第33卷 第13期 计 算 机 工 程 2007年7月
Vol.33 No.13 Computer Engineering July 2007
·工程应用技术与实现· 文章编号：1000—3428(2007)13—0263—03 文献标识码：A 中图分类号：TP393

嵌入式安全网卡在网络监听中的应用研究

巫喜红[1]，凌 捷[2]
(1. 嘉应学院计算机科学与技术系，梅州 514015；2. 广东工业大学计算机学院，广州 510090)

摘 要：论述了嵌入式安全网卡的结构、功能，分析了网络监听原理、检测手段和防范措施，提出了把嵌入式安全网卡应用到网络监听中的方案。在嵌入式安全网卡中有一个重要部件加密机，它能采用不同加解密算法对数据进行加解密，还能解决加密运算的瓶颈。安装了这种网卡的电脑，在进行数据传输中，即使通信内容被监听到，所得到的也是被加了密的内容，不能被破译，从而实现了数据在网络传输过程中的安全。

关键词：嵌入式安全网卡；加密；网络监听

Research on Application of Embedded Safe Network Card in Network Sniffing

WU Xihong[1], LING Jie[2]
(1. Department of Computer Science and Technology, Jiaying University, Meizhou 514015;
2. Computer College, Guangdong University of Technology, Guangzhou 510090)

【Abstract】 This paper discusses the structure and function of embedded safe network card and analyses the principle, the detecting methods and defending measures of network sniffing. It proposes a scheme about putting embedded safe network card to network sniffing. There is an encryptor which is important part in the embedded safe network card. It can encrypt data and decrypt data through different encrypt algorithms and decrypt algorithms, and it can settle the bottleneck of encrypted operation. When the computer that is set such network card transfer data, the data which are sniffed are encrypted. It realizes the security of data in the course of network transmission.

【Key words】 embedded safe network card; encrypt; network sniffing

近年来，网络安全已成为一个突出的问题，它给用户造成极大的损害。网络监听技术被滥用，并逐渐演变成为危害网络安全的一个重要手段，这也越来越引起人们的重视。

网络监听技术本来是提供给网络管理员用于性能分析、排除网络故障、入侵检测等方面的专门技术，通过网络监听软件，系统管理员可以观测分析实时经由的数据包，从而快速地进行网络故障定位，为网络管理带来极大的方便，但被攻击者使用时也给以太网安全带来了极大的隐患，经常会造成口令失窃、敏感数据被截获等安全事故的发生。对付监听的最主要的办法是对传输数据进行加密，如果采用加密软件，数据的加密和解密运算就需要占用大量 CPU 的资源，虽然 PC 的 CPU 速度越来越快，但在这些运算面前，还是显得有些力不从心，从而降低了信息传输的效率，难免导致计算机系统性能下降。本文在论述嵌入式安全网卡的结构、功能和网络监听原理、检测、防范的基础上，重点讨论嵌入式安全网卡在网络监听中的应用。

1 嵌入式安全网卡

嵌入式安全网卡是将安全功能分布到网络中的各个子网、桌面系统、笔记本计算机以及服务器上。分布于整个网络内的嵌入式安全网卡使用户可以方便地访问信息，而不会将网络的其他部分暴露在潜在的非法入侵者面前，避免发生由于某台端系统被入侵，而导致入侵向整个网络蔓延的情况。

本嵌入式安全网卡分布在企业的整个网络或服务器中，因此，它具有无限制的扩展能力。随着网络的增长，它们的处理负荷也在网络中进一步分布，它们的高性能可以持续保持，而不会像边界式网络安全设备一样随着网络规模的增大而不堪重负。

1.1 嵌入式安全网卡的组成

嵌入式安全网卡包括硬件和软件 2 部分。硬件包括微处理器、存储器、外设器件及 IO 端口。软件部分包括嵌入式实时多任务的操作系统和网络安全应用程序。

(1)硬件部分

嵌入式安全网卡以具有ARM内核的嵌入式微处理器为核心，操作系统选用嵌入式系统专用的开放源代码的实时操作系统——μC/OS-Ⅱ[1]。它的开发有 2 个并行的技术线：1)开发以ARM内核为基础的加密芯片；2)开发以通用ARM内核C和RTOS为基础的嵌入式网络安全套件。

加密芯片采用RISCDSP结构[2]，将独立的RISC处理器和独立的DSP集成在一个芯片上，二者的指令流与数据流分离。RISC处理器采ARM9 系列内核，完成通用CPU的计算与调度，DSP内含大数模运算单元、加密算法模块、随机数发生器等多种加密模块单元。利用该模块的各加密运算功能，最大限

基金项目：广东省科技攻关基金资助项目(2005B10101067)；广州市科技攻关基金资助项目(2005Z3D0291)
作者简介：巫喜红(1975－)，女，讲师、硕士研究生，主研方向：信息安全技术，网络安全，软件工程；凌 捷，教授、博士
收稿日期：2006-07-30 **E-mail：**jdwxh@jyu.edu.cn

度地提高整个嵌入式安全卡的操作速度。与加密芯片密切相关的一个重要部分是外接存储单元，在网卡上设置了一个4MB的外接存储模块接口，通过外接存储单元，对密钥进行存储和管理。

嵌入式安全套件以嵌入式微处理器为核心，在嵌入式操作系统基础上运行各种网络安全应用程序。操作系统及重要数据以文件形式保存在 FLASH 存储器中；安全策略可通过网络进行更新；数据和报警信息可通过 PCI 或 PCMICA 接口向主机传输，也可通过以太网口向网管或 Inernet 发布信息。用户通过主机 GUI 界面查看设备状态，设置设备参数，对安全套件实现监控和维护。根据嵌入式安全网卡的布置方式不同，这些操作也可由网管依照统一的安全策略，以集中管理的方式通过网络完成。

考虑一般网络安全系统对嵌入式系统功能的要求，嵌入式安全网卡硬件部分的主要组成包括微处理器、PCI(或PCMCIA)总线连接器、时钟、接口控制与逻辑芯片、扩展存储单元及程序调试接口等[3]。其结构见图 1。

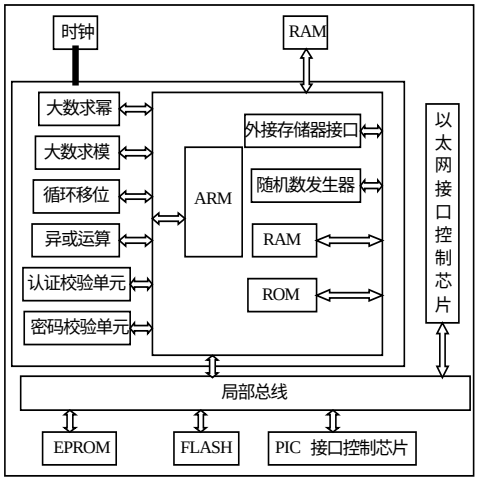

图 1　嵌入式安全网卡结构

(2)软件部分

软件部分有：1)设备驱动程序的编写，如微端口驱动程序、中间层驱动程序、协议驱动程序；2)用户应用程序的编写，如对用户密钥进行管理(密钥管理包括：密钥分发，密钥导入，密钥存储，密钥备份，密钥访问和密钥更新)、提供用户二次开发的接口、对各安全模块的配置与查询功能(均以图形化用户友好界面提供)、远程安全策略管理(管理员可以利用中心管理软件对服务器进行远程管理，实现总体安全策略的策划、管理、分发及日志的汇总、故障诊断模块)。嵌入式安全套件包括嵌入式防火墙、VPN、网络隔离设备、硬盘保护与恢复、加密机。

1.2　嵌入式安全网卡的功能

由于嵌入式安全网卡以ARM内核的SoC和实时操作系统的嵌入式系统[4]为核心，因此它的功能归纳起来主要有以下几点：

(1)以 PCI 和 PCMCIA 网卡为载体，通过引入 SoC 和嵌入式系统，在一个普通的网卡上集成防火墙、VPN、网络隔离设备、信道加密、加密机等网络安全功能，使网卡成为实施网络安全策略的目标设备；

(2)通过引入 SoC 设计方法，在 ARM 内核的基础上设计出通用加密芯片，完成分组加密、序列加密、不对称加密常用算法的芯片化实现，能提高加解密速度；

(3)实现基于网络的对嵌入式安全网卡的维护和升级；

(4)实现网络数据安全的传送。

2　网络监听技术

2.1　基本原理

网络监听软件是提供给系统管理员使用的用于监视网络状态、数据流动情况以及网络上传输信息的管理工具[5]。将网络接口设置为混杂工作模式(Promiscuous)后，便可以源源不断地监听到同一网上传输的信息。网络监听可以在网上的任何一个位置实施，如网关、路由器、远程网的调制解调器或者是网络系统中的某一台主机，它常常被用来获取用户的口令。目前嗅探器(Sniffer)就是最常见，也是最重要的技术之一，它可以是硬件产品或软件产品。

2.2　检测方法[6]

网络监听是很难被发现的。运行网络监听的主机只是被动地接收在局域网上传输的信息，并没有主动行动。既不会与其他主机交换信息，也不能修改在网上传输的数据包。这一切决定了网络监听的检测是非常困难的，一般采用下面的方法来进行检测。

(1)网络通信掉包率异常高。如果网络中有人在监听，那么信息包传送将无法每次都顺畅地传到目的地(这是 Sniffer 拦截每个包导致的)。

(2)网络带宽将出现反常。如果某台计算机长时间地占用了较大的带宽，对外界响应很慢，这台计算机就有可能被监听。在非高速信道上，如 56KDDN 等，如果网络中存在 Sniffer，应该也可以察觉出网络通信速度的变化。

(3)通常一个 Sniffer 的记录文件会很快增大并填满文件空间。在一个大型网络中，Sniffer 明显加重计算机负荷，这些警告信息往往能够帮助管理员发现 Sniffer。

(4)一个主机上的 Sniffer 会将网络接口置为混杂模式以接收所有数据包。对于某些 Unix 系统，通过监测混杂模式的网络接口来判断是否被监听。虽然可以在非混杂模式下运行 Sniffer，但这样只能捕获本机会话。只有在混杂模式下才能捕获以太网中的所有会话，其他模式只能捕获本机会话。

(5)对于怀疑运行监听程序的机器，用正确的 IP 地址和错误的物理地址去 ping，运行监听程序的机器会有响应。这是因为正常的机器不接收错误的物理地址，处于监听状态的机器能接收，如果它的 IPstack 不再次反向检查，就会响应。这种方法依赖于系统工程的 Ipstack，对一些系统可能行不通。

(6)往网上发大量不存在的物理地址的包，由于监听程序处理这些包，将导致性能下降。通过比较前后该机器的性能(icmp echo delay 等方法)，加以判断，这种方法难度比较大。

2.3　常用的网络监听防范措施

(1)数据加密

使用加密技术后，Sniffer 依然可以监视到信息的传送，但显示的是乱码，除非加密算法被破解。一些加密技术的缺点是速度问题和使用一个弱加密术比较容易被攻破。几乎所有的加密技术都将导致网络的延迟，加密越复杂，网络速度就越慢。如果一个黑客正在网络上运行 Sniffer 并发现所有收集到的资料都是乱码，那么大多数会转移到其他的没有使用加密术的站点上。

(2)使用交换机

随着交换机的成本和价格的大幅度降低，交换机已成为非常有效的使 Sniffer 失效的设备。目前最常见的交换机在第 3 层(网络层)根据数据包目标地址进行转发，而很少采用集线

器的广播方式，从理论上讲，通过交换机设备对网络进行分段后，Sniffer 将无法透过边界来窥探另一边的数据包。但是，这是在边界设备不转发广播包的情况下，一旦入侵者使用 spoofer 诱骗某个边界设备而将自己的广播包流入不该进入的网段后，原理上还是在一个共享设备端使用 Sniffer，而实际上将是听到了边界的另一边。

(3)以交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后，局域网监听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，2 台机器之间的数据包(单播包)还是会被同一台集线器上的其他用户所监听。

因此，应该以交换式集线器代替共享式集线器，使单播包仅在 2 个节点之间传送，从而防止非法监听。当然，交换式集线器只能控制单播包而无法控制广播包(broadcast packet)和多播包(multicast packet)。但广播包和多播包内的关键信息远远少于单播包。

(4)使用虚拟局域网(VLAN)技术

运用VLAN技术，将以太网通信变为点到点通信，可以防止大部分基于网络监听的入侵。

3 安全网卡在网络监听中的应用

3.1 安全网卡在数据传输中的作用

不论是单通道DMA还是多通道DMA，在数据经由主机到网卡或由网卡向上传输的过程中，都要经过一个缓冲区。主机可以以程序方式或DMA方式与此缓冲器交换数据，同时它也要在数据包的发送和接收过程中在DMA的控制下与NIC进行快速数据交换。在主机和缓冲存储器间放置一个协处理器，它对传递的信息进行逻辑判断，如果传送中的数据需要进行加密运算和IPSec安全处理，则由它把数据送往网卡和IPSec处理模块，完成数据的处理后，把数据送往缓冲区。接收缓冲区的数据同样经过协处理器的识别，需要经过解密运算和IPSec处理的数据同样会发送到加密机处理模块进行预处理。传送中的数据如果不需要进行处理，则直接送往缓冲存储区[7]。原理框图见图 2。

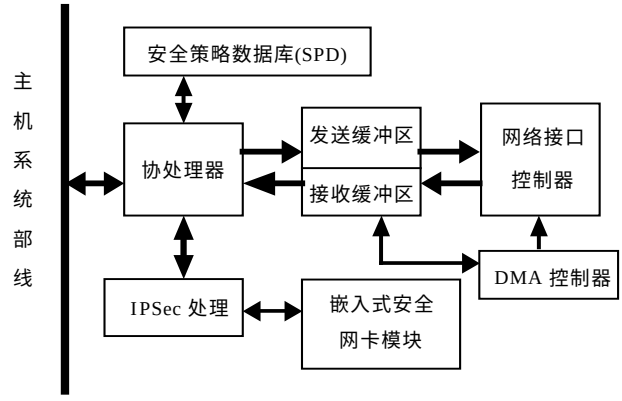

图 2 数据安全处理原理

协处理器模块主要完成 2 个功能：(1)与主机进行通信，执行主机的命令；(2)对进入和外出的数据包进行判断是否需要进行 IPSec 处理。首先处理器模块从主机内存中取出要发送的数据，然后对数据的合法性进行判断，不符合发送数据包要求的则丢弃，否则通过查询 SPD。进一步对它判断是否需要进行安全处理，不需要的送到缓冲区，否则由 IPSec 处理模块进行安全处理。

IPSec 处理模块主要对发送和接收的数据进行安全处理，用来保证数据的机密性和完整性。对进入和外出的数据包采用类似的处理。

加密机处理模块主要是对数据进行加解密，它以加密芯片为基础，开发软硬件结合的加密方式[3]。除满足VPN对加密功能的需要外，还可应用在安全套接层(SSL)服务器、安全电子交易(SET)服务器等众多需要加密运算的场合，解决加密运算的瓶颈。加密机软件部分包括 3 个层次：

(1)实现 RSA,MD5,DES 和 3DES 等其他加密算法应用程序，及与加密芯片的接口程序。

(2)应用编程接口(API)，为用户的使用和 2 次开发提供强大而友好的应用接口。

(3)密钥管理程序，是整个加密机系统的安全核心，密钥管理涉及到密钥生成、分发、导入、存储、备份、访问、更新等几个环节。

3.2 安全网卡的应用

采用软件加密方法，对自身的数据进行加密以实现网络监听是一个较好的措施，但是，如果计算机系统忙于处理复杂繁琐的加解密运算，则无暇顾及其他的任务，如果所收到的信息量超过自己的处理能力，将会造成系统的崩溃。而嵌入式安全网卡中的一个重要部件就是加密机，它能采用不同加解密算法对数据进行加解密，还能解决加密运算的瓶颈，它所特有的功能使得计算机成为一台加密的计算机，达到防范网络信息监听的目的。

4 结束语

嵌入式安全网卡在一定程度上保障了数据的安全传输，网卡的安全性越高，数据的安全性也越高，网络虽然被监听，但传输的信息被破译的可能性就越小。采用嵌入式安全网卡的加密解决方案的优越性会越来越明显，今后一定会得到广泛的应用。

参考文献

1 Labrosse J L. 嵌入式实时操作系统-Ⅱ[M]. 北京: 北京航空航天大学出版社, 2003.

2 罗胜钦. 数字集成系统芯片(SoC)设计[M]. 北京: 北京希望电子出版社, 2002.

3 陈日午, 刘 航, 慕德俊. 一种嵌入式安全网卡总体设计[J]. 西北工业大学学报, 2005, 23(2): 261-265.

4 WayneWolf. 嵌入式计算系统设计原理[M]. 北京: 机械工业出版社, 2002.

5 李 霞, 陆际光. 网络监听的检测与防御[J]. 中南民族大学学报, 2002, 21(1): 67.

6 巫喜红. 知己知彼, 百战不殆——网络监听技术和防范的研究[J]. 五邑大学学报, 2004, 18(1): 68.

7 曹卫兵. 基于 IPSec 安全协议的网卡安全技术研究[D]. 西安: 西北工业大学, 2001-03.