基于 TPM 硬件的移动 Agent 安全模型研究*)

武小平　赵　波　张焕国
（武汉大学计算机学院　武汉 430079）

摘　要　主要讨论了安全强度较高的基于硬件的移动 Agent 安全方案。将可信计算技术与平台引入移动 Agent 的安全机制，基于可信硬件 TPM 所提供的相关安全服务实现移动 Agent 的主动保护机制。设计了在可信硬件平台上的移动 Agent 安全框架模型并进行了详细分析。

关键词　移动 Agent，安全模型，TPM

Research on Mobile Agent Secure Model Based on TPM Hardware

WU Xiao-ping　ZHAO Bo　ZHANG Huan-guo
(Computer School, Wuhan University, Wuhan 430079, China)

Abstract　This paper discusses the secure frame of mobile agent based on hardware which has higher security intensity. Trusted computing technology and platform are introduced into mobile agent security mechanism to achieve mobile agent's active protection based on the trusted hardware TPM. The model of security on trusted hardware platform is designed and analyzedin detail.

Keywords　Mobile agent(MA), Secure model, Trusted platform module(TPM)

1　引言

随着互联网的快速发展，移动 Agent 在电子商务、电子政务、网络安全管理、网格计算等实际应用领域中有着广泛的应用前景。然而，移动 Agent 面临的一个重大挑战就是其安全性。现有的研究基本上从身份认证、数据传输安全、主机资源保护和恶意主机等几个方面展开。基于传统的安全技术，如授权、身份认证、访问控制、通信加密等对于数据传输、主机资源保护等，都已经提出了较为成熟的解决方案[1,2]。但是，在分布式计算环境中，作为资源提供者的主机必须承诺具有保护分布式系统信息安全的能力，也就是能够给分布式应用提供安全的计算环境，才能保证移动的 Agent 不受恶意主机的攻击。这在整个分布式系统的安全问题中是属于最为难以解决的问题。本文针对这方面的问题，提出基于可信硬件的安全模型，从计算终端的体系结构来控制，旨在从源头开始构建可信的分布式计算环境。

2　相关研究工作

现有的针对移动 Agent 系统安全的研究从不同角度进行了尝试，如基于被动检测的安全措施，加入状态评价函数，对计算函数进行加密等[1-5]。然而，这些方案的一个共同点就是都假设终端平台是安全的，然后在上层应用实施这些附加的安全措施。要实现真正的从底层开始保证分布式系统的信息安全，分布式系统的设计者在考虑系统间交换信息时，必须进行通讯终端的身份识别和认定。终端的组成成分在整个系统中和通信协议具有同样的重要性。终端系统除了能提供访问控制机制以外，还要能够向远程系统出具能够保障该机制的相关证明和实现受保护的密钥存储、保护协议数据条例等。

一种完全不同的安全策略是采用基于可信任的、防攻击的硬件来实施对移动 Agent 的主动保护措施。其核心思想是给移动 Agent 系统配置额外的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。这种基于硬件的安全策略能够从更深层次来实现移动 Agent 的保护，因而也得到了研究者的认同，并提出了一些具体的解决方案。文献[3]就是采用符合 JavaCard 规范的智能卡作为可信赖的附加硬件，给出了一种具体的方案模型，而且从可行性的角度进行了相应算法分析。但是该方案的一个主要问题就是没有很好的策略来解决分布式应用中应用与终端、终端与终端之间的信任关系描述和传递问题，仅是采用一种简单的信任替代：移动 Agent 属主对 JavaCard 制作者的信任简单地取代了其对 JavaCard 设备所有者即目的主机的信任。而这种信任是没有任何认证和授权等措施的，一旦被恶意利用，则所有的代理都将失去控制。因此，在可信赖硬件的基础上再引入信任机制来加强系统的安全性，也得到了很多研究者的认同，并将研究的重点放在如何构建适应分布式计算的可信计算环境和各个实体如何进行可信的交互上[7,10,12]。

目前，TCG[8]在可信计算的规范和实现方面已做了大量的工作，其主要思想就是从一个硬件信任根开始建立一条信任链，系统每一次控制权转移之前对下一组件进行完整性度量，因此从信任根开始到硬件平台、操作系统，再到应用，一级认证一级，一级信任一级，逐步把这种信任扩展到整个计算机系统。这种信任链传递机制是可控的并且通过具体的核心硬

*)国家 863 计划：可信 PDA 计算平台关键技术与原型系统研究(2006AA01Z442)，武汉市青年科技晨光计划：可信计算平台上的移动代理安全研究项目(200850731373)。**武小平**　博士，讲师，主要研究方向为可信计算、分布式安全；**赵　波**　副教授，主要研究方向为信息安全；**张焕国**　教授，博导，主要研究方向为信息安全。

件芯片 TPM(Trusted Platform Module,可信平台模块)[9,11]来实现。结合可信计算的思想,我们对移动 Agent 系统的原有安全模型进行了扩展,提出了基于可信硬件平台的移动 Agent 保护体系,该体系的核心就是利用硬件 TPM 芯片来提供密钥管理和系统结构管理,从而提高整个系统的安全性能。

3 基于 TPM 的安全模型分析

3.1 模型简介

我们基于 TPM 硬件模块的安全功能,对移动 Agent 原有的系统框架进行了安全扩展,以满足移动 Agent 应用对安全的需求。其总体系统结构如图 1 所示。主要包括以下几个主要部分:基于 TPM 模块的底层硬件安全平台;信任链机制控制下的可信引导至安全内核;符合 TCG 规范的可信软件服务接口;同样在信任链传递机制作用下在宿主机上为 Agent 构建的可信服务程序即移动 Agent 执行环境;移动 Agents 和通信子系统。

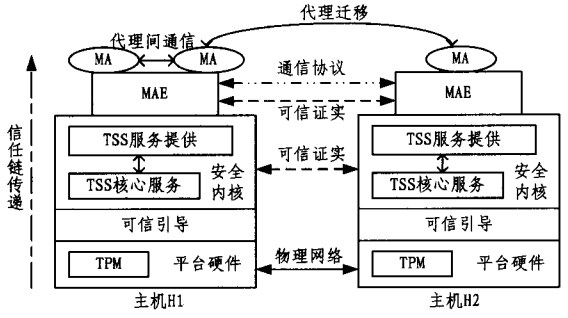

图 1 基于 TPM 的安全体系框架

3.2 模型解析

3.2.1 TPM 支持的可信终端

由可信计算平台支持的终端中,系统在计算平台上引入了"可信根",并利用它来建立信任链[6,8]。一个可信根由可信度量根 RTM(Root of Trust for Measurement)、可信存储根 RTS(Root of Trust for Storage)、可信报告根 RTR(Root of Trust for Reporting)组成。其中 RTM 以软件的形式表现,RTS 和 RTR 则由 TPM 来实现。RTS 保护了委托到 TPM 的密钥和数据。RTS 通过管理一小块非易失性存储器来存储密钥及进行生成签名和加密操作。当 TPM 属主建立时,存储根密钥 SRK(Storage Root Key)由 TPM 生成并且被用来保护形式上应该被存储在 TPM 中的其他密钥。TPM 提供了基本的硬件手段来支持信任链的建立。信任链是实现可信传递的保障。TCG 定义了从计算平台加电 BIOS 执行开始,到引导代码的执行,再到操作系统的启动和上层应用程序的执行一系列过程,信任将通过这个过程一直传递下去,直到整个计算环境的建立。作为对分布式计算终端的支持,TCG 将终端的组成作为保障分布式计算安全的一个重要部分。在通常的分布式安全中,典型的基于非对称密码的消息交换中,针对特定个体的消息将被用公钥进行加密,而且消息可以通过用私钥进行签名来进行保护。而终端上不正确的密钥管理将使整个系统失去安全性。TPM 的目的就是通过保护存储、度量和报告等机制来提供密钥管理和结构管理,而且都能够被组合来密封密钥和平台配置,从而使得终端的定义更为强壮。TCG 还定义了四个基本的类来保护分布式的消息交换:绑定(Binding)、签名(Signing)、密封的绑定(Sealed-Binding)和密封的签名(Sealed-Signing)[8]。

3.2.2 可信系统的初始化

在可信计算体系中,建立可信需要先拥有可信根,然后建立一条信任链,再将可信传递到系统的各个模块,才能建立整个系统的可信。RTM 是信任传递的原点,RTS 维护完整性摘要的值和摘要序列的引擎,一般由对存储加密的引擎和加密密钥组成。RTR 是一个计算引擎,能够可靠地报告 RTS 持有的数据,这个可靠性由签名来保证。这三个根都是可信、功能正确而且不需要外界维护的。这些可信根存在于 TPM 和 BIOS 中,当平台开始操作时,从 RTM 开始启动。RTM 开始自检并检查其他可信构建模块(RTS 和 RTR 等)。在运行系统中的任何硬件和软件模块之前,必须建立对这些模块代码的信任,这种信任是通过在执行控制转移之前对代码进行度量来确认的。在确认可信后,将建立新的一个可信边界,隔离所有可信和不可信的模块。即使确定模块不可信,也应该继续执行这个模块,但是需要保存真实的平台配置状态值。当下一层的代码准备跳转到上一层的时候,需要先对上一层代码进行度量,将度量值存入相应的平台配置寄存器 PCR。通过这种先度量再执行的传递,可信就从 BIOS 和 TPM 一步一步传递到了操作系统和应用程序,构建成了一条信任链。每一级系统运行控制组件只有在确认其下一级系统运行控制组件是可信的时候,才将系统运行的控制权转移给它。操作系统内核在载入每个系统进程之前,都必须控制 TPM 对其进行完整性度量,并将度量的值扩展到相应的 PCR 中。类似地,每次应用程序执行前,也必须由操作系统内核控制 TPM 将应用程序的完整性度量扩展到相应的 PCR 中。TPM 的平台配置寄存器保存了可信引导过程和安全内核的完整性度量值,由于它们只能接受连接操作,不能被任意修改,因此可以作为平台引导过程和安全内核是否可信的凭证。

3.2.3 软件服务接口

在 TPM 的支持下,TCG 定义了安全内核对上层软件服务的三个接口:TPM 设备驱动链接库接口(TPM Device Driver Library Interface,TDDLI)、软件服务栈核心服务接口(TSS Core Service Interface,TCSI)和 TCG 服务提供接口(TCG Service Provider Interface,TSPI)。[8]

1)TDDL 接口

从 TPM 设备和设备驱动向上就是 TDDL 接口,也是用户模式与核心模式的接口。在核心模式的设备驱动以上设置这个接口实现了几个主要功能:1)保证了 TSS 软件栈的不同执行能够各自适当地与 TPM 通信;2)为 TPM 应用提供了独立于 OS 的接口;3)能够允许 TPM 供应者作为用户模式的一个部件提供一个模拟的软 TPM。TDDLI 提供了在核心模式和用户模式之间的转换,但是它不管理 TPM 的线程交互,也不执行 TPM 的大量命令。

2)TCS 接口

TCS 提供了到平台服务的共同集合的接口。虽然在单个平台上可能会有多个 TCG 服务提供者,但 TCS 保证它们都可以提供正常的服务。TCS 主要提供以下几种核心服务:

- 上下文管理:访问 TPM 的执行线程;
- 证书和密钥管理:存储和平台相关的证书和密钥;
- 度量事件管理:联合 PCR 管理登录和访问事件日志;
- 参数块生成:连续、同步的处理 TPM 有关命令。

TCS 作为用户模式下的系统进程进行操作,被用来管理提供给 TPM 的授权信息。

3)TSP 接口

TSP 在基于面向对象的体系下为 TPM 提供了 C 接口。它与上层应用使用同样的进程地址空间。通过使用一个用户接口来对该层编码或者在远程调用时通过在 TCS 进行回调机制来进行授权操作。为了对最终用户提供一个可靠的授权接口，本地应用并不提供授权服务，而是依靠底层的可信硬件平台固有的服务来实现。

TSP 提供两种服务：上下文管理和加密。加密功能是为了充分使用 TPM 提供的保护功能，诸如消息摘要和字节流的生产等，但是大块的数据加密并不出现在接口中。上下文管理提供动态的句柄来允许有效地使用应用程序和 TSP 的资源。每个句柄对相关的 TCG 操作集合提供上下文服务。应用程序的不同线程可以共享相同的上下文或者每个线程可以获得一个单独的上下文。

3.2.4 应用的加载

作为移动 Agent 应用框架的一部分，MAE 的建立将直接影响到整个 MA 系统的安全运行。下面讨论 MAE 如何整合 TCG 的功能。分为两种情况：MAE 作为本地应用与 TPM 的直接交互；与远程系统之间通过 RPC 机制来远程访问时与 TCG 体系的交互。两种体系描述如图 2 所示。

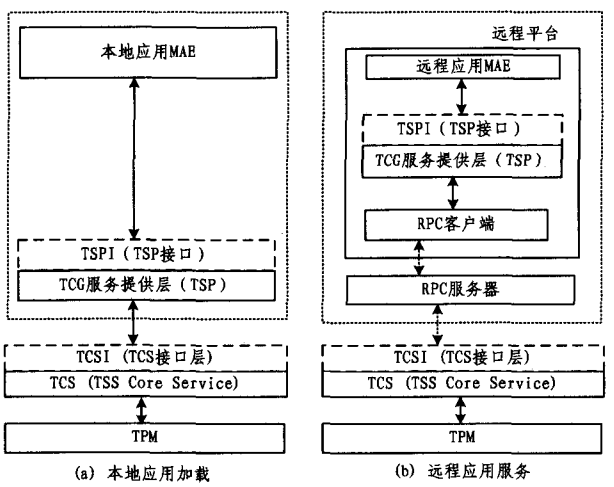

图 2 基于 TPM 的分布式应用交互体系

1)本地应用服务

作为本地应用程序，在用户模式下被加载时，会通过 TSP 接口提供的基本函数(相关函数可参考文献[8])读取包含在 TPM 管理的 PCR 寄存器中的预期的有效证书来验证当前的平台配置情况。须经历以下几个步骤：

- 初始化应用程序对象，准备读取 PCR 的值；
- 读 TPM 中 PCR5 的值；
- 比较 PCR 的值与预期的有效证书值。

对于 TSP，当 TPM 被函数引用时，TCS 要求用来签名 PCR 值的密钥会加载到 TPM，同时对已经生成用来识别 PCR 值进行引用，会要求生成一个索引。当命令执行后，TSP 再调用相关函数进行签名并取回 PCR 的值。而对于 TPM，通过收到加载密钥的消息和恢复 PCR 值的命令，进行解析后执行相应操作。

2)远程交互时读取 PCR 值

当 MA 迁移发生时会与远程主机进行交互。从安全的角度考虑，基于 TPM 的远程 RPC 或其他消息交互将通过 TCS 接口执行。现有的分布式规范的安全策略描述了基于 COM 接口的远程系统通信。在本模型中，远程应用将直接与 TCS 进行交互。当 TCS 服务模块整理了 TPM 消息之后，即可以进行 RPC 调用。对于某一远程 TCS，在收到并整理了 TPM 加载密钥和引用 TPM 消息之后，即可向本地 TCS 发送 TPM 消息，进行 RPC 调用。而对于本地 TCS，在收到远程 RPC 的 TPM 消息后，也会打开 TPM 信道，进行安全传输与应答。

上述两种情况表明，基于 TPM 的平台能够实现从本地应用到远程应用的功能。TCG 提供的软件层也为 TPM 在各种不同应用环境下实现可靠的服务集合提供了保障。

3.2.5 实验分析

本文选用 IBM 的 Aglet[13] 作为实验平台。Aglet 是目前较为成功和完善的一个面向对象的移动代理系统，它拥有一个比较明晰的类体系结构和一套完整的对象应用解决方案，更主要的是 IBM 现已将它作为一个开源项目，因此我们可以更深层次地对它进行分析，并在此基础上进行实验和改进。Aglet 原有的安全模型支持各种安全策略的灵活定义。安全策略是由管理者定义的一组规则集，策略说明了 Aglet 访问对象的条件、用户请求的认证、认证实体所允许执行的操作及实体能否委派它们的权利、Aglet 之间和上下文之间通信的安全要求等等。但是 Aglet 本身的体系结构中并没有提供加密服务。因此，根据前面论述的基于 TPM 硬件的安全模型，我们来分析引入可信平台后的 Aglet 安全体系的改进与实现。

(1)可信平台上 Aglet 服务程序的加载

根据上一节的描述，Aglet 服务程序作为本地应用在可信平台加载时，需要和底层的 TPM 进行交互。因此，我们对 Aglet 服务程序增加了与 TSPI 的交互，通过 TCG 定义的上下文相关类的调用，实现如图 2(a)所描述的加载交互过程。

(2)Aglet 迁移后与远程主机的交互

类似地，当一个 Aglet 远程迁移后，为确保不受恶意主机的威胁，Aglet 也需要对将要运行的 MAE 进行可信的评估与认证。根据 Aglet 的编程机制和 Aglet 的回调模型以及 TCG 定义的相关接口类，我们可以重写 Aglet 类的回调方法、Aglet 基类的初始化方法和获取上下文句柄等方法，从而实现如图 2(b)所描述的基于 TPM 的远程交互。以认证过程为例，在信任链的建立过程中，主机的 MAE 拥有了 TPM 颁发的 ID 和密码，并拥有唯一的密钥/公钥对。Aglet 在移动到远程 MAE 上时，先向 TPM 获取 MAE 的公钥，同时把自己的公钥告诉 MAE，双方用彼此的公钥加密，对方用自己的私钥进行验证，经过两次握手，进行信任的确定。同时 TPM 派发给双方一个会话密钥，Aglet 和 MAE 之间的通信即可通过密钥加密进行，提高了安全强度。

(3)Aglet 间通信安全

Aglet 间通讯所涉及的安全性问题也是另外一个重点需要解决的问题。Aglets 间是通过消息的方式来通信的，每一个 Aglet 都可以有一个消息处理方法来处理由另外一个 Aglet 发来的消息对象。这些消息一般都是做过个性化处理后的重要信息，如直接以明文的方式传输，则很容易被第三方监、盗用和伪造，使得接受主机无法得到正确的信息。而在我们的模型中，经过改进的 Aglet 通过在发送前调用 TPM 的加密功能使得消息能得到保护，类似的通信加密和签名认证等也都可以采用此种策略，安全性能得到大幅提高。

结束语 本文对现有的移动 Agent 安全方案进行了研究，对安全强度较高的基于硬件的保护引入了可信计算平台，

设计了基于 TPM 的安全模型。通过对模型各个组成部分的分析，并结合 Aglet 平台上的安全实验，我们认为本模型可以从硬件体系结构层次上满足移动 Agent 系统的安全需求，并有望从根本上解决恶意主机所带来的安全问题。下一步的工作重点将是进一步完善该模型的原型系统，扩大网络应用环境，在更复杂的网络环境下测试其安全性能。

参 考 文 献

[1] 王红. 移动 Agent 关键技术研究. 学位论文. 中国科学院计算技术研究所，2002

[2] 柳毅. 移动代理技术中若干安全问题的研究. 学位论文. 西安电子科技大学，2005

[3] 王汝传，孙开翠，张登银，等. 基于 JavaCard 的移动代理保护的研究，计算机学报，2004，27(4)：492-499

[4] Varadharajan V. Security enhanced mobile agents// Proc. of 7th ACM Conference on Computer and Communication Security. 2000

[5] Borselius N. Mobile agent security. Electronics & Communication Engineering Journal，October 2002

[6] 沈志东. 可信计算的关键技术与应用研究. 学位论文. 武汉大学，2006

[7] 方艳湘，沈昌祥，黄涛. 分布式系统中计算安全问题的一种解决方案. 计算机工程，2006(9)

[8] Trusted Computing Group. TCG Specification Architecture Overview. Specification Revision 1. 4. http://www. trustedcomputinggroup. org. 2007. 8

[9] Trusted Computing Group. TPM Main Part 2 TPM Structures. specification version 1. 2. http://www. trustedcomputinggroup. org，2007，7

[10] Wu Xiaoping，Shen Zhidong，Zhang Huanguo. The Mobile Agent Security Enhanced by Trusted Computing Technology// The 2nd International Conference on Wireless Communications，Networking and Mobile Computing (WiCOM 2006). Wuhan：IEEE Press，2006

[11] 王新成，袁子建. 可信计算与系统安全芯片设计研究. 国家信息安全测评认证，2005. 5

[12] Lin Ching，Varadharajan V，Wang Yan，et al. Trust Enhanced Security for Mobile Agents// Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC'05). IEEE，2005

[13] The Aglets 2. 0. 2 User's Manual. http://www. trl. ibm. com/aglets/，2004，10

(上接第 82 页)

```
  p 为 T 的第一个元素；
  insert _tree([p|P],M)；}
insert_tree([p|P],M)
{ 设 N 为 T 的子女；
  If N. item_name=p. item_name then
       N. count++；
              else
       { new(N)；N. count=1；
         N. pre_link=T；
         if HTable. tail_link! =NULL then N. node_link=HTable.
         tail_link；
         Htable. tail_link=N；}
  If P 非空 then insert_tree(P,N)；}
```

Step2 挖掘 FP_树

```
按逆序扫描频繁项头表；
t=HTable. tail_link；SF=NULL；
Procedue FP_growth(t,SF)
{repeat
    {得到从 t 到根的节点形成组合 S1，S2，…Sm；
    for (i=1，i<=m；i++)
      {Si. count=t. count；
      If (Si∈SF)then
    SF. Si. count=SF. Si. count+Si. count；
            else Si 加入到 SF 中；
      该路径上其它节点的 count 值减去叶节点的 count 值；}
      t=t. node_link；}
    until t. node_link=NULL；
  取头表中的下一项；
t=HTable. tail_link；}
```

4 实验分析

我们采用美国国防部高级计划研究署 1999 年提供的评估入侵检测系统的测试数据集[4]来测试系统的性能，主要利用 IDS 系统进行异常检测以发现未知的攻击。实验在设定支持度为 50%、置信度为 80%的情况下进行，在 180 个攻击中能检测到 151 个，检测率达到 83. 8%。实验还分别利用 Apriori 算法和 NFP_树算法进行了测试，其结果见图 2 所示。

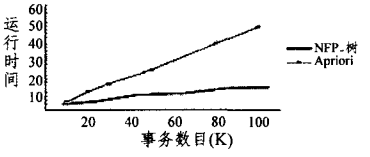

图 2 两种算法运行时间随事务数变化情况

由图 2 可知，当事务数在 20k 以内时，两种算法性能相当，但随着数据的增加，NFP_数算法所用的时间明显比 Apriori 算法的时间少很多，其性能优势有了明显的体现。

结束语 本文描述了一种改进的 FP_树算法-NFP_树算法，并使用它进行入侵检测关联规则的挖掘。实验证明 NFP_树算法比传统关联规则挖掘算法效果更好，但是 NFP_树算法也不能检测出所有的入侵行为，因此如何进一步提高检测的精确度将是我们下一步工作的目标。

参 考 文 献

[1] 胡昌振. 网络入侵检测原理与技术[M]. 北京理工大学出版社，1996

[2] Han Jiawei，Kamber M. Data Mining Concepts and Techniques [M]. 范明，孟小锋，等译. 机械工业出版社，2000

[3] 高俊，施伯乐. 快速关联规则挖掘算法研究[J]. 计算机科学，2005(3)：200-202

[4] Lippmann R，et al. The 1999 DARPA Off-Line Intrusion Detection Evaluation. Computer Networks，2000，34(4)：579-595

[5] Xia Hongxia，Shen Qi，et al. Application of Data Mining Technology to Intrusion Detection System// Proceedings of the 2004 International Symposium on Distruibured Computing and Applications to Business Engineering and Science[R]. Wuhan，china，2004