基于 ARM 的数据包提取转发机制的研究

张功萱, 王平立, 何广生, 张 冲

(南京理工大学 计算机学院, 江苏 南京 210094)

[摘要] 提出了基于 ARM 的数据包提取转发机制. 机制的主要任务由改进的数据包提取转发模型 ENSS系统模块承担, 该模块是在一个独立于 Windows操作系统的硬件平台上运行的一个高安全的系统处理平台. 采取 Netfilter钩子钩取从一个网卡链路层的数据包提取到网络层, 由 ARM 的安全处理模块进行处理, 然后由另一个网卡发送出去. ENSS系统模块取得了良好效果, 为其网络安全处理提供了高速稳定的通信平台.

[关键词] 数据包, 钩子函数, 转发, 安全处理

[中图分类号] TP 393 08 [文献标识码] A [文章编号] 1672-1292(2008) 04-0145-05

Research of Data Packet Extraction and Transfer Mechanism Based on ARM Processor

Zhang Gongxuan, Wang Pingli, He Guangsheng, Zhang Chong

(School of Computer, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract A data packet extraction and transfer mechanism based on ARM processor is proposed, whose main tasks are processed by an improved data packet extraction and transfer model ENSS module, an independent from Windows system, and high secure system platform (called ENSS system card). The data packet is hooked from the data link layer into network layer through a NIC and processed by the ARM secure process, and then transferred away through another NIC. With the test, ENSS system card has better performance and can provide a higher stable communication platform for the network secure processing.

Key words data packet, hook function, transfer, secure processing

随着计算机技术和网络技术的迅猛发展, Internet正在越来越多地融入到社会的各个方面, 成为实现信息收集处理、加强交流、提高工作生活效率和质量的重要方式. 然而, 信息网络的普及和网络协议的缺陷, 以及终端主机操作系统的潜在漏洞给我们带来了新的安全威胁, 使得人们在受益网络所带来的快捷便利的同时, 也正受到日益严重的网络安全威胁[1]. 本文的设计思想是: 在一个独立于 Windows系统的硬件平台 (称为主核系统) 上运行一个高安全的操作系统作为安全处理平台 ENSS(嵌入式网络安全系统, 称为辅核系统). 也就是说, 硬件体系结构采取保持主机系统的软硬件结构不变、增加辅处理系统的方法, 即异构的双处理器体系结构, 且 ENSS系统制成板卡形式插入主机系统 PCI插槽中. 由于将安全处理模块与 Windows操作系统相分离, 且做到 Windows系统与外网物理上的隔离, 克服了传统基于软件的网络安全防护技术的固有缺陷.

对用户来说, ENSS系统卡就是一个普通的 I/O 接口网卡, 对 Windows主机来说, 该系统就是主机的安全隔离卡 . ENSS系统 PCI总线接口芯片的主要功能是实现 32位 PCI总线与 8位的双端口存储器的连接. 双端口存储器起到对数据缓存的作用. ARM 核心板包括 ARM 处理器 S3C2410、SDRAM、FLASH、以太网控制器等必需芯片. 安全处理的主要功能都在 ARM 核心板卡上实现, 在 ARM 板上运行高安全的嵌入式操作系统 Linux系统[2].

收稿日期: 2008-06-18

基金项目: 国家 863 计划 (2006AA01Z447)资助项目.

通讯联系人: 张功萱, 教授, 博士, 研究方向: 多核与嵌入式计算技术、分布式计算技术和 Web服务与信息安全. E-mail: gongxuan@mail.njust.edu.cn

1　Linux内核网络基础理论

1.1　Linux内核网络报文处理

套接字缓冲体系(sk_buff数据结构)是 Linux网络实现灵活性和高效性的一个主要因素,它提供一套管理缓冲区的方法,每个 sk_buff包括一些控制方法和一块数据缓冲区,该区域存放了网络传输的数据包. sk_buff组成双向链表的形式,可实施删除链头元素和添加到链表尾等操作.网卡接收到数据帧后,系统内核为所收数据帧分配一块内存,并将数据整理成 sk_buff的结构,数据以 sk_buff的形式在网络各层之间传递、处理.

(1) sk_buff的结构. sk_buff主要成员如下:

struct sk_buff* next, prev:用来链接由 sk_buff组成的套接字缓存队列;

struct sk_buff_head * list:指向套接字缓存在队列中的当前位置;

struct net_device* dev:表明套接字缓存当前操作所在的网络设备;

h, nh, mac:分别指向传输层(h)、网络层(nh)和 MAC层(mac)的报文帧头的指针;

struct dst_entry* dst:指向路由高速缓存中的一条记录;

unsigned char pkt_type:报文的类型;

unsigned int len:指明套接字缓存所代表的报文长度,只考虑内核可访问的数据;

unsigned char * head,* data,* tail,* end:data和 tail指向当前有效报文数据.

(2) sk_buff的管理. Linux内核提供了一套针对套接字缓存 sk_buff的操作,从而很容易地改变对列管理的实现方式.本文涉及的主要操作有: alloc_skb(size, gpf_mask)、dev_alloc_skb(length)、skb_copy(skb, gfp_mask)、skb_clone()、kfree_skb()、skb_put(skb, len)、skb_push(skb, len)等. sk_buff的套接字缓存队列由 Linux内核队列层通过构建数据结构 struct softnet_data来管理, softnet_data结构包含一个指向接收队列的头指针.

1.2　Linux内核协议栈框架

Linux内核中每个网络设备都对应一个设备驱动程序模块;独立于设备的接口模块为所有网络设备提供了统一的视图,在子系统的高级别上无需关心所使用硬件的特定知识.图 1给出了 Linux内核协议栈的网络数据流程图.

这样,网络接口模块提供一个独立于网络设备和网络协议的接口,其它内核子系统通过该接口模块来访问网络,这种结构具有很强的可扩展性.一方面,新网络协议的开发只需面向抽象接口,可专注于本协议专用操作;另一方面,用户进程和其它内核子系统在访问网络时也只需了解协议的接口[3].

当网卡接收数据时, sk_buff由网络驱动程序的接收例程产生,封装所接收的数据包并送到网络数据包接收队列,通过系统软中断机制进入协议处理层,经过网络层和传输层处理后,把数据递交到 socket;数据发送时, sk_buff在用户通过 socket向下发送并进入协议处理层时分配.图 2给出了发送和接收过程中具体涉及的函数[4,5].

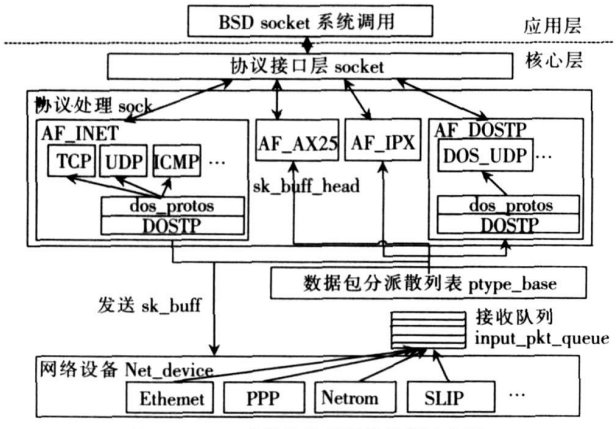

图 1　Linux 内核协议栈网络数据流程图

Fig.1　Network data flow of Linux kernel

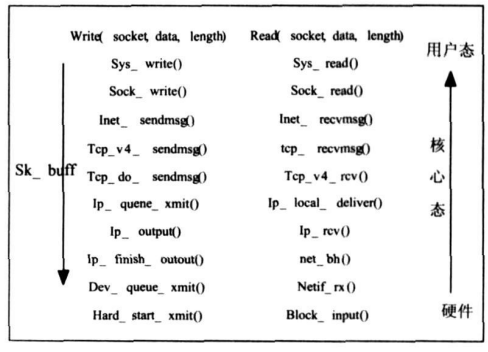

图 2　Linux 内核协议栈函数调用流程

Fig.2　Functions call flow of Linux kernel

2 辅核数据包提取转发模型

2 1 数据包提取转发模型提出

ENSS系统主要对 W indow s主机的网络数据进行安全处理, 主要包括对 IP数据包进行一些安全过滤, 例如数据包过滤、访问控制、端口检测等, 它处于 L inux网络协议栈的网络层, 如图 3所示. W indow s主机发送出去的数据包的数据流程为经过 A、B、C、D、E后发送到外部网络中. W indow s主机接收的数据包的数据流程为经过 a、b、c、d、e后发送到 W indow s主机中. 其中, 辅核提取转发模块完成的功能有两个方面: 将主辅核通信模块以及辅核外网通信模块的数据包提取到网络层, 让网络安全处理模块进行处理; 在网络层经安全处理后的数据包从另一方向发送出去, 让整个辅核系统能够为 W indow s主机和外网通信提供桥梁.

本文采取 Netfilter钩子钩取从一边网卡链路层提取到网络层的数据包, 经过安全处理时由另一边网卡发送出去. Netfilter是 L inux2 4版本以上内核中实现包过滤、NAT 和包处理等的功能模块, 主要包括钩取、注册、用户空间队列 3个功能[6]. N etfilter钩取数据包基本原理是: 在整个网络流程的若干位置放置一些钩子 (HOOK), 且在每个钩子处登记一些处理函数对数据包进行处理. 在一般的防火墙中需要两块网卡, 本文的双端口存储器模拟网卡作为输入端, CS8900A 作为输出端, 并在 L inux内核中应用 Netfilter框架. 根据此思路, 本文提出了一种改进的数据包提取转发模型　　ENSS系统通信模块总体模型, 如图 4所示.

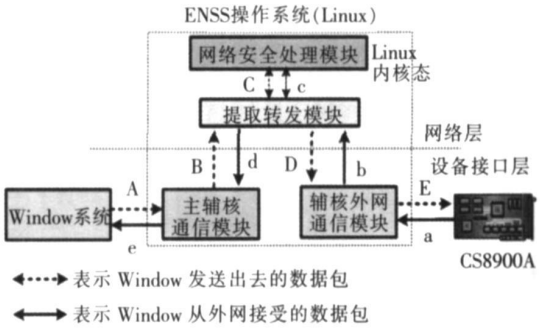

图 3 辅核系统网络数据流程图

Fig.3 Network data flow of slave-core

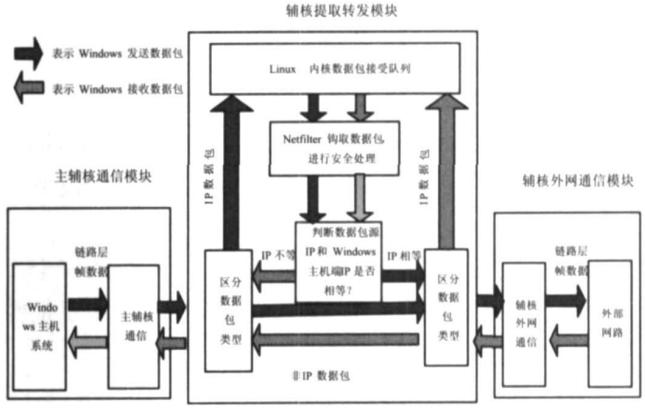

图 4 ENSS 系统通信模块总体模型

Fig.4 Communication model of ENSS

2 2 数据包提取转发模型功能组成

ENSS通信模块总体上分为数据包上提、钩取和转发模块 3个部分.

(1) 数据包上提: 主要针对 IP数据包进行安全处理, 数据包提取模块从设备接口层的双端口存储器或 CS8900A接收到的数据包中, 将 IP类型的数据包提交到 Linux内核的数据包接收队列中, 并触发软中断, 等 Linux空闲的时候对队列中数据包进行安全处理.

(2) 基于 Netfilter的数据包钩取: 存放于数据接收队列中的数据包用 N etfilter钩取并由安全处理程序进行安全分析.

(3) 数据包转发: 将安全处理后的数据包发到外网中. W indow s发送数据包时, PC – ARM 通信模块接收该数据包, 并交给 ENSS提取转发模块. 该模块将数据包提交给安全处理模块处理, 然后将数据包发送给辅核外网通信模块处理. W indow s接收数据包的流程与此相反.

3 主要例程实现技术

3 1 数据包上提

在双端口存储器或者 CS8900A 产生中断时, 中断处理函数从硬件读取接收的数据包, 然后提取程序将数据包提取到 L inux内核接收队列. 数据包上提程序关键代码如下:

```
static void Put_To_Net(struct sk_buff*  skb) / 提取 IP数据包
```

```
{
    if(skb->pkt_type==PACKET_OTHERHOST)
        skb->pkt_type=PACKET_HOST; //改为去往本地,使得数据包能上提到网络层
    //判断如果是 IP数据包并到达本地则上传到网络层
    if((skb->pkt_type==PACKET_HOST)&&(IS_IP_PACKET(ppacketdata)))
    {
        netif_rx(skb); //上传到 Linux内核数据包接收队列中
            }else
    {   Send_CS8900A_skb(skb); //直接发送到 CS8900A芯片
            }}
```

3.2 数据包钩取

对于从双端口接收并提取的数据包,采用 Netfilter截取数据包,并进行安全处理.

首先要在 Linux内核中配置 Netfilter选项,重新编译烧写内核.注册钩子函数时先要描述钩子接口数据结构 struct nf_hook_ops,本文通过调用 nf_register_hook(&pf_hook_ops)注册钩子函数.有数据包时,回调函数 pf_hook_ops将被调用.

3.3 数据包转发

pf_hook_ops为钩子回调函数,参数中包括钩取的数据包,安全处理模块可对该数据包进行安全处理,处理后的数据包通过调用链路层接口函数发送到 CS8900A芯片或者双端口存储器.数据包转发流程主要分为如下几个过程:

(1) 获取数据包,并判断数据包 IP地址;

(2) 根据从 Windows主机获取的配置信息得到 Windows主机的 IP或者 MAC地址,并以此 IP或 MAC地址和数据包中 IP或 MAC地址做比较,判断数据包来源,本文中也可以通过 MAC地址来判断数据包来源;

(3) 对数据包进行安全处理,判断数据包是否安全;

(4) 对不安全的数据包丢弃,并向 Windows主机报警;对安全的数据包,调用 Send_ouNet或者 Send_inNet将数据包发送到目的网络.

4 运行效果与结论

ENSS系统的通信模块由 PC-ARM通信 dpsram.ko,ENSS外网通信 cirrus.ko,提取转发模块 fw.ko等 3个目标文件组成.这些程序可通过超级终端下载到 ENSS系统板卡中并动态加载,同时 Windows端也必须安装定制的相关驱动程序.安装完毕后就可测试该系统的通信情况,如图 5所示.其中, "send Dp-sram packetlength is 1514"表明外网数据包通过双端口存储器发送到 Windows主机的数据包长度为 1514; "send CS8900A packetlength is 92"表明 Windows主机发送经 CS8900A传递到网络的数据包长度为 92.由此可见,ENSS辅核通信模块取得了良好效果,为其网络安全处理提供了高速稳定的通信平台.

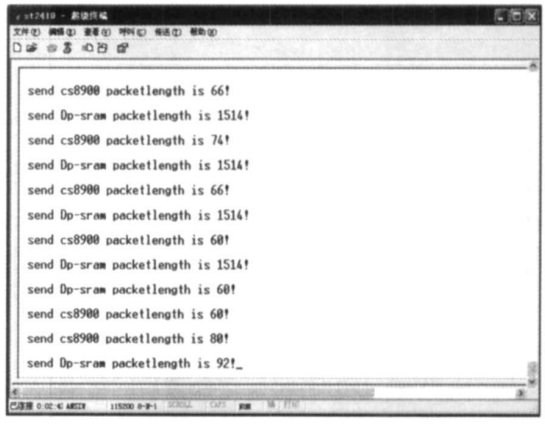

图 5 辅核系统运行情况

Fig.5 Running demo of slave-core system

[参考文献] (References)

[1] 葛广超.嵌入式防火墙的研究与实现[D].南京:南京航空航天大学, 2006.
Ge Guangchao. Research and implementation of embedded firewall[D]. Nanjing: Nanjing University of Aeronutics and Astronutics, 2006. (in Chinese)

[2] Linux与 Windows的系统安全性比较[J/OL]. [2005-01-06]. http://www.hc360.com.
Security comparison between Linux and Windows[J/OL]. [2005-01-06]. http://www.hc360.com. (in Chinese)
[3] 唐续, 刘心松, 杨峰. Linux网络协议栈分析及协议添加的实现[J]. 计算机科学, 2003, 30(2): 130-132.
Tang Xu, Liu Xinsong, Yang Feng. Linux network protocol analysis and protocol addition implementation[J]. Computer Science, 2003, 30(2): 130-132. (in Chinese)
[4] 李善平. Linux内核 2.4版源代码分析大全[M]. 北京: 机械工业出版社, 2004.
Li Shanping. Source Codes Analysis Guide of Linux 2.4[M]. Beijing: China Machine Press, 2004. (in Chinese)
[5] 李长河, 杜辉天, 吕林涛. 一种小型嵌入式 TCP_IP协议栈的设计与实现[J]. 微电子学与计算机, 2003(6): 40-43.
Li Changhe, Du Huitian, Lv Lintao. Design and implementation of new mini-embedded TCP_IP protocols[J]. Microelectronics & Computer, 2003(6): 40-43. (in Chinese)
[6] 毛新宇. Linux内核防火墙 netfilter的原理和应用[J]. 微型机与应用, 2004(4): 35-37.
Mao Xinyu. Principle and application of Linux kernel firewall — netfilter[J]. Microcomputer & Its Applications, 2004(4): 35-37. (in Chinese)

[责任编辑: 丁蓉]

(上接第 98页)

[9] 徐凤亚, 罗振声. 文本自动分类中特征权重算法的改进研究[J]. 计算机工程与应用, 2005(1): 181-184.
Xu Fengya, Luo Zhensheng. An improved approach to term weighting in automated text classification[J]. Computer Engineering and Applications, 2005(1): 181-184. (in Chinese)
[10] 张云涛, 龚玲, 王永成. 文本分类中 TFIDF方法的改进[J]. 浙江大学学报, 2005, 6A(1): 49-55.
Zhang Yuntao, Gong Ling, Wang Yongcheng. An improved TF-IDF approach for text classification[J]. Journal of Zhejiang University, 2005, 6A(1): 49-55. (in Chinese)
[11] 寇莎莎, 魏振军. 自动文本分类中权值公式的改进[J]. 计算机工程与设计, 2005, 26(6): 1616-1618.
Kou Shasha, Wei Zhenjun. Improved weighting formula in auto text classification[J]. Computer Engineering and Design, 2005, 26(6): 1616-1618. (in Chinese)
[12] 李荣陆. 文本分类系统[DB/OL]. http://www.nlp.org.cn/docs/download.php?doc_id=102 2004-08-19.
Li Ronglu. Text classication system[DB/OL]. Data Set, http://www.nlp.org.cn/docs/download.php?doc_id=102 2004-08-19. (in Chinese)
[13] David D. Lewis. Reuters-21578, Test Collections[R/OL]. http://www.daviddlewis.com/resources/testcollections/reuters21578/. 1996.

[责任编辑: 顾晓天]