基于 SSL 技术的 VPN 网关在无线网络中的应用①

单家凌, 谢志成, 赵崇劲

(广东白云学院 计算机系, 广州 510450)

摘 要: 在无线网络的设计和部署中, 安全是一个关键的问题. 现有设备主要采用的安全技术—SSID、MAC 地址过滤、WEP、802.11X 等, 在设计上存在着一定的安全缺陷, 不能很好地保护无线网络的安全. 文章提出了一种将 VPN 技术应用于无线网络中的部署方案, 在 linux 系统环境中, 利用 SSL 技术, 设计一套 VPN 网关, 用于解决目前通过无线网络访问内网资源的安全问题.

关键词: SSL VPN; 无线网络; 身份认证; 私有握手

Application of VPN Gateway Based on SSL Technology in Wireless Network

SHAN Jia-Ling, XIE Zhi-Cheng, ZHAO Chong-Jin

(Guangdong Baiyun institute, Department of Computer, Guangzhou 510450, China)

Abstract: Security is a key issue in design and deployment of wireless network. Security technologies mainly used in existing equipment include SSID, MAC address filtering, WEP, 802.11X etc, which are of certain security flaws in the design and can not well protect wireless network. This paper presents a deployment solution that applying VPN technology in wireless network, which designs a VPN gateway in a Linux system environment by SSL technology, so as to solve the current security issues in accessing resources within the network through wireless network.

Key words: SSL VPN; wireless network; identity authentication; private handshake

现在的很多企业、学校都有自己的 VPN 网络用于解决有线网络的接入与身份认证, 有线网络中的 VPN 在技术和商用上都已经比较成熟. 但针对无线 VPN 的研究和应用相对较少. 由于无线传播媒介是暴露于大气中, 通过空间来传播信号, 与有线网络相比更容易被黑客窃听而获得重要的信息. 因此无线网络的安全问题也显得尤为重要. 论文主要针对怎样利用 SSL VPN 来实现无线网络的安全进行研究.

1 目前解决无线网络的安全方法

目前解决无线网络的安全方法主要体现在访问控制和数据加密两个方面. 访问控制保证敏感数据只能由授权用户进行访问, 而数据加密则保证发送的数据只能被所期望的用户接收和理解. 常用的无线网络安全技术有以下几种[1]:

(1) 服务区标识符(SSID) 匹配. 无线客户端必需设置与无线访问点 AP 相同的 SSID, 才能访问 AP; 如果与 AP 的 SSID 不同, 那么 AP 将拒绝它通过本服务区上网. 缺陷: 可以通过设置隐藏 AP 及 SSID 区域的划分和权限控制来达到保密的目的, 但 SSID 通常只是个简单的口令.

(2) 物理地址(MAC)过滤. 在 AP 中可手工维护一组合法的无线客户端网卡的 MAC 地址列表, 实现物理地址过滤. 缺陷: 这种方法的效率会随着终端数目的增加而降低, 而且非法用户通过网络侦听就可获得合法的 MAC 地址表, 非法用户可盗用合法的 MAC 地址非法接入.

(3) 有线对等保密(WEP). 在 IEEE802.11 中, 定义了 WEP 来对无线传送的数据进行加密, WEP 的核心是采用的 RC4 算法. 缺陷: 密钥固定, 初始向量位数、算法强度太小.

(4) 端口访问控制技术(IEEE802.1x). 当无线工作站

① 收稿时间:2013-07-01;收到修改稿时间:2013-07-22

STA 与无线访问点 AP 关联后, 是否可以使用 AP 的服务要取决于 802.1x 的认证结果[2]. 如果认证通过, 则 AP 为 STA 打开这个逻辑端口, 否则不允许用户连接到网络. 缺陷: IEEE802.1x 提供无线客户端与 RADIUS 服务器之间的认证, 而不是客户端与无线接入点 AP 之间的认证, 采用的用户认证信息仅仅是用户名与口令, 在存储、使用和认证信息传递中存在很大安全隐患.

因此对于高安全要求或大型的无线网络, VPN 方案是一个更好的选择. 因为在大型无线网络中维护工作站和 AP 的 WEP 加密密钥、AP 的 MAC 地址列表都是非常艰巨的管理任务. 对于无线网络, 基于 VPN 的解决方案是当今 WEP 机制和 MAC 地址过滤机制的最佳替代者.

2 SSL协议实现VPN

虚拟专用网 VPN(Virtual Private Network, 简称 VPN)是利用公用网(如因特网)来搭建私人专用网络. 传统 VPN 是基于 IP 安全结构的网络安全体系, 典型代表是基于网络层实现的 IPSec VPN. 其主要问题是: 要求 VPN 远端服务群的防火墙打开多个端口; 客户端要进行繁琐的配置和一定的维护管理; IPSec VPN 不能穿越支持 NAT 的设备. 随着 HTTPS 的广泛应用, 一种基于 SSL/TLS 协议依托 Web Server 的 VPN 构架(SSL VPN) 应运而生, 它相对于传统 VPN 具有“无客户端”特性, 能更好应用在无线网络中[3].

2.1 SSL 通信过程

SSL 安全协议实际是 SSL 握手协议、SSL 修改密文协议、SSL 警告协议和 SSL 记录协议组成的一个协议族, 位于 TCP/IP 协议模型的网络层和应用层之间, 使用 TCP 来提供一种可靠的端到端的安全服务. SSL 协议在应用层通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作, 在此之后, 应用层协议所传送的数据都被加密. SSL 握手由通信双方利用以前建立的有效 SSL 会话建立连接, 以缩短握手时间[4]. 具体过程如下:

(1) SSL 客户端向 SSL 服务端发送客户问候消息, 该消息中的会话 ID 是一个已经建立的会话 ID.

(2) SSL 服务端在接收到 SSL 客户端的问候消息后, 检查是否存在客户指定的会话, 如果不存在该会话, SSL 将通过完全握手协议来建立连接; 如果存在该会话, SSL 服务端给客户端返回的服务端问候消息中会话 ID 与客户端问候消息中的会话 ID 相同, 而且服务端问候消息中协商的加密参数与原会话中选定的加密参数相同.

(3) SSL 服务端随后将向 SSL 客户端发送改变加密规范消息和服务端握手结束消息, SSL 客户端接收到消息后向服务端发送改变加密规范消息和客户端握手结束消息.

2.2 算法实现

SSL VPN 的安全性是基于 SSL 协议, 故 SSL 协议的实现是关键, 文章采用已有的免费库 OpenSSL, 大大简化了整个系统的实现[5]. 首先, 利用函数 SSL_library_init( )对 OpenSSL 进行初始化, 然后使用 SSL_load_error_strings( )进行错误信息的初始化. 一次 SSL 连接会话需要先申请一个 SSL 环境, 基本的过程是:

(1) 创建本次会话连接所使用的协议: SSL_METHOD * SSLv23_server_method(void).

(2) 申请 SSL 会话的环境 CTX: 申请 SSL 会话环境的 OpenSSL 函数是 SSLK _CTX* SSL_CTX_new (SSL_METHOD*). 该函数返回当前的 SSL 连接环境的指针. 然后设置 SSL 握手阶段证书的验证方式和加载自己的证书.

void SSL_CTX _ set_verify (SSL _CTX* , int, int* (in t, X509 _STORE _CTX*))

void SSL_CTX _ load _ verify _ locations (SSL _CTX* , constchar* , constchar*)

int SSL_CTX _use_ certificate_ file(SSL _CTX * ctx, constchar *file, int type)

int SSL_CTX _use_PrivateKey _ file(SSL _CTX * ctx, constchar *f ile, int type)

加载证书和文件之后, 验证私钥和证书是否相符: BOOlSSL_CTX_check_private_key (SSL_CTX*).

(3) 将 SSL 和已经连接的套接字绑定: SSL* SSL_new (SSL_CTX*)该函数申请一个 SSL 套节字, 然后用函数 int SSL_set_fd(SSL*)绑定读写套接字.

(4) 开始 SSL 握手的动作, 使用函数: int SSL_connect (SSL*)

(5) 握手成功之后, 就可以进行通讯, 使用 SSL_read 和 SS_write 读写 SSL 套接字代替传统的 read、write, 函数为:

int SSL_read (SSL * ss,l char* bu ,fint num)

int SSL_write (SSL * ss,l char* bu,fint num)

对于 VPN 网关服务器, 要使用 SSL_accept 代替

传统的 accept 调用，函数为:

int SSL_accept(SSL * ssl).

(6) 通讯结束，需要释放前面申请的 SSL 资源，使用函数:

int SSL_shutdown(SSL * ssl) 关闭 SSL 套接字

void SSL _free (ssl) 释放 SSL 套接字

void SSL _CTX_free (ctx) 释放 SSL 环境

3 无线网络中SSL VPN 网关的构建

3. 1 VPN 网关的总体设计

一个最基本的 SSL VPN 由两部分组成，客户浏览器和 SSL VPN 网关. 客户端浏览器利用 SSL 技术加密访问请求，发送到 SSL VPN 网关，网关将接收到的加密信息解密后再转发到企业网中的 Web 服务器，从而在 Internet 上形成一个客户端到 SSL VPN 网关之间的加密隧道，如图 1 所示. 其中 SSLVPN 网关的核心部分是由多个独立功能服务器组成的，包括 LDAP 服务器负责公用证书和安全密匙的保存，SSLVPN 网关服务器作为 LDAP 客户端查询 LDAP 服务器上的用户信息，来验证用户的身份是否合法. RADIUS 服务器负责访问者的认证相关的控制策略，SSLVPN 网关服务器作为 RADIUS 客户端，通过与 RADIUS 服务器交互认证消息，来验证用户的身份是否合法. AD 是证书验证服务器.

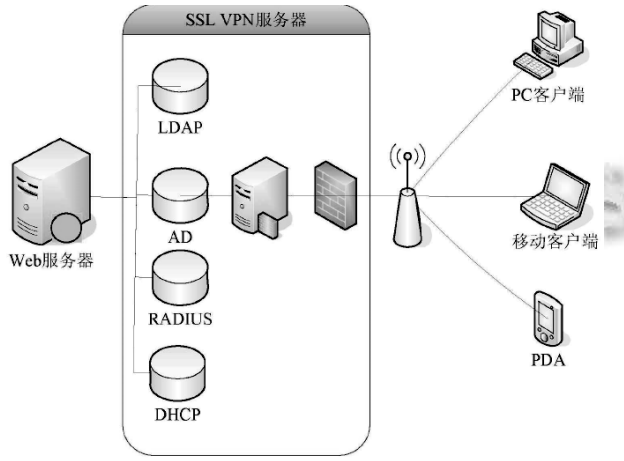

图 1 无线 SSL VPN 网关整体结构

图 1 中 VPN 网关服务器和其他服务器位于内部网络中不同的主机上. 从功能上来说，VPN 网关服务器相当于内部网络中的安全代理，由于与其他各种服务器在同一内部网中，因此他们之间的数据可以用明文进行传输. 对于客户端和 VPN 网关服务器，由于位于不同的网络之间，因此二者之间要形成一个安全通道，必须使用 SSL 进行数据加密通信.

3.2 逻辑结构

(1) 逻辑设计

整个 VPN 系统由 SSL 网关、Web 服务器及 AP 组成[6]. 其中最重要的是 SSL 网关，它保证通信的安全，即保密性、消息完整性和端点的认证. SSL 网关主要由请求处理模块、用户认证模块、隧道协议模块以及密钥管理模块等组成. 逻辑结构如附图 2 所示.

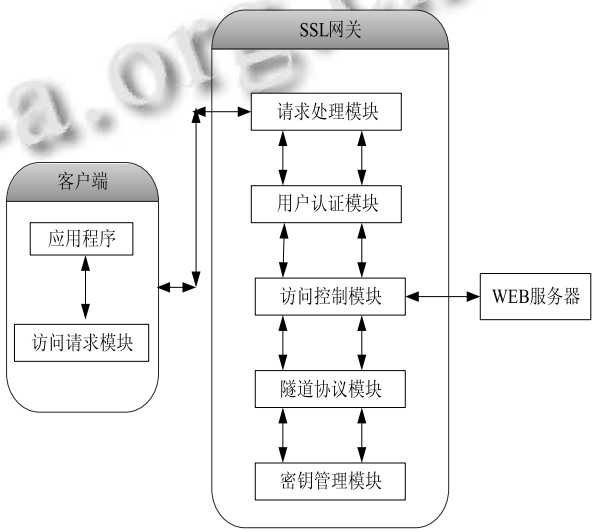

图 2 无线 SSL VPN 系统逻辑结构图

(2) 系统主要模块

请求处理模块: 请求处理模块为常驻内存的守护进程，负责执行 SSL 连接，监听固定的服务端口. 用户认证模块: 采用基于 ECC 椭圆曲线密码体制的公钥证书认证方式. 整个身份认证模块由客户端、AP 和证书服务器组成. 其中证书服务器包含了 CA 和 RA 以及 CRL 数据库，采用 LDAP 数据库. 证书服务器同时承担了认证服务器的作用. 在客户端和认证服务器上保存了由 CA 颁发的数字证书. 当用户连接到 AP 时，必须通过认证服务器进行验证，根据验证结果，只有拥有合法证书的用户才能访问 AP. 密钥管理模块密钥管理也是 CA 系统的一部分，密钥管理模块的主要功能包括: 密钥生成、密钥更新、密钥备份及恢复以及密钥销毁和归档处理等. 访问控制模块: 采用基于内容的访问控制方法，系统管理员通过设置资源列表文件的内容来实现内网资源的访问控制.

4 SSL VPN网关在无线校园网应用

论文提出的 SSL VPN 网关一个典型应用就是无线校园网，高校图书馆购买了大量的外部资源如远程电子数据、出版物，这些资源不是存放在图书馆服务器上，而是存储在内容提供商的服务器上，图书馆支付费用以后，内容服务商是根据访问者的 IP 地址来判断是否是经过授权的用户. 广大师生可以利用无线校园网通过 SSL VPN 认证实现对图书馆资源的安全访问.

4.1 应用系统设计

在不更改现有无线网络的基础上，学校可以在防火墙的后面部署了一台 SSL 网关设备，内部资源服务器群组与 SSL 网关并联到防火墙之后的交换机上，这样不会给系统造成通信瓶颈和单点故障，最大限度地保障了原有系统的稳定性，整个系统由 SSL 网关和内部服务器以及 AP 组成[7]. 其结构如图 3 所示.

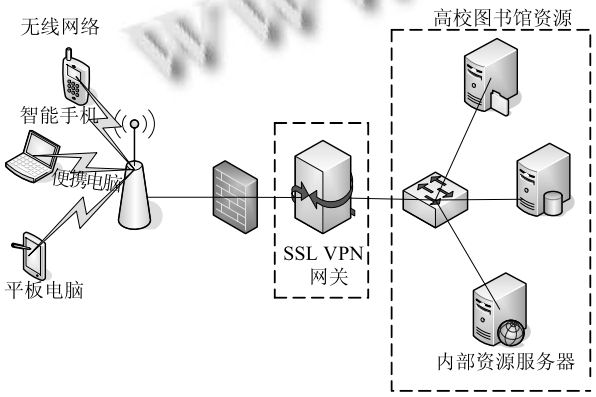

图 3 高校 SSL VPN 应用系统

文章利用 OPEN VPN 软件来建立校园网 VPN 系统. OPEN VPN 是一款开源软件，支持多种身份验证方法：包括预共享私钥，第三方证书以及用户名/ 密码组合，它大量使用 OPEN SSL 加密库，以及 SSL v3/TLS V1 协议，支持远程访问、802.11 和 WiFi 等多种 VPN 接入方案.

4.2 无线用户认证设计

(1) 认证流程

VPN 服务权限进行划分，在进行 SSL 握手协议之前，按图 4 流程对用户环境的安全进行验证，并根据安全程度不同为用户提供相应权限的访问[8]. 具体过程为:

1) 验证用户的密码和令牌. 如果不正确，提示不能建立 SSL 连接，结束会话；如果正确，继续;

2) 对客户环境进行安全验证. 如果环境是可信任的，则向用户提供高权限的服务;

3) 如果环境的安全不可信任，要求用户从 SSL VPN 应用网关下载安全监测和文件清除程序，并限定用户以较低权限访问;

4) 如果客户机不允许下载和安装程序，则由系统强制关闭不安全端点的缓存功能，指定用户以不能缓存显示内容，并限定用户以低权限访问服务器;

5) 按规定的权限与客户进行 SSL 握手，对客户机加密算法强度进行检查. 如果加密算法强度小于网关设置的最小安全级别，则拒绝建立连接;

6) 进行 SSL 握手，建立连接，为用户提供相应的 SSL VPN 访问服务.

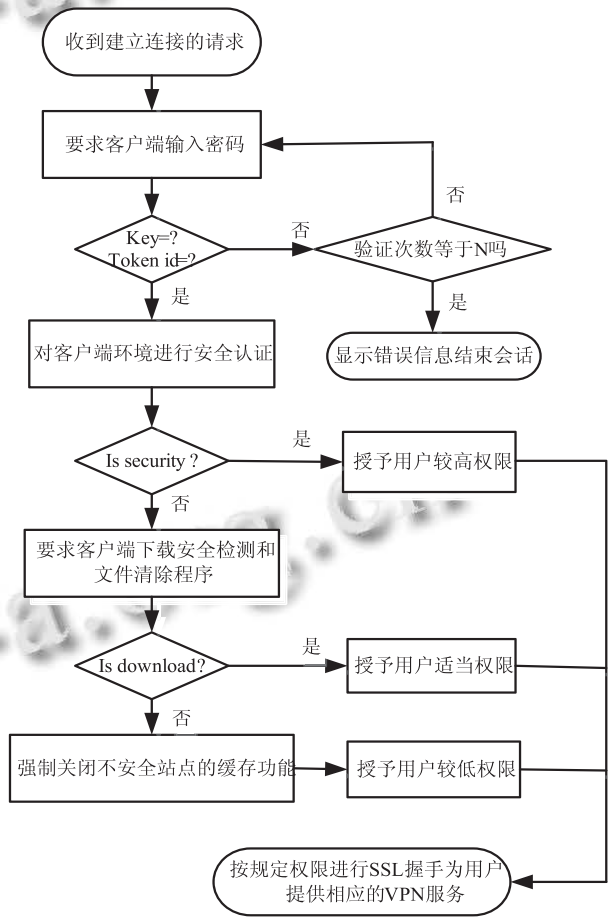

图 4 对客户端安全认证流程图

(2) 认证实现

在 LINUX 系统中 SSL VPN 服务器利用 Openssl 库函数实现其功能，提供 SSL 加密/ 解密，建立 SSL 数据通道， 在客户端和 VPN 服务器之间实现点到点的安全通信. 下面的设计可以做到在 SSL VPN 服务

器上进行客户的认证.

1) 用 Apache Server 管理一份用户访问列表 UserAccessList. 这份列表表示每个成员可以访问哪些服务器, 并且需要通过什么端口. 可以通过请求网页命令得到此列表, 命令格式为 GET url + getserver. list.action + cookie. 其中, url 为服务器的地址; getserver.list.action 表示获取 list 的命令; cookie 是 HTTP 协议提供的, 保证 Web 的时效和安全. 基本数据结构是:

```
typedef struct { char username[32] ;
CList list[size]; }
UserAccessList , * PuserAccessList;
typedef struct { charm_ip[40] ;
charm_netm ask[40];
int32 m _port;
char protocol[10] ; }
CList , * PList;
```

可以用文件的形式进行存储和管理. 当用户请求列表时, 就将 CuserAccessList 结构中的 list 全部返回给 VPN Server.

2) 客户端要与 SSL VPN 服务器端进行私有握手, 并判断该客户是否有权限访问其提出连接请求的真正服务器. 私有握手的建立是在用户端得到了服务器的列表之后进行的, 用自己的数据包格式发送连接请求. 私有握手的头格式要做一些改动, 可以在头部增加一个标识: my head. 整个头部为 myhead GET url+ getserver.List.action + cookie. 这个头对于实际要访问的服务器来说是不能识别的, 因为这是与 SSL VPN 的私有通信数据. SSL VPN 服务器将这个请求 list 的命令去掉标识 my head 之后, 转发给 Apache 服务器, 并同时产生一个标志 Flag. Apache 服务器就会通过步骤 1)返回一个该用户可以访问的服务器列表给 SSL VPN 服务器. Flag 标志表示此客户端已经和 SSL VPN 进行了私有握手, SSLVPN 服务器将 Flag 和 list 一同返回给客户端. 同时, 在 SSL VPN 服务器上也维护一个用于验证用户的列表 Auth-List.

4.3 系统的工作流程

整个 VPN 系统的基本工作流程如下:

(1) 校园网无线用户通过 HTTPS 连接到 SSL VPN 服务器, 网关对用户进行验证 f 目前是通过用户证书验证), 并根据其权限返回可以访问的资源列表.

(2) 请求处理模块接收请求数据包, 进行解密后将数据发送给访问控制模块.

(3) 隧道协议模块负责建立端对端隧道的建立.

(4) 访问控制模块根据设置的访问控制策略决定用户是否可以访问内网资源.

4.4 安全性分析

从图 3 可以看出, 文章设计的 SSL VPN 放在防火墙后面, 把网络内部需要被授权外部访问的应用注册到 SSL VPN 上, 对于防火墙来讲, 仅需要开通 443 端口到 SSL VPN, 而不需要开通所有内部的应用的端口开放给公网用户, 这样大大降低了整个网络被公网来的攻击的可能性. SSL 协议在应用层建立的通道可以防止病毒、蠕虫等经由网络层传输的威胁. 另外, 由于 SSL VPN 还可以起到代理服务器的作用, 所有客户端的访问都是由 SSL VPN 网关转发, 而不能直接访问应用服务器, 从而使服务器不易受到病毒、黑客等攻击, 而且还可以提供细粒度的强访问控制和日志审计.

5 结语

SSL VPN 作为一种新的安全传输技术, 正是在网络安全需求不断提高的形势下应运而生的. 文章设计的 SSL VPN 应用在无线网络中提供了端到端的连接, 数据在客户端到服务器之间都以密文形式传送, 保证了网络资源和用户数据的安全性. 由于 SSL VPN 不需要客户端配置, 可以让用户可以随时随地地采用一些传统的应用工具, 实现了无线网络方便接入.

参考文献

1 卞长喜.无线局域网中 SSL VPN 网关的设计与实现.农业网络信息,2011,3:74–76.

2 罗辉琼等.基于 IVE 的校园网 SSL VPN 安全接入研究.计算机安全,2013,(2):42–46.

3 周明.SSLVPN 体系结构在无线局域网中的应用与设计[学位论文].成都:电子科技大学,2006.

4 寻大勇.SSL VPN 网络安全技术的应用研究.通信技术,2009,42:248–250.

5 吴刚.多种平台的 VPN 应用比较.计算机系统应用,2011,20(8):245–249.

6 孙磊.SSLVPN 网关在无线校园网中设计与应用.黑河学院学报,2011,2(3):124–128.

7 马宗萼等.VPN 系统反馈调整和实时监控集成解决方案.计算机系统应用,2011,20(11):23–26.

8 杨兴良等.安全高效的 SSL VPN 构建方法研究.计算机仿真,2006,23(8):129–133.