利用 Kerberos 协议实现端到端的网络安全系统

Kerberos Protocol is Used to Realize Site to Site Security of Network

张金玲　卿斯汉

(中科院信息安全工程研究中心　北京100080)

Abstract　With the development of network technology, experienced IT personnel have realized that in order to protect private network and useful information from vicious attack, not only access control but also encryption techniques must be implemented in security system. In this essay, a KVPN system based on Kerberos protocol is advanced to realize site to site security of network, and strongpoint in several aspects of this system is discussed in detail.

Keywords　Kerberos, VPN, Authentication, Access control

一、前言

目前 保证网络私有性的最有效方法是利用 VPN 技术建立虚拟私有网。但是，目前的 VPN 技术中存在着诸多的不足之处，主要表现在以下几个方面：

(1)信息的保密性无法保障。VPN 技术的最为重要的作用在于对机密信息进行保密，然而通常这些 VPN 对传输数据的保密性仅限于两个安全网关之间的通路上，在内部网中，所有信息都以明文的形式在整个局域网中广播，造成巨大的安全隐患。

(2)密钥交换过程复杂、管理烦琐。VPN 技术得以运行的一个重要前提是在位于不同地点的子网之间交换 SA，建立策略库，主要有两种方式：手工配置和 IKE 协商。利用手工进行安全关联库的生成，操作上比较简单，但效率极低；而利用 IKE 协议进行协商过程又相当烦琐。不能有效地交换密钥是目前 VPN 技术未能得到普遍应用的主要因素所在。

(3)降低了网络性能。网络中的所有安全操作都集中在安全网关处，这样在网关处就会造成传输的显著延迟，整个网络的性能降低了。

(4)由于 Ipv4的不安全性，极有可能造成检索条件被伪装；对同一台主机上的不同用户无法区分。

基于此种现状，我们通过借鉴 Kerberos 协议和其他安全技术的思想提出了一种崭新架构的 VPN 系统 KVPN，它集内外网通讯数据的保密性、身份认证、安全控制等多种功能于一体，实现端到端的安全性。

二、系统组成

KVPN 系统从总体上包括四个主要部件：客户代理、服务代理、认证服务器(AS)和票据授予服务器(TGS)。

认证服务器(AS)和票据授予服务器(TGS)的功能同 Kerberos 协议中的定义基本相似，AS 利用其所在域中的认证数据库(该数据库中存放该域中所有的 principal 和它们的密钥，Principal 是代表身份的实体)认证数据身份，负责向用户分发向 TGS 证明自己身份的票据 TGT，TGS 为用户分发到最终目的地的 Ticket，客户代理利用这个 Ticket 向服务代理证明自己的身份，在实现上，AS 和 TGS 实际上是由同一程序完成的，它们的实现机制并没有太大区别，只是在加密所发出的 Ticket 时所使用的密钥不同，AS 使用用户的密钥，而 TGS 使用会话密钥。

客户代理运行于用户使用的客户端主机，工作于网络层，在用户申请服务时提示并接受用户登录，自动为用户向认证服务器和票据授予服务器申请相应票据，获得与服务器通讯的会话密钥，向服务代理发出票据，连接建立后负责封装、解封装及加解密传输数据，分别向服务器端和上层应用转发数据，必要时可以对服务端进行反向认证。

服务代理运行于服务器端主机，同样工作于网络层，主要用于验证客户代理所发送的票据，以决定是否向客户端提供服务，获取与客户端通讯的会话密钥，负责封装、解封装、加解密和转发数据。

KVPN 系统的逻辑结构示意图如下图1所示。

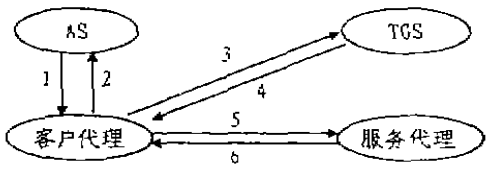

图1　系统结构

三、系统流程

在介绍系统的工作机制之前，先给出所用到的一些符号的含意：

c：客户端的 Principal；s：服务器端的 Principal；n：nonce，一个随机串；TGS：Ticket Granting Server；AS：Authentication Server；*Kx*：x 的密钥；*Kx*、*y*：x 和 y 的会话密钥；*Tx*、*y*：x 向 y 申请服务所用的 Ticket；{abc}*Kx*：用 x 的密钥加密 abc 后的结果；*Ax*：x 发出的用于对方验证自己身份的验证信息。

(1)**Client→AS**：**c**，**tgs**，**n**

用户登录 KVPN 系统时，客户代理提示用户输入并接受用户名和口令，客户代理用指定算法将该口令转化为客户端的私有密钥 Kc 备用，之后客户代理自动向 AS 发出请求，申请与 TGS 通讯的票据 TGT，Client 向 AS 发送的消息主要有：代表自己的 Principal "c"，代表所要连接的服务器端的 Principal"s"，以及一个随机串"n"。

(2)**AS→Client**：{*Kc*，**tgs**，**n**}*Kc*，{*Tc*，**tgs**}*Ktgs*

AS 收到客户代理发送的请求之后，发回应答信息，包括客户与 TGS 通讯的会话密钥 Kc，tgs 和客户用来提交给 TGS 的票据 Tc，tgs（即 TGT），其中会话密钥用客户私钥加密，使得只有客户本身才能正确解读该会话密钥，而 TGT 用 TGS 的私钥加密，使得只有 TGS 才能正确解读该票据。将客户发来的"n"加密后发回的作用是向客户端证明自己就是 AS，从而防止第三方欺骗。

(3)**Client→TGS**：{*Ac*}*Kc*，**tgs**，{*Tc*，**tgs**}*Ktgs*，**s**，**n**

当客户需要使用某一服务时，客户代理首先截获请求连接的 IP 包，并根据用户信息和 Socket 匹配以判断是否已具有与之匹配的 SA，若有且没有过期，则直接对该 IP 包进行有关的封装加密操作，然后发往服务端。否则客户代理用自己的私钥解密收到的 AS 应答信息，对 AS 的身份进行验证，获得并保存与 TGS 通讯的会话密钥及 TGT。然后客户代理将用会话密钥 *Kc*，tgs 加密的客户端的认证信息 Ac（包括用户名、套接字及命令等信息）、TGT、服务端 Principal"s"和一个随机串"n"（作用同第一步中的 n）发送到 TGS。

(4)**TGS→Client**：{*Kc*，**s**，**n**}*Kc*，**tgs**，{*Tc*，**s**}*Ks*

TGS 收到客户代理发来的请求之后，首先用自己的私钥 *Ktgs* 解密 TGT 获得与客户端通讯的会话密钥 Kc，tgs，以及有关客户端的信息，然后用 Kc，tgs 解密 Ac 并与前面的信息进行比较验证正确性，必要时可以通过检索 TGS 上的策略库来判断客户端到服务器端的请求是否被允许，判断允许后 TGS 随机生成客户端与服务器端的会话密钥 *Kc*，*s* 和票据 Tc，s，TGS 从数据库中取出 s 的密钥 Ks，经过一番加密后将{*Kc*，s，n}*Kc*，tgs 和{*Tc*，s}*Ks* 发送给客户端。

(5)**Client→Server**：{*Ac*}*Kc*，**s**，{*Tc*，**s**}*Ks*，**n**

客户代理收到 TGS 的应答，首先用 *Kc*，tgs 解密得到与服务器端通讯的会话密钥 *Kc*，*s* 并验证 TGS 的身份，之后将自己的有关认证信息用该密钥加密连同从 TGS 处得到的票据{Tc，s}*Ks* 发送到服务器端，服务代理将获得与客户端通讯的会话密钥并验证客户信息，验证通过后将会向上层转发，建立与客户端的连接，如果需要反向验证，则执行下一步。

(6)**Server→Client**：{**n**}*Kc*，**s**

连接建立后，客户端和服务器端利用 *Kc*，*s* 协商新的 SA。在以后的通讯中客户代理与服务代理会根据协商好的模式对截获的该连接上的 IP 包进行各种协议封装，以保证数据的保密性和有效性。

四、系统模型

在上面的讨论中，我们从概念上介绍了 KVPN 系统的总体结构和简要的工作机制，下面我们介绍一下该系统在实现上的构造模型、系统的结构模型如图2中所示。

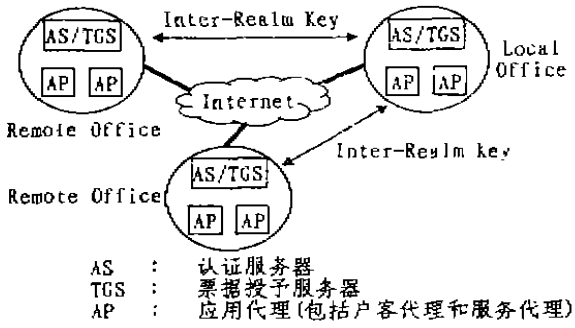

图2 系统模型

该系统继承了 Kerberos 协议中域的概念，系统中分布于不同物理地点的子网建立并维护自己相对独立的域，对应本地用户或应用服务的子集，为了实现用户与处于不同域的服务器之间的身份认证和安全传输，需要在不同管理域之间设立跨域密钥（Inter-Realm Key），在本域中被认证通过的用户或 IP 包可以直接使用与本域建立了信任关系的域中的服务，具体过程如下所述：

(1)首先，远端域中的 TGS 将自己在本地域中注册为一个 Principal；

(2)在本地域中要使用远端域中服务的客户在被本地域的 TGS 认证通过后，获得一张发往远端的 TGS 的票据，并将此票据附加到申请远端服务的请求中发送到远端域的 TGS；

(3)远端域中的 TGS 收到该请求后,首先用它在请求用户所在域中的密钥即跨域密钥 Inter-Realm Key 来解密用户的服务请求,确认票据的正确性,必要时可进行进一步的控制检查,然后该 TGS 发出客户所请求服务的票据给客户代理,客户端利用此票据与远端服务器进行通讯。

五、系统特色

(1)有效地保障内外网的安全 KVPN 系统将安全端点从传统的网关转移到各通讯主机,一方面,可以将信息的保密性延伸到传输层甚至应用层,防止了有用信息在网络内外以明文形式存在和传送,有效地防止了内外攻击者偷听机密信息;另一方面通过 TGS 上的策略库来过滤服务请求和连接,可以防止内网和外网用户的非法访问,防止来自内外网的各种形式的攻击。这样便实现了端到端的安全,这是本系统最重要的特点。

(2)灵活的密钥交换方式 系统通过采用 Kerberos 协议的认证模式,继承了 Kerberos 协议的密钥交换方式,即在对用户连接进行身份认证的票据交换过程中随机地交换会话密钥,从而可以方便地建立和更新 SA 数据库。这种密钥交换方式既保证了策略库的新时性,又避免了传统 VPN 技术中建立安全关联(SA)所必须进行的烦琐过程。

(3)提高了安全系统的效率 传统的 VPN 技术一般将安全控制点放于内外网的连接处,以便于对所有进出的连接进行安全处理,这势必在安全检查点处造成"瓶颈",降低安全系统的效率,造成很大的传输延迟。KVPN 系统通过将认证及加解密工作分布到各个端主机的应用代理上,使整个安全系统的负域得到均衡,使系统具有较高的效率。

(4)透明的认证代理 用户在登录完成后,所有的认证过程均由客户代理自动完成,它负责与 AS、TGS 及服务代理交换票据和认证信息的全过程,用户本身无须与认证服务器和服务代理进行任何连接,所以对用户是完全透明的。

(5)可以实现集中统一的控制和管理 KVPN 系统中,在 TGS 上保存有用于进行访问控制的策略库,TGS 根据策略库对用户连接请求进行统一的过滤,这样系统不仅可以保密传输信息也可以对进出网络的连接进行安全过滤,禁止非法访问,实现了保密与控制的统一。

(6)丰富全面的控制条件 由于本系统是基于 Kerberos 认证协议,所以可以提供用户身份信息,同时由于应用代理都工作于网络层,所以可以提供 IP 地址和端口与信息,通过协议分析技术可以得到服务命令等信息,这样 KVPN 系统就可以实现基于用户身份、套接字信息以及命令信息等多种条件的组合控制,防止各种伪装,提高了安全性能。

小结 从上面的讨论中,我们可以看到 KVPN 系统是一个管理灵活、控制集中的集安全数据传输、身份认证和访问控制于一体的高效安全系统,这种结构的安全系统可以解决传统结构安全系统的诸多弊端,有助于提高安全性和高效性,但它也存在着某些不足之处有待解决,主要表现在以下几个方面:

(1)在用户向 AS 提出认证请求时,AS 服务器对用户的身份不进行验证,而把安全建立在客户端能否正确解密 AS 应答的基础上,这样有利于攻击者积累用 Kc 加密的报文,容易遭受口令猜测攻击。一种可行的解决方法是采用 Challenge/Response 协议,此时 TGT 的信息交换过程为:

AS→Client:n1

Client→AS:{n1}*Kc*,c,tgs,n2

AS→Client:{*Kc*,tgs,n2}*Kc*,{*Tc*,tgs}*Ktgs*

(2)连接认证的过程中所有的认证请求都要经由 AS 和 TGS 服务器处理,同时在 TGS 服务器上要进行访问控制检查,这样极易在这里造成瓶颈,系统的性能和安全就严重地依赖于 AS 和 TGS 的性能和安全,可能的解决方法是使多个 AS 和 TGS 共享认证数据库和策略数据库进行并行处理。

(3)当用户增多时,密钥管理也会变得较复杂。

参考文献

1 Doraswamy N, Dan Harkins D. IPSec: the New Security Standard for the Internet, Intranets, and Virtual Private Networks

2 Neuman B C, Theodore Ts'o Kerberos. An Authentication Service for Computer Networks. IEEE Communications, 1994, 32(9): 33~38

3 Kohl J, Neuman C. (1993-09) RFC 1510: The Kerberos Authentication Service(V5)

4 Bellovin S M, Merritt M. Limitations of the Kerberos Authentication System. ACM SIGCOMM Commputer Communication Review, 1990, 20(5): 119~132