基于公钥密码体制的 Kerberos 协议的改进

范宏生,叶 震,侯保花
(合肥工业大学 计算机与信息学院,安徽 合肥 230009)

摘 要:随着计算机网络的发展,网络安全问题已变得日益重要,而身份认证在安全系统中的地位极其关键,是最基本的安全服务。Kerberos协议是基于私钥密码系统的身份认证协议。文中首先对Kerberos协议的认证原理进行分析;然后基于公钥体制的加密技术和Kerberos协议,提出了一个安全性更高的身份认证协议;最后分析了两种协议的异同。

关键词:身份认证;Kerberos协议;公钥加密
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1005-3751(2006)04-0224-04

Improvement of Kerberos Protocol Based on Public Key Cryptosystem

FAN Hong-sheng, YE Zhen, HOU Bao-hua
(School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: With the development of computer network, the problem of network security is becoming even more important. Authentication is very important and basic security service among the security systems. Kerberos protocol is an authentication protocol based on private key cryptosystem. In this paper, first, the authentication theory of Kerberos protocol is analyzed, then based on the Kerberos protocol and public key encryption system, a higher security of identity authentication protocol is designed. Last analyzed the differences between the two protocols.

Key words: identity authentication; Kerberos protocol; public key encryption

1 Kerberos 协议原理

Kerberos是为TCP/IP网络设计的可信第三方鉴别协议,网络上的Kerberos服务起着可信仲裁者的作用,Kerberos是基于对称密码学,它与网络上的每个实体分别共享一个不同的秘密密钥,是否知道该密钥便是身份的证明[1]。

Kerberos协议通过提供认证中心服务,在客户机和服务器之间架起一个安全桥梁,每个向服务器提交的服务请求及其权限,必须先经过认证中心服务器的认证合格后,才能被指定服务器所执行,同时也需要服务器向用户证明自己的身份[2,3],其认证模型如图1所示。

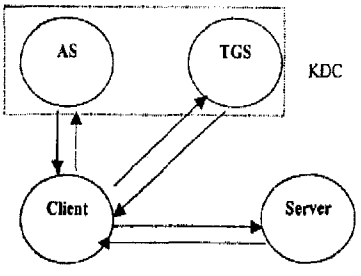

图1. Kerberos认证模型图

图中所用到的符号说明如下:

Client:客户端(C)

KDC:密钥分配中心(Key Distribution Center),由AS和TGS组成

AS:认证服务器(Authentication Server)

TGS:票据授权服务器(Ticket Granting Server)

Server:应用服务器(S)

Kc:客户端C的密钥

Ktgs:TGS的密钥

Ks:应用服务器S的密钥

Kc,tgs:客户端C和TGS共享的会话密钥

TGT:票据授权票,用于访问TGS的票据

在AS服务器中,保存有Kc,Ktgs和Ks密钥,AS服务器分别与客户、TGS服务器和应用服务器共享这些密钥。AS用于在登录时验证用户身份,TGS用于发放身份证明票据。Kerberos中使用两种凭证:票据(Ticket)和鉴别码(Authenticator)。

具体认证过程如下[3,4]:

●第一阶段(最初票据的获取),客户端从AS处获取TGT。

(1)Client->AS:

{c, tgs, timestamp, addr}

客户端向AS发出访问TGS的请求,请求报文包括客户的名称、TGS的名称、客户端的IP地址,以及时戳。请求报文以明文方式发送。

收稿日期:2005-08-11
作者简介:范宏生(1972-),男,安徽无为人,硕士研究生,研究方向为计算机网络与信息安全;叶 震,副研究员,研究方向为信息安全。

(2)AS－Client:

{Kc,tgs,Tc,tgs}Kc

Tc,tgs={tgs,c,addr,timestamp,lifetime,Kc,tgs}Ktgs

AS收到客户请求报文后,在其数据库中查找客户的加密密钥Kc,并产生随机会话密钥Kc,tgs和TGS的票据TGT作为应答报文。TGT的内容包括:TGS的名字、客户名字、客户的IP地址、时戳、有效生存期限,以及会话密钥Kc,tgs,这些数据使用TGS的密钥Ktgs进行加密。客户端收到AS返回的应答报文后,在本地输入口令生成Kc,对报文进行解密,就得到TGS的票据TGT,客户在下一步就可以把TGT发送给TGS来证明自己具有访问TGS的合法身份。客户端同时从AS处得到与TGS进行加密通信的会话密钥Kc,tgs。

●第二阶段(服务器票据的获取),客户从TGS处获取访问应用服务器的票据Tc,s。

(1) Client－>TGS:

{{s,Tc,tgs} Ktgs,Ac,tgs}

Ac,tgs={c,addr,timestamp}Kc,tgs

客户端向TGS发送访问应用服务器S的请求报文,报文内容包括要访问的应用服务器S的名字、TGS的票据TGT以及鉴别码Ac,tgs。TGT的内容是用TGS的密钥Ktgs加密的;鉴别码的内容包括客户的名字、客户的IP地址以及时戳,用客户和TGS的会话密钥进行加密。票据TGT可以重复使用且有效期较长,而鉴别码只能使用一次且有效期很短。

TGS收到客户端发来的请求报文后,用Ktgs对票据TGT进行解密,得到与客户的会话密钥Kc,tgs。TGS用Kc,tgs解密鉴别码,并将鉴别码中的数据与TGT中的数据进行比较,从而验证TGT的发送者C就是TGT的实际持有者。

(2)TGS→Client:

{Kc,s,Tc,s}Kc,tgs

Tc,s={s,c.addr, timestamp,lifetime,Kc,s}Ks

TGS检验客户身份合法后,随机产生客户端C和应用服务器S的会话密钥Kc,s,以及用于访问应用服务器S的票据Tc,s。Tc,s的内容包括:应用服务器的名字、客户的名字、客户的Ip地址、时戳、有效生存期和会话密钥Kc,s。Tc,s的内容用应用服务器S的密钥Ks加密;由会话密钥Kc,s和票据Tc,s组成TGS的应答报文,用客户C和TGS的会话密钥Kc,tgs加密。客户端C收到TGS的应答报文后,用会话密钥Kc,tgs对报文进行解密,可以得到访问应用服务器S的票据Tc,s,以及与S进行加密通信的会话密钥Kc,s。

●第三阶段(服务请求),客户端与服务器相互验证身份。

(1) Client→S:

{s,{Tc,s}Ks.Ac,s}

Ac,s={c,addr,timestamp}Kc,s

客户端C向应用服务器S发送请求报文,报文的内容包括应用服务器的名字S,用于访问应用服务器S的票据Tc,s以及鉴别码。应用服务器S收到客户端发来的请求报文后,用自己的密钥Ks对票据Tc,s进行解密处理,得知客户c已经从TGS处得到与自己的会话密钥Kc,s,S用Kc,s解密鉴别码,并将鉴别码中的数据与Tc,s中的数据进行比较,确认Tc,s的发送者c就是Tc,s的实际持有者,客户端C的身份得到验证。

(2)S→Client:

{timestamp+1}Kc,s

应用服务器S确认客户端C的身份合法后,把时戳加1,用Kc,s加密发给客户。客户C收到报文后,用会话密钥Kc,s进行解密,对新时戳进行验证,通过比较时间戳的有效性实现对S的认证。

整个协议交换过程结束后,客户和应用服务器之间就拥有了共享的会话密钥,双方以后就可以用该会话密钥进行加密通信。

2 Kerberos的安全分析

Kerberos协议设计精巧,优点突出,但分析其认证过程,主要存在以下安全问题[1,5]:

(1)口令猜测攻击问题。

在Kerberos中,当用户C向AS服务器请求获取访问TGS的票据TGT时,AS发往客户C的报文是由从客户口令产生的密钥Kc来加密的。而用户密钥Kc是采用单向Hash函数对用户口令进行加密后得到的,这样攻击者就可以收集大量的TGT,通过计算和密钥分析来进行口令猜测。当用户选择的口令不够强时,就不能有效地防止口令猜测攻击。

(2)时钟同步攻击问题。

在Kerberos中,为了防止重放攻击,在票据和认证符中都加入了时戳,这就要求客户、AS服务器、TGS服务器和应用服务器的机器时间要大致保持一致,一旦时间差异过大,认证就会失败。这在分布式网络环境下其实是很难达到的。由于变化的和不可预见的网络延迟的本性,不能期望分布式时钟保持精确的同步。同时时戳也带来重放攻击的隐患。

3 基于公钥密码体制的Kerberos协议改进

利用密码技术来设计安全的认证系统,应考虑到信息的完整性、新鲜性、信息重放等问题。当一个认证主体接收到一个消息时,首先,需要识别出信息在传输过程中有没有被修改过;其次,需要判断信息发送时间,以便断定信息是否仍有意义;最后,要对发送信息的主体进行认证[6]。

根据上述安全准则,结合认证与密钥分配协议的特点,文中采用公钥密码技术对Kerberos协议进行改进。

在本认证系统中,每个客户端都有一对非对称的加密密钥。客户端的公开密钥可对所有人公开,而私有密钥则

需要由客户安全持有,私有密钥以文件形式存放。每个客户有一个口令,根据该口令可生成客户的加密密钥,加密私有密钥文件。同时需要说明的是,改进协议流程中的其他处理步骤没有发生变化。这样一方面增强了用户密钥的安全性,同时避免了由于Kerberos系统本身作大量的改动而可能导致的问题。

首先对符号说明如下:

PrvKx:x的私有密钥;PubKx:x的公开密钥;

Kx,y:x,y的共享密钥;{m}k:用密钥k加密消息m。

改进协议模型与Kerberos协议模型类似,内容如下:

(1)C→AS:

{c,{tgs,Kc,as}PrvKc}PubKas

客户端登录系统后,向AS发送请求,用来申请TGT,以便将来用于申请服务,而不必再在申请服务时输入口令。请求报文包括客户名C,TGS名,AS给客户端C的应答消息的共享密钥Kc,as。其中Kc,as由客户端随机生成,作用是替代原协议中的时间戳。从KDC返回的应答消息由此Kc,as加密,用来保证应答消息是KDC新生成的,而不是进攻者的消息重发。在原Kerberos协议中,此请求报文是明文发送的,未经加密。进攻者可据此进行流量分析,破获信息。因此,在改进协议中,对报文进行了加密。

消息先用客户端C的私钥PrvKc签名,以证明消息确实是由客户端C发出的。然后用AS的公开密钥PubKas加密,保证AS并且只有AS能解开此消息,以确认AS的身份。客户端名C放在签名消息外,使得AS能得知消息来自哪一个客户端,从而进行身份认证。

(2)AS→C:

{{Kc,tgs}Kc,as,Tc,tgs}

Tc,tgs={as,{Kc,tgs,c,tgs,addr,lifetime}PrvKas}PubKtgs

认证服务器AS在收到客户端的请求报文后,发回应答报文。应答报文中含有一个票据授权票,用于客户端提交给TGS。TGT首先用AS的私有密钥PrvKas签名,然后用TGS的公开密钥PubKtgs加密,使得只有TGS能解密相关信息。TGT包含客户端与TGS通信所用的会话密钥Kc,tgs及其他相关信息。应答报文中还包含由Kc,as加密的客户端与TGS通信的会话密钥Kc,tgs。客户端收到AS发来的消息后,用Kc,as解密,得到与TGS通信用的会话密钥Kc,tgs,保存Kc,tgs及TGT以供申请服务时用。当客户端需要申请某应用服务器的服务时,必须持有获取该服务的票据。

(3)C→TGS:

{Ac,tgs,Tc,tgs}

Ac,tgs={s,addr,lifetime,Nc}Kc,tgs

客户端在向TGS申请获取某应用服务器服务的票据时,向TGS发送请求信息,包括鉴别码Ac,tgs和提交TGS的票据Tc,tgs。Tc,tgs用来证明客户端的身份。鉴别码包括应用服务器名、生成的随机数等信息,用来申请应用服务器的票据,用客户端与TGS的会话密钥Kc,tgs加密。

TGS收到请求消息后,用其私有密钥PrvKtgs将Tc,tgs解密,获取客户端与其的会话密钥。TGS再用会话密钥将鉴别码Ac,tgs解开,并将鉴别码中的数据与TGT中的数据进行比较,从而可以相信TGT的发送者C就是TGT的实际持有者。

(4)TGS→C:

{{Kc,s,Nc}Kc,tgs,Tc,s}

Tc,s={tgs,{Kc,s,lifetime}PrvKtgs}PubKs

TGS生成应答报文,发回客户端。应答报文包括客户端将来用于递交给应用服务器的票据Tc,s,先用TGS私有密钥签名,以保证该票据是由TGS发出的。再用应用服务器的公开密钥加密,以保证只有该应用服务器才能解密出这个票据。该票据包含了客户端与应用服务器间的会话密钥及其他信息。

客户端收到应答报文后,用会话密钥Kc,tgs解开得到随机数信息Nc,与自己发给TGS的随机数相比较,若相等则知这是一条新消息。客户端保存用于获取应用服务器的票据Tc,s,以及两者间的会话密钥Kc,s。

(5)C→S:

{Ac,s,Tc,s}

Ac,s={c,addr,Nc}Kc,s

当客户端希望获得某应用服务器的服务,并且持有该应用服务器的有效票据时,可以向应用服务器发请求报文。请求报文包括客户端持有的该应用服务器的票据,以及鉴别码。鉴别码包含了随机数等信息,是用客户与该应用服务器的会话密钥加密的,用来保证客户端的确知道相互间的会话密钥,而不是非法获得的票据的重发。

应用服务器收到请求报文后,用私有密钥PrvKs解开票据,获取会话密钥,再进一步比较Tc,s和Ac,cs中的数据以验证客户端身份。

(6)S→C:

As,c={Nc}Kc,s

应用服务器验证了客户端身份后,若客户要求应用服务器证明身份,则可用会话密钥加密,发回随机数等信息,以证明应用服务器获得了TGS指定的会话密钥,证明其身份。至此,客户端C通过了身份认证,可以获取应用服务器的服务。

4 改进协议与原有协议的比较

从以上描述及认证过程可知,新协议较好地满足了安全准则,与原Kerberos协议相比较,新协议具有如下特点:

(1)采用公钥加密技术,便于密钥的管理和分配,对系统的安全性有极大的增强:有效地解决了口令猜测攻击,同时保证了认证速度[6]。

原协议中使用对称密码体制加密的信息,在改进协议

中改用非对称加密体制加密,即先用发送方的私有密钥加密,再用接收方的公开密钥加密,保证只有用接收方的私有密钥解密后,才能知道用什么公开密钥解密得到最终信息。

(2)改进后的协议采用随机数技术替代时间戳,避免了网络中时钟难于同步的问题。

当客户端 C 收到 TGS 发来的信息,用 C 与 TGS 之间的会话密钥解密得到的 Nc 与自己发给 TGS 的随机数相比,若相等则确认这是一条新消息,以此来防止重放攻击。

(3)原协议中客户端 C 与 TGS 间的会话密钥 Kc,tgs 用 C 的密钥 Kc 加密,而 Kc 由用户键入的口令导出,易被窃听和猜测攻击。

改进后的协议中改用 Kc,as 加密 Kc,tgs。Kc,as 为用户随机产生,每次都可能不同,增强了安全性。同时,从 AS 返回的应答信息用此密钥加密,保证应答信息是 AS 新生成的,防止重放攻击。

(4)在 Kerberos 协议中,认证服务器需访问数据库。数据库中存放了与所有客户通信用的密钥,一旦数据库被非法访问,则必须更换与所有用户通信的密钥;而改进协议中,数据库中只存放每个客户的公开密钥,即使数据库被非法访问,也不会带来太大的安全问题。

综上所述,改进后的 Kerberos 协议既保留了原有的优点,又克服了 Kerberos 协议模型的弱点,利用这样的协议系统用于网络间的认证、加密等安全控制,能较好地满足网络的安全需求。

5　结束语

文中在对 kerberos 协议的研究基础上,利用基于公钥体制的密码认证技术,改进现有的 kerberos 协议,摈弃原有协议的不足之处,设计出一个基于公钥密码体制的身份认证协议,使得整个协议的安全性和适用性得到进一步的提高。尽管文中对身份认证服务的协议设计与密码技术做了一些研究探索工作,但对这一领域的深入研究还有待进一步的努力。

参考文献:

[1] Schneier B. 应用密码学[M]. 吴世忠,祝世雄,张文政,等译. 北京:机械工业出版社,2000. 404－408.

[2] 段云所,魏仕民,唐礼勇,等. 信息安全概论[M]. 北京:高等教育出版社,2003. 108－112.

[3] Tanenbaum A S. 计算机网络(第 4 版)[M]. 潘爱民,徐明伟译. 北京:清华大学出版社,2004. 682－684.

[4] RFC 1510. The Kerberos Network Authentication Services (v5)[S]. 1993.

[5] 卢开澄. 计算机密码学[M]. 北京:清华大学出版社,2003. 363－370.

[6] 张玉清,王　磊,肖国镇. Needham－schroeder 公钥协议的模型检测分析[J]. 软件学报,2000,11(10):1348－1352.

(上接第 223 页)

中间件和构件技术,系统通过建立关键领域的审计构件库,组装完成审计数据的采集、分析和处理功能,同时可以动态地进行构件的装配。数据采集端使用了 Agent 技术,数据采集 Agent 能够根据数据采集目标,对目标环境进行持续的自动侦测和分析,并自主地决定采用适当采集规则进行数据采集,同时也使系统模型具有较好的容错性和防范攻击的特点[6]。

4　系统不足及改进

在系统构建于新的业务领域时,由于业务的不同,将会影响到具体的数据采集的方案以及数据挖掘模块的构建,系统的可重用性及可扩展性有待提高。备份恢复模块中的软件方法,由于其在查看数据、定位索引和数据挖掘模块中使用的频繁性,对系统效率影响较大,尤其表现在网络服务器本身负荷很重的时候。目前在大量受控终端方式下,传送器对数据传送的效率还比较差,且服务器的负载会比较大,可以考虑建立多传送器连接,定义多服务模式,但其中存在着对受控主机的 I/O 资源消耗比较大,以及对共享数据访问的互斥的问题。另外需要加强系统集成性,不仅考虑不同层面的安全审计技术集成,同时考虑与硬件的集成,比如目前很多防火墙/IDS 功能与交换机/路由器集成在一起。

5　结束语

文中提出的基于安全审计的监控系统,只是信息系统安全的一个环节,系统主要对网络中的应用层面进行审计监控,侧重对业务过程和内部审计行为的审计,系统还需要综合考虑涉及系统安全的其他方面,另外解决信息安全问题不能只从技术上考虑,必须形成对人、技术和操作三方面并举的安全策略,并将这种安全策略贯彻落实于信息安全当中,只有这样信息系统安全的长期性和稳定性才能有所保证。

参考文献:

[1] 李　文. 计算机监控系统及发展趋势分析[J]. 计算机应用与软件,2004(3):75－77.

[2] 王伟钊,李　承,李家滨. 网络安全审计系统的实现方法[J]. 计算机应用与软件,2002(11):24－26.

[3] 王崇霞. 数据库双机热备份系统解决方案[J]. 微机发展,2003,13(S):79－85.

[4] 周洪昊,张　剡,柏文阳. 安全审计系统的设计和实现[J]. 计算机应用研究,2004(7):105－107.

[5] Han Jiawei, Kambr M. 数据挖掘概念与技术[M]. 范　明,孟小峰,等译. 北京:机械工业出版社,2004.

[6] 刘　姝,姜　浩,姜文峰. 多 Agent 技术在入侵检测中的应用[J]. 微机发展,2003,13(12):50－52.