基于可信平台控制模块的信任评估系统研究

黄坚会，张江江，沈昌祥，张建标，王亮

引用本文

黄坚会，张江江，沈昌祥，张建标，王亮. 基于可信平台控制模块的信任评估系统研究[J]. 计算机科学, 2024, 51(11A): 240200109-6.

HUANG Jianhui, ZHANG Jiangjiang, SHEN Changxiang, ZHANG Jianbiao, WANG liang. Study on Trust Evaluation System Based on Trusted Platform Control Module [J]. Computer Science, 2024, 51(11A): 240200109-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240200109

基于可信平台控制模块的信任评估系统研究

黄坚会[1,2]　张江江[1,2]　沈昌祥[1,2]　张建标[1,2]　王　亮[3]
1 北京工业大学信息学部　北京 100124
2 可信计算北京市重点实验室　北京 100124
3 上海算石科技有限公司　上海 201203
(jackweyhuang@163.com)

摘　要　现有的可信评估都是基于计算机软件扫描或可信模块通过本机报告或网络远程证明来实现的,这提供了本机执行环境构建过程及运行态的可信度量保障,但从网络应用角度来看,还存在着系统性的安全风险。文中提出一种在可信平台控制模块(TPCM)内部增加实现的网络节点信任评估方法来解决这个问题。该方法在双体系架构(计算+防御)下通过防御单元的TPCM来实现快速可靠的信任评估系统,评估后的可信值通过TPCM进行存储和维护。该方案既避免设备受攻击后的伪造,又释放了CPU的计算资源。通过研究基于TPCM支撑的网络节点信任评估系统,实现了轻量级计算机网络平台节点可信性的系统性评估,保障了网络的安全可信运行。

关键词:可信平台控制模块;信任评估;安全可信;动态度量;可信计算3.0
中图分类号　TP393

Study on Trust Evaluation System Based on Trusted Platform Control Module

HUANG Jianhui[1,2],ZHANG Jiangjiang[1,2],SHEN Changxiang[1,2],ZHANG Jianbiao[1,2] and WANG liang[3]
1 Faculty of Information Technology,Beijing University of Technology,Beijing 100124,China
2 Beijing Key Laboratory of Tusted Computing,Beijing 100124,China
3 Shanghai Suanshi Technology CO.,LTD,Shanghai 201203,China

Abstract　The existing trust assessment is based on computer software scanning or trust modules that are achieved through local reporting or remote network authentication,which solves the trust measurement guarantee for the construction process and running status of the local execution environment. However,from the perspective of network applications,there are still systemic security risks. This paper proposes a network node trust evaluation method that adds implementation within the trusted platform control module(TPCM) to address this issue. This method achieves a fast and reliable trust evaluation system under a dual architecture(computing+defense) through the TPCM of defense units,and the evaluated trust values are stored and maintained through TPCM. This scheme not only avoids device forgery after being attacked,but also frees up CPU computing resources. This paper studies a network node trust evaluation system based on TPCM support to achieve a systematic evaluation of the credibility of lightweight computer network platform nodes,ensuring the safe and reliable operation of the network.

Keywords　TPCM,Trust evaluation,Safe and trust,Dynamic measurement,Trusted computing 3.0

1　引言

现有网络信任管理机制的研究对象包含各种联网模型[1-2],如无线传感器网络[3]、ad-hoc网络[4]、车联网[5]等。Das等[6]提出的一种基于模糊理论的分层信任管理方案,包括基于实时过去经验和信誉的直接信任计算以及基于同伴推荐的间接信任计算,该方案降低了通信开销、计算时间和内存利用率。Alnasser等[7]提出了一种基于推荐的信任模型,用以抵御车联网中的内部攻击,并通过分析4种不同类型的攻击表明了该方案的有效性。Shayesteh等[8]针对物联网环境下的健康/无障碍监测服务,提出了一种混合实体和数据的信任计算方案,该方案依赖于贝叶斯学习对用户进行评分,并基于Dempster-Shafer理论进行数据融合和计算数据本身的可信度。

以上方法都是建立在使用计算单元的CPU计算资源之上,这样实现存在两大缺点:1)计算资源占用,特别是在实时性要求高的场合,容易争抢计算CPU的计算资源;2)安全性不够,计算系统容易遭受病毒攻击,比如木马等,那么一旦黑客成功入侵,信任评估系统则会完全失去功能。

物联网、车联网、工业网络、石油管网等由于其所处环境的恶劣性,更易遭受恶意攻击,而且终端CPU算力资源有限,限制了该类信任评估方案的推广应用。本文在充分研究各种信任模型的基础上,根据可信计算3.0双体系防护体系结构[9]思想提出了一种基于可信平台控制模块(Trusted Plat-

基金项目:北京市自然科学基金(M21039)
This work was supported by the Natural Science Foundation of Beijing,China(M21039).
通信作者:张江江(jiangofyouth@163.com)

form Control Module,TPCM)可信根的可信评估系统,该系统通过优化及算法加速设计可以提升运算效率及安全性,适用于开放性互联网、工业网络、物联网、车联网等。

本文的主要贡献如下:

1)将基于信任评估模型引入可信计算体系,补全可信计算在网络系统性安全评估方面的缺失。

2)使用完全中国自主的主动防御 TPCM 模块作为节点设备信任评估系统基台,保证评估环境、过程和结果的可靠。

3)在 TPCM 支撑下结合三阶度量[11],通过网络交互信任系统算法全面评估对方网络节点的可信性和安全性。

4)本可信评估系统涉及的历史数据、度量值和数据传输受可信计算 3.0_TPCM 可信根的主动防御保护,为信任评估的准确性和可信性提供依据和保障。

5)本系统模型针对 TPCM 的算力及信任时效性特点,采用贝叶斯理论对网络节点进行综合评估。

2 基于 TPCM 的可信节点架构及模型构建原理

本文采用可信计算 3.0_TPCM 可信根作为信任评估系统的计算载体。TPCM 是网络节点的信任源点,为信任评估提供证据支撑。同时,TPCM 实体为信任评估提供算力和执行环境保障。信任评估是网络安全可信体系构建和维系的重要保障机制。

信任评估系统运行和数据来自于 TPCM 防护单元,从而能够保障数据来源和执行环境的可靠可信。通过信任评估综合分析给出对计算机目标节点客观公正的可信评估,同样,交互结果通过 TPCM 记录交易作为直接和间接信任评估的数据输入。

本文可信评估系统根据可信计算 3.0 场景和 TPCM 算力环境[9]需求,对贝叶斯理论进行优化改进。首先根据信任的获取方式,分别从直接信任度模块和间接信任度模块两方面进行分析。直接信任度评估数据来自 TPCM,同时算法上引用信任衰减函数进行直接信任度的计算。在间接信任度模块中通过设计相似度和评价一致性计算节点可靠性,优化了推荐节点的权重。针对间接信任评估中存在的不诚实推荐行为的问题,设计节点推荐行为一致性优化策略,完成了对网络节点的间接信任评估。最后综合直接信任度、间接信任度及可信度量值计算综合信任度,并将节点更新行为考虑在内。最后通过实验验证系统的优越性。

3 基于 TPCM 的信任评估系统

本文所提方法主要基于 TPCM 执行环境下的信任评估系统建立。为了简化推演描述,以下所有算法执行及数据存储都由 TPCM 可信根独立提供,并根据 TPCM 执行环境进行算法和存储优化。

3.1 基本定义

1)信任定义

信任是在请求节点对目标节点的认可程度,即可信度。节点的可信度量值不仅是两个节点间的历史信任评估经验,而且也可以作为推荐信息为其他节点的信任度量提供间接依据。

两个节点间的相互信任通常与可靠性与合作性有关,也会在计算过程中引入相关定义[12]:

(1)可靠性:通常考虑节点间的相似度。将两个节点的可信度量值进行比较,推荐节点与请求节点间的信任值相似程度越高,推断两个节点间的评估过程越接近,则推荐节点提供的推荐信息可靠性也就越高。

(2)合作性:具体表现为两个节点间的合作次数,侧面表现为受欢迎程度。合作次数越多,暗示其他节点越愿意与目标节点进行交互,进而说明该目标节点的可信度越高。

2)节点定义

根据评估过程中担当的角色不同,可将节点分为 3 种:

(1)请求节点:该节点提起需求,同时担当对目标节点进行信任评估的角色。

(2)目标节点:该节点为被评估信任值的节点,是提供服务的角色。

(3)推荐节点:该节点是请求节点的朋友节点,为请求节点传递关于目标节点的推荐信任值。

3)信任可信度量值定义

(1)直接信任度量值是请求节点分析与目标节点历史可信值数据后,对目标节点未来交互可信度的预测,记作 $DTrust$。

(2)间接信任度量值是请求节点根据推荐节点传递的对目标节点的信任数据,判断并预测目标节点提供服务的能力,记作 $RTrust$。

4)贝叶斯模型

贝叶斯定理是一种可用于多个领域中的概率计算法则。贝叶斯定理的公式为:

$$P(B_i|A)=\frac{P(B_i)P(A|B)}{\sum_{j=1}^{n}P(B_j)P(A|B_j)} \tag{1}$$

贝叶斯定理是通过 A 事件发生前的先验概率 $P(B_i)$ 来推断在 A 事件发生后 B_i 事件发生的可能性(称为后验概率 $P(B_iA)$)。通过贝叶斯模型不仅可以对不确定概率事件进行推理,也可以对不完整的数据进行预测[13]。因此,本文在式(1)的基础上进行信任评估模型的构建。

5)其他符号定义

在综合信任评估模型构建中,一些常用模型基本符号被定义,SV_{ij} 表示节点 i 对 j 的服务质量评价向量。具体地,综合信任评估模型基本符号定义细节如表 1 所列。

表 1 综合信任评估模型基本符号定义

Table 1 Basic symbol definition of comprehensive trust assessment model

指标符号	描述
SV_{ij}	节点 i 对 j 的服务质量评价向量
θ	服务评估概率
p	交互合作中可信的次数
n	节点间交互总次数
RED_{im}	节点 i 对推荐节点 m 评估的可靠程度
D_i	节点 i 交互节点的集合
D_m	节点 m 交互节点的集合
U_m	推荐节点 m 的一致性

6)模型描述

两个节点交互合作,请求节点基于这一事件对目标节点进行评估,而目标节点拥有的所有评价共同组成其信誉。请求节点又可通过该目标节点表现出的信誉选择是否交互。

对评估过程基本的描述为:假设可信管理中心的节点 A

将对终端节点 B 发起合作验证,则需要确定节点 B 的信任值,以保证节点 B 是可信的。评估流程分为 3 部分:

1)在直接信任度评估模块中,根据贝叶斯定理构建信任的 beta 分布,首先计算先验概率,再由先验概率推出后验概率。并通过引入衰减因子进行直接信任参数的动态更新,最终得到目标节点的直接信任可信度量值。

2)在间接信任度评估模块中,需要根据推荐节点的推荐信息确定推荐信任值。首先计算推荐节点与目标节点交互的节点集合间的相似度,再将其评价结果与所有推荐节点的评价结果进行比较。然后,结合节点间的相似性和一致性,对其进行可靠性评价。最后,通过对每个推荐节点的可信度进行权重计算,得出节点的推荐可信度量值。

3)在综合信任度评估模块中,根据直接和间接信任度模块各自的权重,最终通过加权和得出综合信任可信度量值。

3.2 直接信任度评估计算

3.2.1 问题分析

直接信任是两个节点在直接交互情况下请求节点产生的对目标节点的评价信息。请求节点的评估结果可以分为可信和不可信两种状态[14]。基于此,我们可以将评估结果抽象为集合{可信:1;不可信:0},即为一种二元离散状态分布。因此,可以通过引入基于 Beta 分布的贝叶斯方法进行信任评估。但现有的 Beta 分布模型大多没有考虑到信任衰减的特性,先前可信的节点可能随着时间的推移变得不可信,但不考虑时间衰减因素的模型,会依旧认为该节点可信,恶意节点容易抓住这一漏洞伪造自己提供可信服务的表象,在获取请求节点的信任后再实施自己的攻击目的。为解决此类问题,直接信任度评估模块设计加入一个衰减函数,对参数进行实时的更新,以提高其评估可靠性。

3.2.2 直接信任度计算

有节点 i 对目标节点 j 进行 n 次交互的评价记录保存在服务质量评价向量 $SV_{ij}=(x_{ij}(1),x_{ij}(2),\cdots,x_{ij}(n))$ 中,其中有 p 次交互行为是可信的。根据历史评价经验计算节点 i 对节点 j 的直接信任度量值的步骤如下[15]:

1)建立初始 Beta 分布

用 θ 表示节点 i 对节点 j 网络交互评估为可信或不可信("0"或"1")的概率。根据比例随机变量特点,构建贝塔模型:

$$p(\theta)=Beta(\alpha,\beta) \tag{2}$$

其中,$\theta\in[0,1]$,且 $\alpha\geqslant 0,\beta\geqslant 0$,$\alpha$ 和 β 是由物联网直接信任模型的先验假设确定的参数。在节点 i 和 j 的 n 次有限网络交互中,可信的比例可表示为 θ_{ij} 的简单的估量值:

$$\hat{\theta}_{ij}=\frac{p}{n} \tag{3}$$

2)计算先验概率

在本文中假设节点间每次的网络交互都是随机的,则对于交互行为评价 p 次可信和 $(n-p)$ 次不可信的似然函数可表示为:

$$p(SV_{ij}\mid\hat{\theta})=\hat{\theta}^{p}(1-\hat{\theta})^{n-p} \tag{4}$$

根据似然函数和 Beta 分布,可以设定 $\hat{\theta}_{ij}$ 的先验概率分布:

$$f(\hat{\theta};\alpha,\beta)=\frac{\hat{\theta}^{\alpha-1}(1-\hat{\theta})^{\beta-1}}{\int_0^1 u^{\alpha-1}(1-u)^{\beta-1}\mathrm{d}u} \tag{5}$$

$$f(\hat{\theta};\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\hat{\theta}^{\alpha-1}(1-\hat{\theta})^{\beta-1} \tag{6}$$

3)推出后验概率

根据贝叶斯定理可推出:

$$f(\hat{\theta}\mid SV)\propto f(SV\mid\hat{\theta})\times f(\hat{\theta}) \tag{7}$$

即 $\hat{\theta}$ 的后验概率与其对应的似然函数和先验概率成正比。

因此,通过式(4)、式(6)共同计算得出 $\hat{\theta}$ 的后验概率为:

$$f(\hat{\theta}\mid SV)=\frac{\Gamma(n+\alpha+\beta)}{\Gamma(p+\alpha)\Gamma(n-p+\beta)}\hat{\theta}^{p+\alpha-1}(1-\hat{\theta})^{n-p+\beta-1} \tag{8}$$

即 $\hat{\theta}$ 的后验概率也遵从 beta 分布:

$$p(\hat{\theta}\mid SV)=Beta(\alpha+p,\beta+n-p) \tag{9}$$

4)引入衰减函数

根据信任的属性可知,对节点评估的信任具有时效性[16]。通常来说,用距离交互时间节点越远的信任值来反映当前行为可信水平的能力越低。反之,节点间的交互行为时间越近,其属性评价越能代表节点间的可信水平。而某些未考虑信任时间因素的评估模型,则会缺乏辨别历史评价中不同时刻对节点信任水平影响不同的能力。

文献[17]指出,信任的衰减程度不是线性的,所以既要保证最近交互记录的重要程度,也不能完全抛弃历史交互评价。同时,文献[18]中提出了一种定义交互时间间隔来反映信任衰减强弱的方法。虽然该方法考虑了信任衰减特性,但对于节点的动态加入和退出情况下的信任具有局限性。

所以设定下列时间衰减函数,利用信任评价产生与当前时间的距离作为考量信任衰减的评判,并加入衰减因子来适应不同场景的行为下的衰减速度,具体方法如下:

$$TD(t_{k+1})=h\times TD(t_k) \tag{10}$$

其中,t 为每次交互的时间标记,每个时刻的信任程度是由每个时间标记来表达的;t_k 为当前时间标记,t_{k+1} 为下一时刻时间标记;h 是用于控制衰减率的衰减系数。

5)更新参数

进一步通过引入衰减函数更新参数 α 和 β,同时引入 $\sigma=\{1,0\}$ 因子来保证 Beta 密度函数。根据节点交互状态设定 σ 的值,交互成功取 $\sigma=1$,反之取 $\sigma=0$。具体更新公式如下:

$$\begin{cases}\alpha=\gamma\sum\limits_{m=1}^{n}TD(t_m)\cdot\alpha_m\cdot\sigma_m+p\\ \beta=\eta\sum\limits_{m=1}^{n}TD(t_m)\cdot\beta_m\cdot(1-\sigma_m)+(n-p)\end{cases} \tag{11}$$

其中,γ,η 为自适应值。

6)直接信任值计算

节点 i 对节点 j 的信任预测,也可表示为节点 i 与 j 之间下一次交互概率的估计。最终,节点 j 的信任值是 beta 分布的统计期望,由此可得节点 j 的直接信任值为:

$$DTrust_{ij}=E(Beta(\alpha+1,\beta+1))=\frac{\alpha+1}{\alpha+\beta+2} \tag{12}$$

3.3 间接信任度评估计算

3.3.1 问题分析

根据对间接信任分类的分析,指出间接信任是通过第三方的推荐信息得出的间接信任值。如何最大化利用推荐节点的推荐信息,是本文研究的重点[19]。首先考虑影响信任计算

的因素，通常来自两个方面：

1)推荐节点的诚实度。越诚实的节点提供的信息才更具有价值。

2)请求节点对推荐节点的信任度。推荐节点的信任程度越高，那么此节点的服务质量越好，则认为其提供的信息也越有价值。

考虑最大化推荐信息的参考价值，结合前文中对信任的定义分析，本文提出利用节点的相似性及自身可信度综合评估推荐节点的可靠性，并结合推荐节点与推荐节点整体间的偏差来对推荐节点进行加权优化，从而降低恶意节点的攻击风险，提高推荐信任的可信程度。

3.3.2 间接信任度计算

节点 i 对节点 j 的间接信任 $RTrust_{ij}$ 计算流程如下：

1)计算推荐节点可靠性

定义 1 推荐节点的可信度通过请求节点与推荐节点间都交互的节点反馈的相似度以及与节点间的一致性共同评估。

推荐节点 m 的可靠度具体计算式如下：

$$RDE_{im}=\frac{Sim(i,m)}{\sum_{m\in M}Sim(i,m)}\cdot U_m \tag{13}$$

其中，RDE_{im} 为推荐节点可信度，是节点 i 对推荐节点 m 评估的信任程度。该推荐节点的信任程度表达为节点 i 与节点 m 均直接交互过的节点对它们反馈的相似度以及节点 m 与整体评价的偏差。

2)计算节点相似度

推荐节点与请求节点间公共节点越多，证明节点间的行为偏好和需求愈接近，则该推荐节点的推荐信息参考性更高。

定义 2 节点相似度 $Sim(i,m)$ 是对两个节点的交互节点的相似程度的评估。

基于 Jarccard 函数[20]，计算式如下：

$$Sim(i,m)=\frac{|D_i\bigcap D_m|}{|D_i\bigcup D_m|} \tag{14}$$

其中，D_i，D_m 分别是节点 i 和节点 m 发生交互节点的集合。若与节点都合作过的公共节点占总节点的比重越大，则认为对公共节点的相似度越高。

3)计算节点一致性

网络中的恶意节点为传递恶意评价行为，或采用提供高质量服务以获取请求节点的信任。在获取高信任值后，再进行恶意评价，释放恶意的推荐信息。这就导致恶意节点实际的信任值与请求节点预期不一致。因此考虑用推荐节点传递的信任度与整体评价是否一致的评估来降低恶意节点的权重。

定义 3 推荐节点的一致性是用来表示推荐节点与其他节点推荐行为一致的程度。则计算式如下：

$$U_m=\lambda(1-Diff_m) \tag{15}$$

其中，λ 为自适应值，$Diff_m$ 是推荐节点 m 的评价差异度。

定义 4 评价差异度是请求节点的某一推荐节点与全体推荐节点对目标节点综合评价行为的偏差。具体表达式为：

$$Diff_m=\mu\frac{DTrust_{mj}-\overline{DE_m}}{\sum_{i=1}^{m}DTrust_{mj}-\overline{DE_m}} \tag{16}$$

其中，μ 为自适应值，$\overline{DE_m}$ 为全体推荐节点对目标节点 j 的直接信任度的期望。

4)推荐信任值计算

根据节点的相似度、一致性综合得出的权重结合推荐节点自身可信度，综合得出请求节点 i 对目标节点 m 的推荐信任度。最终计算式如下：

$$RTrust_{ij}=\sum_{m\in M}RDE_{im}\times DTrust_{mj} \tag{17}$$

3.4 综合信任度评估计算

3.4.1 综合信任度计算

再通过集成直接信任度量值和间接信任度量值，得出综合信任 $GTrust_{ij}=\langle\mu_{GTrust_{ij}},\nu_{GTrust_{ij}}\rangle$，计算式公式如下：

$$GTrust_{ij}=ITrust_j(\omega_D DTrust_{ij}\oplus\omega_R RTrust_{ij}) \tag{18}$$

其中，$ITrust_j$ 为节点 j 内置 TPCM 对计算机上电启动及运行态全生命周期可信度量值(简称可信度量值)，具体计算如下：

$$ITrust_j=\sum_{k=1}^{n}\omega_k T_k \tag{19}$$

其中，ω_k 为各可信度量项的权重，由节点 TPCM 安全可信策略决定。

ω_D 与 ω_R($\omega_D\geqslant 0$，$\omega_R\geqslant 0$ 且 $\omega_D+\omega_R=1$)分别为直接信任度和间接信任度的权重。在以往的方法中，通常直接将各部分权重平均分配，或是按照不同系统由管理员直接拟定。但固定权重会忽视节点交互的动态变化对信任的影响，无法结合实际情况动态分配直接信任和间接信任的重要程度。因此，本文拟定结合节点间的交互次数，对各部分权重进行分配。

权重具体数值可由式(20)、式(21)得出：

$$\omega_D=\frac{n_D}{n_D+n_M} \tag{20}$$

$$\omega_R=\frac{n_M}{n_D+n_M} \tag{21}$$

3.4.2 综合信任度的更新与存储

1)更新信任度

在很多计算环境中，节点的行为不是固定不动的，如果信任值不随着行为的变化而一同改变，可能会对节点间的合作造成不可预料的影响。因此，当请求节点与目标节点完成合作后，需要及时进行节点的更新。具体的更新方式如下：

$$GTrust'_{ij}=ITrust_j(\sigma\times DTrust_{ij}+(1-\sigma)GTrust_{ij}) \tag{22}$$

其中，σ 为直接信任度的权重占比，可根据不同系统设置不同的权重。

2)存储信任度

构建信任度表(见图 1)，在交互结束后，将此次更新后的信任记录在表格中。若列表中无该节点的信任度，则首先验证是否还有存储空间。如果没有，则丢弃时间最久的信任记录，在表尾插入新的记录；如果有，则直接在表尾插入。若列表中含有该节点的信任度，那么历史信任值将被直接更新。

节点1	节点2	节点3	...	n	
信任值1	信任值2	信任值3	...	n	

队列更新方向→

图 1 信任值存储示意图

Fig. 1 Schematic diagram of trust value storage

4 测试

本实验通过联合研制 FPGA TPCM 卡来构造信任评估系统环境，然后通过服务器与节点终端组成的网络（见图 2）来验证该系统的有效性。测试设备包括：

1）可信服务器端一台（见图 3），含 FPGA TPCM 卡的服务器、M2 服务器硬盘、CentOS-7 操作系统；

2）可信网络节点终端（见图 4）多台，含 FPGA TPCM 卡的计算机、SSD 硬盘、CentOS-7 操作系统；

3）路由器、交换机等网络设备测试过程。

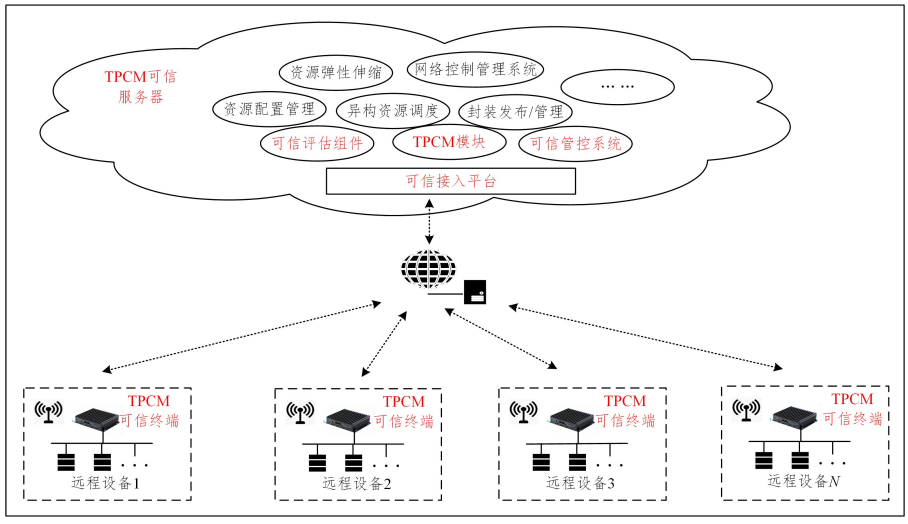

图 2 可信评估验证系统测试意图

Fig. 2 Test Intent for trustworthiness assessment verification system

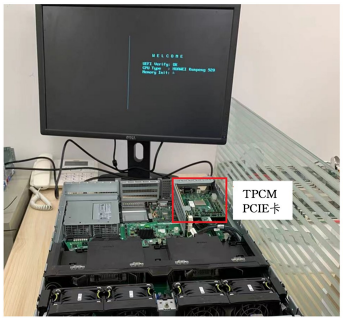

图 3 可信服务器实物图

Fig. 3 Physical picture of trusted server

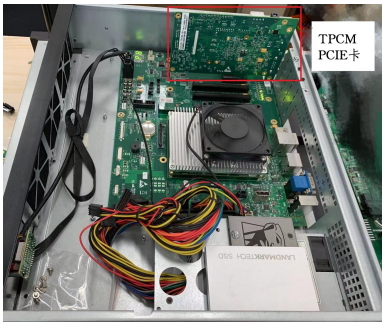

图 4 可信终端实物图

Fig. 4 Physical picture of trusted terminal

测试过程如下：

每个网络节点（包括服务器和终端节点计算机）从连接电源开始到网络连接，TPCM 记录整个度量和安全可信判定全过程[21]，并可通过可信管理中心进行可信策略下发、进程可信管理、可信状态管理、可信远程证明请求等。

实际操作过程中，通过网络节点信任值变化及模拟设备内部攻击（例如修改 BIOS 固件、注入非法软件、修改操作系统内容文件等）来测试评估系统（见图 5）。

可信管理中心通过直接和间接信任两个维度进行网络节点评估，最后通过综合信任度模型进行判定记录。

在进行直接信任度评估时，获取网络节点历史信任值数据，通过直接信任模型进行计算评估。

进行间接信任度评估时，寻找推荐节点，通过信任间接评估模型进行计算评估。

最后综合直接信任度量值、间接信任度量值及可信度量值数据，并引入权重算法得出综合信任评估结果作为该次可信网络接入评估依据，并及时更新该节点的信任度值表。

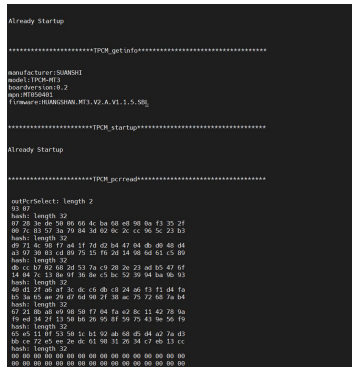

图 5 TPCM 度量 BIOS 固件相关信息

Fig. 5 TPCM measures BIOS firmware related information

当综合信任评估通过时，可信管理中心允许该节点接入可信网络，进行正常功能服务请求直至下次可信评估失败或该次网络连接退出。

表 2 中的数据是在设定直接信任度和间接信任度权重的前提下采用模拟攻击方式测试系统对可信度量值做出的节点综合评估。该测试中，当网络节点综合评估值大于 0.6 时，系统判定综合评估结果为通过，允许该节点接入可信网络，否则阻止接入网络，并由 TPCM 记录评估结果作为以后评估的历史参考数据。

表 2 模拟攻击实验结果

Table 2 Simulation attack experiment results

接入测试	模拟攻击	直接信任度权重	直接评估结果	间接评估结果	可信度值	综合评估值	综合评估结果
1	启动代码(BIOS)攻击	0.8	不通过	通过	0.8	0.5	不通过
2	PCI 设备卡恶意替换	0.2	不通过	通过	0.7	0.7	通过
3	操作系统 Boot loader	0.2	不通过	通过	0.8	0.6	不通过
4	操作系统内核文件	0.8	通过	不通过	0.8	0.8	通过
5	程序进程攻击	0.8	通过	通过	0.7	0.7	通过
6	USB 设备非法接入	0.8	通过	不通过	0.7	0.8	通过
7	系统配置参数串改	0.6	不通过	通过	0.6	0.6	不通过
8	内存数据修改	0.6	不通过	不通过	0.5	0.4	不通过

通过多组模拟测试及平台厂家评估，达到预期的网络节点防护的目的，而且经过一个星期的压力测试丝毫没有影响正常业务运行状态，计算机节点及网络系统工作正常稳定。

结束语 针对现有的可信评估机制存在一定的系统性安全风险问题，本文基于可信平台控制模块(TPCM)可信根，按照可信计算 3.0 双体系防护体系结构设计要求构建一套计算机网络的信任评估系统。首先该系统使用完全中国自主主动防御 TPCM 模块作为信任根，并且 TPCM 经过国家密码局的安全检测，可为信任评估系统提供信任基础。利用 TPCM 最早上电度量收集计算平台代码及可信执行环境信息作为信任评估的基础依据参考。在 TPCM 独立算力支持下，通过网络交互信任系统算法全面评估对方网络节点的可信性和安全性。本系统算法执行环境、历史数据、度量值受可信计算 3.0 主动防御保护，为信任评估的准确性和可靠性提供依据和保障。本系统算法针对信任具有时效性的特点，改进贝叶斯理论对网络节点进行直接信任评估，同时结合间接信任评估方法，来得到终端的综合信任值。最后，通过搭建平台测试，证明该系统达到了安全保障要求。

参 考 文 献

[1] ALWARAFY A, AL-THELAYA K A, ABDALLAH M, et al. A survey on security and privacy issues in edge-computing-assisted internet of things[J]. IEEE Internet of Things Journal, 2020, 8(6): 4004-4022.

[2] LIU L, MA Z, MENG W. Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks[J]. Future Generation Computer Systems, 2019, 101: 865-879.

[3] SOUISSI I, AZZOUNA N B, SAID L B. A multi-level study of information trust models in WSN-assisted IoT[J]. Computer Networks, 2019, 151: 12-30.

[4] HE Y, YU F R, WEI Z, et al. Trust management for secure cognitive radio vehicular ad hoc networks[J]. Ad Hoc Networks, 2019, 86: 154-165.

[5] LU Z, QU G, LIU Z. A survey on recent advances in vehicular network security, trust, and privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 20(2): 760-776.

[6] DAS R, DASH D, SARKAR M K. HTMS: fuzzy based hierarchical trust management scheme in WSN[J]. Wireless Personal Communications, 2020, 112(2): 1079-1112.

[7] ALNASSER A, SUN H, JIANG J. Recommendation-based trust model for vehicle-to-everything (V2X)[J]. IEEE Internet of Things Journal, 2019, 7(1): 440-450.

[8] SHAYESTEH B, HAKAMI V, AKBARIA. A trust management scheme for IoT-enabled environmental health/accessibility monitoring services[J]. International Journal of Information Security, 2020, 19(1): 93-110.

[9] SHEN C X. Building Cyber Security Defense by Trusted Computing 3.0[J]. Journal of Information Security Research, 2017, 3(4): 290-298.

[10] GB/T 40650-2021. 可信平台控制模块[S]. 北京：中国标准出版社，2021.

[11] HUANG J H, SHEN C X, XIE W L. The TPCM 3P3C Defense Architecture of Safety and Trusted Platform [J]. J. Wuhan Univ. (Nat. SCI. Ed.), 2018, 64(2): 109-114.

[12] ZHANG J, NING Z, CAO H. An Intelligent Trusted Edge Data Production Method for Distributed Internet of Things, Neural Computing and Applications[J]. Neural Computing & Applications, 2023, 35(29): 21333-21347.

[13] ZHANG J, NING Z, WAQAS R A M, et al. A Many-objective Ensemble Optimization Algorithm for the Edge Cloud Resource Scheduling Problem[J], IEEE Transactions on Mobile Computing, 2023, 23(2): 1330-1346.

[14] SINGH J, BELLO Y, HUSSEINA R, et al. Hierarchical Security Paradigm for IoT Multiaccess Edge Computing[J]. IEEE Internet Things J., 2021, 8(7): 5794-5805.

[15] ZHANG P, JIANG C, PANG X, et al. STEC-IoT: A Security Tactic by Virtualizing Edge Computing on IoT[J]. IEEE Internet Things J., 2021, 8(4): 2459-2467.

[16] BASSET M A, MANOGARAN G, MOHAMED M. A Neutrosophic theory based security approach for fog and mobile-edge computing[J]. Computer Networks, 2019, 157: 122-132.

[17] ELGENDY I A, ZHANG W, TIAN Y C, et al. Resource allocation and computation offloading with data security for mobile edge computing[J]. Future Generation Computer Systems, 2019, 100: 531-541.

[18] TSAI J L, LO N W. A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services[J]. IEEE Systems Journal, 2017, 9(3): 805-815.

[19] HUANG B, LI Z, TANG P, et al. Security modeling and efficient computation offloading for service workflow in mobile edge computing[J]. Future Generation Computer Systems, 2019, 97: 755-774.

[20] AAKASH B, ZACHARY E, ZACHARY K, et al. Graph Context Encoding for Neural Source Code Summarization[J]. IEEE Transactions on Software Engineering, 2023, 49(9): 4268-4281.

[21] HUANG J H, SHEN C X. Trusted Platform Design of Server with TPCM Active Defense [J]. Journal of Zhengzhou University(Natural Science Edition), 2019, 51(3): 1-6.

HUANG Jianhui, born in 1979, Ph. D. His main research interests include cyberspace security and trusted computing.

ZHANG Jiangjiang, born in 1994, Ph.D. His main research interests include cyberspace security and big data modeling.