面向大规模网络应用的移动主体系统安全机制

史 亮，王备战，姜青山，陈黎飞

(厦门大学软件学院 福建 厦门 361005)

【摘要】从系统整体安全的角度，提出一种面向大规模网络应用的移动主体系统安全机制方案。该方案采用基于混合加密的双向认证技术解决移动主体系统的局部安全问题，通过各级移动主体安全管理平台完成密钥的分配与管理，并对移动主体的迁移进行合理的任务分配与调度，通过任务传递模式解决移动主体的跨网段安全迁移问题，这些措施较为全面的解决了当前移动主体系统的整体安全问题。而且由于采用层次化的系统结构和管理模式，使得该方案非常适合当前面向大规模网络的应用开发。

关 键 词 身份认证； 移动主体； 网络应用； 安全机制
中图分类号 TP393 文献标识码 A

A Mobile Agent System Security Mechanism for Large Scale Network Applications

SHI Liang，WANG Bei-zhan，JIANG Qing-shan，CHEN Li-fei

(Software School, Xiamen University Xiamen Fujian 361005)

Abstract This paper presents a mobile agent system security mechanism for large scale network applications. In this mechanism, we use a bidirectional authentication technology based on mixed encryption to resolve the mobile agent system local security problem. Mobile Agent Security Management Platforms (MASMP) working on different levels is applied to deal with the key distribution and management and control the emigration and task attribution of mobile agents. In order to resolve the problem of mobile agent security transference from one network to another, a task transfer model based on the credibility between two conjoint level MASMPs is designed. All these plans together resolve the mobile agent system security problem well. Because of its hiberarchy system structure and management model, this mechanism is very suit for large scale network applications.

Key words identity authorization; mobile agent; network applications; security mechanism

移动主体(Mobile Agent，MA)技术[1]所具有的良好特性为基于网络的应用提供了许多新的技术解决方案。但移动主体技术的推广在很大程度上受移动主体安全问题的制约[2]。移动主体需要移动到主机上并执行相应的代码，但移动主体和服务设施又都不能完全准确地预见相互的行为及后果，所以移动主体系统的安全机制必须是双向的，即服务设施和移动主体既是安全策略的实施者，同时又是被实施的对象。

从现有的移动主体安全问题解决方案[2-9]来看，在保证MA对某个MA平台进行访问时的双方安全，即解决局部安全问题时是卓有成效的。但对于解决具有分层网络结构、包含大量节点、建立在移动主体技术上的应用系统的安全问题，即解决整体安全问题，仍存在一些急待解决的问题，例如如何在保证系统整体和局部两方面安全的前提下，减少系统的运行和维护难度，提高系统应用的灵活性，满足大规模网络应用层次化的系统结构和管理模式的要求等。

本文针对目前移动主体技术在大规模网络应用中存在的安全性问题，结合局部安全问题的解决方案，提出了一种基于层次化系统结构和管理模式的安全机制，尝试从整体安全角度解决移动主体系统的安全问题。

1 局部安全问题解决方案

移动主体系统局部安全问题主要涉及移动主体在与服务设施进行交互时，如何保证双方的安全性，需要解决的是双向的权限和信任问题。

对于移动主体权限问题，本文利用Java自身的

收稿时间：2007 – 08 – 17
基金项目：福建省自然科学基金(2006J0222)
作者简介：史 亮(1973 –)，男，博士，讲师，主要从事智能信息处理与网络信息安全方面的研究.

安全机制[10]来解决。对于移动主体的信任问题，本文采用一种基于混合加密[9]的解决方案。在这种加密通信模式下，通信双方各拥有对方的公钥信息，通信的发起方在每次通信时随机产生一个对称会话密钥Key(如DES密钥)，并用该Key对通信内容以及通信内容的信息摘要进行加密，形成密文C_1，同时用发送方的私钥和接收方的公钥对密钥Key进行加密，得到密文C_2，然后发送C_1、C_2。接收方收到密文后，先用自己的私钥和对方的公钥对C_2解密，得到Key，然用Key对C_1解密，得到通信内容和对应的信息摘要，最后再对该通信内容重新计算信息摘要并将结果与收到的信息摘要比对，以确保通信内容的真实性。如果移动主体的身份被确认，则该主体可以按设定的任务工作，否则该主体将被舍弃。

这种混合加密技术一般不需要额外的通信即可实现双重的身份确认。

(1) 对于发送者，不必担心伪装的接受者会窃取密文中的有用信息，因为它没有真正接受者的私钥，所以它不能进行第一重解密。

(2) 对于接受者，只要它能够完成第二重解密并确认得到的明文是有效的，即可确认发送者的身份无误，因为伪装的发送者没有真正发送者的私钥。

该移动主体局部安全解决方案必须建立在各MA平台持有的私钥是绝对安全的基础上。移动主体按上述局部安全解决方案在接收平台上完成双向认证后，就可以通过移动主体服务设施所提供的平台和接口执行任务。由于移动主体携带的会话密钥Key是一次一密而且不为第三方所知的，所以该移动主体可以用该密钥与发送平台进行后续通信，从而降低计算开销。

2　整体安全问题解决方案

2.1　存在的问题

在解决局部安全问题后，可考虑解决系统整体安全问题。当一次任务的执行只牵涉到一台目标主机时，其安全问题的解决可以参照本文所提出的局部安全问题解决方案，而当所牵涉到的目标主机不止一台时，需分析在沿用现有MA系统的MA迁移机制情况下，系统在安全管理上可能存在哪些问题。

(1) MA从主机A被发送到主机B，为了实现身份认证，收发双方都必须拥有对方的公钥，即如果网络中有安装了MA平台的N台主机，那么每台主机上都需要保存其他N–1台主机的公钥信息。如果某一台主机更换它的公私钥信息，为了保证移动主体在整个系统内的正常迁移，那么其他N–1台主机的相关信息都需要得到及时调整，因此会给系统的管理和维护带来极大的不便。

(2) 如果系统中的某一台主机被入侵者攻克，该入侵者就拥有了向其他N–1台主机发送MA的权力，并且可以篡改经过该主机的MA的代码或截取该MA所携带的数据，威胁整个系统的安全。

(3) 现有的网络系统结构基本上都采用了一种分层的管理模式，如果MA任务执行需要涉及不同子网内部的多台主机，那么对于现行的MA迁移和任务执行模式，以及基于MA和MA平台的安全解决方案来说，是一个很大的挑战。

2.2　改进措施

本文在移动主体系统局部安全问题解决方案的基础上，根据大规模网络拓扑结构和管理模式，对移动主体系统的结构、任务管理和迁移模式进行了设计与改造。

1) 为便于面向大规模网络的应用，本文采用同网络的拓扑结构相似的移动主体系统结构，如图1所示。该移动主体结构由分布在不同网络层面的移动主体安全服务平台(MASMP)和底层的叶节点组成，其中第N层的MASMP负责第N+1层的移动主体及其服务设施的安全管理，包括公钥证书的产生与分发(仅针对相邻的下一层节点)，以及移动主体的迁移和任务管理。

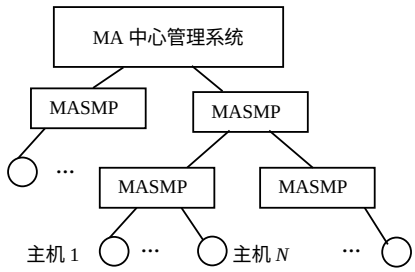

图1　移动主体系统结构

2) 对于任务管理和迁移模式的改进措施主要包括以下两点。(1) 对于子网内部叶节点之间的MA迁移任务，改变以往的多点任务执行模式为单点任务执行模式，即一个MA在一次任务执行过程中仅仅涉及一个目标主机。如需要对子网内部的三台主机A、B和C进行信息采集，不同于以往派遣一个MA依次访问这三个主机，而是分别派遣三个MA到不同主机去执行任务的方式，将原先的串行工作模式改变为并行工作模式。(2) 利用任务传递的方式解决跨网段的移动主体任务执行。移动主体(MA)在执行跨网段任务时，各个网段的MASMP在对该MA进行身份认证后，会将该MA的代码以及执行状态信息重新

封装，生成新的MA，再将新的具有原先MA功能的移动主体发送到子网内部的指定主机，如果涉及多个主机，则可以通过克隆获得多个MA，并分别发送到这些主机。当MA完成任务返回该级的MA监控设施后，就将执行结果汇总后添加到恢复后的原MA中，由其携带相关信息按其原先的路径返回。

在以上两个改进措施的基础上，可以建立一套较为可行的移动主体系统安全框架。由于整个系统采用层次化管理模式，每层的管理由该层之上的MASMP负责，可为MA系统的安全管理和维护提供良好的技术支持，具体的方案如下。(1) 在整个MA系统中，MA和MA平台的双向安全措施将采用本文所提出的权限管理和混合加密的方案。(2) 在每个MASMP上将保存其所管理的下一级网络节点和上一级MASMP上所有MA平台所采用的RSA公钥信息，从而保证从MASMP出发的MA可以在混合加密的情况下访问上级、下级的各个网络节点。(3) 除MASMP外，所有主机上都只保存自身的RSA私钥和上一层MASMP的RSA公钥，而不保存其他同级主机的RSA公钥限制MA在叶节点之间进行直接移动。(4) 只有各级的MASMP具有派遣MA到下级节点(包括MASMP和叶节点)执行任务的权力，底层的叶节点和低层次MASMP无权发起一次涉及到其上层MASMP的MA任务。

3 改进后系统的运行方式

以下分析采取上述措施对移动主体系统的运行方式的影响，以及在新的运行模式下如何保证整个系统的安全。

3.1 子网内的MA迁移模式

在子网环境中，假定一次移动主体任务的执行要涉及到主机1和主机2。在改进的移动主体系统中，由于移动主体从一个平台迁移到另外一个平台必须通过混合加密的身份认证，而主机1和主机2相互间并不拥有对方的RSA公钥，所以主机1和主机2之间的MA迁移通道实际上是被阻塞的。在这种情况下，要完成上述任务可以通过并行方式来实现，即任务发起方MASMP克隆两个功能相同的移动主体，分别派往主机1和主机2执行任务。

3.2 跨网段的MA迁移模式

对于移动主体的跨网段任务执行问题，本文采用任务传递的解决方案。以图2为例，处于上层网络的$MASMP_1$需要派遣MA到子网A中的主机2上执行任务，其整个执行过程如下。(1) 首先利用前面所提出的混合加密方法，用$MASMP_1$的私钥和子网A中$MASMP_2$的公钥对该MA进行封装，并将其发送到子网A中的$MASMP_2$。(2) 当子网A中的$MASMP_2$对来自$MASMP_1$的MA进行身份认证后，将赋予该MA一个ID编号，然后利用自身的私钥和主机2的公钥对解密后的MA和该MA的ID编号进行混合加密，并将生成的MA^*发送到主机2。(3) 在到达主机2并经过身份认证后，该MA^*就可以在本地执行任务，完成后携带结果返回子网A中的$MASMP_2$。(4) 该MA^*携带数据返回$MASMP_2$后，$MASMP_2$首先对其进行身份认证，得到解密后的MA及其携带的数据和该MA的ID编号，$MASMP_2$根据自身的任务分配记录和MA的ID编号查看该MA的来源，如果来自自身、子网内同级MASMP或子网外的上一级MASMP，则继续执行；否则将该MA遗弃。在完成上述认证后，$MASMP_2$将利用$MASMP_2$的私钥和$MASMP_1$的公钥对该MA及相关数据进行封装(即混合加密)，并将其发送回MASMP。

通过上述过程就可以实现基于任务传递的跨网段MA迁移。

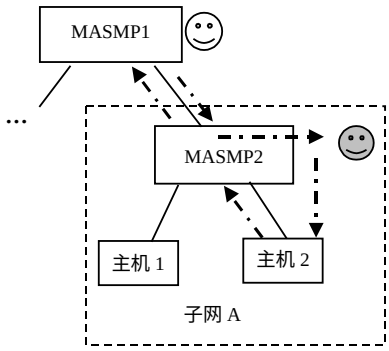

图2 基于任务传递的MA迁移方案

3.3 实际应用中的考虑

对于同网段内的MA迁移和任务执行，本文所提出的迁移模式基本能满足目前网络应用的要求，具有可行性。

本文所提出的基于任务传递的方案可以解决由高级别MASMP发起的跨网段MA迁移。但需要指出的是，根据MA迁移措施，同级别的不同子网之间不能进行MA迁移，而且低级别的MASMP也无法派遣MA到高级别的子网中去执行任务。而在实际应用中，有时需要这类模式的MA迁移，如在基于MA的分布式入侵检测中，需要利用MA在不同级别的子网中收集信息，完成诸如入侵追踪等工作。本文的解决方案是：采用非MA技术完成任务定制(如将相关信息沿系统层次结构由低向高进行汇总)，然后由该

次任务所涉及到的最高级别的MASMP发起该次MA任务，就可以在满足系统约束的前提下，完成这类模式的MA迁移和任务执行，基本满足目前大规模网络应用对MA的要求。

4　系统安全性分析

4.1　对移动主体自身性能的影响

从改进后的方案来看，由于各个叶节点之间的MA通道被阻塞，使得移动主体迁移的灵活性受到一定制约，但可以通过采用MA的并行任务执行模式得到解决，并不影响移动主体技术自身所具有优点的发挥。跨网段MA安全迁移扩展了MA的任务执行能力。而且需要指出的是，在进行了上述改造后，移动主体系统在整体安全性、可管理性、可维护性等方面较之原先的移动主体系统，其解决方案更为可行、实用，保持了移动主体技术的可移动性、自治性、跨平台等良好特性。

4.2　密钥分配与管理

由于子网内部各个叶节点的公钥信息是由其上一层MASMP统一管理的，而每个叶节点并不拥有其他叶节点的公钥，所以任一叶节点密钥的改动仅牵涉其自身以及上一层的MASMP，在减轻了系统安全维护任务的同时，大大降低了整个系统的安全隐患。

4.3　典型攻击下系统的安全性分析

可通过一些典型的案例来分析系统的安全性。可能的攻击有：(1) 某一叶节点被攻克，该节点不能为MA提供服务。(2) 某一叶节点被攻克，入侵者通过该节点上的MA平台对到达的MA进行篡改。(3) 某一叶节点被攻克，入侵者通过该节点上的MA平台发送恶意的MA到其他叶节点。由于移动主体的任务执行模式为单点任务执行模式，每个移动主体的工作对象仅局限于一个目标主机，对于攻击(1)，如果该主机不能向MA提供服务，那么受影响的仅仅是该主机本身，而对MA在系统中其他主机上的任务执行不构成影响。对于攻击(2)，道理也一样，由于MA的工作模式为单点任务执行模式，叶节点之间不存在直接的MA通道，所以即使MA被篡改，也无法对其他主机造成后续影响。至于攻击(3)，由于叶节点之间没有直接的MA通道，而且系统中MA任务的发起者只能为各级的MASMP，所以入侵者想通过被攻克的叶节点上的MA平台向其他叶节点发送恶意MA的方案是行不通的。(4) 某一叶节点被攻克，入侵者通过在该节点进行嗅探，截取其他MA的信息进行分析。由于每个叶节点并不拥有其他叶节点的RSA密钥信息，所以即使截获MASMP发向其他叶节点或MASMP的MA，由于无法获取RSA密钥对DES密钥进行解密，所以无法了解该MA的实质内容。(5) 某一叶节点被攻克，入侵者通过该节点上的MA平台以上一层MASMP的身份发起一次MA的任务执行过程。MASMP发起一次MA的任务执行过程时，其发送的MA要么去某个下级叶节点，要么发送到其他MASMP。对于第一种情况，由于该叶节点上没有其他叶节点以及其他MASMP节点的公钥信息，所以即使该MA被发送到对方节点上，也会由于无法通过身份认证而被对方舍弃。(6) 某个MASMP被攻克，入侵者以其为平台对系统中的其他主机进行破坏。(7) 某个MASMP遭到拒绝服务攻击，无法响应外部请求并提供服务。

在系统设计时，作为系统重要组成部分的MASMP一般都设置在安全级别较高的主机上(可以通过技术手段实现，虽然会增加每个MASMP的防御成本，但由于MASMP的数量相对于整个系统的节点数来说较少，因此总的成本增加幅度并不大)，入侵者很难获取访问权限。因此，对于攻击(6)，其实现的可能性很小。但是由于MASMP仍需要保留部分服务，所以系统仍会受到拒绝服务攻击的影响，即攻击(7)的情况是有可能发生的。本文采用较为成熟的防御拒绝服务攻击的技术(如双机热备份、容侵技术等)，使得在MASMP遭到拒绝服务攻击的情况下，系统仍可以正常工作。

由上面的分析可知，本文提出的移动主体系统在密钥的分配与管理上更为方便可靠，在保持移动主体良好技术特性的前提下，较好地解决移动主体系统局部和整体安全问题。

5　结 束 语

移动主体的安全性问题是该技术推广应用的一个主要障碍，本文从整体安全的角度，提出一种面向大规模网络应用的移动主体安全问题解决方案，该方案较好地解决移动主体系统局部安全和整体安全问题，使得跨网段移动主体安全迁移成为可能。而且由于其层次化的系统结构和管理模式，使得该系统非常适合当前面向大规模网络的应用开发。

本文研究工作得到厦门大学985期创新平台(0000-X07204)和引进人才科研启动费(0680-XK0002)支持，特此表示感谢！

(下转第1218页)

具有更好的实时性。

表1 IADW与其他异常入侵检测方法比较

方法	检测率/(%)	错误告警率/(%)	漏检率/(%)	分类率/(%)
IDS-ANN	90.44	2.78	6.78	78.50
ID3-ids	93.65	1.64	4.70	77.25
IADW	96.61	2.78	2.78	80.56

从实验结果可以看出，IADW较传统的基于神经网络和ID3算法的Web攻击检测方法，具有更好的学习识别能力和自适应能力，同时也具有很好的实时性。

3 结 论

IADW吸取了生物免疫系统快速学习并识别新病原体之优点，能有效检测针对Web服务器的攻击，克服了传统Web攻击检测方法不能检测未知Web攻击和误报率高、实时性差等缺陷，具有高检测率、高分类率、低漏检率和实时性好等特性，是检测Web攻击的一种有效新途径。

本文的研究工作得到了四川大学青年教师基金(JS20070411506428)的资助，在此表示感谢！

参 考 文 献

[1] KLEIN D. Defending against the wily surfer: web-based attacks and defenses[C]//Proceedings of the USENIX Workshop on Intrusion Detection and Network Monitoring. California, USA: [s.n], 1999.

[2] ADEVA J J G, ATXA J M P. Intrusion detection in web application using text mining[J]. Engineering Applications of Artificial Intelligence, 2007, 20(4): 555-566.

[3] ALMGREN M, DEBAR H, DACIER, M. A lightweight tool for detecting web server attacks[C]//Proceedings of Network and Distributed Systems Security. [S.l.]: [s.n.], 2000: 157-170.

[4] ALMGREN M, LINDQVIST U. Application-integrated data collection for security monitoring [C]//RAID 2001, LNCS 2212. Berlin: Springer-Verlag, s2001: 22-36.

[5] VIGNA G, ROBERTSON W, KHER V, et al. A stateful intrusion detection system for World-Wide Web servers[C]//Proceedings of the Annual Computer Security Applications Conference. [S.l.]: [s.n.], 2003: 34-43.

[6] GARCIA V H, MONROY R, QUINTANA M. Web attack detection using ID3[C]//Proceedings of the 2nd IFIP International Symposium on Professional Practice in AI. [S.l.]: [s.n.], 2006: 323-332.

[7] 李 涛. 计算机免疫学[M]. 北京: 电子工业出版社, 2004.

[8]焦李成, 杜海峰. 人工免疫系统进展和展望[J]. 电子学报, 2003, 31(10): 1540-1548.

[9] LI T. An immune based dynamic intrusion detection model [J]. Chinese Science Bulletin, 2005, 50(17): 1912-1919.

[10] DASGUPTA D. An immunity-based technique to characterize intrusions in computer networks[J]. IEEE Transactions on Evolutionary Computation, 2002, 6(3): 281-291.

[11] HARMER P K, WILLIAMS P D, GUNSCH G H, et al. An artificial immune system architecture for computer security applications[J]. IEEE Transactions on Evolutionary Computation, 2002, 6(3): 252-280.

[12] FORREST S, HOFMEYR S, SOMAYAJI A. Computer immunology[J]. Communications of the ACM, 1997, 40(10): 88-96.

编 辑 漆 蓉

(上接第1205页)

参 考 文 献

[1] PHAM V A, KARMOUCH A. Mobile software agents: An overview[J]. IEEE Communications Magazine, 1998, 36(7): 26-37.

[2] GREENBERG M S, BYINGTON L C, HARPER D G. Mobile agents and security [J]. IEEE Communications Magazine, 1998, 36(7): 76-85.

[3] TARDO J, VALENTE L. Mobile agent security and telescript[C]//In: Proceedings of COMPCON Spring '96. Santa Clara: IEEE Computer Society press, 1996.

[4] WALSH T, PACIOREK N, WONG D. Security and reliability in Concordia TM[C]//Proceedings of the Thirty-First Hawaii International Conference on System Sciences. Hawaii: [s.n.], 1998.

[5] JANSEN W A. Countermeasures for mobile agent security [J]. Computer Communications, 2000, 23(17): 1667-1676.

[6] KARJOTH G, LANGE D, OSHIMA M. A security model for aglets[J]. IEEE Internet Computing, 1997, 1(4): 68-77.

[7] 王汝传, 徐小龙, 郑晓燕, 等. 移动代理安全机制的研究[J]. 计算机学报, 2002, 25(12): 1294-13011.

[8] 杨 博, 杨 鲲, 刘大有. 面向网络管理的移动主体安全设施[J]. 软件学报, 2003, 14(10): 1761-1767.

[9] 狄晓龙, 庄镇泉, 张仕山. 移动主体技术的安全机制研究[J]. 小型微型计算机系统, 2004, 25(4): 493-496.

[10] GONG Li. Java 2平台安全技术-结构、API设计和实现[M]. 机械工业出版社, 2000.

编 辑 熊思亮