文章编号 1004-924X(2008)11-2252-05

高安全 VPN 的嵌入式 PPPoE 接入研究

于 晓[1,2],隋永新[2],杨怀江[2],王 欣[3],赵 铭[1]
(1.空军航空大学 训练部,吉林 长春 130022;2.中国科学院 长春光学精密机械与物理研究所 应用光学国家重点实验室,吉林 长春 130033;3.吉林大学 计算机科学与技术学院,吉林 长春 130012)

摘要:提出了一种高强度的虚拟专用网(VPN)安全通信解决方案。该方案将 VPN 的安全协议脱离开操作系统,嵌入到网络设备(安全网卡)之中,使得任何程序在使用网络设备时都无法绕开安全协议,从而使系统在完成保密通信的同时具有防止主动攻击的能力。介绍了安全网卡的硬件平台和内部软件结构,讨论了该 VPN 的多种接入方式。给出了在安全网卡内部基于 PPPoE 协议的 ADSL 宽带接入 VPN 的实现方法,验证表明该方法达到了预期的结果。

关 键 词:虚拟专用网;PPPoE;网络安全;安全隧道
中图分类号:TP393.08 **文献标识码**:A

Research on embedded PPPoE access method based on highly secure VPN

YU Xiao[1,2], SUI Yong-xin[2], YANG Huai-jiang[2], WANG Xin[3], ZHAO Ming[1]

(1. *Training Ministry, Aviation University of Airforce, Changchun* 130022, *China*;
2. *State Key Laboratory of Applied Optics, Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun* 130033, *China*;
3. *College of Computer Science and Technology, Jilin University, Changchun* 130012, *China*)

Abstract: In order to provide high quality information security service in public network, a new scheme is developed for constructing a secure Virtual Private Network(VPN). In this scheme, security protocols are separated from operating system and integrated into the network equipment—safe Ethernet card. When a program makes use of network equipments, the protocols cannot be bypassed. So the scheme can be used in security communication and can prevent active attack. The hardware platform and inner software structure of the Ethernet card are introduced, and the multiple access manners of the VPN are discussed. A method accessing ADSL in VPN based on PPPoE in the card is presented, which is validated to achieve the expected purpose.

Key words: Virtual Private Network(VPN); PPPoE; network security; secure tunnel

收稿日期:2008-01-03;**修订日期**:2008-06-30.
基金项目:吉林省科技发展计划基金资助项目(No. 20040527)

1　引　言

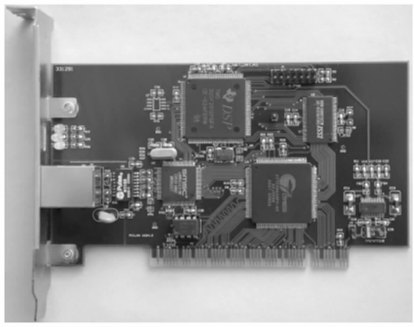
利用已有的网络资源，在其中建立安全子网可以明显降低保密通信的建设成本和维护费用，并便于开展各种信息安全服务。虚拟专用网(VPN)便是针对上述应用所提出的新型网络安全技术，其核心思想是利用安全协议在不安全的公共网络中建立一个安全的连接。然而，目前承载 VPN 安全协议的用户操作系统都不可避免地存在着各种安全漏洞，因此系统有可能被木马和黑客所控制，从而恶意程序可以绕开安全协议通过网络设备直接将敏感信息发送出去[1]。

针对上述问题，本文提出了一种新型的高安全 VPN 解决方案，该方案将 VPN 的安全协议脱离开操作系统，嵌入到网络设备之中，使得任何程序在使用网络设备时无法绕开安全协议，从而使系统在完成保密通信的同时具有防止主动攻击的能力。由于目前基于 PPPoE[2] 协议的 ADSL 宽带接入公共网络得到了广泛的应用，因此本文研究了在嵌入式网络设备中用 PPPoE 方式接入新型 VPN 的方法。

2　新型高安全 VPN

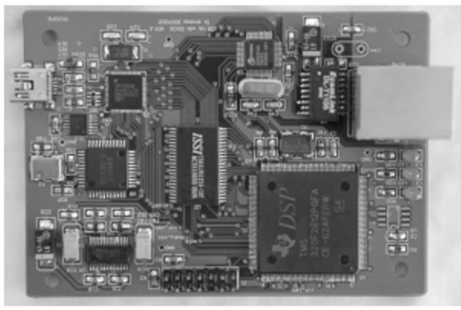
鉴于网络安全技术对于国家安全的特殊意义，发达国家对相关产品的核心技术严格保密。为充分发挥目前丰富的公共网络资源和提高我国网络安全应用水平，必须开发自主的网络安全产品。因此，本文大胆提出了一种新型的高安全 VPN 方案。该方案将硬件密码组件技术嵌入到通用的以太网卡内部，研制出具有身份认证、密钥自动生成与交换和保密通信功能的安全以太网卡，其硬件平台如图 1 所示。这种安全网卡中的安全机制彻底脱离了操作系统的参与，可用于组建高安全性的 VPN 网络，为安全 VPN 的构建提供了一个新思路[1,3]。

在安全网卡中嵌入式处理器是其硬件结构的核心。图 1 中两款网卡都选用了 TI 公司的 TMS320F2812 芯片作为嵌入式处理器，其片内具有一个 128 bit 的密码锁，用于保护片内 FLASH 和 SRAM 中的程序和数据不被非法读写。图 2 是利用测试工具 IxChariot 对 USB 接口安全网卡进行测试的结果(测试方式：点对点保密通信，测试结果：数据传输平均速度为 20.7 Mbit/s)。



(a)安全网卡 PCI 接口

(a)PCI interface of safe Ethernet card



(b)安全网卡 USB 接口

(b)USB interface of safe Ethernet card

图 1　安全网卡硬件平台

Fig. 1　Safe Ethernet card of hardware platform

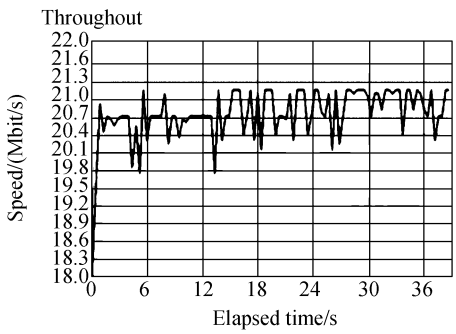


图 2　USB 接口安全网卡速度测试

Fig. 2　Speed test of USB safe Ethernet card

安全网卡内部的软件结构如图 3 所示，运行在安全网卡内部的软件主要包括：(1)嵌入式内核：为一种简单的实时操作系统。可使用 TI 提

供的 DSP/BIOS[4] 内核。为了达到更高的安全性，本文没有使用 DSP/BIOS，而是自行编写了系统的内核程序。(2)接口管理模块：主要负责管理 PCI/USB 接口芯片、以太网接口芯片，完成各个接口的配置，并监控经由上述接口的数据收发过程。(3)网络层封装模块：通信过程中，需要将加密后的数据进行重新封装才能使其顺利地跨越公共的 IP 网络。(4)安全策略模块：是安全网卡的核心，并对所有经由网络接口的数据流进行安全处理(包括身份认证、密钥管理、加解密编码和完整性校验等[5-6])。

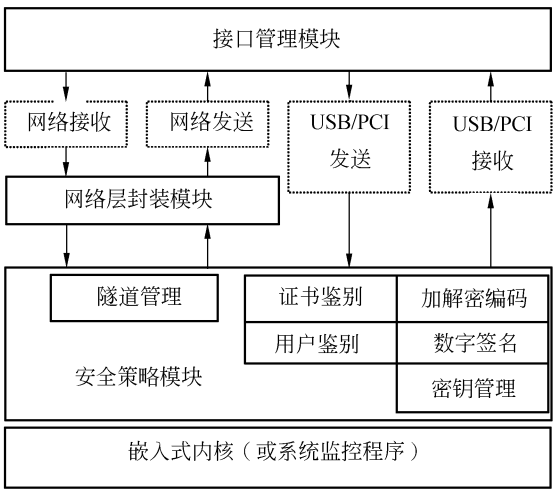


图 3　安全网卡的软件组成框图

Fig. 3　Software framework in safe Ethernet card

在利用安全网卡组建 VPN 网络时，接入 VPN 中的安全网卡用户可能具有固定合法的 IP 地址，也可能是动态的合法 IP 地址，甚至是在子网中的私有 IP 地址。图 4 是在 Internet 公共网络上使用安全网卡构建的高安全 VPN 物理网络拓扑，其中给出了多种 VPN 接入方式。

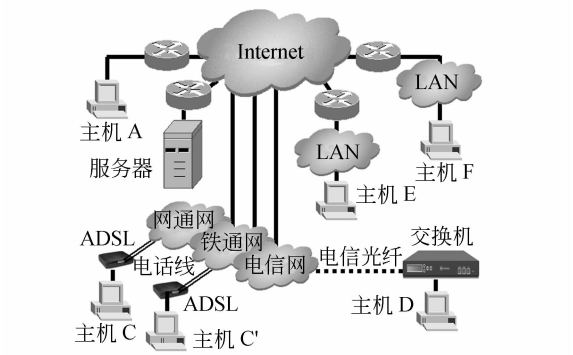


图 4　高安全 VPN 物理网络拓扑

Fig. 4　High security VPN physical topology

图 4 中服务器具有固定的合法 IP 地址；主机 A 具有固定的合法 IP 地址；主机 C、C′和 D 具有动态的合法 IP 地址，分别通过 ADSL 或电信光纤等方式接入到互联网；主机 E 和 F 具有私有的 IP 地址，位于内部子网之中，并通过 NAT 网关进行网络地址转换。主机 A、C、C′、D、E 和 F 都安装 USB 接口的安全网卡，而服务器则安装高性能的 PCI 接口安全网卡，它们在逻辑上组成了与互联网其它用户完全隔离的高安全 VPN 网络。

主机 C、C′和 D 的 IP 地址是动态分配的，这样主机 A 或 B 并不知道它们的 IP 地址。因此，在通信之前所有主机都需要到服务器上进行登录，成功之后可以获得其它用户的 IP 地址，进而可以在任意两个主机之间创建加密隧道，实现点对点的实时保密通信。主机 E 和 F 的 IP 地址是非法的私有 IP 地址，这样其它主机发送给主机 E 或 F 的信息将被它们的 NAT 网关丢弃，因此必须求助于服务器才能实现直接的点对点通信。主机 E 与 F 的通信过程则要复杂得多，主要取决于各自的 NAT 网关。如果 NAT 属于 IP 地址转换类型，则主机 E 与 F 相当于具有动态的合法 IP 地址，但是此种类型 NAT 网关的使用范围已经大为减少。目前，普遍使用的 NAT 网关属于 CONE NAPT(网络地址端口转换)，在此情况下，主机 E 与 F 的点对点通信需要使用 Hole Punching 技术(参见 RFC 3027)。

3　PPPoE 宽带接入新型 VPN

目前，在国内 ADSL 宽带方式接入互联网得到了广泛的应用，其中的数据链路主要采用 PPPoE 协议来实现。下面简要介绍此类接入方式，具体地讨论安全网卡内部如何实现基于 PPPoE 协议的 ADSL 拨号以及其在新型 VPN 中的数据通信方法。

PPPoE 是一种在以太网上进行 PPP 点对点拨号连接的协议。由于以太网属于专网，网络是直接连通的，不须拨号，所以物理层上的链接是没有问题的。但为了确保连接安全，并且只允许合

法用户连接，所以采取了类似电话拨号方式的身份验证，此时所拨的不是电话号码，而是用户的账户，属于数据链路层的协议。

PPPoE 协议的工作流程包含发现(Discovery Stage)和 PPP 会话(PPP Session Stage)两个阶段，发现阶段是无状态的，目的是获得 PPPoE 终结端(在局端的 ADSL 设备上)的以太网 MAC 地址，并建立一个唯一的 PPPoE 会话 ID(Session-ID)。发现阶段结束后，即进入标准的 PPP 会话阶段。这两个阶段的具体规定和流程参见 RFC2516、RFC1661、RFC1312 和 RFC1570。下面讨论安全网卡内部具体的实现方法。

3.1　PPPoE 拨号连接

如图 5 所示，这是安全网卡内部 PPPoE 拨号连接的过程，共有 4 个阶段：

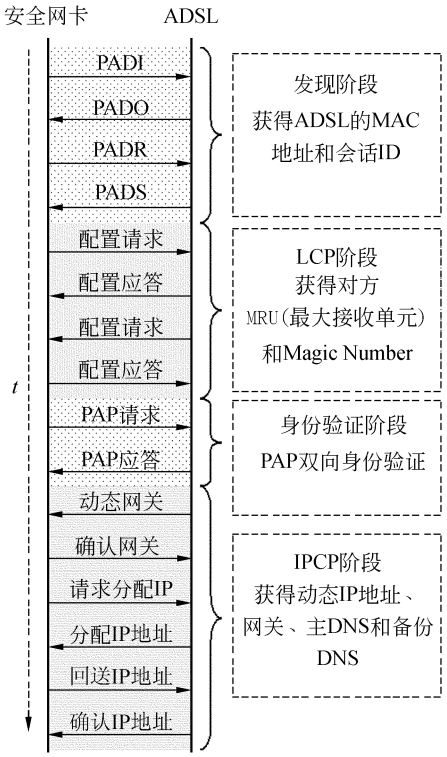


图 5　安全网卡内部实现 ADSL 拨号连接

Fig. 5　ADSL dial-up in safe Ethernet card

3.1.1　发现阶段

通过交互 PADI、PADO、PADR 和 PADS 4 个消息来获得局端 ADSL 设备物理地址并获得一个 PPPoE Session-ID[8]。

3.1.2　LCP(Link Control Protocol Stage)阶段

通过交互双方的配置信息来获得对方的 MRU 和 Magic Number[7]，还包括身份验证方法的确定(由局端指定)。

3.1.3　身份验证阶段

PPPoE 有两种身份验证方法：CHAP[10] 和 PAP[9]，前者为三向验证后者为双向验证。图中可以看出在 LCP 阶段，局端给出的是 PAP 方法。目前该阶段需要的 ADSL 帐号和密码，采用专用通信协议从用户系统中获得。

3.1.4　IPCP(Internet Protocol Control Protocol Stage)阶段

用于获得局端动态分配的 IP 地址、网关、主 DNS 和备份 DNS 等，详细过程参见 RFC1332。

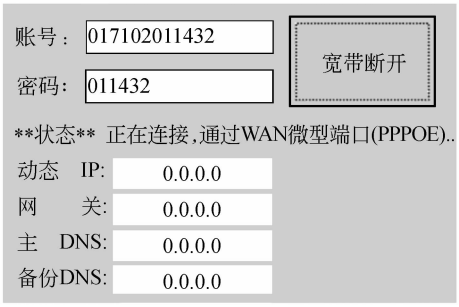
3.2　PPPoE 包的封装和解封

建立 PPPoE 拨号连接后，需要对进出完全网卡的 IP 数据包进行 PPPoE 封包和 PPPoE 解封。如图 6 所示，这是安全网卡内部 PPPoE 数据包的出栈和入栈所经历的基本处理过程。

图 6　安全网卡内部 PPPoE 数据包的基本流程

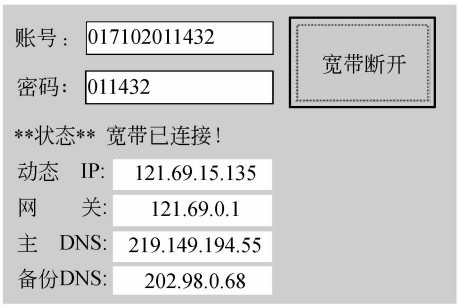
Fig. 6　PPPoE data packet flow in safe Ethernet card

图 7 显示了用户通过客户端界面软件来控制安全网卡内部的 PPPoE 拨号连接过程。客户端软件与安全网卡之间使用专用通信协议交互信息。图 7(a)：通信协议将 ADSL 的帐号和密码下



(a)正在建立 PPPoE 连接

(a)Establishing PPPoE link



(b)PPPoE 连接建立成功

(b)Established PPPoE link

图 7　ADSL 拨号客户端界面

Fig. 7　ADSL dial-up client interface

载到安全网卡中，然后触发安全网卡内部的 ADSL 拨号进程建立 PPPoE 连接。图 7(b)：ADSL 拨号连接建立后，用户在客户端图形界面上看到了通信协议上传的动态 IP 地址、网关和 DNS 等信息。

4　结　论

针对目前日益强烈的网络安全需求，提出了一种高安全 VPN 方案，其特色是将硬件密码组件技术嵌入到通用的以太网卡内部，使其具有身份认证、密钥自动生成与交换和保密通信功能。这种安全网卡中的安全机制彻底脱离了操作系统的参与，使得任何程序在使用该设备时都无法绕开安全协议，从而使 VPN 系统中的用户在进行保密通信的同时具有防止主动攻击的能力。介绍了安全网卡的硬件平台、软件结构和 VPN 组网；给出了一种具体的基于 PPPoE 协议的 ADSL 宽带接入该 VPN 的实现方法，实验测试了方法的可行性，经验证达到了预期的结果。

参考文献：

[1] 于晓. 一种内嵌安全机制的安全以太网卡实现技术研究[D]. 长春：长春光学精密机械与物理研究所，2006.
YU X. *Research on safe ethernet network interface card embedded with security mechanism* [D]. Changchun: Changchun Institute of Optics, Fine Mechanics and Physics, 2006. (in Chinese)

[2] MAMAKOS L, LIDL K, EVARTS J, *et al*.. A method for transmitting PPP over ethernet (PPPoE)[Z]. *RFC*2516, *February* 1999.

[3] 于晓. 高安全机制 VPN 组网关键技术研究[R]. 中国科学院博士后出站报告，2008.
YU X. The study on key techniques of VPN with highly secure mechanism [R]. *Report of Post Doctoral Research Submitted to Chinese Academy of Sciences*, 2008. (in Chinese)

[4] 于 晓，王 欣，闫 丰，等. 电晕探测系统中 JPEG 截图文件系统的设计[J]. 光学 精密工程，2005，13(6)：721-726.
YU X, WANG X, YAN F, *et al*.. Design of JPEG image file system in coroa detection system[J]. *Opt. Precision Eng.*, 2005, 13(6): 721-726. (in Chinese)

[5] 张焕国，刘玉珍. 密码学引论[M]. 武汉：武汉大学出版社，2003.
ZHANG H G, LIU Y ZH. *Cryptology Introduction* [M]. Wuhan: Wuhan University Press, 2003. (in Chinese)

[6] WILLIAM S. *Cryptography and Network Security Principles and Practices*, *Fourth Edition* [M]. Beijing: Publishing House of Electronics Industry, 2006.

[7] SIMPSON W E. The Point-to-Point Protocol (PPP)[Z]. *RFC*1661, *July* 1994.

[8] MCGREGOR G. The PPP Internet Protocol Control Protocol (IPCP)[Z]. *RFC*1332, *May* 1992.

[9] LIOYD B, SIMPSON W. PPP Authentication Protocols[Z]. *RFC*1334, *October* 1992.

[10] SIMPSON W. PPP Challenge Handshake Authentication Protocol (CHAP)[Z]. *RFC*1994, *August* 1996.

作者简介：于　晓(1973－)，男，吉林通化人，讲师，博士后，主要研究方向为计算机网络及信息安全；E-mail：wx_yxy@163.com

通讯作者：隋永新(1970－)，男，副研究员，硕士生导师，主要从事信息安全方面的研究。E-mail：suiyx@sklao.ac.cn

赵　铭(1963－)，男，吉林长春人，副教授。