API hooking using the detours library

Intercepting API function calls

What is API hooking?

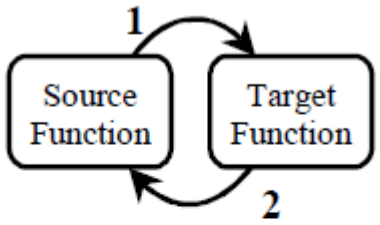
- To add functionality into a program where the source code is not available
- Make modifications at runtime without modifying the binary
- In game cheats, api hooking can intercept function which checks for player health and return 100% health
- Debuggers also use API hooking when you set breakpoints

What is Detours?

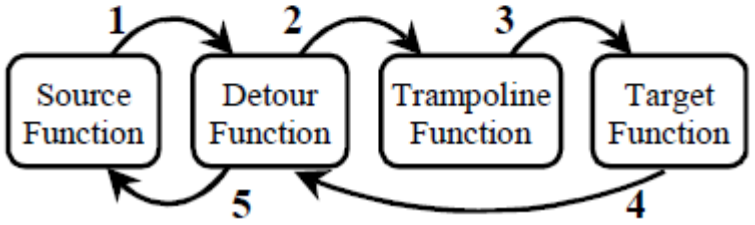
- A library for extending Win32 functions
- Intercepts Win32 functions by re-writing target function images
- Includes utilities to attach arbitrary DLLs and payloads to any Win32 binary

Calling function with and without interception

Invocation without interception:



Invocation with interception:



Source: Detours: Binary Interception of Win32 Functions, Galen Hunt and Doug Brubacher

Target and Trampoline Functions, before and after hooking

Before hooking

```
;; Target Function
            ...
TargetFunction:
  push   ebp
  mov    ebp,esp
  push   ebx
  push   esi
  push   edi
            ...

;; Trampoline
            ...
TrampolineFunction:
  jmp   TargetFunction
            ...
```

After hooking

```
;; Target Function
            ...
TargetFunction:
  jmp    DetourFunction


TargetFunction+5:
  push   edi
            ...

;; Trampoline
            ...
TrampolineFunction:
  push   ebp
  mov    ebp,esp
  push   ebx
  push   esi
  jmp    TargetFunction+5
            ...
```

Thank you