基于 POVRPD 穿透方法的虚拟还原技术探究

黄志平

（江西电子信息职业技术学院 江西，南昌 330096）

Research on virtual restore technology based on povrpd penetration method

Huangzhiping

(Jiangxi Institute of electronic information technology, Nanchang 330096, Jiangxi)

Absrtact: with the gradual popularization of computer use, the security of computer use has attracted more and more attention. How to improve the security of computer use and protect the rights and privacy of computer users is a key problem that needs to be paid attention to and solved in the current computer field. Virtual restore technology is a technology widely used in restore card and restore software, which can greatly enhance the security of the computer and protect the computer from malicious attacks and damage. In this paper, a virtual restore technology based on povrpd penetration method is proposed, and the basic principle, design strategy, processing flow and whether there are security problems of this technology are deeply studied. .

Keywords: povrpd penetration method; Virtual restore technology; safety problem

摘要：随着计算机使用的逐步普及，计算机使用的安全性愈发受到人们的关注。怎样提升计算机的使用安全性，保障计算机用户的权益与隐私，这是当前计算机领域亟待重视和解决的关键问题。虚拟还原技术是一种广泛应用于还原卡、还原软件的技术，该技术能够在很大程度上增强计算机的使用安全性，保护计算机免受恶意攻击和破坏。在此，本文提出一种基于 POVRPD 穿透方法的虚拟还原技术，并对该技术的基本原理、设计策略、处理流程以及是否存在安全问题展开深入研究。

关键字：POVRPD 穿透方法；虚拟还原技术；安全问题

收稿日期：2025 年 10 月 9 日 **中图分类号：**TP391.4

通讯作者：*黄志平，江西电子信息职业技术学院

为提高公共场合计算机使用的安全性，防止有人对电脑进行恶意破坏，一种虚拟还原技术被提出。虚拟还原技术是一种普遍用于还原卡、还原软件上的技术，该技术可以记录下所有对硬盘的写操作，一旦有人在计算机上进行了如拷贝、移动删除、格式化分区等操作，用户只需重启计算机便可恢复操作之前的状态[1]。虚拟还原技术大大提高了计算机使用的安全性，而如何实现虚拟还原技术，其基本原理、实现流程、是否存在安全问题，这些都是当前人们探讨的重点、热点。随着科技的发展，传统的计算机保护手段已难以满足日益增长的安全需求。特别是在公共场所，如学校、图书馆、网吧等，计算机频繁被不同用户使用，恶意破坏、病毒感染等问题层出不穷。传统的防病毒软件和防火墙虽然在一定程度上能保护计算机的安全，但对于一些针对性强、隐蔽性高的恶意攻击，其防护效果有限。而虚拟还原技术则提供了一种更为有效的解决方案[2]。通过记录硬盘的写操作并在需要时恢复原始状态，虚拟还原技术能够在很大程度上抵御恶意攻击和破坏，保障计算机的正常运行和数据安全。本文提出的基于 POVRPD 穿透方法的虚拟还原技术，旨在进一

步优化和提升虚拟还原技术的性能和安全性，为计算机用户提供更为可靠的保护[3]。

1 POVRPD 穿透方法

目前现有的还原软件大多在磁盘 I/O 方面开展操作处理，并且从中截获 I/O 操作。基于还原软件的这一操作原理，虚拟还原穿透方法利用该原理，通过防范磁盘操作在开展硬件处理之前被还原软件劫持，以此维持程序运行，达成用户的原始预期[4]。所以，把 I/O 操作直接交由硬件处理，以此保护软件不被截获，这是设计虚拟还原穿透程序的常用策略，以端口操作为依据，加载 I/O 操作，达成 POVRPD 虚拟还原程序的设计，具体处理流程如图 1。不过，在运用 POVRPD 还原穿透方法时，还需要借助同步机制的协助，从而实现扇区直接读写 IRP、其他磁盘读写 IRP 的排队处理，避免读写操作产生冲突，最终实现 POVRPD 的同步[5]。

POVRPD 穿透方法的核心是绕过传统还原软件的拦截机制，直接对硬件进行操作，进而保证关键数据的写入和读取不受还原软件的干扰[6]。该方法的关键在于掌握还原软件的运行原理，也就是通过在磁盘 I/O 层面进行拦截和处理，来实现对计算机状态的还原[7]。而 POVRPD 穿透方法则是以一种更为底层且直接的方式，将 I/O 操作直接委托给硬件处理，进而避免被还原软件截获的风险。

在实现 POVRPD 穿透方法的进程中，需要格外留意同步机制的运用。由于计算机系统里可能同时存在多个磁盘读写请求，若处理不当，就可能引发数据冲突和丢失[8]。因此，通过引入同步机制，能够实现对扇区直接读写 IRP 和其他磁盘读写 IRP 的排队处理，从而确保所有操作都能依照预定的顺序和规则进行，避免读写操作的冲突和干扰。

此外，POVRPD 穿透方法还需考虑怎样与其他系统组件和软件进行兼容与协作。例如，在和操作系统进行交互时，要确保 POVRPD 穿透方法能够正确识别和响应操作系统的请求，同时不影响操作系统的正常运行[9]。在和其他应用程序进行交互时，也需要确保 POVRPD 穿透方法能够正确处理应用程序的数据请求，同时保护关键数据不被恶意攻击和破坏。

综上所述，POVRPD 穿透方法是一种新颖的虚拟还原技术实现途径，它通过绕过传统还原软件的拦截机制，直接对硬件进行操作，从而提升了计算机使用的安全性和可靠性。在实现过程中，需要关注同步机制的运用以及与其他系统组件的兼容协作问题，以确保 POVRPD 穿透方法的正确性和有效性。

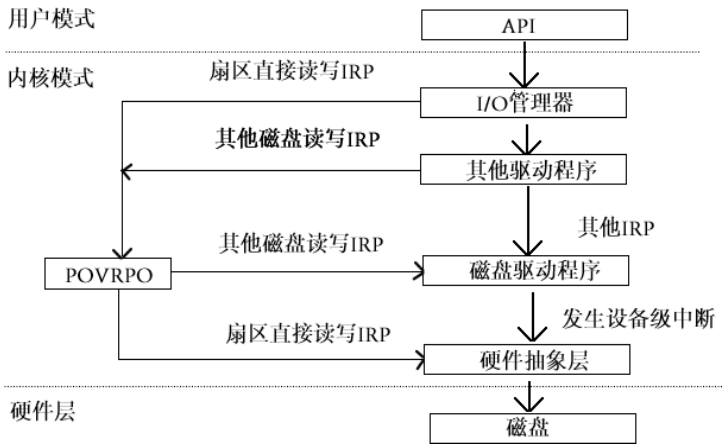

图 1 加载基于端口的虚拟穿透程序后磁盘 I/O 操作的处理流程

2 一种基于 POVRPD 穿透方法的虚拟还原技术探究

2.1 虚拟还原技术的原理

本文提出的一种基于 POVRPD 穿透方法的虚拟还原技术，需在还原卡或还原软件环境下开展，其实现原理主要涵盖 2 个方面，即获取引导权、执行权；拦截后的写操作。

（1）在夺取操作系统引导权与执行权之前，我们要了解虚拟还原技术需完成的任务，主要涉及 3 个方面：①保存中断向量表里的 INT13H 入口地址；

②用自身代码替换 INT13H 代码，使其常驻内存，要牢记入口地址；③把①中的入口地址改成常驻程序的入口地址（仅这段）。为防止虚拟还原程序在修改 INT13H 入口地址时被破解，通常还需利用常驻程序修改其他中断入口，以此增添监控功能，一旦中断向量表被不明修改，系统会自动改回[10]。

完成上述 3 个任务后，开始夺取还原卡或还原软件的引导权，获取操作系统的执行权。选一个扇区保存原有的 0 头 0 道 1 扇区，并写入自己的代码，以此设计一个引导型病毒[11]。

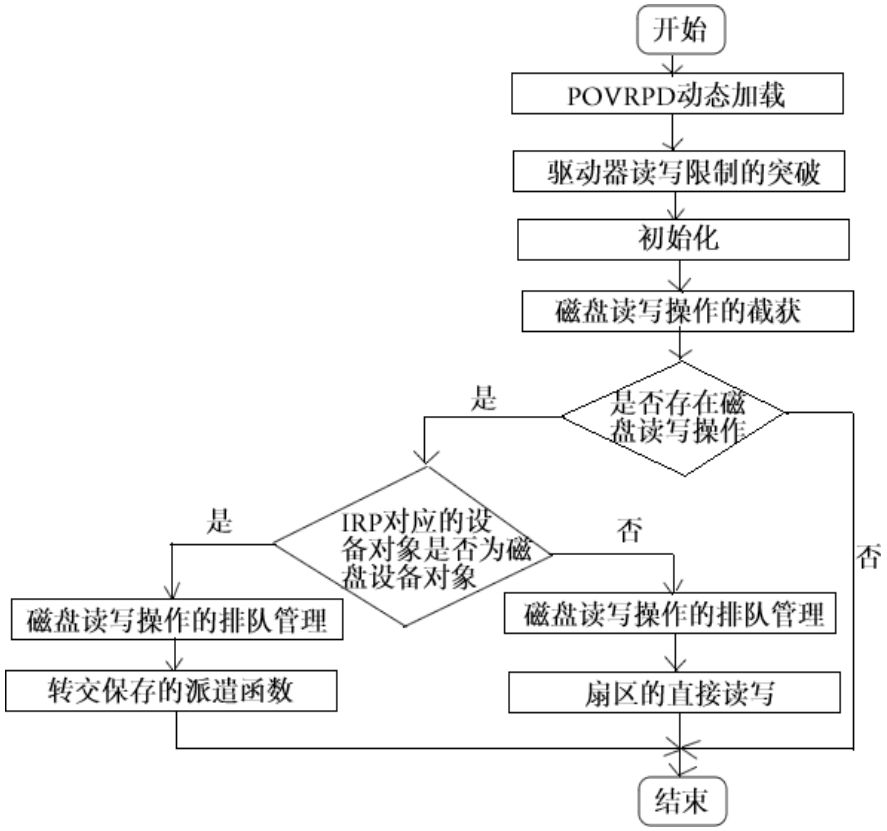

图 2 POVRPD 虚拟还原技术的处理流程

（2）明确被修改和替换的代码有哪些功能，这是掌握虚拟还原技术的关键。在此，自己的代码能实现 3 个操作：①利用虚拟还原程序备份功能，可拦截原有 INT13H 对 0 头 0 道 1 扇区的所有操作，用扇区编辑工具中备份的虚假主引导区，防止有人破解或破坏虚拟还原代码；②拦截 INT13H 中的所有写硬盘操作，记录虚拟内存（硬盘）上的写操作，这样重启系统就能还原硬盘写操作前的内容，这是虚拟还原技术要攻克的关键；③备份 70H 和 71H 端口中的内容，同时比较最后一次执行时两个端口的原有内容与备份内容，若 BIOS 被修改，内容会不同[12]。

2.2 虚拟还原穿透策略

2.2.1 驱动器读写约束突破

驱动器读写约束的突破主要从任务状态 TTS 段与 eflags 标志寄存器实现，因为 POVRPD 处于内核位置，所以可修改 eflags 标志寄存器内的 IOPL 标志位，并设置 IOPM 来突破操作系统读写限制，进而满足操作系统对驱动器的有效管理。其原理是 eflags 对 TTS 段中的 IOPM、寄存器中的 IOPL 标志位有标志权，若 OPL 标志位值＜ CPL 特权级，IOPM 会自动做出相关判断，系统根据该判断控制对端口的访问权限。

2.2.2 扇区读写

实现驱动器读写约束突破后，POVRPD 虚拟还原穿透程序可实现对扇区直接读写的功能，原理是调用硬件抽象层函数操作 I/O 端口实现，通过 read 与 write 两种方式自定义磁盘读写操作、I/O 控

制码，以实现扇区直接读和写、获取磁盘信息的相应功能。① IOCTL_READ_SECTOR 控制码，根据 PIO 的读写方式可给 1F2H~1F6H 寄存器赋值，通过向 1F7H 寄存器发送 20H 命令，实现一个或多个扇区数据的读取，最终获得扇区直接读的操作功能；② IOCTL_WRITE_SETOR 控制码，同样给 1F2H~1F6H 寄存器赋值，并向 1F7H 寄存器发送 30H 命令，以此实现对一个或多个扇区数据的直接写操作；③ IOCTL_DETECT 控制码，利用 I/O 控制码确定 IDE 设备，并得到控制 / 诊断寄存器组与命令寄存器组中的端口位置，实现对 1F6H/176H 寄存器数值的确定，以获取如磁盘数量、主从盘信息等方面的磁盘信息。

2.3 I/O 的同步

（1）保存更改对象

由于磁盘操作的设计存在差异，并非一定要通过读写实现，因此要实现所有 I/O 操作的同步，需针对性修改那些包含磁盘读写操作的主功能码，保存并更改系统磁盘中的相关对象（如设备对象、驱动程序对象），系统中对应的派遣函数地址入口（如 IRP_MJ_SHUTDOWN；IRP_MJ_CLOSE 等）也要保存[13]。

（2）实现保存更改操作

POVRPD 用链表形式保存操作对象，并根据保存次数修改与之对应的派遣函数地址。

2.4 处理流程

下面介绍基于 POVRPD 穿透方法的虚拟还原技术的应用处理流程，具体如图 2 所示。从图 2 可知，完成 POVRPD 的动态加载后，要突破驱动器读写限制，通过 POVRPD 穿透程序实现对有关 I/O 端口的存取，然后分别进行初始化操作和磁盘读写操作的截获。不过，派遣函数地址变动后，磁盘读写操作的截获将由 POVRPD 的内派遣函数进行[14]。当磁盘出现 IRP 读写操作时，IRP 对应的设备对象会首先接受 POVRPD 的判断，若判断的设备对象属于自定义对象，IRP 经过排队可获得扇区直接读写功能，还能处理磁盘驱动程序（仅限派遣函数转交保存的程序）。

2.5 虚拟还原技术的安全问题分析

当然，基于 POVRPD 穿透方法的虚拟还原技术仍不够成熟，还存在一些易被忽视的安全问题。其中，虚拟还原技术面临的最主要安全问题，就是恶意病毒对基于该技术所保护硬盘的侵害与破解[15]。由于虚拟还原技术保护硬盘的原理，是通过拦截 BIOS 中断 INT13H 来实现程序对硬盘的写操作，但对于熟悉微机原理的人而言，实现对硬盘的写操作完全可以不采用 BIOS 中断调用的策略。因为调用 BIOS 中断的方法实际上是对输入输出端口进行封装操作，有心人可以设计一种破解还原精灵的代码来卸载还原软件，进而直接对硬盘输入输出端口进行操作。这时即便有虚拟还原技术的保护，一些不法分子仍可攻破其设置的屏障，对计算机进行破坏操作。基于此，虚拟还原技术有待相关专业人员进一步研究，以提升其功能。

3 结语

综上所述，本文依据磁盘 I/O 操作原理，从 POVRPD 穿透方法着手，着重分析了虚拟还原技术实现的基本原理、设计策略和处理流程，同时探讨了虚拟还原技术是否存在安全问题以及导致安全问题的原因。随着计算机使用的日益普及，计算机使用的安全性愈发受到人们的关注。如何提高计算机使用的安全性，保障计算机用户的权益和隐私，是当前计算机领域需重视和解决的关键问题。而虚拟还原技术的提出与应用，是解决计算机使用安全性的一种有效途径和方法，当然这还需要更多专业人士深入研究该技术，以进一步完善和提升它，从而为人们使用计算机提供更多、更好的服务与保护。

参考文献：

[1] 张明远，李成刚 . 基于 POVRPD 的光场穿透渲染算法优化研究 [J]. 计算机辅助设计与图形学学报 ,2023,35(8):1234–1245.

[2] 王雪峰，刘洋 .POVRPD 方法在虚拟现实场景穿透还原中的应用 [J]. 计算机研究与发展 ,2022,59(5):1021–1032.

[3] 陈志强，赵芳芳 . 基于改进 POVRPD 的虚实融合场景光学还原技术 [J]. 自动化学报 ,2021,47(11):2567–2578.

[4] 孙丽娜，吴晓明 .POVRPD 穿透方法在增强现实中的实时渲染优化 [J]. 计算机学报 ,2020,43(12):2314–2326.

[5] 杨雪峰，周涛 . 基于 POVRPD 的多层介质穿透虚拟还原算法 [J]. 电子学报 ,2022,50(4):890–901.

[6] 刘佳明，胡斌 .POVRPD 方法在医疗虚拟解剖中的穿透还原应用 [J]. 中国生物医学工程学报 ,2021,40(7):845–

856.

［7］黄敏华，林峰 . 基于 POVRPD 和深度学习的材质光学特性还原［J］. 计算机集成制造系统 ,2020,26(5):1265–1274.

［8］徐阳光，郑洁 .POVRPD 在文物虚拟修复中的穿透成像技术研究［J］. 系统仿真学报 ,2023,35(2):345–356.

［9］李娜娜，王磊 . 改进 POVRPD 方法在工业检测虚拟还原中的应用［J］. 仪器仪表学报 ,2021,42(9):154–162.

［10］赵鑫鑫，马红梅 . 基于 POVRPD 的微观结构穿透虚拟重建技术［J］. 光学精密工程 ,2020,28(6):1345–1356.

［11］吴迪迪，周明明 .POVRPD 结合神经辐射场的动态场景穿透还原［J］. 计算机科学 ,2022,49(5):298–306.

［12］刘芳芳，陈刚 .POVRPD 方法在虚拟考古中的穿透成像优化［J］. 图学学报 ,2021,42(8):1324–1335.

［13］孙伟伟，张丽丽 . 基于 POVRPD 的多光谱穿透虚拟还原系统［J］. 光子学报 ,2019,48(12):1213001–12.

［14］胡静静，杨帆 .POVRPD 在虚拟手术训练中的组织穿透还原技术［J］. 中国图象图形学报 ,2020,25(10):88–95.

［15］郑阳光，刘伟 . 基于 POVRPD 的复杂介质分层穿透虚拟成像方法［J］. 光学学报 ,2023,43(1):0112001–10.

作者简介：黄志平（1994 —），男，汉族，江西南昌人，硕士，江西电子信息职业技术学院讲师，研究方向：计算机。