公钥Kerberos的跨域认证研究与性能分析*

黄美东

(暨南大学 深圳旅游学院，广东 深圳 518053)

摘 要：Kerberos是目前广泛被采用的成熟的认证协议，跨域认证是Kerberos在网络中的应用，实现远距离网络认证功能。传统的Kerberos基于对称密钥加密技术，为了使网络认证更加安全有效，在Kerberos认证过程中采用公钥加密。对kerberos集成公钥跨域认证进行深入研究，并对集成公钥后的Kerberos跨域过程进行模拟环境测试和性能分析。

关键词：Kerberos；认证；跨域认证；公钥；加密；公钥Kerberos

中图分类号：TP309 **文献标识码**：A

The performance analysis and cross-realm authentication research of public-key Kerberos

HUANG Mei Dong

(Shenzhen Tourism College, Jinan University, Shenzhen 518053,China)

Abstract: Kerberos is an advance protocol which adopped widely. Cross-realm authentication is the application of Kerberos in intenert to realize authentication in remote realm. For the traditional Kerberos, which is base to make sure sharing secret key,for the authentication more effective and secure, the public-key infrastructure is adopt. This paper focuses on cross-realm authentication of public-key kerberos and analizees the performance of it.

Key words: Kerberos; authentication; cross-realm authentication; public-key; encryption; public-key Kerberos

1 Kerberos系统概述

1.1 Kerberos V5

Kerberos是MIT在20世纪80年代为Aihenal计划开发的一种基于KDC概念和Needham.schroeder方法的分布式认证服务系统，它可以在不安全的网络环境中为用户对远程服务器的访问提供自动鉴别、数据安全性和完整性服务，以及密钥管理服务。在Kerberos 认证过程中服务器应能确定客户的身份，但在开放环境中则给服务器增加了过重的负担。为此引入了被称为认证服务器AS(Authenticator)的第三方来承担对用户的认证，AS 知道每个用户的口令，并将口令存在一个中心数据库。AS 将收到的用户口令和中心数据库存储的口令相比较以验证用户身份。如果验证通过， 则向用户发放允许用户得到服务器服务的票据，用户根据这一票据去获取服务器V 的服务；如果用户需多次访问同一服务器或不同服务器，为了避免每次都重复以上获取票据的过程，引入另一新服务器称为票据许可服务TGS(ticket-granting server)。TGS向已经通过AS 认证的客户发放用于获取服务器V 的服务票据。为此用户应首先向AS 获取访问TGS 的票据Tickettgs(票据许可票据)，保存后可反复使用。用户每次欲获得服务器V 的服务时，将Tickettgs 出示给TGS，TGS 再向用户发放获得服务器V 服务的许可票据Ticketv。Kerberos V5运作程序如图1所示。

运作步骤：

认证身份与取得TGT门票：

$Ticket_{TGS} = E_{KTGS}[Flages \| K_{A,TGS} \| Realm_A \| ID_A \| Times \| Authen\_Data]$

索取服务门票：

$Ticket_B = E_{KB}[Flages \| K_{A,}B \| Realm_A \| ID_A \| AD_A \| Times \| Authen\_Data]$

$Authen\_1_A = E_{KA,TGS}[ID_A \| Realm_A \| TS_1]$

要求服务：

$Authen\_1_B = E_{KA,}[ID_A \| Realm_A \| TS_1 \| Subkey \| Seq\#]$

*基金项目：广东省非物质文化遗产的数字化管理与开发式保护研究(07JA630042)

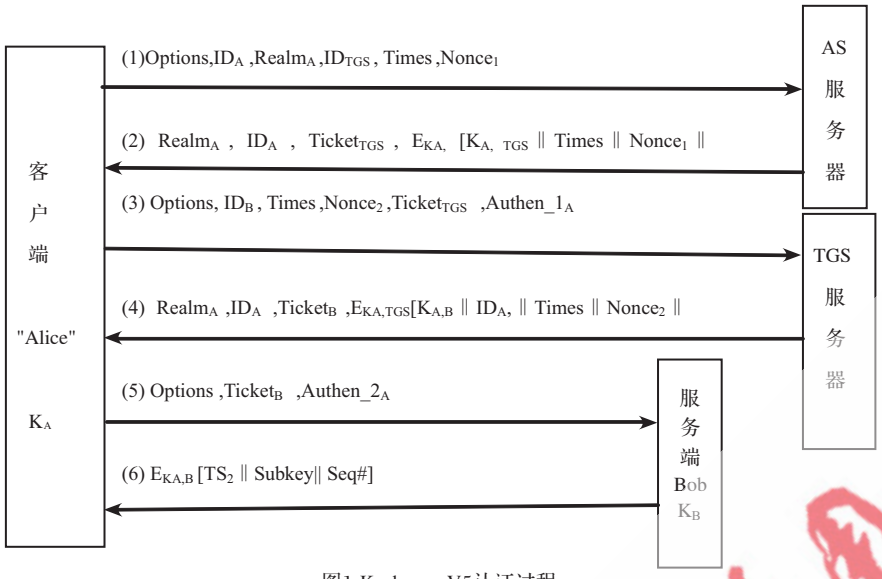

图1 Kerberos V5认证过程

参数： 领域 (Realm) ；选项(Options)；时间参数(Times)；乱数 (Nonce)；A：客户机；AS：认证服务器；V：服务器；ID_A：客户机用户的身份；TGS：票据许可服务器；IDv：服务器V 的身份；IDtgs：TGS的身份；AD_A：A 的网络地址；P_A：A 上用户的口令；TSi：第i 个时戳；lifetimei：第i 个有效期限；K_C：由用户口令导出用户和AS的共享密钥；K_A，tgs：A 与TGS 的共享密钥；K_V：TGS 与V 的共享密钥；Ktgs：AS 与TGS 的共享密钥；K_A，v：A 与V 的共享密钥。

1.2 Cross-realm Kerberos

Kerberos支持跨域认证，每个域由1组用户、1个KDC和若干应用服务器组成。通过跨域认证用户可以共用1个用户访问各个域内的资源。在Kerberos 5中，域R1中的用户C要访问域R_n中的服务S，Kerberos将R_n的KDC登记为R_1的1个特殊服务，用户C在R_1中请求1个TGT然后将R_n的KDC看做R_1的本地服务，获得1个服务票。这个服务票的格式与用户C在R_n中的TGT格式一样，通过这个票访问Rn的KDC获得访问S的服务票。R_1的KDC用于加密这个特殊服务票访问R_n的KDC的密钥被称为跨域密钥。如果R_1与R_n没有互相认证的关系，R_1中的用户C要访问R_n中的S，可以通过中间域R_2、R_3……R_{n-1}、R_n，但是两个相邻域间必须有认证关系。跨域认证关系如图2。

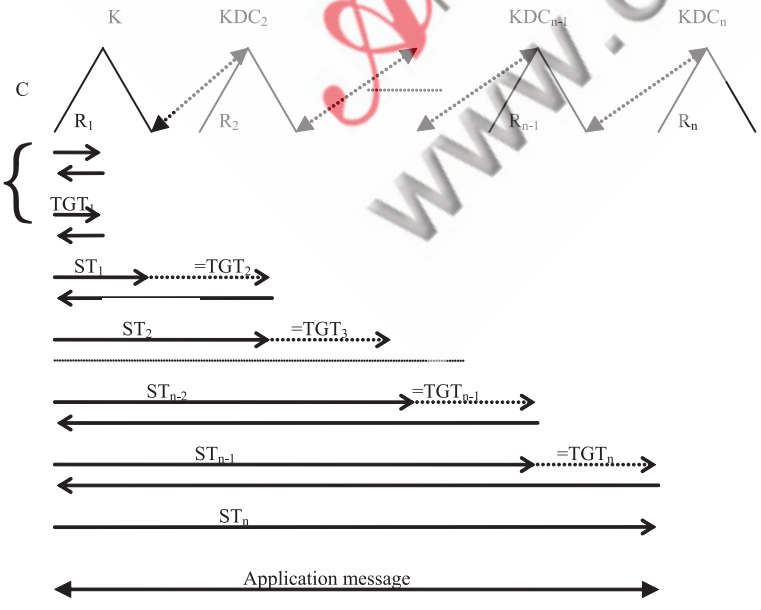

图2 跨域认证过程图

2 公钥Kerberos

Kerberos的1个潜在限制是它依赖于对称密钥加密，每个用户和KDC之间、每个应用服务器和KDC之间、不同域的KDC之间必须分享密钥。公钥的使用使密钥管理从KDC转换到CA。公钥加密不需要在用户、服务器和KDC之间建立大量的连接去分享密钥。尽管公钥加密相对于私钥加密的优势没有确切的计算数值，但是很多协议已经采用了公钥加密以改变密钥管理模式。目前有3种可选择的Kerberos集成公钥的方式：

(1)在Kerberos的初始身份验证过程采用公钥加密(PKINIT)；

(2)在Kerberos跨域认证过程中采用公钥加密

(3)把公钥应用于应用服务器的票。(PKCROSS)；

(PKTAPP)其中PKINIT是核心，PKCROSS和PKTAPP都是用PKINIT的信息格式和数据结构的变换形式在kerberos认证的不同环节中应用公钥加密。PKINIT是指在Kerberos最初交换信息时，使用公钥加密代替私钥加密。具体过程如图3所示。

客户端必须先发送1个公钥证书和证书序列号给KDC建立信任关系，同时客户端也要发送1个用客户端私钥签名的认证数据包。KDC通过验证数据包内的数字签名证实客户端的身份，KDC回复客户端一条信息，包含KDC的公钥证书序列号，KDC的数字签名和用客户端公钥加密的会话密钥。客户端通过验证KDC的数字签名验证KDC的身份。

PKCROSS是PKINIT逻辑上的扩展，是在多域间用公钥进行加密。KDC与KDC间的认证过程用公钥加密，将其中1个KDC视作客户端。具体认证过程如图4所示。当客户端要访问远程服务时，本地KDC就执行PKCROSS与相对应的远程KDC的认证。KDC与KDC间的认证遵循PKINIT协议，有一点不同的是远程KDC响应1个用于PKCROSS请求的特殊对称密钥，TGT用这个特殊的对称密钥封装，一旦客户端拥有这个远程TGT，客户端即可请求这

个域的其他票，不必经过本地KDC。

PKTAPP：在传统Kerberos中KDC在自己的域内分配所有的TGS、远程KDC和服务票据等，大多数认证信息都传输给KDC，这会造成一种瓶颈现象。尽管在一些系统中设有从KDC，但是它们只是当主KDC出现故障时做备份用，不能解决瓶颈问题。PKTAPP可以通过用户和应用服务器直接进行认证交换，减少通信阻塞情况消除这种潜在的瓶颈。PKTAPP在信息交换方面比传统的Kerberos协议更有效，客户端可以与应用服务器直接交互。PKTAPP认证过程如图5所示。

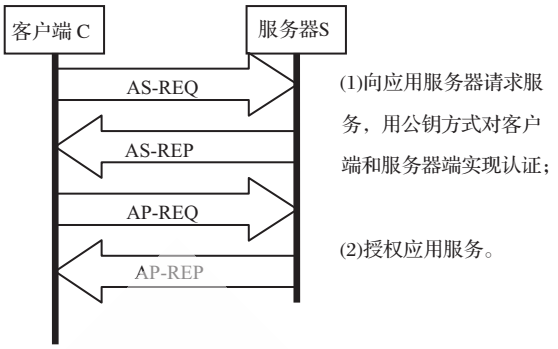

图5 PKINIT处理流程

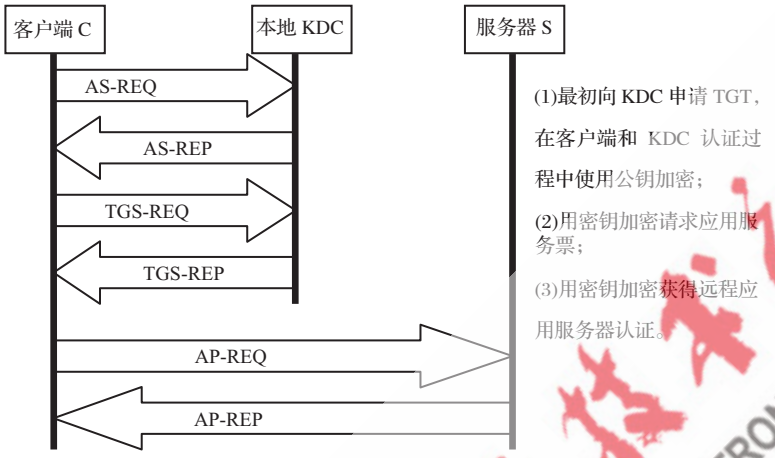

图3 PKINIT处理流程

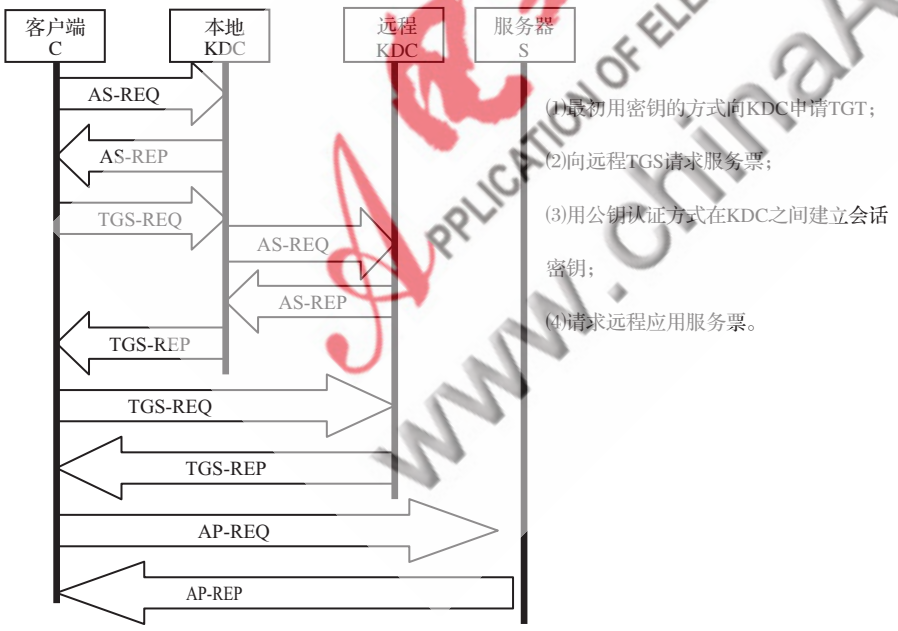

图4 PKCROSS处理流程

客户端发出第一条消息AS-REQ，包含客户端的证书序列号和请求的服务票据验证。服务器响应1条信息AS-REP，包含服务器的证书序列号和用服务器私钥加密的会话密钥。认证完成后，客户端用Kerberos的请求信息请求应用服务票，全部的认证过程被减少到2个消息对。

以上的公钥扩展，没有明确要求客户端与KDC之间或不同KDC之间预先知道彼此的身份，不需要提前建立连接分享密钥或者在Kerberos数据库中存储用户记录，这些实体之间唯一信任基础是证书序列号。显而易见，PKTAPP减少了很多信息传输的开支。

3 PKCROSS与PKTAPP协议性能分析

在Kerberos认证过程中，KDC、应用服务器、传输网络和客户端工作站的处理能力都是有限的，因此用封闭的排队网络对集成公钥的Kerberos两种形式进行随机测试。测试结构由1个局域网内的本地KDC、客户端、服务器和一个外网的远程KDC、客户端、服务器组成，这种封闭的排队网络测试对每个站点和系统的要求都是平均的，因此可以对比两种集成公钥的Kerberos形式进行对比分析。设定客户端、KDC和应用服务器程序都执行1 024 bit RSA公钥或者标准DES。表1概括了认证过程中PKTAPP和PKCROSS执行的加密操作。从认证过程上看，1个单一的应用服务器的认证过程二者执行的公钥和私钥操作是一样的，但是PKCROSS 需要更多的密钥操作。根据以上设定的标准，在应用服务器数量不断增加的情况下进行测试，随着应用服务器数量的增长，在每次处理过程中相应服务器产生的访问次数随之增长。PKTAPP对于每个增加的应用服务器，处理过程中都包括一项新增的公钥计算量。在PKCROSS的执行过程中，在当地KDC和远程域KDC之间只有一次公钥认证，与远程域中应用服务器数量多少无关。

通过测试，对PKTAPP和PKCROSS随着应用服务器数量的增加，在处理响应时间和处理能力方面进行对比分析。PKCROSS的处理过程中远程域中的应用服务器分别为1个和16个。PKTAPP处理过程中远程域的服务器分别是1个、2个和4个。两个协议的处理速率都不停地增长直到响应时间不稳定和迅速的增长。测试结果显

示PKCROSS处理过程中，远程域中的服务器1个和16个的时候随着处理任务的增加，响应延迟时间变化趋于一致，性能变化不大。在PKCROSS处理过程中第一个瓶颈是远程KDC的处理能力，它要承担两项处理任务，一是监测UDP传输，二是监听PKINIT在TCP连接上的处理并且处理KDC到KDC的PKINIT交换的一半的公钥计算量。第二个瓶颈是有相似工作量的本地KDC。应用服务器管理最后用户只用密钥加密的认证，它的处理能力没有充分利用。PKTAPP在测试过程中，远程域中只有一个应用服务器时的性能明显优于PKCROSS，当远程域中应用服务器数量为2时，PKTAPP与PKCROSS性能接近，但是当远程域中的应用服务器数量为4时，随着处理任务的增加，响应延迟时间迅速上升，认证性能下降明显。原因是当远程域中应用服务器数量为1时，PKTAPP因为单一认证过程只有两个消息对，而显示出良好的性能。当服务器数量增加时，由于每个服务器都要进行认证，造成认证性能下降。

表1 PKCROSS与PKTAPP认证处理的加密操作情况

认证处理	私钥执行次数	公钥执行次数	密钥执行次数
PKCROSS			
客户端	0	0	7
本地KDC	2	3	5
远程KDC	1	4	4
应用服务器	0	0	3
总计	3	7	19
PKTAPP			
客户端	2	3	3
应用服务器	1	4	4
总计	3	7	7

分析表明，远程域中只有一个应用服务器时PKTAPP是更好的选择。对于远程域中应用服务器多于2个的，PKCROSS明显地更加稳定。在测试时笔者只考虑应用服务器的工作量由认证产生。一般来说应用服务器还要执行其他处理工作，如果将这些工作量考虑进去，PKCROSS应该是更加适用的。

使PKCROSS的性能超过PKTAPP性能的应用服务器的数量被称为“cross-over”，“cross-over”会随着服务器和网络的能力的不同而不同，本次测试的结构是低性能服务器和高性能网络。若改变测试环境，将服务器和KDC的处理能力提高一到两个数量级，将网络能力降低，当远程域多于2个应用服务器的时候，PKCROSS的性能应该更加突出。

通过对PKTAPP与PKCROSS两种协议的分析对比，PKCROSS在远程域中服务器数量大于一个时比PKTAPP更好，这个结果有利于将两种协议更好地组合提高公钥Kerberos的认证性能。

使用这种公钥Kerberos协议要求服务器对PKTAPP和传统的Kerberos协议都支持，同时要求客户事先知道远程域中应用服务器的数量，客户在开始执行服务器认证之前，会进行服务器信息的搜索，得到一个服务器清单。这样就允许在认证过程中使用PKCROSS或者使用PKTAPP根据每个域的服务器数量。以上只是在一种环境下对PKTAPP与PKCROSS两种协议的分析对比，随着网络环境的不断复杂和服务器的处理能力不断提高PKTAPP与PKCROSS的对比分析研究也将不断深入。

参考文献

[1] KOHL J.The Kerberos network authentication service (V5), C. Neuman, Editor. 1993:http://www.ietf.org/rfc/rfc1510.txt?number=1510.

[2] ASHELY P，BROOM B.A survey of securemulti-domain distributed architectures，Queensland University of Technology, Faculty of Information Technology.1997.

[3] BASSHAM L E.Efficiency testing of ANSIC implementations of round 1 candidate algorithms for the advanced encryption standard，Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.1999.

[4] 刘壮，郭荷清，张娟娟.基于公钥的Kerberos 分布式认证方法研究[J].计算机工程与应用，2006，(04).

[5] HARBITTER A，MENASCÉ D.Performance of public- key-enabled Kerberos authentication in largenetworks[C].2001 IEEE Symposium on Security and Privacy Proceedings，IEEE Computer Society Press，2001.

（收稿日期：2009-01-09）

(上接第40页)

Circuits， Syst. Signal processing， 1990，9(3):271-300.

[3] MCARTHUR D， REILLY J P. An efficient self-calibrating direction-of-arrival estimator: Statistical Signal and Array Processing[C].[S.l.]:[s.n.]， IEEE Seventh SP Workshop on June 26-29，1994：129-132.

[4] DAVID A，SWINDLEHURST A L. Spatial signature estimation for uniform linear arrays with unknown receiver gains and phase[J]. IEEE Transactions on Signal Processing，1999，47(8):2128-2138.

[5] 王布宏，王永良，陈辉．方位依赖阵元幅相误差校正的辅助阵元法[J]．中国科学E辑，2004，34(8)：906-918.

[6] 王建英，尹忠科，张春梅．信号与图像的稀疏分解及初步应用[M]．成都：西南交通大学出版社，2006.

[7] MALLAT S， ZHANG Z. Matching pursuits with time-frequency dictionaries[J]. IEEE Trans. Signal Process，1993，41:3397-3415.

(收稿日期：2009-01-12)