一种面向网络信息系统的TCP应用架构设计

金 雷 徐开勇 李剑飞 成茂才
(信息工程大学密码工程学院 郑州 450004)

摘 要 针对可信计算平台在网络信息系统中的应用需求,提出了一种面向网络信息系统的TCP应用架构TCPAA。将该架构主要分为访问认证子系统和信息交互子系统两部分来进行设计。在访问认证子系统中,为了增强可信计算应用的灵活性,提出一种基于证明代理的可信验证机制PATAM,并对改进的访问认证模式进行了协议设计和流程说明。在信息交互子系统中,设计了内外网之间数据的可信传输流程,并提出了一种改进的金字塔可信评估模型PTAM。最后通过测试实验验证了该架构的良好性能。研究结果表明,该方案对于网络信息系统环境内可信计算平台的应用开发具有良好的通用性。

关键词 网络信息系统,可信计算平台,应用架构,可信验证机制,访问认证模式,金字塔可信评估模型
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.10.031

Design of TCP Application Architecture for Network-oriented Information System

JIN Lei XU Kai-yong LI Jian-fei CHENG Mao-cai
(Cryptography Engineering College, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract According to the application requirements of trusted computing platform in the network-oriented information system, a TCP application architecture TCPAA was proposed for the network-oriented information system. The architecture was designed by dividing it into the access authentication subsystem and the information exchange subsystem two parts. In order to enhance the flexibility of trusted computing applications in the access authentication subsystem, a trust authentication mechanism PATAM based on proof agent was proposed in this paper, and an improved access authentication mode was proposed with a detailed description of its authentication protocol and application process. Beyond that, the trusted information transmission processes inside and outside were designed in the information exchange subsystem, and an improved pyramid trusted assessment model PTAM was proposed. Finally, the test experiments verify the good performance of the architecture. The results show that the application architecture has better support ability for the application development of trusted computing platform in the network-oriented information system environment.

Keywords Network-oriented information system, Trusted computing platform, Application architecture, Trust authentication mechanism, Access authentication mode, Pyramid trusted assessment model

随着信息化技术的发展和网络普及程度的加深,党政等重要部门因其网络信息系统的特殊性和重要性对网络可信安全提出了更高的要求。可信计算平台(Trusted Computing Platform,TCP)的出现和应用,为增强信息系统的安全性提供了一种从根源上解决计算机系统平台完整性和安全性的思路,旨在为建设安全体系提供更加完善的底层基础设施。而如何最优地利用可信计算平台来提高信息系统的安全性成为实现整个系统信息安全共享的关键[1]。

针对网络信息系统环境,合理利用可信计算平台能够对其数据安全性、网络可信性等安全需求提供更加有效和灵活的安全防护。目前国内外学者就可信计算平台如何合理地应用在安全性要求较高的网络信息系统中相继开展了一些研究。2009年,Dave研究设计了一个实现网络接入控制的可信接入系统[2],但未考虑数据流和终端接入平台的可信认证和度量。Vanessa等人通过引入学习算法自动更新接入控制策略,提出了一种基于行为轮廓的可信信息系统接入模型[3],但同样未提及可信计算平台在网络系统中的典型应用架构。国内的学者对可信计算平台在涉密网络系统中应用方案的探索也从未停止,如2009年,梅芳等人基于可信网络连接框架提出一种实用性较强的可信修复网络模型[4]来为不满足安全策略的终端提供修复服务,但未对模型的应用模式进行分析和测试;2010年,张焕国等人分析总结了可信网络连接的体系结构、消息流程以及相关规范,并对可信网络连接技术日后的发展方向进行了深入的探讨[5,6];2011年,孙守胜提出一种基于国产可信计算平台的涉密终端应用体系[7],对提出的应用体系架构以及功能模块进行了分析,但对改进后的可信终端如何应用于网络系统未给出典型应用架构;2012年,王浩等人分析了多级涉密网安全接入的需求,提出了一个基于可信

到稿日期:2014-10-20 返修日期:2015-01-24

金 雷(1989-),男,硕士生,主要研究方向为可信计算,E-mail:984522340@qq.com;徐开勇(1963-),男,研究员,主要研究方向为信息安全、可信计算;李剑飞(1991-),男,硕士生,主要研究方向为可信计算;成茂才(1991-),男,硕士生,主要研究方向为信息安全。

网络连接的多级涉密网安全接入模型[8]，该模型通过引入安全属性检查规则和完整性度量规则使得多级涉密网的效率有所提升，但不具有普遍适用性；2013 年，王宇等人针对涉密信息系统的网络可信安全需求构建了一个涉密信息系统网络的可信安全防护体系[9]，防护体系着重于终端的防护，但未对其远程访问和数据传输典型架构给予说明。综合来看，以上研究都针对网络信息系统中的网络连接、终端防护等需求利用可信计算技术提出了相应的改进方案，但都未就可信计算平台如何综合部署于信息系统提出典型的安全体系架构从而实现整个体系真正的信息安全共享。

本文第 1 节对提出的 TCP 典型应用架构进行描述；第 2 节对访问认证子系统中改进的可信验证机制进行设计和算法说明；第 3 节对访问认证子系统中访问认证模式的访问协议和应用流程进行了说明；第 4 节设计了应用架构中与外网相连的信息交互子系统，并在其中提出了一种金字塔信任度量算法；第 5 节对架构整体进行安全性分析；第 6 节通过验证实验对应用架构的子系统功能进行性能分析；最后总结全文。

1 TCPAA 架构设计

一个面向网络信息系统的可信计算平台典型应用架构必须具有典型性和普适性。根据可信网络的结构特点，提出一种典型的可信应用架构（Trusted Computing Platform Application Architecture，TCPAA），如图 1 所示。TCPAA 架构内的终端和服务器设备都是由可信密码模块引导启动的可信计算平台，可信终端装有具有可信收集和度量计算功能的证明代理。可信服务器端包含认证、应用等功能服务器，并配有综合管理系统。管理员控制单元主要负责对外网流入的数据进行审计及可信评估。本文把架构划分为两个核心子系统：访问认证子系统和信息交互子系统（Information Interaction Subsystem，IIS）。

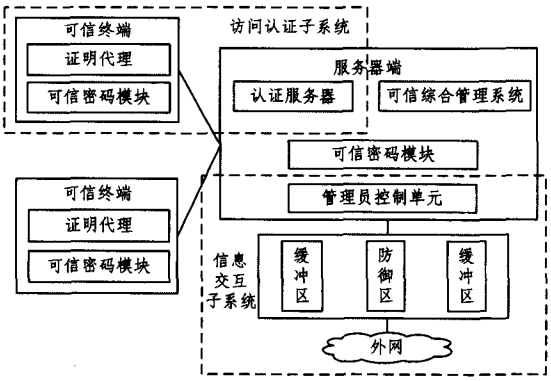

图 1　可信计算平台应用架构

1.1 访问认证子系统

根据高安全性网络信息系统灵活且安全的应用需求，通过在终端加入证明代理来对不具备可信来源却有实用性的应用程序进行可信验证，优化了信任链传递路径，使整个终端的应用层可信授权更加便利灵活。在访问认证子系统内提出一种基于证明代理的可信验证机制（Trust Authentication Mechanism Based on Proof Agent，PATAM），并在认证部分提出一种基于二进制代码度量的直接信息交互模式（Binary Direct Interaction Mode，BDIM）来减小信息的瓶颈泄漏隐患，其在安全性要求较高的该体系架构中将具有典型性和实用性。

1.2 信息交互子系统

信息交互子系统设计的目的是针对网络信息系统与外网之间的数据传输安全，内部架构在面对外网的数据交互时，设有数据缓冲区以及对接入方进行可信认证与评估的深层防御区，并由管理员控制单元进行安全审计和监督。在子系统评估过程中结合信任评估理论[11]，提出一种金字塔信任评估模型（Pyramid Trust Assessment Model，PTAM），其合理性和实用性为整个子系统的外网数据安全接入起到了关键作用。

2 PATAM 可信验证机制

在目前可信终端的信任链传递中，应用层的度量依靠相对固定的程序列表验证机制，使得只有列表中的可信软件才能启动，极大地限制了一些具有实用可信性的自由软件的应用，很不灵活。本文通过在终端加入证明代理模块为可信软件的灵活授权提供了一种思路。

定义 1（应用程序证明代理 P_{Agent}）　P_{Agent} 是安装在可信终端的具有收集平台信息、存储和计算可信度量值等功能的代理应用模块，由各个终端进行单独维护和管理。对于终端上的非可信应用程序，只要通过 P_{Agent} 主导的验证机制便可正常运行，同时保证了可信链在应用层的正常传递。

在 PATAM 机制中，应用程序证明代理 P_{Agent} 起着非常重要的作用。为了保证 P_{Agent} 可信，扩展终端的信任传递过程如下：

$$CRTM \rightarrow BIOS \rightarrow OSLoader \rightarrow OS \rightarrow P_{Agent} \rightarrow Application$$

其中，将 P_{Agent} 作为可信平台链式度量的重要一环，P_{Agent} 的度量由 OS 主导完成，并且 OS 将 P_{Agent} 程序作为第一个应用程序首先启动。PATAM 验证机制的应用流程如图 2 所示。

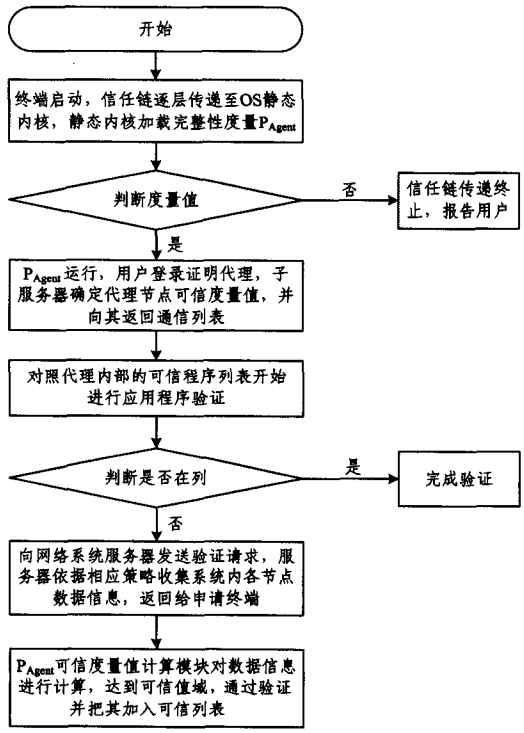

图 2　PATAM 应用流程

当内网架构各终端节点针对某个应用程序的数据信息判定不够准确时，用户可向服务器发出申请消息，通过信息交互子系统从符合一定标准的外部网络系统收集评估资源，并结

合管理服务器做出判定。

PATAM结合数据统计理论，策略要求服务器收集上来的数据信息含有终端可信度量值、相同程序终端数、系统内终端总数和用户评价值等数据信息。本文的应用程序可信值验证算法是建立在系统内的各个终端含有同一验证程序总数达到一定比例、用户评价值为可信且符合客观事实的假设条件下，下面对算法中各部分进行定义和说明。

定义 2(应用程序最终度量值 T_T) T_T 表示应用程序最终计算出的可信度量值，是证明代理做出判定的依据。

定义 3(全部系统终端可信度量值 A_T) A_T 表示整个内部网络系统内所有终端可信度的统计值。由此可得可信度集合 A，B_A 为所有收集终端的集合。

$$A=\{A_{b1},A_{b2},\cdots,A_{bi},\cdots,A_{bn},b_i\in B_A\}$$

定义 4(相同程序终端统计值 S_T) S_T 表示所有含有相同验证应用程序终端的统计值，X 表示其总数目。由此可得各终端对应用程序评价值集合 C，D_C 为各个类似终端集合。

$$C=\{C_{d1},C_{d2},\cdots,C_{di},\cdots,C_{dm},d_i\in D_C\}$$

定义 5(所有终端可信评价 E_T) E_T 表示所有系统内统计终端对该应用程序的可信评价。可信评价和不可信评价集合分别为 E 和 F。

$$E=\{e_1,e_2,\cdots,e_i,\cdots,e_r,e_i\in[0,1]\}$$

$$F=\{f_1,f_2,\cdots,f_i,\cdots,f_t,f_i\in[-1,0]\}$$

由以上定义可得应用程序最终度量值：

$$A_T=\sum_{i=1}^{n}A_{bi}/n \tag{1}$$

其中，$i=1,2,\cdots,n$；$0\leqslant A_{bi}\leqslant 1$。

$$S_T=m/X \tag{2}$$

$$E_T=(\sum_{i=1}^{r}e_i+\sum_{i=1}^{t}f_i)/(r+t) \tag{3}$$

$$T_T=\alpha_1\times A_T+\alpha_2\times S_T+\alpha_3\times E_T \tag{4}$$

其中，$0\leqslant\alpha_1,\alpha_2,\alpha_3\leqslant 1$ 且 $\alpha_1+\alpha_2+\alpha_3=1$。$\alpha_1$、$\alpha_2$ 和 α_3 分别为 A_T、S_T 和 E_T 三者在应用程序最终度量值计算中的权重，具体设定依据应用场景需求而定。

本文针对安全需求较高的网络信息系统应用环境，作如下设定。当 $A_{bi}\geqslant 0.75$ 时，认为节点可信，将其数据加入计算，否则放弃该节点数据；当 $A_T\geqslant 0.8$ 时，表明总体节点可信度达到要求，进行可信值计算，否则终止计算；当 $S_T\geqslant 0.3$ 时，表明拥有相同文件的节点数达到统计比例，进行可信值计算，否则终止计算。

3 BDIM 模式

从 TCPAA 内网架构来看，终端的访问接入是内网系统信息安全共享的基础。典型的远程证明方案有两种，对于高安全性信息系统应用场景，其要求访问请求终端都应该向服务器提供自己完整的平台配置信息来进行认证，根据掌握的所有平台配置信息来更准确地做出访问决策，因此适合以二进制代码度量方案为基础进行改进。为避免可信第三方成为安全瓶颈，针对高安全级别的信息系统应用需求且为减少信息泄露隐患，在子系统中提出一种改进的基于二进制度量的直接信息交互模式 BDIM，设计的服务访问协议如图 3 所示。

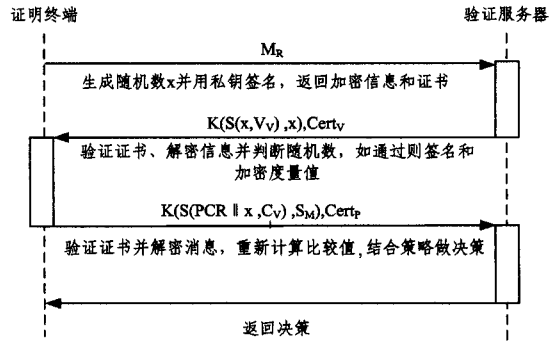

图 3 BDIM 访问协议

定义 6(证明终端 P_T) 证明终端为架构的访问认证子系统内一个发起访问服务请求的实体平台，内部含有可信密码模块，其 AIK 公私钥分别是 C_P 和 C_V，AIK 证书为 $Cert_p$。

定义 7(验证服务器 V_T) 验证服务器为一个含有可信密码模块的客体验证平台，其 AIK 公私钥分别是 V_P 和 V_V，AIK 证书为 $Cert_V$。

请求终端访问认证协议流程如下：

Step 1 $P_T\rightarrow V_T:M_R$。M_R 为证明终端向验证服务器发送的访问请求。

Step 2 验证服务器收到来自证明终端的访问请求，随机生成随机数 x，并用自身的 AIK 私钥对其进行签名，最后使用会话密钥对随机数和签名值进行加密。

Step 3 $V_T\rightarrow P_T:K(S(x,V_V),x),Cert_V$。如式中所示，服务器把会话共享密钥加密后的随机数、签名值以及自身 AIK 证书发送给证明终端。

定义 8(签名函数 $S(a,b)$) $S(a,b)$表示用密钥 b 对 a 进行签名。

定义 9(加密函数 $K(x)$) $K(x)$表示使用会话共享密钥对随机数 x 进行加密。

Step 4 终端对验证服务器发来的 AIK 证书进行有效性验证。证明终端使用双方会话共享密钥解密被加密的信息，然后用验证服务器 AIK 公钥 V_P 对签名进行身份来源判断，如果成功，再对随机数进行验证比较来判断其在传输过程中是否被篡改，如果身份和随机数均一致，则认证继续。

Step 5 证明终端将自身的平台配置信息进行可信度量后扩展存储在 PCR 中，并把度量值和组建度量序列等存储于 SML 中，用私钥 C_V 签名 PCR 和随机数，最终将签名值和日志用会话共享密钥加密。

Step 6 $P_T\longrightarrow V_T:K(S(PCR\|x,C_V),S_M),Cert_P$。$S_M$ 为终端度量存储日志，证明终端将加密后的签名值、度量存储日志以及自身 AIK 证书发送给验证服务器。

Step 7 验证服务器对证书有效性进行验证，利用会话共享密钥解密被加密的信息，得到签名和度量存储日志；利用证明终端的公钥 C_P 验证签名，如果身份和消息来源通过验证，重新扩展计算 SML 中的度量值得到 PCR 值并作比较来验证信息的完整性；对签名中的随机数与验证终端产生的随机数进行对比以验证消息新鲜性。

Step 8 结合完整性报告对证明终端做出访问决策，将访问决策返回证明终端。

4 IIS 系统设计

基于可信计算平台的信息系统架构在保证内部终端安全及访问认证可信的同时，还要考虑与外部信息的交互，达到可信交互的关键是要确保数据交换的可信性和传输的高效性。针对此应用需求，本文对网络互联体系进行改进，设计了信息交互子系统 IIS，并在其核心功能可信认证部分提出一种改进的金字塔可信评估模型 PTAM。系统应用流程如图 4 所示。

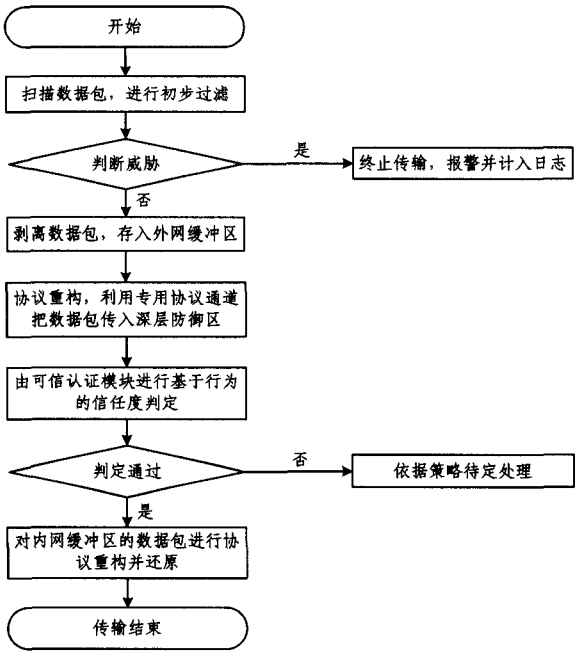

图 4 IIS 应用流程

内外网缓冲区由独立的操作系统和存储设备等组成，其协议转换单元剥离传入数据包的数据头并加上通道协议的包头进行传输。深层防御区通过内部的可信认证模块对接入者的身份进行认证，对其可信度基于 PTAM 模型进行计算。

管理员控制单元的主要功能是审计和分析各个数据包的头文件中的信息，并时刻监视日志信息，一旦发现危险立即采取相应措施。

各安全处理单元既相互独立，有效实现内外网的相互隔离；又协同工作，完成内外网之间授权数据的高效可信传输。下一小节对系统详细应用流程进行描述。

4.1 IIS 应用流程

当一个外部数据包准备接入内部系统时，其认证与判定过程如下。

Step 1 一个数据包从外网通过专用的通信通道准备传入内部信息系统时，首先在外部接口处进行内容的扫描和初步过滤。根据协议信息对数据包进行威胁的判断，如果没有威胁，则进入下一个区域；如果存在威胁，则传输停止并记入日志，同时由设置好的报警功能进行提示，此过程中管理员控制单元始终进行监视。

Step 2 数据包的外部协议标识被协议转换单元剥离，同时进入外网缓冲区。对数据进行协议重构，并转入深层防御区域。

Step 3 对进入到深层防御区的数据包进行可信认证，通过身份认证和可信度估算，并利用改进的金字塔可信评估模型 PTAM 进行评估，得出结论。

Step 4 根据评估结果进行决策，如果通过，则识别服务类别，分配合理的资源；如果评估无效，则依据相应策略进行处理。

Step 5 协议重构到达内网缓冲区的数据包，还原数据包。

4.2 PTAM 模型设计

在整个信息交互子系统中，对接入者的可信度判定是该体系的核心功能，来自外部的接入者的状态极可能为非可信计算平台。所以综合考虑，只能从其历史度量记录和持续行为着手[12]，结合信任评估理论，提出一种改进的金字塔可信评估模型 PTAM，如图 5 所示。

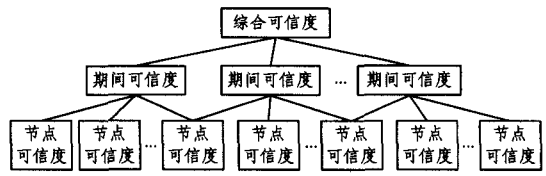

图 5 金字塔可信评估模型

PTAM 模型分为 3 个可信度量收集层，最下层的节点可信度表示每次交互所计算出的时间点可信度量值；中间层的期间可信度表示在一段时间内的综合可信度量值，其结果取决于下面对应的各个节点可信度；处于模型塔尖的综合可信度是综合所有历史行为记录而评估出的最终结果，是判断接入者可信与否的依据。下面对 PTAM 模型具体属性定义和评估算法进行说明。

定义 10（节点可信度量值 $T(x)$） $T(x)$表示节点在第 x 次交互时所产生的度量值，且 $0\leqslant T(x)\leqslant 1$，其计算公式如下：

$$T(x)=(\alpha\cdot T_{Direct}(x)+\beta\cdot T_{Indirect}(x)+\chi\cdot T_{Reputation}(x)\cdot S(x)) \tag{5}$$

其中，$\alpha+\beta+\chi=1$，$T_{Direct}(x)$表示节点 x 的交互直接度量值，$T_{Indirect}(x)$表示节点 x 的交互间接度量值，$T_{Reputation}(x)$表示节点 x 的交互信誉度量值；α 表示直接度量状态的权重，β 表示间接度量状态的权重，χ 表示信誉度量状态下的权重，三者总和为 1。

定义 11（网络安全度 $S(x)$） $S(x)$表示在一次交互过程中网络的整体安全状态，计算公式如下：

$$S(x)=1-b\cdot D_{\max}(x) \tag{6}$$

公式借鉴模糊数学中的“贴近度理论”，其中 b 为数据来源外网的网络复杂程度，$D_{\max}(x)$表示网络的最大风险度，并且 $0\leqslant D_{\max}\leqslant 1$。

定义 12（期间度量节点度量值 $O(t)$） $O(t)$位于金字塔可信度量模型的第二层，表示在第 t 个时间段内节点的期间度量值。其中 t 表示时间段的序数，$t=1,2,3,\cdots,m$，序号越大表示越接近现在的状态。n 表示时间段内子节点的个数。其算法为：

$$O(t)=(\sum_{x=1}^{n}T(x))/n \tag{7}$$

定义 13（时间衰减函数为 $P(t)$） 依据文献[13]，将其表示为：$P(t)=0.38e^{-\sqrt{m-t}}$，其中 m 和 t 分别表示最近的时间段和现在正在计算的时间段。

$trusted(V)$为模型最顶层的综合可信度量值，即接入用

户 V 最终的评估结果。综上所得，接入内网的用户 V 综合可信度计算公式为：

$$trusted(V)=\sum_{t=1}^{m}P(t)\cdot O(t)=\sum_{t=1}^{m}[0.38e^{-\sqrt{m-t}}\cdot(\sum_{x=1}^{n}T(x))/n] \quad (8)$$

5 安全性分析

与传统的信息系统安全防护架构相比，本架构具有以下优点。

(1)认证安全性。通过子系统中的 BDIM 认证模式，在保证请求者身份可信的同时，达到了终端和服务器之间的双向认证。改进的远程访问机制根据该场景的应用需求，保证了平台配置状态的完整性和不可篡改性，也能够抵御重放攻击和平行对话攻击。

(2)信道安全性。在访问认证子系统中，数据都以非明文的方式在信道上传输，BDIM 模式中的随机数认证机制使得传输的信息具有不规则性和不可预计性。在 IIS 系统中，数据通过专用传输通道协议进入缓冲区和防御区，减少了其他传输威胁。

(3)传输安全性。在 IIS 系统中确保了每次数据交换的可信性和高效性，通过专用传输协议的功能严格防范非法通道，提出的 PTAM 模型及其应用流程满足了系统数据传输可监督性和可信性的应用需求。

6 性能分析

(1)访问认证子系统。网络信息系统在加入 TCPAA 应用架构后的认证机制有所变化，所以需要对其所带来的时间代价进行考虑分析。子系统中的认证时间代价分为运算时间和通信时间两大部分，运算时间又分为终端可信模块运算时间和验证服务器运算时间，由于在交互时数据传输量较小，因此通信时间可以忽略不计。总时间用 t 表示，运算时间为 t_O，通信时间为 t_T，终端运算时间为 t_{te}，验证服务器运算时间为 t_{ca}。由此可得：$t_O=t_{te}+t_{ca}$；$t=t_O+t_T=t_{te}+t_{ca}+t_T\approx t_{te}+t_{ca}$。

从整个认证流程可以看出系统中哈希运算共需进行 4 次：在证明终端中进行了 2 次，验证服务器进行了 2 次。加密运算一共需要进行 2 次：证明终端和验证服务器中各进行了 1 次。解密运算一共需要进行 2 次：证明终端和验证服务器中各进行了 1 次。验证终端中一次哈希运算时间用 t_{hc} 表示，一次加密时间为 t_{ec}，一次解密时间为 t_{dc}；验证服务器中一次哈希运算时间用 t_{ht} 表示，一次加密时间为 t_{et}，一次解密时间为 t_{dt}。可得 $t\approx t_{te}+t_{ca}\approx t_{ec}+t_{et}+t_{dc}+t_{dt}+2t_{hc}+2t_{ht}$。

假设在终端和服务器的加解密 DES 运算、哈希 SHA-1 运算时间均将近 0.2s，则总时间代价 $t\approx 1.6$s。该子系统虽然增加了时间复杂度，但达到了用户和平台的可信认证和提高安全性的目的，因此这样的计算代价可以接受。

通过建立实验仿真环境，对提出的 PATAM 可信验证机制的 CPU 消耗情况和可信程序列表内存占用情况进行了测试。本文实验的可信计算平台配置信息如下：内存为 2GB，CPU 为 P4 3.06GHz，硬盘为 320GB，Linux 内核版本为 2.4.20。当可信程序列表项数分别为 500、1000、2000，列表占用的磁盘空间大小及内存情况如表 1 所列。

表 1 可信程序列表大小及内存占用

可信列表项数	大小/MB	内存占用/kB
500	0.23	14
1000	0.31	29
2000	0.60	53

相同实验环境下，PATAM 在验证应用程序过程中的 CPU 占用率的变化情况如图 6 所示。

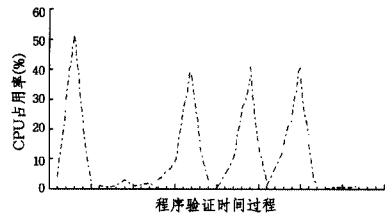

图 6 PATAM 测试实验曲线

由图 6 可知，PATAM 的 CPU 占用率曲线在验证过程中会产生波峰，其原因是 PATAM 在对可信应用进行验证时，通过终端证明代理 P_{Agent} 统计架构内的数据并计算最终度量值，所以 CPU 占用率会提高；而在不验证应用程序时，PATAM 比较稳定，CPU 占用率低。

(2)信息交互子系统。本文使用软件 MATLAB 来对 PTAM 模型的评估准确性进行实验和仿真。实验设有两个接入用户 V 和 T，对两者进行 200 次交互度量实验，平均分成 10 个时间段，每个时间段内发生 n 次交互，观察变量 n 逐渐增大的过程中综合度量值 $trusted(V)$ 和 $trusted(T)$ 的变化趋势。为了更好地分析实验结果，设置如表 2 所列的实验参数。

表 2 实验参数设置

实验参数	参数值
α	0.5
β	0.3
χ	0.2
D_{max}	5%
m	10

利用专家系统得到接入者 V 和 T 在信息交互的过程中成功的概率分别为 75%和 55%，测试实验结果评估曲线如图 7 所示。

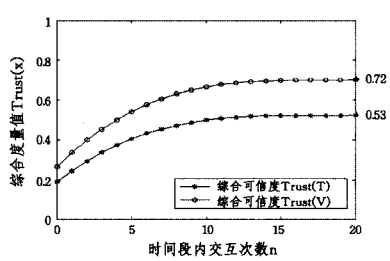

图 7 实验结果曲线

通过实验结果可知，在变量 n 从 1 增加到 20 的过程中，开始的时候可信度综合值的变化幅度较大，随着 n 的变大曲线趋于平缓，即 $trusted$ 值增幅逐渐微小，趋于稳定，与模型算法的“时间越接近现在综合度量值越稳定”的目标一致。由图可知，$trusted(V)$ 和 $trusted(T)$ 在 $n=20$ 时分别为 0.72 和 0.53，接近理论预置值。在排除偏差影响的前提下，验证了 PTAM 模型算法的合理性和实用性。

结束语 本文分析了网络信息系统环境中信息传输的安

(下转第 163 页)

科学出版社，2009
Li Shun-dong, Wang Dao-shun. Modern Cryptography: Theory, Method, Research Fronts[M]. Beijing: Science Press, 2009
[18] Rabaey J, Ammer J, Da Silva Jr J L. Pieo Radio: Ad-hoc wireless networking of ubiquitous low-energy sensor and monitor nodes [C]// Proceedings of IEEE Computer Society Workshop on VLSI. April 2000: 9-12
[19] William P, Brian F, Saul T, et al. LU Decomposition and its applications[M]// 2nd Numerical Recipes in Fortran: The Art of Scientific Computing. Cambridge: University Press, 1992
[20] Lin H Y, Tzeng W G. An efficient solution to the millionaires problem based on homomorphic encryption [C]// Proceedings of Applied Cryptography and Network Security 2005 (LNCS3531). NY: Springer, 2005: 456-466
[21] 李顺东，戴一奇，尤启友. 姚氏百万富翁问题的高效解决方案[J]. 电子学报，2005，33(5)：770-773
Li Shun-dong, Dai Yi-qi, You Qi-you. An Efficient Solution to Yao's Millionaires Problem[J]. Acta Electronica Sinica, 2005, 33(5): 770-773
[22] Li S D, Wang D S, Dai Y Q, et al. Symmetric cryptographic solution to yao's millionaires problem and an evaluation of secure multiparty computations [J]. Information Sciences, 2008, 178 (2): 244-255
[23] 李顺东，王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报，2013，41(4)：798-803
Li Shun-dong, Wang Dao-shun. Efficient Secure Multiparty Computation Based on Homomorphic Encryption[J]. Acta Electronica Sinica, 2013, 41(4): 798-803
[24] Malek B, Miri A. Combining attribute-based and access systems [C]// Proc. of 12th IEEE International Conference on Computational Science and Engineering (CSE 2009). IEEE Computer Society, 2009: 305-312

（上接第 158 页）

全需求，设计了 TCPAA 可信应用架构。架构通过把可信计算技术应用到网络信息系统中，分别在访问认证子系统和信息交互子系统中构建了面向场景需求的应用模式和相应的应用流程，并经过实验进行分析，验证了该架构的合理性和通用性。此架构的研究在弥补可信计算相关规范不足的同时，发挥了可信技术的实用性，为如何运用可信计算来增强环境体系安全性和完整性提供了一种思路，使可信计算平台在面对网络信息系统的信息安全应用需求时有依据可循，从而能够实现信息系统真正的信息安全共享的功能。

参 考 文 献

[1] 冯登国，秦宇，汪丹，等. 可信计算技术研究[J]. 计算机研究与发展，2011，48(8)：1332-1349
Feng D G, Qin Y, Wang D, et al. Research on Trusted Computing Technology[J]. Journal of Computer Research and Development, 2011, 48(8): 1332-1349
[2] McDysan D, Lee T H, Yao Lei. Network Access System Including a Programmable Access Device Having Distributed Service Control 7499458B2[P]. 2009-03-03
[3] Frias-Martines V, Sherrick J, Stolfo S J. A Network Access Control Mechanism Based on Behavior Profiles[C]// Annual Computer Security Application Conference (ACSAC'09). Honolulu, 2009: 03-12
[4] 梅芳，刘衍珩，王健，等. 基于可信网络的修复建模与实现[J]. 计算机研究与发展，2009，46(zl)：328-331
Mei F, Liu Y Y, Wang J, et al. Modeling and Realizing of Remediation Based on Trusted Network[J]. Journal of Computer Research and Development, 2009, 46(zl): 328-331
[5] 张焕国，陈璐，张立强. 可信网络连接研究[J]. 计算机学报，2010，33(4)：706-717
Zhang H Q, Chen L, Zhang L Q. Research on Trusted Network Connection[J]. Chinese Journal of Computers, 2010, 33(4): 706-717
[6] 沈昌祥，张焕国，王怀民，等. 可信计算的研究与发展[J]. 中国科学：信息科学，2010，40(2)：139-166
Shen C X, Zhang H G, Wang H M, et al. Research and Development of Trusted Computing[J]. Science China Information Sciences, 2010, 40(2): 139-166
[7] 孙守胜. 基于国产可信计算平台的可信终端的应用研究[D]. 北京：北京交通大学，2011
Sun S S. Research on Application of Secrecy-involved Terminal Based on Trusted Computing Platform[D]. Beijing: Beijing Jiaotong University, 2011
[8] 王浩，陈泽茂，李铮，等. 基于可信网络连接的多级涉密网安全接入方案[J]. 计算机科学，2012，39(12)：65-69
Wang H, Chen Z M, Li Z, et al. Secure Access Scheme Based on TNC for Multi-level Classified Network[J]. Computer Science, 2012, 39(12): 65-69
[9] 王宇，王飞. 涉密信息系统网络安全需求分析与解决方案[J]. 装备学院学报，2013，24(4)：105-109
Wang Y, Wang F. Trusted Security Demand Analysis and Solution of the Secret Information System Network[J]. Journal of Academy of Equipment, 2013, 24(4): 105-109
[10] 谷德丽. 可信网络接入远程证明方案的研究[D]. 哈尔滨：哈尔滨工程大学，2013
Gu D L. Research on Trusted Network Access and Remote Attestation and Scheme[D]. Harbin: Harbin Engineering University, 2013
[11] 刘迎春，郑小林，陈德人. 信任网络中基于角色信誉的信任预测[J]. 北京邮电大学学报，2013，36(1)：72-76
Liu Y C, Zheng X L, Chen D R. Trust Predication Based on The Credibility of The Role in Trust Network[J]. Journal of Beijing University of Posts and Telecommunications, 2013, 36(1): 72-76
[12] 刘一博，殷肖川，高培勇，等. 基于可信计算的网络互联模型[J]. 计算机应用，2014，34(7)：1936-1940
Liu Y B, Yin X C, Gao P Y, et al. Network Interconnection model Based on Trusted Computing[J]. Journal of Computer Applications, 2014, 34(7): 1936-1940
[13] 戴桦. 基于可信计算技术的信任评估机制研究[D]. 南京：南京邮电大学，2011
Dai H. Research on Trust Evaluation Mechanism Based on Trusted Computing Technology[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2011