DLL 注 入

七日成蝶—Windows 高级编程

七日做茧，一朝成蝶！

主讲：袁春旭

从需求开始

从需求开始

想要所有的图形界面程序运行时都执行我的程序进行屏幕录制

想要目标应用程序一旦运行就给我发邮件通知我

想要了解目标进程都调用了哪些模块哪些库，从而了解原理

想要了解用户在记事本中都敲击了哪些按键

希望……

任何不谈需求的技术都是耍流氓

需求的总结

需求的总结

为已有产品扩展功能

监视目标进程的行为或进程调试

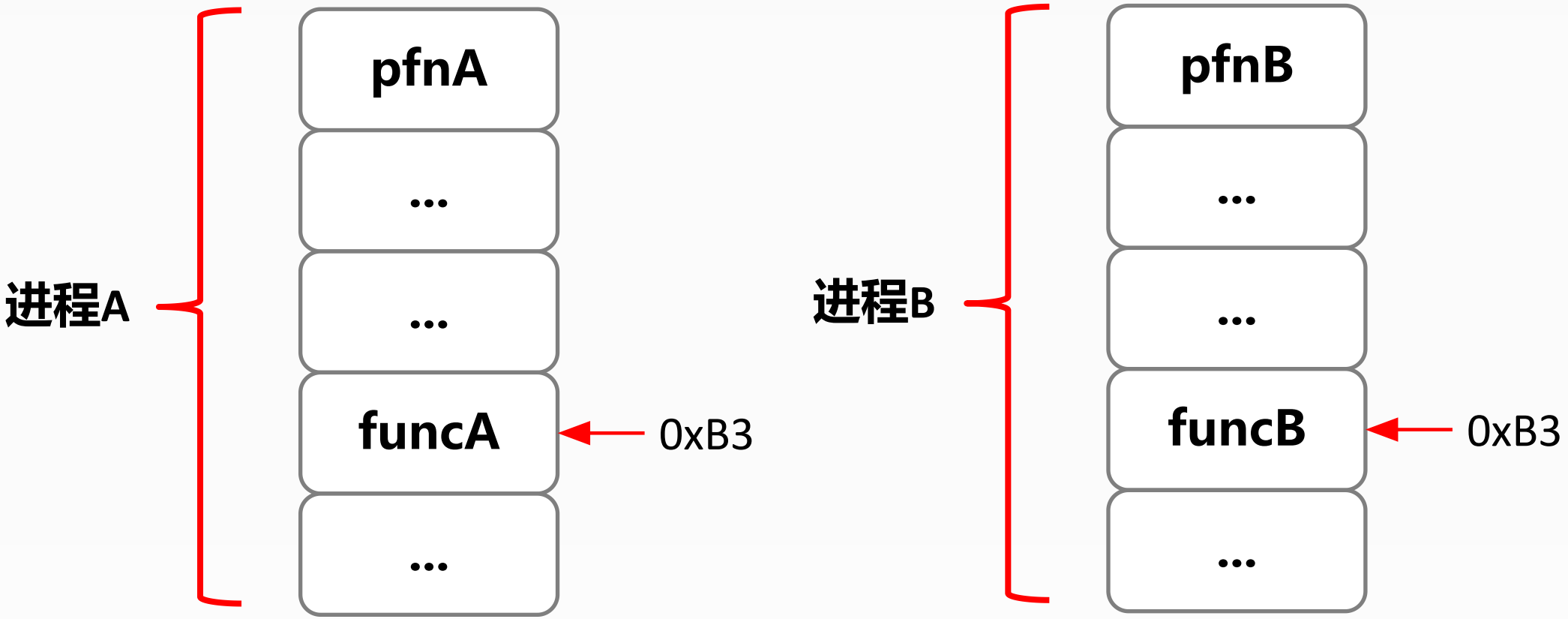
为所有进程添加统一处理模式

软件逆向工程

进程地址空间

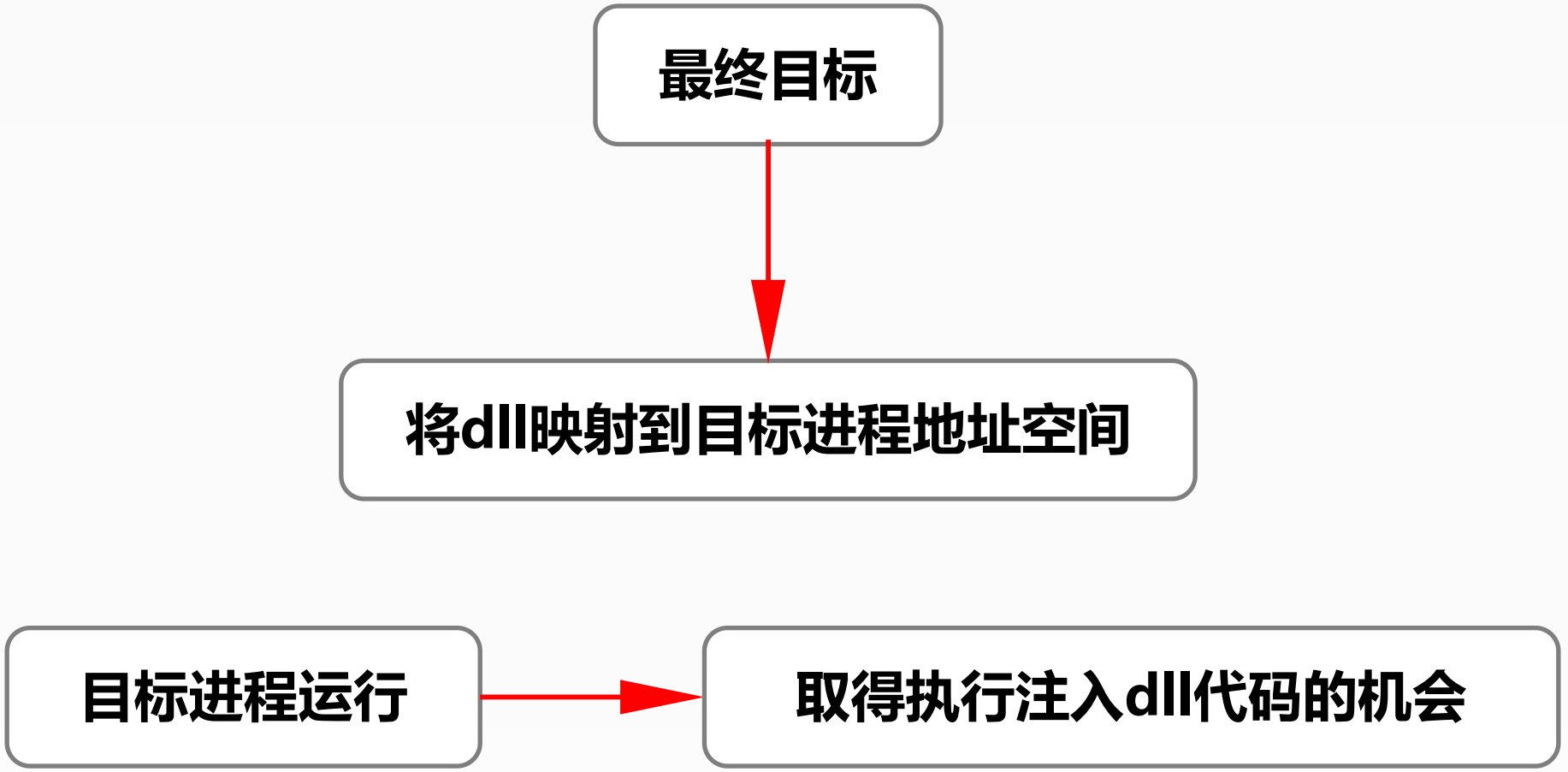
进程地址空间

进程间的内存地址空间是相互独立的



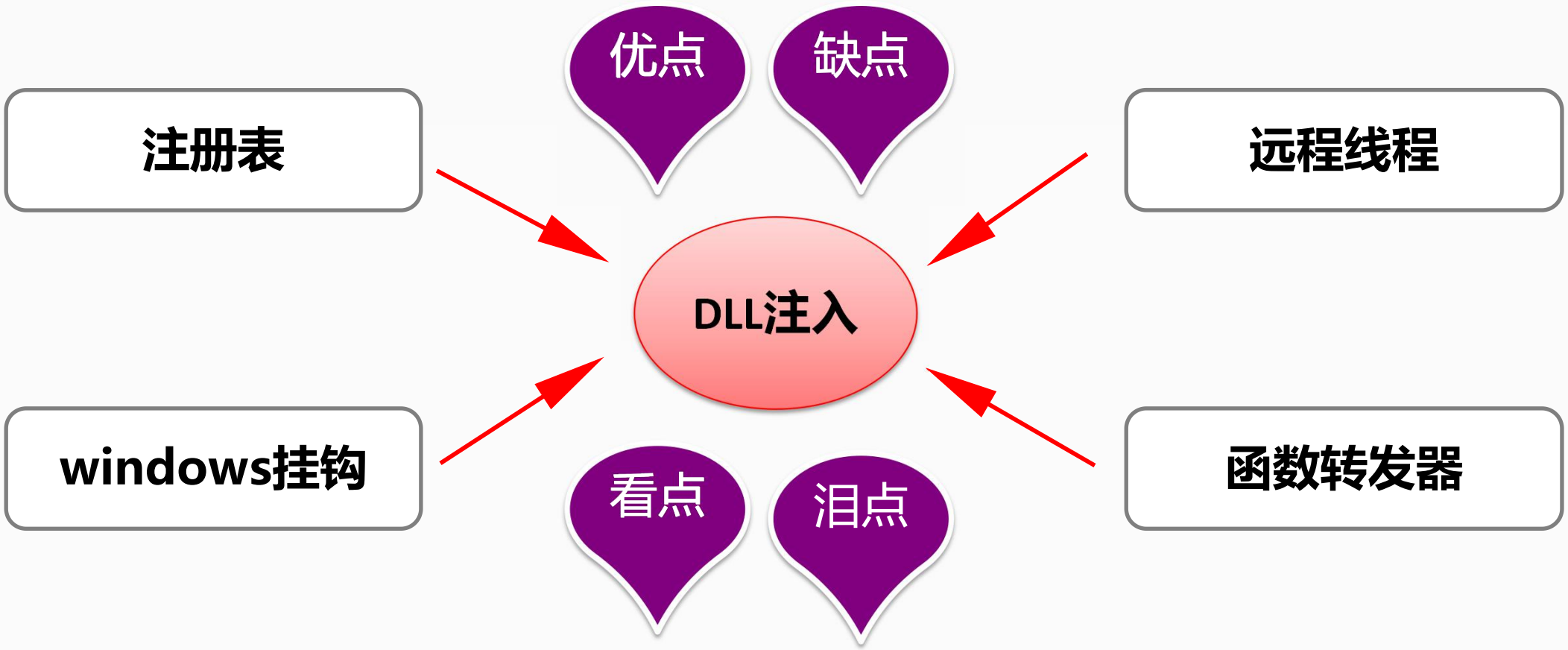
DLL注入

DLL注入



DLL注入的方式

DLL注入方式



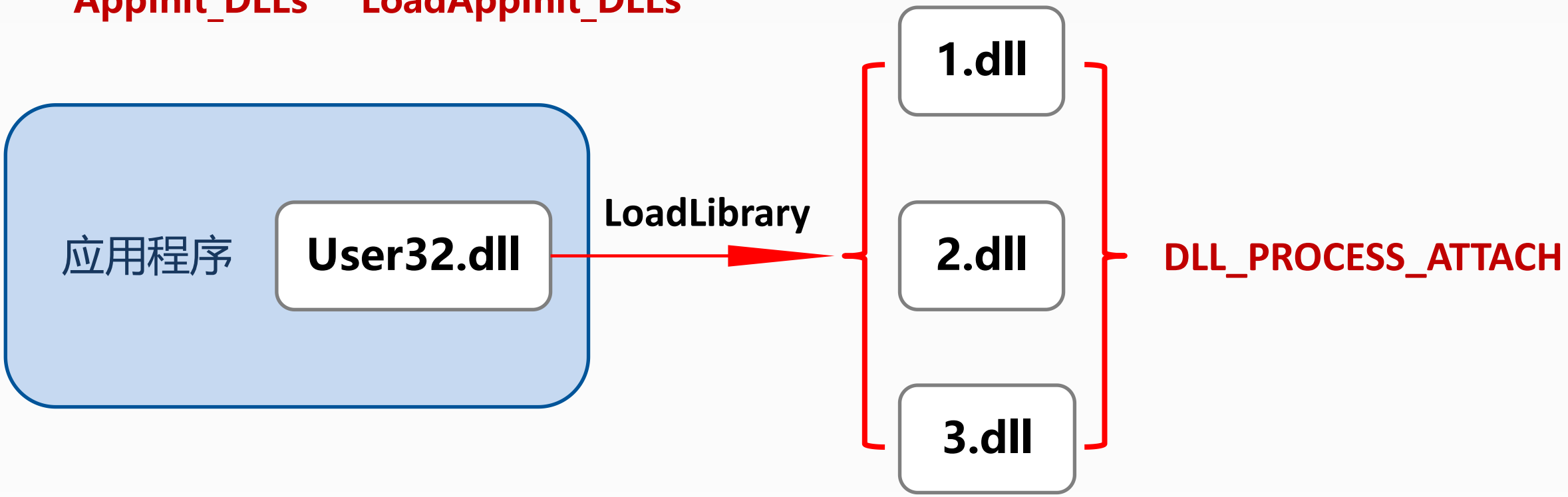
DLL注入的常用方式

注册表注入DLL

注册表注入DLL

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\

AppInit_DLLs　LoadAppInit_DLLs



优点：简单　看点：全局注入　缺点：死板　泪点：不实用，不主动，不稳定

注册表注入DLL

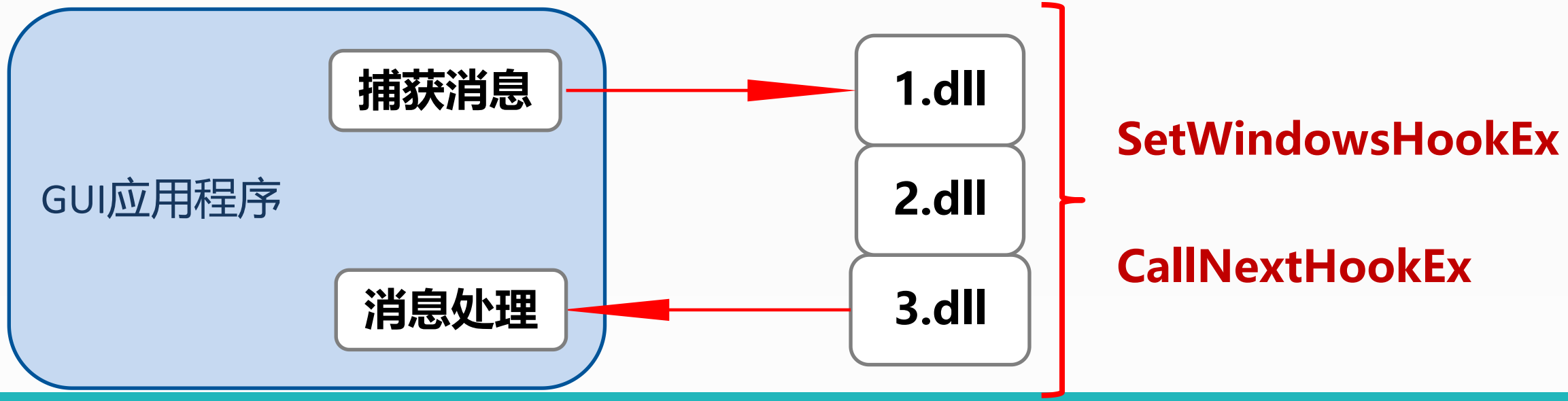
注册表API	说明
RegOpenKeyEx	打开注册表键值
RegQueryValueEx	查询键值
RegSetValueEx	设置键值
RegCloseKey	关闭键值

Windows挂钩注入DLL

挂钩注入DLL

SetWindowsHookEx(int idHook, HOOKPROC lpfn, HINSTANCE hMod, DWORD dwThreadId)
UnhookWindowsHookEx(HHOOK hhk)
LRESULT WINAPI CallNextHookEx(HHOOK hhk, int nCode, WPARAM wParam, LPARAM lParam)

优点：灵活主动
看点：线程、全局
缺点：只能消息处理
泪点：前面的粗心，后面的伤心



远程线程注入DLL

远程线程注入DLL

OpenProcess
CreateRemoteThread
LoadLibraryA LoadLibraryW
VirtualAllocEx
VirtualFreeEx
ReadProcessMemory
WriteProcessMemory

优点：线程独立
看点：针对进程
缺点：复杂
泪点：没有权限，一切白干

函数转发器注入DLL

函数转发器注入DLL

偷梁换柱，瞒天过海

优点：用户无感
看点：防不胜防
缺点：误入歧途
泪点：签名不过，就是假货

注入DLL查看工具ProcessExplorer

查看工具ProcessExplorer

百度搜索：七日成蝶 ProcessExplorer

所用功能：查看进程中被注入的DLL文件

编码实战