一种开放式PKI身份认证模型的研究*

周晓斌 许 勇,张 凌
(华南理工大学 计算机学院,广州 510640)

摘 要:分析了传统PKI(Public Key Infrastructure)身份认证模型存在的问题,基于OCSP(Online Certificate Status Protocol)协议的证书状态验证服务和密钥验证服务相分离,造成了传统PKI身份认证模型的信任度下降,增加了身份认证的风险,跨CA(Certificate Authority)认证复杂度高,CA机构提供的身份认证服务不完整等问题。提出了一种开放式PKI身份认证模型,由CA中心独立完成两个验证服务,将OCSP应答机制改进为提供身份证明文件的方式,可有效解决上述问题。通过云信任评估模型对两种认证模型进行了量化评估,证明了本文提出的开放式身份认证模型可有效提高信任度。对该模型进行了原型实现,重点对性能问题进行了优化,实验测试表明,该模型具有实用价值。

关键词:PKI; OCSP; CA;开放式身份认证
中图分类号:TP39 **文献标志码**:A **文章编号**:1001-2486(2013)01-0169-06

Research on open identity authentication model for PKI

ZHOU Xiaobin, *XU Yong*, *ZHANG Ling*
(School of Computer Science and Engineering, South China University of Technology, Guangzhou 510640, China)

Abstract: Some problems about the traditional identity authentication model for PKI(Public Key Infrastructure) were analyzed. For example, because certificate status verification service and key verification service depend on different service providers who have not enough trust degree in open network environment, the trust degree of the traditional model decreases and its risk increases. Additionally, there are other problems about cross-CAs and incomplete authentication service in the traditional model. Thus a new open identity authentication model was put forward for PKI, which can solve the above problems. In this model, the above two verification services were both provided by CA, and the service result was applied by providing identity certification file instead of OCSP answer. The trust degree of the traditional model and our model by using the cloud trust model presented by other researchers was calculated. The result of the calculating test shows that our model can improve the trust degree obviously. Finally, the prototype system of our model was completed, and especially the performance of the model was optimized. The test shows that the model has good practical value.

Key words: PKI(public eey infrastructure); OCSP(online certificate status protocol); CA(certificate authority); open identity authentication

1 传统PKI身份认证模型存在问题分析

基于第三方数字证书的传统PKI身份认证的模型主要是基于可信第三方认证机构CA中心提供的OCSP协议,对用户的数字证书身份进行真实性和有效性验证。其中第三方CA提供OCSP服务,验证用户数字证书身份的有效性,应用方采用PKI密钥运算,验证用户身份的真实性。

1.1 基本概念

OCSP协议:在线证书状态协议(Online Certificate Status Protocol,OCSP)作为证书废止列表(Certificate Revocation List, CRL)方式证书状态查验的补充,是一种用于OCSP请求者(客户端)和OCSP响应者(服务器)之间相对简单的请求/响应协议。

1.2 传统PKI身份认证流程

基于OCSP协议进行用户身份认证,并不能完整地完成对用户身份确认。在基于OCSP认证协议完成用户身份认证时,必须依赖于应用系统开发一套密钥验证逻辑对用户的身份进行进一步确认。基于OCSP协议进行身份认证的流程如图1所示,主要分为两部分。

(1)应用方通过密钥验证逻辑完成用户身份与证书相关性确认,确认请求者即数字证书持有者;

(2)应用方通过OCSP客户端向服务提供方

* 收稿日期:2012-03-15
基金项目:国家973项目(2009CB320505)
作者简介:周晓斌(1975—),男,湖南衡阳人,高级工程师,博士研究生,E-mail:zxb@gz.gov.cn;
张凌(通信作者),男,教授,博士生导师,E-mail: ling@scut.edu.cn

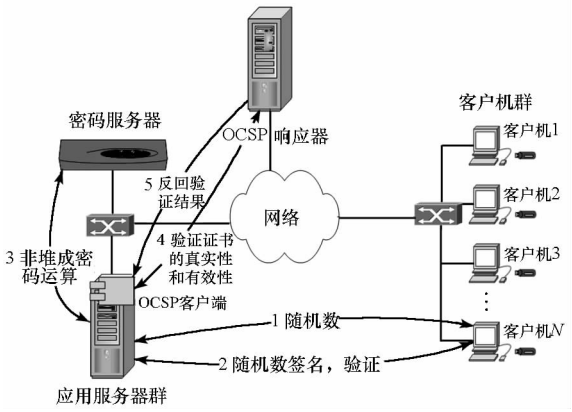

图1 基于 OCSP 协议的身份认证流程图

Fig. 1 OCSP authentication flow diagram

CA 中心发送用户证书验证请求，由 CA 中心的 OCSP 响应器完成数字证书有效性的验证。

(3)应用系统结合 2 次验证结果，确认用户身份是否可信，决定用户是否可以进入应用系统。

1.3 认证模型存在的问题

(1)密钥验证与证书有效性验证的服务提供方是分离的

如图 2 所示，在认证模型中，密钥验证与证书有效性验证分别由两个角色担任，一般为应用系统开发商与 CA 中心，这两个角色担当者之间没有建立互信关系，将导致验证结果的信任度下降。

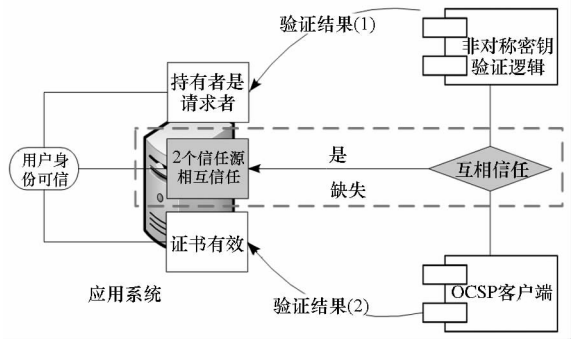

图2 传统 PKI 身份认证的验证示意图

Fig. 2 Traditional authentication diagram

在实际应用中，应用系统的拥有者，其本身不是应用系统的开发者。作为应用服务方而言，密钥验证是一个独立的信任方。实际的信任模型如图 3 所示。

(2)支持多家认证机构可实施性差

虽然可以通过统一的密钥运算接口统一，但 OCSP 只是一个请求/ 响应协议，它并没有明确协议所使用的传输机制，也没有明确 OCSP 系统的结构。因此，建立不同 CA 系统的 OCSP 实现模式是各不相同的，其客户端也是千差万别的。应用系统在面对多个 OCSP 时需要部署不同的 OCSP

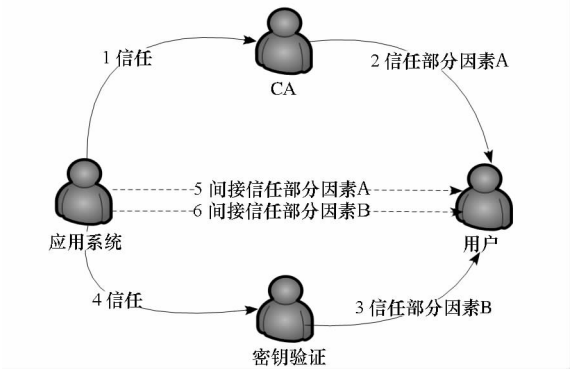

图3 传统 PKI 身份认证信任关系示意图

Fig. 3 Trust relationship of traditional authentication

客户端，实施非常复杂。

(3)没有对用户身份验证结果的证明

用户身份认证的作用是验证用户是否可信用户。作为身份认证服务的提供者需要明确地提供验证结果。

在 OCSP 协议的响应中：1)没有对证书验证结果明确答复(只有证书状态：正常或撤销)；2)没有对用户身份验证结果的描述(缺乏描述用户是否为本人)；3)没有验证结果有效期的描述。

1.4 传统 PKI 身份认证模型的信任度分析

综合各种不同的文献[4-6]，首先给出与信任相关的一些描述性定义。

定义 1 信任度就是信任的定量表示，也可以称为信任程度、信任值、信任级别、可信度等。

定义 2 直接信任度表示在给定的上下文中，一个实体根据直接接触行为的历史记录而得出的对另外一个实体的信任程度。

定义 3 间接信任度表示实体间通过第三者的间接推荐形成的信任度。

定义 4 总体信任度是直接信任度和间接信任度的加权平均。

为了便于分析，本文采用图 4 的身份认证信任模型对传统 PKI 身份认证信任关系(图 3)进行抽象描述，$T_{A,B}$ 代表了 A 对 B 的信任度，其中 A 对 D 的信任度由 2 个间接信任度 $T'_{A,D}$、$T''_{A,D}$ 组成。因此 A 对 D 的信任度由两个信任因素 $T'_{A,D}$、$T''_{A,D}$ 聚合而形成的。

关于信任度的量化计算已有很多学者[7-8]进行了大量的研究，本文采用适应性较好的云信任模型[9]进行评估。云信任模型的主要计算方法如下：

在没有实际交互的情况下，两个实体的信任关系，需要多个实体的推荐来实现。假设有(n + 1)个实体分别为 $E_1, E_2, E_3 \cdots\cdots E_n, E_{n+1}$，这些实体组成一条信任云路径，$E_1$ 对 E_{n+1} 的信任云 tc

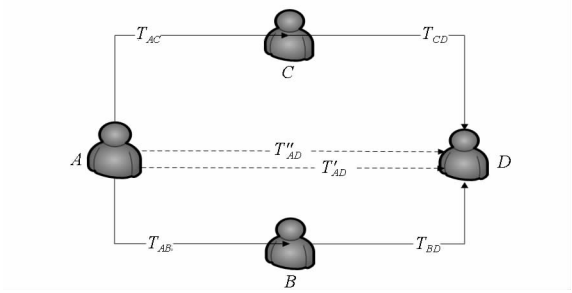

图 4　传统 PKI 身份认证信任模型示意图

Fig. 4　Trust model of traditional authentication

(E_x, E_n, H_e)(E_x 为信任度,E_n 为信任度的熵,描述 E_x 的不确定性;H_e 是信任度的超熵,描述 E_n 的不确定性;若实体间不信任,则 $E_x=0$;若实体间信任值不知道,则 $E_n=1, H_e=1$)为:

$$tc(E_x,E_n,H_e) = tc_1 \otimes tc_2 \otimes tc_3 \cdots\cdots \otimes tc_n$$

$$= \prod_{i=1}^{n} tc_i(E_{x_i},E_{n_i},H_{e_i})$$

$$E_x = \prod_{i=1}^{n} E_{x_i}, E_n = \min\left(\sqrt{\sum_{i=1}^{n} E_{n_i}^2}, 1\right)$$

$$H_e = \min\left(\sum_{i=1}^{n} H_{e_i}, 1\right)$$

在计算信任关系时,如果两个实体之间存在多条信任路径,就需要把不同的信任路径上的信任云合并成一个信任云。实体 E 对实体 E' 的信任 $tc(E_x,E_n,H_e)$ 是合并 n 条不同路径上的信任而获得到的,第 i 条路径上的信任为 $tc_i(E_{x_i},E_{n_i},H_{e_i})$,则信任云 $tc(E_x,E_n,H_e)$ 为:

$$tc(E_x,E_n,H_e) = tc_1 \otimes tc_2 \otimes tc_3 \cdots\cdots \otimes tc_n$$

$$= \sum_{i=1}^{n} tc_i(E_{x_i},E_{n_i},H_{e_i})$$

$$E_x = \sum_{i=1}^{n} E_{x_i}, E_n = \min\left(\frac{1}{n}\sum_{i=1}^{n} E_{n_i}, 1\right)$$

$$H_e = \min\left(\frac{1}{n}\sum_{i=1}^{n} H_{e_i}, 1\right)$$

在传统的 CA 身份认证模型中,各因素的情况如下:

(1)在 CA 认证流程中,CA 中心与密钥验证逻辑的信任度不确定。因此,在云信任模型中 CA 中心与密钥验证逻辑之间的信任云为:

$$tc_{BC}(E_x,E_n,H_e) = tc_3(0,1,1)$$

(2)CA 中心与用户之间没有进行完整的身份认证流程,CA 中心仅通过 OCSP 服务验证了用户证书的有效性,故不能确定用户身份的有效性。因此,在云信任模型中 CA 中心与用户之间的信任云为:

$$tc_{BD}(E_x,E_n,H_e) = tc_4(0,1,1)$$

(3)密钥验证逻辑与用户之间没有进行完整的身份认证流程,通过密钥算法仅验证了用户与密钥的匹配关系。因此,在云信任模型中密钥验证逻辑与用户之间的信任云为:

$$tc_{CD}(E_x,E_n,H_e) = tc_5(0,1,1)$$

A 对 D 的信任关系中存在 4 个实体 A、B、C、D,那么 A,D 的信任推荐关系是 AB,AC,BC,BD,CD 的信任关系形成的信任云。则 A 对 D 的信任云 $tc_{AB}(E_x,E_n,H_e)$ 为:

$$tc_{AD}(E_x,E_n,H_e) = \sum_{i=1}^{5} tc_i(E_{x_i},E_{n_i},H_{e_i})$$

$$tc_{AB}(E_x,E_n,H_e) = tc_1(1,0,0)$$

$$tc_{AC}(E_x,E_n,H_e) = tc_2(1,0,0)$$

$$tc_{BC}(E_x,E_n,H_e) = tc_3(0,1,1)$$

$$tc_{BD}(E_x,E_n,H_e) = tc_4(0,1,1)$$

$$tc_{CD}(E_x,E_n,H_e) = tc_5(0,1,1)$$

$$E_x = \frac{2}{5}, \quad E_n = \frac{3}{5}, \quad H_e = \frac{3}{5}$$

2　基于开放式身份认证模型研究

2.1　CA 机构独立完成身份认证服务

为了解决密钥验证逻辑与 OCSP 响应服务之间的互信问题及 OCSP 服务差异性的问题,需要将密码验证逻辑与 OCSP 响应服务整合成一个标准的身份认证协议,由 CA 中心提供完整的身份认证服务。基于开放式身份认证模型的主要流程如图 5 所示。

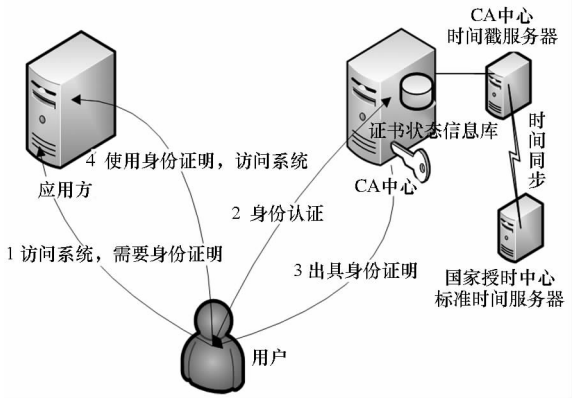

图 5　开放式身份认证的流程示意图(a)

Fig. 5　Open authentication flow diagram(a)

(1)用户访问应用系统,应用系统向 CA 机构发起用户身份验证的请求;

(2)用户端访问 CA 机构的认证界面,进行身份认证;

(3)用户与 CA 通过数字证书的身份认证流程完成用户的身份认证;

(4)CA 完成用户身份认证后,出具用户的身份认证证明附加 CA 机构的数字签名;

(5)用户使用身份证明,访问应用系统。

第(4)步的详细流程如下:

CA 机构对用户的身份认证过程,包括密钥验证和证书有效性状态的验证,CA 机构在与用户完成密钥验证之后,查询本地证书状态信息库确定证书有效性状态,确认状态为有效后,从 CA 中心局域网内的时间戳服务器取得标准时间源,时间戳服务器通过广域网定期与国家授时中心的标准时间源进行时间同步。根据标准时间源提供的时间服务,按照身份证明有效期的策略要求,生成身份证明的有效期,会同其他必要标识信息生成身份证明文件,并用 CA 机构的私钥对身份证明文件进行数字签名,最终的身份证明文件中包含如下相关信息:

(a)身份认证请求者(应用系统)标识;

(b)用户的身份标识;

(c)用户的名称;

(d)身份证明的有效期;

(e)身份证明出具机构标识;

(f)身份证明出具机构名称;

(g)身份证明出具机构数字签名。

2.2 建立开放式认证模型

应用系统通过标准协议,根据不同的 CA 机构的证书用户标识,将用户引导到去各自 CA 机构的认证服务器完成身份认证而并获得认证服务器发布的用户身份证明,用户身份证明采用标准的 XML 信息描述,从而屏蔽了各 CA 机构自身内部的身份认证实现的差异性,可较好地支持跨多 CA 的认证需求。

2.2.1 身份认证请求

应用系统通过约定的协议完成身份认证的请求。请求信息包括,应用系统的标识,身份证明的返回地址以及请求标识。应用系统需要实现或者部署身份认证客户端,以协助应用系统方实现身份认证请求协议。

(1)身份证明返回地址

用来接收身份认证服务的响应信息。

(2)请求标识

用来维护应用系统与身份认证服务之间的请求和响应关系,在接收到用户的身份证明后需要验证是否为合法的请求标识。

2.2.2 身份认证响应

身份认证服务器在接收到申请认证请求后,并完成用户身份认证后,对请求信息进行响应。响应信息包括,用户的身份证明文件,身份证明的类型及应用系统发送的请求标识。

2.2.3 认证客户端

由于整个身份认证过程,应用系统需要和认证服务完成身份认证的请求和响应的接收,因此应用系统需要按照协议实现或部署符合协议的客户端。流程如图 6 所示。

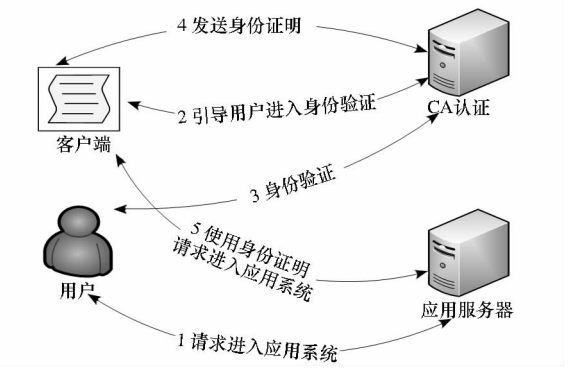

图 6 开放式身份认证的流程示意图(b)

Fig. 6 Open authentication flow diagram(b)

(1)用户访问应用系统,应用系统请求用户身份证明;

(2)客户端引导用户去指定认证方进行身份验证;

(3)用户到 CA 认证中心完成身份验证;

(4)CA 中心验证,出具用户身份证明;

(5)客户端获得 CA 中心签发的身份证明后,协助用户访问应用系统。

客户端在验证身份证明的有效期时,可分为两个等级来验证:通过标准时间源验证有效期;通过本地时间验证有效期。应用系统根据业务对时间的敏感度不同,可选用相应等级的时间源进行验证。

2.3 开放式身份认证模型的信任度分析

在开放式身份认证模型中,应用服务方作为认证请求的发起方,自身不参与身份认证的任何逻辑或者流程,全部由 CA 机构完成用户全部的身份认证流程。因此,信任模型由以前的四方变为现在的三方,其中 CA 机构与应用服方、CA 机构方与用户都已经存在直接的信任关系,如图 7 所示。信任模型的主要原理就是依赖双方都信任的第三方完成信任关系的传递以达到彼此的信任。根据三方的信任关系,其信任模型的示意图如图 8,其中 A 代表应用系统,B 代表 CA 中心,C 代表用户。

假定两方的信任值在 0 到 1 之间。根据三方的信任关系,由于 A 对 B 的信任是基于数字签名的验证判定的,故 A 对 B 的信任度为 1。B 对 C 是通过点对点的数字证书的身份认证,故 B 对 C 的信任值为 1。

仍然采用云信任模型来计算 A 与 C 的信任度。

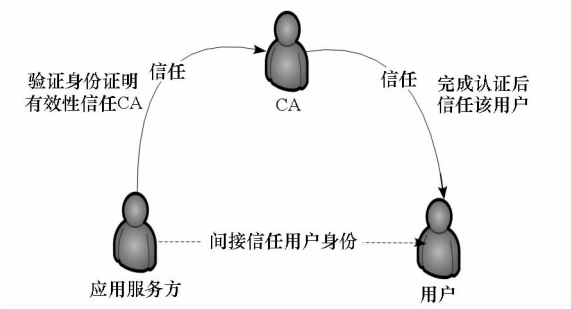

图 7　开放式身份认证模型的信任关系示意图

Fig. 7　Trust relationship of open authentication

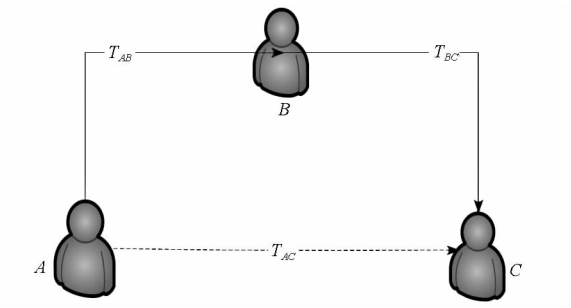

图 8　开放式身份认证模型的信任模型示意图

Fig. 8　Trust model of open authentication

A 对 *C* 的信任关系是建立在 *B* 的推荐之上的。*AC* 的信任度,同样采用云信任计算模型。在模型中一共设计 *A*、*B*、*C* 三个实体。因此 *A*,*C* 的信任推荐关系是 *AB*, *BC* 的信任关系形成的信任云:

$$tc_{AC}(E_x,E_n,H_e)=\sum_{i=1}^{2}tc_i(E_{x_i},E_{n_i},H_{e_i})$$

$$tc_{AB}(E_x,E_n,H_e)=tc_1(1,0,0)$$

$$tc_{BC}(E_x,E_n,H_e)=tc_2(1,0,0)$$

$$E_x=1,E_n=0,H_e=0$$

由上述可以得出,在模型中 tc_{AC} 的信任度为 1 标识 *AC* 之间完全信任。

3　模型实现和性能分析

在开放式认证模型中,由于 CA 中心提供的服务,从简单的 OCSP 查询响应服务,转变为提供完整的身份证明服务,这势必增加 CA 中心的计算量。增加的计算量主要为:集中进行密钥验证运算;生成并签署用户的身份证明文件。

本文主要进行了两个方面的研究来优化 CA 中心的计算工作量和计算能力。

一是减少 OCSP 服务的开销:在开放式身份认证过程中,由于用户身份验证的所有流程都在 CA 中心内部进行,因此证书有效性的验证不需要通过 OCSP 协议进行验证,CA 中心通过本地查询有效期黑名单即可完成证书状态有效性验证,可减少该部分的计算开销。

二是采用分布式计算的架构,实现大请求量的数字签名验证及数字签名运算的并行处理,以提高 CA 中心的计算能力。对于数字签名/验证运算,采用 map/reduce 分布式模式进行,将数字签名的 hash 运算、公钥解密运算、hash 值对比运算、私钥加密运算分解为 4 个不同的工作任务。该架构可以根据各任务的运算量,分布式部署,可通过增加硬件投入来平滑扩张计算能力。

对传统 PKI 认证模型,采用 Loadrunner 测试工具,对 100 用户并发测试传统 PKI 认证方式登录应用系统的压力测试结果:用户全部完成登录的总耗时:30s;证书状态有效性验证平均耗时:0.09s;密钥验证逻辑平均耗时:0.15s;签发身份证明平均耗时:0.06s。

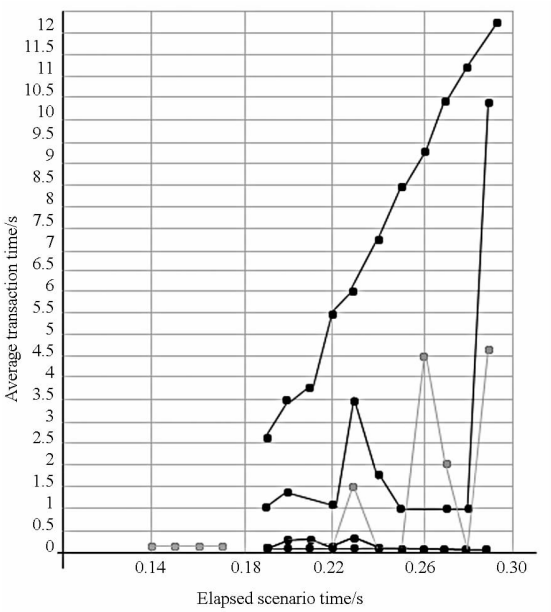

图 9　传统认证测试结果

Fig. 9　Test result of traditional authentication

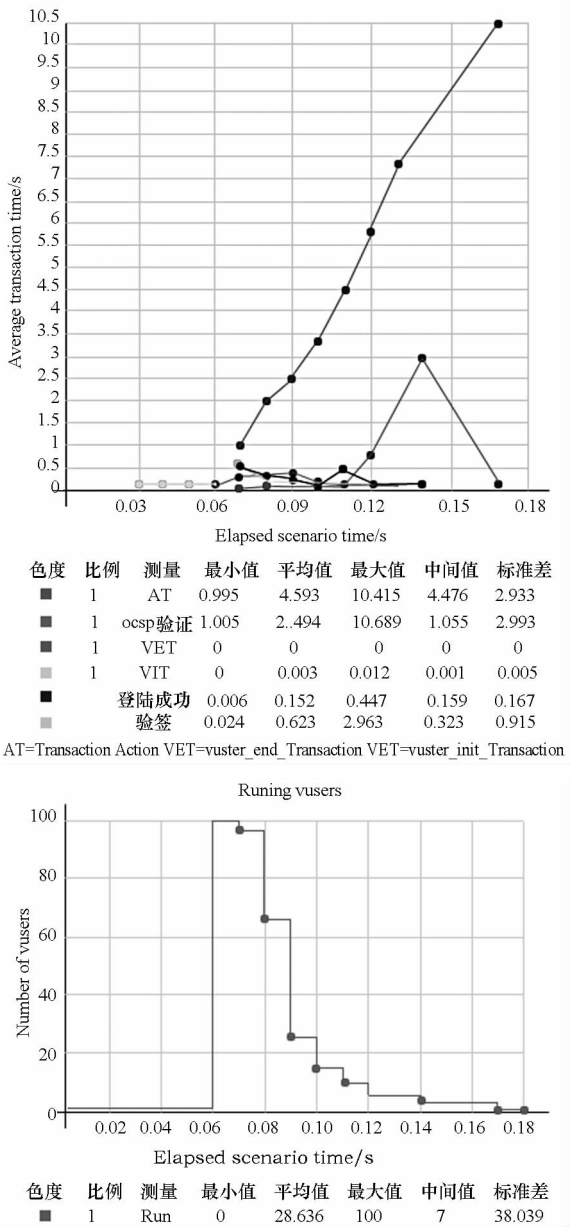

图 10 开放式认证测试结果

Fig. 10 Test result of open authentication

在分别对传统 PKI 认证方式(图 9)和开放式身份认证性能(图 10)进行性能测试后,通过对测试结果的对比,开放式身份认证在单个用户平均总耗时上虽然增加了签发身份证明流程,但是由于减少了 OCSP 的请求验证时间,两种模式认证方式的总体耗时基本一致。由于本文的实验条件投入并行计算的服务器只有两台,通过增加投入,可进一步优化性能。

4 结论

提出的开放式 PKI 身份认证模型具有简单、灵活的优点。应用方可以不再了解 PKI、数字证书的情况下,实现基于数字证书的身份认证。同时,开放式身份认证模型具有良好的信任模型,解决了传统的数字证书认证协议,身份验证流程分散信任模型无法保证的问题。基于该认证模式更加有利于第三方认证、数字证书的应用及推广使用。同时,该模型对于支持跨多 CA 的应用变得非常简单,基于标准的身份证明来实现多 CA 认证服务的统一,而无需关注不同 CA 的 OCSP 实现的差异性问题。身份证明信息中也包含了证明时效性内容,对于身份认证的审计也变得很简单。本文最后对开放式身份认证模型所带来的 CA 中心计算量增加的问题,进行了优化,并通过性能测试,本模型的性能开销与传统模式基本一致,可应用于实际系统。

参考文献(References)

[1] 谢冬青, 冷健. PKI 原理与技术[M]. 北京: 清华大学出版社, 2003.
XIE Dongqing, LENG Jian. Principle and technology of PKI [M]. Beijing: Tsinghua University Press, 2003. (in Chinese)

[2] IETF. X.509 internet public key infrastructure online certificate status protocol OCSP[S]. RFC 2560, 1999.

[3] Adams C, Lloyd S. Understanding pubkic key infrastructure: Concepts, standards and deployment considerations [M]. Macmillan Technical publishing, 1999.

[4] He R, Niu J W, Zhang G W. CBTM: A trust model with uncertainty quantification and reasoning for pervasive computing [M]. Berlin: SpringeR-Verlag, 2005.

[5] Jameel H, Hung L X, Kalim U, et al. A trust model for ubiquitous systems based on vectors of trust values [C]// Proceedings of the 7th IEEE Int Symp. on Multimedia, Washington, IEEE Computer Society Press, 2005:674 - 679.

[6] Theodorakopoulos G, Baras JS. On trust models and trust evaluation metrics for ad - hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):318 - 328.

[7] 李勇军, 代亚非. 对等网络信任机制研究[J]. 计算机学报, 2010, 33(3):1 - 18. (in Chinese)
LI Yongjun, DAI Yafei. Research on trust mechanism for PeeR - to - Peer network[J]. Chinese Journal of Computers, 2010, 33(3):1 - 18. (in Chinese)

[8] 李小勇, 桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报, 2007, 18(6):1510 - 1521. (in Chinese)
LI Xiaoyong, GUI Xiaolin. Research on dynamic trust model for large scale Distri[J]. Journal of Software, 2007, 18(6):1510 - 1521. (in Chinese)

[9] 王新生, 等. 普适环境中基于云理论的信任模型[J]. 计算机工程, 2010, 36(7):282 - 284. (in Chinese)
WANG Xinsheng. Trust todel based on cloud theory in pervasive environment[J]. Computer Engineering, 2010, 36(7):282 - 284. (in Chinese)