计算机研究与发展
Journal of Computer Research and Development

ISSN 1000-1239/CN 11-1777/TP
42(9): 1587~1593, 2005

# 安全域间信息资源访问的协议和方法

彭双和[1,3] 韩 臻[1] 沈昌祥[2]
[1](北京交通大学计算机与信息技术学院 北京 100044)
[2](海军计算技术研究所 北京 100841)
[3](北京机械工业学院 北京 100085)
(shhpeng@sohu.com)

# Security Protocol and Scheme for Inter-Realm Information Accessing

Peng Shuanghe[1,3], Han Zhen[1], and Shen Changxiang[2]
[1](*School of Computer and Information Technology, Beijing Jiaotong University, Beijing* 100044)
[2](*Institute of Naval Computer Technology, Beijing* 100841)
[3](*Beijing Institute of Mechanical Technology, Beijing* 100085)

**Abstract** In order to improve the security of Intranet, application boundary security devices must be set. In order to access resources in different application areas on Internet in a security way, authentication is the first key step. Kerberos is an authentication protocol that is widely used. It is applied in application boundary security devices such as socks5. But there exists some limitation. In the processing of authentication between application boundary security devices, the object authenticated by application boundary security device at resource realm is not client which requests the resource, but application boundary security device at principal realm. So the object audited by application boundary security device at resource realm isn't the really one. A new inter-realm authentication protocol and a new identity-passing protocol based on Kerberos v5 inter-realm authentication protocol are presented in this paper. The proposed protocols can not only supply the security audit for user's access requests at application boundary security devices but also improve the efficiency of communication system because it needs only two connections between realms and the connection is setup not by subjects and objects but by application boundary security device. The proposed scheme can solve the problem of security information transferring between enterprise networks which will expand its application boundary including current enterprise network.

**Key words** Kerberos authentication; application boundary; inter-realm authentication; identity passing

**摘 要** 为了保护内部网络的安全,必须设置应用边界安全设备. Internet 上不同的应用安全域间要实现信息资源的安全访问,首先需要认证. Kerberos 是目前比较常用的认证协议,一般的应用边界安全设备(如 Socks5)中就应用了该认证协议,但应用该协议存在一定的缺陷:在应用边界安全设备链的认证过程中,资源域中的应用边界安全设备认证对象是主体域中的应用边界安全设备,而不是真正发起资源请求的客户端,因此资源域中的应用边界安全设备审计的对象是主体域中的应用边界安全设备,而不是真正的客户端.在 Kerberos 域间认证的基础上,给出了新的域间认证协议以及身份传递协议,使用新的协议不仅能够提供应用边界安全设备对用户访问请求的安全审计而且只需要两次域间的网络连接,这两次域间网络连接不需要主体和客体直接进行,而是通过应用边界安全设备完成的,提高了系统的通信效率,扩大了该系统的应用范围,适合于现有的企业网环境,能有效地解决企业网与企业网之间的信息安全传输.

**关键词** Kerberos 认证;应用边界;域间身份认证;身份传递

**中图法分类号** TP393.04

**收稿日期**:2004-03-16;**修回日期**:2005-05-11

**基金项目**:国家"八六三"高技术研究发展计划基金项目(2002AA144020,2002AA1Z2101);国家"九七三"重点基础研究发展规划基金项目(TG1999035801)

## 1 引 言

在电子商务交易中,一个公司要访问另一个公司的资源时就存在跨公司的资源访问问题. 各公司都有自己的共享服务器(如数据库服务器、Web 服务器、邮件服务器等),为保护这些服务资源免受非授权用户(如非法接入的非可信终端)的访问,需在公司的安全域边界设置应用边界安全设备,对访问共享资源的用户进行身份认证和安全审计,以保护公司内部的共享服务资源. 应用边界安全设备的用法如图 1 所示:

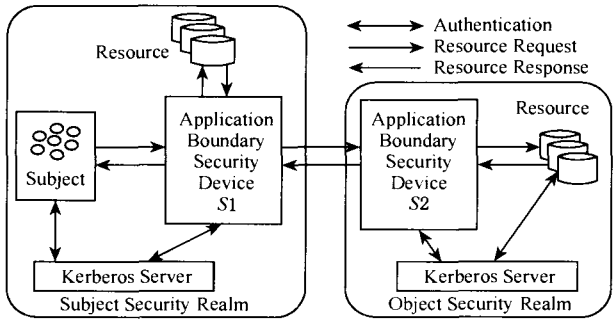


Fig. 1 Security resource access between realms based on application boundary security device.

图 1 基于应用边界安全设备的域间信息资源的安全访问

主体安全域中的主体想访问资源时,首先向本地的应用边界安全设备发出资源访问请求,本地的应用边界安全设备对用户的资源请求进行检查,若判断出主体请求的是本地的资源,则对主体认证后,检索本地的相关资源返回给主体;若请求的是远程的资源,则需联合远程的应用边界安全设备对主体的访问请求进行审查,若允许则转发本地主体的资源访问请求至远程的应用边界安全设备,最后由远程的应用边界安全设备获取资源后返回给主体域中的主体.

由上述过程看出,应用边界安全设备为用户提供服务时必须验证用户的身份,以确保只有经授权的合法用户才能得到相关的服务. 因此,我们需要对信息系统的每一个使用者都经过可信终端认证和授权,使其操作都是符合规定的. 由于可信终端的资源访问请求需经由 Internet 才能最终到达提供资源服务的目的端,我们还需确保资源访问请求在传输的过程中不被窃听和插入,这样就不会产生攻击共享服务资源的事故,确保整个信息系统的安全.

现有的方法在实现安全的跨域间的信息资源访问时尚存在不足. 例如,Kerberos 提供跨域间的身份认证功能,其域间身份认证步骤如图 2 所示[1]:

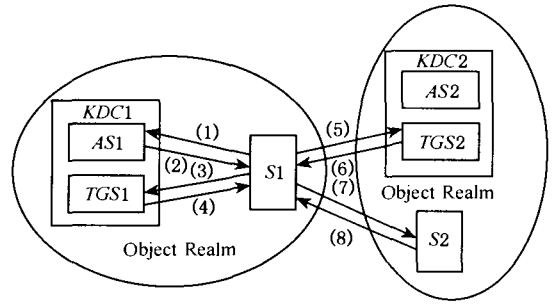


Fig. 2 Authentication between realms using Kerberos.

图 2 Kerberos 域间的身份认证

Kerberos 环境中有一个极为安全的计算机,我们称之为密钥分配中心 KDC(key distribution center). 该机用来保存用户口令和访问权限,逻辑上由两部分组成,一个是认证服务 AS(authentication service),另一个是票据服务 TGS(ticket granting service). 网络上所有的计算机和用户都要依赖这个服务器提供的认证与授权信息使用网络资源,而网络中所有其他的计算机都是不可信任的.

Kerberos 服务使用两类凭证[2-4]:票据(ticket)和鉴别码(authenticator). 票据用于秘密地向应用服务器发送持有票据用户的身份识别,票据中包括有一些信息,应用服务器能够用这些信息来确认使用票据的客户与发给票据的客户是同一个客户. 票据是由票据服务 TGS 产生的,票据的格式为

$$T_{c,s} = S, \{C, a, v, K_{c,s}\} K_s,$$

其中,$S$ 表示服务器,$C$ 表示客户,$a$ 表示客户的网络地址,$v$ 表示票据的有效起止时间,$K_{c,s}$为 $C$ 与 $S$ 的会话密钥. 这些信息用服务器的秘密密钥 $K_s$ 加密.

鉴别码是另外一个凭证,与票据一道发送. 鉴别码是由客户产生的. 鉴别码的格式为

$$A_c = \{c, t, key\} K_{c,s},$$

其中包括用户名 $c$,时戳 $t$ 以及一个可选的附加会话密钥 $key$,它们用服务器与客户共享的会话密钥 $K_{c,s}$加密. 客户在每次需要使用服务器上的服务时都要产生一个鉴别码.

主体域中的 $S1$ 与客体域中的 $S2$ 间的 Kerberos 域间的身份认证的步骤如下:

(1) $S1$ 向本地的认证服务器 $AS1$ 申请访问本地的 $TGS1$ 服务器的初始票据:

$S1 \rightarrow AS1$: $S1, TGS1, n$,

其中,$n$ 是防止重放攻击而设的 $nonce$.

(2) 本地认证服务器 $AS1$ 向 $S1$ 返回访问

$TGS1$ 的初始票据 $\{T_{S1,TGS1}\}K_{TGS1}$ 及同 $TGS1$ 通信的会话密钥,会话密钥以 $S1$ 的私钥加密后返回.

$AS1 \rightarrow S1: \{K_{S1,TGS1}, n\}K_{S1}, \{T_{S1,TGS1}\}K_{TGS1}$.

(3) $S1$ 向 $TGS1$ 申请访问远地 $TGS2$ 的票据:

$S1 \rightarrow TGS1: \{A_{S1}\}K_{S1,TGS1}, \{T_{S1,TGS1}\}K_{TGS1}, TGS2, n$.

(4) 本地 $TGS1$ 返回给 $S1$ 访问远地 $TGS2$ 的票据以及会话密钥:

$TGS1 \rightarrow S1: \{K_{S1,TGS2}\}K_{S1,TGS1}, \{T_{S1,TGS2}\}K_{TGS2}$.

(5) $S1$ 向远程的 $TGS2$ 申请访问远程应用服务 $S2$ 的票据及会话密钥:

$S1 \rightarrow TGS2: \{A_{S1}\}K_{S1,TGS2}, \{T_{S1,TGS2}\}K_{TGS2}, S2, n$.

(6) 远程 $TGS2$ 返回给 $S1$ 访问远地应用服务 $S2$ 的票据以及会话密钥:

$TGS2 \rightarrow S1: \{K_{S1,S2}\}K_{S1,TGS2}, \{T_{S1,S2}\}K_{S2}$.

(7) 本地 $S1$ 向远程应用服务 $S2$ 提出访问请求:

$S1 \rightarrow S2: \{A_{S1}\}K_{S1,S2}, \{T_{S1,S2}\}K_{S2}, N$.

(8) 远程应用服务 $S2$ 对 $S1$ 提出的访问请求进行认证后,向 $S1$ 返回请求应答,进而实现了客户与服务的双向认证.

$S2 \rightarrow S1: \{N+1\}K_{S1,S2}$.

可以看出,该协议不适合于图 1 的应用边界安全设备应用环境,其原因有两点:①$S1$ 若想跟 $S2$ 进行认证的话,需要进行 4 次跨域间的连接,开销较大;②在图 1 所示的环境下,$S1$ 只能跟 $S2$ 进行通信,不能直接跟 $TGS2$ 建立网络连接. 本文对现有的 Kerberos 域间身份认证协议进行修改,提出了适合于图 1 所示环境的域间安全认证方法.

## 2 应用边界安全设备间的认证和域间信息的安全传输

我们在 Kerberos 域间身份认证的基础上,对之进行了修改,修改后的域间身份认证模型如图 3 所示. 这里我们将主体域中的应用边界安全设备 $S1$ 当成客户端,客体域中的应用边界安全设备 $S2$ 当成应用服务端.

要实现安全域间的信息安全传输,应用边界安全设备之间需要进行相互认证以及会话密钥的协商.首先,主体域与客体域中的 $KDC$ 之间必须建立起共同的会话密钥 $K_{KDC1,KDC2}$. $KDC$ 之间的会话密钥建立好以后,主体域与客体域中两个应用边界安全设备之间的身份认证和密钥协商过程如下:

(1) $S1$ 向本地的认证服务器 $AS1$ 申请访问本地的 $TGS1$ 服务器的初始票据:

$S1 \rightarrow AS1: S1, TGS1, n$,

其中,$n$ 是 $nonce$,防止重放攻击.

(2) 本地认证服务器 $AS1$ 向 $S1$ 返回访问 $TGS1$ 的初始票据 $\{T_{S1,TGS1}\}K_{TGS1}$ 及同 $TGS1$ 通信的会话密钥,会话密钥以 $S1$ 的私钥加密后返回.

$AS1 \rightarrow S1: \{K_{S1,TGS1}, n\}K_{S1}, \{T_{S1,TGS1}\}K_{TGS1}$.

(3) $S1$ 向 $TGS1$ 申请访问远地 $S2$ 的票据:

$S1 \rightarrow TGS1: \{A_{S1}\}K_{S1,TGS1}, \{T_{S1,TGS1}\}K_{TGS1}, S2, n$.

(4) 本地 $TGS1$ 返回给 $S1$ 访问远地 $S2$ 的票据以及会话密钥:

$TGS1 \rightarrow S1: \{S1, S2, N, K_{S1,S2}\}K_{KDC1,KDC2}, \{K_{S1,S2}\}K_{S1,TGS1}$.

(5) $S1$ 向远地 $S2$ 提出访问请求:

$S1 \rightarrow S2: S1, S2, \{S1, S2, K_{S1,S2}\}K_{KDC1,KDC2}, \{A_{S1}, N\}K_{S1,S2}$.

(6) $S2$ 接收到 $S1$ 发来的访问请求后,由于票据 $\{S1, S2, K_{S1,S2}\}K_{KDC1,KDC2}$ 是由 $K_{KDC1,KDC2}$ 加密了的,$S2$ 不能解密该票据,只有域间的 $KDC$ 共享 $K_{KDC1,KDC2}$,于是 $S2$ 向本地的认证服务器 $AS2$ 申请访问本地的 $TGS2$ 服务器的初始票据:

$S2 \rightarrow AS2: S2, TGS2, n$.

(7) 本地的认证服务器 $AS2$ 向 $S2$ 返回访问 $TGS2$ 的初始票据 $\{T_{S2,TGS2}\}K_{TGS2}$ 及同 $TGS2$ 通信的会话密钥,会话密钥以 $S2$ 的私钥加密后返回.

$AS2 \rightarrow S2: \{K_{S2,TGS2}, n\}K_{S2}, \{T_{S2,TGS2}\}K_{TGS2}$.

(8) $S2$ 得到访问 $TGS2$ 的初始票据 $\{T_{S2,TGS2}\}K_{TGS2}$ 及同 $TGS2$ 通信的会话密钥后,于是向本地 $TGS2$ 进行认证,并转发第(5)步从 $S1$ 发来的访问请求票据 $\{S1, S2, K_{S1,S2}\}K_{KDC1,KDC2}$ 给 $KDC2$.

$S2 \rightarrow TGS2: \{A_{S2}\}K_{S2,TGS2}, \{T_{S2,TGS2}\}K_{TGS2}, \{S1, S2, K_{S1,S2}\}K_{KDC1,KDC2}$.

(9) $TGS2$ 认证完 $S2$ 后,用 $K_{KDC1,KDC2}$ 解密 $\{S1, S2, K_{S1,S2}\}K_{KDC1,KDC2}$,得到 $K_{S1,S2}$,并向 $S2$

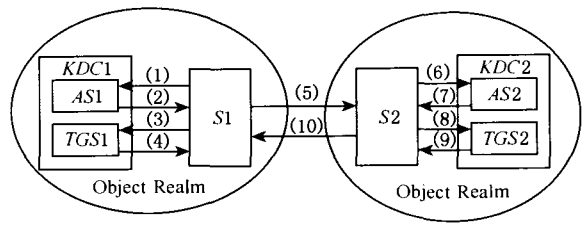


Fig. 3 Authentication and session key negotiated between $S1$ and $S2$.

图 3 $S1$ 与 $S2$ 之间的身份认证以及会话密钥的协商

返回 $S1$ 同 $S2$ 通信的会话密钥 $K_{S1,S2}$:

$TGS2 \rightarrow S2: \{K_{S1,S2}\}K_{S2,TGS2}$.

(10) $S2$ 得到同 $S1$ 的会话密钥后,解密第(4)步 $S1$ 发来的证 $\{A_{S1}, N\}K_{S1,S2}$,认证完 $S1$ 后,向 $S1$ 返回如下的信息:

$S2 \rightarrow S1: \{N\}K_{S1,S2}$.

这样,主体域中的应用边界安全设备 $S1$ 与客体域中的应用边界安全设备 $S2$ 之间实现了相互的身份认证,并拥有了共同的会话密钥 $K_{S1,S2}$. 两应用边界安全设备可以利用协商的会话密钥 $K_{S1,S2}$ 实现信息的安全传输.

## 3 身份传递及域间资源的安全访问

上面给出的基于 Kerberos v5 的新协议实现了应用边界安全设备之间的身份认证及会话密钥的协商. 但是,正如图 1 所示,真正的访问请求发起者和服务提供者不是应用边界安全设备,而分别是主体域中的主体 $C$ 和客体域中的客体 $B$. 主体域中的应用边界安全设备 $S1$ 只是代理主体 $C$ 发出对客体域中的资源 $B$ 的访问请求. 客体域中的应用边界安全设备 $S2$ 也只是代理客体 $B$ 接收主体 $C$ 对资源的访问. 若该资源访问请求被许可的话,对该资源访问请求的审计应该针对的是主体 $C$ 而不是应用边界安全设备 $S1$. 因此,我们首先需要解决主体 $C$ 与应用边界安全设备 $S1$ 之间的身份认证. 身份认证完成后,主体 $C$ 才将自己的身份以及与本地 $TGS1$ 通信的会话密钥及初始票据通过安全通道传递给 $S1$,使 $S1$ 能代理主体 $C$ 同外界通信,同时又不泄露主体 $C$ 的秘密信息 $K_C$. 同样,客体域中的客体 $B$ 也需要与应用边界安全设备 $S2$ 之间进行身份认证,身份认证完后,客体 $B$ 才授权应用边界安全设备 $S2$ 对资源的访问请求进行检查,并将自己与本地 $TGS2$ 通信的会话密钥及初始票据通过安全通道传递给 $S2$,使 $S2$ 能代理客体 $B$ 同外界通信,同时又不泄露客体 $B$ 的秘密信息 $K_B$.

我们假设主体域中的主体 $C$ 想访问客体域中的服务 $B$. 要完成这个服务主要进行 4 个步骤:

(1) 主体域中的主体与边界安全设备的身份认证以及主体的身份传递;

(2) 主体域中的边界安全设备代理主体向客体域中的客体资源发出访问请求;

(3) 客体域中的应用边界安全设备与客体资源的身份认证以及应用边界安全设备对资源的代理;

(4) 客体域中的边界安全设备代理客体资源向主体返回请求应答.

### 3.1 主体 C 的身份传递及其资源访问请求的转发

协议步骤如图 4 所示:

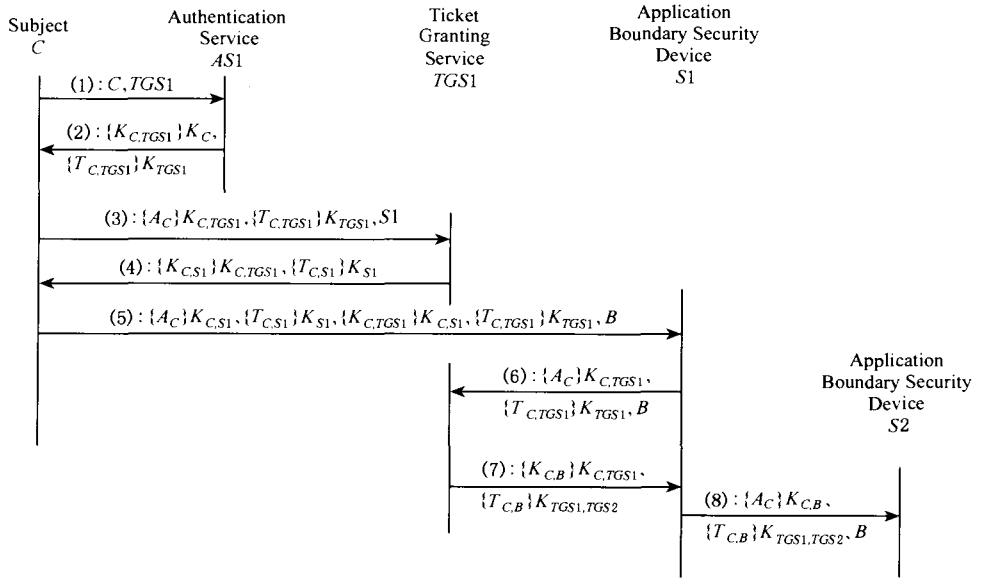


Fig. 4 Passing of subject C's identity and transmitting of resource request.

图 4 主体 C 的身份传递及其资源访问请求的转发

主体 $C$ 与应用边界安全设备 $S1$ 之间的身份认证及主体 $C$ 的身份传递协议如图 4 步骤(1)~(5)所示.

首先,主体 $C$ 向本地 Kerberos 服务器获取同本地应用边界安全设备 $S1$ 通信的会话密钥和票据,具体步骤如图 4 步骤(1)~(4)所示.

(1) $C \rightarrow AS1: C, TGS1$

$C$ 向$AS1$申请获取访问 $TGS1$ 的初始票据.

(2) $AS1 \rightarrow C: \{K_{C,TGS1}\}K_C, \{T_{C,TGS1}\}K_{TGS1}$

$AS1$返回给 $C$ 访问 $TGS1$ 的初始票据以及会话密钥.

(3) $C \rightarrow TGS1: \{A_C\}K_{C,TGS1}, \{T_{C,TGS1}\}K_{TGS1}, S1$

$C$ 向 $TGS1$ 申请访问本地应用边界安全设备 $S1$ 的票据和会话密钥.

(4) $TGS1 \rightarrow C: \{K_{C,S1}\}K_{C,TGS1}, \{T_{C,S1}\}K_{S1}$

$TGS1$ 返回给 $C$ 同本地应用边界安全设备 $S1$ 通信的会话密钥和票据.

上述的(1)~(4)步表示 $C$ 向 $AS1$ 认证自己的身份并获取了访问本地应用边界安全设备 $S1$ 的票据和会话密钥.

由于 $C$ 不能跟远程的 $B$ 直接建立连接,于是 $C$ 便委托本地应用边界安全设备 $S1$ 发起访问远程资源 $B$ 的请求. 如步骤(5)所示.

(5) $C \rightarrow S1: \{A_C\}K_{C,S1}, \{T_{C,S1}\}K_{S1}, \{K_{C,TGS1}\}K_{C,S1}, \{T_{C,TGS1}\}K_{TGS1}, B$

其中,前两项$\{A_C\}K_{C,S1}, \{T_{C,S1}\}K_{S1}$用于向本地应用边界安全设备 $S1$ 证实自己的身份以及访问本地应用边界安全设备 $S1$ 的票据. 后 3 项$\{K_{C,TGS1}\}K_{C,S1}, \{T_{C,TGS1}\}K_{TGS1}, B$ 用于委托本地应用边界安全设备$S1$ 发起访问远程资源 $B$ 的请求.

本地应用边界安全设备 $S1$ 收到上述委托请求后,首先验证 $C$ 的身份,并通过解密服务票据$\{T_{C,S1}\}K_{S1}$得到同 $C$ 通信的会话密钥 $K_{C,S1}$,并由会话密钥 $K_{C,S1}$解密$\{K_{C,TGS1}\}K_{C,S1}$,得到 $K_{C,TGS1}$. 这样,$S1$ 便拥有了 $C$ 同 $TGS1$ 通信的会话密钥 $K_{C,TGS1}$和票据$\{T_{C,TGS1}\}K_{TGS1}$,同时 $C$ 的秘密密钥$K_C$ 并未泄漏给 $S1$. $S1$ 拥有了 $C$ 同 $TGS1$ 通信的会话密钥 $K_{C,TGS1}$和票据$\{T_{C,TGS1}\}K_{TGS1}$后,便可以代理 $C$ 同外部进行通信.

$S1$ 代理 $C$ 同外界进行通信,并将 $C$ 的身份传递给 $S2$,分析如图 4 步骤(6)~(8)所示:

(6) $S1 \rightarrow TGS1: \{A_C\}K_{C,TGS1}, \{T_{C,TGS1}\}K_{TGS1}, B$

$S1$ 代理 $C$ 向 $TGS1$ 请求同应用服务器 $B$ 进行通信,并向 $TGS1$ 证实 $C$ 的身份.

(7) $TGS1 \rightarrow S1: \{K_{C,B}\}K_{C,TGS1}, \{C, B, T_{C,B}\}K_{KDC1,KDC2}$

$TGS1$ 返回给 $S1$, $C$ 访问 $B$ 的服务票据$\{C, B, T_{C,B}\}K_{KDC1,KDC2}$和会话密钥 $K_{C,B}$.

(8) $S1 \rightarrow S2: \{A_C\}K_{C,B}, \{C, B, T_{C,B}\}K_{KDC1,KDC2}, B$

$S1$ 代理 $C$ 向 $S2$ 请求同 $B$ 进行通信,并向 $S2$ 证实 $C$ 的身份.

### 3.2 应用边界安全设备对客体 $B$ 的代理以及主、客体会话密钥的协商

客体域中的安全边界设备与客体的身份认证以及安全边界设备对客体的代理如图 5 所示.

其中步骤(1)~(4)可以和图 4 并行执行,作用和图 4 中步骤(1)~(4)的类似. 即客体 $B$ 向本地的 $KDC$ 申请同安全边界设备 $S2$ 通信的会话密钥和票据. 图 5 步骤(5)可以和图 4 步骤(5)作用类似. 即

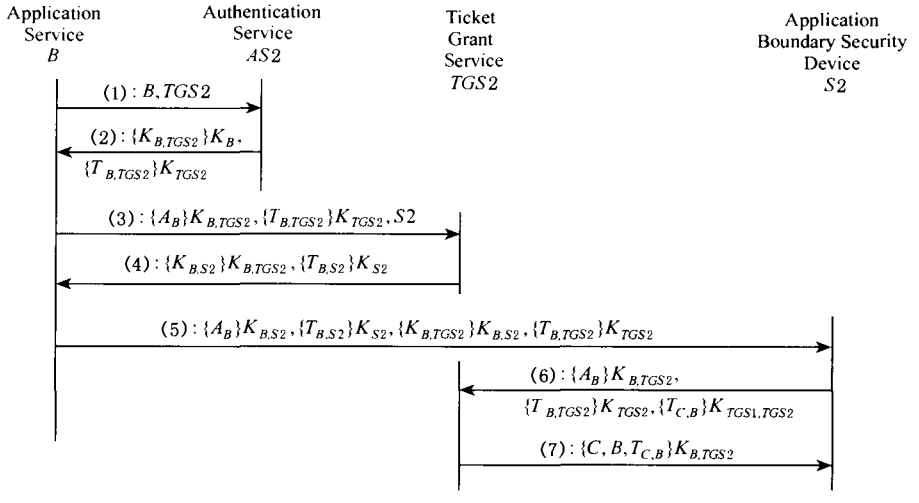


Fig. 5 Application boundary security device's action as object B and session key negotiated between subject and object.

图 5 应用边界安全设备对客体 $B$ 的代理以及主、客体会话密钥的协商

客体 $B$ 委托安全边界设备 $S2$ 向外界提供服务. 安全边界设备 $S2$ 获取了 $B$ 同 $TGS2$ 通信的会话密钥. 由此, $S2$ 可以代理 $B$ 同外界进行通信.

应用边界安全设备 $S2$ 代理 $B$ 向 $KDC$ 请求返回 $B$ 同主体 $C$ 通信的会话密钥 $K_{C,B}$. 如图 5 步骤(6)~(7)所示:

(6) $S2 \rightarrow TGS2$: $\{A_B\}K_{B,TGS2}$, $\{T_{B,TGS2}\}K_{TGS2}$, $\{C,B,T_{C,B}\}K_{KDC1,KDC2}$

$S2$ 代理 $B$ 向 $TGS2$ 进行认证, 并要求返回 $C$ 与 $B$ 通信的会话密钥.

(7) $TGS2 \rightarrow S2$: $\{C,B,T_{C,B}\}K_{B,TGS2}$

$TGS2$ 返回给 $S2$, $C$ 与 $B$ 通信的会话密钥 $K_{C,B}$. 这样, $S2$ 就得到了主体 $C$ 同客体 $B$ 通信的会话密钥 $K_{C,B}$.

于是, 当 $C$ 想访问客体域中的资源时, 可以用密钥 $K_{C,B}$ 将信息加密, 然后, 通过应用边界安全设备 $S1$ 再将加密的信息转发给客体域中的应用边界安全设备 $S2$, 在 $S2$ 端将加密的信息解密, 若资源访问请求经过 $S2$ 的访问控制策略检查, 表示允许, 那么 $S2$ 便可将资源访问请求转发到具体的客体(即应用服务器), 进行相关资源的访问, 并将访问到的资源经过会话密钥 $K_{C,B}$ 加密后返回给主体 $C$. 主体 $C$ 用会话密钥 $K_{C,B}$ 解密资源信息, 便得到了所要请求的资源.

## 4 安全性、效率分析

### 4.1 安全性分析

在本文提出的新协议及方法中, 资源的访问请求以及资源的返回都是用会话密钥 $K_{C,B}$ 加密的, 窃听者即使从网络上截获了这些信息, 由于无法得到主体 $C$ 与客体 $B$ 的会话密钥 $K_{C,B}$, 因此, 也无法解密截获的信息; 主体 $C$ 在向应用边界安全设备 $S1$ 传递自己的身份和 $TGS1$ 通信的会话密钥时是以会话密钥 $K_{C,S1}$ 加密的, 网络窃听者不能获取 $C$ 与 $TGS1$ 的会话密钥 $K_{C,TGS1}$, 而且主体在传递这些信息时, 没有泄露自己的秘密信息 $K_C$, 这样便保证了主体身份传递的安全性. 客体域中客体 $B$ 与应用边界安全设备的认证与身份传递的分析也类似.

但由于该系统采用的是基于 Kerberos 的域间认证机制, 必然会存在 Kerberos 系统的局限性, 其局限性表现在: ①在分布式系统中, 认证中心星罗棋布, 域间会话密钥的数量惊人, 密钥的管理、分配、存储都是很严峻的问题; ②Kerberos 防止口令猜测攻击的能力很弱, 攻击者可以收集大量的许可证, 通过计算和密钥分析进行口令猜测. 当用户选择的口令不够强时, 更不能有效地防止口令猜测攻击.

### 4.2 效率分析

由第 1 节 Kerberos 域间的身份认证可知, 现有的 Kerberos V5 域间认证需要进行 4 次域间的网络连接, 而本文在此基础上, 对之进行修改后提出的域间身份认证方法只需要两次域间的网络连接, 这样便提高了系统的通信效率. 而且这两次的域间网络连接不需要主体和客体直接进行, 而是通过应用边界安全设备完成的. 也就是说, 主体域中的主体想访问客体域中的资源时, 只要求主体域中的应用边界安全设备与客体域中的应用边界安全设备能直接通信即可, 不需要主体与客体的直接网络连接. 这样, 便扩大了该系统的应用范围, 适合于现有的企业网环境, 能有效解决企业网与企业网之间的信息安全传输. 上述模型中, 我们采用 Socksv5[5] 服务器作为应用边界安全设备的实现平台. Socksv5 能有效地代理客户端和应用服务器完成跨域间的信息资源的安全访问.

## 5 结束语

本文提出的基于 Kerberos 认证的安全的跨域间的信息资源访问模型能有效地利用现有的技术, 较好地解决跨域的资源安全访问问题. 正如第 4 节所述, 该系统也有一定的不足, 我们以后的改进方向是在用户身份认证方面增加双因子认证, 使用智能卡以增强用户的密钥安全; 在原有 Kerberos 服务的基础上增加权限分配的功能, 主体能向应用边界安全设备传递角色信息, 使应用边界安全设备能代理主体以特定的角色发起对客体域中资源的访问请求; 使应用边界安全设备中增加基于角色的访问控制策略.

## 参 考 文 献


1 John T. Kohl, B. Clifford Neuman, *et al*. The evolution of the Kerberos authentication system. In: Distributed Open Systems. Los Alamitos, CA: IEEE Computer Society Press, 1994. 78~94

2 B. Clifford Neuman, Theodore Y. Ts' o. Kerberos: An authentication service for computer networks. IEEE Communications, 1994, 32(9): 33~38

3 Ian Downard. Public-key cryptography extensions into Kerberos. IEEE Potentials, 2002, 21(5): 30~34

4 M. Steven. Bellovin, Michael Merritt. Limitations of the Kerberos authentication system. Computer Communication Review, 1990, 20(5): 119~132

5 M. Leech, M. Ganis, Y. Lee, *et al*. SOCKS Protocol Version 5. RFC1928. http://archive. socks. permeo. com/rfc/rfc1928. txt, 1996

**Peng Shuanghe**, born in 1974. Ph. D. candidate. Her main research interests include: information and network security.

**彭双和**,1974 年生,博士研究生,讲师,主要研究方向为信息与网络安全.

**Han Zhen**, born in 1962. Professor. His research interests include graphics, information and network security.

**韩臻**,1962 年生,教授,主要研究方向为图形学、信息与网络安全(hz@computer. njtu. edu. cn).

**Shen Changxiang**, born in 1940. Professor and Ph. D. Supervisor, Member of the Chinese Academy of Engineering, His research interests include secure operation system and architecture of information system.

**沈昌祥**,1940 年生,教授,博士生导师,中国工程院院士,主要研究方向为安全操作系统、信息安全体系结构.

**Research Background**

In order to improve the security of Intranet, application boundary security devices must be set. In order to access resources in different application areas on Internet in a security way, authentication is the first key step. In the processing of authentication between application boundary security devices, the object authenticated by application boundary security device at resource realm is application boundary security device at subject realm. So the object audited by application boundary security device at resource realm isn't the real one. A new inter-realm authentication protocol and a new identity-passing protocol based on Kerberos v5 inter-realm authentication protocol are presented in this paper. The proposed protocols can solve the problem of security audit for user's access requests at application boundary security devices. As analyzed by section 4, there are some space to improve in this paper. Future work such as adding two factors authentication by using smart card and adding priviledge allocation function and RBAC(role based access control) etc. will be included into this system. The work is supported by the Chinese National Advanced Science and Technology 863 Grant (2002AA144020, 2002AA1Z2101) and 973 Research Foundation Grant (TG1999035801).