基于 JavaCard 的移动代理系统安全性研究*)

陈志贤　王绍棣　王汝传　孙知信
(南京邮电学院计算机系　南京210003)

Research on Security of JavaCard based Mobile Agent System

CHEN Zhi-Xian　WANG Shao-Di　WANG Ru-Chuan　SUN Zhi-Xin
(Computer Science & Technology Department, Nanjing Univ. of P&T, Nanjing 210003)

Abstract　With wide and increasing range applications of mobile agent technology, the security problem has gotten more and more focus. This paper discusses the security problems that the mobile agent system faces with at present and the existing protesting schemes for it. Then a solving method based on JavaCard is proposed to protect mobile agents. And a feasible solving method is also provided to solve the security problems of JavaCard itself.

Keywords　Mobile agent, JavaCard, TPE, Security

1　引言

移动代理是一种独立的可确认的计算机程序，它可自主地在异构网络上按照一定的规程移动，寻找合适的计算资源、信息资源和软件资源，利用与这些资源同处一台主机的优势处理或使用这些资源，代表用户完成特定的任务。

移动代理具有以下三个基本特征，它们是界定移动代理的必要准则：

(1)移动代理必须具有一定的身份，并代表用户的意愿。

(2)移动代理必须能自主地从一个节点移动到另一个节点，这是它最基本的特征，也是区别于其它代理的标志。

(3)移动代理必须能在不同的地址空间中连续运行，即保持运行的连续性，也即它在下一节点开始运行时必须与在上一节点挂起时刻的状态相同。

实际上，移动代理就是一段代表用户利益的程序代码，它可以转移到不同的地址空间中执行，在转移过程中保持自身的状态不变。图1为一个典型的移动代理系统的参考模型。

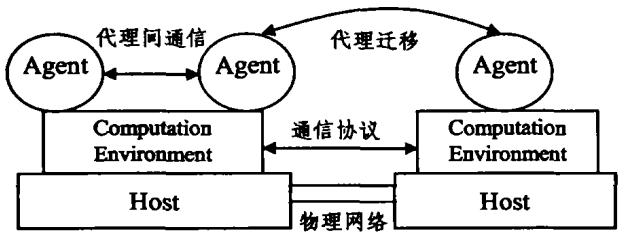

图1　移动代理系统参考模型

移动代理的应用要求分布式系统中相互协作的主机提供移动代理的执行环境，因而这些主机可能会受到恶意代理的攻击。与此类似，移动代理系统也要保证在主机上运行的移动代理的安全，以防止恶意主机的攻击。所以，设计移动代理系统时，其安全性是主要考虑的问题之一。为此，我们提出采用Java 智能卡构造一个移动代理的安全执行平台，以此来确保移动代理系统的可靠性和安全性。

2　移动代理系统的安全问题及现有的保护方案

2.1　移动代理系统的安全问题

移动代理可能遭受以下两种攻击：来自恶意服务器(或运行环境)的攻击、来自其它代理和实体的攻击。后一种攻击与前一种攻击在某些方面是相同的，如窃听移动代理与其主人之间的通信，这类问题在传统的网络中也是存在的。事实上，只要解决了前一种攻击问题，后一种也能迎刃而解。因此，下面的讨论均针对第一类攻击，即解决移动代理受恶意主机攻击的问题。

移动代理的安全性问题可以归纳为以下三个方面：

(1)移动代理能否保护自己不受恶意主机的攻击，即保护移动代理的代码、数据以及执行过程的完整性(Integrity)；

(2)移动代理能否对主机隐藏其所要执行的真正的功能，即保护移动代理的隐私(Privacy)；

(3)移动代理能否在远端签约而不暴露其主人的私钥。

2.2　现有的移动代理保护方案

2.2.1　*基于检测的安全性措施*　这是一种被动式检测，通过对运行环境进行检测来判断其是否安全，并通过对移动代理运行结果的检测来判断其是否受到了攻击。其主要方法有：

(1)不让移动代理到不被信任的运行环境中去执行任务；

(2)在移动代理中加入一个状态评价函数[1]，移动代理根据该函数的运算结果决定下一步的行动。但是，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；

(3)用加密和跟踪来保护移动代理(加密跟踪法)[2]。该方法能检测到恶意主机对移动代理的数据、代码、状态和控制流

*)本文得到国家自然科学基金(编号60173037)、江苏省自然科学基金(BK2001123)、江苏省计算机信息重点实验室基金(kjs01025)和中兴研究基金资助。陈志贤　硕士研究生，研究方向为计算机在通信中的应用。王绍棣　教授，博士生导师，主要研究方向是计算机网络和信息安全。王汝传　教授，博士生导师，主要研究方向是计算机软件理论、计算机网络、信息安全及移动代理技术等。孙知信　博士，副教授，主要研究方向是软件工程理论、计算机网络。

的攻击；

(4)在整个系统中为每一个主机建立可信度档案，以自动维护各主机的声望，确保移动代理不到声望低的主机上去执行任务，以此来惩罚检测出的恶意主机。

2.2.2 *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。为了让移动代理在不信任的运行环境中安全运行，必须采取主动的保护措施。

(1)加密函数[3]：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。

Sander 和 Tschudin[3]提出了一个加密函数计算方法(CEF，computing with encrypted function)。该保护措施的关键是为任意一个函数 f 找到一个加密方法。

(2)有限的黑匣子安全法：此方法对整个移动代理进行加密。因此在 CEF 的基础上，Stuttgart 大学的 Hohl[4]提出了黑匣子的思想，用黑匣子来防御恶意主机对移动代理的攻击。其核心是从一个给定的代理规范来产生可执行的代理，并且产生的代理是不可被攻击和修改的，见图2。

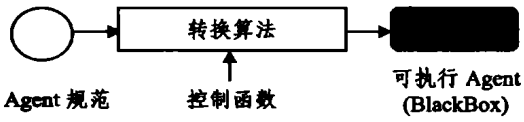

图2 黑匣子保护法

黑匣子保护法的关键就是找到一种转换算法，将旧的移动代理转换成一种新的移动代理，要求新的移动代理的输入与输出与旧的完全一致，即不能改变移动代理所要完成的任务。

(3)共享秘密和互锁：由两个或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，只有当它们达成协议才能最终完成任务。

(4)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。

在 UWE G. Wilhelm 等人提出的研究方案中[5]，这种硬件设备被称作可信赖处理环境(Trusted Processing Environment，简称 TPE)。TPE 实质上是一个完整的代理运行平台。它实际上就是一台完整的计算机，有自己的 CPU，RAM 和 ROM。ROM 里存有启动 TPE 所需的全部代码，包括操作系统和虚拟机(VM)。VM 提供一个代理运行平台并确保代理得到正确的执行。TPE 里还有一个扩展的密码库，可以提供加密功能。密码库里有一个不为外界所知的私钥，即便 TPE 的所有者也不知道，在 TPE 内部产生密钥对可以保证这一点。TPE 连在一台由其所有者控制的计算机上，该计算机只能通过一个明确的接口访问 TPE。

3 采用 Java 智能卡保护移动代理

在上述的 UWE G. Wilhelm 等人提出的研究方案中[5]，他们提议用可信赖硬件 TPE 保护移动代理不受恶意主机的攻击。对可信赖硬件，我们选择符合 JavaCard 规范的智能卡，即将能动态装载新应用程序、多功能且安全的 JavaCard 用作移动代理的可信赖计算基地，从而得到保护移动代理的 Java 智能卡解决方案。

我们提出的采用 JavaCard 保护移动代理的安全参考模型如图3所示。

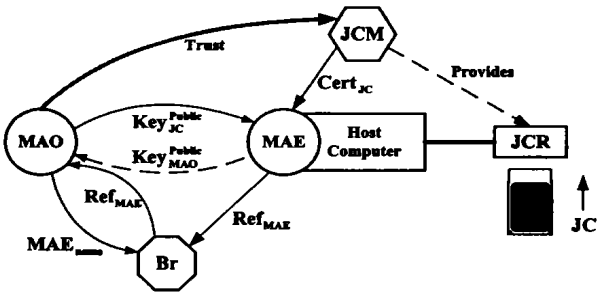

图3 采用 JavaCard 保护移动代理的安全参考模型

其中 JCM 是生产 Java 卡设备(包括 Java 卡和读卡器)的设备制造商。MAE 指位于服务器上的移动代理执行环境，负责为代理提供落脚点。经纪人 Br 扮演的角色与域名服务器 DNS 类似，它提供一种目录服务。MAE 可在一个或多个 Br 处登记下列参考信息：所在主机的机器名及物理网络地址、提供何种安全策略以及 JCM 证书，这些信息用于为 MAO 定位 MAE。JCM 证书里包含下列信息：JC 的制造商、JC 的类型、JC 提供的安全策略以及 JC 的公钥。MAO 持有 JCM 公钥的一个真实拷贝，用于验证其签发的 JCM 证书。

JC 中的 Java 虚拟机提供一个代理运行平台并确保代理得到正确的执行。同时 JC 中还应该有一个加密协处理器，由它产生密钥对可以保证私钥不为外界所知，即便 Java 卡设备的所有者也不知道。与读卡器 JCR 相连的主机只能通过一个明确的接口访问它。

一个典型的过程如下(假定各 MAE 都已注册成功)：首先，MAO 向 Br 提交某个 MAE 的名字，获得与之有关的信息，比如 JCM 证书。然后，MAO 用自己持有的 JCM 公钥的拷贝验证 JCM 证书的有效性。验证失败，则放弃此 MAE；反之，接着核实该 MAE 提供的安全策略是否足以保护自身利益。若策略不够充分，就放弃该 MAE；反之，用目的卡的公钥(在 JCM 证书中)加密移动代理中的代码段并将代理派往目的主机。目的 MAE 不知道卡的私钥，因而无法破译加密的代码段，除了将它上载至 JC 之外什么也做不了。接下来，JC 解密此加密代码段，获得可执行代码。代码段运行起来之后便可与所属代理、MAE 以及 JC 中的其它代码段进行交互。最后，移动代理提取出 JC 用不同的公钥加密的代码段，迁移到新主机并将代码装入目标卡，或是返回宿主机。

4 Java 智能卡自身的保护问题

上面重点讨论了使用 Java 智能卡保护移动代理不受恶意主机攻击，与此同时也不能忽略 Java 智能卡自身的保护问题，因为恶意代理也可能对它进行攻击，比如窃取卡的私钥。

对于 Java 智能卡可以从三个方面加以控制：

(1)从智能卡上信息的读取方面来控制，这又可以分为两类：

(下转第116页)

在EVE算法中，我们假设候选集复制到所有处理器上，但实际处理问题时，候选集通常会很大，为了降低处理器内存需求和避免遗漏计算序列，提出了事件候选集分布算法(Event and Candidate Distribution)。

EVECAN算法基本思想是：输入数据的划分和EVE算法类似。候选集存在分布的哈希表中，哈希分布本着让所有处理器上候选集数目相等的原则。EVECAN算法中处理器需要处理输入数据和候选集，当ms的值较小时，可将候选集静态置于处理器上，建立本地哈希树，而输入数据采取类似于IDD算法的round-robin方式；当ms值较大时，则反之。

4 实验结果及分析

为了分析和比较串行算法和并行算法的性能，我们对某超市自2000年4月5日至2000年6月19日的销售数据应用上述算法，该销售数据共包括132144条数据，1034种商品。并行机采用曙光3000，3个节点。测试数据如表1所示。

表1 各种算法时间开销比较

测试算法	时间开销/分
串行算法	16.8
EVE-S	15.3
EVE-R	15.5
EVECAN	15.1

在大型数据库上进行序列模式挖掘时，由于海量数据和高维模型的出现，算法的开销往往很大。本文提出的并行算法能加速挖掘过程，提高挖掘效率。进一步的工作包括并行算法复杂性研究。

参 考 文 献

1 Hong J. Incremental Discovery of Rules and Structure by Hierarchical and Parallel Clustering In Knowledge Discovery in Database. In: G. Piatestsky-Shapiro and W. J. Frawly, eds. AAAI/MIT Press, 1991

2 Agrawal R, Imielinski T, Swami A. Mining Association Rules Between Sets of Itenms inLarge Databases. SIGMOD'93, ACM, 1993

3 Agrawal R, Shafer J C. Parallel Mining of Association Rules. IEEE Trans. on knowledge and Data Engineering, 1996, 8(6)

4 周斌，吴泉源. 序列模式挖掘的一种渐进算法[J]. 计算机学报，1999, 22(8): 882～887

5 Joshi M, Karypis G, Kumar V. A Universal Formulation of Seuential Patterns: [Technical Repirt N0. 99-021]. Department of Computer Science, University of Minnesota, 1999

6 Joshi M, Karypis G, Kumar V. Parallel Alogrithms for Mining Sequenctial Associations: Issues and Chanllges: [Technical Repirt N0. 01-021]. Department of Computer Science, University of Minnesota, 2001

7 Ahola J. Ming Sequential Patterns. VTT Information Technology, 2001, 5

(上接第113页)

① 限制智能卡用户的范围

·有些智能卡，任何人都可以读取卡上信息，像记录病人姓名和血型的医疗卡，这种智能卡一般不设密码，只要拿到卡的人都可以读取卡上信息。这时卡体本身就是一种保护。

·对于只许持卡人读取信息的智能卡通常采用一种叫PIN(个人识别码)的密码形式来保护卡上的信息，通过键盘输入读卡器，只有PIN码核对正确了，用户才能对该卡进行操作。典型的应用是手机的SIM卡。

·对于只许第三方读取信息的智能卡便只有发卡人才读取卡上信息，比如银行卡。这时这些智能卡由16～32位数字的密码来保护。Java智能卡可以采取这种方式。

② 限制读取Java智能卡信息的方式(只读、可添加、可修改或可擦写)。存储在Java智能卡上的信息一般被划分为若干个部分：只读信息、只可添加的信息、只可更新的信息和无法读取的信息。这样有些密码信息就可以存储在无法读取的存储区域中。

(2)从卡的结构和支持的加密算法来控制

如上所述只有知道密码的人才有权使用Java智能卡，但如果需要通过无线电或电话线将卡上的信息向异地传送，还必须要有额外的防护手段。

防护手段之一就是加密。Java智能卡有加密和解密的功能，使得在传送存储在卡上的信息的同时，也不用担心会发生泄密。

由于Java智能卡带有微处理器，同时又支持对称密钥算法和公开密钥算法，而且它的尺寸大小极便于携带，因此它本身就是网络数据传递和身份认证极佳的安全模块。目前Java智能卡支持DES算法和RSA算法，可以选择适当的加解密算法。这种防范机制可以确保所用的卡和计算机都真实有效，使得几乎没有可能半路窃取传送的信息。

(3)从是否执行指定的代码段来控制

可根据代码段计算出一个散列函数值，并将其附在代码段后面，然后再加密代码段。这样，Java智能卡可通过验证代码段的散列函数值来决定是否执行该代码段，从而避免执行恶意的代码段，躲开可能的攻击。

结束语 本文在论述当前移动代理的安全性问题及现有的移动代理保护方案的基础上，主要提出了采用Java智能卡(JavaCard)来保护移动代理，构建了采用JavaCard的移动代理系统的安全参考模型，同时对Java智能卡自身的安全问题进行了分析，并给出了较为有效可行的方案。

参 考 文 献

1 Hohl F. A Protocol to Detect Malicious Hosts Attacks by Using Reference States: [Technical Report Nr. 09/99]. Faculty of Informatics, University of Stuttgart, Germany, 1999

2 Vigna G. Cryptographic Traces for Mobile Agents. in Mobile Agents and Security Lecture Notes in Computer Science, Springer-Verlag, June 1998

3 Sander T, Tschudin C F. Towards Mobile Cryptography: [Technical Report 97-049]. International Computer Science Institude, Berkeley, 1997

4 Hohl F. Time Limited Blackbox Security: Protecting Mobile Agents From Malicious Hosts. In: Giovanni Vigna, ed. Mobile Agents and Security, LNCS 1419, Springer, 1998. 44～60

5 Wilhelm U G, Staamann S M, Buttyan L. A Pessimistic Approach to Trust in Mobile Agent Platforms. IEEE Internet Computing, September/October 2000

6 丁建国，柳惠琳，陈涵生，白英彩. 移动代理的一种安全认证机制. 计算机工程，2001, 27(2)

7 朱向华，万燕，孙永强. 移动代理系统的安全机制. 计算机科学，2001, 28(1)

8 李增智，李刚，韩冬，王志文. 智能卡的新发展——JavaCard技术综述. 计算机科学，2001, 28(7)