Agent 系统的安全性是急需解决但又难以解决的问题之一，它直接影响着移动 Agent 系统的实用性。本文讨论了解决上述问题的技术方法。语言技术是移动 Agent 系统安全需要考虑的另一个重要问题。

移动 Agent 系统的安全模型和结构要适应未来移动 Agent 系统的发展，有关移动 Agent 系统的安全问题的研究工作正在普遍开展，例如，IBM 公司基于 Java 语言开发了一个移动 Agent 系统的安全模型，它由开发工具和运行平台组成；Dartmouth 学院开发了一个多语言移动 Agent 安全系统，然而，在移动 Agent 系统真正应用于电子商务之前尚有许多理论问题需要解决，这是我们今后需要进一步研究的工作。

参 考 文 献

1 Shieh Shiuh-Pyng, et al. Optimal assignment of mobile agents for software authorization and protection. Computer Communications, 1999, 22(Issue 1): 46～55

2 Wang X F, et al. Secure Information Gathering Agent for Internet Trading. LNAI 1544. In: Zhang Lukose eds. Multi-Agent System. Springer, Berlin, 1998

3 Hohl F. Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts. In: Vigna G ed. Mobile Agents and Security. Lecture Notes in Computer Science1419. Springer, Berlin, 1998. 92～113

4 Chess, D M. Security Issues in Mobile Code. In: Vigna G ed. Mobile Agents and Security. Lecture Notes in Computer Science1419. Springer, Berlin, 1998. 1～14

5 Morreale P. AGENTS on the MOVE. IEEE Spectrum, 1998

6 Oaks S. Java Security. O'Reilly and Associates, Sebastopol, CA, 1998

7 Necula G C, Lee P. Safe, Untrusted Agents Using Proof-Carrying Code. In: Vigna G ed. Mobile Agents and Security. Lecture Notes in Computer Science1419. Springer, Berlin, 1998. 61～91

8 Jennings N R. Agent-Based Computing: Promise and Perils. In: IJCAI-99. 1429～1436

9 Wang Ju, et al. Security Mechanism in Multi-Agent Systems. Journal of Computer Research & Development, 1999, 36(5): 553～559

10 Zapf M, et al. Security requirements for mobile agents in electronic markets. Trends in Distributed Systems for Electronic Commerce, 1998, 1402, 205～217

11 Yi X, et al. A secure intelligent trade agent system. Trends in Distributed Systems for Electronic Commerce, 1998, 1402, 218～228

12 Corradi A, et al. Mobile agents integrity for electronic commerce applications. Information Systems, 1999, 24(6): 519～533

13 Bergadano F, et al. Jave-based and secure learning agents for information retrieval in distributed systems. Information Sciences, 1999, 113(1～2): 55～84

14 Vigna G. Cryptographic Traces for Mobile Agents. In: Vigna G ed. Mobile Agents and Security. Lecture Notes in Computer Science1419. Springer, Berlin, 1998. 137～153

15 董红斌，石纯一. 移动 Agent 技术研究. 计算机科学，2000，27(4)：58～61