Linux 操作系统可视化中的“雷区”暨一个小地方的展示

齐划一

201605130105

研究过程

- 80386 芯片缺少 80387（FPU）时的表现。
- 编译不同版本的 Bochs，尝试关闭 FPU 指令。
- 寻找旧版 Bochs 附带的主板 BIOS 和显卡 BIOS。
- 退路：用 MMX 指令代替 FPU 指令。
- 从新版 Linux 编译 32 位的 ELF 可执行文件，调用 MMX 指令。
- 摆脱 Linux 0.11 不完善的权限机制带来的麻烦。
- Linux 0.11 不支持 ELF，只支持 a.out 格式的可执行文件。
- 退路：用不存在的指令代替 FPU 指令。

研究过程（续）

- 在 Linux 0.11 下编译程序，用 objdump 查看文件结构，用 0x90 替换部分语句。在 0x90 中插入不存在的指令。
- 尝试修改硬件中断程序 asm.s 和 traps.c，来忽略“指令不存在”
- 未果，用 0xCC 代替不存在的指令，修改中断，成功忽略
- 猜测是处理器遇到指令不存在时，不再给地址+1
- 尝试在中断处理时直接修改 EIP，未果

研究过程（续2）

- 放弃“协处理器”部分，转战块设备驱动程序
- 研究块设备驱动中的“电梯算法”
- 进行调试，断点，输出数据
- 硬盘速度太快，链表无法形成，一旦有新的请求会被立刻处理
- 使用“半假半真”的数据完成可视化，即：
  请求的内容是真的，但何时完成该请求由用户控制

体会

- 1. 要想完美模拟旧时的环境，非常困难，部分机制几乎无法复现
- 2. 察觉到问题时，应该根据进度和预测的难度考虑是否放弃

块设备驱动之电梯算法可视化