运用SOCKS V5/TLS协议构建VPN的研究与实现

杨 春*

(四川师范大学数学与软件科学学院 成都 610066)

【摘要】提出了在SOCKS防火墙之间建立VPN的架构与技术的思想，利用SOCKS V5对认证方法的可扩充性，采用x.509规范与数字签名实现了SOCKS防火墙之间的证书及身份验证，并运用TLS协议协商数据加密算法与密钥对其数据进行加密传送，介绍了其关键技术的实现。

关 键 词 VPN服务； 证书； 数字签名； TLS协议； SOCKS服务器

中图分类号 TP309.1

虚拟专用网络(Virtual Private Network, VPN)是利用公众数据网(Internet)传输安全可靠的用户专用数据以及一些控制信息的一种专用网络，对于加入Internet的众多企业和公司来说，它降低了远程访问代价及企业网络复杂度。利用虚拟专用网络技术构建自己的专用网络具有很高的商业价值，且实现成本低，服务项目灵活、安全可靠。采用具有加密功能的防火墙技术实现VPN，可充分利用已有的网络设备，代价小且易于升级，可实现网络安全的集中控制和管理。

SOCKS V5协议是一种用于防火墙的新型技术[1]，它支持多种认证方法，可以实现数据完整性和可加密性，提供一种有效建立VPN的方式[2]。SOCKS V5支持用户名与口令认证和通用安全应用程序接口(GSS-API)[3]，许多SOCKS产品就是利用GSS-API来实现Kerberos构建VPN。因而我们在进行企业外部网研究过程中利用SOCKS V5对认证方法的可扩充性，采用x.509规范与数字签名实现SOCKS防火墙之间的证书及身份验证，并运用TLS协议协商数据加密算法与密钥，对其数据进行加密传送，从而构建一个具有基于用户的认证、通信信道加密、透明访问和访问控制审计等优点的虚拟专用网。

1 架构与技术思想

一般来说，防火墙内部子网及用户之间是安全的、可以信赖的，如果在Internet上两个远程防火墙服务器之间是相互信任的，可以认为内部子网及用户之间也可以相互信任，双方应用加密数据传输信息，就可以实现一个VPN服务。问题的核心就在于两个防火墙之间如何取得彼此的信任，如何协商数据加密算法与密钥。对于一个已拥有SOCKS防火墙系统的局域网来说，与远程主机或另外一个SOCKS防火墙服务器之间建立虚拟专用网，主要应考虑以下几项技术：

1) 通信双方信任机制。SOCKS防火墙内部客户机与其服务器有较好的认证机制，因而它们之间是相互信任的，我们要完成的任务是SOCKS防火墙服务器与远程主机或另外一个SOCKS防火墙服务器之间的身份验证。采用x.509协议[4]，通过证书的签名验证可以很好地建立双方信任机制，设定通信双方共有一个CA服务器，可以申请获得各自的有效证书，如图1所示。

2) 证书双向验证机制采用双方数字签名，双方公钥与私钥由CA服务器产生，私钥通过外带方式，各自保管。公钥、私钥由CA服务器产生随机数和一个任意指定数调用RSA系统函数生成。

3) TLS协议应用于SOCKS V5中将进一步实现防火墙强安全性[2]，数据加密传输，加密密钥生成，通过TLS握手协议，由双方Hello报文协商会话密钥，选择数据压缩方式和加密算法[5]。关键技

2001年1月17日收稿

* 男 30岁 在职博士生 讲师

术是会话密钥的协商与产生，可通过双方随机数组合并经哈希函数运算求得。

2 VPN服务过程

VPN服务过程如图1所示，其过程为：SOCKS服务器Alice与Bob向CA服务器申请证书，通过外带方式获得各自私钥；SOCKS服务器启动时，通过读配置文件，由Interface配置参数设置两个SOCKS服务器地址范围，如果SOCKS客户机代理请求类型值为x‘04’，本地SOCKS服务器向它提供VPN服务[2]；本地SOCKS服务器Alice根据VPN请求中的目的地址和目的端口，向远程SOCKS服务器发送ClientHello信息，包含了一个随机数用于以后产生密钥，Hello消息中还包含一个可变长的会话标识符(session identifier)，用于指定会话参数[5]；双方证书签名验证，包括证书的验证，数字签名进行身份验证；TLS会话密钥协商与生成见文献［5］；将认证结果与加密密钥返回VPN服务申请者与远程通信者；最后VPN申请者对数据加密传送，远程主机解密数据；数据传输完毕，结束VPN服务，关闭相应的连接。

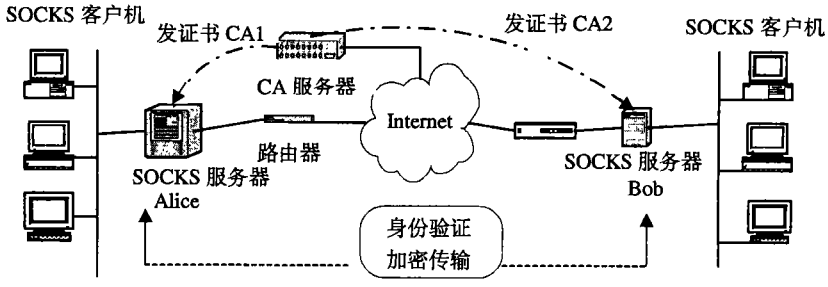

图1　SOCKS客户服务器构建VPN示意图

3 身份认证与数据加密

3.1 证书与SOCKS服务器双向身份鉴别

1）证书生成。证书遵循x.509标准[6]，发证机构CA服务器为多个SOCKS服务器签发证书，如图1所示。证书格式中定义如下信息：struct certification {

ASN1_INTEGER　*version　/*版本号*/ ；SSN_INIEGER　*seralNumber　/*证书序号*/；

X509_ALGOR　*signature　/*数字签名算法RSA*/；X509_NAME　*issuer；　/*证书签发者*/；

X509_VAL　*validity　/*证书有效期*/；　X509_NAME　*subject；　/*证书申请者*/；

X509_PUBKEY　*key　/*公开密钥信息*/ ；　X509_ISSUER　*identifier /*证书签发者标识*/；

X09_SUBJECT *identifier　/*证书申请者唯一标识*/；X509_CA　*ignature　/*CA签名*/　}

2）证书请求与发放。一方SOCKS服务器以客户机身份向CA服务器发送证书申请，CretifiReqnest()，CA服务器收到请求后，为申请者填写证书，以备证书验证，这一过程由ca.c与req.c源程序实现。

3）验证证书。在进行身份验证之前，双方须验证证书的有效性，即确认双方所持证书是否是公共CA服务器所签发的。通过对比各字段，如证书序号、证书签发者，证书申请者来确定证书的有效性。这一过程由verify ［-verbso,-CApath,path,-CAfile］完成。

4）数字签名与身份验证。验证双方私钥在证书请求时产生，用户以外带方式保管。设Alice与Bob(两个SOCKS服务器)已在证书签发机关(CA服务器)申请了证书，各自保管自己的私钥。实现双向认证协议包括：(1) Alice产生一个随机数R_A；(2) Alice构造一条消息：$M=(T_A,R_A,I_B)$，其中T_A是Alice的时间标记，I_B是Bob的身份证明；(3) Alice将M用其私钥加密为$D_A(M)$，将(CA1，$D_A(M)$)发送给Bob；(4) Bob确证CA1并得到Alice公钥E_A，并确认密钥没有过期；(5) Bob用E_A去解密$D_A(M)$，这样证明了

Alice的签名又证明了信息完整性；(6) Bob检查M中的I_B、T_A以及R_A以便进一步证实Alice；(7) Bob产生另一个随机数R_B；(8) Bob构造一条消息，$M'=(T_B,R_B,I_A, R_A)$，其中T_B是Bob的时间标记，I_A是Alice的身份证明，R_A是Alice在步骤(1)中产生的随机数；9) Bob用其私钥加密M'为$D_B(M')$，将(CA2，$D_B(M')$)送给Alice；(10) Alice用Bob的公钥E_B解密$D_B(M')$，以确认Bob的签名和消息的完整性；(11) Alice检查M'中的T_B、R_B、R_A的确保消息不是被替换的其他消息。证书认证使用的公钥与私钥可由RSA系统函数生成：

```
char  *cb_arg= "1236789105"     /*人为指定参数*/
```

RSA_generate_key(512,ox10001,NULL,cb_arg)，证书身份验证的安全性在于用户对私钥的保管

3.2 会话密钥协商、数据加密密钥生成[5]

TLS握手协议另一个主要任务是协商数据加密算法和会话密钥以及数据压缩方式，双方服务器之间通过交换Hello报文来实现会话密钥的协商。发送数据方Hello报文包含协议版本号、随机数数组、会话连接标识、加密算法列表以及数据压缩封装方式。接收数据方收到报文后，产生一个交换Hello报文，确认并指定与客户机相匹配的会话连接标识和加密算法以及压缩封装方法。会话密钥用于双方协商加密算法中对数据传输加密，通过Server key exchange message消息交换premaster secret密钥，由双方产生的随机数相连形成一个参数，Master_secret=PRF(pre_master_secret, "master secret", ClientHello.random+ServerHello.random) [0..47]，经哈希函数运算，为每一个连接产生独立的加密密钥和MAC密码，然后选择TLS 支持加密算法簇如3DES或IDEA加密算法进行加密。

参 考 文 献

1 Yang Chun, Liu Jing, Zhou Mingtian. Application and research SOCKS protocol version5 in firewall. Journal of University of Electronic Science and Technology of China,1999,28(2):199~201[杨 春，刘 玉景 周明天. SOCKS协议在防火墙中的应用研究. 电子科技大学学报，1999，28(2):199~201]

2 杨 春，周明天. SOKS V5运用TLS协议实现防火墙强安全性的应用与研究. 电讯技术，2001,(2): 96~100

3 Yang Chun. Application and research of a user name&password authentication based on SOCKS V5. Journal of University of Electronic Science and Technology of China, 2001,30(2):162~165[杨 春. 用户名与口令认证在SOCKS中的应用研究. 电子科技大学学报，2001, 30(2): 162~165]

4 Michael N. Draft-ietf-pkix-ocspv2-02.txt. Internet Draft. March, 2001

5 Dierks T. The TLS protocol version 1.0. Networking Group, 1999

6 Ian Curry. Version 3 x.509 certificates. Entrust Technologies White paper, 1996

Study of Making up VPN with TLS Protocol Based on SOCKS V5

Yang Chun

(Institute of Mathematics and Software, Sichuan Normal University Chengdu 610066)

Abstract In this paper, a framwork and mechanism of making up VPN between SOCKS fire walls in Internet are proposed. Their identification are implemented using certificate verify supported by x.509 and digital signing, which are the authentication method extension to SOCKS V5 protocol. TLS protocol is also applied to the implement negotiation of their encryption algorithms and cryptographic keys which are used as data encryption and transmission. As well as some relative key techniques are introduced, a strong security system is shown by integrating the advantages of two protocols in this paper.

Key words VPN service; certification; digital signing; TLS protocol; socks server