文章编号:1001 - 9081(2008)06 - 1382 - 03

一种基于信任度的跨异构域动态认证机制

裴俐春,陈性元,王 婷,张 斌,徐 震
(信息工程大学 电子技术学院, 郑州 450004)
(Heaven623007@163.com)

摘 要:为了适应大规模网络环境下异构域认证机制不一致、域间信任关系动态变化的特点,提出了一种基于信任度的跨异构域的动态认证方法,该方法根据交易双方的满意度打分来计算信任值,动态地建立域间信任关系。应用实例表明,该方法能够有效解决跨域认证中域间信任关系的建立问题。

关键词:信任度;异构域;动态认证
中图分类号: TP393.08;TP309 **文献标志码**:A

Credit-based dynamic authentication mechanism crossing heterogeneous domains

PEI Li-chun, CHEN Xing-yuan, WANG Ting, ZHANG Bin, XU Zhen
(*Institute of Electronic Technology, Information Engineering University, Zhengzhou Henan* 450004, *China*)

Abstract: Since the authentication methods used in domains are always different and the trust relationship changes frequently, a dynamic cross-domain authentication method based on credit was proposed. The value of credit was calculated and the trust relationship was dynamically formed. Based on this relationship, cross-domain authentication could be realized. Analysis of the application instance shows that the proposed method can solve the problem of establishing trust relationship between heterogeneous domains.

Key words: credit; heterogeneous domain; dynamic authentication

0 引言

在大规模分布式网络环境中,异构域采用的认证机制往往不同,域间的信任关系随着交易活动而动态变化,由于跨不同信任域的访问频繁发生,从而如何实现大规模网络环境下跨异构域的动态认证是迫切需要解决的问题。

现有的跨域认证方法有许多。文献[1]提出了一种基于公钥基础设施(Public Key Infrastructure,PKI)的 Kerberos 跨域认证协议,它通过将两个域中的票证发放服务器(Ticket Granting Server, TGS)互相注册为对方域中的用户来实现跨域认证,但前提是任意两个域必须都采用 Kerberos 认证机制,并且通过互相注册是一种静态建立域间信任关系的方法。文献[2]解决了分别使用 PKI 和 Kerberos 作为鉴别机制的异构域之间的身份认证问题,但在大规模异构网络环境中,各信任域的认证机制可能有多种,仅解决几种已有认证机制的异构域间的认证问题不能从根本上实现大规模分布式环境下多异构域的跨域认证。此外,也有些跨域认证方法如文献[3 - 5],它们采用静态建立域间信任关系的方法来解决跨域认证问题,这种静态建立的信任关系不能跟随企业活动的变化而发生改变。由此可见,已有的跨域认证方法或者与域内认证机制相关,或者把域间信任关系静态化,不能很好地适应大规模网络环境的特点。

为了更好地适应大规模分布式环境下异构域认证机制不一致,域间信任关系动态变化的特点,本文提出了一种基于信任度的跨异构域的动态认证方法,该方法引入域间信任度的计算,根据信任域之间信任度的变化来建立信任关系,与域内采取的认证机制无关,实现了跨异构域的动态认证。

1 基于信任度的跨域认证方法

1.1 认证架构

跨域认证问题最重要的就是建立域与域之间的信任关系,本文通过计算域间的信任度来建立与远程域的信任关系。这里的信任度反映的是一个域对另一个域的信任程度。如果域 B 对域 A 的信任度在域 B 可接受的范围内,则域 B 可与域 A 建立信任关系,此时域 B 信任经过域 A 认证的用户身份。这种信任关系是单向的,即域 A 并不一定信任经过域 B 认证的用户身份,要通过计算域 A 对域 B 的信任度从而建立信任关系才能确定。

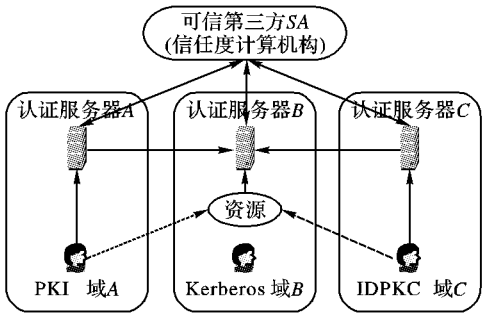

图 1 跨异构域动态认证架构

用户首先要通过本域认证服务器的认证,然后通过和远程域的信任关系来实现用户的跨域认证。信任度由可信第三方 SA(信任度计算机构)负责计算,本文中假设各个域的认证

收稿日期:2007 - 12 - 26;**修回日期**:2008 - 03 - 04。 **基金项目**:国家 863 计划项目(2006AA01Z457)。

作者简介:裴俐春(1981 -),女,山西朔州人,硕士研究生,主要研究方向:跨域认证、跨域授权; 陈性元(1963 -),男,安徽无为人,教授,博士生导师,主要研究方向:网络安全、入侵检测; 王婷(1982 -),女,河南洛阳人,博士研究生,主要研究方向:资源管理、访问控制; 张斌(1969 -),男,河南南阳人,副教授,主要研究方向:网络安全; 徐震(1980 -),男,河南郑州人,讲师,硕士,主要研究方向:网络安全。

服务器都无条件地信任由可信第三方 SA 所计算出的信任度。该跨域认证架构如图 1 所示。

这里域 A 对域 B 的信任度与域 A 对域 B 用户的信任度相关,其中用户的可信程度随着用户的行为而变化,如图 1,用户在跨域访问结束后,远程域会对用户行为做一个评测(即打分),并提交给 SA 来计算其信任度,从而使用户的可信程度根据用户行为的评测来动态调整,如果多次评测均为良好,用户的可信度会上升,反之,用户的可信度下降。用户的可信度直接影响到域间信任度的计算,从而间接影响域间信任关系的建立。这样,基于信任度的动态跨异构域认证能够在一定程度上遏制恶意行为的发生。

1.2　信任值计算

广义上的信任是指 Trustor 在特定上下文中对于 Trustee 的能力、诚实度、安全和可靠性的相信程度的量化表示[6]。在本文中的信任是指某域的认证服务器对另一个域的认证服务器所提供的声称其域内某用户为合法用户的相信程度的量化表示,即某域对另一个域的认证服务器的诚实度、安全性和可靠性的相信程度。如果域 B 对域 A 认证服务器的信任度在域 B 可接受的范围内,则它与域 A 建立暂时的信任关系,并认可经过域 A 认证的用户。

这里域 B 对域 A 的信任程度是动态变化的,它的变化取决于三个方面的因素:域 B 对域 A 的原始信任度、域 B 对域 A 用户的信任度、其他域对域 A 的信任度。在初始状态下,由各域的认证服务器指定对其他域的信任初始值,其中域 B 对域 A 的信任度和对域 A 中任意用户的信任度相同。这个初始值的高低直接影响到将来域 B 对域 A 的信任度的变化,初始值可以根据域 B 了解的域 A 的情况做出主观评估。域 B 对域 A 用户的信任度是对域 A 所有已知用户的信任度的均值,域 B 对域 A 内某用户的信任度即域 B 对该用户在域 B 内访问过程的满意程度,它的变化直接影响到域 B 对域 A 认证服务器的信任程度。其他域对域 A 的信任度反映了其他域对域 A 的诚实度、安全、可靠性的评估水平,如果其他域对域 A 认证服务器的信任度有所变化,那么域 B 对域 A 认证服务器的信任度也会随之变化。如果将某次访问事件发生之前域 B 对域 A 的信任度记为 $C(B\rightarrow A)^{i-1}$,那么通过该次访问过程,域 B 对域 A 的信任度可用式(1)计算:

$$C(B\rightarrow A)^{i}=\frac{\sum_{s=1}^{n}cred(B,u_A^s)^{i}}{n}\times 50\%+\frac{\sum_{j=1且j\neq B,j\neq A}^{m}C(j\rightarrow A)^{i}}{m-2}\times 25\%+C(B\rightarrow A)^{i-1}\times 25\% \tag{1}$$

其中 n 为已知的域 A 用户数,u_A^s 表示 A 域第 s 个用户,$cred(B,u_A^s)^{i}$ 表示 B 域认证服务器对 A 域第 s 个用户的当前信任度,D_j 表示网络环境下第 j 个信任域。上式中第一项即为域 B 认证服务器对域 A 中所有已知用户的当前信任度的均值,为了使信任值能反映用户最近的行为,我们让该项在信任度计算中占有较大比例(50%)。第二项为除域 B 外其他域对域 A 信任度的均值,第三项为域 B 对域 A 在此次交易之前的原始信任值,这两项在信任度计算中各占 25% 的比例。

域 B 对域 A 认证服务器的信任度计算是建立在域 B 对域 A 用户的信任度计算的基础上的。域 B 对域 A 内某用户的信任度取决于该用户在访问域 B 资源时,域 B 对用户身份、行为的满意程度。当域 A 用户完成对域 B 资源的访问后,域 B 会对该次访问过程进行满意度打分,并将该打分提交给 SA,由 SA 根据域 B 提交的打分,结合域 B 对该用户的原始信任度,计算域 B 对域 A 该用户的新信任度。

假设域 A 用户 u_A 第 i 次访问域 B 某资源后,域 B 对该次访问过程的满意度打分记为 $\mathrm{rank}(B,u_A)^{i}$,其中 $-1\leqslant \mathrm{rank}(B,u_A)^{i}\leqslant 1$,负值表示对本次访问过程不满意,反之,正值表示满意。经过该次满意度打分后,域 B 对该用户的信任度记为 $cred(B,u_A)^{i}$,其中 $-1\leqslant cred(B,u_A)^{i}\leqslant 1$,则域 B 在该次访问后对用户 u_A 的新的信任值可用式(2)来计算:

$$cred(B,u_A)^{i}=\mathrm{rank}(B,u_A)^{i}\times 50\%+cred(B,u_A)^{i-1}\times 50\% \tag{2}$$

为了使信任值能反映用户最近的行为,我们让最近一次访问的打分在信任值计算中占有 50% 的比例。

1.3　跨域认证协议

跨域认证是实现跨域访问的前提,当用户有跨域访问需求时,才会产生跨域认证问题。在本文提出的跨域认证方法中,当用户要访问远程域的资源时,首先需要通过本地域认证服务器的认证,认证通过后由本地认证服务器代表用户向远程认证服务器提交远程访问请求,远程认证服务器向第三方查询此刻它对该请求域认证服务器的信任度,如果该值在它可接受的范围内,则与该域建立信任关系,该信任关系意味着它认可该域用户的合法身份,并为用户颁发临时允许访问票据,同意其进入该域进行资源访问,但该用户在域内的访问权限由域内资源的访问规则进一步约束,至此一次成功的跨域认证过程结束。

设域 A 认证服务器的公私钥分别为 K_{PubA}、K_{PrivA}。设经过会话密钥的协商,A、域 B 认证服务器之间的会话密钥为 K_S,可信第三方 SA 与域 B 认证服务器的共享密钥为 K_B'。则域 A 用户 u 跨域访问域 B 资源的认证过程描述如下:

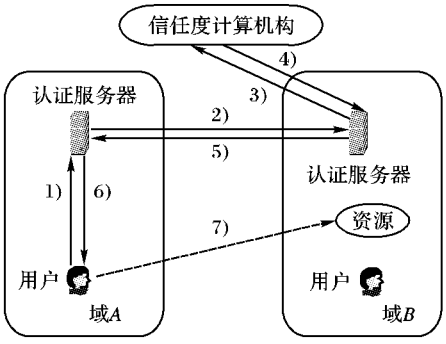

图 2　跨域认证协议

1) 用户 u 向本域认证服务器提交自己的身份凭证,并向其提出访问域 B 资源 R 的请求。

$$U:M=K_{\mathrm{PubA}}(Id(u),B,R,Times)\rightarrow A$$

用户将要访问资源的所在域的标识、资源标识及自己的身份凭证用本域认证服务器的公钥加密发送给域 A 认证服务器,其中 $Times$ 表示用户提出访问请求的时间。

2) 域 A 认证服务器收到用户 u 的请求后,验证 $Id(u)$ 的有效性,验证通过后,向域 B 认证服务器发送用户 u 的访问请求。

$$A:M=K_S(K_{\mathrm{PrivA}}(Id(u),R,Times,Ts(1),Nonce(1)))\rightarrow B$$

域 B 认证服务器将用户的身份凭证、要访问的资源标识

R、用户发出请求的时间($Times$)、随机数($Nonce(1)$)及时间戳($Ts(1)$)用自己的私钥签名再用 K_S 加密发送给域 B 认证服务器,认证服务器通过检查时间戳来防止重发攻击。

3)域B认证服务器向可信第三方请求当前状态下域B对域 A 的信任度,同时产生随机数 $Nonce(1)$,并用自己的私钥签名再用共享密钥 K_B' 加密发送给 SA。

$$B:M = K_B'(K_{PrivB}(B,A),Nonce(2)) \rightarrow SA$$

4) 可信第三方 SA 返回域 B 对域 A 的信任值到域 B 认证服务器。

$$SA:M = K_B'(K_{PrivSA}(C(B \rightarrow A)^i),Nonce(2)) \rightarrow B$$

可信第三方用自己的私钥对信任度签名再用共享密钥 K_B' 加密后发送给域 B。域 B 认证服务器中记录了自己可以接受的对外域认证服务器的信任值范围,它用共享密钥及可信第三方的公钥解密收到的消息,验证随机数的正确性,以保证是自己先前发送请求对应得回复,验证通过后判断信任度是否在自己所接受的范围内,如果在,则与域 A 建立暂时的信任关系,否则拒绝。

5)域B认证服务器根据自己可接受的信任值范围向A返回允许/拒绝票据。

向 A 返回允许访问票据:

$$B:M = K_S(K_{PrivB}(Id(u),A,R,TS(2),Times,VaildTimes,Nonce(1))) \rightarrow A$$

向 A 返回拒绝访问票据:

$$B:M' = K_S(K_{PrivB}(Id(u),Nonce(1))) \rightarrow A$$

域B认证服务器在与域A建立了信任关系之后,为域A返回允许/拒绝用户 u 访问的票据,其中允许票据中包含了用户 u 的身份凭证($Id(u)$)、用户所属的域标识 A、用户要访问的资源标识 R,时间戳($Ts(2)$)、用户提交访问请求的时间($Times$)、随机数($Nonce(1)$)、票据的有效期($VaildTimes$)等信息。该信息用域 B 认证服务器的私钥签名成为允许票据,用会话密钥 K_S 加密发送给域 A 认证服务器。

6)域 A 认证服务器收到域 B 认证服务器返回的消息后,验证票据中请求时间($Times$)和随机数($Nonce(1)$)的有效性,验证通过后将票据回复给用户 u。

7)用户收到回复后,持允许访问票据访问域 B 资源 R。

由于域与域之间的信任关系会动态变化,因此允许票据的有效期一般较短。允许票据表明票据的拥有者通过票据颁发者的认证,可以对该域进行资源访问,但仍受到该域访问控制策略的进一步约束。

2 应用实例分析

设某分布式环境下有三个信任域,分别为 A、B、C,它们当前状态下的信任度取值如表1所示。

表1 域A、B、C间的信任值

域	A	B	C
A	—	0.1	0.8
B	0.5	—	0.6
C	0.4	0.7	—

假设域 A 某用户想要访问域 B 某资源,前几次表现良好以获得好的信任度,然后开始恶意行为,如图3所示,浅色柱是域 B 对域 A 该用户的打分,深色柱是域 B 对域 A 的信任度。从图中可以看出,前几次用户表现良好获得了较好的信任值,域 B 与域 A 保持信任关系,但是用户一旦开始恶意操作,打分降低,信任值会随之骤然下降,域 B 与域 A 建立的原有信任关系会随之消失。从表2可知域 B 对域 A 的信任度可接收的范围为[0.5,1],因此当第6次访问用户开始恶意行为时,域 B 对域 A 的信任度下降到0.5以下,从该次恶意行为开始,域 B 对域 A 的信任关系就消失了。

表2 各域可接受的信任值范围

域	可接受的信任值范围
A	[0.7,1]
B	[0.5,1]
C	[0.6,1]

图3反映了满意度打分对信任度的影响,在本文提出的方法中,如果两个域之间的信任关系消失,是不允许跨域访问的,因此随后的打分也会随之消失。

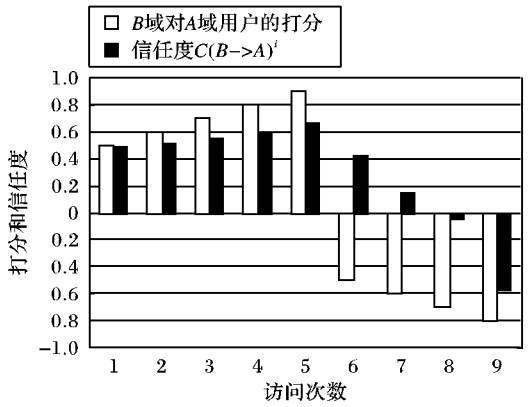

图3 满意度评分对信任度的影响

3 结语

在多个异构信任域的大规模分布式环境下,跨域认证协议是实现安全跨域访问的前提,有着重要的现实意义。本文基于信任度提出了一种跨多个异构域的认证机制,该机制根据用户的行为计算信任度,根据域间信任度动态的建立信任关系,从而实现跨域认证,更符合大规模环境下异构域之间信任关系多变的现状。分析表明,该信任度计算方法能够有效反映域间在诚实度、可靠性方面的信任程度,可以用于作为建立域间信任关系的依据。

参考文献:

[1] 顾文刚,程朝晖,荆金华,等.基于PKI的Kerberos跨域认证协议的实现与分析[J].计算机科学,2002,28(10):78-80.

[2] 罗琛,李沁,马殿富.网格环境中跨异构域身份鉴别系统的研究与实现[J].计算机工程,2005,31(22):67-69.

[3] 戴怡,杨庚.网格环境下多域间的认证机制研究[J].计算机工程与应用,2007,43(5):130-132.

[4] ZHANG DA-CHENG, XU JIE, LI XIAN-XIAN. Dynamic cross-realm authentication for multi-party service interactions [C]// Proceedings of 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Washington: IEEE Press, 2007: 440-449.

[5] 沈海波,洪帆.基于Cookie的跨域单点登录认证机制分析[J].计算机应用与软件,2006,23(12):48-51.

[6] 黄辰林.动态信任关系建模和管理技术研究[D].长沙:国防科学技术大学,2005.