Industrial Strength Software Hacking

Simon McPartlin

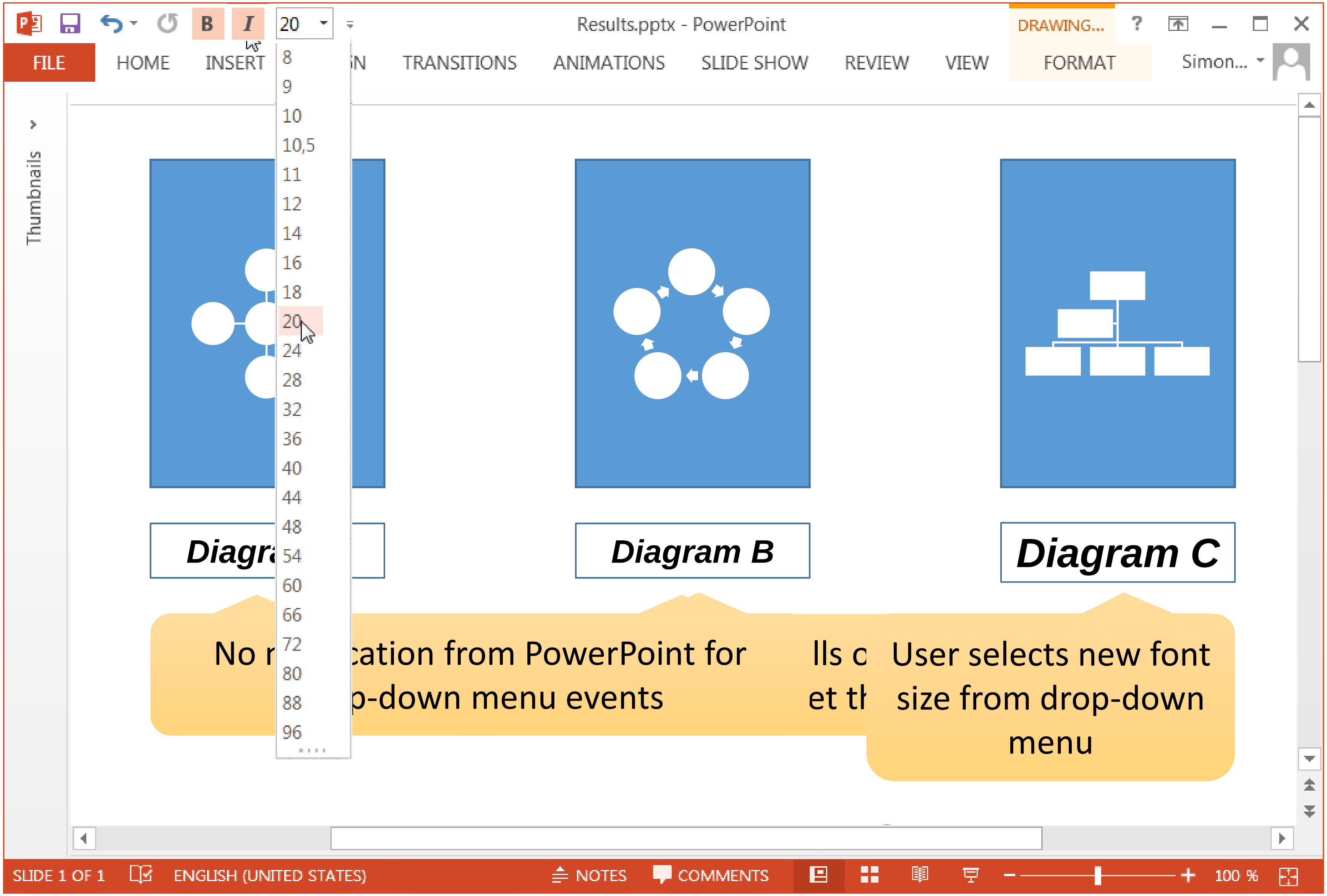
Berlin, December 3rd, 2015

Workshop Outline

- **Case study: Interacting with PowerPoint**
- Function Detouring
- Detouring exercises

Case study: Interacting with PowerPoint

- XML to customize the user interface
- APIs to access the PowerPoint object model
- Event notification mechanism

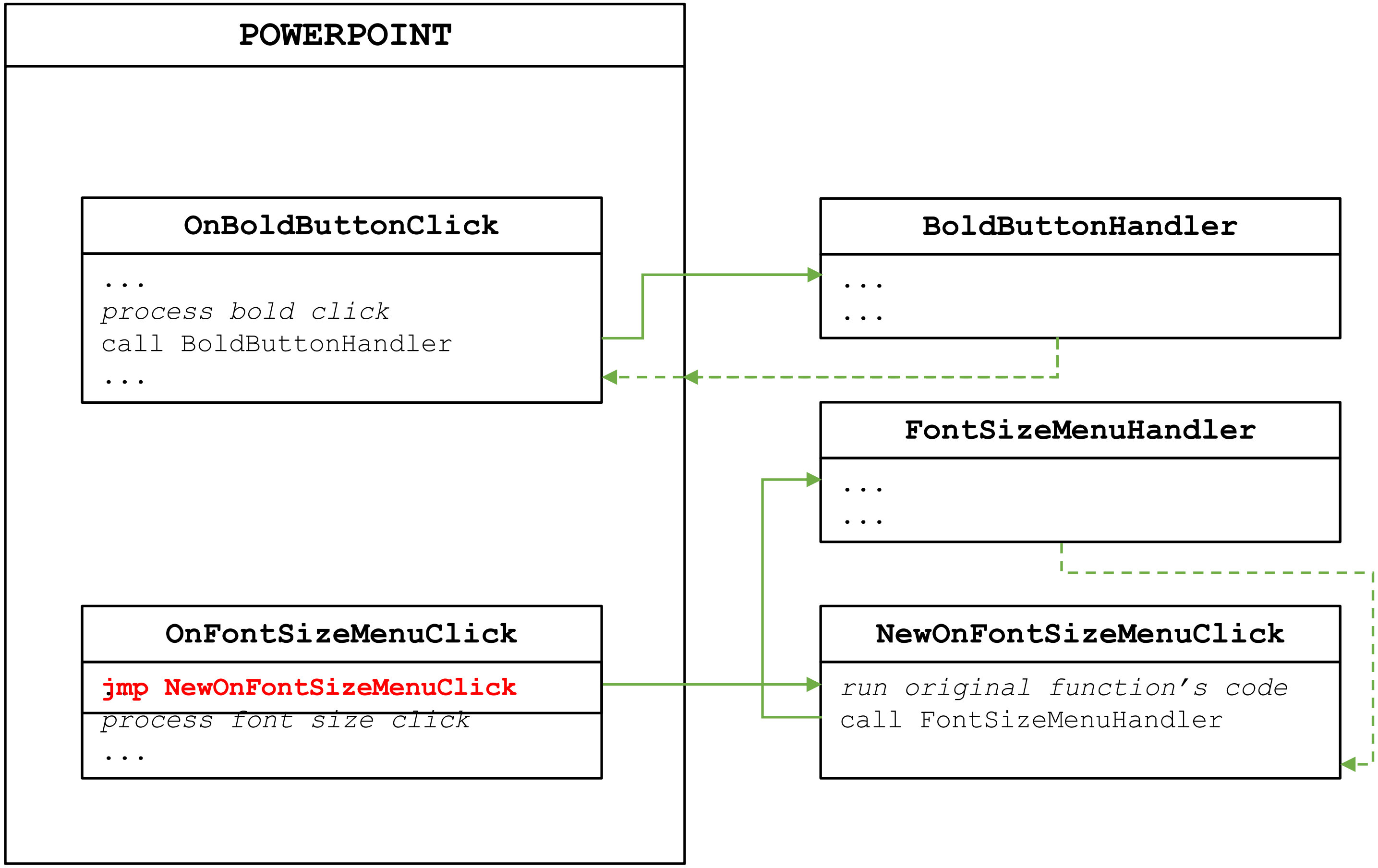


No r cation from PowerPoint for p-down menu events

lls c et th

User selects new font size from drop-down menu

Case study: Interacting with PowerPoint



Workshop Outline

- Case study: Interacting with PowerPoint
- **Function Detouring**
  - **Frequently asked questions**
  - Finding the target function
  - Function detouring framework
- Detouring exercises

Frequently asked questions

- Is function detouring legal?
  - Digital Millennium Copyright Act
  - Electronic Frontier Foundation (www.eff.org)
- Does it really work?
- It’s just really for cracking, isn’t it?
  - Function monitoring
  - Bug fixing
  - Undocumented APIs

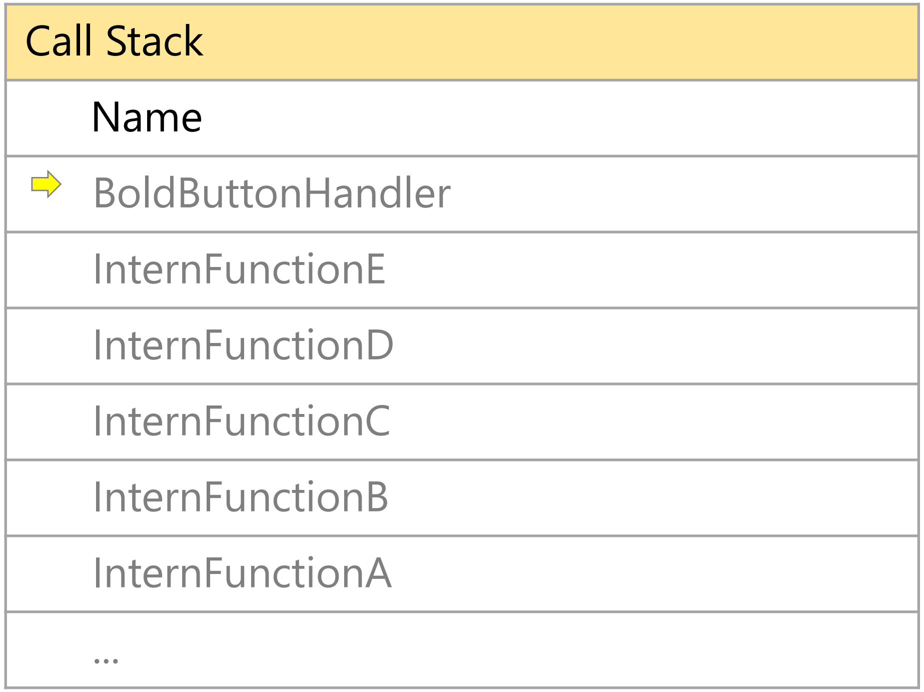
Workshop Outline

- Case study: Interacting with PowerPoint
- **Function Detouring**
  - Frequently asked questions
  - **Finding the target function**
  - Function detouring framework
- Detouring exercises

Finding the target function

- Public API function
- Search for candidate function(s)
  - Disassemblers and debuggers
  - Function entry/exit tracing
  - Window sub-classing

Finding the target function



Call Stack

	Name
⇨	BoldButtonHandler
	InternFunctionE
	InternFunctionD
	InternFunctionC
	InternFunctionB
	InternFunctionA
	…

Finding the target function

- Exported function
    - OS call, e.g. GetProcAddress
- Internal function
    - Store target function address
        - Only valid for particular build
    - Search for the target function

Finding the target function

- Search for binary code

```
   push   ebp
   mov    ebp,esp
   push   esi
   mov    esi,ecx
   cmp    dword ptr [esi],0
   jz     done
   push   1Bh
   call   sub_445DD3BB
   push   65345609
   mov    ecx,esi
   call   sub_451286E4
done:
   pop    esi
   retn
```

```
55
8B EC
56
8B F1
83 3E 00
74 13
6A 1B
E8 09 10 00 00
68 09 56 34 65
8B CE
E8 26 C3 B4 00

5E
C3
```

Finding the target function

- Reduce size of binary code to match

```
   push   ebp
   mov    ebp,esp
   push   esi
   mov    esi,ecx
   cmp    dword ptr [esi],0
   jz     done
   push   1Bh
   call   sub_445DD3BB
   push   65345609
   mov    ecx,esi
   call   sub_451286E4
done:
   pop    esi
   retn
```

```
55
8B EC
56
8B F1
83 3E 00
74 13
6A 1B
E8 09 10 00 00
68 09 56 34 65
8B CE
E8 26 C3 B4 00

5E
C3
```

Finding the target function

- Partially defined instructions

```
    push    ebp                             55
    mov     ebp,esp                         8B EC
    push    esi                             56
    mov     esi,ecx                         8B F1
    cmp     dword ptr [esi],0               83 3E 00
    jz      done                            74 13
    push    1Bh                             6A 1B
    call    sub_445DD3BB                    E8 09 10 00 00
    push    65345609                        68 09 56 34 65
    mov     ecx,esi                         8B CE
    call    sub_451286E4                    E8 26 C3 B4 00
done:
    pop     esi                             5E
    retn                                    C3
```

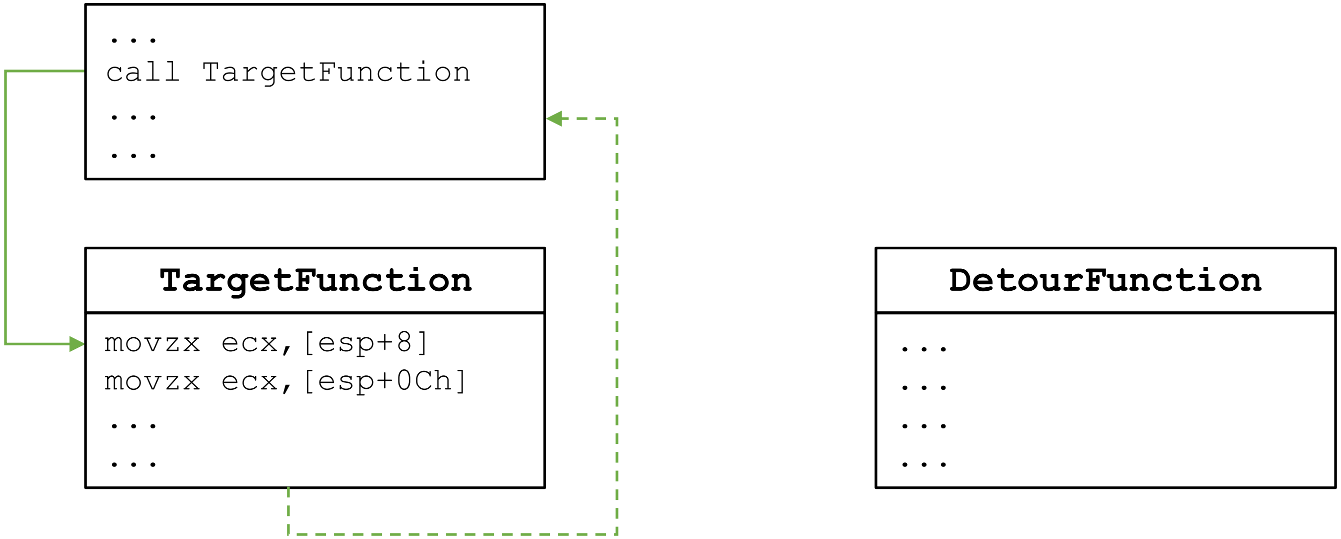
Workshop Outline

- Case study: Interacting with PowerPoint
- **Function Detouring**
  - Frequently asked questions
  - Finding the target function
  - **Function detouring framework**
- Detouring exercises

Function detouring framework

- Patch the target function start
- Make the original target function code available
- As robust as possible

Function detouring framework



```
...
call TargetFunction
...
...
```

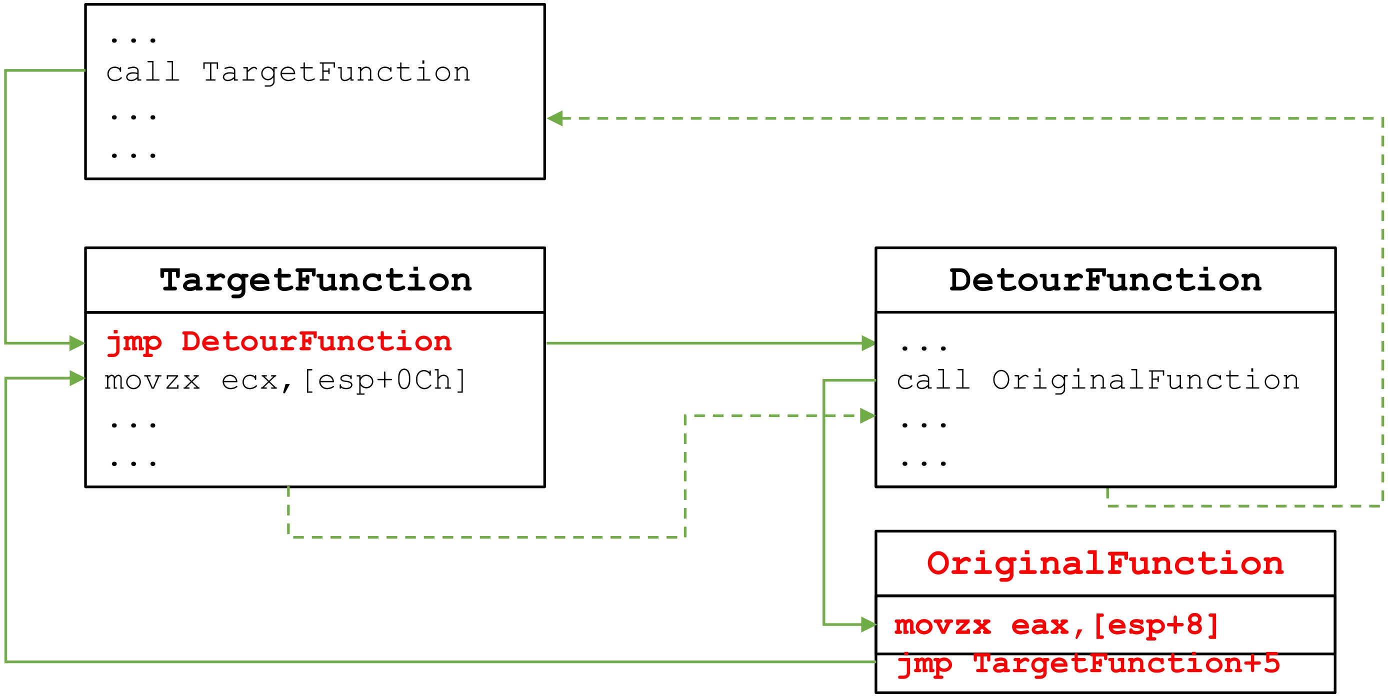
TargetFunction

```
movzx ecx,[esp+8]
movzx ecx,[esp+0Ch]
...
...
```

DetourFunction

```
...
...
...
...
```

Function detouring framework



```
...
call TargetFunction
...
...
```

TargetFunction

```
jmp DetourFunction
movzx ecx,[esp+0Ch]
...
...
```

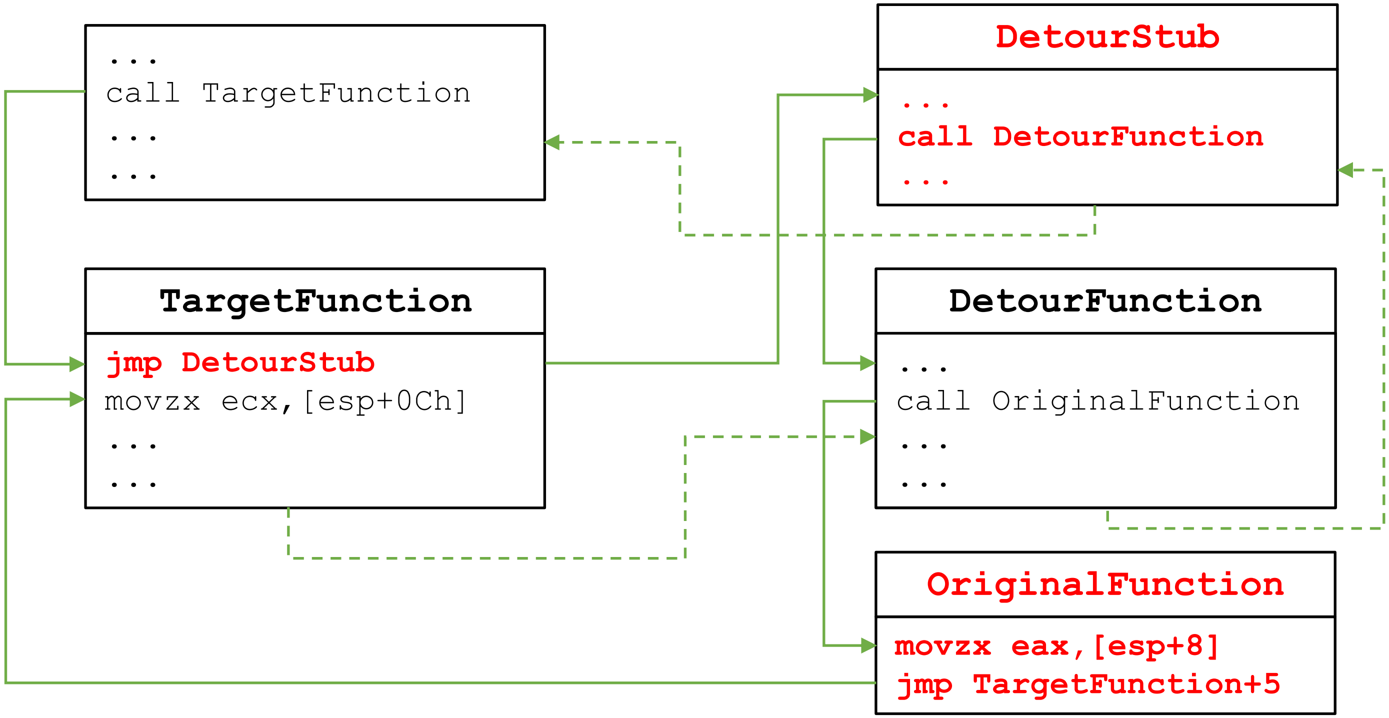
DetourFunction

```
...
call OriginalFunction
...
...
```

OriginalFunction

```
movzx eax,[esp+8]
jmp TargetFunction+5
```

Function detouring framework



```
...
call TargetFunction
...
...
```

TargetFunction

```
jmp DetourStub
movzx ecx,[esp+0Ch]
...
...
```

DetourStub

```
...
call DetourFunction
...
```

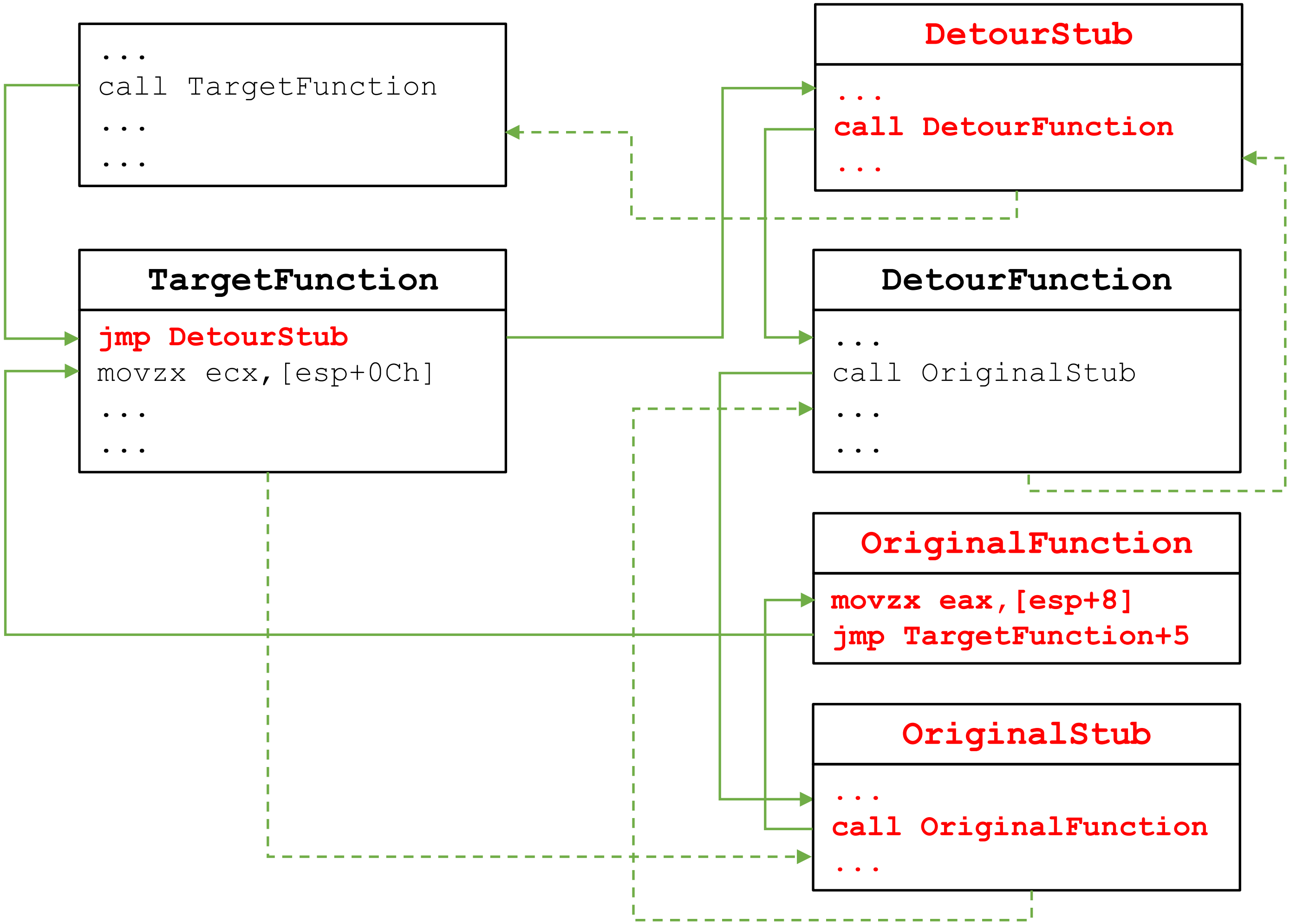
DetourFunction

```
...
call OriginalFunction
...
...
```

OriginalFunction

```
movzx eax,[esp+8]
jmp TargetFunction+5
```

Function detouring framework



```
...
call TargetFunction
...
...
```

TargetFunction

```
jmp DetourStub
movzx ecx,[esp+0Ch]
...
...
```

DetourStub

```
...
call DetourFunction
...
```

DetourFunction

```
...
call OriginalStub
...
...
```

OriginalFunction

```
movzx eax,[esp+8]
jmp TargetFunction+5
```

OriginalStub

```
...
call OriginalFunction
...
```

Workshop Outline

- Case study: Interacting with PowerPoint
- Function Detouring
- **Detouring exercises**

hr@think-cell.com

think-cell
Chausseestraße 8/E
10115 Berlin
Germany

Tel	+49-30-666473-10
Fax	+49-30-666473-19

www.think-cell.com

think-cell