基于模糊集合的可信计算信任模型评估*)

陈书义[1] 闻英友[1,2] 赵 宏[1,2]

(东北大学计算机软件国家工程研究中心 沈阳 110004)[1] (东软研究院 沈阳 110179)[2]

摘 要 可信计算是信息安全的重要研究领域,而信任模型的可信性评估是该领域中亟待解决的关键问题。在深入研究可信计算信任根、信任链及其可信性影响因素的基础上,提出了基于模糊集合理论的可信计算信任模型评估方法。基于模糊集合理论的评估方法定义了不同的可信度度量规则和模糊集合,基于计算得到的可信度,评价信任模型的可信性。分析结果表明,基于模糊集合的信任评估方法能够有效评估可信计算信任模型的可信性,丰富了可信计算信任评估理论。

关键词 可信计算,可信计算平台,信任链,可信度,模糊集合

Trust Evaluation of Trusted Computing Models Based on Fuzzy Set

CHEN Shu-yi[1] WEN Ying-you[1,2] ZHAO Hong[1,2]

(Software Center of Northeastern University, Shenyang 110004, China)[1] (Neusoft Research, Shenyang 110179, China)[2]

Abstract Trusted computing is a significant research aspect of information security. The problem is urgent to resolve that how to evaluate the trust level of trusted computing model. The theories of trusted root, trusted chain and influence factors of trust were studied. Trust level evaluation method of trusted computing models was proposed based on fuzzy set. The different measurement rules and fuzzy sets were defined according to influence factors of trust, and the properties of trusted models were evaluated based on the trust level calculated. Analyzing results show that trusted computing system can be exactly and effectively evaluated with provided methods, which enriches the evaluation theory of trusted computing.

Keywords Trusted computing, Trusted computing platform, Chain of trust, Trust level, Fuzzy set

1 引言

可信计算技术旨在通过增强现有 PC 终端的安全性,在源头上控制不安全的因素,从根本上解决信息安全问题。目前可信计算领域存在的主要问题是理论研究远远落后于技术发展。国际上一些著名机构积极开展可信计算相关技术的研究。TCG (Trusted Computing Group,可信计算组)制定了 TPM(Trusted Platform Module,可信平台模块)、可信计算平台和可信网络连接等技术规范[1];微软提出了 NGSCB(Next-Generation Secure Computing Base)[2];Intel 公司的 LT(La Grande Technology)[3]以及 AMD 的 SEM(Secure Execution Mode)[4]等。国内学者也提出了基于可信计算的移动终端用户认证方案[5]、可信安全计算平台等应用模型[6]。但是国内外还没有公认的能够对可信计算信任模型的可信性进行形式化分析、度量的理论。

对可信计算信任模型进行可信性评估具有重要的理论意义和应用价值。有许多可信计算应用模型虽然是经过安全专家认真地分析、设计和实现的,但是仍然存在漏洞。因此,在可信计算应用模型设计过程中引入形式化分析、验证方法,从理论上分析可信计算应用模型的可信性,对于保证可信计算信任模型的安全性具有重要意义。

目前,国内外学者针对分布式环境中信任管理进行了大量研究,并取得了一定的成果[7-9]。然而信任管理理论是针对不同应用背景的,例如,分布式环境下的信任模型强调动态性和不确定性,电子商务中的信任模型强调交互双方的互信,而可信计算中的信任模型强调基于信任根的可信性传递。所以,分布式环境中的信任管理模型并不适合用于基于信任根,沿着信任链,通过信任扩展保障可信性的可信计算应用环境,可信计算需要一种能反映可信计算应用特性的可信性评估方法。如果在深入分析可信计算中可信性影响因素的基础上,提出针对可信计算应用环境的信任模型可信性度量的方法,对可信计算信任模型进行评估,将会更准确、更有效。

2 可信计算技术

2.1 可信计算平台

TCG 可信计算技术从 3 个方面提高计算机系统的安全防护能力:确保用户工作空间的完整性与私有性;确保硬件环境配置、OS 内核、服务及应用程序的完整性;确保存储、处理、传输信息的机密性、完整性。2001 年 2 月,TCG 发布了可信计算平台规范。可信计算平台是保证计算可信的基础,是本地用户和远程实体可以信任的平台[10]。可信计算平台的完整性机制如图 1 所示。信任链的建立从构建信任根开始,信任根由 CRTM(Core Root of Trust Measurement,核心可信测量根)和完整性报告可信根 TPM 组成,是主板上唯一的可信

*)基金项目:国家自然科学基金(60602061),国家高技术研究发展计划(2006AA01Z413)。**陈书义** 博士研究生,主要研究方向为网络与信息安全、下一代网络;**闻英友** 博士,主要研究方向为网络与信息安全、下一代网络;**赵 宏** 教授,博士生导师,主要研究方向为网络与信息安全、网络管理。

组件，然后到 BIOS、操作系统、应用和网络。计算机每次启动都从 CRTM 开始，沿信任链一级认证一级，一级信任一级，完成对信任链组件可信性的度量，把信任扩展到整个平台。

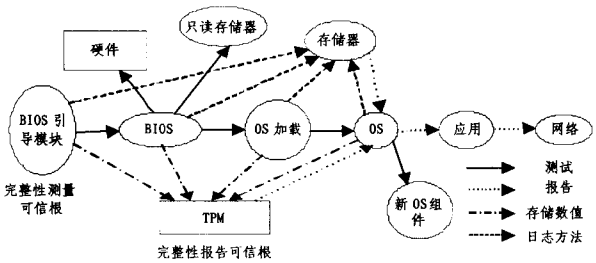

图 1　可信计算平台完整性机制

2.2　可信计算中可信的语义和影响可信性的因素

根据 TCG 的定义，可信是主体的行为与行为结果对预期要求的满足，可信性是同具体的预期相联系的一种属性。可信计算不仅关注基于身份真实性的访问控制，而且引入了对系统完整性的度量。引入完整性可信的观念是信息安全领域一次重大的飞跃。

2.2.1　完整性可信

实体的完整性可信主要通过可信测量、可信存储和可信报告来实现。可信测量实现可靠的实体完整性测量；可信存储模块能够防止存储结果的非授权改变；可信报告能够可靠地报告可信存储模块中存储的测量结果。本地用户或远程实体可以通过可信报告模块查询被验证实体的可信完整性值，然后对实体当前的完整性进行测量，测量结果同可信完整性值进行对比。如果两个值相匹配，那么本地用户或远程实体相信被验证的实体满足完整性。

影响完整性测量可信性的主要因素是委托链长度和测量服务的属性。首先，信任传递中委托链的长度是测量可信性的一个约束条件，委托链越长，信任损失的可能性就越大。其次，完整性测量执行实体的测量服务属性也会对测量的可信性产生影响。例如本地测量一般要比经过网络的远程测量可信，固件、系统软件一般比应用软件具有更可信的测量属性。

2.2.2　真实性可信

实体的真实性可信主要通过公钥密码学来保障。公钥机制使得通信各方在保证私钥保密性的同时，又保证公钥的公开性。系统中的用户相信认证机构能够准确地建立并维护有效的证书，基于公钥机制对通信对方的身份真实性进行鉴别。

影响真实性测量可信性的主要因素是证书链长度和证书策略。证书链表达了自证书签发者起允许的认证路径长度，认证路径长度越长，CA 越不可信。证书策略指出了证书的适用范围，用户对 CA 的信任是通过承认其所颁发的一定策略的证书体现的。证书策略的有效范围和映射过程将影响证书的可信度。

3　基于模糊集合理论的可信计算信任评估方法

可信计算基于信任根，利用委托测量的方式扩展信任域，使可信性成为可以度量的属性。本文在深入分析影响实体可信性因素的基础上，提出了可信度计算方法，用 0 到 1 之间的连续值来表示可信度。并且利用模糊集合对可信性进行分类，根据隶属函数判断实体的信任属性，提供更有针对性的信任可信性评估手段。

3.1　可信计算中可信度的模糊集合描述

可信度不是一个静态的属性，是一种统计的体现，可信度受成功以期望的行为完成期望的任务统计情况和来自其它实体推荐的影响。在深入分析这些影响因素的基础上，我们提出了可信的可信度计算方式。

3.1.1　完整性可信度的计算

对于观察者 e_0 来说，被测量对象 e_1 的完整性可信度主要受测量执行实体完整性测量能力可信性的影响。此外，如果测量过程中委托其他实体进行测量，委托链的长度也会影响测量的结果：委托链越长，测量结果越不可信。因此，被测量对象 e_1 的完整性可信度计算如式(1)所示：

$$T_{\text{integ}}(e_0,e_1)=\begin{cases}\gamma & ,e_0 \text{ 直接执行测量}\\ \alpha_{\text{cur}}(e_0,e_m)\cdot(1-\mu\beta)^i\cdot\gamma & ,e_0 \text{ 委托 } e_m \text{ 执行测量}\end{cases} \tag{1}$$

其中 $T_{\text{integ}}(e_0,e_1)$ 是观察实体 e_0 得到的被测量实体 e_1 的完整性可信度，为 0 到 1 之间的实数；α_{cur} 是 e_0 认为完整性测量实体 e_m 完整性测量能力的可信度，为 0 到 1 之间的实数；β 是一级委托测量所带来的信任损失值，可以在系统初始化的时候设置；μ 是信任损失系数，随着信任链上实体测量可信度的提高而减小，如果为 0 则表示没有信任损失；i 是委托测量链的长度；γ 是测量的结果，如果测量得到的完整性等于期望的完整性值，$\gamma=1$，否则 $\gamma=0$。

完整性测量能力可信度除受实体本身的测量服务属性约束外，还受经验和推荐信息等因素的影响。测量能力可信度在系统初始化的时候可以赋一个 0 到 1 之间的值。赋值时要考虑实体本身的测量服务属性，例如测量执行者是固件、系统软件或者应用软件，测量是本地测量或者远程测量等。经验信息主要是正确执行完整性测量的记录和来自其他实体的推荐评价等。可以根据这些信息调整测量可信度，调整的方式如下：

$$\alpha'_{\text{cur}}(e_0,e_m)=r\cdot\alpha_{\text{cur}}(e_0,e_m)+s\cdot\alpha_{\text{dir}}(e_0,e_m)+t\cdot\alpha_{\text{rec}}(e_0,e_m,e_{\text{rec}})$$

其中 $r+s+t=1$。α'_{cur} 是新的测量可信度，α_{cur} 是原来 e_0 认为完整性测量实体 e_m 完整性测量能力的可信度；α_{dir} 是 e_0 根据 e_m 正确执行测量的统计得到的直接评价值；α_{rec} 是其它实体对 e_m 测量可信度的推荐值。加权系数 r，s，t 的选择要考虑到每种可信度对新可信度计算的影响程度、推荐实体的推荐能力等因素。如果其中某项可信度为 0，那么其系数也为 0，但仍然满足三个加权系数的和为 1。

如果评价整个信任链 E 的完整性可信度，该信任链可信度由完整性可信度值最小的实体决定。整个信任链的完整性可信度表示为

$$T_{\text{integ}}(e_0,E)=\min\{T_{\text{integ}}(e_0,e_i)\}$$

($\forall e_i,e_i\in E,1\leqslant i\leqslant n,n$ 是信任链上实体的总个数)

3.1.2　真实性可信度的计算

在基于公钥机制的信任模型中，对观察者 e_0 来说，e_1 公钥的真实性主要由 e_1 的证书签发者建立和维护有效证书能力的可信性决定。此外在分层授权委托 CA 的信任模型中，认证路径长度，即委托深度也会影响公钥的可信性。综合分析对证书绑定的公钥可信性的影响因素，得到 e_0 对 e_1 公钥真实性可信度的计算公式如下：

$$T_{\text{auth}}(e_0,e_1)=\begin{cases}\theta & ,e_0 \text{ 是 } e_1 \text{ 的证书签发者}\\ \varphi_{\text{cur}}(e_0,e_{ca})\cdot(1-\mu\psi)^i\cdot\theta & ,e_{ca} \text{是 } e_1 \text{ 的证书签发者}\end{cases}$$

其中 $T_{\text{auth}}(e_0,e_1)$ 是从观察实体 e_0 的角度看来 e_1 的公钥真实

性可信度，为 0 到 1 之间的实数；φ_{cur} 是 e_0 认为 e_1 的证书颁发实体 e_{ca} 建立和维护有效证书能力的可信度，为 0 到 1 之间的实数；ψ 表示一跳认证路径长度所带来的信任损失值，可以在系统初始化的时候设置；μ 是信任损失系数，随着认证路径上 CA 可信度的提高而减小，如果为 0 则表示没有信任损失；i 是证书的认证路径长度；θ 是 e_0 对证书有效性的验证结果，如果证实证书有效，$\theta=1$，否则 $\theta=0$。

CA 建立并维护有效证书能力的可信度在系统初始化的时候可以赋一个 0 到 1 之间的值。在系统运行过程中，根据 CA 成功完成证书中心功能的统计值和来自其它实体对 CA 的推荐信任值，调整 CA 的可信度，调整的方式如下：

$$\varphi'_{cur}(e_0,e_{ca})=r\cdot\varphi_{cur}(e_0,e_{ca})+s\cdot\varphi_{dir}(e_0,e_{ca})+t\cdot\varphi_{rec}(e_0,e_{ca},e_{rec})$$

其中 $r+s+t=1$。φ'_{cur} 是 e_{ca} 新的建立和维护有效证书能力可信度，φ_{cur} 是原来 e_0 认为 e_{ca} 具有的建立和维护有效证书能力的可信度，φ_{dir} 是 e_0 根据 e_{ca} 正确完成证书中心功能的次数得到的统计评价值，φ_{rec} 是实体 e_{rec} 对 e_{ca} 建立和维护有效证书能力可信度的推荐值。加权系数 r，s，t 的选择要考虑到每种可信度对新可信度计算的影响程度、推荐实体的推荐能力等因素。如果其中某项为 0，那么其系数也为 0，但是仍然满足三个加权系数的和为 1。

3.1.3 *模糊集合及其隶属函数*

信任不是绝对的概念。为了更科学地表现信任的特点，本文将可信性分为不同的模糊集合，定义了很可信 A_{high}、比较可信 A_{mid}、比较不可信 B_{mid} 和很不可信 B_{high} 4 个不同信任等级的信任集合。利用计算得到的可信度，通过隶属函数根据最大隶属原则可以判断被测量实体所属的信任集合。这些模糊集合的隶属函数如下列公式所示，其中 t 为实体的可信度：

$$A_{high}(t)=\begin{cases}0, & \text{当 } 0\leqslant t\leqslant 0.5\\ 2(\frac{t-0.5}{0.5})^2, & \text{当 } 0.5\leqslant t\leqslant 0.75\\ 1-2(\frac{t-1}{0.5})^2, & \text{当 } 0.75\leqslant t\leqslant 1\end{cases}$$

$$A_{mid}(t)=\begin{cases}0, & \text{当 } 0\leqslant t\leqslant 0.25\\ 2(\frac{t-0.25}{0.5})^2, & \text{当 } 0.25\leqslant t\leqslant 0.5\\ 1-2(\frac{0.75-t}{0.5})^2, & \text{当 } 0.5\leqslant t\leqslant 0.75\\ 0, & \text{当 } 0.75\leqslant t\leqslant 1\end{cases}$$

$$B_{high}(t)=\begin{cases}1-2(\frac{t}{0.5})^2, & \text{当 } 0\leqslant t\leqslant 0.25\\ 2(\frac{0.5-t}{0.5})^2, & \text{当 } 0.25\leqslant t\leqslant 0.5\\ 0, & \text{当 } 0.5\leqslant t\leqslant 1\end{cases}$$

$$B_{mid}(t)=\begin{cases}0, & \text{当 } 0\leqslant t\leqslant 0.25\\ 1-2(\frac{t-0.25}{0.5})^2, & \text{当 } 0.25\leqslant t\leqslant 0.5\\ 2(\frac{0.75-t}{0.5})^2, & \text{当 } 0.5\leqslant t\leqslant 0.75\\ 0, & \text{当 } 0.75\leqslant t\leqslant 1\end{cases}$$

这些模糊集合的隶属函数曲线如图 2 所示，横坐标是根据可信度计算公式得到的实体可信度，纵坐标是根据隶属函数计算得到的隶属度。

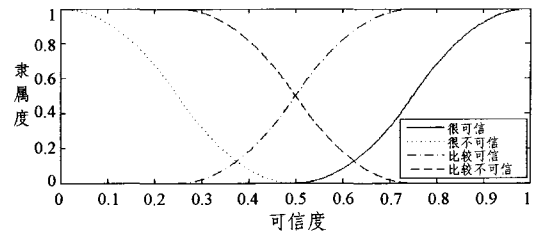

图 2 模糊集合的隶属曲线

4 可信计算安全引导过程的可信性评估

可信计算平台由安全引导保障，可信计算的安全引导过程如图 3 所示。信任根由 CRTM 和完整性报告可信根 TPM 组成。从信任根开始，沿信任链逐级对部件的完整性值进行测量，将信任域从信任根开始扩展到整个平台，完成对平台可信性的度量。

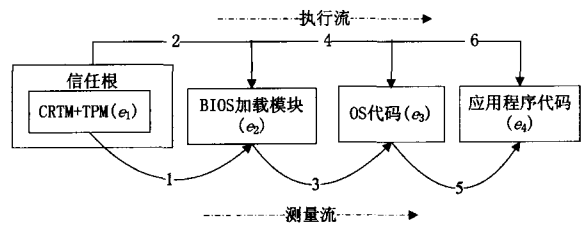

图 3 可信计算平台安全引导

下面举例对图 3 中经过安全引导后的可信计算平台完整性可信度进行分析。首先利用式(1)计算信任链上每个实体的完整性可信度。这里只讨论静态测量的情况，不考虑测量能力和损失系数在动态运行过程中的调整。按照信任链上实体的类型，分别赋予不同的初始可信测量能力值，并且假设完整性测量值等于预期的完整性值，即 $\gamma=1$。每级委托测量带来的信任损失值 β 为 0.1，损失系数 μ 为 1。信任链上每个实体的完整性可信度的值如表 1 所示。表中 $\alpha_{cur}(e_0,e_i)$ 表示测量执行实体测量能力的可信度；$T_{integ}(e_0,e_i)$ 表示实体对应的完整性可信度。

表 1 信任链上实体完整性可信度

测量执行实体	e_0	e_1	e_2	e_3
$\alpha_{cur}(e_0,e_i)$	1	0.95	0.9	0.9
被测量实体	e_1	e_2	e_3	e_4
委托链长度 i	0	1	2	3
$T_{integ}(e_0,e_i)$	1	0.855	0.729	0.6561

平台的完整性可信度由信任链上完整性可信度值最小的实体决定，即平台的可信度等于被测量实体 e_4 的可信度 0.6561。根据上面定义的隶属函数，可以计算得到平台可信度对应不同集合的隶属度，计算结果如表 2 所示。该平台属于集合 A_{mid} 的隶属度为 0.965，根据最大隶属原则，平台属于集合比较可信，因此从 e_0 的角度看来平台是比较可信的。

表 2 可信计算平台的隶属度

模糊集	A_{high}	A_{mid}	B_{mid}	B_{high}
隶属度	0.195	0.965	0.071	0

从表 1 中可以看出信任损失主要受委托测量和测量执行者的测量能力可信度影响，这为我们提出可信计算平台的改

（下转第 97 页）

VITE 请求或者 BYE 请求中进行发送。由于 CSeq 字段在一次会话的不同 SIP 事务中不会重复出现，因此这一密文即使被截获，也不能被攻击者重复使用。被叫方用公钥解密这一密文后进行检查，如果符合最近一个 CSeq 值，则认为是合法的 re-INVITE 或 BYE 请求，否则丢弃。图 5 显示了这一过程。应用这一认证机制后，攻击者发出的伪造 BYE 请求无法通过认证，拆卸会话攻击失败，而用户发出的含有正确加密信息的 BYE 请求则合法地结束了会话。

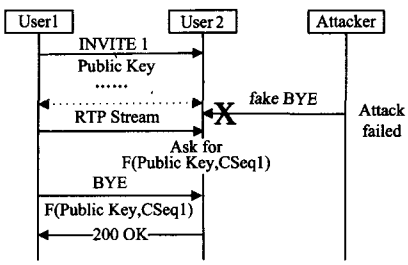

图 5　端到端认证机制

在图 5 的场景中，User 1 发出的 INVITE 请求包含有公钥信息 E 和 N，报文内容如图 6 所示。

```
INVITE sip:0109@10.6.2.162:5060 SIP/2.0
From:sip:0116@10.6.12.98:5061;tag=1205
Call-ID:6335122000@10.6.12.98
CSeq:2666 INVITE
Authentication-Info:E="162D",N="8F932EF1"
.....
```

图 6　INVITE 报文内容

User 1 最终发出的 BYE 请求包含用私钥加密上述 CSeq 字段 2666 生成的密文，因而可以通过认证并正常结束会话，报文内容如图 7 所示。

```
BYE sip:0109@10.6.2.162:5060 SIP/2.0
From:sip:0116@10.6.12.98:5061;tag=9962
Call-ID:6335481563@10.6.12.98
CSeq:10 BYE
Authorization:C="534DA5C7"
```

图 7　BYE 报文内容

通过上述被叫方对主叫方的认证，有效阻止了攻击者在两个用户正常通话过程中冒充主叫方发送 re-INVITE 和 BYE 请求。同理，被叫用户可以在首个对主叫用户的响应信息中加入自己的公钥，采取与上面相同的方法，主叫方就可以对被叫方的 BYE 请求进行认证。这样就实现了主叫和被叫的双向端到端认证，阻止了消息篡改和拆卸会话攻击。

结束语　本文针对 SIP 协议存在的安全问题，在原有的 HTTP 摘要认证机制的基础上进行了扩展。针对 SIP 会话的特点，引入简单可行的公钥分发方式，以较小的代价加强了域内认证，并实现了原有机制所不能提供的端到端认证，增强了 SIP 的安全性。在未来的工作中，我们将进一步研究用户对服务器的认证机制和更高效可行的公钥分发机制。

参 考 文 献

[1] Rosenberg J, Schulzrinne H, Camarillo G. SIP: Session Initiation Protocol. RFC 3261, 2002

[2] Hong Y, Hui Z, Sripanidkulchal K, et al. Information leak vulnerabilities in SIP implementations. IEEE Networks, 2006, 20(5): 6-13

[3] 俞志春，方滨兴，张兆心. SIP 协议的安全性研究. 计算机应用，2006，26(9)：2124-2126

[4] Samer S, Pascal U. SIP Security Attacks and Solutions: A State-of-the-Art Review// Proc. of IEEE International Conference on Information and Communication Technologies. 2006, 2: 3187-3191

[5] 王宇飞，范明钰，王光卫. 一种基于 HTTP 摘要认证的 SIP 安全机制. 重庆邮电学院学报：自然科学版，2005，12(17)：749-751

[6] Schmidt H, Chi-Tai D, Hauck F J. Proxy-based Security for the Session Initiation Protocol (SIP)// Proc. of the Second International Conference on Systems and Networks Communications. 2007: 24-28

[7] Stefano S, Luca V, Donald P, et al. SIP security issues: the SIP authentication procedure and its processing load. IEEE Network, 2002, 16(6): 38-44

[8] 李荣森，秦杰，窦文华. RSA 系列算法在工程中的应用研究. 计算机科学，2007，34(2)：86-90

(上接第 41 页)

进方案提供了很有价值的参考。

结束语　本文在深入分析可信计算信任模型可信性影响因素的基础上，提出了针对可信计算应用环境的可信性评估方法。分析结果表明，利用所提出的方法较好地实现了对可信计算信任模型的评估。基于评估过程，能够发现影响信任模型可信度的因素，为信任模型的改进和完善提供参考。下一步的工作是为新一代移动网络设计可信接入模型，并且对模型进行评估分析，根据分析结果完善可信接入方案。

参 考 文 献

[1] TCG. TPM Work Group[EB/OL]. https://www.trustedcomputinggroup.org/groups/tpm/, 2007-10

[2] Microsoft. Next-Generation Secure Computing Base home page [EB/OL]. http://www.microsoft.com/resources/ngscb, 007-01

[3] Intel. LaGrande Technology Architectural Overview [EB/OL]. http://www.intel.com/technology/security/downloads/LT_Arch_Overview.pdf, 2007-01

[4] Alan Z. Coming soon to VMware, Microsoft, and Xen: AMD Virtualization Technology Solves Virtualization Challenges [EB/OL]. http://www.devx.com/amd/Article/30186, 2007-01

[5] 郑宇，何大可，何明星. 基于可信计算的移动终端用户认证方案. 计算机学报，2006，29(8)：1255-1264

[6] 余发江，张焕国. 可信安全计算平台的一种实现. 武汉大学学报，2004，50(1)：69-75

[7] JØsang A. A Subjective Metric of Authentication// Proceedings of the European Symposium on Research in Security (ESORICS'98). Louvain-la-Neuve, Belgium, 1998: 329-344

[8] 李小勇，桂小林. 大规模分布式环境下动态信任模型研究. 软件学报，2007，18(6)：1510-1521

[9] Patel J, Teacy W T, Luke, et al. A Probabilistic Trust Model for Handling Inaccurate Reputation Sources// Proceedings of Trust Management Third International Conference (iTrust 2005). INRIA-Rocquencourt, France, 2005: 193-209

[10] TCG. TCPA Main Specification version 1.1b[EB/OL]. https://www.trustedcomputinggroup.org/specs/TPM/TCPA_Main_TCG_Architecture_v1_1b.pdf, 2007-10