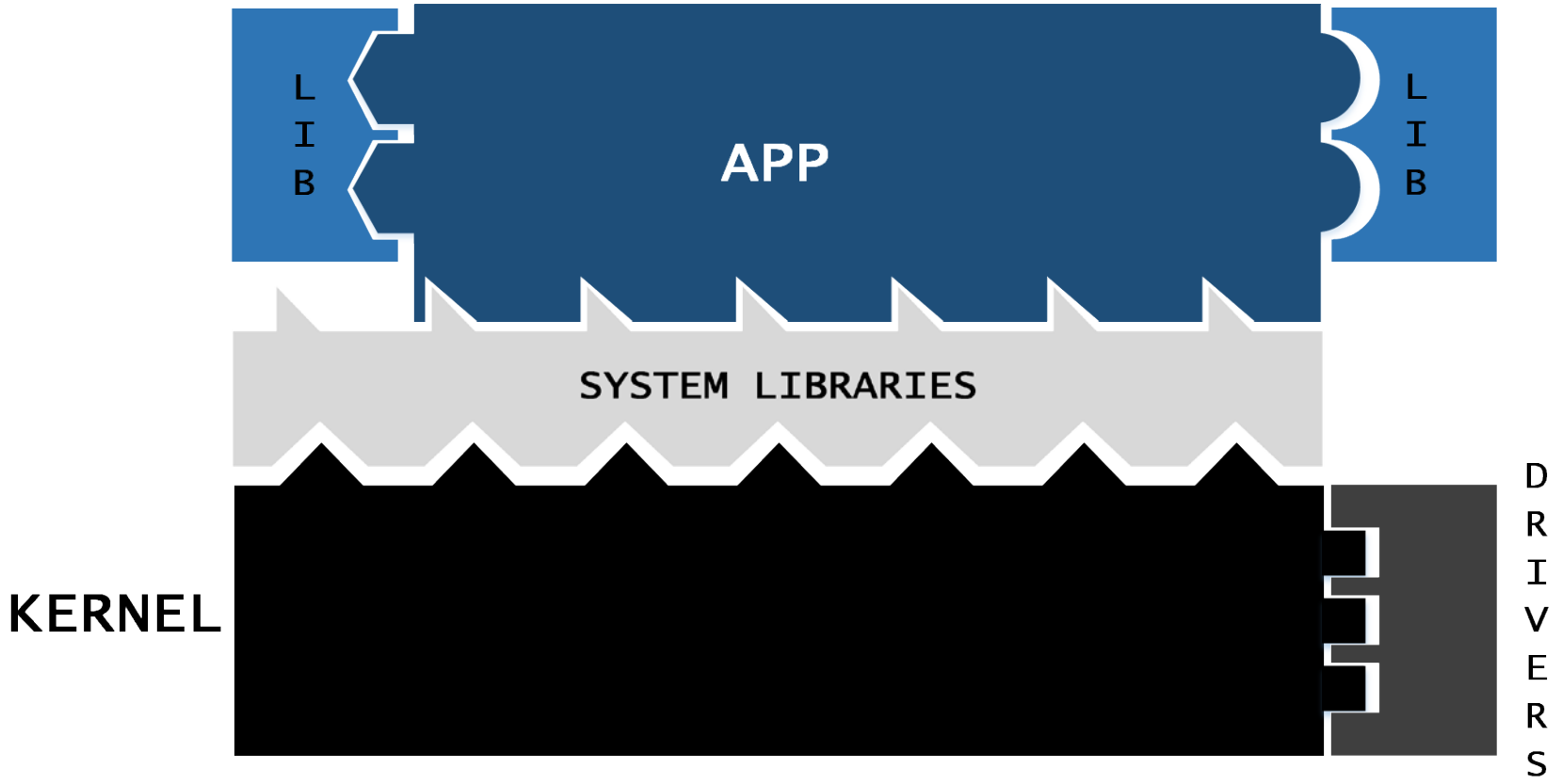
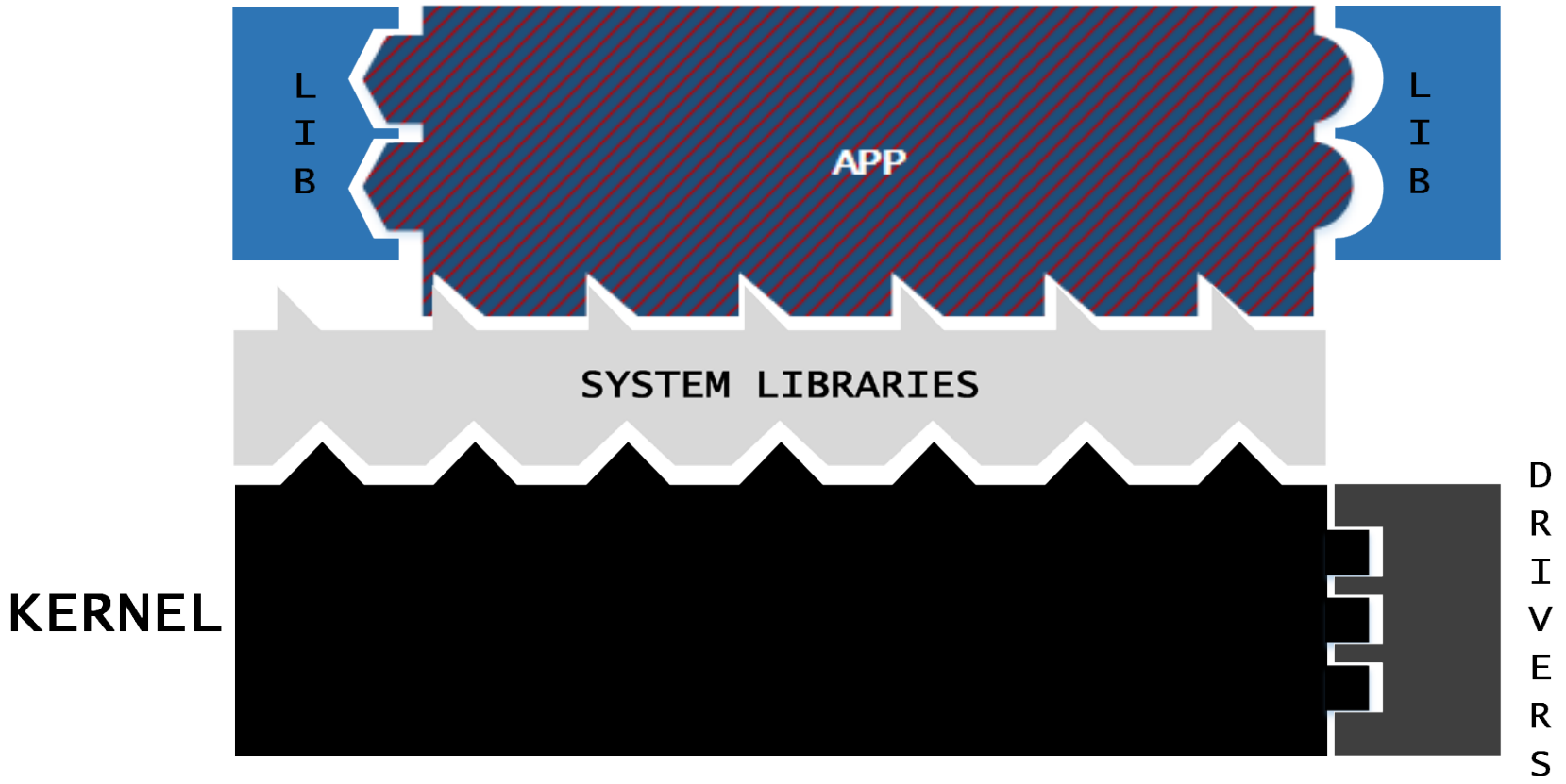
Obfuscating Windows DLLs

Bert Abrath, Bart Coppens, Stijn Volckaert & Bjorn De Sutter

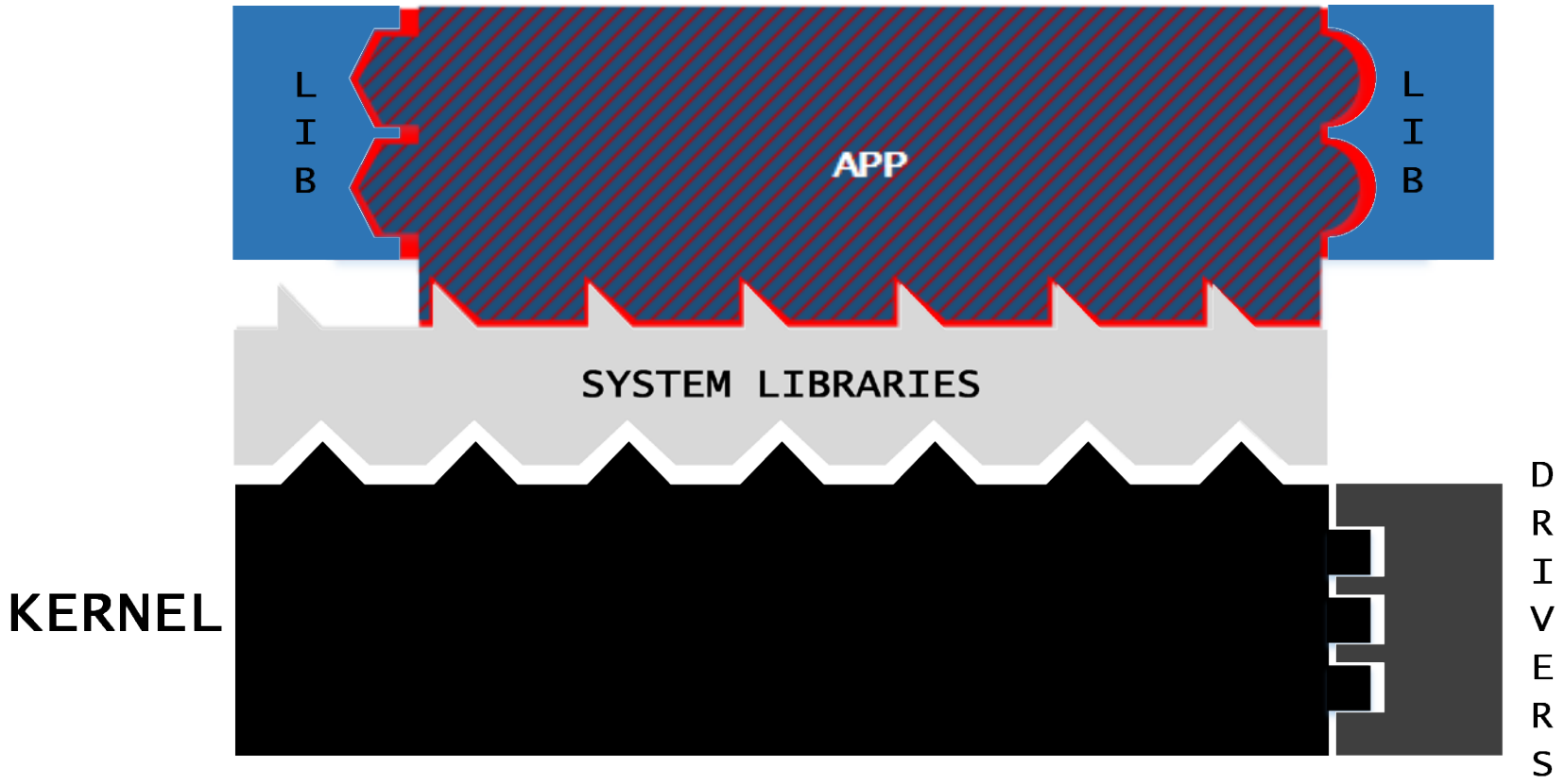
Software Stack – Dynamically linked



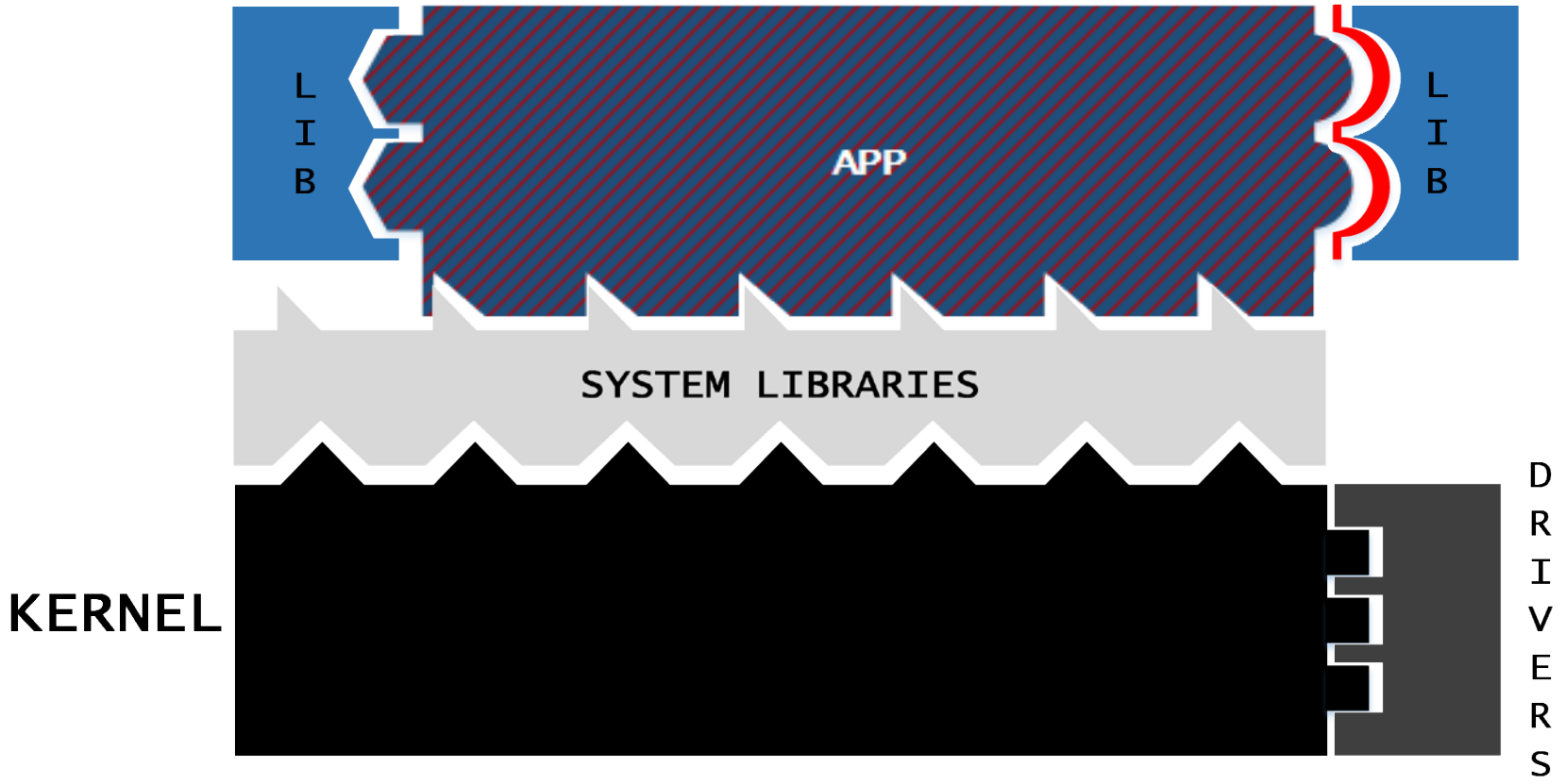
Software Stack – Dynamically linked



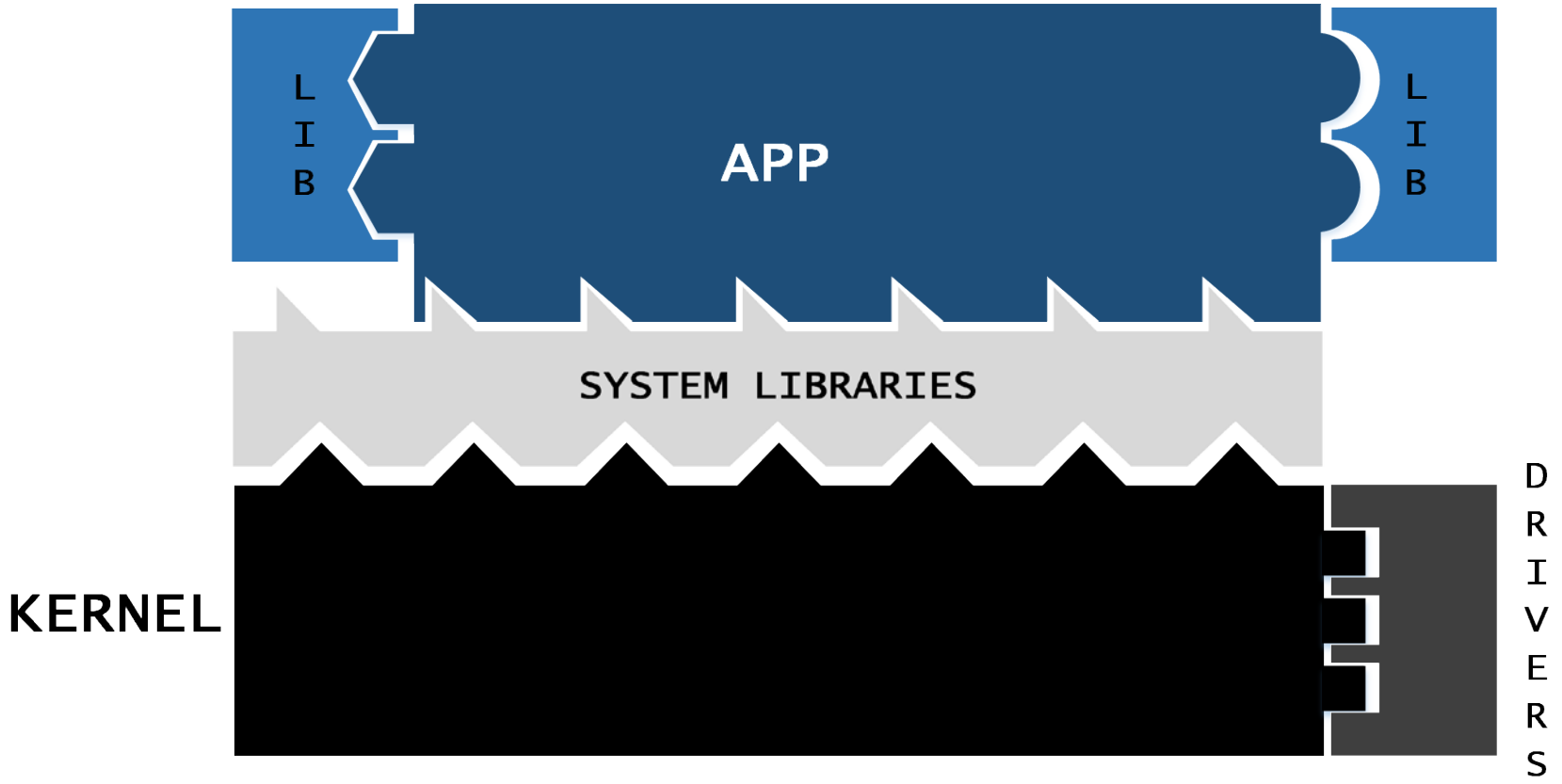
Software Stack – Dynamically linked



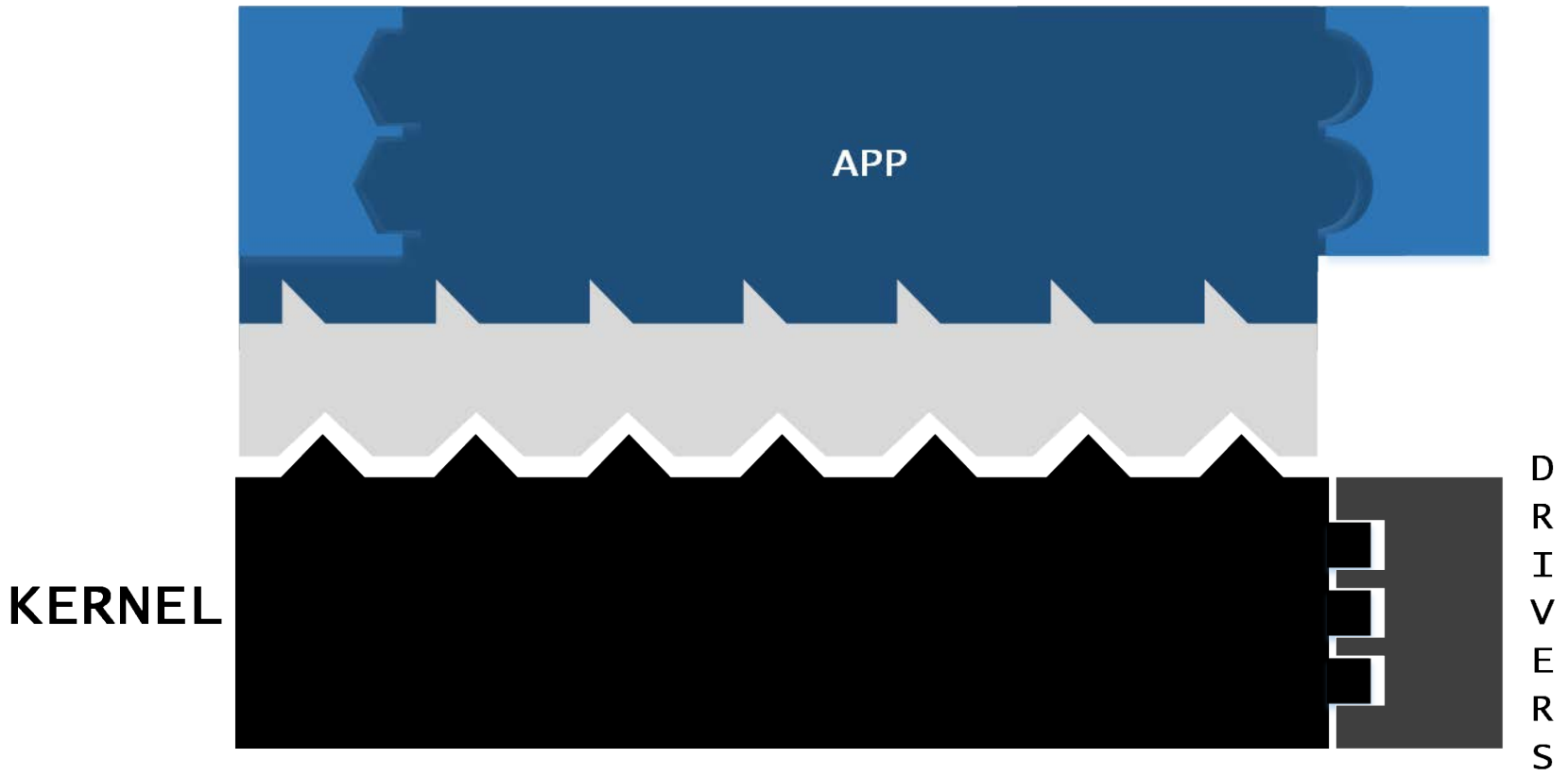
Software Stack – Dynamically linked



Software Stack – Dynamically linked

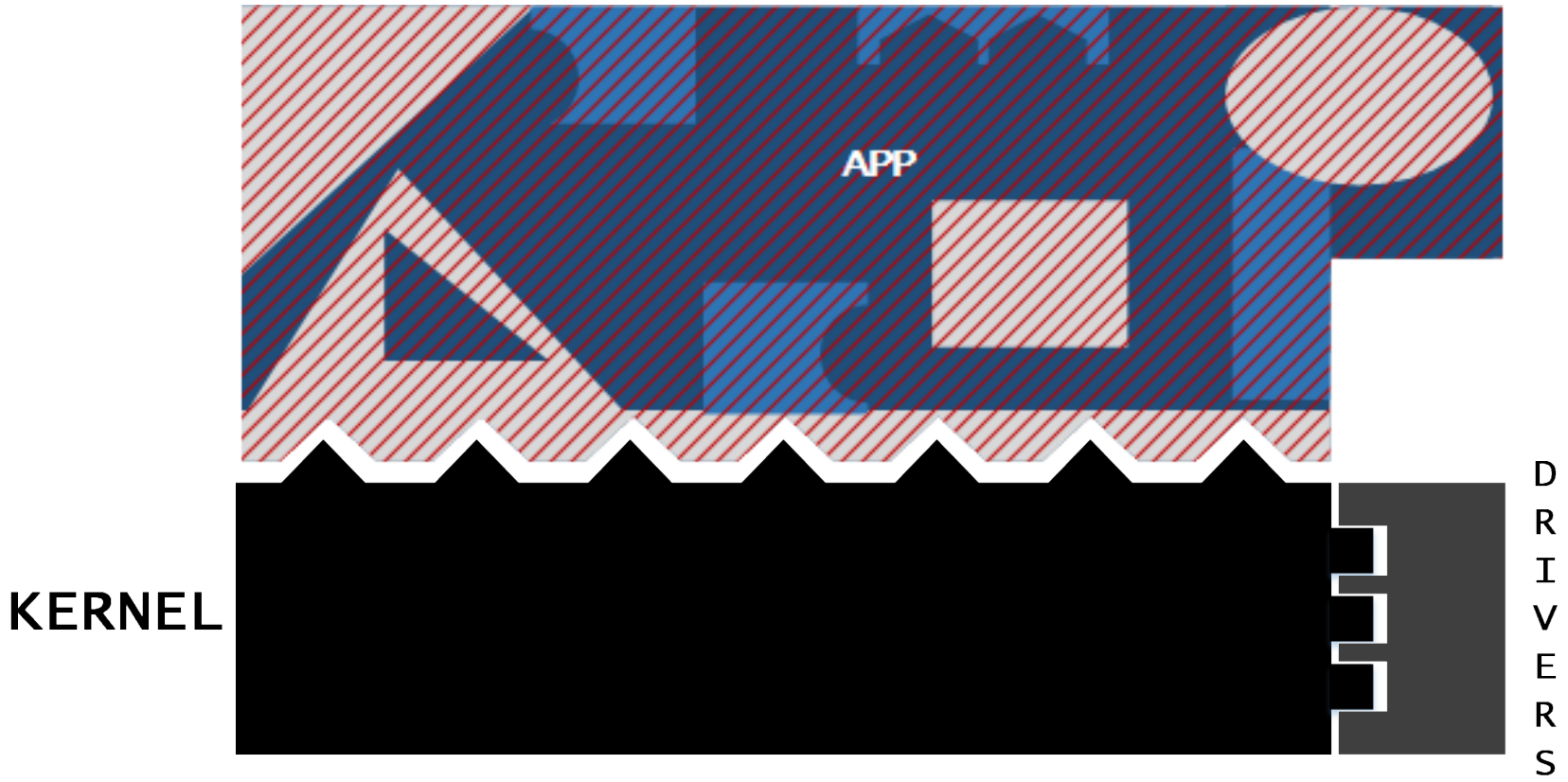


Software Stack – Statically linked



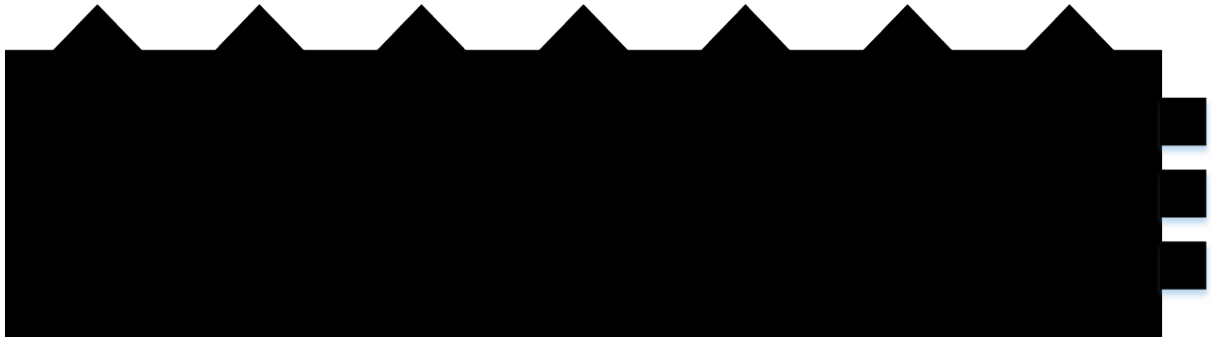
Software Stack – Statically linked

Software Stack – Statically linked

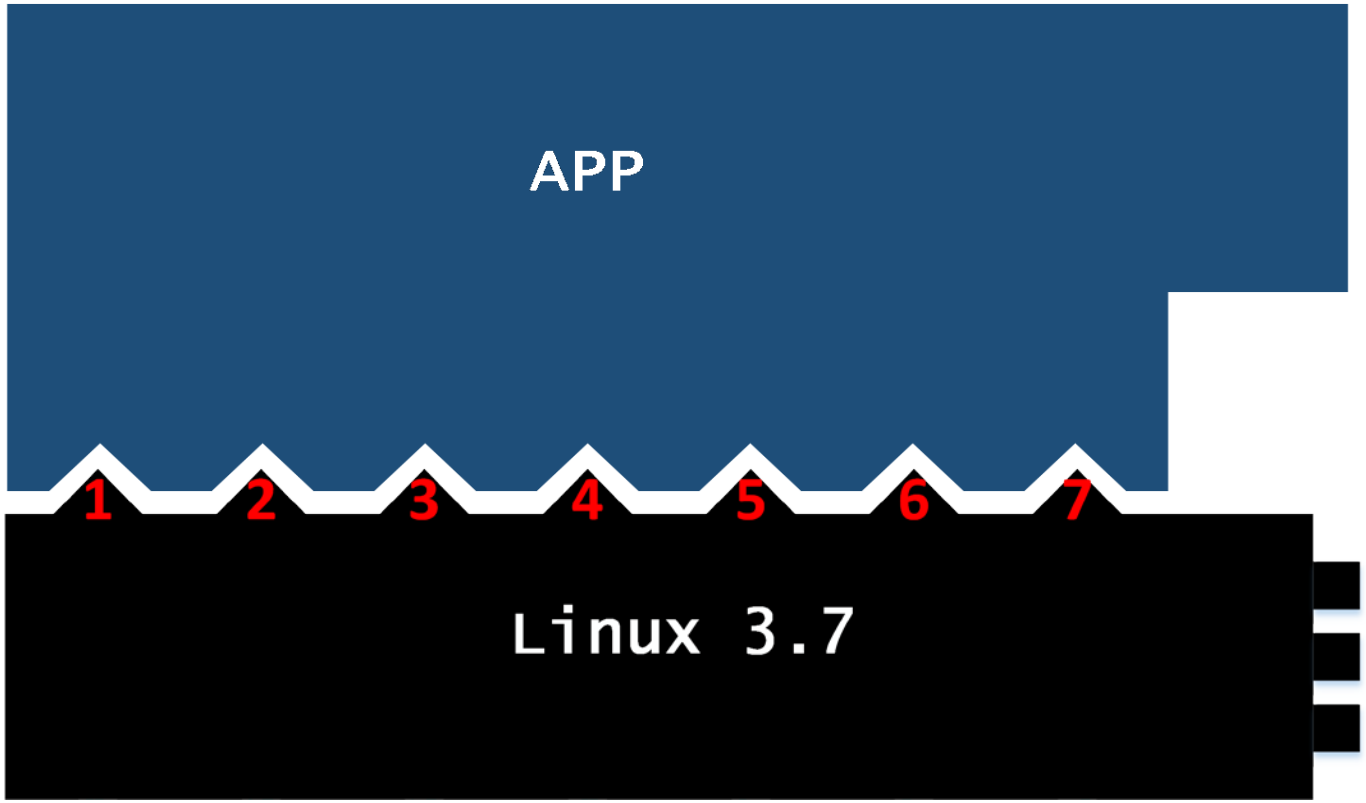


Kernel Interface

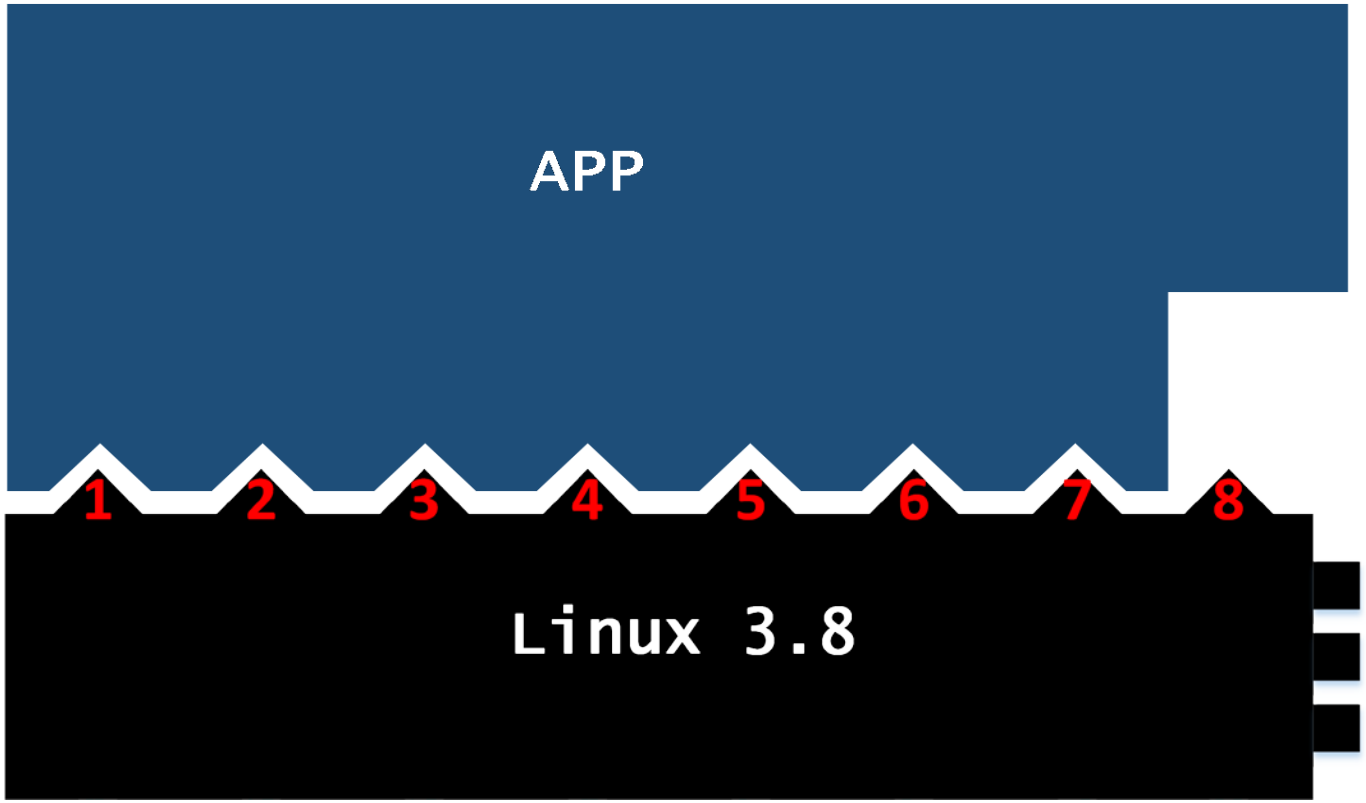
```
MOV EAX, SCN          (System Call Number)
SYSCALL
```



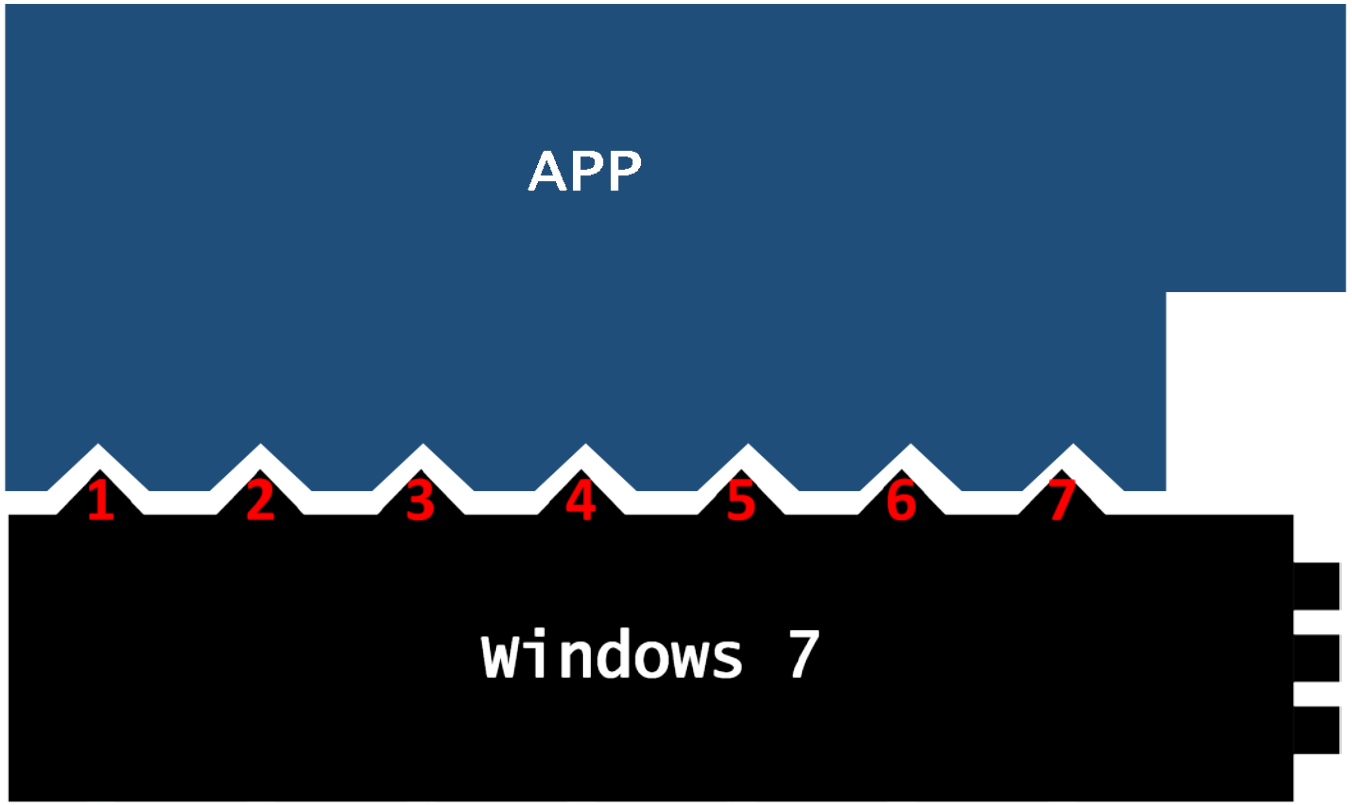
Kernel Interface



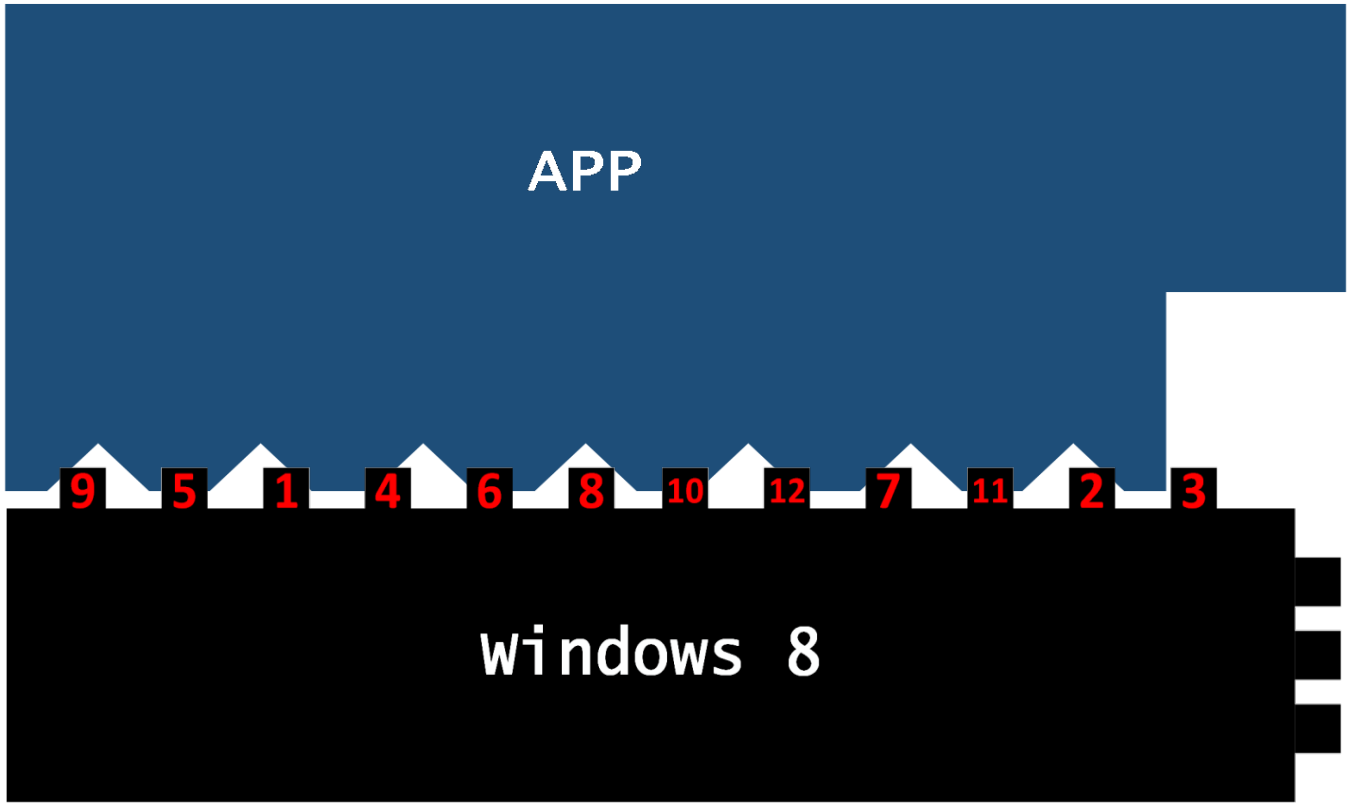
Kernel Interface



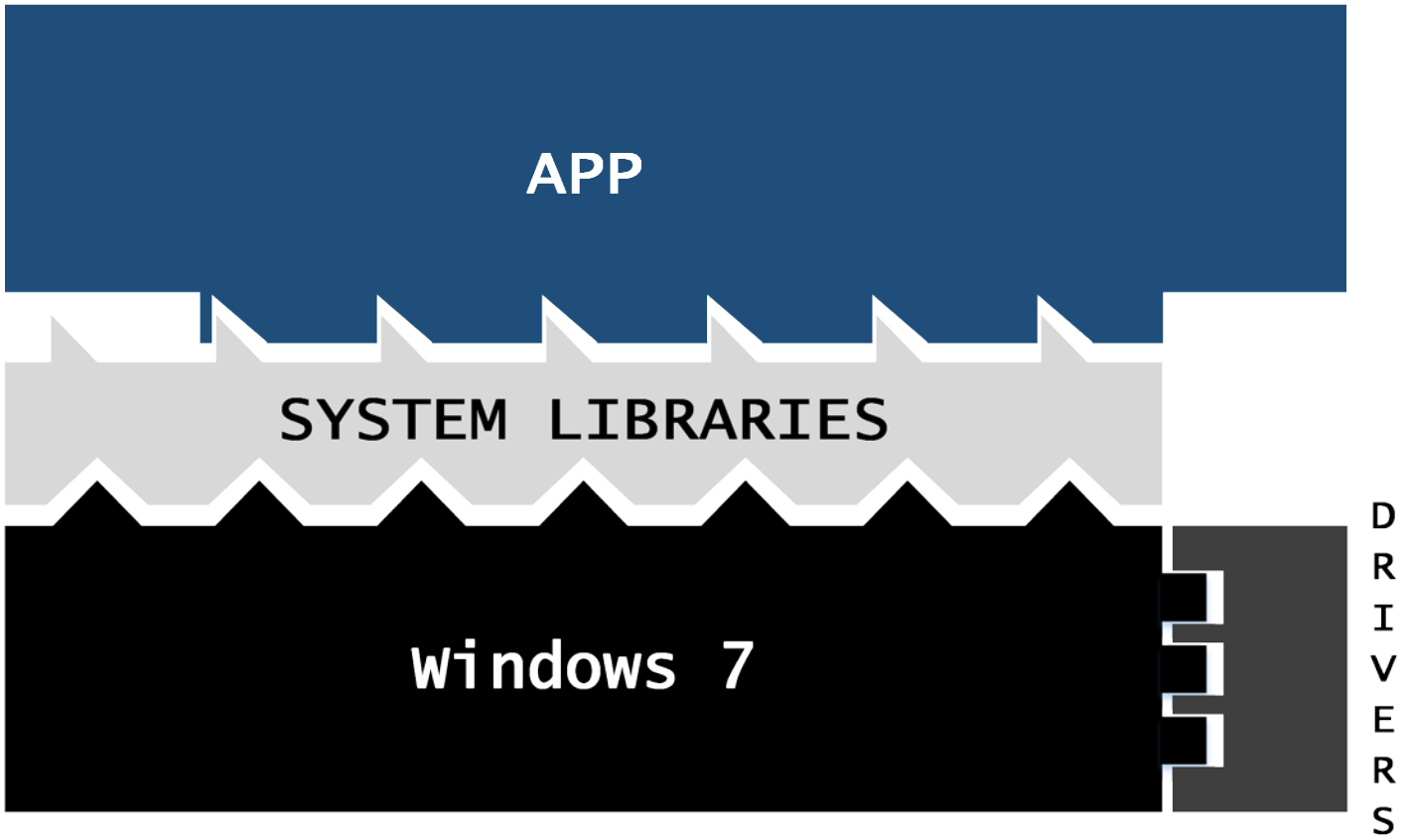
Kernel Interface



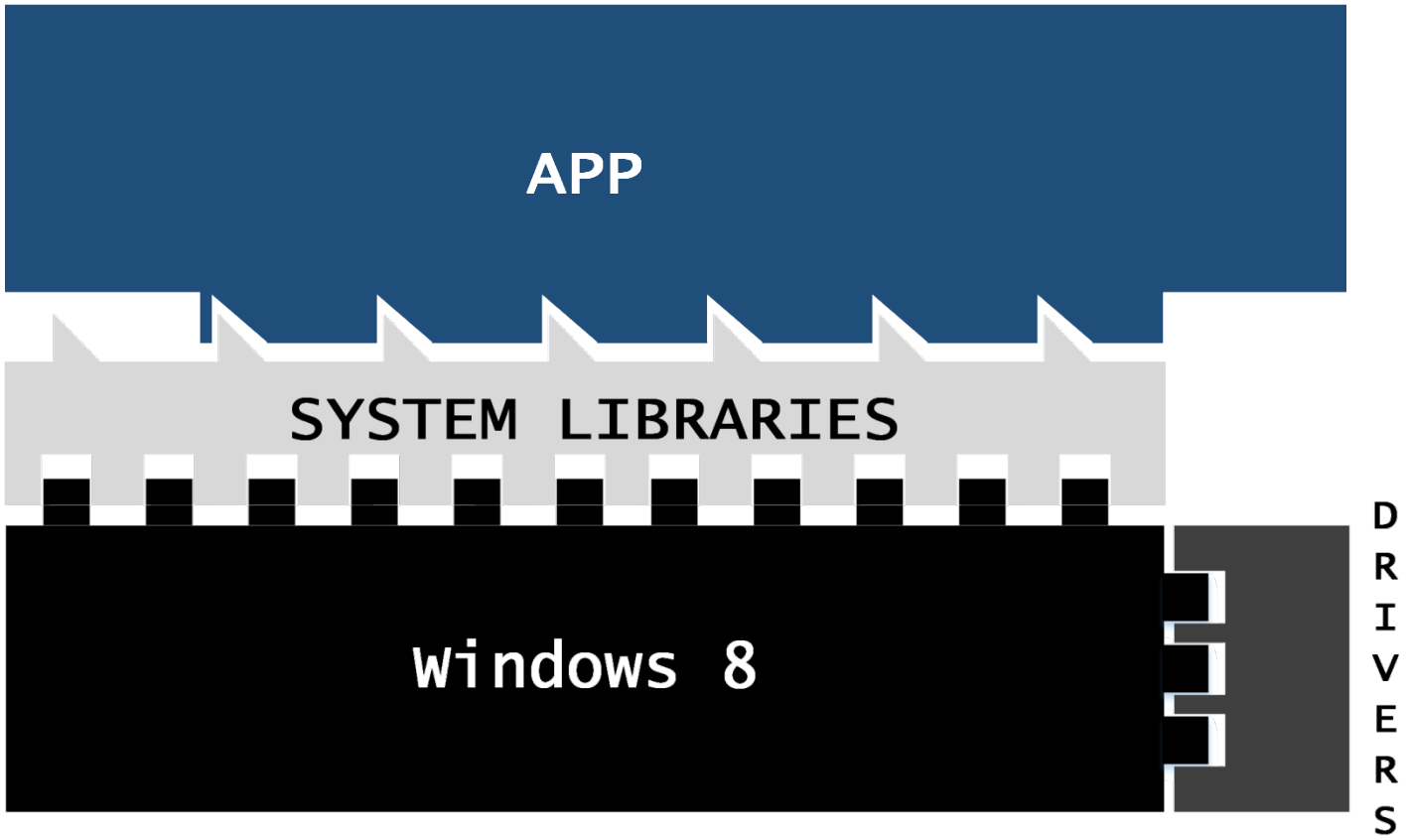
Kernel Interface



Kernel Interface



Kernel Interface

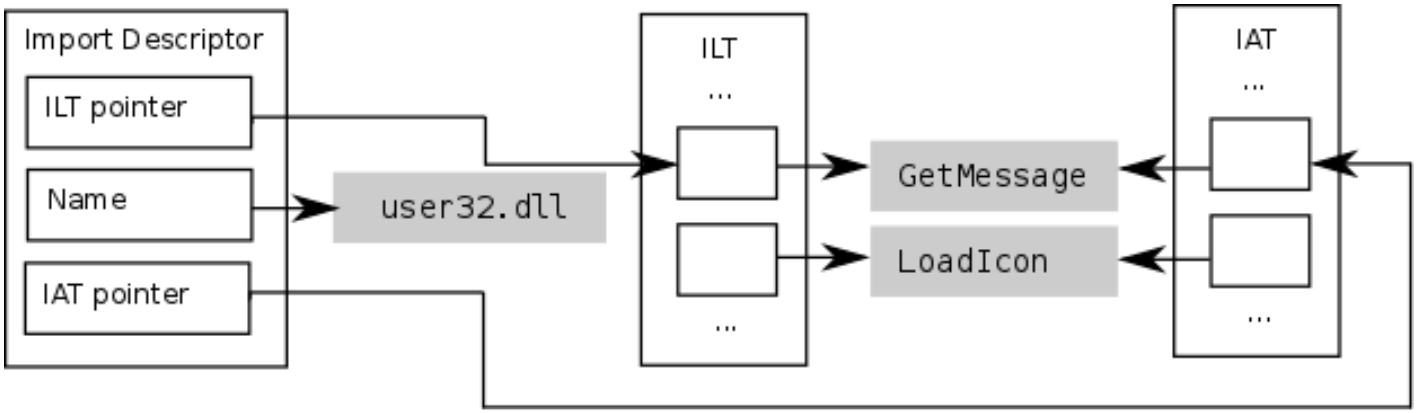


Overview

1. Dynamic Linking on Windows
2. Removing Program Import Information
3. Static Linking of Binaries
4. Implementation
5. Evaluation
6. Conclusions

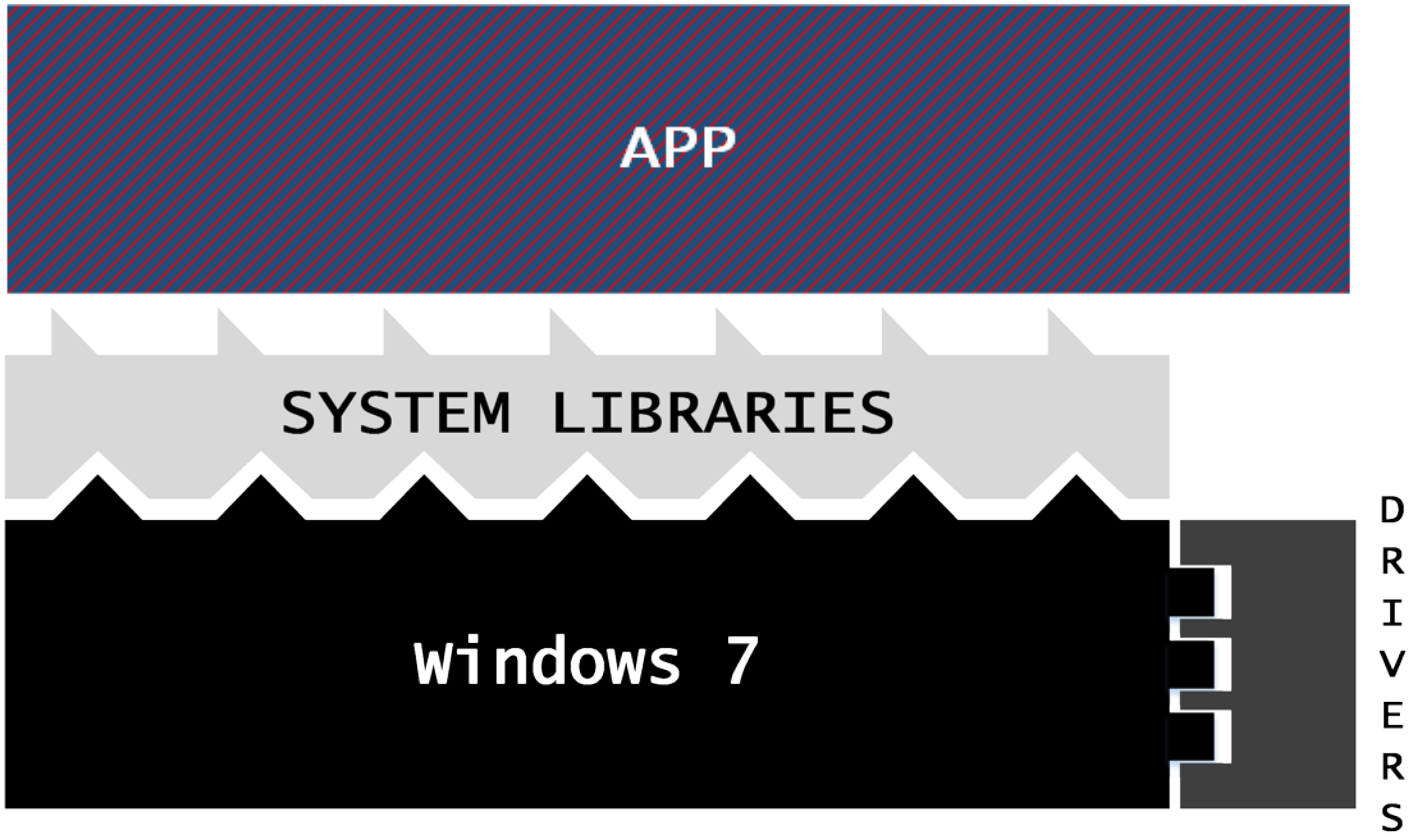
Dynamic Linking on Windows

- PE (= Portable Executable) format
- Import tables

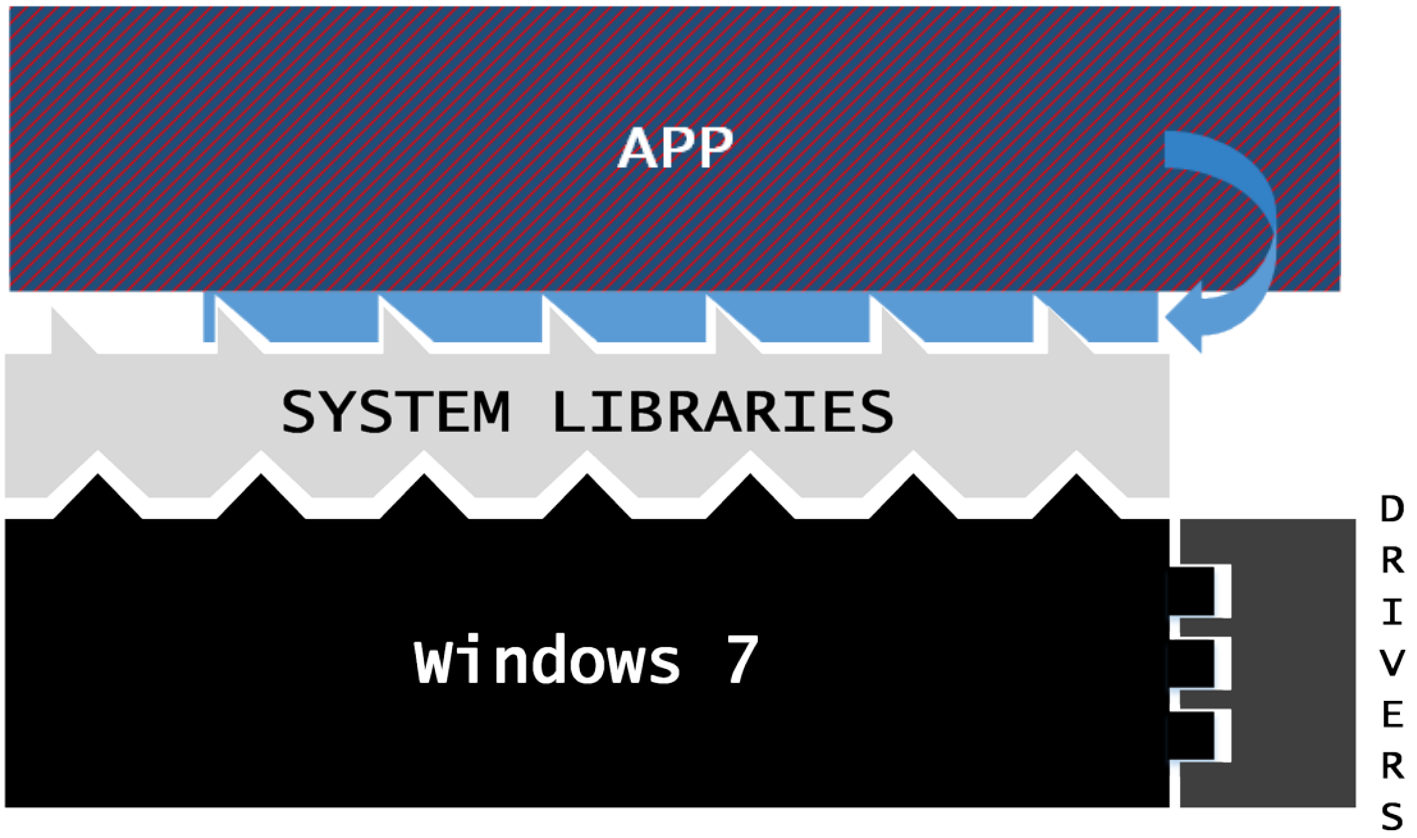


call [IAT+offset]

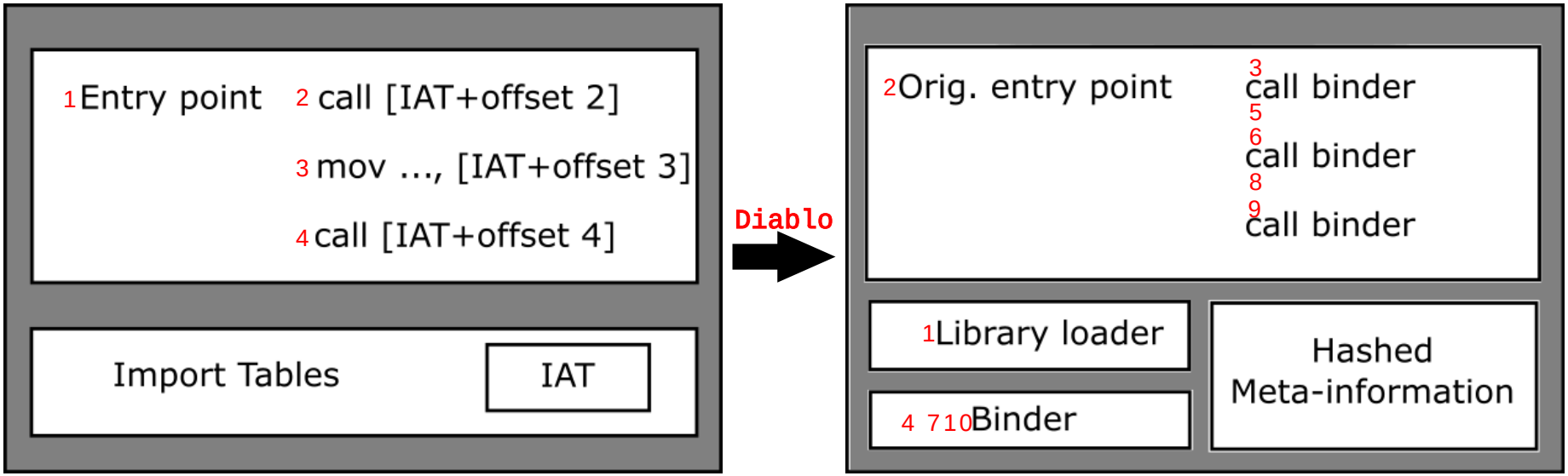
Removing Program Import Information



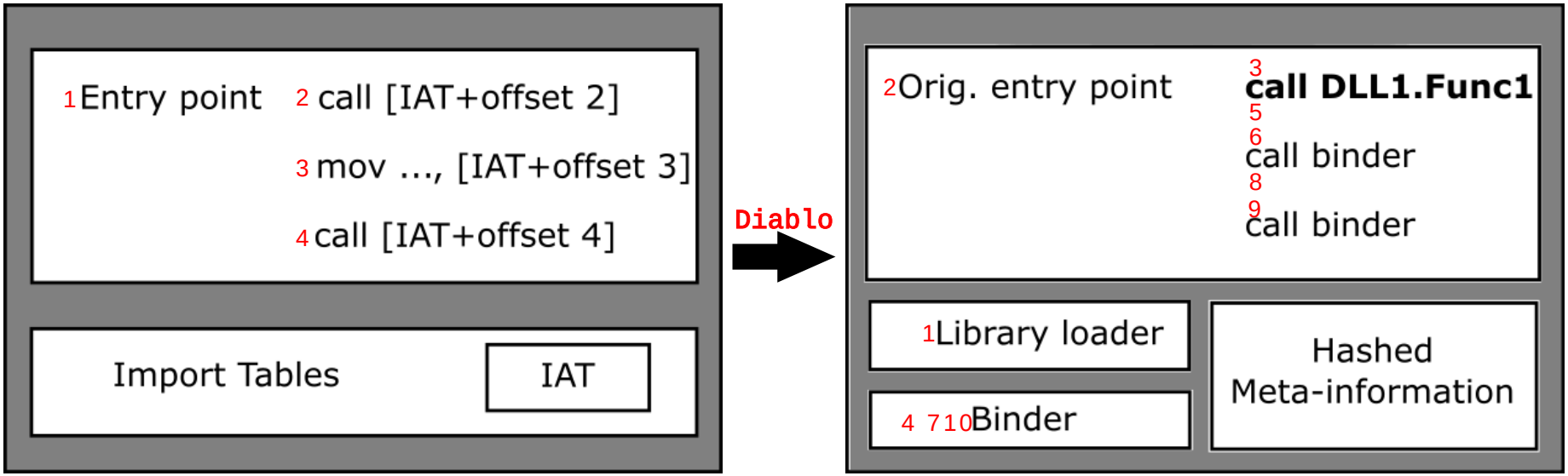
Removing Program Import Information



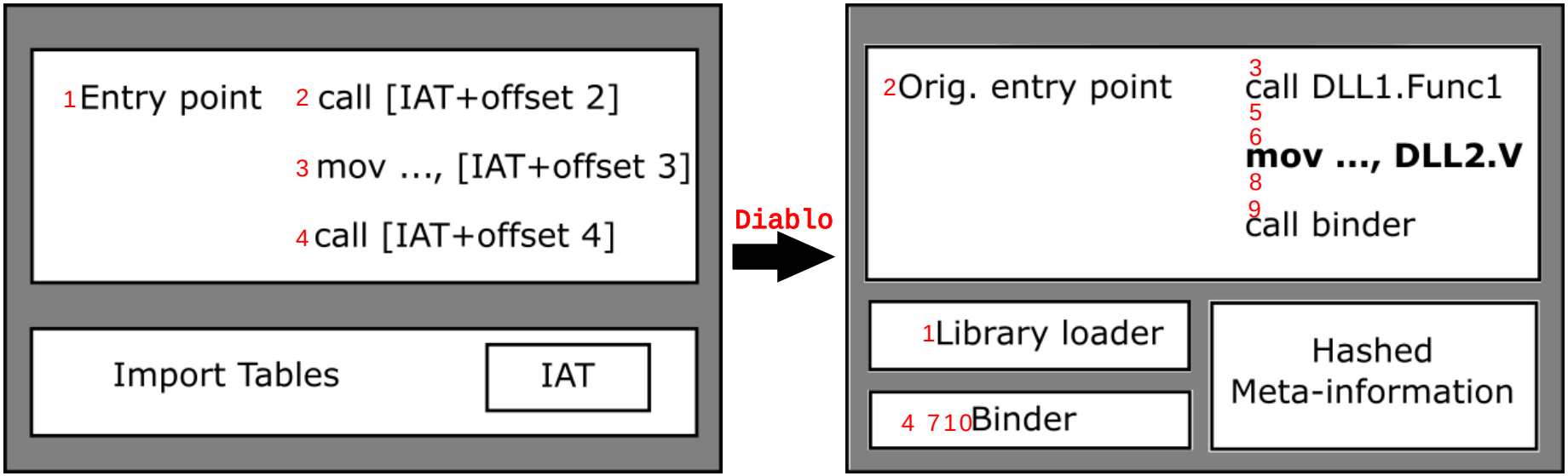
Removing Program Import Information



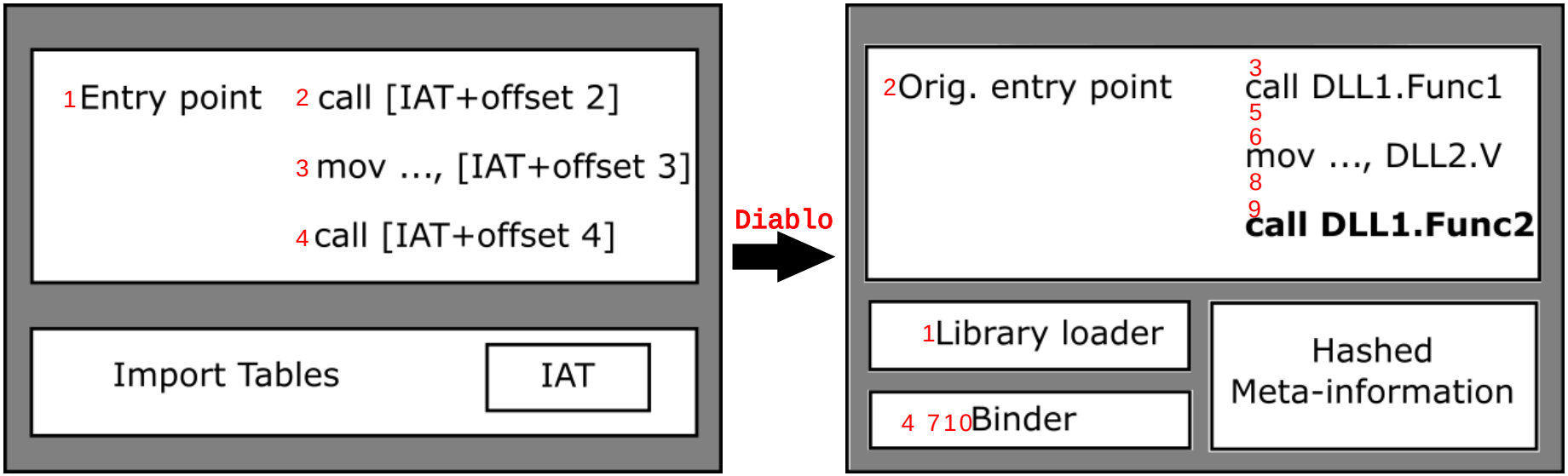
Removing Program Import Information



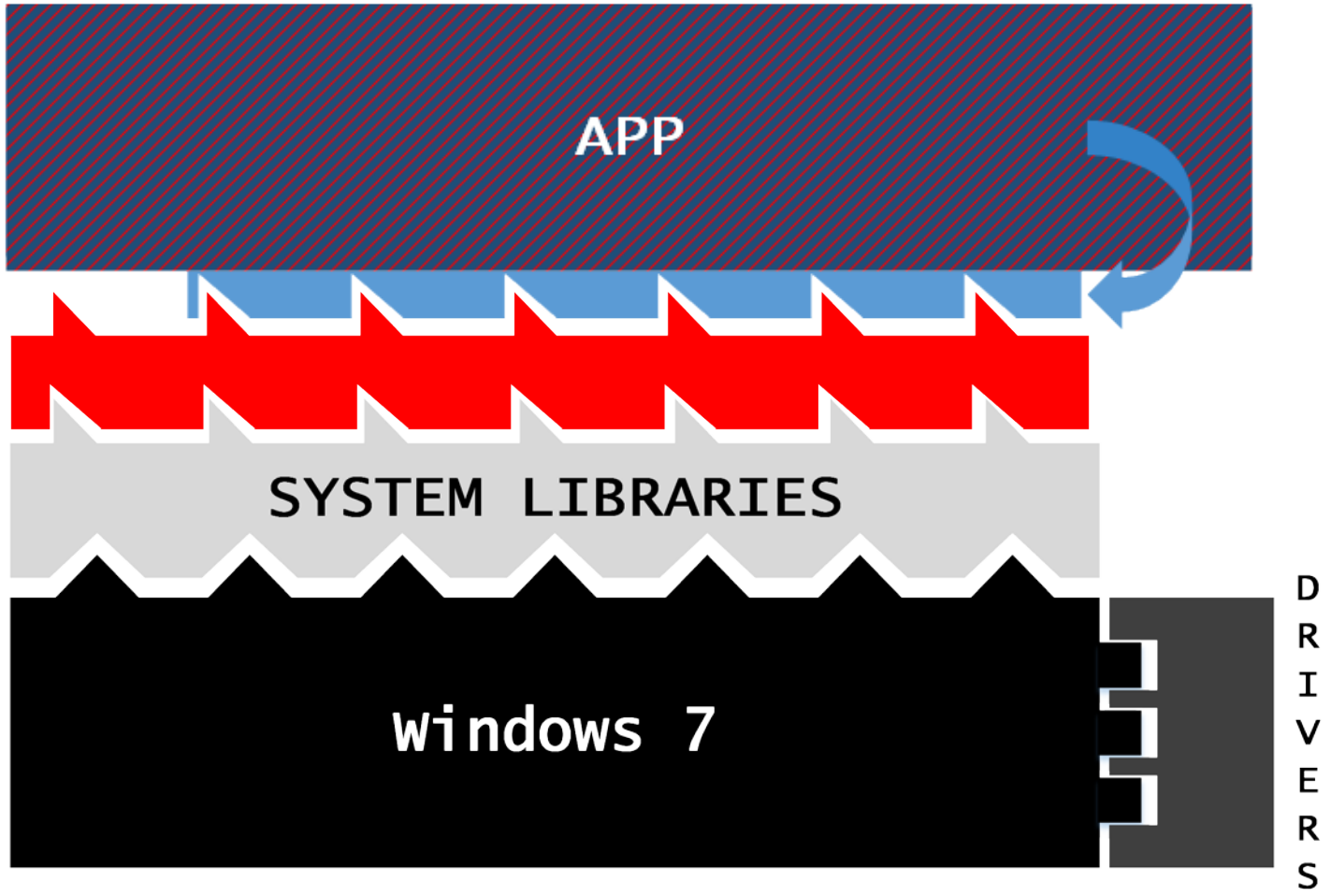
Removing Program Import Information



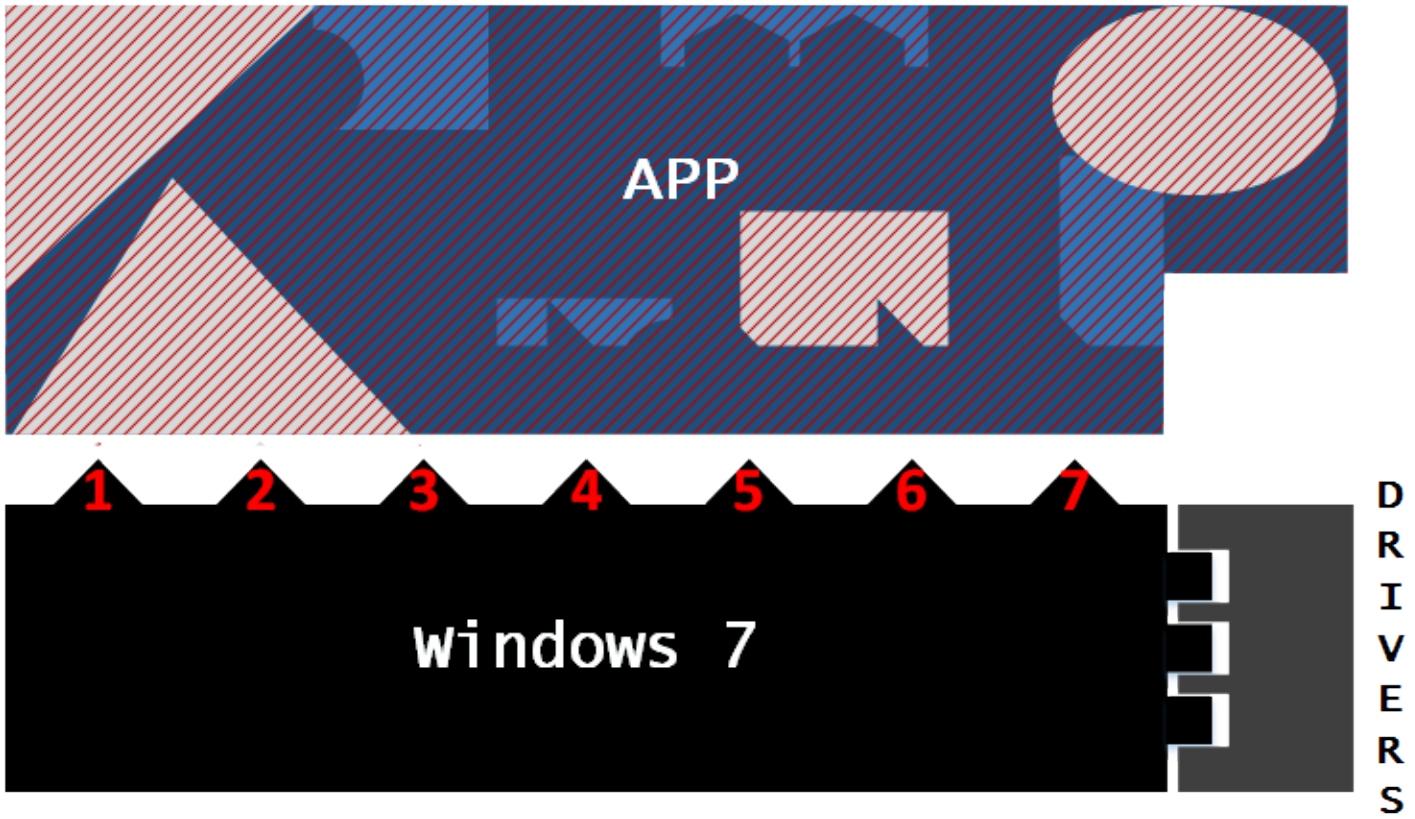
Removing Program Import Information



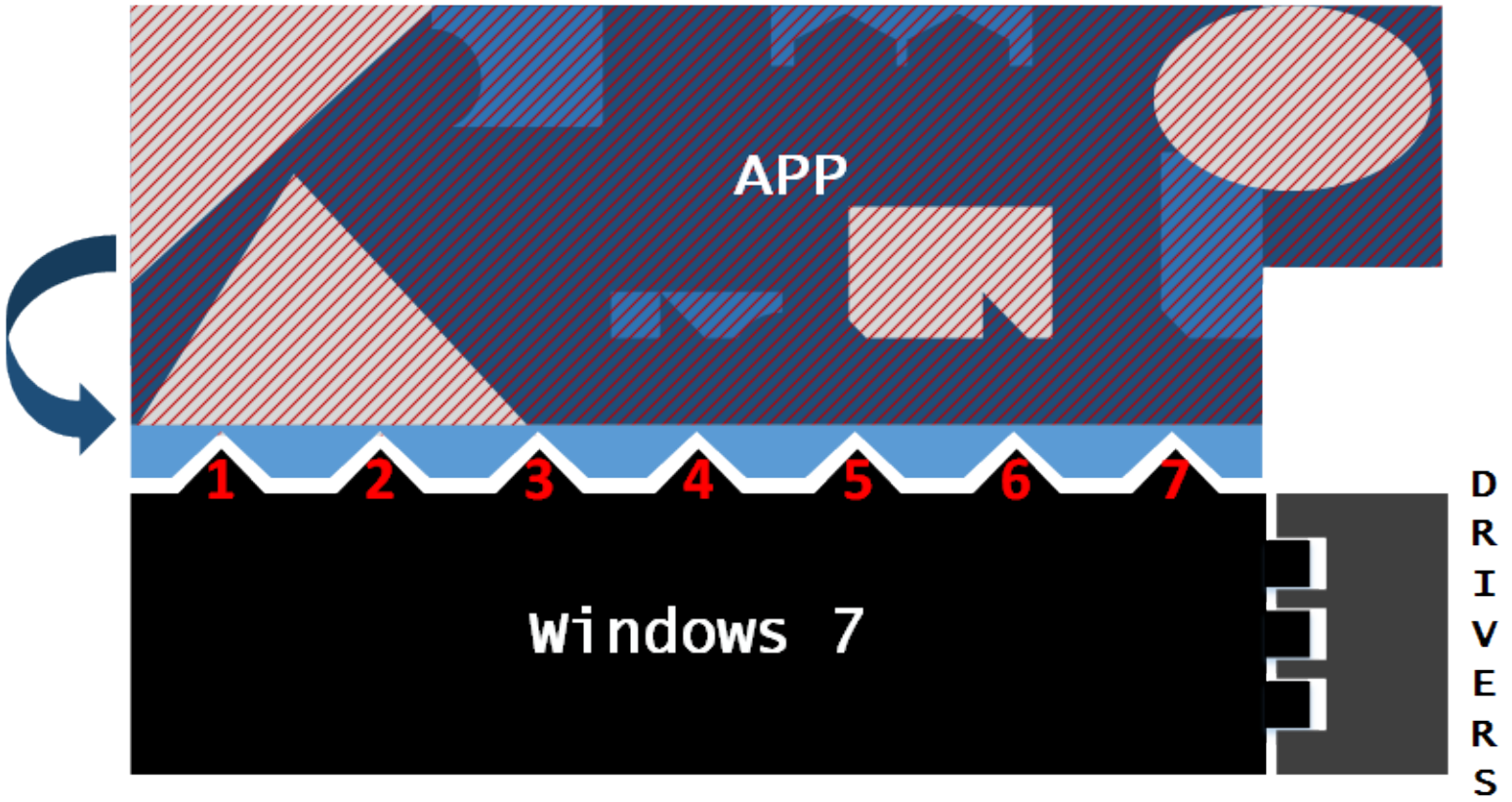
Removing Program Import Information



Static Linking of Binaries

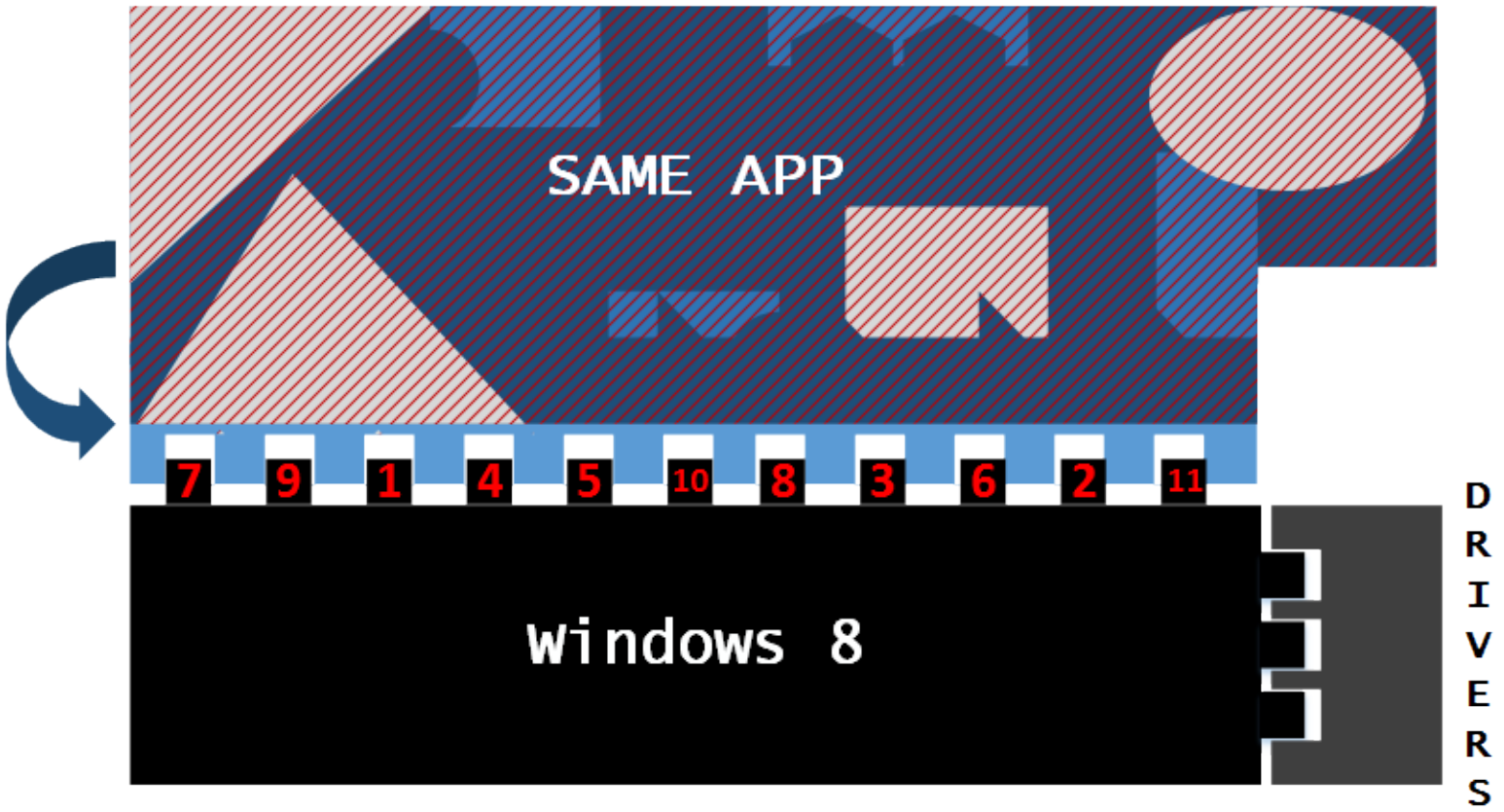


Static Linking of Binaries

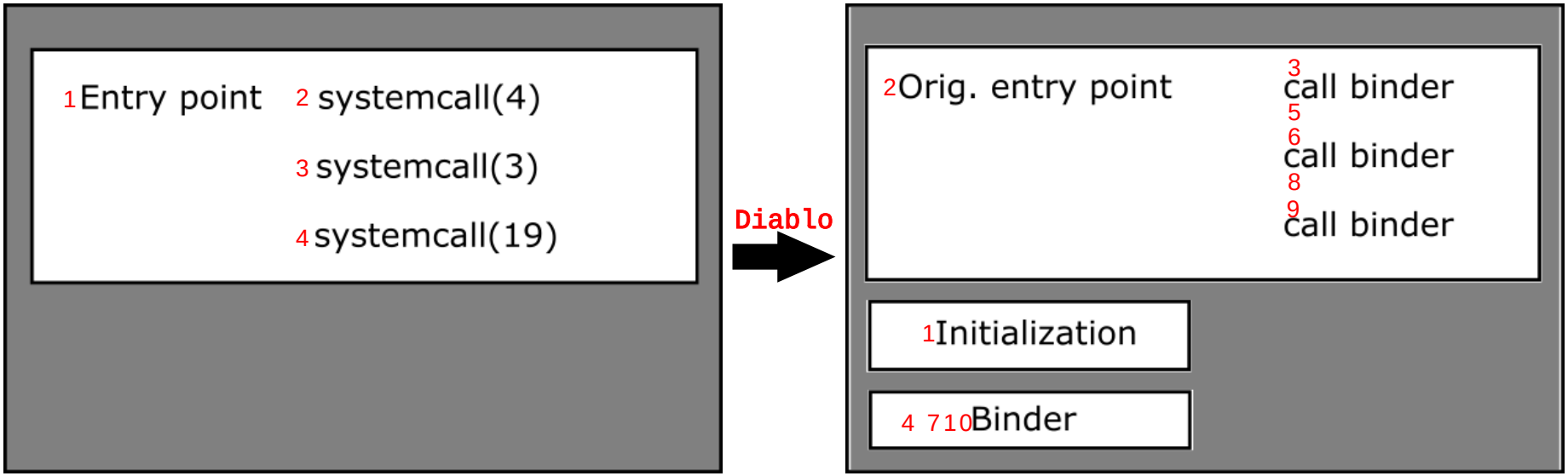


Static Linking of Binaries

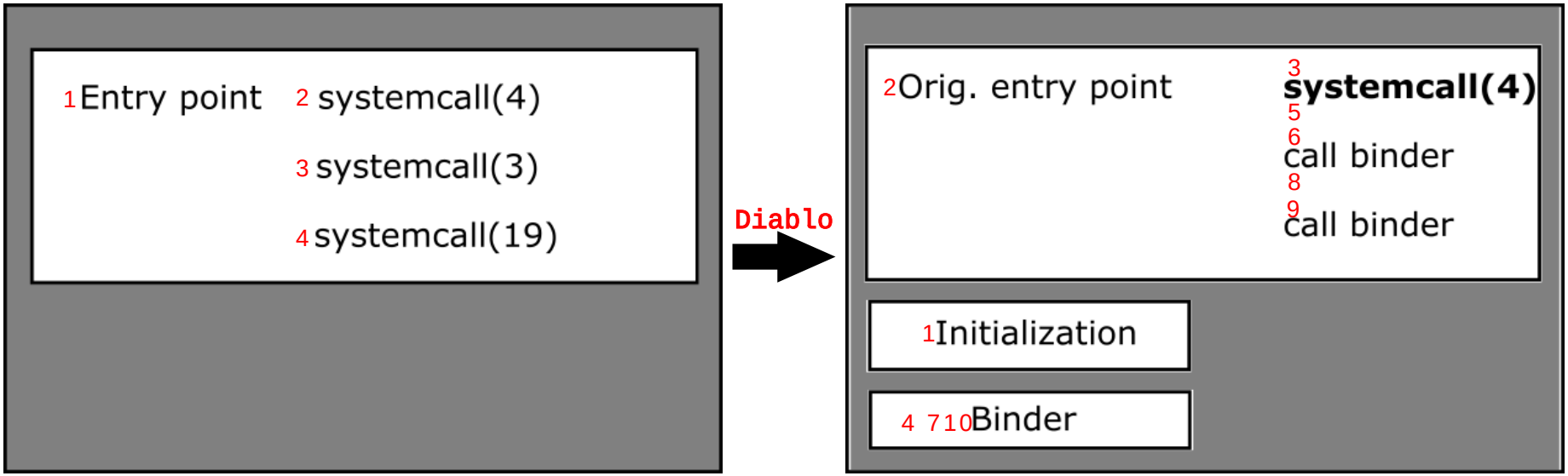
Static Linking of Binaries



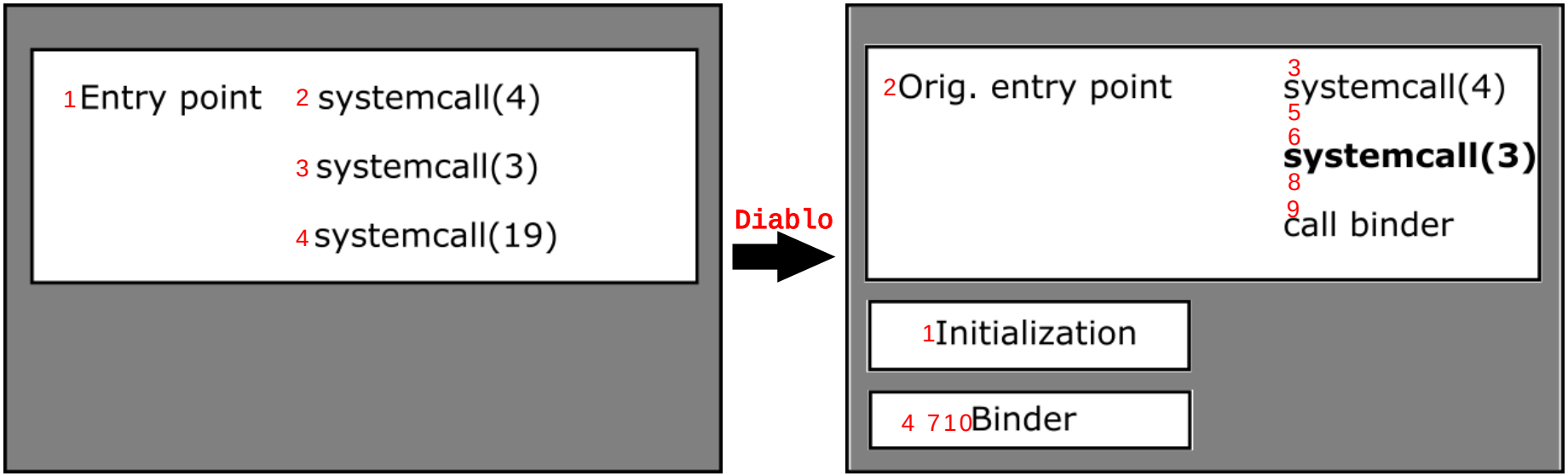
Static Linking of Binaries



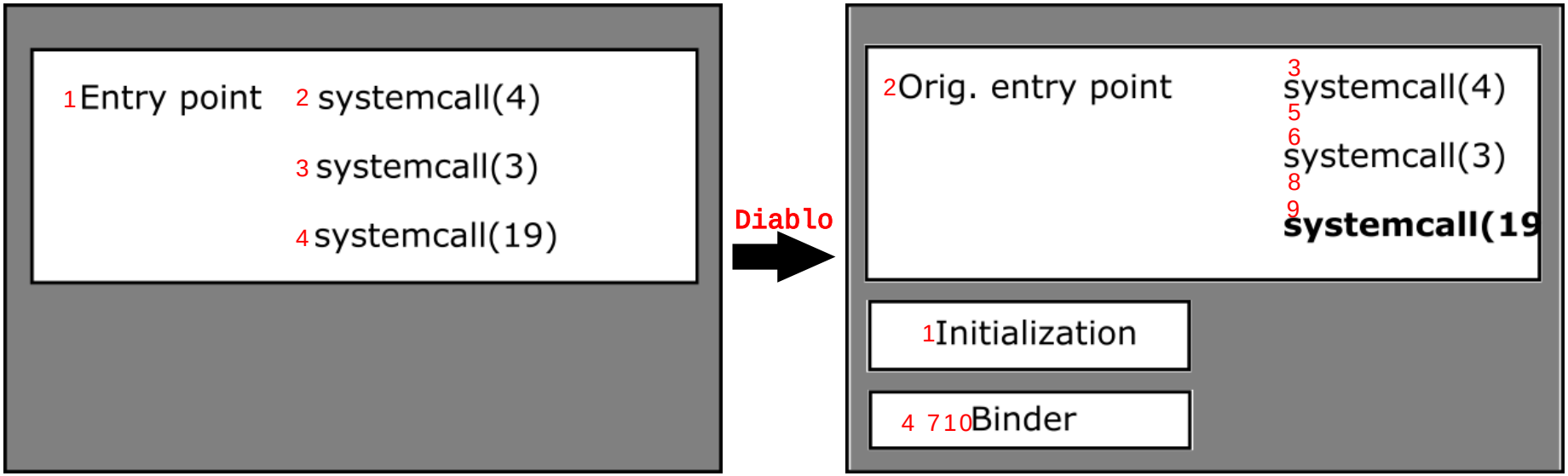
Static Linking of Binaries



Static Linking of Binaries



Static Linking of Binaries



Implementation

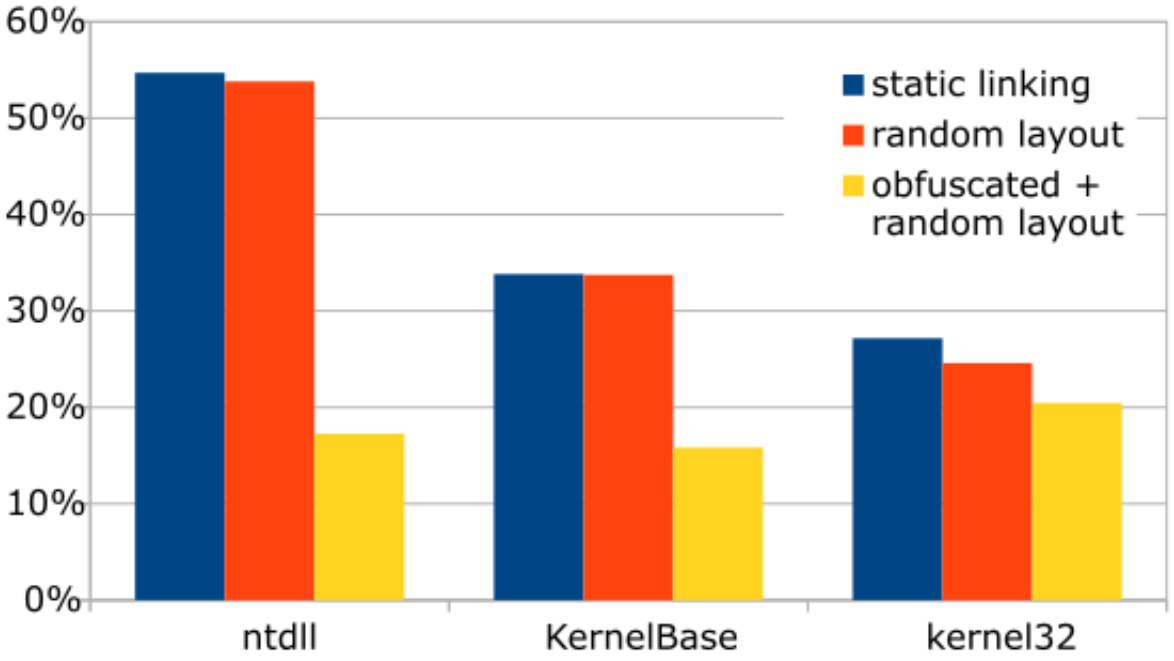
Evaluation (Program size)

- Simple test program
- Three versions for second technique
- Tested on Windows 7, Windows 8 and Windows 8.1

Input files	
original	2560 B
kernel32	1036288 B
ntdll	1467384 B
KernelBase	838144 B
Total	3344376 B

Rewritten programs	
static linking	2385408 B
random layout	2477568 B
obfuscated	2607104 B

Evaluation (BinDiff)



Conclusions

- Two techniques to automatically obfuscate interface
- Compatibility retained