文章编号:1001 - 9081(2007)08 - 1919 - 03

一种改进的公钥证书抗攻击信任度模型

李 想[1],王 宇[1],张建伟[2]
(1. 装备指挥技术学院 研究生院, 北京 101416; 2. 装备指挥技术学院 信息装备系, 北京 101416)
(mumubb@sohu.com)

摘 要:由信任的相关概念及信任特性入手,阐述了信任度提出的原因,介绍了几种信任度模型,分析了各模型的特点和共性。重点对 Levien 信任度模型进行了研究,分析了其存在的缺陷,并从攻击者角度提出一种改进的节点信任度模型。新模型基于 Levien 信任度模型结构特点,根据计算攻击者的攻击能力参数,引入信任传递衰减因数,综合度量每一节点的信任度,分析得出提高信任度的途径。

关键词:公钥基础设施;信任;信任度;信任度模型
中图分类号: TP393.08 **文献标志码**:A

Improved attack-resist trust metric model for public key certification

LI Xiang[1], WANG Yu[1], ZHANG Jian-wei[2]
(1. *Graduate School, Academy of Equipment Command and Technology, Beijing* 101416, *China*;
2. *Department of Information and Equipment, Academy of Equipment Command and Technology, Beijing* 101416, *China*)

Abstract: From the concept of trust and confidence related characteristics, the reason of raising the trust metric was introduced. Several trust metric models were recommended, and their characteristics and commonness were analyzed. The study focused on the Levien trust metric model and its shortcomings, and a modified node trust metric model was proposed from the perspective of the attacker. The new model, based on the structure of Levin's model, is used for computing attackers' capacities for a successful attack. It imports a descending factor of trust transmission to measure the trust metric of each node synthetically, and gives a better way to improve trust metrics through analysis.

Key words: Public Key Infrastructure (PKI); trust; trust metrics; trust metric model

0 引言

信任及信任的传递是实现网络系统中实体身份鉴别的基础,也是验证与保护信息完整性,实现访问控制的前提。基于公钥的公钥基础设施(Public Key Infrastructure, PKI)是维护信息网络信任关系的有效方案之一。理论上 PKI 的几种信任模型都是通过证书的"个体—公钥属性"的绑定来建立信任,并构造证书路径实现信任的拓展,但现实中可能还存在很多不确定因素,例如拥有者误操作或有意与假密钥绑定等,这就使得信任网络中的实体难于控制,由此引出信任度的概念。国外很多学者提出了各种信任度的机制[1-6],在一定程度上缓解了 PKI 的信任危机,但这些机制由于各自信任模型结构、推理规则等方面的限制,在信任的表述和度量、信任的推导和综合计算等方面存在差异。

本文要讨论的信任度模型的相关问题如下:

1)已有的信任度模型通常从防御者的角度采用惩罚机制(例如降低实体推荐能力)事后处理攻击事件,所采用的推荐信任合成算法并不能有效地抵制攻击带来的影响;

2)从攻击者角度提出的信任度模型能否优化 PKI 抗攻击的信任度;

3)信任链中访问路径的长度对节点间的信任度有何影响。

1 信任度

1.1 相关概念

PKI 用公钥概念和技术实施并提供安全服务的具有普适性的安全基础设施。

信任 在 PKI 中,可以信任的定义具体化为:如果一个用户认证中心 CA 可以把任一个公钥绑定到某个实体上,则称该实体信任该 CA。

信任模型 是指建立信任关系和验证证书时寻找和遍历信任路径的模型[7]。

信任特性 信任一般分为主观信任和客观信任两种[8]。信任的基本属性包括主观性、内容相关性、可能性预期和传递衰减性[9]。信任的特性可具体化为[1]:

1)信任多样性:信任的多种属性可以用多元表示,例如:信任源、信任目的、信任目标、关联到每个信任关系的度量、时间组件等。

2)信任传递性:假定一个信任传递链,节点出入度均为 1。从主观来看,信任会随着链的加长(信任的传递)而衰减。

3)信任结合性:在并行结构的信任网中,一个信任多个(或直接信任,或信任其推荐)。在考虑拓扑图时,当拓扑图很大,或者部分图未知时,肯定信任的并行结合性具有增强推导信任的效果。例如:源节点若信任多个节点的推荐,就可能存在多条独立节点不相交的信任路径,用以推导出信任目标,即使有一条路径被攻击而不能通行,也还有其他几条可用路径继续服务,因此增强了源节点对目标节点的相信程度。

1.2 信任度概念的提出

由于密码系统中每个用户都拥有信任密钥,运用密码学可以保证认证和推荐的完整性与真实性,因此在设计中,还需要假设用户拥有用于加密和认证的公私密钥对,在所交互的推荐者的完整性与真实性得到认证之后,再用信任拓扑图进

收稿日期:2007 - 03 - 05。

作者简介:李想(1983 -),女,北京人,硕士研究生,主要研究方向:管理信息系统; 王宇(1971 -),男,云南人,副教授,主要研究方向:信息安全; 张建伟(1957 -),男,山东人,教授,主要研究方向:管理信息系统。

行拓扑分析。但信任网络中的实体难于控制,信任不确定,因此还需要考虑认证机构本身的信任度。

信任度是指对节点集合中的某一节点能完成其被期待完成任务的信任程度。目前很多信任的度量都是从防御者的角度直接度量两实体间的信任[1],这种被动估测的方法大都通过经验获得信任度,获得的信任度并不能及时有效地反映出实体抵御攻击能力,特别是在一个结构复杂且动态变化的信任网络中,由于信任关系的错综复杂,更难获得准确的信任度。

2 几种信任度模型及其局限性

建立良好的信任度模型对于度量信任十分重要。国外许多学者基于 PKI 体系的信任模型,根据现实中人们建立信任的特点,提出一些信任度的机制,以此来增强实体间建立信任的安全性,缓解 PKI 中的信任危机。下面介绍几种具有代表性的信任度模型,并从信任的表述和度量、信任的推导和综合计算等方面简要分析各种算法的差异。

1) Beth-Borcherding-Klein 模型[3]

Beth 等人率先进行了基于信任的逻辑推理,对其量化得出了一种估算信任度的方案,并得出了在多个认证服务中心之间信任关系的传递以及推理规则,也称为 BBK 方案。BBK 模型就是典型的主观信任模型。该模型用一个值来表示信任值,把信任关系分为直接信任和间接信任两种,根据实体之间交互成功和失败的次数得出信任值,采用简单的算术平均对推荐信任值进行合成。由于该方案用节点表示实体,使得证书确切来源很难确定,具有其局限性。

2) Maurer 模型[4]

Maurer 从用户角度建立模型,引入推荐机制,得出了估算实体公钥真实性和实体可信性的确定性和概率性方案,但考虑认证实体间有多条平行认证路径时,其效率会变得很低。此方案中由于既考虑了实体证书公钥的真实性,又考虑了实体的可信性,其重点是追求信任模型中建立信任的精确性,因此推理规则比较烦琐,效率很低,操作性差。此外,Maurer 模型也是用节点表示实体,虽然声明了密钥签发证书,但没有完全弥补 Beth 信任模型的缺陷,并且 Maurer 模型中术语不统一,以至于用户必须从其他用该公钥进行验证的签名证书中推断出该证书的签发者。

3) Reiter & Stubblebine 模型[5]

Reiter 和 Stubblebine 提出了 PGP(Pretty Good Privacy)中信任度的推理计算方法,在该模型中用节点代表公钥(真实密钥,不涉及到任何实体),从而保证了实体间的认证性和完整性。又通过引入两种度量,计算出一个使不相交节点路径存在的最大节点个数集合,即节点的割集。若去掉这个割集,源节点就不能到达目标节点。这种方法适用于多条并行认证路径的信任模型。

4) Zimmermann 模型[6]

Zimmermann 的这一度量是用于 PGP 的,Zimmermann 的图与 Reiter&Stubblebine 的很相似,用节点代表公钥,不同的是用户为每个节点赋予了四个不同的信任值,即不清楚、不信任、部分信任、完全信任,用这些离散数值来评估公钥的真实性。

5) Jøsang 模型[1,9]

Jøsang 模型也是一种主观信任模型,该模型并没有像 Zimmermann 模型那样按照离散的方法限定和表示信任来计算公钥的真实性,也不是一次性地得出是完全还是部分接受公钥,而是在某一特定环境下确定使用公钥的权限值,但这种信任合成算法无法对不确定值为 0 的信任值进行合成。

6) Levien 模型[2]

Levien 基于 PGP 模型,提出一个分析结构来理解抗攻击的信任度量的有效性。受到 Reiter&Stubblebine 用计算割集度量源节点到目标节点不相交节点访问路径存在理论的启发,将度量信任的关键锁定到计算攻击多少个公钥可以使认证系统中的源公钥接受伪造目标。Levien 通过计算得出了一个使攻击成功的最小证书数。提出了一种基于最大网络流的最佳信任度模型。Levien 模型的缺点主要有:1)由于模型过于简单,没有考虑诸如证书的有效周期和撤销等时间依赖性行为;2)该模型假设大多数公钥节点为真,致使在计算信任度时可以忽略路径长度的影响,但在现实公钥认证系统中,信任度会随着信任链长度的递增而下降。

以上各种模型中对信任的度量都是从防御者的角度考虑的,有其局限性。本文从攻击者的角度度量信任的方法,是对以往信任度量的一种改进,更适用于公钥证书系统网络结构中的节点信任度量。

3 改进的信任度模型

针对 Levien 模型存在的缺陷,在引用 Levien 模型中信任的度量规则、直接信任和推荐信任的含义及其推理规则的条件下,可以对攻击节点信任度数值的计算方法进行改进,建立新的公钥证书抗攻击信任度模型。

3.1 AC 模型的建立

PKI 关于信任模型中包括:一种附加配置代理 CA 的模型,如图 1 所示;一种等级命名空间且带有目录结构的 Up-Cross-Down 的模型结构[10],如图 2 所示。

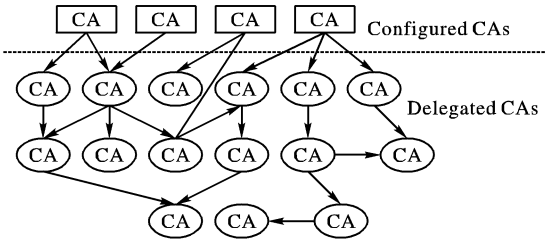

图 1 附加配置代理 CA 模型

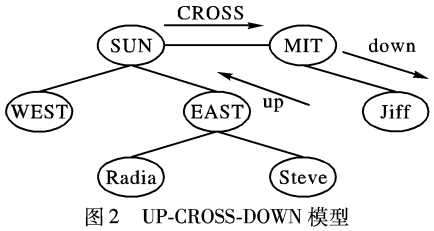

图 2 UP-CROSS-DOWN 模型

结合附加代理 CA 和 Up-Cross-Down 模型的代理认证和交叉认证的特点,可以构造一种以证书公钥代表节点、以绑定信任和代理信任代表节点间信任关系的信任度模型,可以称该模型为攻击能力(Attack Capacity, AC)模型,该模型假设条件如下:

1)假设绝大多数的名字/公钥绑定都可被完全接受;

2)假设命名空间隐藏,即不能从姓名中获得任何相关信息实现窃密。

AC 模型与 Levien 模型相似,将对证书系统攻击的类型分为节点攻击和边攻击。节点攻击是指攻击者直接窃取私钥相关资料进行攻击,例如:口令窃取。边攻击是指用欺骗的手段使某个公钥拥有者接受另一公钥拥有者颁发的假证书,即攻击者对认证证书的伪造。但 AC 模型在结构上更突出信任度模型是基于 PKI 信任模型构建的思想,并且与 X.509 在命名空间隐藏和交叉认证上也有相似之处,如图 3 所示。

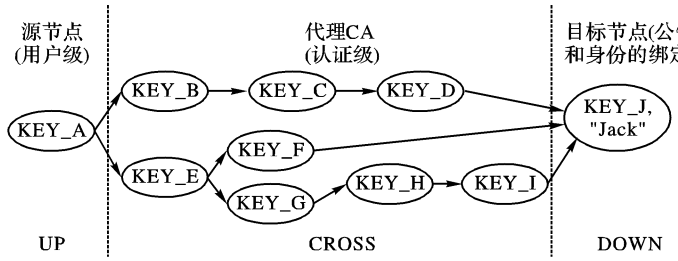

图 3　AC 模型

以节点攻击为例,图 3 表示一个电子签名过的证书集合,实际中用户是不能推断公钥和公钥拥有者绑定的,特别是当一个模型中具有代理 CA 时,只有公钥对应的 CA 才签发证书,所以模型中各节点代表公钥或公钥与身份的绑定。如图 3 中节点{Key_A, Key_B,…,Key_I}表示证书公钥,节点{Key_J, Jack}表示公钥与用户身份的绑定。用户级的源节点的定义是相对的,除了目标节点,图 3 中的任何节点都可能成为源节点,用户信任的各个公钥节点代表各个代理 CA 的公钥。模型中节点之间的边代表两种信任:一种是绑定信任,如图 3 中 Key_D→Key_J,"Jack",它代表 Key_D 相信 Key_J 是用户 Jack 的公钥;另一种是委托信任(delegation trust),如图 3 中 Key_B→Key_C,它代表 Key_B 信任由公钥 Key_C 对应私钥签发的证书。明显地,源节点 Key_A 到目标节点{Key_J,"Jack"}的多条访问路径都是由这两种信任边构成的。

边攻击的信任度量思想与节点攻击相似,这里不再赘述。

3.2　AC 模型信任度量及结论

按照 Levien 模型中给出的节点攻击信任度的计算方法,AC 模型从两个方面定义信任度计算公式:

1)完全从攻击者的角度定义一个度量信任度的参数,能力 $C_{(s,t)}(n)$,用它表示节点 n 被成功攻击的可能性概率,也可以理解为攻击者攻击的能力。

2)假设信任关系可以传递,信任度随信息链长度的增加而递减,并设递减的比率为 $\lambda(0 \leqslant \lambda \leqslant 1)$。

基于以上两种考虑,借鉴节点攻击信任度的公式,给出如下公式:

$$C_{(s,t)}(n) = \begin{cases} \max\left(\frac{1}{d}, \frac{1}{|succ(s)|}\right) * \frac{1}{\lambda}, & L = 1 \\ \frac{1}{d} * \left(\frac{1}{\lambda}\right)^{L}, & L \geqslant 2 \end{cases} \quad (1)$$

其中,s 表示源节点,t 表示目标节点,n 表示源节点与目标节点之间的某个节点,L 表示从 s 出发的路径长度,$succ(s)$ 表示源节点 s 的直接后继节点的个数,即源节点的出度,d 表示目标节点入度。在图 3 中:源节点 Key_A 的出度 $succ(s) = 2$,目标节点{Key_J,"Jack"}的入度为 $d = 3$,根据式(1)很容易就得出 Key_B 的能力数值是 0.5,再乘以递减的比率 的倒数计算得出了 AC 模型的节点攻击能力数值,并将这些数值赋给 AC 模型实例图中的各个节点,如图 4 所示。

由式(1)可知,能力值越高,攻击者攻击成功率越大。易得,能力的大小取决于源节点的出度和目标节点的入度,即源节点所信任的节点越多(即出度越多),攻击者成功攻击的几率越小,系统就越难攻击。这一点印证了 Jøsang 的结论[1,9]:并行网络拓扑增强了源点对目标点的信任。反之,出度越少,越易攻击。对于目标节点的入度也可以如上推理。

3.3　分析与比较

下面分别从防御者和攻击者两种角度对能力数值 C 的含义进行具体分析:

1)假设该公钥证书系统未遭受节点攻击之前的图为 G,各公钥节点的能力数值 C 代表了节点在整个公钥证书系统中抵御恶意行为攻击所需的能力,即只有当节点的信任度大于或等于该能力数值时,才能成功抵御攻击。明显地,图中源节点的出度是 2,即从源节点到目标节点的不相交节点访问路径最多有两条。

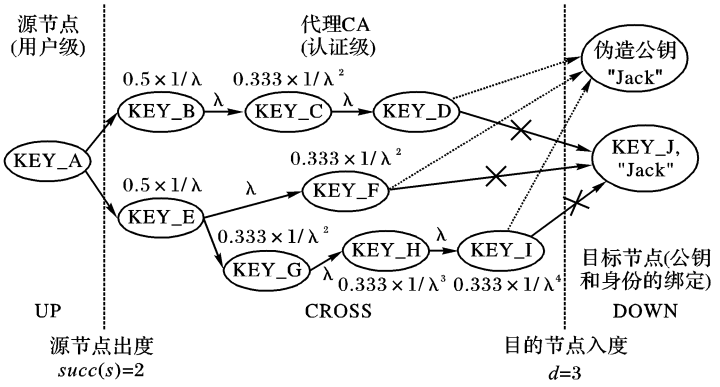

图 4　AC 模型实例

2)假设该公钥证书系统已遭受节点攻击的图为 G',则源节点最终误信任 Jack 与伪造公钥的绑定。由于攻击前的图 G 与攻击后的图 G' 是同构图,所以节点在 G' 中的信任度数值的大小没有变,但含义改变了——求出的信任度参数(能力 capacity),在 G 中表示防御者的防御能力,而在 G' 中表示攻击者的攻击能力。

与 Levien 模型和以往信任度模型相比,AC 模型优势在于:

1)在建模上,从攻击者角度,用能力大小度量攻击者攻击节点的能力,从而得出节点的可信度。

2)在计算信任度上,考虑链长对计算信任度的影响。节点的信任度会随着信任链长度的递增而下降,甚至当超过某个阈值时,信任度下降为 0。

由此可见,AC 模型更突出了 PKI 信任模型的特点,增加了信任传递衰减因数,定义了简单的信任度量公式,并强调了从节点可信程度度量信任的方法。

4　结语

主要分析了基于公钥证书抗攻击信任度模型的特点,从攻击者的角度提出了一种改进的信任度模型。经分析与比较,这种信任度模型克服了前者未考虑信任随链长递减方面的不足,更适合于度量错综复杂的PKI信任网络中的节点信

(下转第 1925 页)

出鲁棒水印,说明本算法对帧编辑处理也具有鲁棒性且可随机检测。但对 P 帧水印而言,由于需要前后多帧的帧间预测进行编码,在遭到帧编辑攻击后,则可能导致预测残差和预测模式都发生很大变化,因而不可能进行正确的水印提取,水印表现很脆弱。

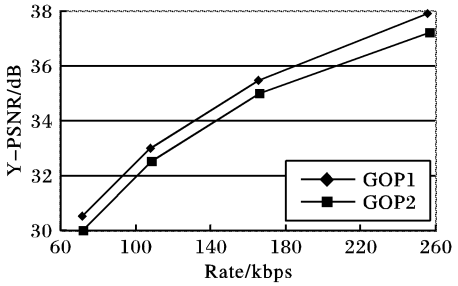

图 4　不同 GOP 结构率失真曲线

4　结语

分别通过在 I 帧 DCT 域量化系数中嵌入鲁棒水印和在 P 帧运动矢量中嵌入脆弱水印,提出了一种针对H.264/AVC低比特视频码流的双水印算法。本算法充分结合 H.264/AVC 编码标准及新特性,在嵌入过程中利用 Lagrangian 最优编码控制技术,达到了较好的率失真平衡。所嵌入的 I 帧水印对重量化编码、帧编辑、滤波及加噪等具有一定的鲁棒性,所嵌入 P 帧水印对各种基本攻击都有较强的脆弱性,可同时实现对数字视频进行版权保护和完整性认证。本算法复杂度低,计算简单,可满足实时随机盲检测的需求,具有较好的有效性和实用性。

参考文献:

[1] HARTUNG F, GIROD B. Watermarking of uncompressed and compressed video[J]. Signal Processing, 1998, 66(3):283 - 301.

[2] SIMITOPOULOS D, TSAFTARIS S A, BOULGOURIS N V, *et al.* Compressed-domain video watermarking of MPEG streams[C]// IEEE International Conference on Multimedia and Expo (ICME 2002). Lausanne, Switzerland: IEEE Communications Society, 2002, 1:569 - 572.

[3] BISWAS S, DAS S R, PETRIU E M. An adaptive compressed MPEG-2 video watermarking scheme[J]. IEEE Transactions Instrumentation and Measurement, 2005, 54(5):1853 - 1861.

[4] JORDAN F, KUTTER M, EBRAHIMI T. Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video, ISO/IEC/JTC1/SC29/WG11/MPEG97/M2281[R]. 1997.

[5] SONG J, LIU K J R. A data embedding scheme for H.263 compatible video coding[C]// Proceedings of IEEE International Symposium Circuits and Systems. Spain: IEEE Computer Society, 1999, 4: 390 - 293.

[6] ALATTAR A M, LIN E T, CELIK M U. Digital watermarking of low bit-rate advanced simple profile MPEG-4 compressed video[J]. IEEE Transactions Circuits Systems Video Technology, 2003, 13(8): 787 - 800.

[7] ZHANG J, HO A T S. Robust digital image-in-video watermarking for the emerging H.264/AVC standard[C]// IEEE 2005 Workshop on Signal Processing Systems (SIPS 2005). [S.l.]: IEEE Press, 2005: 657 - 662.

[8] SAKAZAWA S, TAKISHIMA Y, NAKAJIMA Y. H.264 native video watermarking method[C]// Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS 2006). [S.l.]: IEEE Press, 2006:4.

[9] QIU G, MARZILIANO P, HO A T S, *et al.* A hybrid watermarking scheme for H.264/AVC video[C]// Proceedings of the 17th International Conference on Pattern Recognition. Washington: IEEE Computer Society, 2004, 4: 865 - 869.

[10] WIEGAND T, SULLIVAN G J, BJNTEGAARD G, *et al.* Overview of the H.264/AVC video coding standard[J]. IEEE Transactions Circuits Systems Video Technology, 2003, 13(7):560 - 576.

[11] SULLIVAN G, WIEGAND T. Video compression from concepts to the H.264/AVC standard[J]. Proceedings of the IEEE, 2005, 93(1):18 - 31.

[12] MARPE D, SCHWARZ H, WIEGAND T. Context-based adaptive binary arithmetic coding in the H.264/AVC video compression standard[J]. IEEE Transactions Circuits Systems Video Technology, 2003, 13(7):620 - 636.

[13] JOCH A, KOSSENTINI F, SCHWARZ H, *et al.* Performance comparison of video coding standards using Lagrangian coder control [C]// IEEE International Conference on Image Processing (ICIP'02). [S.l]: IEEE Press, 2002, 2: II-501 - II-504.

[14] WIEGAND T, SCHWARZ H, JOCH A, *et al.* Rate-constrained coder control and comparison of video coding standards[J]. IEEE Transactions on Circuits and Systems, 2003, 13(7):688 - 703.

(上接第 1921 页)

任。本信任度模型仍有待完善,将时间的因素考虑到信任度模型中是今后研究的重点和难点。

参考文献:

[1] JØSANG A, GRAY E, KINATEDER M. Analysing topologies of transitive trust[C/OL]// Proceedings of the Workshop of Formal Aspects of Security and Trust (FAST), 2003 [2007 - 01 - 01]. http://citeseer.ist.psu.edu/cache/papers/cs/32947/http:zSzzSzwww.informatik.uni-stuttgart.dezSzipvrzSzvszSzdezSzpeoplezSzkinatemlzSzpaperszSzJosangGrayKinateder_FAST2003.pdf/jsang03analysing.pdf.

[2] LEVIEN R, AIKEN A. Attack-resistant trust metrics for public key certification[C/OL]// 7th USENIX Security, Symposium, January 26 - 29, 1998, San Antonio, Texas. (2002 - 04 - 12)[2007 - 01 - 05]. http://www.usenix.org/publications/library/proceedings/sec98/full_papers/levien/levien_html/levien.html.

[3] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[C]// Proceedings of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994: 3 - 18.

[4] MAURER U. Modeling a public-key infrastructure[C]// BERTINO E. Proceedings of 1996 European Symposium on Research in Computer Security (ESORICS' 96), LNCS 1146. Berlin: Springer-Verlag, 1996: 325 - 350.

[5] REITER M K, STUBBLEBINE S G. Toward acceptable metrics of authentication[C]// Proceedings of 1997 IEEE Symposium Security and Privacy. Washington: IEEE Computer Society, 1997: 10 - 20.

[6] ZIMMERMANN P. Pretty good privacy user's guide: volume I and II [Z]. Distributed with PGP software, 1993.

[7] 周建峰, 马玉祥, 欧阳雄. PKI 信任模型研究[J]. 电子科技, 2006(4):75 - 78.

[8] 白保存, 李中学, 陈旺. 一种新的 PKI 信任度模型算法设计[J]. 计算机测量与控制, 2005, 13(8): 843 - 845.

[9] JØSANG A. An algebra for assessing trust in certification chains[C/OL]// Proceedings of the Network and Distributed Systems Security Symposium (NDSS' 99), 1999 [2007 - 01 - 15]. http://sky.fit.qut.edu.au/~josang/papers/Jos1999-NDSS.pdf.

[10] PERLMAN R. An overview of PKI trust model[J]. IEEE Network Novermber, 1991, 3(6): 38 - 43.