面向网络管理的移动主体安全设施*

杨 博+, 杨 鲲, 刘大有

(吉林大学 计算机科学与技术学院,吉林 长春 130012)
(吉林大学 符号计算与知识工程国家教育部开放实验室,吉林 长春 130012)

Mobile Agent Security Facility for Network Management

YANG Bo+, YANG Kun, LIU Da-You

(College of Computer Science and Technology, Jilin University, Changchun 130012, China)
(Open Symbol Computation and Knowledge Engineering Laboratory of State Education Department, Jilin University, Changchun 130012, China)
+ Corresponding author: Phn: 86-431-5166479, Fax: 86-431-5166063, E-mail: yangbojlu@sina.com
http://www.jlu.edu.cn
Received 2003-04-03; Accepted 2003-06-04

Yang B, Yang K, Liu DY. Mobile Agent security facility for network management. *Journal of Software*, 2003,14(10):1761~1767.
http://www.jos.org.cn/1000-9825/14/1761.htm

Abstract: Mobile Agent technology provides a new means for network management, but it also brings some insecurity factors at the same time. Based on the analysis of the security threats and the corresponding measures that may occur during the policy and mobile agent based network management applications, the MASF (mobile Agent security facility) for network management is presented. MASF supports a wide span of security mechanisms such as storage protection, confidentiality, authentication, integrity, authorization and security log, all these mechanisms are seamlessly integrated to secure the network management. Based on MASF, a practical network management application, inter-domain virtual private network configuration, is developed. Verified by the application, MASF can satisfy with most security requirement of network management.
Key words: mobile Agent; security; policy; networking management; virtual private network

摘 要: 移动主体技术为网络管理提供了一种新方法,但同时也带来了一些不安全因素.全面分析了采用策略与移动主体技术进行网络管理所面临的各种安全问题和相应的解决方案,提出了面向网络管理的移动主体安全设施MASF(mobile Agent security facility).MASF 无缝集成了存储保护、加密、鉴别、完整性验证、授权、访问控制、安全日志等安全机制.基于 MASF 开发了一个实际的域间虚拟专用网络管理系统,应用表明,MASF 能较好地满足网络管理的安全需求.
关键词: 移动主体;安全;策略;网络管理;虚拟专用网络

* Supported by the National High-Tech Research and Development Plan of China under Grant No.2001AA115160 (国家高技术研究发展计划(863))

第一作者简介: 杨博(1974－),男,河南新乡人,博士,讲师,主要研究领域为移动 Agent 技术,多 Agent 系统,知识工程.

中图法分类号: TP393 文献标识码: A

客户/服务器模式是当前网络管理的基本模式.随着网络日趋复杂、规模不断扩大、应用服务数量巨增,这种管理方式的缺点越来越明显,已无法胜任管理像 Internet 这样开放、分布、异构的大型网络.寻求一种新型网络管理技术,满足自动、灵活和智能的网络管理需求是当前网络管理的一个研究趋势.

基于策略的网络管理(policy based network management,简称 PBNM,)是 IETF(Internet Engineering Task Force)推荐的一种新型的大型网络管理方法.PBNM 有别于传统网络管理方法,可以对位于不同域、不同类型的网络设备进行控制,使它们有机地、协同地工作,以提供所需的服务[1].PBNM 的研究和应用已成为网络管理领域的一个热点,Cisco,Nortel,Lucent 等大型网络设备制造公司都推出了自己的 PBNM 实验平台.现阶段,PBNM 的主要缺点在于自动化程度较低,管理大规模网络时需要管理员过多地干预.采用移动主体技术(mobile Agent technology,简称 MAT)可以很好地解决这个问题.

MAT 是一种新兴的软件技术.该技术能有效地降低分布式计算的网络负载,具有跨平台计算能力,支持离线计算、并行计算,支持实时远程交互、异步自主交互,还能动态适应网络环境、提供个性化服务[2].移动主体(mobile Agent,简称 MA)可作为网络管理员的智能代理,携带需要实施的管理策略,自主地移动到需要配置的网络设备或附近的设备上,执行参数设置、故障诊断与恢复、软件安装与升级等任务.研究表明,MAT 与 PBMN 两种方法的结合能够自动、灵活、快速地管理网络中的设备和资源[3].

尽管采用 MAT 进行网络管理具有很多优点,但该技术也给网络管理带来一些新的问题,其中最主要的是安全问题.例如,配置位于不同域的多个路由器,在执行任务过程中,MA 的状态或代码被途经节点篡改,致使 MA 到达目标设备后不能进行正常的管理工作,甚至对网络设备进行恶意攻击.

在移动主体研究领域,研究者对安全问题展开了广泛的研究,提出了多种方法和技术[4],如基于软件的错误隔离、代码数字签名、状态评估、携带证明代码、相互记录旅行历史等.这些方法在一定程度上保护了移动主体系统和移动主体的安全性.与这些研究不同的是,本文重点从网络管理的角度研究移动主体系统的安全问题,针对采用 MAT 实施网络管理过程中面临的各种安全问题给出相应的解决方法,在此基础上提出一套全面、实际的解决方案——面向网络管理的移动主体安全设施 MASF(mobile Agent security facility).

1 基于 MAT 与 PBNM 网络管理系统及其安全性分析

1.1 体系结构和工作原理

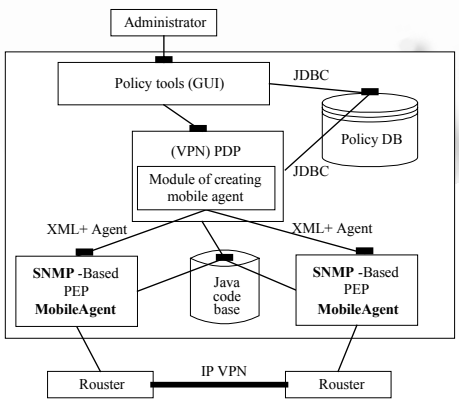

Fig.1 Network management based on the mobile Agent and the policy

图 1 基于移动主体和 Policy 的网络管理

图 1 给出了基于 MAT 和 PBNM 网络管理的基本结构和工作原理. 管理员在网络管理站上通过 policy 管理工具进行 policy 的定制、修改和实施,实现对网络的管理,基本过程如下:

步骤 1:新生成的 policy 转化为规则形式,以 XML 格式存储在 policy 库中;步骤 2:被实施的 policy 从网络管理站通过 PDP(policy decision point)接口(图中小黑框表示接口)传输到各管理域的 PDP 模块上;步骤 3:PDP 模块通过 JDBC 访问 policy 库,对需要实施的 policy 进行冲突验证;步骤 4:PDP 模块基于被实施的 policy 进行决策,规划出需要访问的网络设备列表以及在每个设备上需要执行的动作,给出该动作在代码库(code base)中的链接,最后调用“移动主体生成模块”生成一个或多个 MA;步骤 5:MA 根据路由表规定的路线移动到指定的 PEP(policy enforcement point)上,PEP 可以是路由器等网络设备,也可以是管辖该网络设备的工作站;步骤 6:在 PEP 上,MA 执行规定的动作,如使用 SNMP(simple network

management protocol)协议对网络设备进行配置.步骤 7:反复执行步骤 5 和步骤 6,直到规定的管理任务完成为止.在图 1 中,PDP 同时生成两个 MA,分别移动到不同的 PEP 上建立 VPN 隧道的左端和右端.

1.2 问题与对策

在上述过程中,网络管理会面临多种安全威胁,这些威胁可能来自恶意 MA,也可能来自恶意主机.

威胁 A. 在步骤 1 中,policy 库被入侵,待实施的 policy 被篡改或被窃取.

威胁 B. 在步骤 2 和步骤 3 中,policy 在网上传输过程中被窃取或被篡改.

威胁 C. 在步骤 4 中,代码库被入侵,组成 MA 的代码被篡改,从而使生成的 MA 行为异常,更为严重的是,该 MA 变为攻击网络设备的恶意 MA.

威胁 D1. 在步骤 5 中,MA 经过多个网络节点甚至跨越多个域到达 PEP,MA 携带的保密数据(如网络设备的登录密码)被途经节点或其他 MA 窃取.

威胁 D2. 在步骤 5 中,MA 的执行逻辑被途经节点修改,如 MA 的路由表被修改或 MA 的代码被替换.代表网络管理员的 MA 具有较大权限,它们可以对路由器和防火墙等重要网络设备进行配置,一旦这些 MA 的行为被恶意地修改,不仅达不到网络管理的目的,还有可能破坏整个网络.

威胁 D3. 在步骤 5 中,MA 到达的 PEP 是恶意主机伪装的,其目的是偷窃 MA 携带的保密数据.

威胁 E1. 在步骤 6 中,MA 虽然到达正确 PEP,但遭到“服务拒绝”攻击,该 PEP 不允许 MA 对其所管辖的网络设备进行配置,或不提供 MA 执行任务过程中所需要的资源或服务.

威胁 E2. 在步骤 6 中,不能确保 MA 来自信任方,PEP 或其所管辖的网络设备被 MA 攻击、破坏.

威胁 E3. 在步骤 6 中,MA 虽然来自信任方,但其行为超出规定的权限.

威胁 E4. 在步骤 6 中,MA 虽然来自信任方,但它没有执行规定的管理任务.

针对以上分析的各种安全威胁,移动主体安全设施 MASF 采用以下安全策略:

(1) 鉴别(authentication).第一,针对威胁 A,用于检查 policy 库访问者的身份;第二,针对威胁 C,用于检查 MA 代码库访问者的身份;第三,针对威胁 D3 和 E1,用于检查目标主机的身份,保证 MA 只移动到具有合法身份和正确服务品质协议(service level agreement,简称 SLA)的主机;第四,针对威胁 E2 和 E4,用于检查 MA 的身份,身份认证失败或不具有正确 SLA 的 MA 被驱逐出主机.

(2) 机密性(confidentiality).第一,针对威胁 A,对 policy 库中的 policy 加密,避免被窃取;第二,针对威胁 B,对网络中传输的 policy 加密,避免被窃取;第三,针对威胁 D1,对 MA 携带的重要数据进行加密,避免被恶意主体或主机窃取.

(3) 完整性(integrity).网络传输错误或内部信息遭篡改都会导致完整性验证失败.第一,针对威胁 A 和 B,检查经过数字签名的 policy 的完整性,避免 policy 被篡改;第二,针对威胁 C 和 D2,目标主机接收 MA 以后,对 MA 内部状态和代码的完整性进行验证,若验证失败,则要求重发 MA.

(4) 授权(authorization).根据身份认证的结果为 MA 分配访问权限.

(5) 访问控制(access control).根据授权的结果,实时监视 MA 对系统资源的访问行为,判断访问行为是否允许,如果允许,MA 继续执行,否则掷出异常,终止 MA 对资源的访问.访问控制可避免资源被过度使用或被未经授权的 MA 使用,从而避免威胁 E3.

(6) 安全日志(security logging).安全日志服务跟踪、记录与安全有关的所有活动,如身份认证成功或失败、服务和资源被访问情况,事后系统自动或管理员手工分析安全日志文件记录的不安全事件,并作出相应的处理,避免类似事件再次发生.第一,分析 MA 的安全日志,将有“服务拒绝”攻击行为的主机放入“黑名单”,确保 MA 不再移动到其上,避免威胁 E1;第二,分析主机的安全日志,将没有完成管理任务的 MA 放入“黑名单”,确保不再接纳具有相同身份的 MA,从而避免威胁 E4.

2 移动主体安全设施 MASF

2.1 MASF的设计目标

MASF 主要解决采用移动主体技术进行网络管理过程中所面临的安全问题,具体达到如下安全指标:(1) 提供 policy 和 MA 的存储保护机制,保证 policy 和 MA 代码的安全存储;(2) 提供加密通信机制,保证 policy 和 MA 携带的重要数据不被窃取;(3) 提供鉴别机制,保证 MA 和 Agency 具有合法身份且具有正确的 SLA;(4) 提供完整性验证机制,保证 policy 和 MA 不被篡改;(5) 提供授权认证和资源访问控制机制;(6) 提供安全日志机制,跟踪、记录与安全有关的所有事件,包括 MA 安全日志和 Agency 安全日志;(7) 遵循现有安全技术的工业标准.

2.2 MASF的体系结构

MASF 分为两层,高层是功能层(function layer),底层是基本服务层(basic service layer),如图 2 所示.

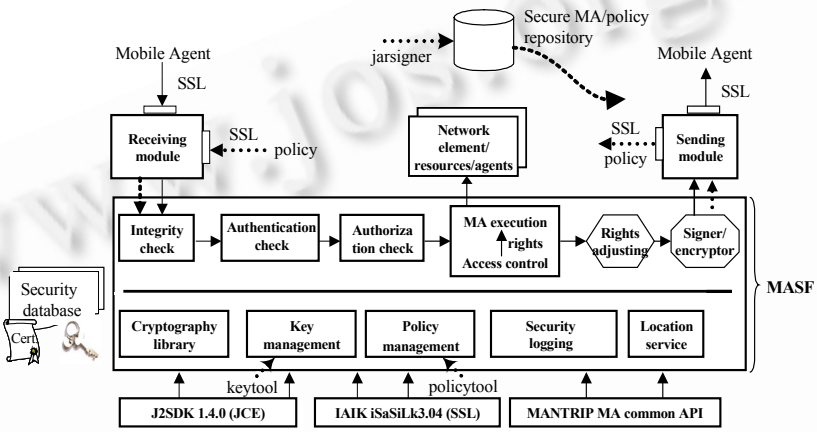

Fig.2 The architecture of mobile Agent security facility
图 2 移动 Agent 安全设施的体系结构

功能层提供面向网络管理的高层安全服务,包括安全存储(security MA/policy repository)、完整性验证(integrity check)、身份认证(authentication check)、授权认证(authorization check)、访问控制(access control)、权限调整(rights adjusting)、数字签名和加密(signer/encryptor).

基本服务层提供与具体应用无关的底层安全服务.功能层中的许多服务都需要使用对称或非对称密钥进行加密、解密或数字签名,因此,MASF 的基本服务层集成了密码库(cryptography library),提供常用的对称和非对称加密算法.密钥管理(key management)服务用于存储和管理公/私密钥对和相关的 X.509 证书链(certificates chain),证书链用于鉴别与私密钥相应的公密钥是否来自信任方.策略管理(policy management)服务用于安全策略的定制和管理.通过认证的管理员或其代理软件使用策略管理服务提供的 API 或 GUI 定义或修改 Agency 或 MA 的访问控制策略.安全日志(security logging)服务跟踪、记录与安全有关的所有活动.定位服务(location service)记录当前系统中运行的角色,用于角色查找和定位.

2.3 MASF的工作原理

(1) 密钥存储与证书交换

使用 JDK 提供的密钥、证书管理工具 keytool 生成用于存放公/私密钥对和 X.509 证书链的 keystore 数据库.keystore 数据库以加密文件形式存放,用密码保护其中的私有信息.

PBNM 的 PDP 模块根据 policy 进行决策,制定 MA 的路由表.路由表分为静态路由表和动态路由表.前者给出完整的迁移路线,后者只给出初始迁移路线,在 MA 迁移过程中,可根据任务的执行情况动态地扩充和修改.每次移动之前,MA 当前所在的 Agency 和目标 Agency 彼此交换证书,相互认证.采用静态路由表,认证的对象和次

序可以事先安排好.若采用动态路由表,认证的对象和次序无法事先确定,认证过程也是动态的.MASF 采用 J2SDK 1.4 提供的 API 进行证书交换,能够实现动态认证过程.

(2) policy 和 MA 的存储保护

所有 policy 策略和组成 MA 的代码都存储在 JAR 文件中,管理员使用 JDK 提供的 jarsigner 工具对这些 JAR 文件进行加密和数字签名.当管理员或其软件代理(如 PDP 模块)需要访问 JAR 文件中的 policy 或代码时,执行如下步骤:(1) 提供表示其身份的证书并通过认证;(2) 解密 JAR 文件;(3) 对 JAR 文件内容进行完整性验证,确保其中的 policy 或代码类没有被篡改或替换.

(3) 移动主体平台的安全设置

在各管理域中的 PDP 和 PEP 上均安装有基于 MASF 的安全移动主体平台 MANTRIP,网络管理员负责设置这些平台的安全属性.

第一,设置功能开关,开启或关闭 MASF 功能层的功能模块.被关闭的模块不再提供相应的安全服务.关闭某些安全检测虽然降低了系统的安全性,但可以提高系统的运行效率.管理员根据网络管理任务的性质权衡安全与性能指标,作出恰当的选择.

第二,定制平台的访问控制策略,生成 policy 配置文件.平台的 policy 配置文件至少包含如下条目(entry):URL location,keystore,alias name 和多个 permission.URL location 指明 MA 来自哪个 Agency;keystore 指明存放 keystore 数据库的路径;alias name 用于在 keystore 中查找 MA 签名者的公有密钥;每个 permission 规定了来自某个 Agency、具有某个管理员签名的 MA 能够以何种方式访问系统的何种资源.

第三,为 Agency 分配密钥对和证书.一个 MANTRIP 移动主体平台中可同时运行多个 Agency.这些 Agency 具有各自的公/私密钥对和证书.MA 能够进入平台中的某一个 Agency 并不意味着它能够进入其他 Agency.

(4) 基于 MASF 的安全网络管理工作流程

在各平台的安全属性设置完毕之后,网络管理员可以实施 policy 执行具体的网络管理任务.考虑安全性以后,第 1.1 节描述的网络管理过程可细化如下:

步骤 1. 新生成的 policy 经管理员加密、数字签名后存储在安全的 policy 库中.

步骤 2. 被实施的 policy 经过 SSL 通道从网络管理站传输到管理域的 PDP 上.

步骤 3. PDP 的接收模块(receiving model)接收来自 SSL 通道的 policy,并将其送入 MASF 接受安全检查.

步骤 4. 完整性验证模块(integrity check)首先解密 policy,然后检验 policy 的数字签名,验证其完整性.若通过验证,则执行步骤 5,否则要求重发 policy,转步骤 3.

步骤 5. 通过 SSL 通道访问 policy 库,对需要实施的 policy 进行冲突验证.

步骤 6. PDP 模块基于 policy 进行决策,形成路由表,从安全代码库中选择代码类创建 MA.

步骤 7. PDP 代表网络管理员对 MA 数字签名,并附上表示管理员身份的证书,证书中包含 MA 创建者和 Home Agency 等信息.

步骤 8. PDP 使用策略管理工具定义 MA 执行期间的安全策略,为 MA 分配必要的访问权限.

步骤 9. PDP 的发送模块(sending model)通过 SSL 通道将 MA 传送到指定的 PEP 上.

步骤 10. PEP 的接收模块(receiving model)接收来自 SSL 通道的 MA,并将其送入 MASF 接受一系列安全检查与控制.

步骤 11. 完整性验证模块(integrity check)首先解密 MA,然后检验 MA 的数字签名,验证其完整性.若通过验证,则执行步骤 12,否则要求重发 MA,转步骤 10.

步骤 12. 鉴别模块(authentication check)对 MA 进行身份认证,获得 MA 的创建者、Home Agency、MA 迁移过程中经过的所有 Agency 等信息.若通过认证,则执行步骤 13,否则要求重发 MA,转步骤 10.

步骤 13. 授权认证模块(authorization check)根据 MA 携带的安全策略、身份认证结果和本地 policy 配置文件为 MA 分配适当的资源访问权限.

步骤 14. 激活 MA,MA 在访问控制模块(access control)的监督下执行规定的网络管理任务.

步骤 15. 当 MA 完成任务需要移动到新位置时,权限调整模块(rights adjusting)根据任务的执行情况修改

MA 的安全策略,改变 MA 在下站 PEP 上的访问权限.

步骤 16. 签名加密模块(singer/encryptor)加密 MA,并对 MA 数字签名,以确认 MA 在该 PEP 上的状态改变.

步骤 17. 与下站 PEP(确切的是 PEP 上的某个 Agency)交换证书和 SLA 协议.若双方彼此通过证书认证和 SLA 审核,则执行步骤 18;否则,结束 MA 本次迁移过程,转向步骤 6,PDP 参考本次任务的执行结果决策新的实施方案.

步骤 18. 重复执行步骤 10 和步骤 17,直到 MA 完成规定的任务.

在网络管理任务的执行过程中,安全日志模块(security logging)追踪、记录所有与安全有关的事件,生成 MA 安全日志和各 PDP,PEP 的 Agency 安全日志.

2.4 MASF的实现

(1) 鉴别的实现.MASF 采用 X.509 证书表示和鉴别 MA,Agency 的身份.采用 J2SDK1.4 的 keytool 工具提供证书管理的基本功能,如创建和存储公/私密钥对;创建、存储、显示(display)、引入(import)和输出(export)X.509 证书等.

(2) 机密性的实现.多数移动主体系统采用非对称的 RSA 加密算法.该算法安全性很高,但计算量太大,不适合大数据量的加密.MASF 采用链式加密算法 RIM[5].RIM 对数据量大的明文采用计算量相对较小的对称加密算法 IDEA 来加密,对 IDEA 的 128 位密钥采用 RSA 算法加密.收件方用 RSA 算法解密出 IDEA 密钥,再用 IDEA 密钥解密数据本身.RIM 既有非对称算法的高安全性和密钥分发的方便性,又有对称算法的快捷性.MASF 采用 JCE(Java cryptography extension)提供的基本加密算法实现了 RIM,对 policy 和 MA 中的保密数据加密,实现了应用层上的数据加密;采用 Java 实现的 IAIK SSL(secure socket layer)加密和认证 TCP 字节流,实现传输层上的数据加密.

(3) 完整性的实现.数字签名时,先用散列算法产生信息量相对较少的信息摘要(message digest),然后用 RSA 私有密钥对信息摘要加密,再加上作者及日期等信息作为一个签名;在验证完整性时,首先用发送方的 RSA 公有密钥解密出信息摘要 D1,然后用相同的散列算法产生接收信息的摘要 D2,若 D1 不同于 D2,则完整性验证失败.MASF 采用单向散列算法 MD5 产生 policy 或 MA 代码类的信息摘要,对任意长度的输入得到 128 位的信息摘要,再使用 J2SDK1.4 的 jarsigner 工具对信息摘要签名.

(4) 授权的实现.采用 J2SDK1.4 的 policytool 工具定义 MA 和 MA 平台的安全策略.这些策略规定了 MA 在 MA 平台上的资源访问权限.

(5) 访问控制的实现.采用 Java 提供的访问控制机制(Java access control mechanism)实现资源的访问控制.在 MA 执行过程中,访问控制器截获 MA 对资源的访问请求,检查该 MA 是否具有访问的权利.

(6) 安全日志的实现.采用 Java Logging 提供的 API 函数追踪、记录与安全有关的所有事件.

2.5 安全与效率

加密/解密、身份鉴别和完整性验证等安全检测带来的开销必定会降低系统的运行效率.网络管理员需要权衡安全性与运行效率两个方面,在保证系统安全的前提下尽量提高系统的运行效率.MASF 采用如下准则处理安全与效率的关系:在执行域内(intra-domain)网络管理任务时,实施弱安全检测;在执行域间(inter-domain)网络管理任务时,实施强安全检测.安全检测的强弱通过设置移动主体平台的安全属性加以控制.在弱安全检测中,关闭 MASF 的大部分功能模块,而在强安全检测中,开启 MASF 的大部分功能模块.例如,当管理公司内部的 Intranet 时,主要考虑运行效率,只需开启 MASF 的访问控制模块和安全日志模块,使用一般 socket 协议传输 MA 和 policy;当被管理的网络由多家公司的 Intranet 组成时,为保护各公司的利益,首要的应是考虑安全性,开启 MASF 中的所有安全检测与控制模块,签名的 MA 和 policy 通过安全的 SSL 通道在域间传输.

3 安全域间虚拟专用网络管理系统

基于 MASF 安全设施开发了基于 IP 协议的域间虚拟专用网络(inter-domain IP VPN)管理系统,用于测试和评价 MASF 的各项安全指标,如图 3 所示.

该系统包括 Blue 和 Yellow 两个域,分别位于吉林大学和英国伦敦城市大学(UCL),每个域包括一个 Cisco 路由器、一台 PBNM 管理站(policy based network management station)和一台作为 PEP 的 Linux 工作站.网络管理员使用 SLA/Policy 管理站实施 VPN 的建立与管理.被实施的 policy 转换为 XML 文件,经管理员加密、签名后从 SSL 通道传输到各域的 PBNM 管理站上.PBNM 的 PDP 模块基于 policy 进行决策,通过 SSL 通道从安全代码库下载经过加密签名的代码类,创建 MA 及其路由表.被签名的 MA 移动到各域的 Linux 工作站上,使用 SNMP 协议对各域的 Cisco 路由器进行配置,分别建立 VPN 的左端和右端,从而建立 VPN 的 IP 隧道.

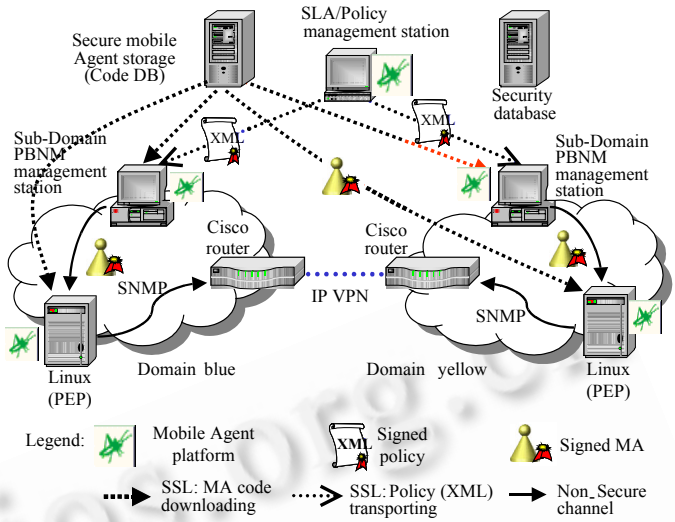

Fig.3 Safe inter-domain virtual private network management system

图 3 安全的域间虚拟专用网络管理系统

域间网络管理涉及诸多不安全因素.实验表明,MASF 能够较好地解决域间网络管理所面临的安全问题,达到设计目标中规定的各项安全指标.

4 结 语

使用移动主体技术进行网络管理具有很多优点,但同时也带来了诸多不安全因素.本文全面分析了这些不安全因素,并给出了相应的安全策略,提出了面向网络管理的移动主体安全设施 MASF.MASF 提供存储保护、加密、鉴别、完整性验证、授权、访问控制和安全日志等多种安全机制,可以有效地解决网络管理中的大多数安全问题.基于 MASF 实现了一个基于 IP 协议的域间虚拟专用网络管理系统.实验表明,MASF 可以较好地解决域间网络管理涉及的诸多不安全因素.虽然 MASF 是针对网络管理提出的安全模型,但其具有通用性,也可用于基于移动主体技术的其他应用领域.结合 SNMP 自身的安全措施进一步改进和增强 MASF 的安全性能是本文进一步的研究工作.

References:

[1] Sloman M, Lupu E. Policy specification for programmable networks. In: Covaci S, ed. Proceedings of the 1st International Working Conference on Active Networks. Berlin: Springer-Verlag, 1999. 73~84.

[2] Lange DB. Mobile object and mobile Agent: The future of distributed computing. In: Jlu E, ed. Proceedings of the European Conference on Object-Oriented Programming. Berlin: Springer-Verlag, 1998. 1~12.

[3] Yang K, Galis A, Mota T, Gouveris S. Automated management of IP networks through policy and mobile agents. In: Karmouch A, Magedanz T, eds. Proceedings of the 4th International Workshop on Mobile Agents for Telecommunication Applications. Berlin: Springer-Verlag, 2002. 249~258.

[4] Tschudin CF. Mobile Agent security. In: Klusch M, ed. Intelligent information agents: Agent based information discovery and management in the Internet. Berlin: Springer-Verlag, 1999. 431~446.

[5] Yang K, Liu DY, Guo X. A template architecture for mobile agent system of high security. Journal of Software, 2002,13(1):130~135 (in Chinese with English abstract).

附中文参考文献:

[5] 杨鲲,刘大有,郭欣.一个具有高安全性的移动 Agent 系统模板结构.软件学报,2002,13(1):130~135.