第 33 卷　第 2 期　　计　算　机　工　程　　2007 年 1 月
Vol.33　No.2　　Computer Engineering　　January 2007
·安全技术·　文章编号：1000—3428(2007)02—0114—03　文献标识码：A　中图分类号：TP309

移动代理在入侵检测中的安全性分析与研究

阳凌怡[1]，陈建华[1,2]，张丽娜[1]
(1. 武汉大学数学与统计学院，武汉 430072；2. 武汉大学密码研究中心，武汉 430072)

摘　要：将移动代理技术引入侵检测这个领域形成了一种新的入侵检测模式。基于移动代理的入侵检测系统存在多种安全威胁，这成为该项检测技术的发展瓶颈。该文分析了基于移动代理的分布式入侵检测系统的工作模式和移动代理的工作过程，结合目前先进的椭圆曲线密码技术，给出了基于移动代理分布式入侵检测系统的一种安全解决方案。

关键词：移动代理；分布式入侵检测系统；安全机制；椭圆曲线密码系统

Security Analysis and Research of Mobile Agents in Intrusion Detection System

YANG Lingyi[1], CHEN Jianhua[1,2], ZHANG Lina[1]
(1. School of Mathematics and Statistics, Wuhan University, Wunhan 430072;
2. Cryptology Research Center, Wuhan University, Wunhan 430072)

【**Abstract**】A much more effective measurement for intrusion detection is provided by introducing the technique of mobile agent into intrusion detection system. This paper explains the integral structure and working modes of the instruction detection system based on mobile agents, and analyzes the main security problems that current mobile agent technique face with. A security mechanism based on elliptic curve cryptosystem is given in the end.

【**Key words**】Mobile agent; Distributed intrusion detection system(DIDS); Security mechanism; Elliptic curve cryptosystem(ECC)

移动代理是独立的可确认的计算机程序，可以为用户完成特定的任务。它可以自主地在网络上按照一定的协议移动，寻找适合自身运行和符合自身任务目标的计算机资源，利用与这些资源同处一台主机的各种优势，处理或使用这些资源，代表用户完成已定的任务。它的智能、灵活的运行机制可以很好地适应入侵检测的多项要求，将它引入到入侵检测中，将会创造更为优越的检测模式。

1 移动代理在入侵检测中的应用

在 DIDS 中采用移动代理技术主要是在所监控网络的重要主机上安装主机监控代理，在各局域网络结点安装网络监控代理。各类监控代理协作完成整个网络的入侵检测功能，并对入侵行为进行处理。移动代理技术可有效地简化分布式系统的设计、实现和维护，并且可减轻网络负担，节约系统资源。

1.1 基于移动代理入侵检测系统的模型结构

本文所研究的基于移动代理的分布式入侵检测系统主要由中心控制分析系统和被监控主机检测系统两个大的模块组成，模型结构如图 1 所示。

中心控制分析系统：包含代理管理服务器 ASM(Agent Manage Sever)负责移动代理的产生，分配和控制管理；数据分析中心 DS(Data Statistics)负责统计分析各个代理采集反馈的数据，根据设计标准选择得出所需要的数据结论，然后送给决策中心；决策响应库(Decision-Making Databases, DMD)在得到需要的数据后，根据已有的知识库储备给出相应的处理决策。

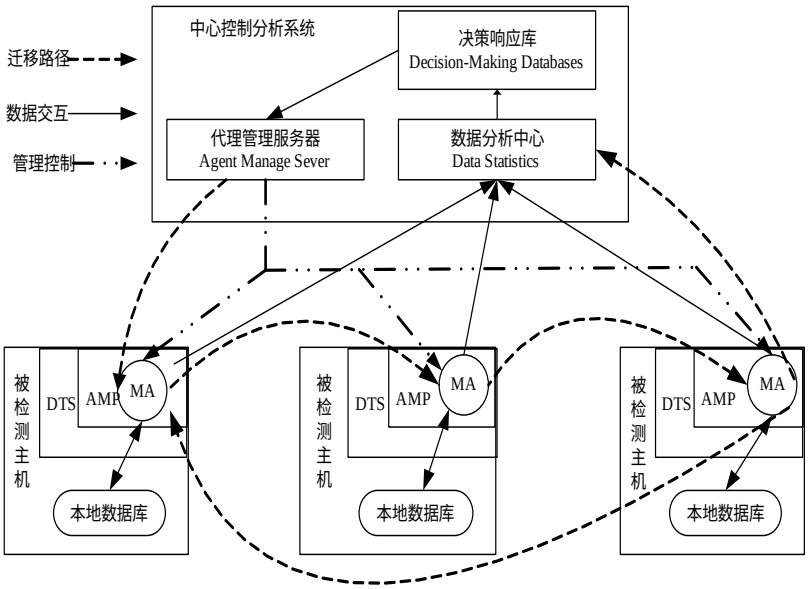

图 1 移动代理入侵检测系统的模型结构

被监控主机上的入侵检测系统：包含入侵检测子系统

作者简介：阳凌怡(1981－)，女，博士生，主研方向：密码学计算算法，芯片设计，快速算法研究；陈建华，博导；张丽娜，博士生
收稿日期：2006-02-10　**E-mail：**ooyli@163.com

DTS(Detector System)负责所在节点的入侵检测工作；可移动代理 MA(Mobile Agent)用于处理各子系统之间通信或协同工作的程序体，必要时可携带数据在网络中移动；代理工作环境 APM(Agent Platform)提供 MA 运行的条件和保护机制，协调和监视 MA 的运行以及处理 MA 与入侵检测系统之间的交互。

1.2 基于移动代理入侵检测系统的工作模式

根据图 1 中迁移、数据交互、管理控制的路径所示，完整的移动代理工作流程如下：

(1)AMS 根据入侵检测系统的检测需求创建相应的 MA，并赋予一定的迁移信息和智能，发送给相应的被监控主机。

(2)MA 到达被监控主机后，就以特定功能的软件实体在新的被监控主机上执行检测任务。

(3)MA 一方面直接从主机获取实时的网络数据，另一方面从本地数据库中获取历史数据。然后对数据进行过滤和分析，并根据既定规则进行判定和处理。

(4)当 MA 在当前主机上的任务完成后，它将根据本身信息和当前主机的信息来决定下一个要到达的被监控主机。然后迁移，在到达新的被监控主机上后继续执行任务。

(5)根据 MA 迁移信息，它可以在所有被监控主机间循环迁移，这个过程中它保存各个处理过程的数据信息。它也可以根据自身检测任务的需要随时返回 DS。

(6)检测后的结果和 MA 不能肯定的可疑数据，将反馈给中心控制分析器的 DS。

(7)DS 将 MA 送过来的检测结果和可疑数据进行综合分析，形成报告发送给 DMD。DMD 对检测到的网络入侵行为给出处理决策。

2 采用椭圆曲线密码技术解决安全隐患

2.1 基于移动代理的安全性问题

从入侵检测的整体角度来看，采用移动代理的入侵检测系统是一个更为开放的网络环境，安全漏洞更容易发生。这主要包括 3 个方面的安全威胁：

(1)恶意代理对代理环境的攻击。恶意代理非法获得 APM 上的有用信息，并利用已获得的合法权限对整个 DTS 进行不被期望的或破坏性的活动。即使恶意代理无法通过授权获得 APM 所在主机的资源，也可通过消耗 APM 所在还境的计算资源来达到拒绝为其他代理服务的目的。

(2)非法代理平台对移动代理的攻击。恶意 AMP 可以方便地从捕获的移动代理中提取信息，破坏或修改移动代理的代码、状态或迁移路径；还可以拒绝请求的服务甚至于将移动代理任务终结。

(3)移动代理在传输过程中受到攻击。窃听，篡改和伪造都是移动代理在传输中经常遭受的攻击，移动代理信息的泄漏和工作性质的改变都会为整个入侵检测带来难以估计的损失。

2.2 椭圆曲线密码技术

公钥密码中的椭圆曲线密码(Elliptic Curve Cryptosystem, ECC)以其得天独厚的技术优势迅速地发展起来。ECC 较短的密文和签名数据可以减少在系统和应用程序之间数据传送量，从而节省了通信带宽。更重要的是在标准模型下论证的 ECC 加密机制在最强的攻击行为下能达到最高的安全性。

以 ECC 构造的签名机制可描述如下：设 E(Fp’)中有一阶为素数 q 的生成元点 G，函数 fx(P)表示取 E(Fp’)的点 P 的 x 坐标，h 为安全 Hash 函数。

密钥生成 选择随机数 $d \xleftarrow{R} Z_q$ 作为私钥，计算 Q←dG 作为公钥。

签名算法 设待签名的消息为m，选择随机数 $k \xleftarrow{R} z_q$，计算R←kG和r←fx(R)，s←k^{-1}(h(m)+dr)modq，输出签名(r,s)。

验证算法 验证等式 r=fx(s-1h(M)G+s-1rQ)是否成立。

2.3 安全解决方案

2.3.1 移动代理的传输安全保障

基于移动代理的入侵检测系统最关键的就是对于迁移中的移动代理 MA 给予足够的安全保护。在 SSL 基础上以 ECC 为加密套件的传输层安全协议将更有效的保护移动代理，同时节约带宽提高传输的效率。

假定检测主机 A 和主机 B 需要进行移动代理的迁移通信。在通信前双方通过可信机构获得对方的公钥证书，验证对方可信度。

当双方建立信任之后启动共享密钥的子程序。这个过程是采用 ECC 签名机制实现。

(dA，QA)是用户 A 的密钥对，用户 B 可通过访问系统可信 CA 获得 QA；(dB，QB)是用户 B 的密钥对，用户 A 可通过访问系统可信 CA 获得 QB；RA、RB 为用户 A、用户 B 选定的随机整数；TA，TB 为时间标识；F(x)是在 ECC 算法的基础上设计的运算函数。x 是前述参数的组合。具体过程如下：

(1)用户 A 选定一个随机整数 RA，计算出 b1＝F(RA)。用户 A 将 b1 用用户 B 加密证书上的公钥 QB 利用 ECC 算法加密，附上时间标识 TA 后，采用自己的数字证书的私钥 dA ，利用 ECC 算法进行数字签名，然后发送给用户 B。

(2)用户 B 选定一个随机整数 RA，计算出 b2＝F(RB)。用户 B 将 b2 用用户 A 加密证书上的公钥 QA 利用 ECC 算法加密，附上时间标识 TB 后，采用自己的数字证书的私钥 dB ，利用 ECC 算法进行数字签名，然后发送给用户 A。

(3)用户 A 将收到加密与签名后的消息先用用户 B 的公钥 QB 进行验证，然后利用自己的私钥 dA 解密，得到 b2。

(4)用户 B 将收到加密与签名后的消息先用用户 A 的公钥 QA 进行验证，然后利用自己的私钥 dB 解密，得至 b1。

(5)用户 A 利用 ECC 算法原理，计算 RAb2＝F(RARB)＝KA。用户 B 利用 ECC 算法原理，计算 RBb1＝F(RBRA)＝KB。则 KA＝KB 双方启动对称密钥加密传输程序进行保密通信。

利用对称算法为需要传输的移动代理数据加密，使有用信息在网络中以密文形式传递。

采用这种方式设计的密钥交换协议和数据传输，从以下几个方面提高了性能和安全性：

(1)产生会话密钥的数据在网络传输中关键步骤仅一步。并且是双方经过不同的密钥加密而来，有很强的即时效应，而且时密钥动态产生可随时更换，网络攻击者没有充分的时间来分析破解。

(2)用可信任 CA 机构签发的数字证书中的公钥传输产生通信密钥的数据，既可验证双方身份又不需要第 3 方密钥的介入。

(3)在消息中附上时间标识，可以预防重放攻击与消息延迟，也保障了协商的有效期。

(4)利用该方法得到的密钥在产生中得到了分配，简化了密钥的管理，提高了密钥的安全性。

通信过程如图 2 所示。

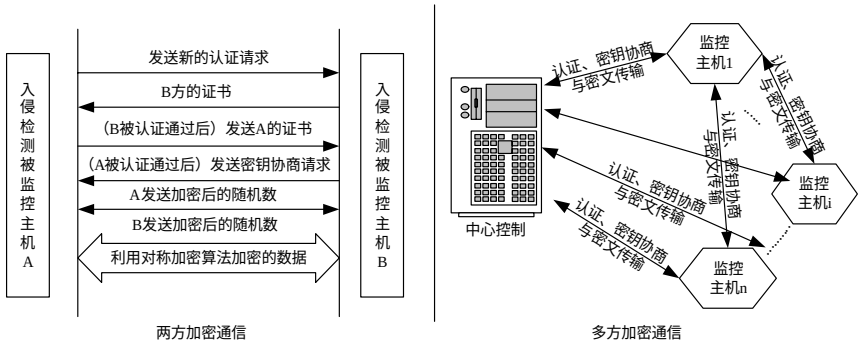

图 2 移动代理的加密传输

2.3.2 入侵检测中实体的可信认证机制

采用椭圆曲线公钥密码机制实现身份认证与授权。假设中心控制分析系统是处于严格安全保护下的，能被MA和AMP信任，拥有自己的证书(C_0)和密钥对(Puk_0/Prk_0)。同一个检测区域中的被监控主机上的AMP也分别拥有自己的证书($C_1,C_2,\ldots,C_n$)和密钥对(Puk_1/Prk_1, $Puk_2/Prk_2,\ldots$, Puk_n/Prk_n)。所有的密钥都是采用ECC算法生成，有可信CA统一颁发证书(即所有被监控主机和中心控制系统可以通过可信渠道获得彼此的公钥)。这时可信实体的私钥保护就显得尤为重要。值得注意的是入侵检测中的监控实体都是具有特殊功能的检测节点主机(包括中心控制分析系统)，拥有很强的实体特征。将这些实体引入到实体认证中，可大大提高实体的安全性。例如可以把实体的特征如网卡物理地址，实体磁盘物理特性，实体管理者口令等信息用混合抽样算法合并后产生保护密钥对私钥加密，让实体存储加密形式的密钥。这样就可以保证在缺少前述信息中任何一项的情况下无法得到实体的私钥，在需要原始私钥时只需利用相同的有用信息再次生成保护密钥解密即可。采用私钥保护的签名如图 3 所示。

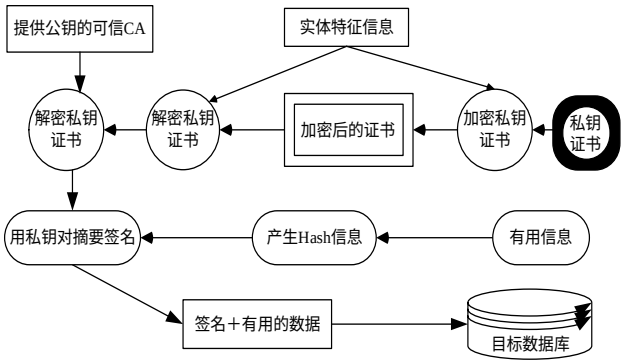

图 3 采用私钥保护的签名

移动代理在整个入侵检测系统中运行的认证检测流程如下：

(1)中心控制分析系统根据系统的策略创建相应的MA，利用中心私钥Prk_0加密证书C_0，并且对加密后的证书C_0’、MA的执行代码P、迁移信息R和有效时间信息T的摘要，进行签名Sig(h(C_0’, P, R, T))。

(2)中心控制分析系统与目标主机之间利用已经设计好的基于ECC算法密钥交换协议进行密钥协商，产生会话密钥K_0。利用会话密钥采用既定的对称算法对带有签名信息的MA数据加密。

(3)将加密数据E_{K0}(MA，Sig)送达目标主机。

加密的移动代理到达目标主机后。1)主机的APM用会话密钥K_0解密数据，计算Ver(Sig)判定签名是否合法有效。2)利用中心的公钥C_0解密证书。根据得到的信息判定MA的来源是否有效，MA的使用信息是否有效，MA的使用效力是否仍在有效期内。如果所有判定通过，移动代理通过身份认证，根据自身特性获得相应的权限，AMP启动MA进行工作。

在MA的任务完成后，需要进行迁移。采用类似中心控制分析系统的工作方式，MA此时所在的检测平台APM_i利用Prk_i、C_i、P_i、R_i、T_i，形成新的签名Sig_i。需要注意的是此时一般是对MA的新的敏感信息(如该主机的信息，MA的新的迁移信息等)摘要签名。也就是说Sig_i所对应的签名内容并不完全一致，根据迁移的变化增加、删除、更改了相应的信息。此后，该主机与下一目标主机协商形成会话密钥K_i，加密代理将数据E_{ki}(MA，Sig_i)送达目的地。以后MA的迁移认证过程依此类推。

这种安全机制实现了移动代理入侵检测系统中的认证与加密需求，确保对了基于移动代理的分布式入侵检测系统的安全性。整个解决方案建立的以 ECC 为基础的检测安全机制是同时具备认证性、机密性和完整性的运行机制，为 DIDS 建立了适合移动代理的加密和认证运行方案，确保移动代理在分布式入侵检测系统中的安全运作。

3 结束语

移动代理本身的安全问题的研究还不太成熟，但是发展很快。结合分布式入侵检测系统传统研究移动代理的安全性更具有针对性和特殊性。通过分析入侵检测系统的运行过程，把握移动代理灵活的迁移特性，将侧重于研究检测平台的保护措施转移到发展移动代理在入侵检测环境中的传输、认证保护技术上，从而使其具有更为实效的意义。同时需要注意的是，设计移动代理系统安全框架的原则是在不降低系统性能的基础上提高安全服务。这需要开发者结合移动代理的运行领域特性在安全、性能和成本中做出权衡。

参考文献

1 Krugel C, Toth T. Applying Mobile Agent Technology to Intrusion Detection[C]. Proc. of ICSE Workshop on Software Engineering and Mobility, 2001.

2 Wilhelm U G, Staamann S M. A Pessimistic Approach to Trust in Mobile Agent Platforms[J]. Internet Computing, IEEE, 2000, 4(5).

3 Mar J, Lee K M. Application of Certificate on the ECC Authentication Protocol for Point-to-point Communications[C]. Proc. of the IEEE 37th Annual 2003 International Carnahan Conference, 2003: 222-224.

4 Nash A, Duane W, Joseph C, et al. 公钥基础设施(PKI)——实现和管理电子安全[M]. 北京: 清华大学出版社, 2002: 182-185.

5 史卫军，马健峰. 一种基于移动代理的入侵检测系统模型[J]. 计算机工程与设计, 2003, 24(8): 4-7.

6 徐小龙，王汝传. 移动代理安全机制的研究[J]. 计算机工程与应用, 2004, 22(8).

7 王惠芳. 移动代理的安全解决方案[J]. 计算机工程, 2002, 28(1).

8 张险峰，秦志光，刘锦德. 一个基于 ECC 的双向认证协议[J]. 计算机科学, 2002, 29(8): 36-38.