第36卷 第15期 计 算 机 工 程 2010年8月
Vol.36 No.15 Computer Engineering August 2010
·软件技术与数据库· 文章编号：1000—3428(2010)15—0074—03 文献标识码：A 中图分类号：TP311

安全Windows终端软件系统的研究与实现

李新明[1,2]，李 艺[2]，张功萱[1]，王平立[1]
(1. 南京理工大学计算机学院，南京 210094；2. 装备指挥技术学院重点实验室，北京 101416)

摘 要：针对Windows终端的安全问题，提出主/辅式双处理器、双操作系统的安全Windows终端解决方案。在阐述方案的总体架构和硬件平台的基础上，设计软件框架，分析设备管理、系统管理和安全控制等关键技术的设计与实现，包括主辅核设备的协同管理、多种内部通道的设计、网络数据包的流转等。

关键词：操作系统；网络安全；双处理器；驱动程序

Research and Implementation of Secure Windows Terminal Software System

LI Xin-ming[1,2], LI Yi[2], ZHANG Gong-xuan[1], WANG Ping-li[1]
(1. College of Computer, Nanjing University of Science & Technology, Nanjing 210094;
2. Key Laboratory, Institute of Command and Technology of Equipment, Beijing 101416)

【Abstract】Aiming at the security problems of Windows terminal, a schema of security Windows terminal which is called main and accessorial dual-processors and double operating systems is proposed. The overall construct and hardware architecture of the schema are described, software structure are designed. The design and implementation of key technologies such as device management, system administration and security control are analyzed. The key points include the main and accessorial kernel co-operating management of devices, the design of multi internal channel and translation of network data.

【Key words】operating system; network security; dual-processors; driver

1 概述

随着计算机技术的发展，终端与网络的安全显得尤为重要。目前我国的安全处理技术与产品大多基于国外的软硬件基础平台，给我国信息系统特别是民用关键业务和国防领域的信息化建设带来很大的安全隐患。我国信息终端仍然以Windows终端为主，而Windows一直是网络攻击的重点，由于Windows源代码和核心技术不公开，有关微软预留后门的问题已成为公开的秘密，Windows的安全问题不仅严重，而且存在不可知、不可控的特性，从而导致整个系统的不可信。为解决Windows终端的安全问题，本文提出主/辅式双处理器、双操作系统的安全Windows终端体系结构，对其中软件系统的设计与实现进行了分析和说明。

2 总体架构

主/辅式双处理器、双操作系统的Windows终端系统的设计思想是将Windows系统与外网物理上隔离，将安全处理与Windows系统相分离，通过一个独立运行的高安全等级的嵌入式操作系统来对所有进出Windows系统的网络数据进行全面的处理和控制，从而解决Windows系统的网络安全问题。终端系统采用双处理器结构，在保持主核Windows系统的软硬件结构不改变的基础上，增加辅核系统来进行Windows系统的网络安全处理。双处理器上分别运行不同的操作系统，主处理器运行Windows操作系统，承担终端计算、人机交互等原有功能，辅处理器运行高安全的嵌入式操作系统，承担网络环境下安全处理。这种结构在克服基于Windows自身进行网络安全防护的固有缺陷、主动防御、从结构上解决Windows系统的“黑箱”问题、隐藏目标系统、实施数据包加密等方面具有许多优点。

在本体系结构下，辅核是所有安全处理的平台，自身的安全性是整个系统安全性的基础。辅核最终将运行具有自主版权、国产、高安全的嵌入式操作系统。目前，在原型系统的设计与实现阶段，辅核采用嵌入式Linux操作系统。

基于双处理器双操作系统的安全Windows终端硬件结构如图1所示。

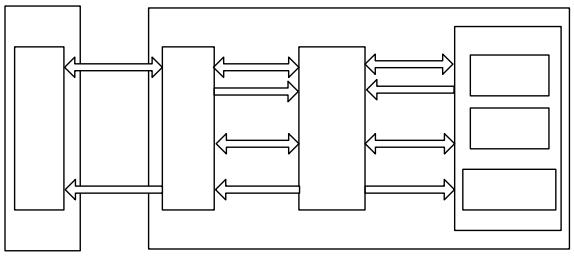


图1 基于双处理器双操作系统的安全Windows终端硬件结构

本终端系统采用Intel PC/ARM9双核硬件系统、Windows/Linux双操作系统的总体框架，辅核采用ARM9嵌入式系统，硬件架构可简单描述为“PC处理器+PCI控制系

基金项目：国家“863”计划基金资助项目(2006AA01Z447)
作者简介：李新明(1965－)，男，教授、博士生导师，主研方向：操作系统，网络安全；李 艺、张功萱，教授；王平立，副教授
收稿日期：2010-06-21 **E-mail：**liyi1221@263.net

统+双端口缓冲+ARM 处理器+网络接口”[1]。辅核系统以板卡形式插入主核系统 PCI 插槽中，通过各种处理，使得对 Windows 用户来说该卡就是一个普通的 I/O 接口卡。设置双端口缓冲存储器来保证双核系统正常高速通信。

3 软件框架

基于双处理器双操作系统的安全Windows终端的软件框架如图 2 所示。软件系统分别在 Windows 主核系统和安全辅核系统上设计并实现，包括辅核设备驱动程序模块[2]、双端口存储器驱动程序模块、网络控制器驱动程序模块、系统管理模块和安全控制模块[3]。

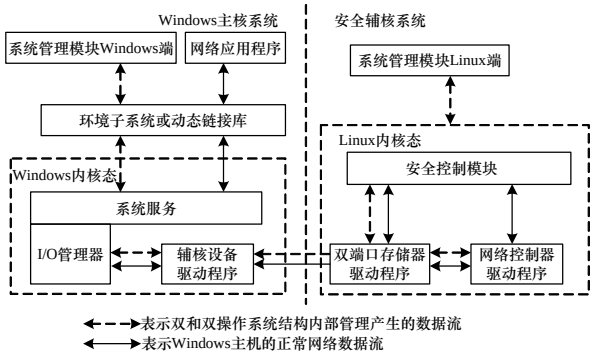


图 2 基于双处理器双操作系统的安全 Windows 终端的软件框架

4 关键技术的设计与实现

4.1 设备管理

由于体系结构的改变，必须解决主核和辅核设备协同管理，以及主核对辅核的透明管理等问题。本系统要管理的设备包括辅核系统、双端口存储器、网络控制器、串口和 USB 等。最主要的驱动程序[4-5]如下：

(1)辅核设备驱动程序。必须保证对 Windows 用户来说辅核就是一个普通的 I/O 接口卡，不会影响用户和网络程序的运行。在 Windows 系统中实现的辅核设备驱动程序除了驱动辅核板卡的正常运行外，一个主要功能是保证 Windows 主机访问网络的各种 I/O 数据流的正常传输，使得辅核系统对 Windows 主机用户和应用程序的透明。

(2)双端口存储器驱动程序。双端口缓冲存储器作为一个数据缓存，是保证双核系统正常高速通信的桥梁。采用 IDT 公司的 IDT70V05S。在辅核 Linux 内核中实现的双端口存储器驱动程序完成对双端口存储器数据的读/写等操作[6]。

(3)网络控制器驱动程序。目前网络控制器采用的是以太局域网控制器 CS8900A，包括片上 RAM、10Base-T 传输和接收滤波器，以及带 24 mA 驱动的直接 ISA-总线接口。在辅核 Linux 内核中实现的网络控制器驱动程序完成对网络控制器的驱动[6]。

4.2 系统管理

系统管理包括 2 部分：(1)用户交互管理，通过内部专用通道完成 Windows 系统与辅核的通信，包括正向的用户登录信息，以及反向的安全事件警告信息等；(2)安全配置管理，通过专用的安全管理通道，实现安全管理员对辅核系统中安全管理信息配置等管理，如安全规则、策略、用户密码和安全级等。

为了保证系统管理的安全性，辅核系统设计了 3 种通道：

(1)主通道：用于传输进出 Windows 系统的网络数据。

(2)内部专用通道：用于传输 Windows 主核和辅核系统间的交互信息，如主核向辅核传输的用户登录信息、辅核向主核发送的安全警告信息等。用户交互管理模块完成 Windows 系统与辅核系统的交互，通过 Windows 的图形界面，对辅核的各种参数进行配置，同时提供安全事件的告警等。

(3)安全管理通道：用于安全管理员对辅核系统进行安全配置。在辅核系统中，各种安全管理配置信息，如用户及权限、涉密关键字等，都只能通过本通道配置，彻底杜绝黑客通过 Windows 系统修改配置的可能。安全管理员账号与 Windows 账号无关，安全管理员可以通过另一台服务器，或者通过 PDA 等对 Windows 终端系统进行安全配置。日志记录数据也可以通过此通道，存放到后台的服务器上。

终端系统中 3 种通道、主要驱动程序及系统管理模块的关系如图 3 所示。系统中有 3 条主要的数据流：Windows 原有的网络数据流、用户交互管理数据流[2]和安全管理数据流。

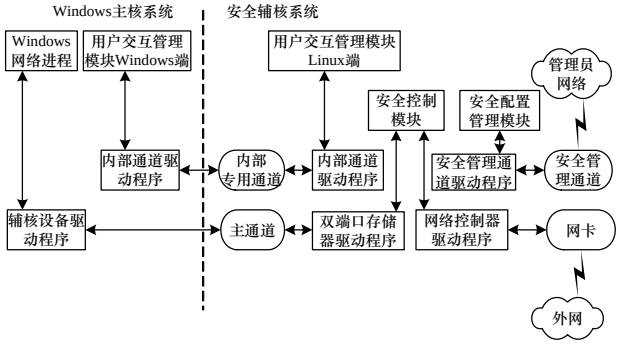


图 3 数据通道、驱动程序及系统管理模块关系

4.3 安全控制

安全控制模块完成在辅核系统中对流入和流出 Windows 系统数据的安全控制。通过对终端上网络进程的监控，并结合身份鉴别、协议认证、关键字匹配、访问控制等安全技术，在辅核系统上实现对通信数据包的分析和过滤，在 Windows 主机和外部网络之间构建一道“安全墙”，从而保证外部非法数据无法进入 Windows 主机，而内部的机密敏感数据不会外泄。

辅核系统要对所有流经的数据包，依据所制定的安全策略进行监控，提供的功能[3]包括：(1)对 Windows 终端计算机敏感信息资源提供明确的访问控制约束能力，防止终端用户无意泄密或者是有意越权泄密等行为，同时阻止外网未授权数据的入侵，并防范常见的基于协议漏洞的网络攻击。(2)对每个使用网络的用户进行身份鉴别和权限控制，在辅核系统设置不同安全等级的用户账号，将终端用户使用网络的权限按照安全属性分级，在某个安全级别内的用户只能向外网发送其权限范围内的信息，拒绝越权的网络访问操作。(3)依照协议认证策略、关键字策略、访问控制策略，对通过辅核的所有网络数据进行过滤和处理。(4)对辅核系统安全处理中的违规行为进行详细的日志记录，日志可记录在附加的 U 盘或者通过内部线路连接的后台服务器上。

安全控制模块的功能结构如图 4 所示。

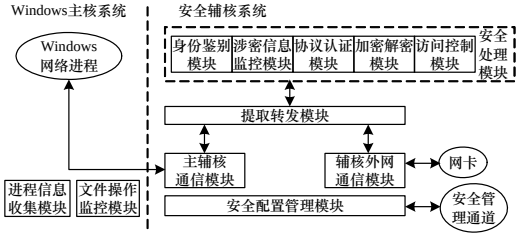


图 4 安全控制模块的功能结构

主核 Windows 系统和外网的任何数据的传输都必须通过辅核安全辅核系统的“中转”。辅核的“中转”主要是进行安全控制，当接收到来自 Windows 终端或者外网的报文时，辅核根据数据包的相关信息进行分析和判断，符合系统安全策略的数据包才允许通过，否则被丢弃。

Windows 网络进程的所有网络数据必须经过主辅核通信模块、提取转发模块、安全处理模块和辅核外网通信模块的处理后，才能通过网卡完成与外网的输入输出操作，其中，主辅核通信模块完成辅核 ARM 处理器和 Windows 主机的通信。辅核外网通信模块完成辅核和外部网络的通信。这 2 个通信模块都在 Linux 网络协议栈的链路层实现。辅核提取转发模块完成 2 个功能：(1)将主辅核通信模块以及辅核外网通信模块的数据包都提取到网络层，交给网络安全处理模块进行处理；(2)把经过安全处理后的数据包从正确的方向发送出去，从而保证整个辅核系统是 Windows 主机和外网通信的唯一桥梁。辅核提取转发模块实际上完成双端口存储器与网络控制器之间的网络数据包的提取与转发。

以 Windows 向外发送数据包为例(Windows 接收数据包的流程与此相反)，数据包经过了 3 个主要流转过程：

(1)数据包上提。将双端口存储器中的数据提取到 Linux 内核接收队列。当 Windows 主机要发送数据包时，双端口存储器产生中断，中断处理函数从硬件读取接收的数据包。如果是 IP 数据包，则将数据包上传到网络层的数据包接收队列中，并触发软中断，使得 Linux 内核接收数据包。否则，直接将网络数据包发送到外部网路。

(2)数据包钩取。将存放于数据接收队列中的数据包用 Netfilter 钩取，交由安全处理模块进行安全处理。Netfilter 是 Linux 内核中的一个功能模块，用于实现包过滤、NAT 和包处理等功能。利用 Netfilter 在 IP 层的 PREROUTING 钩子，注册钩子函数，将数据包钩取出来，交给安全处理模块。

(3)数据包转发。将安全处理完毕后的数据包交给辅核外网通信模块，发布到外部网络中。利用钩子回调函数来实现。处理后的数据包直接调用链路层接口函数发送到网络控制器中。

辅核能够对截获的网络数据包进行各种安全处理，是本系统最核心的功能。但目前的关键和重点并不是各种安全处理的具体细节，而是系统是否具备进行这些安全处理的技术途径。目前的安全处理包括身份鉴别、涉密信息监控、协议认证、访问控制、加密解密等[3]。

5 结束语

Windows 是全球最通用的操作系统，拥有众多的用户和许多成熟的应用程序，其安全问题不容忽视。不从根本上解决 Windows 的黑箱等安全问题，Windows 系统就无法应用到国防等关键领域。本文提出了主/辅式双处理器、双操作系统的 Windows 终端安全解决方案，在突破基于 Windows 实现 Windows 安全的现有模式、彻底防止 Window 预留后门等问题上进行了有益探索。下一步将完善系统，提高效率，为系统的产品化打下基础。

参考文献

[1] Zhang Gongxuan, Wang Ling, Song Bin. A Designing Method for High-rate Serial Communication[C]//Proc. of APPT’07. Guangzhou, China: [s. n.], 2007.

[2] 喻　刚. 基于双核的安全 Windows 终端 I/O 及系统管理技术研究与实现[D]. 北京: 装备指挥技术学院, 2008.

[3] 郭祥艳. 基于双核的安全 Windows 终端系统安全技术研究与实现[D]. 北京: 装备指挥技术学院, 2008.

[4] 陈　昨, 刘　航. 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.

[5] 武安河. Windows 2000/XP WDM 设备驱动程序开发[M]. 北京: 电子工业出版社, 2006.

[6] 孙纪坤. 嵌入式 Linux 系统开发技术详解——基于 ARM[M]. 北京: 人民邮电出版社, 2006.

编辑　顾姣健

（上接第 73 页）

```
    {case 0x8f:
      MsgHandler8f(msg.m_nParam, msg.m_sText);
      …    }
    m_queue.removeOneMessage();   } }
  public void run()
  { try { while(true) { MessageHandler();
                        Thread.sleep(0);   }
      …   }
    catch(Exception e)   { System.out.println("Error!");} }   }
```

其中，函数 MessageHandler()在线程函数 run()中被反复调用处理消息，调用函数 sleep(0)的目的是暂时释放 CPU 控制权，以便每个线程都有更均等的机会获得 CPU 控制权。注意，队列 m_queue 中的消息由进程消息处理函数负责插入，因篇幅限制，这里没有给出该部分代码，也没有考虑公共存储对象访问同步控制。

3 应用实例

本文提出的消息机制被用于一款基于 LEGO 机器人的协同式智能化多机器人系统中，其软件系统规模较大、功能很丰富；硬件系统由 4 个 LEGO 机器人和一个作为通信控制器的笔记本电脑组成，机器人及其与通信控制器间采用蓝牙通信，软件系统使用 Java 开发平台 Eclipse Platform version 3.4.0 及 LEGO 提供的 Java 工具包 leJOS[4] version 0.8，含有多种消息处理机制，既有单个机器人内部的消息处理机制，也包括采用面向对象技术封装后机器人之间的消息处理机制，各机器人之间可以通过软件封装的各种功能框架和用户提供的具体控制模块进行协同工作，共同完成某项任务。

4 结束语

本文提出一种采用 Java 语言标准语法实现的对象消息机制，能够以与 FMC 中 framework 的消息机制类似的方式应用于应用程序，从而给在嵌入式开发中使用 Java 实现面向对象模型带来便利。实践证明，本文的对象消息机制具有合理性、有效性，且易于实现。

参考文献

[1] Mitchell J D. 在 Java 中实现回调过程[Z]. [2009-04-22]. http://www.cn-teacher.com/fuwu/dn/bcjs/javajc/200704/191966.html.

[2] 羌翼亭, 陈昊鹏. 一种基于新型事件驱动机制的 Java 构件交互方法[J]. 计算机工程, 2007, 33(15): 103-105.

[3] 王　鹏. 零基础学 Java[M]. 北京: 机械工业出版社, 2008.

[4] leJOS——Java for LEGO Mindstorms[Z]. [2009-04-02]. http://leJOS.sourceforge.net/nxt/nxj/tutorial/index.htm.

编辑　张　帆