

# 基于 Kerberos 协议的用户到用户认证系统的研究

杨战海

(延安大学 计算中心, 陕西 延安 716000)

**摘 要:**基于 Kerberos 协议的典型系统为单点登录身份认证系统,即单域身份认证系统,而关于用户到用户的身份认证系统,多采用 NTLM 协议。为了研究基于 Kerberos 协议的用户到用户认证系统,在充分研究 Kerberos 协议的体系结构和 workflows 的基础上,对用户到用户的 Kerberos 身份认证系统的认证过程进行了详细的设计,分析了用户到用户的 Kerberos 身份认证系统的典型结构。研究表明,当一个客户端需要访问另一个客户端中运行的服务时,Kerberos 身份认证协议支持在两个客户端之间的身份认证。

**关键词:**身份认证;Kerberos;密钥分发中心;认证服务器;单点登录;用户到用户

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2010)10-0180-04

## Research on Kerberos Protocol Based User-to-User Authentication System

YANG Zhan-hai

(Computer Center, Yan'an University, Yan'an 716000, China)

**Abstract:**Kerberos protocol based typical system is the single sign-on identity authentication system, namely, the single-domain identity authentication system, whereas, user-to-user identity authentication system mainly based on NTLM protocol. In order to research Kerberos protocol based user-to-user identity authentication system, detailed designs the authentication course of the Kerberos protocol based user-to-user identity authentication system and analyzes the typical structure of the Kerberos protocol based user-to-user identity authentication system on the basis of researching the architecture and workflow of the Kerberos protocol. The research shows that when a client-side needs access to the running service of another client-side, Kerberos protocol based identity authentication is applied to the identity authentication between the two client-sides.

**Key words:**identity authentication;Kerberos;KDC;AS;SSO;user-to-user

## 0 引言

Kerberos 协议是一种计算机网络授权协议,用来在非安全网路中,对个人通信以安全的手段进行身份认证。这个协议是 20 世纪 80 年代麻省理工学院(MIT)开发的一套计算机软件<sup>[1,2]</sup>,是为 TCP/IP 网络设计的可信第三方鉴别协议<sup>[3-5]</sup>,Kerberos 服务器提供了安全的网络鉴别,允许用户访问网络中的不同服务器。

Kerberos 基于对称密钥体制,它与网络上的每个网络实体共享一个不同的秘密密钥,Kerberos 通过网络实体是否知道秘密密钥验证其身份。

## 1 Kerberos 的体系结构

在 Kerberos 模型中,网络实体是指位于网络上的客户机(Client)和应用服务器(Server)。客户机可以是用户,也可以是处理事务所需要的独立的软件程序。Kerberos 拥有一个存储所有用户秘密密钥的数据库,对于每个用户而言,秘密密钥是一个加密口令,需要鉴别的网络业务以及希望运行这些业务的客户机需要使用其在 Kerberos 注册的秘密密钥。Kerberos 知道每个网络实体的秘密密钥,因此,它能够产生一个消息,用于证实实体的身份。

另外,Kerberos 还能够产生会话密钥,提供给通信的双方实体,用于加密双方间的通信信息,通信结束后,销毁会话密钥。

Kerberos 体系结构主要由密钥分发中心(Key Distribution Center, KDC)、客户端(Client)和应用服务器(Server)三大部分组成。

收稿日期:2010-01-30;修回日期:2010-04-26

基金项目:陕西省科研计划项目(09BY37)

作者简介:杨战海(1972-),男,讲师,硕士研究生,研究方向为计算机教育与网络技术。

### 1.1 Kerberos 的 KDC

对称密码学的一个缺点就是需要通信双方事先对密钥达成一致协议。在现实中,有时从未见过面的双方试图应用对称密钥密码进行通信。由于它们只能通过网络彼此通信,故而无法提前协商密钥。采用的解决方案是使用双方都信任的密钥分发中心。

密钥分发中心(KDC)是一个独立的可信网络实体,是一个服务器,它同每个注册用户共享不同的秘密对称密钥<sup>[6]</sup>。这个密钥可能是在用户第一次注册时手工设置的,通过 Kerberos 注册设置秘密密钥的过程不能是通过网的,必须是面对面的。KDC 持有一个存有所有用户秘密密钥的数据库,每个网络实体(无论是客户还是服务器)共享了一套只有它自己和 KDC 知道的秘密密钥。秘密密钥的内容用于证明实体的身份,即进行身份认证<sup>[7,8]</sup>。对于两个实体间的通信,KDC 还能产生一个会话密钥,用来加密它们之间的通信信息,通信完毕,立即销毁会话密钥。

Kerberos 模型中的密钥分发中心(KDC)实际上包含认证服务器(Authentication Server, AS)和票据授权服务器(Ticket Granting Server, TGS)两个独立的逻辑部分。认证服务器(Authority Server, AS)验证实体的身份,若通过身份验证则提供票据授权票据(Ticket Granting Ticket, TGT),客户依据 TGT 票据从票据授权服务器中申请得到服务授权票据(Service Ticket, ST),客户再依据 ST 票据申请应用服务器提供相应的服务。用于证明用户身份的票据(Ticket)是 Kerberos 工作的基础,因此,KDC 是整个系统的核心<sup>[9]</sup>。

### 1.2 Kerberos 的 Client

Kerberos 的客户端(Client)程序把用户输入登录密码通过单向散列函数转换为该用户的秘密密钥。此密钥对应于 KDC 中存储的该用户的信息通过相同的单向散列函数转换得到秘密密钥。客户端的主要功能是向 KDC 和应用服务器发送各种请求消息,并接收从 KDC 和应用服务器返回的各种消息和服务。

Kerberos 的客户端与操作系统的集成可以采用两种实现方式。第一种方式称为结合式,即把 Kerberos 的客户端与操作系统的 Login 等软件集成或者关联。每当用户输入用户名以及对应的口令进行系统登录时,Kerberos 客户端软件也得到了同样的用户名和口令。该客户端软件能够立即向 Kerberos 服务申请身份验证或者等到用户申请具体应用服务时再向认证服务器(AS)申请身份认证票据(TGT)。第二种方式称为分离式,即把客户端软件独立于操作系统,当客户端首次申请应用服务时,客户端检测缓存中是否有身份认证票据(TGT),若有说明用户已经向 Kerberos 服务申

请注册并验证成功;若无则要求用户输入用户名或口令,向服务器申请身份认证票据(TGT)。用户在得到票据授权服务器(TGS)服务认证后,在本地得到了身份认证票据(TGT)以及与应用服务的会话密钥,不同的应用服务对应于不同的会话密钥,因此如果用户使用文件服务器和邮件服务器,他将有一个身份认证票据(TGT)以及两个会话密钥。客户端功能中的一个子项是修改和设置用户密码。具体讲,当用户由于某些原因想要更改自己密码的时候,需要向服务器证明自己身份并提交密码修改请求。这是很重要的一步,如果处理不慎,可能被他人从网络上非法截取到。

### 1.3 Kerberos 的 Server

Kerberos 的应用服务器(Server)接收用户的服务请求消息,通过服务器的秘密密钥从服务授权票据(ST)中提取会话密钥,依据会话密钥解密加密信息验证用户的身份,用户身份得到认证后,依据票据提供的服务请求,提供给合法用户所需求的服务。

## 2 Kerberos 的工作流程

Kerberos 的工作流程分三个阶段<sup>[10~12]</sup>,如图 1 所示。

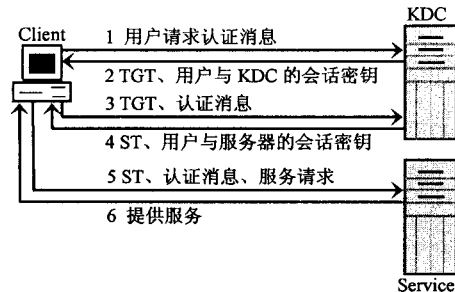


图 1 Kerberos 的工作流程

### 2.1 Client 与 AS 的通信

用户通过客户端(Client)向认证服务器(AS)发出认证服务请求。认证服务请求消息中的用户名以明文的形式发送,而不可以以密文形式发送。因为认证服务器只有在解密密文后才能得知用户名,显然,认证服务器不能使用用户存储在它的数据库中秘密密钥进行解密。如果认证服务请求消息以密文传送,并且发送密文的加密密钥,也是不必要的。因为网络中入侵者完全可以得到该密文和加密密钥,解密后可以得到用户名,显然,这种做法毫无意义。

虽然认证服务请求消息中的用户名以明文的形式传送,但请求信息中的其它信息如用户的身份识别信息使用用户的秘密密钥进行加密传送。

认证服务器验证用户是否存在和合法。认证服务器从用户的请求消息中提取出用户名,并在自己的数

数据库中查找该用户名。如果查找到该用户名,使用该用户的秘密密钥解密认证服务请求消息中的其它消息,得到用户的身份识别消息,比对存储在数据库中的该用户的身份识别消息,从而判断用户的身份是否合法。

认证服务器验证用户身份合法后,返回以下两条信息给用户:

消息 A: 用户与票据授权服务器之间的会话密钥。

消息 A 使用用户的秘密密钥进行加密。

消息 B: 票据授权票据(TGT), 票据中的信息包括用户身份、用户网络地址、票据有效期、用户与票据授权服务器会话密钥。消息 B 使用票据授权服务器秘密密钥进行加密。

当用户收到消息 A 和消息 B 后,使用自己的秘密密钥解密消息 A 得到用户与票据授权服务器之间的会话密钥。应该注意,用户不能解密消息 B,因为消息是用票据授权服务器秘密密钥加密的。

## 2.2 Client 与 TGS 的通信

用户通过客户端(Client)向票据授权服务器(TGS)发出用户服务认证服务请求。此时,用户向票据授权服务器发送以下两条消息:

消息 C: 由从消息 B 中获取的票据授权票据和申请的服务的身份组成。

消息 D: 用用户票据授权服务器会话密钥加密的认证消息,该消息由用户身份和时间戳组成。

当票据授权服务器收到消息 C 和消息 D 后,授权服务器从消息 C 中重新获取消息 B,并且使用自己的秘密密钥解密消息 B,得到用户身份、用户网络地址、票据有效期、用户与票据授权服务器会话密钥等信息。使用该会话密钥解密消息 D,取出用户信息,与 TGT 中的用户信息相比较,验证用户身份的合法性。

票据授权服务器验证用户身份合法后,从消息 C 中提取用户申请服务的身份信息,即用户指定的应用服务器的信息,然后返回给用户以下两条信息:

消息 E: 用户与应用服务器之间的会话密钥。消息 E 使用用户的秘密密钥进行加密。

消息 F: 服务授权票据(ST), 包括用户身份、用户网络地址、票据有效期、用户与应用服务器间会话密钥等信息。消息 F 使用应用服务器秘密密钥进行加密。

当用户收到消息 E 和消息 F 后,使用自己的秘密密钥解密消息 E 得到用户与票据授权服务器之间的会话密钥。应该注意,用户不能解密消息 F,因为消息是用应用服务器秘密密钥加密的。

## 2.3 Client 与 Server 的通信

用户通过客户端(Client)向应用服务器(Server)发

出用户服务认证服务请求。此时,用户向应用服务器发送以下两条消息:

消息 F: 用户从票据授权服务器接收的服务授权票据(ST), 包括用户身份、用户网络地址、票据有效期、用户与应用服务器之间的会话密钥等信息。消息 F 使用应用服务器秘密密钥进行加密。

消息 G: 用应用服务器会话密钥加密的认证消息,该消息由用户身份和时间戳组成。当应用服务器收到消息 F 和消息 G 后,应用服务器使用自己的秘密密钥解密消息 F,得到用户身份、用户网络地址、票据有效期、用户与应用服务器会话密钥等信息。使用该会话密钥解密消息 G,取出用户信息,与 ST 中的用户信息相比较,验证用户身份的合法性。如果用户得到认证,应用服务器返回以下消息给用户,确认用户的身份真实,并乐于向用户提供服务:

消息 H: 在用户认证中找到时间戳,加 1,使用用户与应用服务器会话密钥加密。

用户使用用户与应用服务器会话密钥解密确认函,并检查时间戳是否被正确地更新。如果是,用户可以信赖服务器,并可以向服务器发送服务请求。

## 3 用户到用户的身份认证的解决方案

当一个客户端需要访问另一个客户端中运行的服务时,Kerberos 身份认证协议也支持在两个客户端之间的身份认证,也就是这里所说的用户到用户(User-to-User)身份认证。图 2 显示了用户到用户的 Kerberos 身份认证的典型结构。

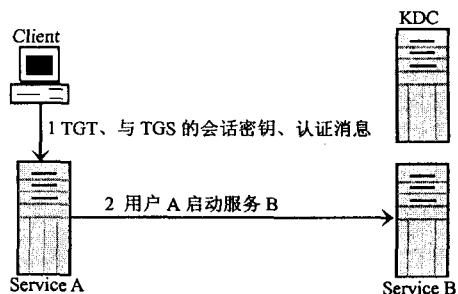


图 2 用户到用户身份认证的典型结构

对于用户到用户的 Kerberos 身份认证需要以下两个典型过程:

(1) 一个用户登录并开始应用,称为服务 A(Service A),并以自己的标识继续这个应用。服务 A 现在可以依据用户所拥有权限访问网络资源了。

(2) 服务 A 扮演用户,开始了另一个应用,称之为服务 B(Service B)。服务 B 与用户的服务 A 标识是一致的。

这样一来,3 个网络实体都共享一个用户标识:客

户端、服务 A、服务 B。但服务 B 比较独特,它是 3 个中唯一一个不用登录的。

在服务 A 开始服务 B 时,是使用用户已有的标识。服务 B 将与活动目录服务中的这个用户相关联,但是服务 B 没有用户密码或密钥信息。服务 B 已有了一份用户 TGT 副本和客户端的 TGS 会话密钥(登录会话密钥),所以它从不需要用户密码信息。但是,这种身份认证方式中存一个问题。在一般的身份认证中,用户将向服务 B 发送由 TGS 和由用户的服务 B 会话密钥加密的认证符提供的票证。服务 B 将解密票证和认证符,得到会话密钥。问题就在于,服务 B 不能解密票证,因为它没有用户密钥副本。Kerberos 的用户到用户身份认证就是这个问题的解决方案,具体的步骤如图 3 所示。

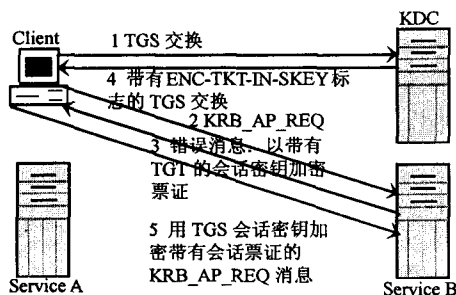


图 3 用户到用户身份认证过程

用户到用户身份认证描述如下:

(1) 用户为服务 B 请求一个服务票证。TGS 检查活动目录,以查找与服务 B 关联的用户账户。因为服务 B 仅是一个角色,其账户还是用户。所以,TGS 检查用户对象,得到用户密钥,然后用它加密票证。具体的 TGS 服务票证申请过程如前面正常身份认证过程一样。

(2) 用户发送服务票证给服务 B。

(3) 即使服务 B 拥有了用户凭证,它仍没有用户密码信息,不能计算出用户密钥,这样它还是不能解密票证。这样的结果就是用户不能以服务 B 进行身份认证,也就不能使用应用系统。

此时,服务 B 会以 KRB\_AP\_REQ 消息响应一条错误的信息。以这条错误消息,服务 B 把用户 TGT,连同从服务 B 的 TGT 中得到的会话密钥加密的新的票证请求一起发送给用户。

(4) 用户为服务 B 向 TGS 请求一个新的服务票证。在这个请求消息中,用户发送它自己的 TGT,在票证字段中附加的服务 B 的 TGT,ENC-TKT-IN-SKEY 标志。这是一个可选请求,用来附加票证会话密钥加密票证。

TGS 联系服务 B 附加票证,因为它在票证请求中

是目标服务器。KDC 查找服务 B,发现它是与用户对象关联的,获取用户密钥,解密服务 B 的 TGT。TGS 从服务 B 的 TGT 中获得会话密钥,为用户创建新的票证,并用会话密钥加密。

(5) 用户发送新的 KRB\_AP\_REQ 消息给服务 B,进行正常的身份认证过程。

## 4 结束语

Kerberos 基于对称密钥体制,它与网络上的每个实体共享一个不同的密钥,通过是否知道秘密密钥来验证身份。Kerberos 软件设计上采用客户端/服务器结构,并且能够进行相互认证,即客户端和服务端均可对对方进行身份认证。同时,当一个客户端需要访问另一个客户端中运行的服务时,Kerberos 身份认证协议也支持在两个客户端之间的身份认证,也就是文中所研究的用户到用户身份认证系统。

Kerberos 身份认证协议是 10 年前由 MIT 开发的。第一个公开发行的是 Kerberos V4 身份认证协议,在得到广泛的工业应用和重视后,又开发了 Kerberos V5 身份认证协议。Kerberos 身份认证协议的当前版本是 Kerberos V5。Kerberos V5 是域内主要的安全身份认证协议。Kerberos V5 协议可验证请求身份认证的用户标识,以及提供请求身份认证的服务器。这种双重认证也就是通常所说的“相互身份认证”。Kerberos V5 身份认证协议提供了一种在客户机和服务器之间,或者一个服务器与其他服务器之间进行相互身份认证的机制。

## 参考文献:

- [1] 陈 锋,徐正全,徐彦彦.一种利用 Diffie-Hellman 密钥协商改进的 Kerberos 协议[J]. 计算机应用,2007,27(12): 116-117.
- [2] 卢小良,袁 丁.对一种基于动态密码体制的 Kerberos[J]. 四川师范大学学报,2006,29(2):239-243.
- [3] 马佩勋,李 杰. Kerberos 协议及其授权扩展的研究与设计[J]. 计算机技术与发展,2006,16(5):109-111.
- [4] Needham R M, Schroeder M D. Using encryption for authentication of large networks of computers[J]. Communications of the ACM,1978,21(12):993-999.
- [5] Denning D, Sacco G. Timestamps in key distribution protocols [J]. Communications of the ACM,1981,24(8):533-536.
- [6] 教育部考试中心.全国计算机等级考试三级教程——网络技术[M]. 北京:高等教育出版社,2008: 216-217,223.
- [7] 范宏生,叶 震,侯保花.基于公钥密码体制的 Kerberos 协议的改进[J]. 计算机技术与发展,2006,16(4):224-227.

(下转第 188 页)

8G,本地磁盘 73 \* 4 块),可以运行 30 个 Guest OS,用户使用感受上无明显延迟感。表 1 是根据 vCenter 统计数据取 15 个工作日的使用情况得出的性能数据。

经过对数据分析可以看出,刚开始上班时服务器较为忙碌,由于刚上班,使用 Internet 收发邮件的员工较多,这一时间段用户使用率较高。另外发现中午由于员工休息时间较长,使用互联网访问 Internet 的频率高,造成服务器负载较重。

表 1 CPU 和内存占用率(I)

测试时间	CPU 占用率	内存占用率
8:30-9:30	84%	87%
9:30-10:30	78%	88%
10:30-11:30	75%	88%
11:30-12:30	91%	89%
12:30-13:30	88%	86%
13:30-14:30	82%	83%
14:30-15:30	76%	85%
15:30-16:30	79%	86%
16:30-17:30	75%	83%

针对这种情况,原补丁更新时间从早上 8:30 开始调整到午夜 12 点,同时制作定时关机脚本,强制在空闲时间段关闭用户虚拟机释放内存和 CPU 资源。通过一系列控制措施,使高峰数据得到缓解(见表 2)。

表 2 CPU 和内存占用率(II)

测试时间	CPU 占用率	内存占用率
8:30-9:30	81%	85%
9:30-10:30	78%	86%
10:30-11:30	75%	86%
11:30-12:30	83%	85%
12:30-13:30	85%	87%
13:30-14:30	82%	85%
14:30-15:30	76%	84%
15:30-16:30	78%	85%
16:30-17:30	75%	82%

## 5 结束语

通过对虚拟化技术的研究,提出一种基于虚拟交

换机的 Internet 安全访问控制方法。在文中,作者详细剖析技术实现方法以及深层次原理,同时就信息中心级的 Internet 安全访问架构给出了关键部分解决方案。并深刻反思了虚拟化产品的网络安全问题,关于潜在安全问题提出了一个较为可行的解决方案。

当采用虚拟化基础实现网络隔离技术时,如果将本方案反向使用,即可完成基于虚拟化技术的安全 VPN 访问,可通过在外部 DMZ 区的 MP 安全地对内网设备进行操作,达到 VPN 和内部网没有七层协议的作用。

## 参考文献:

- [1] Heiser G, Elphinstone K, Kuz I, et al. Towards Trustworthy Computing Systems: Taking Microkernels to the Next Level[J]. SIGOPS Operating Systems Review, 2007(7):3-11.
- [2] Ave H. VMware Virtual Networking Concepts[EB/OL]. 2007. <http://www.vmware.com>.
- [3] 熊林. VMware 的技术与应用探析[J]. 开发研究与设计技术, 2007(12):428-429.
- [4] 刘志平. 基于 VMware 虚拟网络的构建[J]. 内蒙古大学学报:自然科学版, 2007(1):94-98.
- [5] Whitaker A, Shaw M, Gribble S D. Denali: lightweight virtual machines for distributed and networked applications[R]. Washington: University of Washington, 2002.
- [6] 杨少春. 采用 VMware 构建虚拟并行计算网[J]. 计算机工程与设计, 2006, 27(14):2546-2547.
- [7] 王一剑, 刘美玲. 虚拟化技术在金融业的应用[J]. 金融电子港, 2008(5):56-57.
- [8] 赵长林. 虚拟化中的网络性能和吞吐量[J]. 第一发现, 2009(3):29-30.
- [9] 李芳社. 虚拟化技术在通信基础设施中的应用[J]. 现代电子技术, 2009(8):149-151.
- [10] 那罡. 虚拟化的风险[J]. 网络传播, 2008(8):80-81.
- [11] 阮越, 秦峰, 周建钦. 基于 Linux Shell 的安全审计机制[J]. 计算机技术与发展, 2007, 17(6):155-158.
- [12] 刘涛, 邓璐娟, 丁孟宝. 计算机反病毒技术及预防新对策[J]. 计算机技术与发展, 2007, 17(5):105-110.

(上接第 183 页)

- [8] Tanenbaum A S. 计算机网络[M]. 第 4 版. 潘爱民, 徐明伟译. 北京:清华大学出版社, 2004:682-684.
- [9] 汪冬. 基于 Kerberos 协议的单点登录系统的研究与实现[J]. 办公自动化, 2007(8):24-26.
- [10] 贾淑红, 刘万军. 基于 Kerberos 协议的单点登录系统的设计[J]. 计算机应用, 2007, 27(6):238-239.
- [11] Kohl J T, Neuman B C. The Kerberos Network Authentica-

tion Service (V5)[R]. [s. l.]: Digital Equipment Corporation, ISI, 1993.

- [12] Steiner J G, Neuman B C, Schiller J I. Kerberos: An Authentication Service for Open Network Systems[C]// Proceedings of the USENIX Winter 1988 Technical Conf. Dallas, Texas: USA: USENIX Association, 1988.