文章编号: 1008-1534(2011)03-0164-03

基于 ARM-Linux 的防火墙设计

刘泽玲

(河北城乡建设学校, 河北石家庄　050031)

摘　要: 设计并实现了以 ARM11 内核 S3C6410 处理器和 2 片 DM9000 网卡控制器为平台的主动防火墙硬件平台, 设计了 DM9000 的 Linux 驱动, 以 Linux 操作系统的 Netfilter 防火墙框架为基础加入入侵检测模块和响应模块, 形成一个以规则策略集为中心的集检测、防护和响应为一体的主动防御系统。

关键词: 防火墙; ARM; Linux; 主动防御系统

中图分类号: TP391　　文献标志码: A

Design of firewalls based on ARM-Linux

LIU Ze-ling

(College of Urban and Rural Construction, Shijiazhuang Hebei 050031, China)

Abstract: A hardware platform of active firewall by using ARM11 kernel S3C6410 and two DM9000 NIC controllers is put forward. The Linux driver of DM9000 is designed. Then a kind of active defense system including functions of detection, protection and responding, centering about rule sets, is constructed by adding the intrusion module and response module into the firewall Netfilter of Linux.

Key words: firewall; ARM; Linux; active defense system

随着互联网的发展和广泛应用, 网络安全问题也日益受到关注。在众多的网络安全技术中, 防火墙是其中主要的一种。防火墙是设置在被保护网络和外部网络之间的一道屏障, 以防止发生不可预测的、潜在的破坏性的侵入[1-2], 它是一种较早出现的网络安全保障技术, 也是现阶段网络安全解决方案中重要的组成部分, 伴随着互联网的快速发展而得到广泛的应用。这些防火墙通常置于网络的入口处或内部网络的边缘, 因此也称为 边界防火墙 。防火墙技术的开发及准确的系统配置和管理对于正确地发挥其在安全方面的功能至关重要。

笔者设计并实现了以 ARM11 内核 S3C6410 处理器和 2 片 DM9000 网卡控制器为平台的主动防火墙硬件平台, 并将主动防火墙软件系统移植到该平台上, 实现了嵌入式系统中对具有双网卡防火墙系统的配置。

1　硬件系统设计

1.1　整体设计

硬件系统主要由 CPU 和网络控制器组成。CPU 选用三星的 S3C6410, 它采用 ARM1176JZF-S 的核, 包含 16 KB 的指令数据 Cache 和 16 KB 的指令数据 TCM, ARM Core 电压为 1.1 V 的时候, 可以运行到 553 MHz, 在 1.2 V 的情况下, 可以运行到 667 MHz。网络控制器选择 DM9000, 它是 DAVICOM 公司的(10/100) Mb/s 自适应的低功耗快速以太网芯片, 成本相当低廉。它支持 8 位、16 位、32 位数据总线宽度, 集成了 MAC(媒体控制访问子层协议)控制器, 3.3 V 接口电平, 容易使用, 还可以使用 MII 接口和片外的 PHY 芯片连接, 可

收稿日期: 2011-01-22; 修回日期: 2011-03-09
责任编辑: 李　穆

作者简介: 刘泽玲(1972-), 女, 河北沧州人, 讲师, 主要从事教学研究与管理方面的工作。

以容易地完成不同系统的软件驱动的开发。防火墙的硬件系统整体设计见图 1。

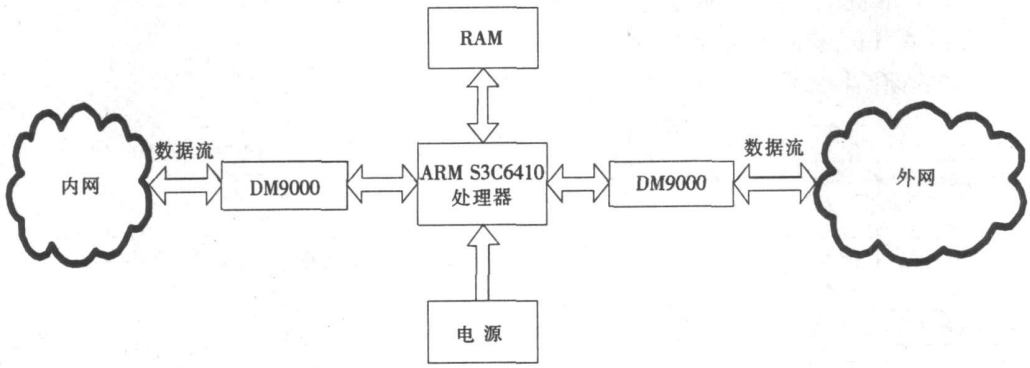

图 1　防火墙硬件平台整体设计图

Fig. 1　Overall design of firewall hardware

1.2　DM9000 和 S3C6410 处理器的逻辑连接

在 S3C6410 处理器上连接 2 片 DM9000 网卡控制器 eth0 和 eth1, 网卡连接的片选信号和中断信号如下。

eth0: 片选信号为 ncsn4, 中断号为 int8; eth1: 片选信号为 ncsn5, 中断号为 int9。

处理器与网卡的连接图见图 2。

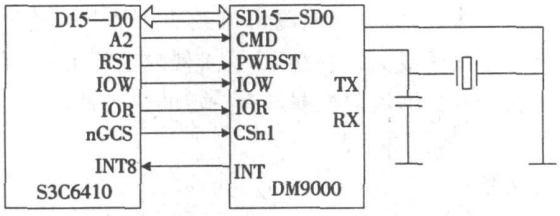

图 2　DM9000 和 S3C6410 处理器的逻辑连接图

Fig. 2　Logical connection of DM9000 and S3C6410

图 2 中表示了处理器和 1 片 DM9000 网卡控制器的逻辑连接。DM9000 是 16 位的。将 S3C6410 处理器的 D15　D0 与 DM9000 网卡控制器的 SD15　SD0 相连接。CMD 信号是地址/数据线, 该信号决定传输的是地址还是数据, 根据软件的设计, 将其连接到 A2 上。IOR 和 IOW 是读写信号, 分别将这 2 个信号与处理器的读写信号相连。INT 是中断信号, 与处理器的 1 个中断源相连, 其中 eth0 连接处理器的中断号 int8, eth1 连接处理器的中断号 int9。TX 和 RX 都与网络变压器相连, 之后连上 RJ45 口。CSn1 是片选信号, 与处理器的 nGCS 连接, 其中 eth0 连接 nGCS4, eth1 连接 nGCS5。Reset 复位信号与 CPU 使用同一个复位信号。

2　软件系统设计

防火墙系统的软件包括操作系统、驱动程序和防火墙 3 部分。本系统采用 Linux 系统作为操作系统, 并在此基础上设计了 DM9000 驱动程序, 最终实现了防火墙系统的设计。

2.1　网络驱动设计

Linux 网络驱动程序的体系结构可划分为网络协议接口、网络设备接口层、网络应用功能的设备驱动功能层和网络设备媒介层。

网卡设备驱动程序的设计主要是对网卡设备进行描述、初始化和注册, 之后实现网卡的接收和发送的功能[3-4]。在进行网卡驱动程序的设计时, 主要做的工作和实现的功能有以下 3 个方面[5-8]。

1) 网络设备描述　与其他的硬件设备一样, 每个网络接口都会由 1 个 net_device 结构来描述。描述网络设备的结构可以使用如下内核函数动态分配。

Struct net_device * alloc_netdev(int sizeof_priv, const char * mask, void(* setup) (struct net_device *)); 或 Struct net_device * alloc_etherdev (int sizeof_priv)。其中: sizeof_priv 指的是私有数据区大小; mask 指的是设备名; setup 是初始化函数。

2) 网络设备的注册　网络接口的驱动注册中没有主次设备号, 这和字符驱动有所不同。设备注册的函数为

int register_netdev(struct net_device * dev)。

3) 网络设备的初始化　网络设备的初始化工作主要是由结构体 net_device 中的 init 函数指针所指向的初始化函数来完成。初始化函数原型如下:

int (* init) (struct net_device * dev) /* 初始化函数, 该函数在注册时被调用, 来完成对 net_device 的初始化* /。

2.2 防火墙设计

本文中研究的主动防火墙是以 Linux 操作系统中自带的 Netfilter/ iptables 防火墙框架为基础的。Netfilter/ iptables 在 Linux 内核的版本为 2.4 或 2.6, Netfilter 的框架结构见图 3。

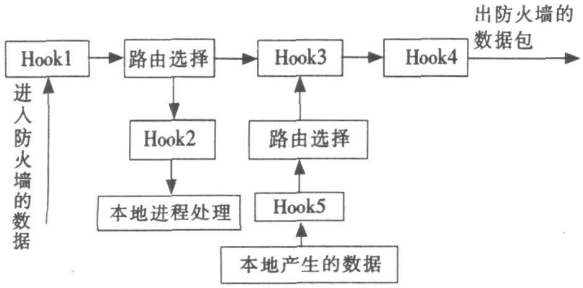

图 3 Netfilter 在 IPV4 中的结构

Fig. 3 Structure of Netfilter in IPV4

流经防火墙的数据报文从左面进入过滤框架, 首先进入 Hook1, 进行规则过滤, 如果通过了 Hook1 的规则过滤, 则进入路由选择, 由路由决定数据报文是继续转发给其他的网络, 还是传递给本地进程处理。如果是转发给其他网络的则进入 Hook3, 继续则转发给 Hook4; 如果是发给本地进程处理则发给 Hook2, 进而由本地进程接收进行处理。最后, 转发出去的数据报文通过 Hook4 的过滤后发送给其他的网络。在防火墙框架中的 5 个钩子点中, 协议栈主要是将数据报和钩子函数的标号作为参数进行调用。

防火墙中加入入侵检测模块, 并不是整个入侵检测系统都嵌入到防火墙中, 而是具有检测功能的一个模块, 主要目的是实现对流经防火墙的数据流进行入侵行为的检测。在了解了 Linux 系统的 Netfilter/ iptables 防火墙的框架及其工作流程之后, 为了可以捕捉到流经防火墙的数据包并进行检测, 可以通过将入侵检测模块挂载到 Netfilter 框架的钩子点处来实现。入侵检测模块挂载到防火墙的钩子点处后, 每当有数据包经过该钩子点时就会调用入侵检测模块, 实现对数据报文的入侵检测。

入侵检测模块的工作流程可以分为数据包的捕获, 数据包分析及特征的提取, 检测数据包等几个部分, 其工作流程见图 4。

3 结 论

为了保证入侵检测模块的功能, 对入侵检测模块的测试中使用的数据来自 KDDCup99 数据集。数据集 KDDCup99 是由美国国防部高级研究计划局与麻省工学院的林肯实验室于 1988 年共同推出的入侵检测系统(IDS) 评测计划。经过对防火墙的测试, 测试结果表明本系统具有一定的拦截入侵攻击行为的功能, 即可以检测出流经防火墙的带有入侵行为的数据报文, 主动拦截了入侵攻击行为, 对流经防火墙的数据流的控制具有一定的主动性。

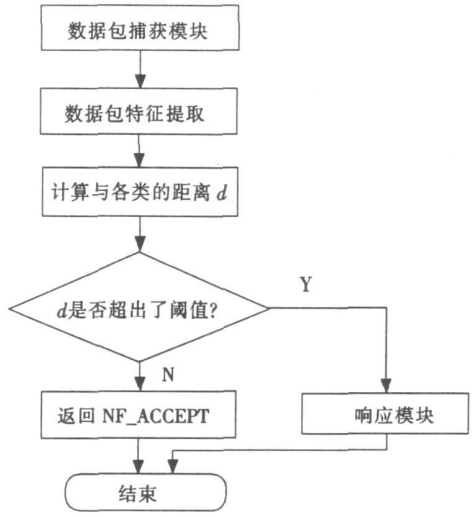

图 4 入侵检测工作流程图

Fig. 4 Workflow of intrusion detection

参考文献:

[1] 林江钦. 基于入侵检测的 Linux 综合型防火墙研究与实现[D]. 成都: 电子科技大学, 2005.

[2] 胡 东. 防火墙技术综述[J]. 山东气象, 2002, 22(1): 45-46.

[3] 杨明军, 王风芹. Linux 命令、编辑器与 Shell 编程[M]. 北京: 清华大学出版社, 2009.

[4] RICHARD S W, STEPHEN A R. UNIX 环境高级编程[M]. 尤晋元, 张亚英, 戚正伟译. 北京: 人民邮电出版社, 2006.

[5] 赵 洁, 丁香乾. 嵌入式 Linux 网络驱动程序的开发及实现原理[J]. 微计算机信息, 2008, 24(6-2): 64-66.

[6] 王亚林. 嵌入式 Linux 中断处理程序的设计与注册[J]. 电脑开发与应用, 2009, 22(1): 46-48.

[7] 周立功, 陈明计, 陈 渝. ARM 嵌入式 Linux 系统构建与驱动开发范例[M]. 北京: 北京航空航天大学出版社, 2006.

[8] STERGIOS S, APOSTOLOS M, GEORGE S. The internals of advanced interrupt handing techniques: Performance optimization of an embedded Linux network interface[J]. Computer Communications, 2008, 31: 3 460-3 468.