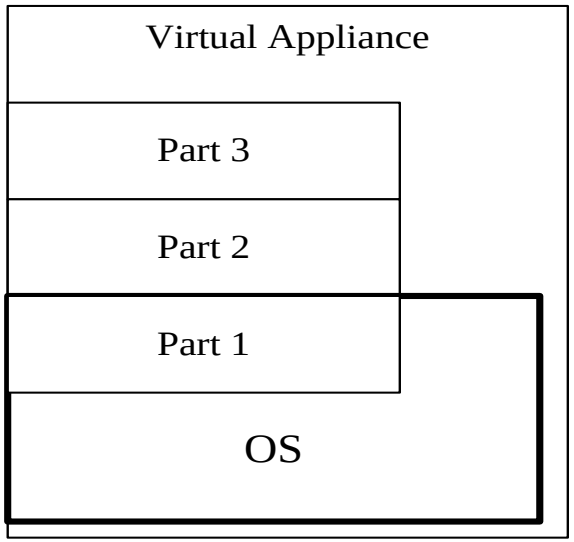
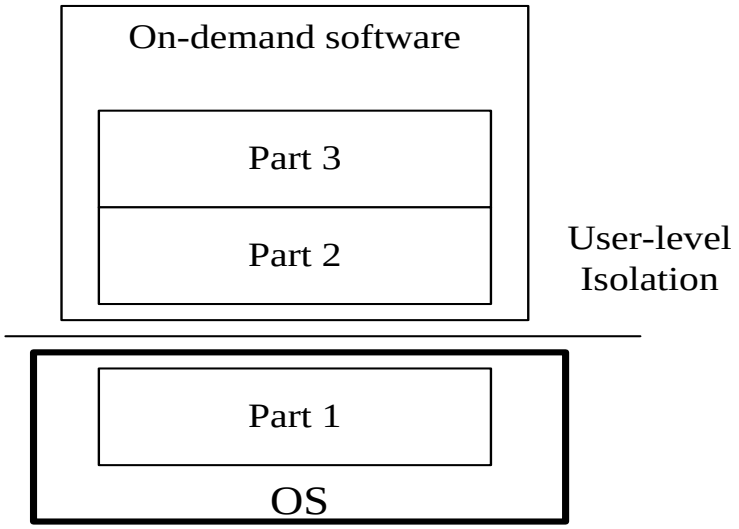
存储课实验说明

2014/3

- 应用层文件系统虚拟化
  - 应用层虚拟化的概念
  - 技术路线
  - 实验要求

- 概念
  - This mode has the virtualization layer positioned between the operating system and applications.
    - Every virtualization environment of an application shares the same execution environment as the host machine.
    - Application virtualization decouples software from OS.





– 特点

- Flexibility
- Storage efficiency

- Dependent on the host OS
- Difficulty to implement (?)

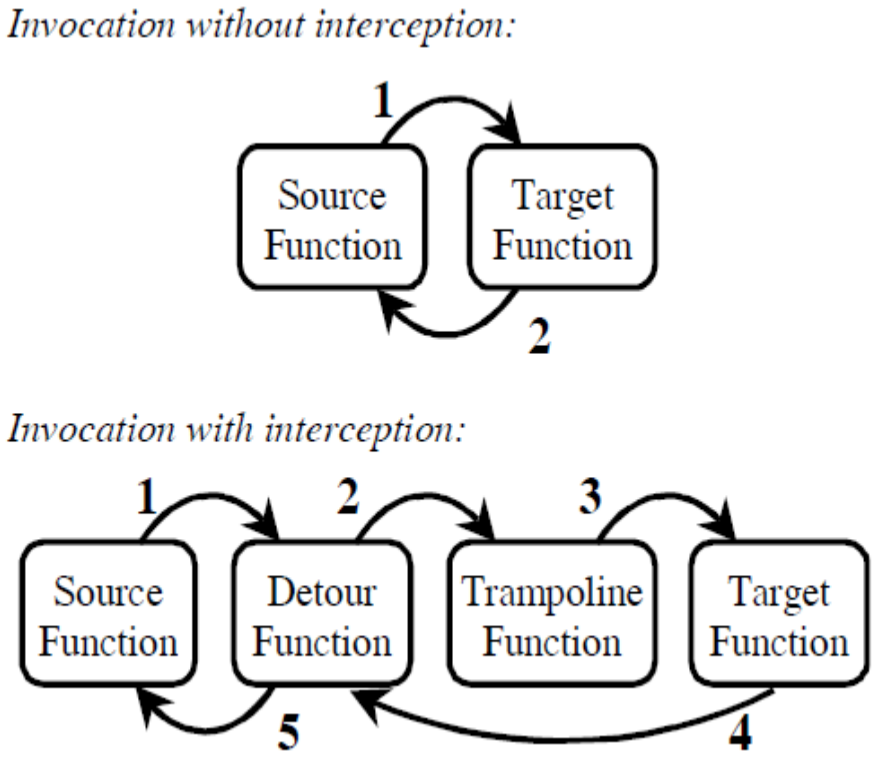
– 技术路线

- Hook！

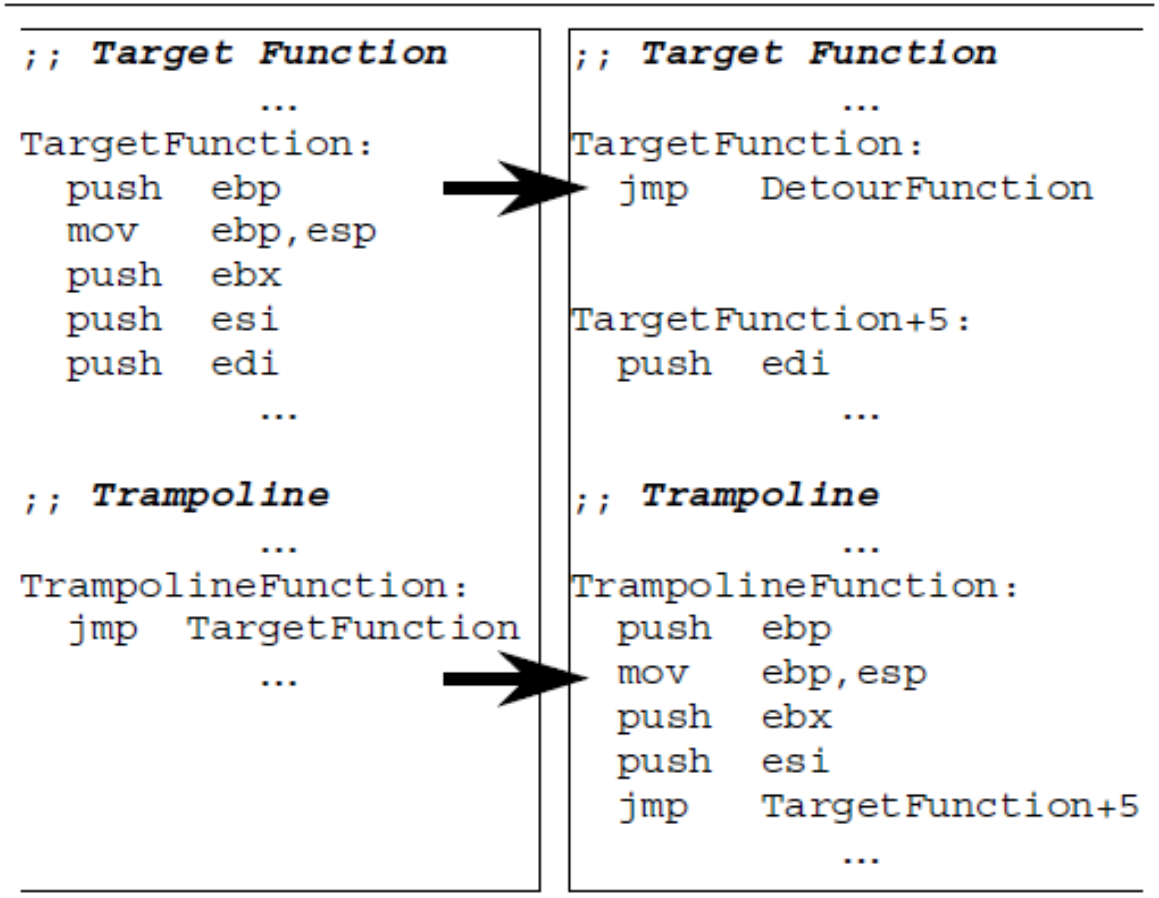
- The target software runs in a user-level virtualization environment layered on top of the local machine’s OS. This environment intercepts all related APIs, including those accessing the system registry and files/ directories, from the software.
  - Then, your code (inserted) can catch the function-call before and / or after invoking the original version and do everything you like.

- Detours Lib
  - By Microsoft
  - http://research.microsoft.com/en-us/projects/detours/

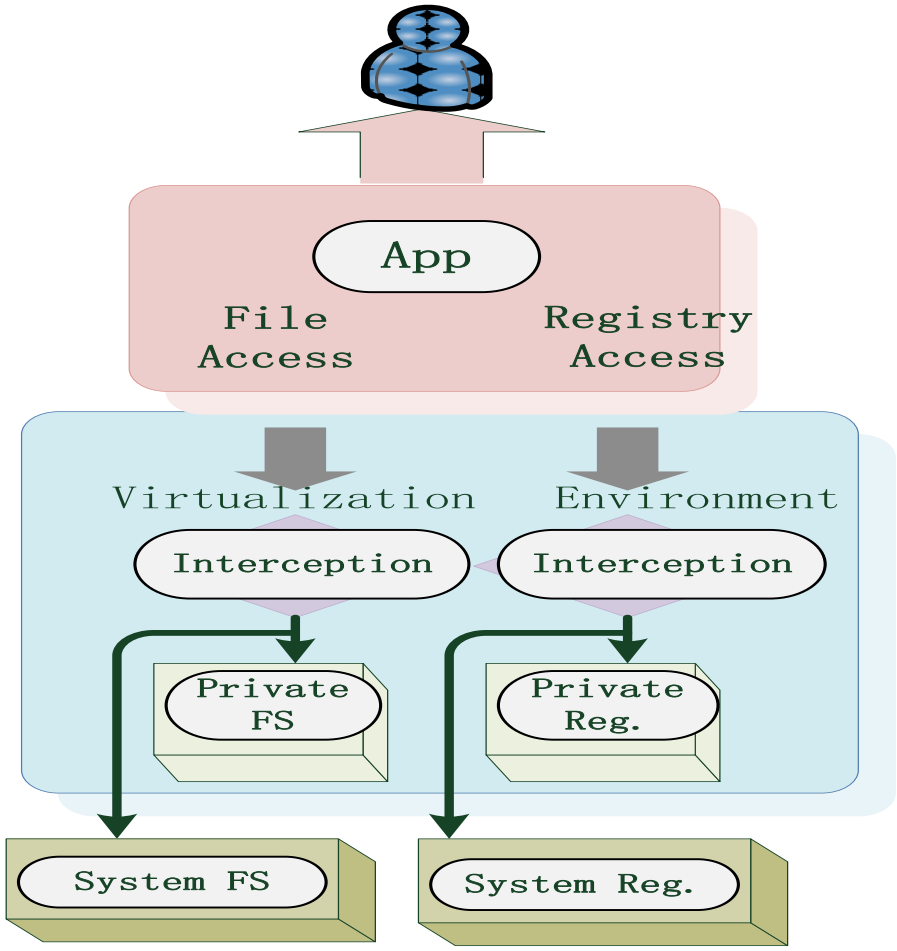
- A full-function HOOK lib with all source code and samples.



Invocation with and without interception


;; Target Function
...
TargetFunction:
push ebp
mov ebp,esp
push ebx
push esi
push edi
...
;; Trampoline
...
TrampolineFunction:
jmp TargetFunction
...
;; Target Function
...
TargetFunction:
jmp DetourFunction
TargetFunction+5:
push edi
...
;; Trampoline
...
TrampolineFunction:
push ebp
mov ebp,esp
push ebx
push esi
jmp TargetFunction+5
...

- 针对游戏应用的文件/注册表虚拟化
  - 特色技术——轻量级应用虚拟化技术
    - 分离传统桌面软件的运行环境与存储位置，从而能够实现服务端应用的用户个性化管理与迁移
      - 性能优于基于虚拟机的方案



– 实验要求

- 掌握文件系统调用相关的API的detours技术
- 利用这一技术，*detours* Video Game软件，使得目标软件对于其配置目录/文件的访问被透明的重定向到预置的其他目录/文件
- 建议自己做扩展设计！

- 注意
  - 文件API分为A/W版本
  - Detours开源的为32位版本
  - 其他操作系统如Linux的支持更多

- 实验报告要求
  - 实验目标
    - 简要设计、达到什么效果、detours的目标软件
  - 实验实现
    - 具体detours的API、软件流程
  - 测试
    - 功能
    - 性能（与非detours 的相比）