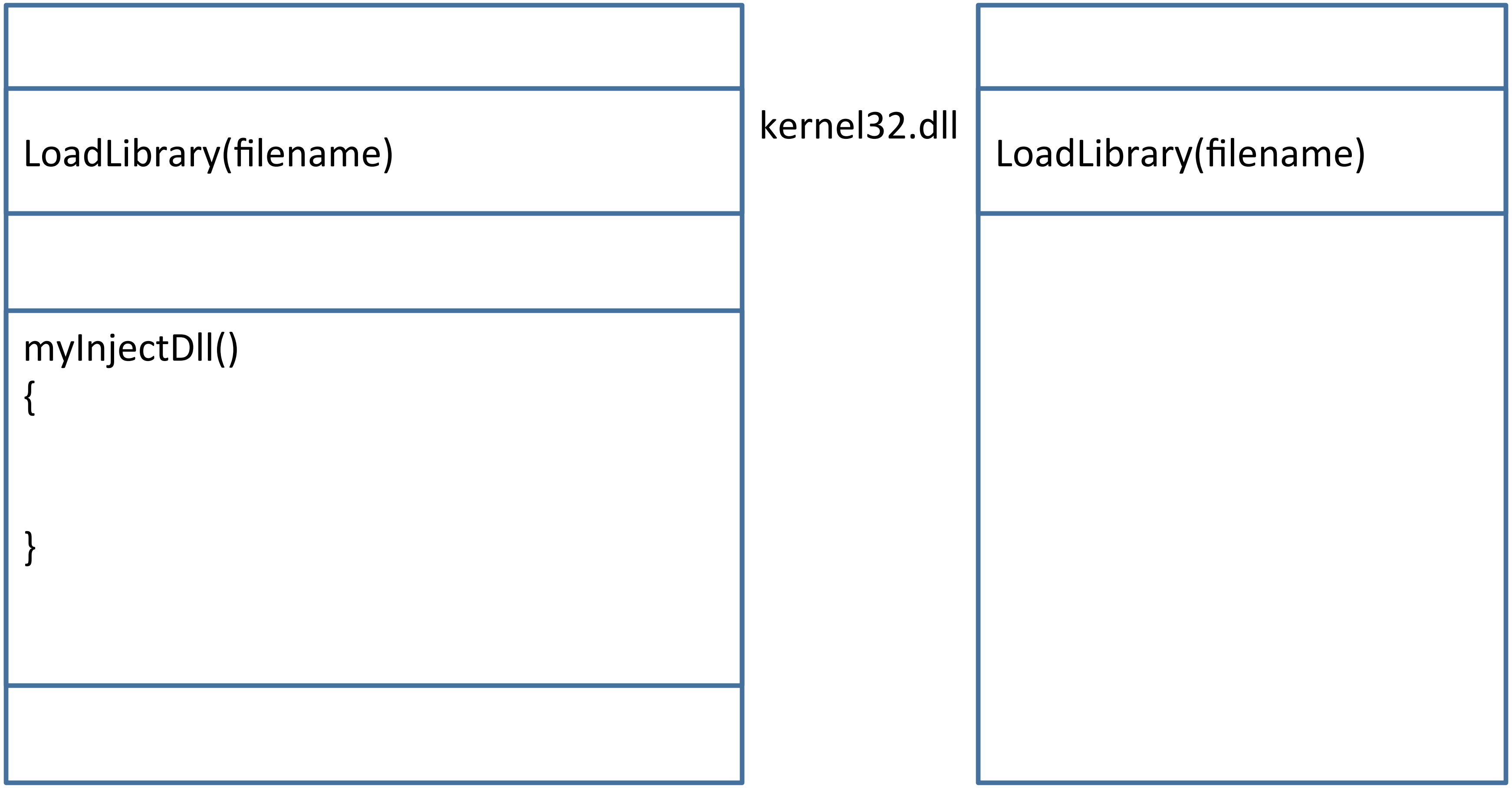


LoadLibrary(filename)

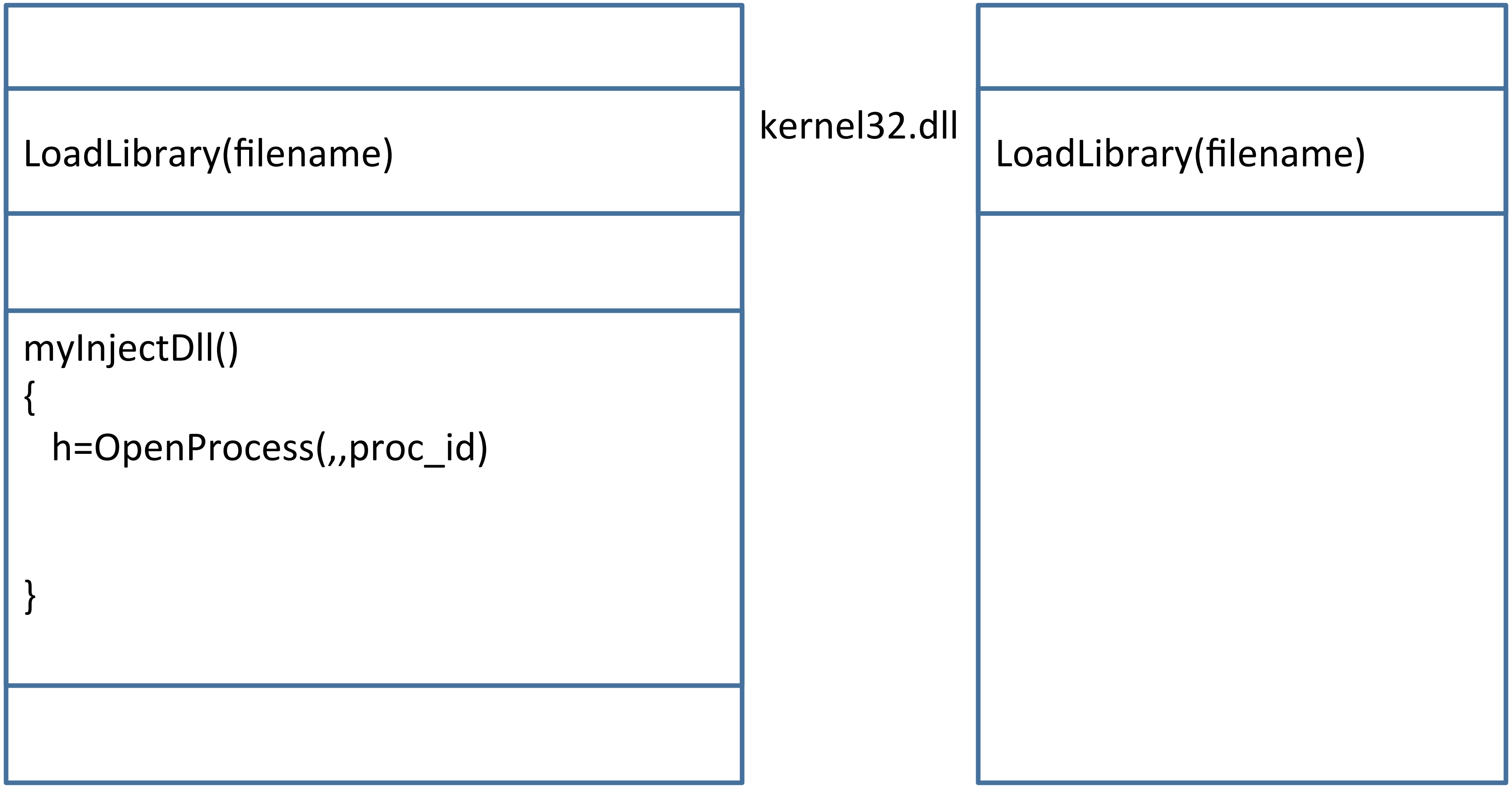
```
myInjectDll()
{


}
```

kernel32.dll

LoadLibrary(filename)

malicious process

Internet Explorer process



LoadLibrary(filename)

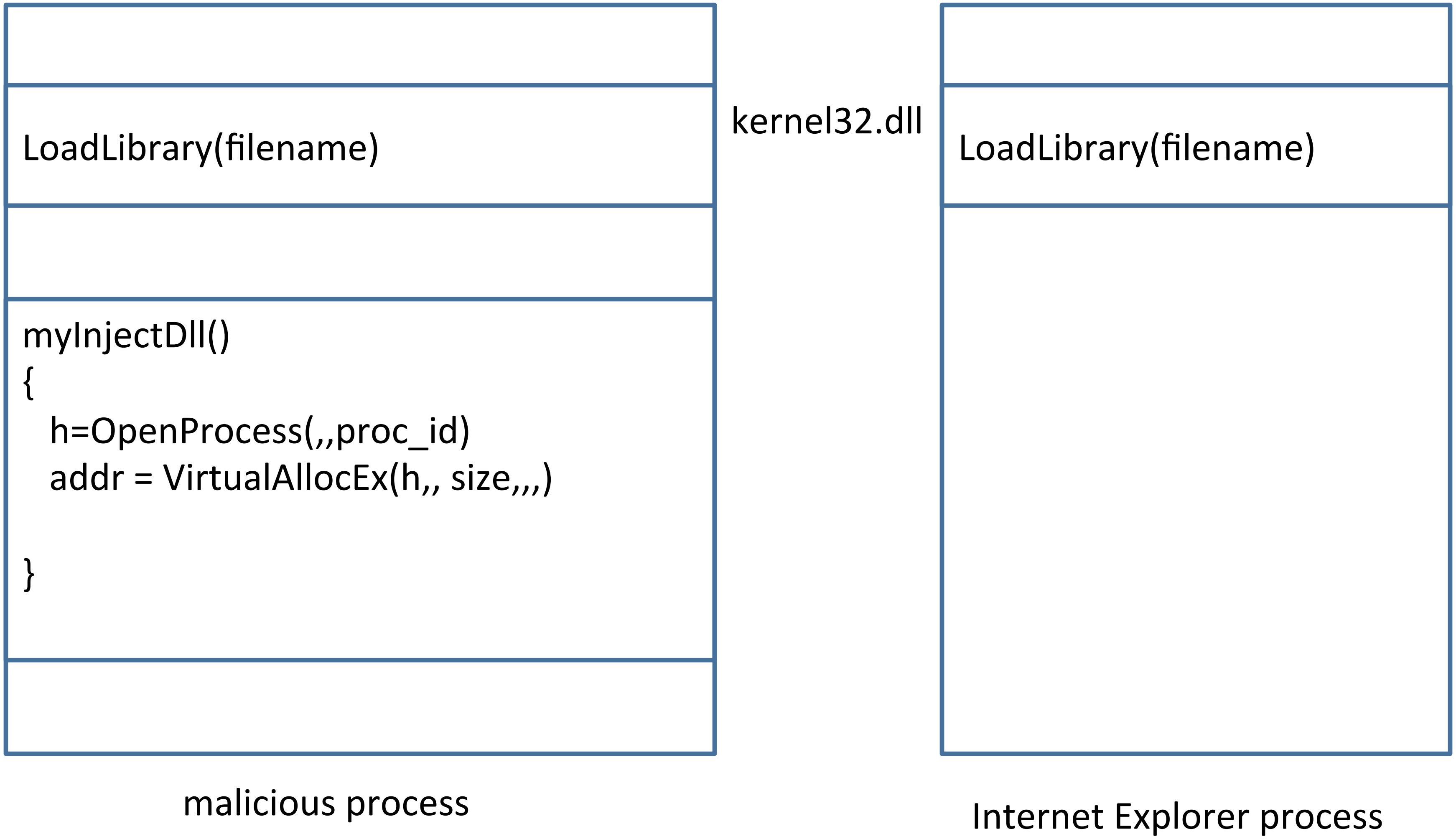
kernel32.dll

LoadLibrary(filename)

```
myInjectDll()
{
   h=OpenProcess(,,proc_id)


}
```

malicious process

Internet Explorer process



LoadLibrary(filename)

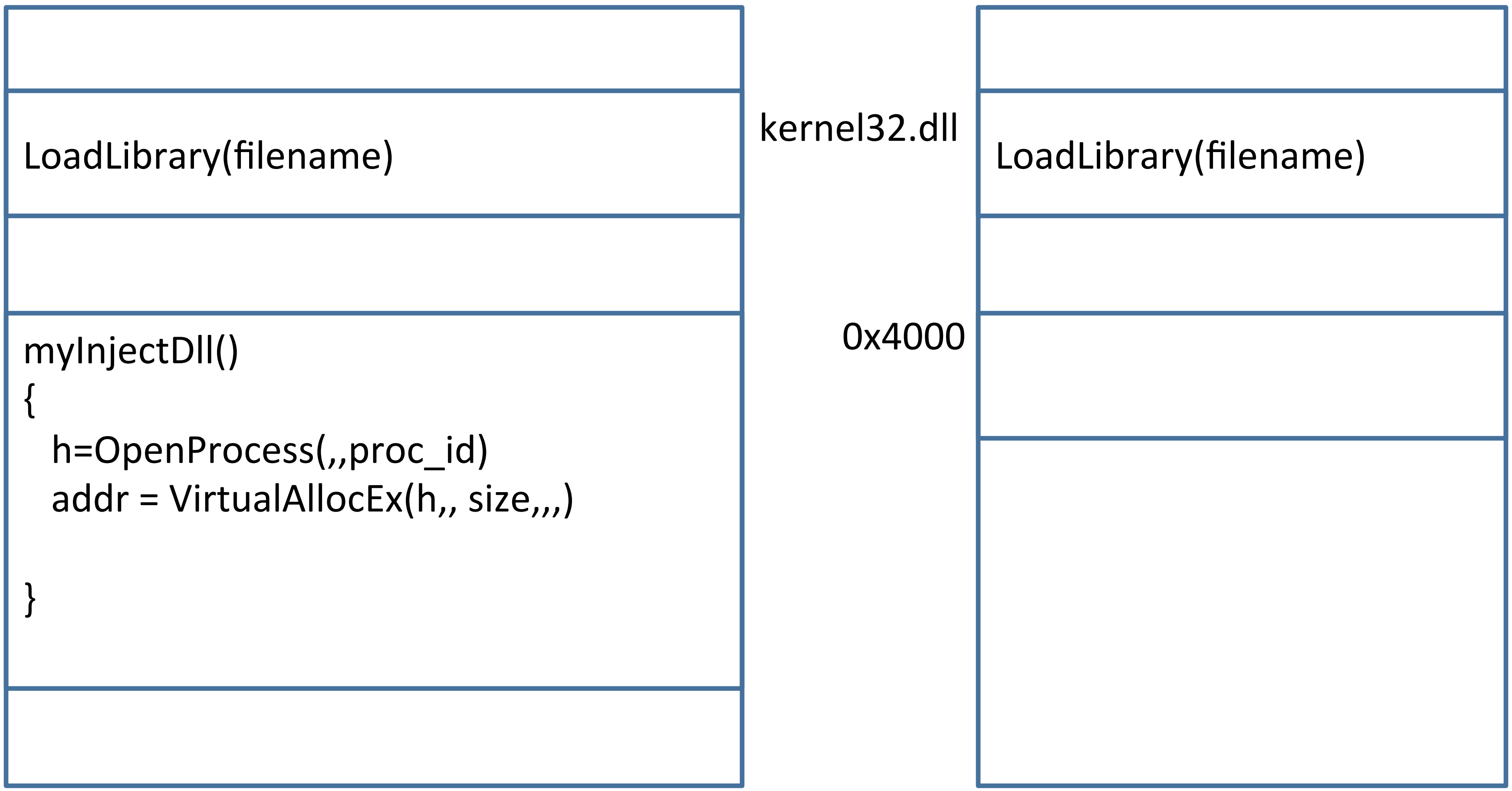
kernel32.dll

LoadLibrary(filename)

```
myInjectDll()
{
   h=OpenProcess(,,proc_id)
   addr = VirtualAllocEx(h,, size,,,)

}
```

malicious process

Internet Explorer process



LoadLibrary(filename)

```
myInjectDll()
{
   h=OpenProcess(,,proc_id)
   addr = VirtualAllocEx(h,, size,,,)

}
```

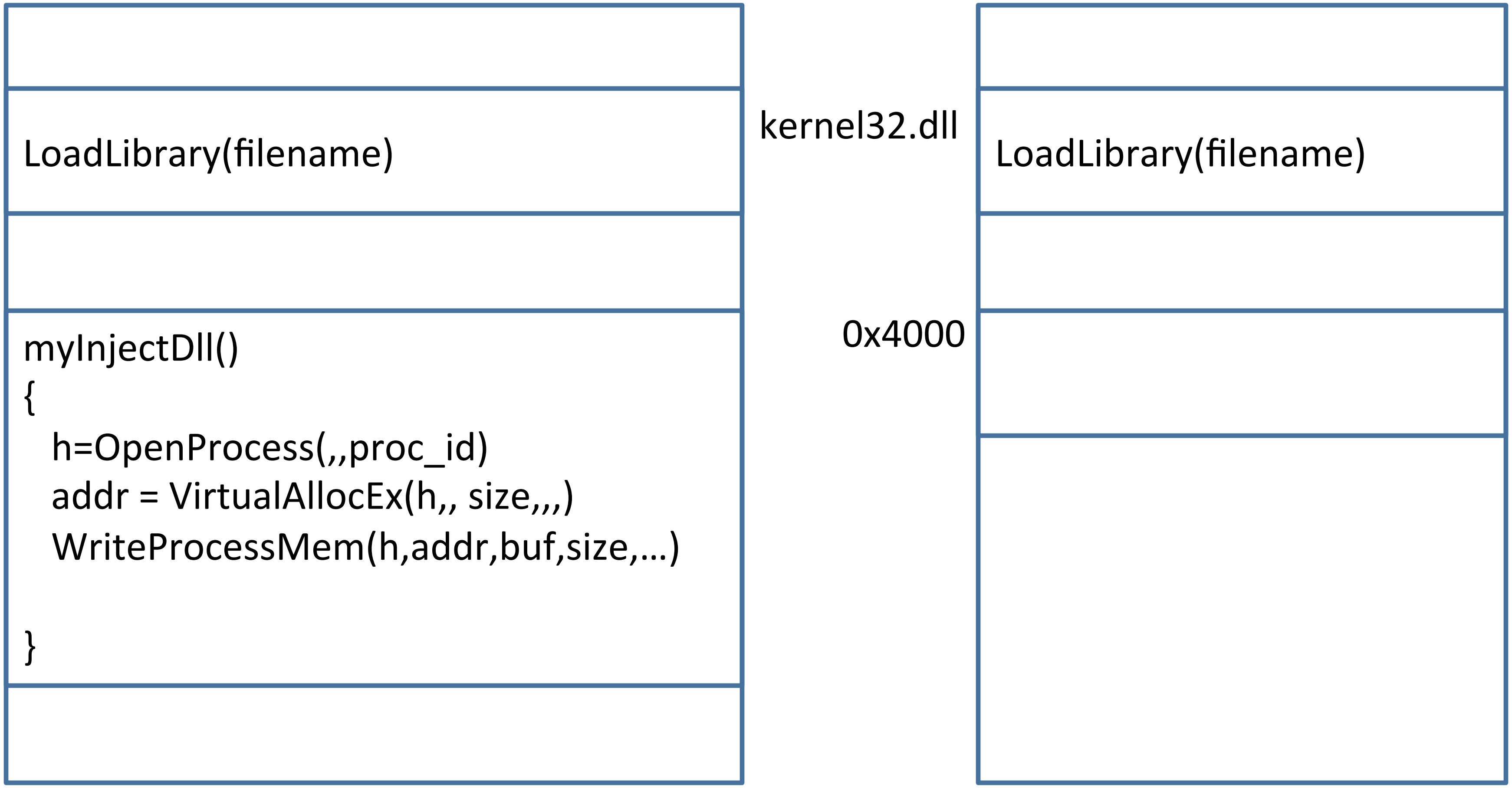
kernel32.dll

0x4000

LoadLibrary(filename)

malicious process

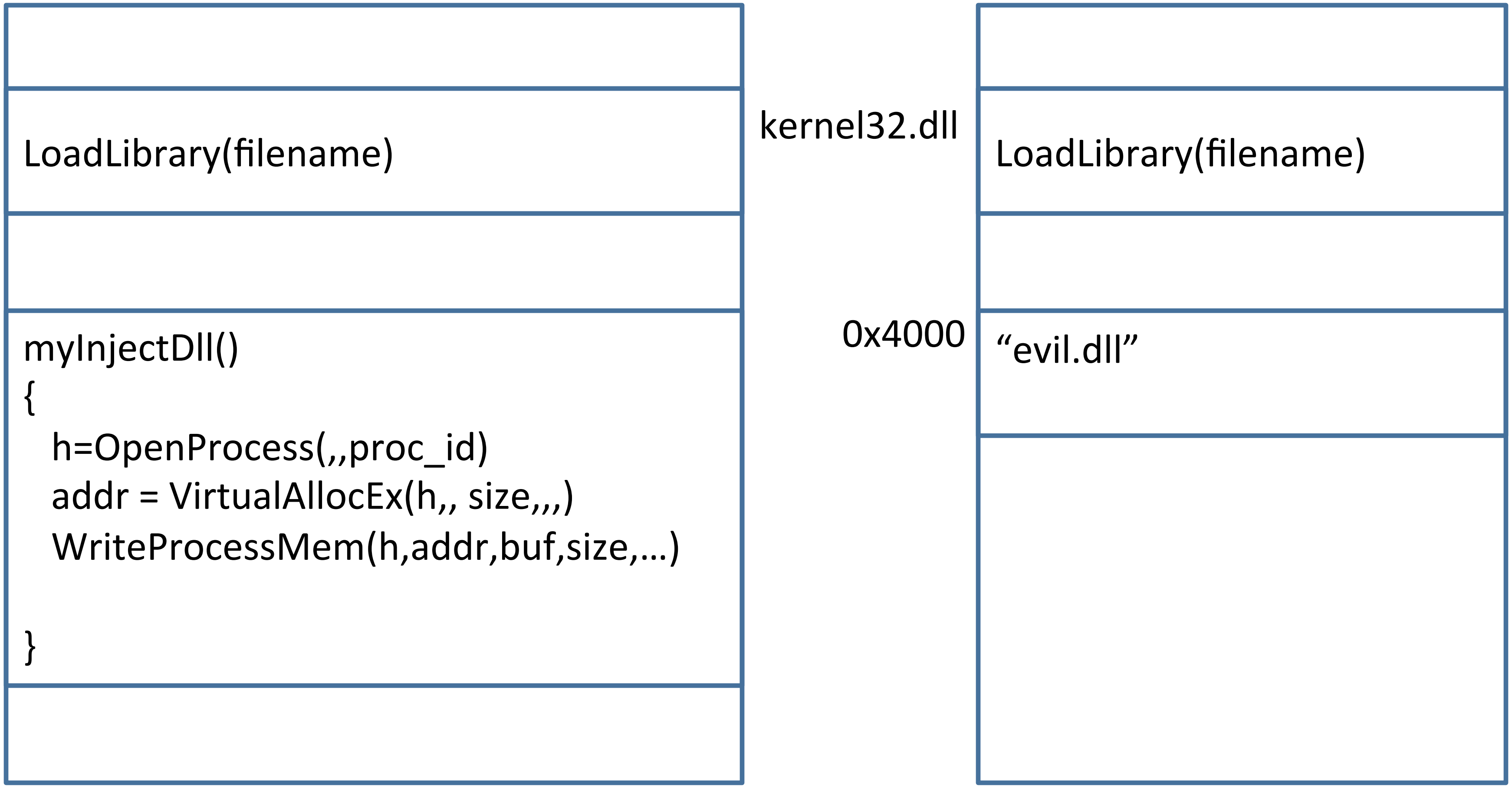
Internet Explorer process



```
myInjectDll()
{
   h=OpenProcess(,,proc_id)
   addr = VirtualAllocEx(h,, size,,,)
   WriteProcessMem(h,addr,buf,size,...)

}
```

malicious process

Internet Explorer process



LoadLibrary(filename)

```
myInjectDll()
{
  h=OpenProcess(,,proc_id)
  addr = VirtualAllocEx(h,, size,,,)
  WriteProcessMem(h,addr,buf,size,...)

}
```

kernel32.dll

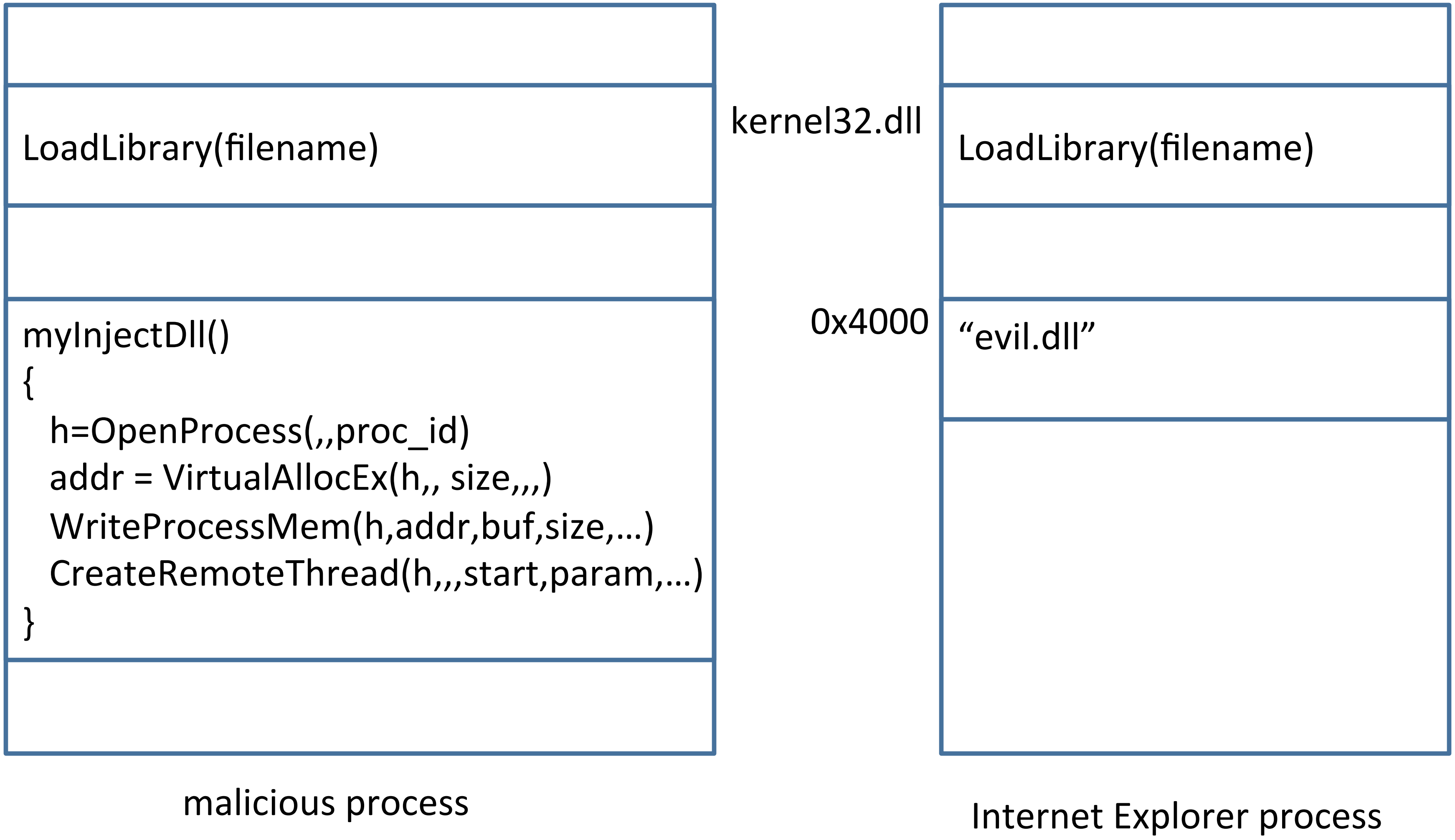
0x4000

LoadLibrary(filename)

“evil.dll”

malicious process

Internet Explorer process



kernel32.dll

LoadLibrary(filename)

```
myInjectDll()
{
  h=OpenProcess(,,proc_id)
  addr = VirtualAllocEx(h,, size,,,)
  WriteProcessMem(h,addr,buf,size,...)
  CreateRemoteThread(h,,,start,param,...)
}
```

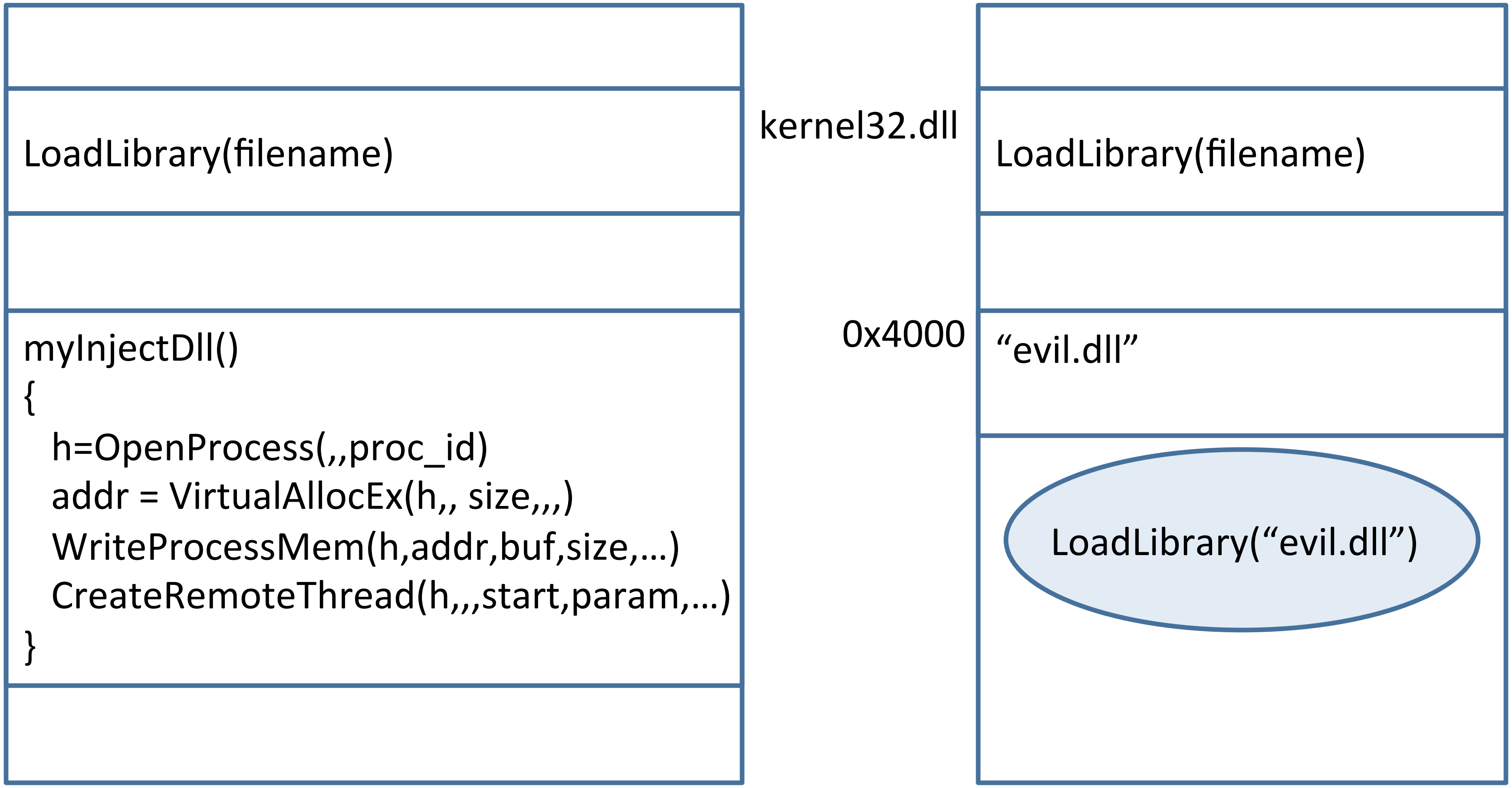
malicious process

LoadLibrary(filename)

0x4000

“evil.dll”

Internet Explorer process



LoadLibrary(filename)

kernel32.dll

```
myInjectDll()
{
  h=OpenProcess(,,proc_id)
  addr = VirtualAllocEx(h,, size,,,)
  WriteProcessMem(h,addr,buf,size,…)
  CreateRemoteThread(h,,,start,param,…)
}
```

LoadLibrary(filename)

0x4000

“evil.dll”

LoadLibrary(“evil.dll”)

malicious process

Internet Explorer process