第 34 卷 第 1 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.1 Computer Engineering January 2008
·开发研究与设计技术· 文章编号：1000—3428(2008)01—0281—02 文献标识码：A 中图分类号：TP393.08

基于扩展 ROM 技术的网络安全隔离卡设计

李清宝，孟庆倩，曾光裕
(解放军信息工程大学信息工程学院，郑州 450002)

摘 要：漏洞扫描还不能完全将网络终端中存在的各种复杂攻击检出，许多传统安全技术时常失效，从信息安全技术层面上还不能有效解决现代网络中的安全问题。该文介绍了 PCI 扩展 ROM 规范、网络通信链路切换机制和机密信息存储原理，分析了主机和外部设备互连关系以及攻击特征，提出一种新的基于扩展 ROM 防止机密信息泄漏的安全网络终端结构，该结构支持网络终端内外网的物理隔离。
关键词：安全隔离卡；扩展 ROM；物理隔离

Design of Security Isolation Card Based on Extended ROM

LI Qing-bao, MENG Qing-qian, ZENG Guang-yu
(College of Information Engineering, PLA Information and Engineering University, Zhengzhou 450002)

【Abstract】Now, as vulnerability scanning can not fully check out complex attack existing in network, many of the traditional security technologies are no longer valid and failure to prevent effective solutions to modern network security problems from information technology, so many methods based on security model are presented. This paper analyzes the PCI extended ROM specification, the mechanism of network communications link switch, the principle of secret information storage, the connection relation of host computers and devices and the characteristic of attack, presents a novel security architecture of network terminal, which is based on extended ROM and PCI bus to carry out the physics gap of a network terminal between interior and exterior network. It discusses the principle and hardware design of the security isolation card based on PCI bus.
【Key words】security isolation card; extended ROM; physical isolation

计算机软硬件系统漏洞和后门的存在为网络黑客、木马和病毒程序的泛滥提供了物质基础，涉及机密信息上网的终端将面临信息泄漏的危险，信息安全问题已日益严峻[1-3]。目前流行的安全防护技术主要有两类：一类是从纯软件方面入手，采用诸如防火墙、入侵检测、身份认证、加密、防病毒等技术；另一类则是从硬件隔离入手，采取内外网隔离的研究思路，较典型的是采用物理隔离等技术。伴随着攻击工具与手段的复杂多样，软件策略已无法满足对安全高度敏感部门的需要。国家保密局也明文规定，凡涉及国家秘密的计算机终端不得直接或间接地与国际互联网或其他公共信息网连接，必须实行物理隔离。本文介绍了一种基于PCI扩展ROM控制实现的安全隔离技术，即采用内外网通信链路和存储通信链路彼此物理隔离，并将内外网通信链路切换时机选择在操作系统启动之前，使网络终端用户既能方便地享受互联网资源，又能保证终端的机密信息不被非法攻击和窃取。

1 PCI 扩展 ROM 技术

一台 PC 网络终端，在开机或重启后，首要的工作便是系统引导，即跳转到 BIOS 启动代码处执行 BIOS 代码。BIOS 取得网络终端的控制权后，关闭中断并开始检测各基本设备的运转状态，检测完成后，系统 BIOS 内部支持即插即用的代码(配置软件)开始检测和配置系统中安装的即插即用设备，即为已安装的 PCI 设备分配中断、DMA 通道、存储空间和 I/O 端口等资源。接着，配置软件会搜索扩展设备上是否存在 ROM，如果存在将执行 ROM 里的程序。最后，打开不可屏蔽中断，调用中断 INT19h 进行操作系统自举。

可见，要想让物理隔离控制程序在操作系统启动前获得计算机的控制权，完成网络状态的切换，就必须利用 BIOS 的上述特性，即将隔离控制程序存储在扩展板卡上的 ROM 芯片中，待网络终端开机或重启时，让 BIOS 将 ROM 中的控制程序加载到内存执行。

1.1 扩展 ROM 概述

嵌入在主板上的PCI器件或PCI扩展卡都是PCI设备。每个PCI设备都有一个配置空间，该空间一般位于PCI接口芯片内，它是PCI设备与BIOS之间的信息交换区。通过该信息交换区，PCI设备向BIOS反馈其状态和要求，同时BIOS对PCI设备进行辨识、配置和控制[1]。如果PCI设备具有扩展ROM，就要通过位于其配置空间偏移地址30H处的扩展ROM基址寄存器通知BIOS的自动配置软件。扩展ROM基址寄存器的格式如图 1 所示。其中，位 0 为 1 表明设备ROM地址译码器被使能。当配置空间偏移地址 02H处命令寄存器的存储器空间位也被置为 1 时，扩展ROM才会被访问；位[10…1]保留；位[31…11]用于指定ROM起始地址。

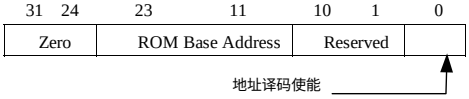


图 1 扩展 ROM 基址寄存器格式

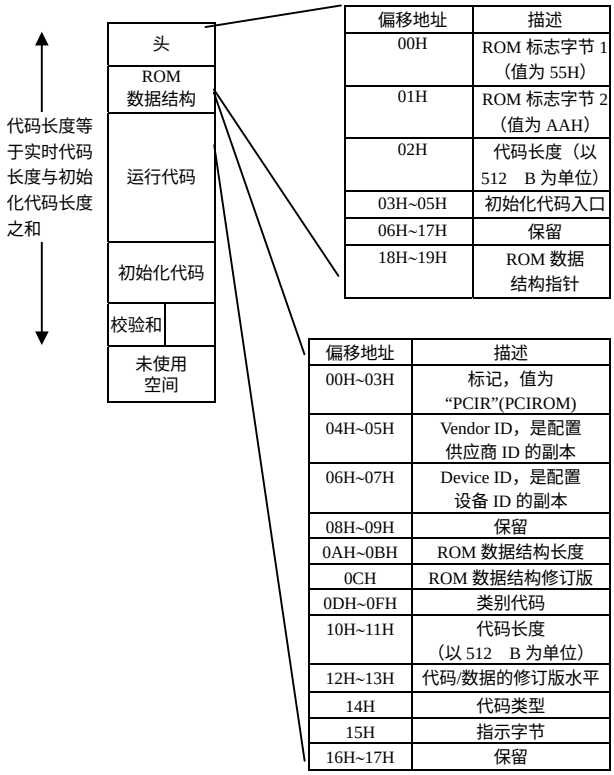
BIOS 中的配置软件向扩展 ROM 基址寄存器写 FFFFFFFEH(清除位 0，直到扩展 ROM 基址被分配后才使能 ROM 地址译码器)，然后读回其值，若读回的值里有 1，则表

作者简介：李清宝(1967－)，男，教授、博士，主研方向：信息安全；孟庆倩，硕士研究生；曾光裕，副教授
收稿日期：2007-01-08 **E-mail：**lqb215@vip.371.net

示设备里有扩展 ROM，且可知扩展 ROM 要求的空间大小，之后配置软件为其分配一块不冲突的存储器空间并将该空间的起始地址写回到扩展 ROM 基地址寄存器中，同时将位 0 置为 1 以使能设备 ROM 地址译码器。所有即插即用设备配置完后，BIOS 即检查 PCI 设备上是否有扩展 ROM，若有则还要检查 ROM 的前面两个单元是不是扩展 ROM 标志 AA55H，以确定 ROM 是否被安装，若安装，则 BIOS 将 ROM 中的代码拷贝到系统存储器中同时使 ROM 地址译码器无效。对于扩展 ROM，需将其映射到内存地址范围为 000C0000H~000DFFFFH 的区域中，才能与网络终端的标准 BIOS 兼容。

1.2 扩展 ROM 代码格式

PCI 规范允许一个扩展 ROM 包含多个代码段，这些代码段可能是供应商生产的各种类型设备的驱动程序，配置软件从中选择一个最适合处理器类别的代码段加载到系统存储器。每个 ROM 代码由 ROM 首部、ROM 数据结构、运行代码和初始化代码 4 部分组成，其格式如图 2 所示。



偏移地址	描述
00H	ROM 标志字节 1（值为 55H）
01H	ROM 标志字节 2（值为 AAH）
02H	代码长度（以 512 B 为单位）
03H~05H	初始化代码入口
06H~17H	保留
18H~19H	ROM 数据结构指针

偏移地址	描述
00H~03H	标记，值为“PCIR”(PCIROM)
04H~05H	Vendor ID，是配置供应商 ID 的副本
06H~07H	Device ID，是配置设备 ID 的副本
08H~09H	保留
0AH~0BH	ROM 数据结构长度
0CH	ROM 数据结构修订版
0DH~0FH	类别代码
10H~11H	代码长度（以 512 B 为单位）
12H~13H	代码/数据的修订版水平
14H	代码类型
15H	指示字节
16H~17H	保留

图 2 扩展 ROM 代码格式

ROM 首部包含了 ROM 数据结构的 16 位指针。ROM 数据结构部分给出了设备和代码的信息。运行代码在操作系统加载后保留在主存储器中并保持可运行状态。初始化代码用于设备的初始化，配置软件将 ROM 代码拷贝到主存储器后可立即调用初始化代码，一旦执行完即被清除。

(1)ROM 首部。ROM 首部中各字段如下：1)ROM 标志。2 B，内容为 AA55H，用于标识设备 ROM。2)代码长度。以 512 B 为单位的代码长度。3)初始化代码入口。指示初始化代码的入口地址。4)ROM 数据结构指针。是 ROM 数据结构相对于 ROM 代码起始位置的 16 位偏移量。

(2)ROM 数据结构。ROM 数据结构中的一些字段含义如下：1)供应商 ID 与设备 ID。由于 ROM 中可以有多个代码段，为保证加载正确的代码到主存，配置软件需比较该结构中的供应商 ID 与设备 ID 是否与配置空间中给出的一致。2)代码类型。指示代码的类型，值为 00H 时为 Intel86 可执行代码。3)指示字节。用于指示该代码是否是最后一个代码，位 7 为 1 指示最后代码。

1.3 扩展 ROM 初始化代码的执行

正确的代码拷贝到系统存储器后，配置软件将 ROM 地址译码使能位清零，并保持系统存储器驻留有 ROM 代码的区域可读、可写，之后执行以下步骤：(1)使用参数总线号、设备号以及功能号调用 ROM 中的初始化模块。(2)初始化代码用这些参数调用 BIOS，获取配置软件为其分配的系统资源，以初始化设备并为正常操作做准备。(3)如果运行模块中嵌入了中断服务程序，则读取设备配置空间中的中断线寄存器，以确定设备的中断请求被配置到系统中断控制器的那个输入引脚上，即获取中断号。当 CPU 响应中断时自动进入该中断服务程序。(4)初始化代码执行完毕，即将偏移地址 02H 处的代码长度单元的值减去初始化代码的长度，重新计算校验并置于运行代码的结尾。(5)返回到调用它的配置软件。

配置软件接着做如下处理：1)审查偏移地址 02H 处的代码长度，若被修改，则调整分配给 ROM 代码的存储空间。2)对驻留有 ROM 代码的主存区域进行写保护，防止操作系统取得控制权后改写该区域的内容。

2 安全隔离卡设计

要将外部的攻击彻底屏蔽于内网之外，在安全隔离卡的设计中主要采用了以下关键技术：(1)隔离卡控制程序存放于卡上的扩展 ROM 中，工作于扩展 BIOS 方式。(2)网络以及存储介质的链路切换由固件控制实现，隔离硬件不提供编程软接口，不受操作系统和应用软件控制，黑客无法从远程获得隔离硬件的控制权。(3)每次进行切换时自动清除内存区域并重启计算机，保证数据不经过内存被窃取。

安全切换工作示意图如图 3 所示，安全隔离卡通过切换网络通信链路和划分不同存储区域的方式将一台计算机虚拟为两台上网终端，实现终端的双重状态，即内网态和外网态，相应地将存储介质划分为安全区和公共区，两个数据区分别安装各自的操作系统，且终端用户将需要保护的重要数据存放于存储设备的安全区。当用户将网络终端设定在外网态时，用户只能访问信息公共区，不能访问机密信息区域，此时的计算机仅仅作为外部网络的一台终端来使用；当用户将网络终端设定在内网态时，用户可访问存储介质的安全区，且所有处于内网态的用户之间可共享信息资源、提高办公效率。

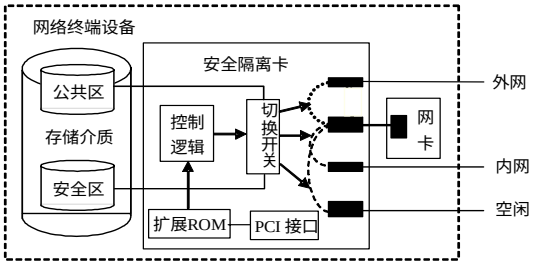


图 3 安全隔离卡工作示意图

基于扩展 ROM 技术的安全隔离卡由 PCI 总线接口模块、系统配置模块、扩展 ROM 模块、控制逻辑和切换接口模块构成，如图 3 所示。PCI 接口芯片作为 PCI 总线与本地总线之间的桥，连接 PCI 扩展卡的本地端逻辑到 PCI 总线上，并将 PCI 命令(例如读写某个寄存器、内存、I/O 端口)翻译到本地端；系统配置模块主要由一块串行 EEPROM 芯片构成，用

（下转封三）