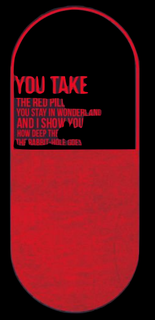
Windows OS internals, security & attack surfaces

Ganchuluun .Z
CEO @VKNC LLC

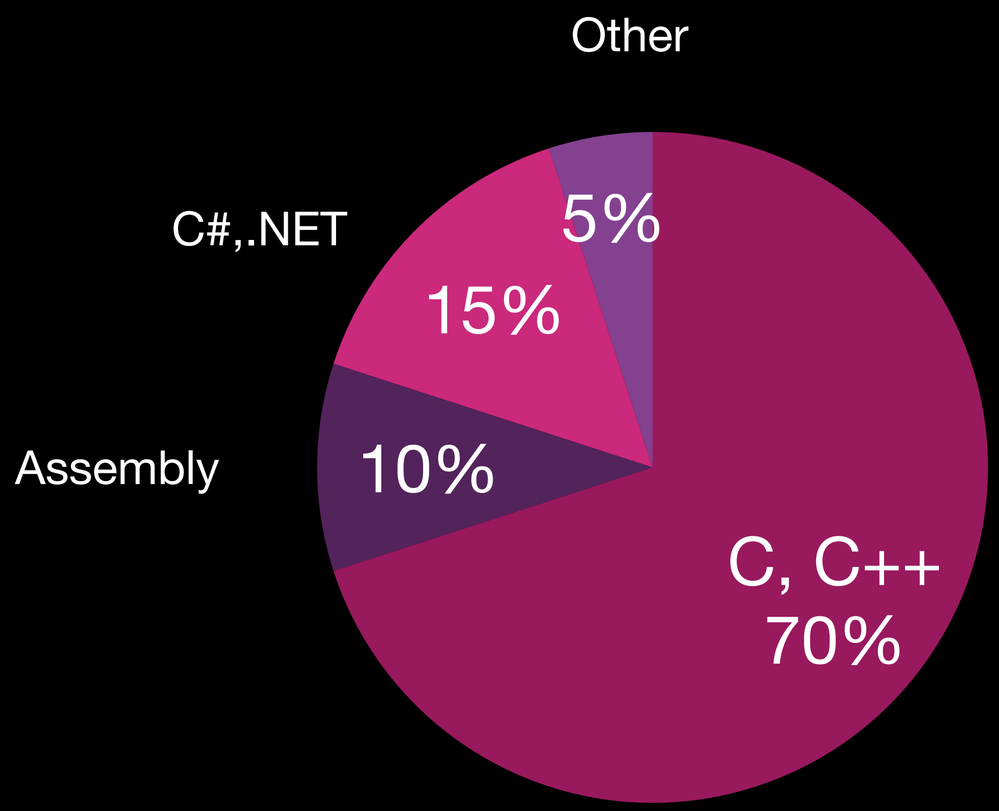


Is it really secure?

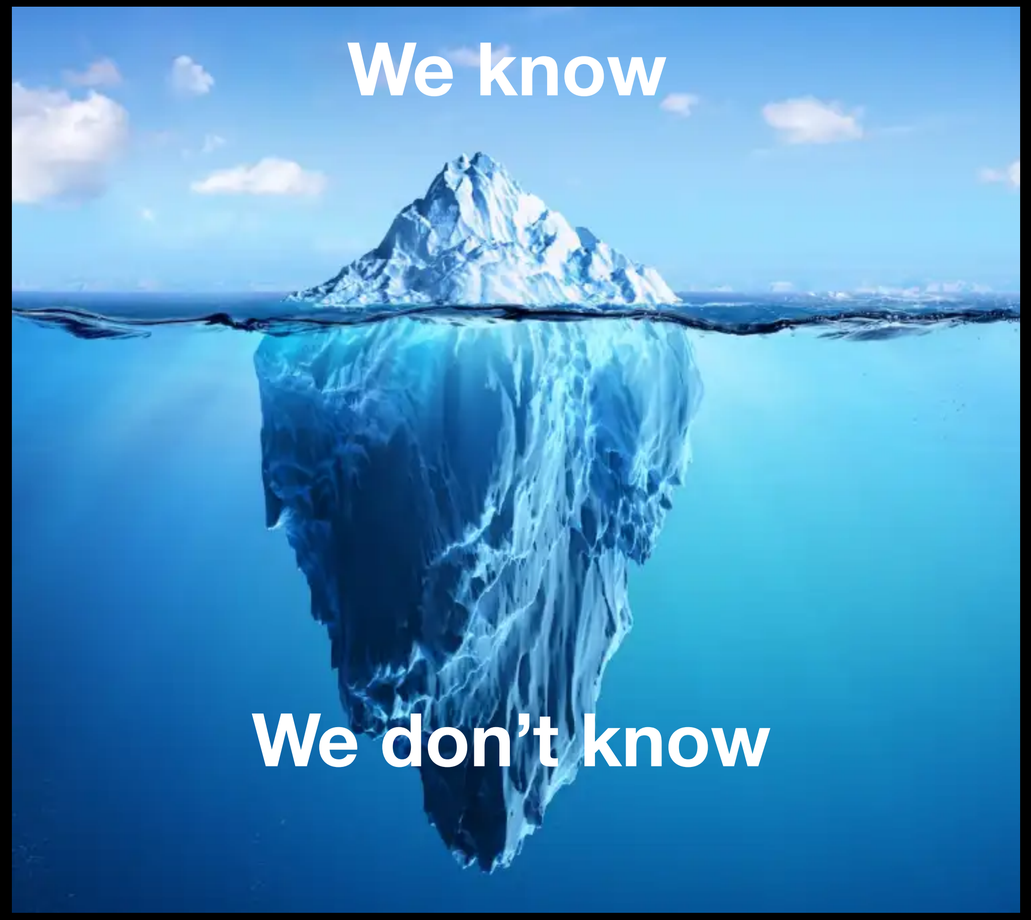
Is it really vulnerable?

*“I'm trying to free your mind, Neo. But I can only show you the door. You're **The One** that has to walk through it”*
The Matrix 1999

Written languages



Closed source code???



Closed source code???

Microsoft

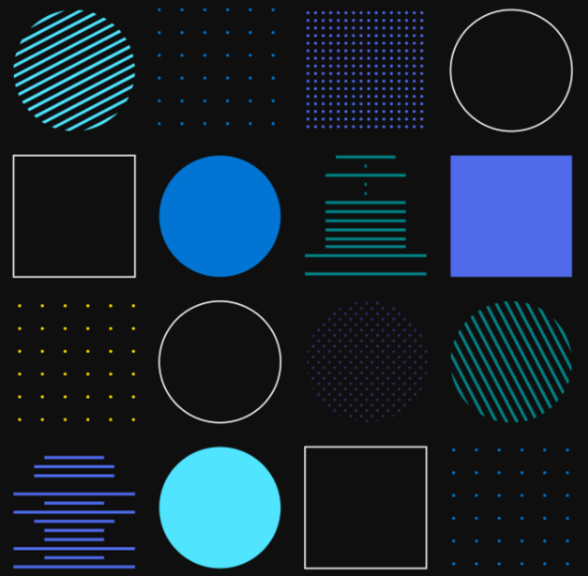
Open source projects and samples from Microsoft

Verified

75.3k followers | Redmond, WA | https://opensource.microsoft.com | @OpenAtMicrosoft

README.md

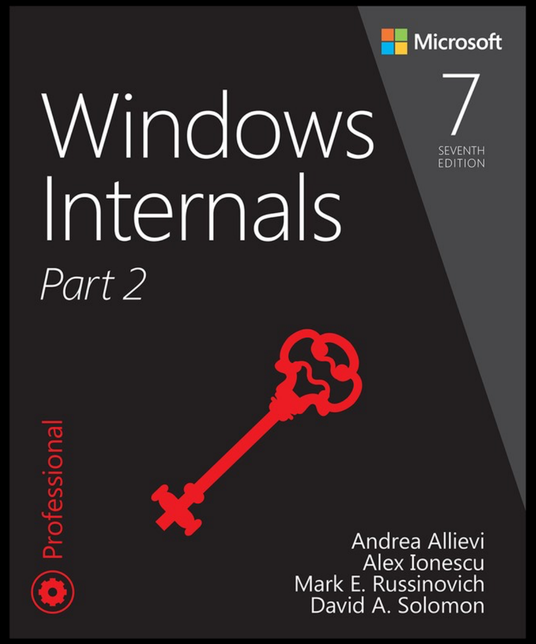
Open.
Collaborative.
Flexible.

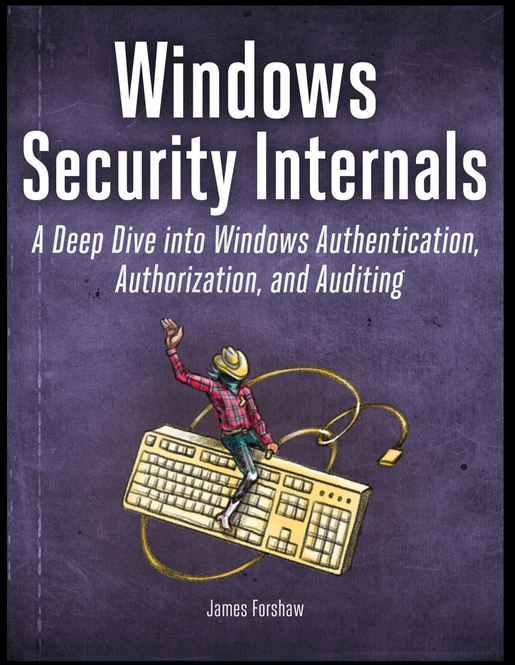


Open Source enables Microsoft products and services to bring choice, technology and community to our customers.

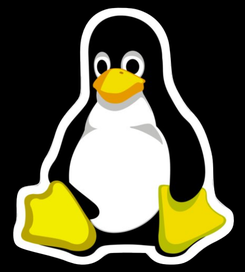
Resources

- learn.microsoft.com
- Books
- Training courses
- Official documents
- Leaked codes
- Blog posts of security researchers
- Alex Ionescu - Reversing without reversing

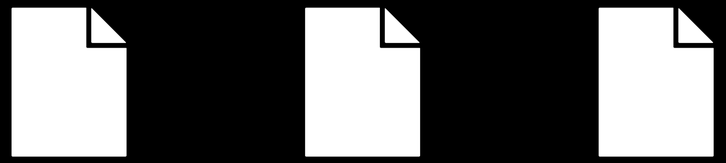


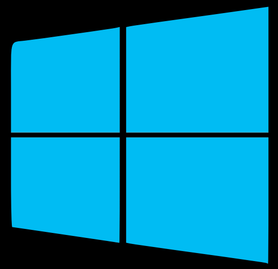


Compared to *nix

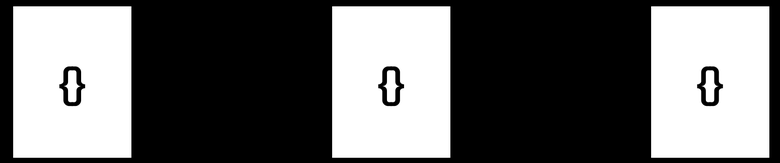


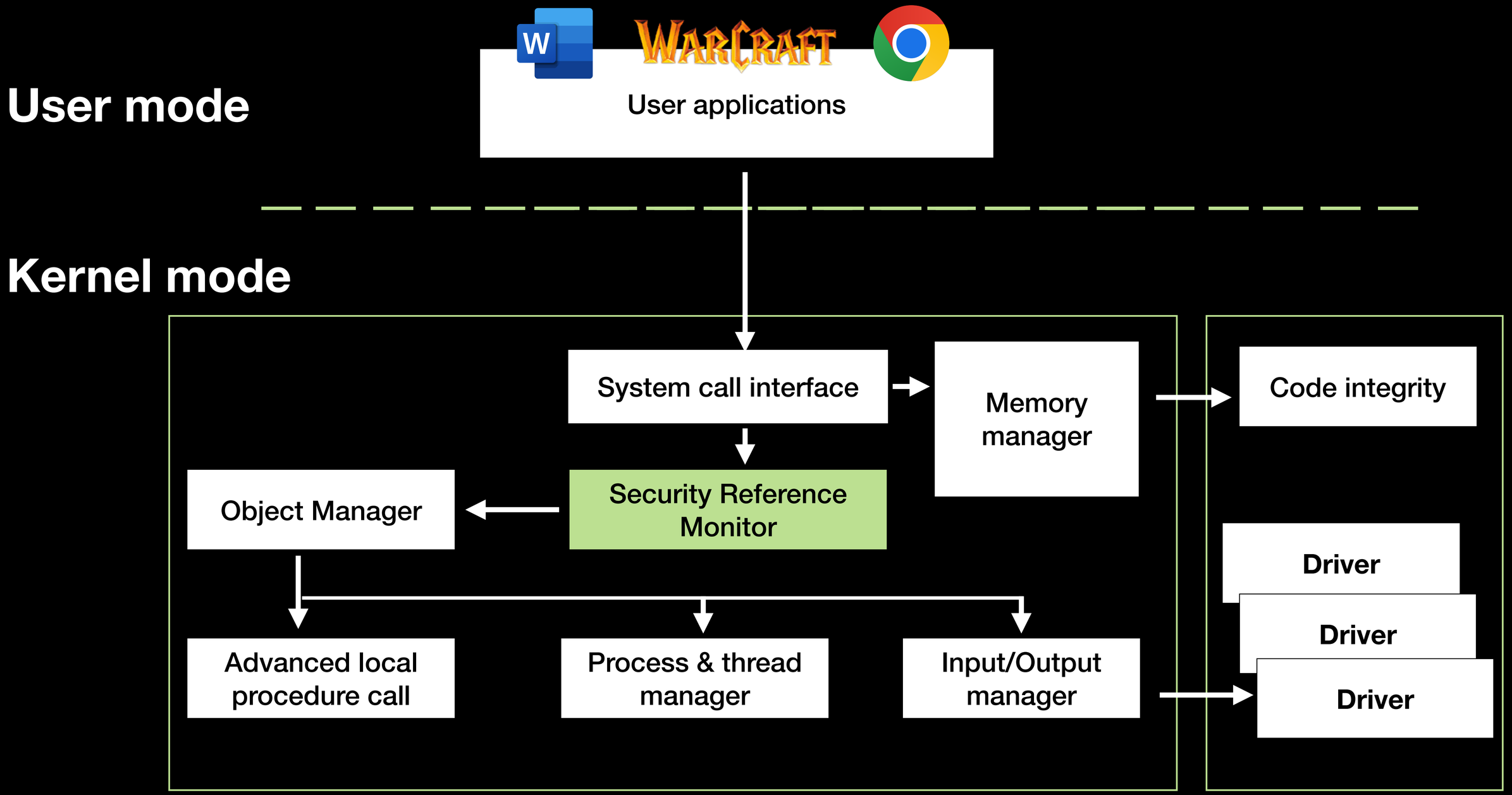
Everything is FILE



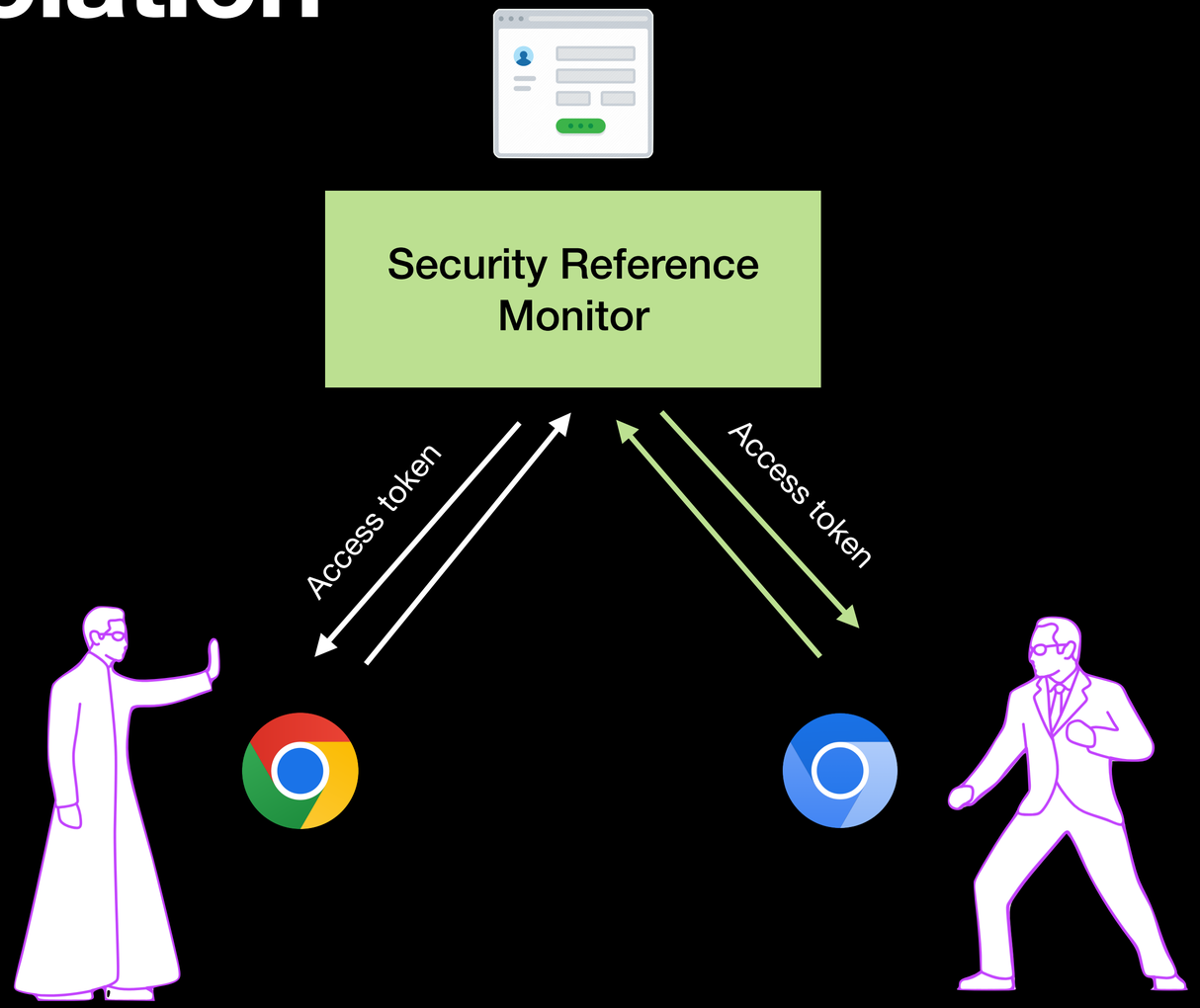


Everything is OBJECT

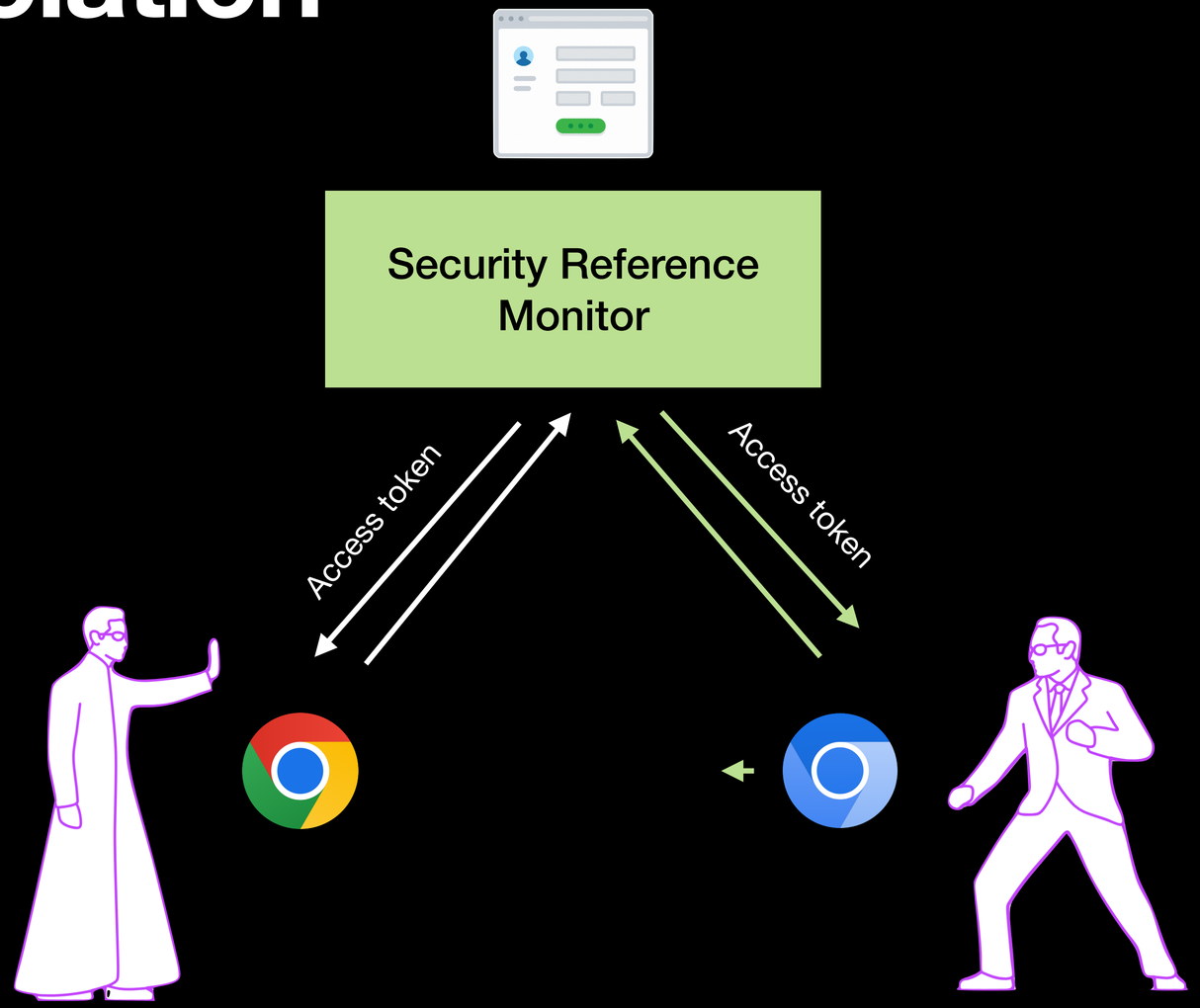



User mode
User applications
Kernel mode
System call interface
Memory manager
Code integrity
Security Reference Monitor
Object Manager
Driver
Driver
Driver
Advanced local procedure call
Process & thread manager
Input/Output manager

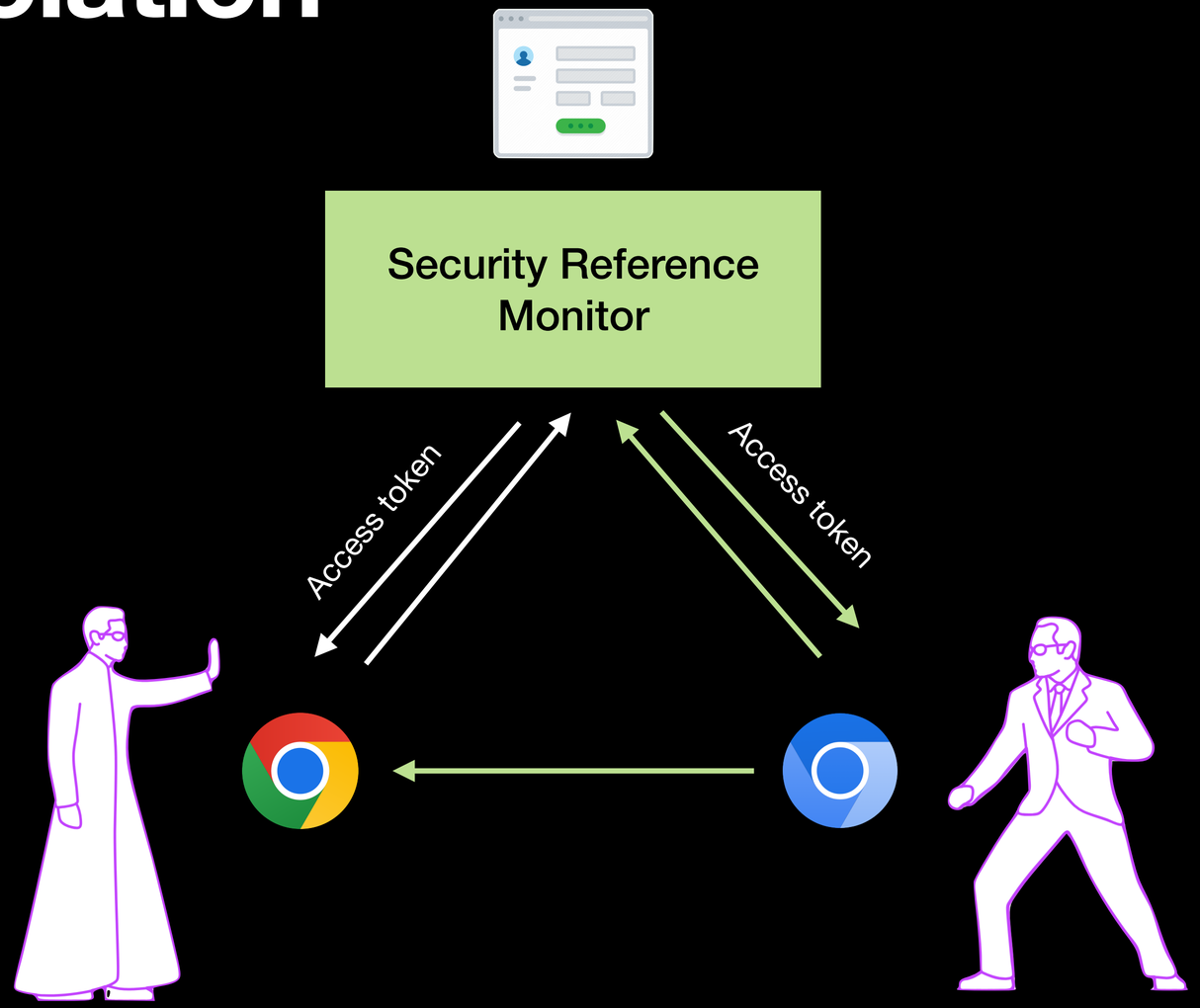
Process Isolation



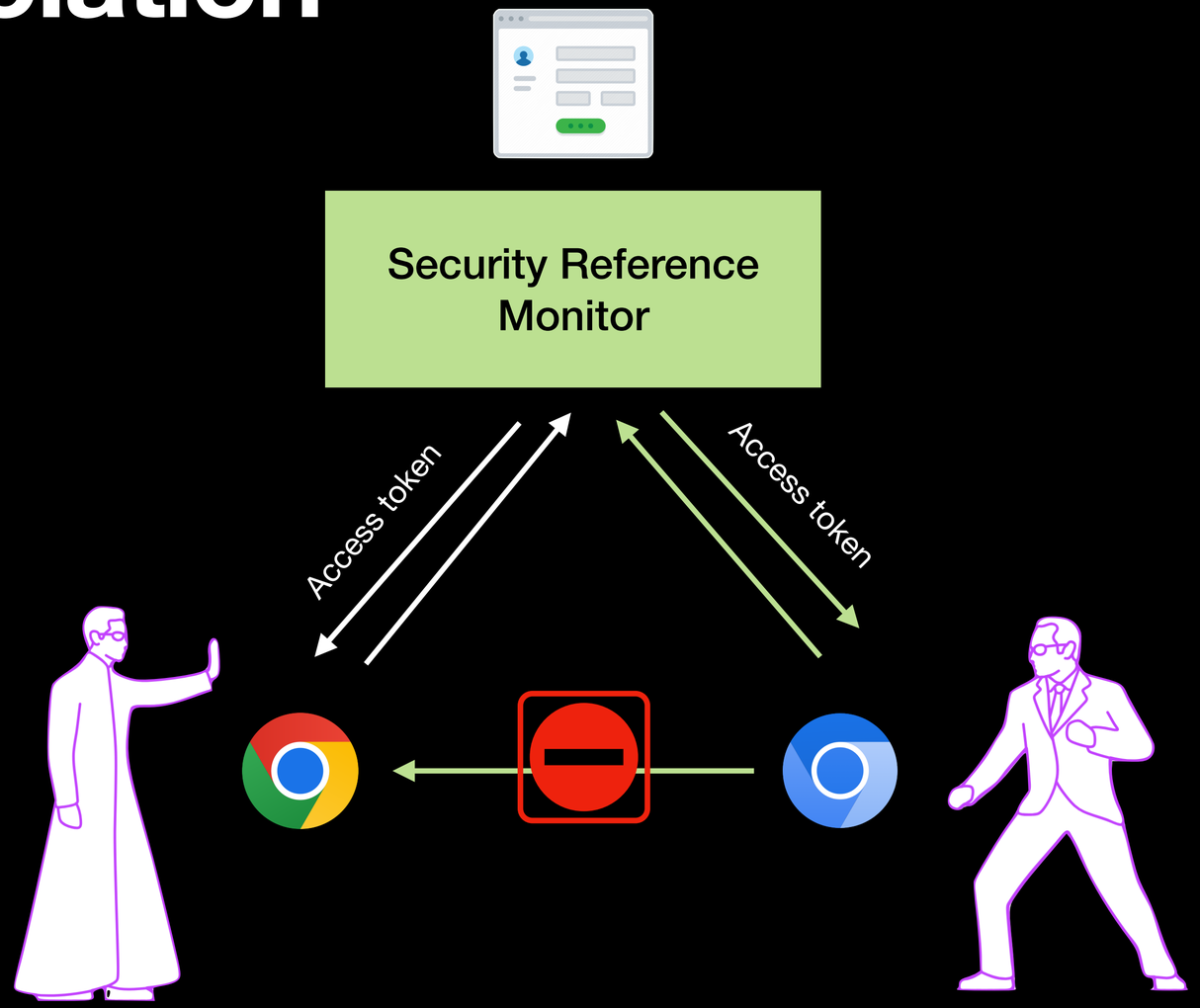
Process Isolation



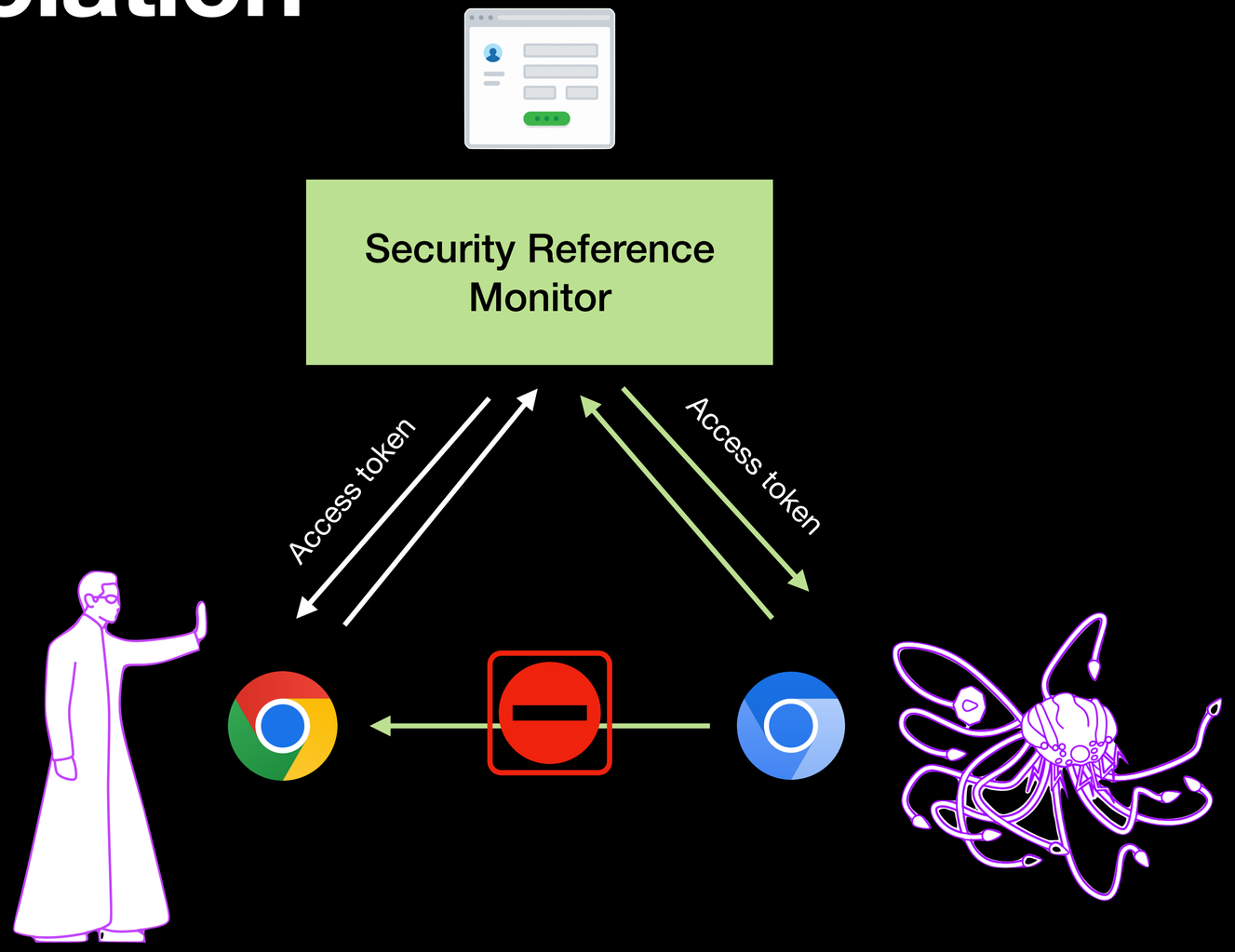
Process Isolation

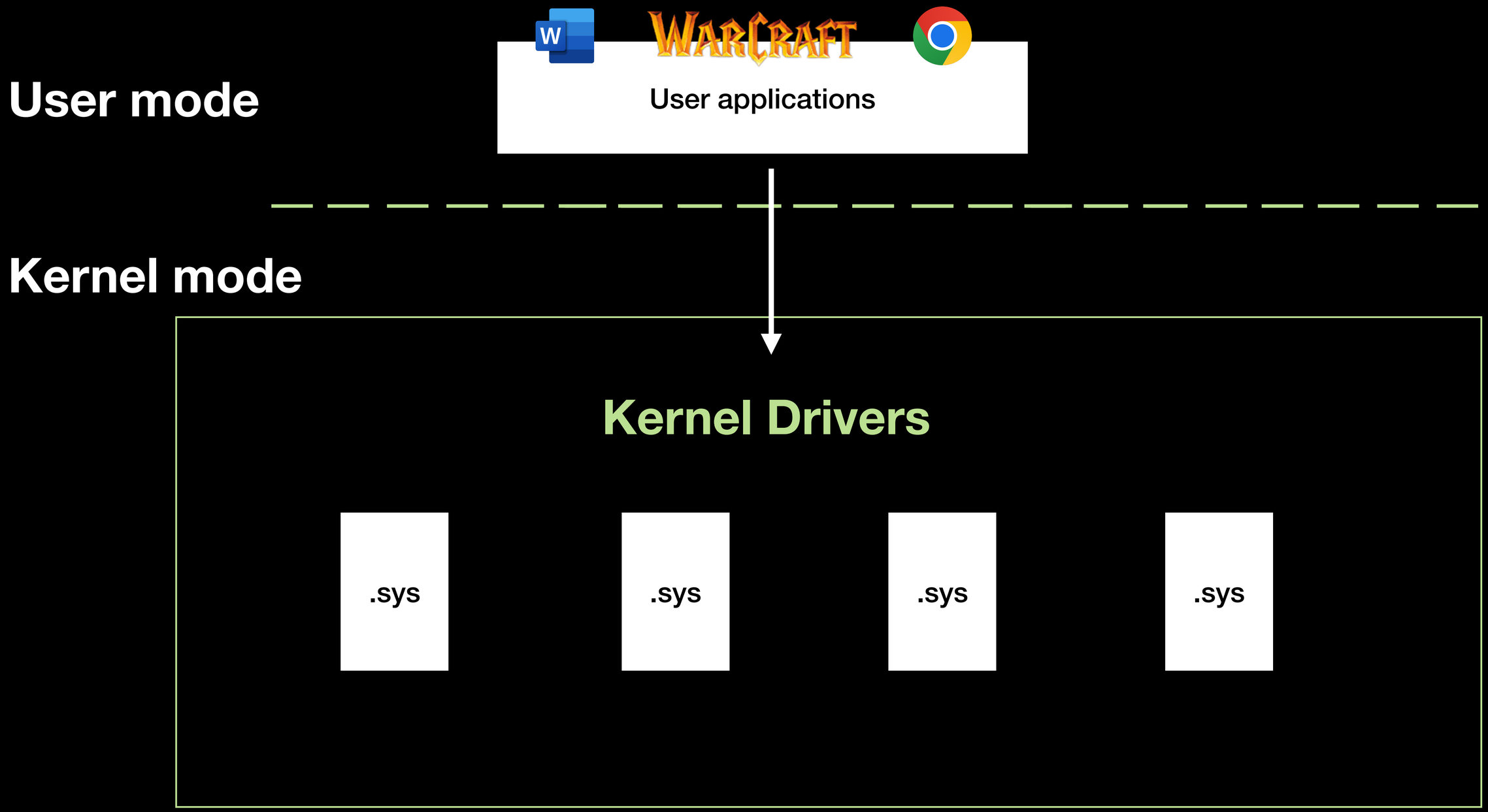


Process Isolation



Process Isolation




User mode
WARCRAFT
User applications
Kernel mode
Kernel Drivers
.sys
.sys
.sys
.sys

User mode

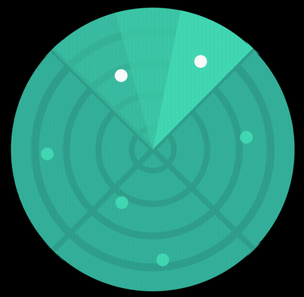
Kernel mode

Kernel Drivers

User mode

Kernel mode

Kernel Drivers



ETW - Event Tracing for Windows

User mode

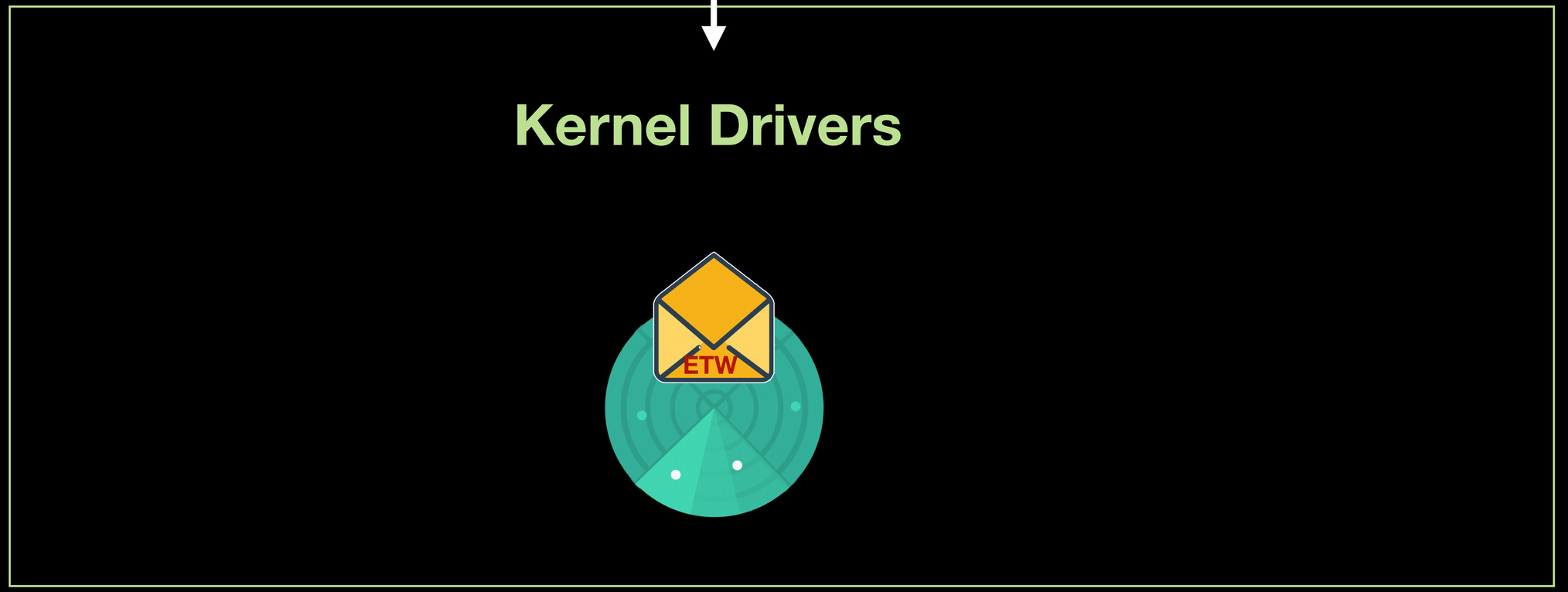
Kernel mode

Kernel Drivers

ETW - Event Tracing for Windows

User mode

Kernel mode

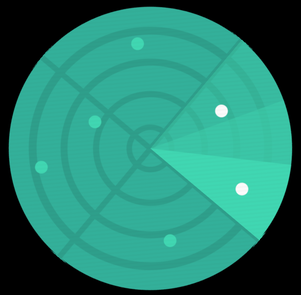


ETW - Event Tracing for Windows

User mode

Kernel mode

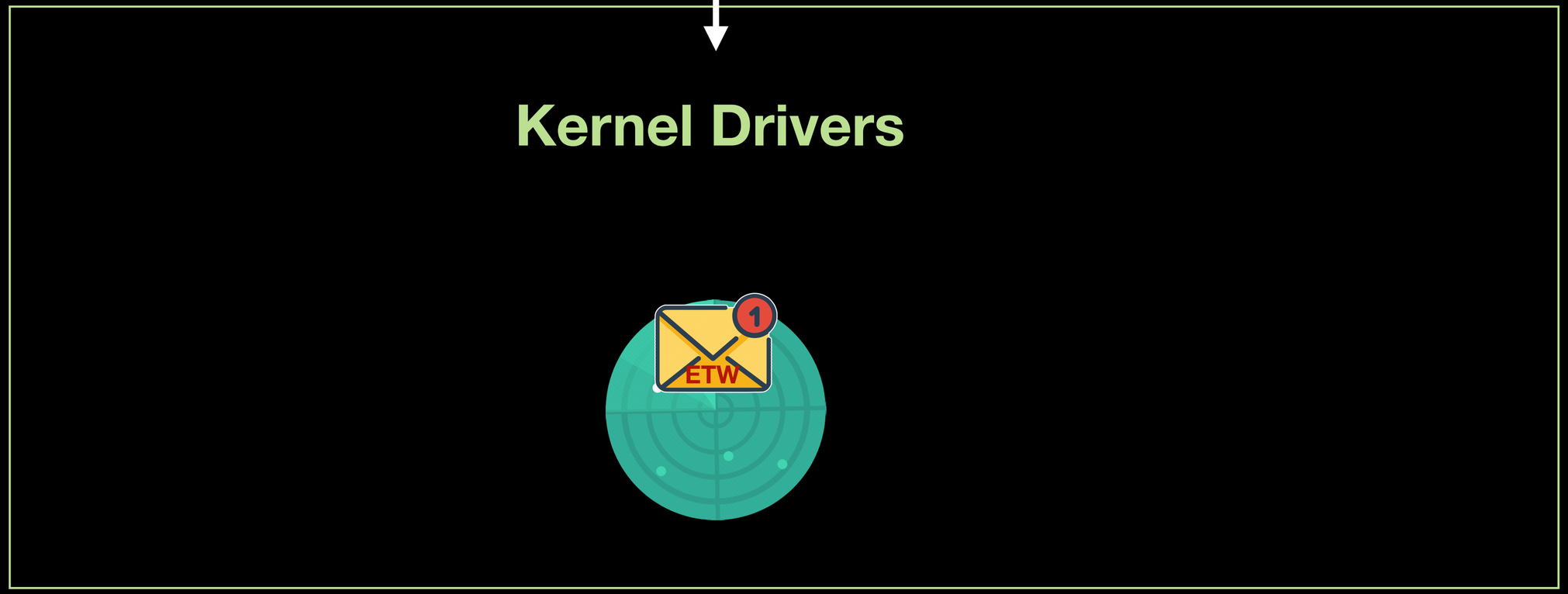
Kernel Drivers



ETW - Event Tracing for Windows

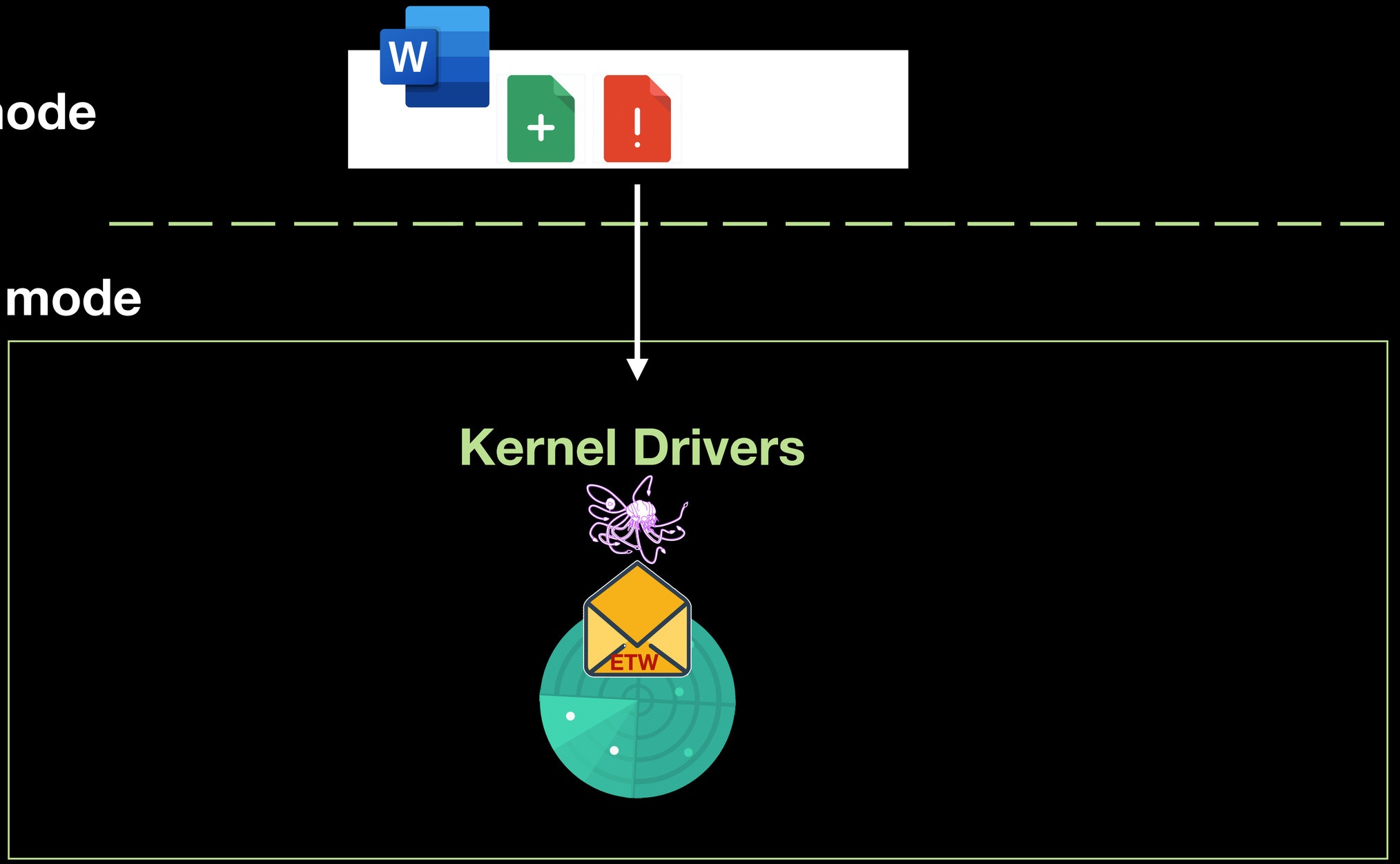
User mode

Kernel mode

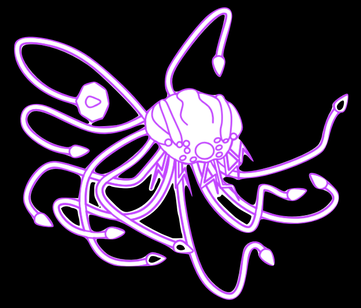


User mode

Kernel mode



User mode



Kernel mode

Kernel Drivers

User mode

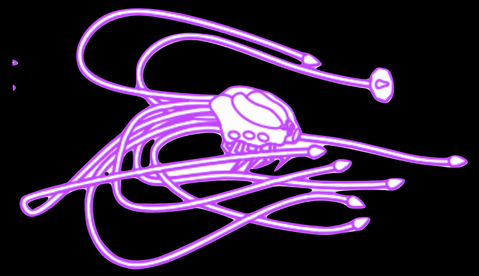
Kernel mode

Kernel Drivers

User mode

Kernel mode

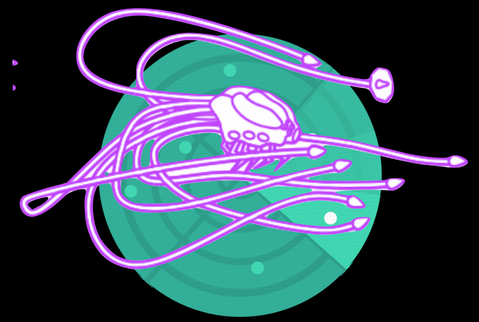
Kernel Drivers



User mode

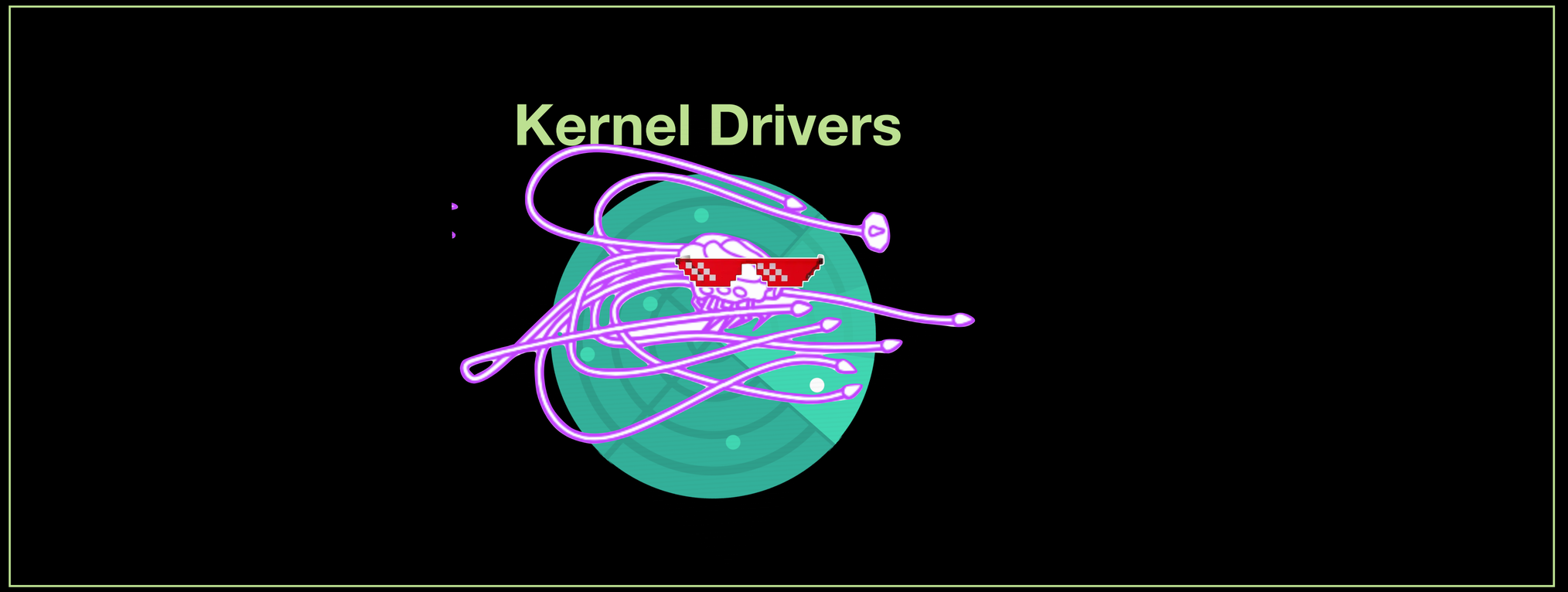
Kernel mode

Kernel Drivers



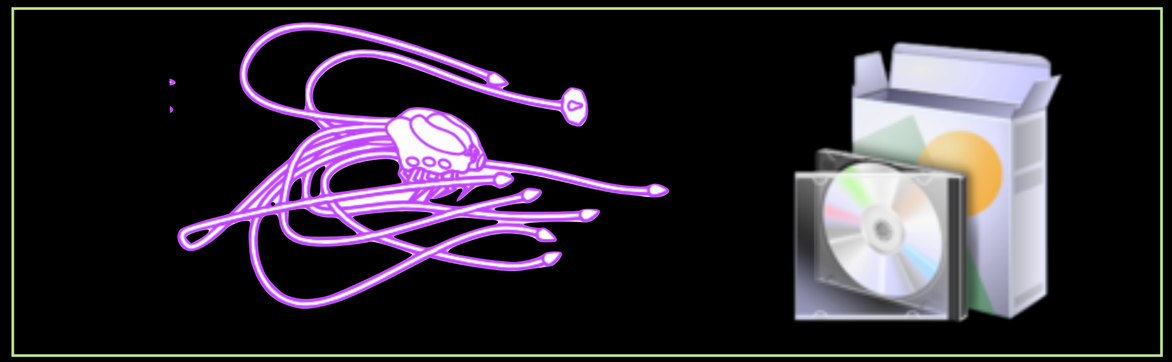
User mode

Kernel mode



Bring Your Own Vulnerable Driver

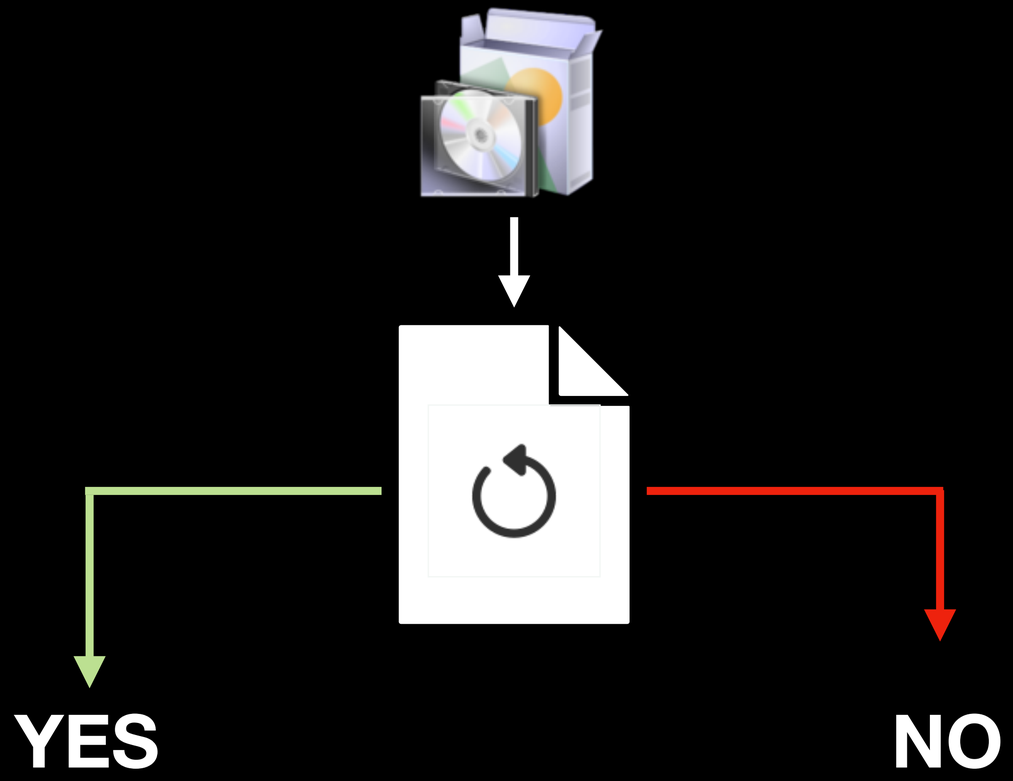
User mode



Kernel mode

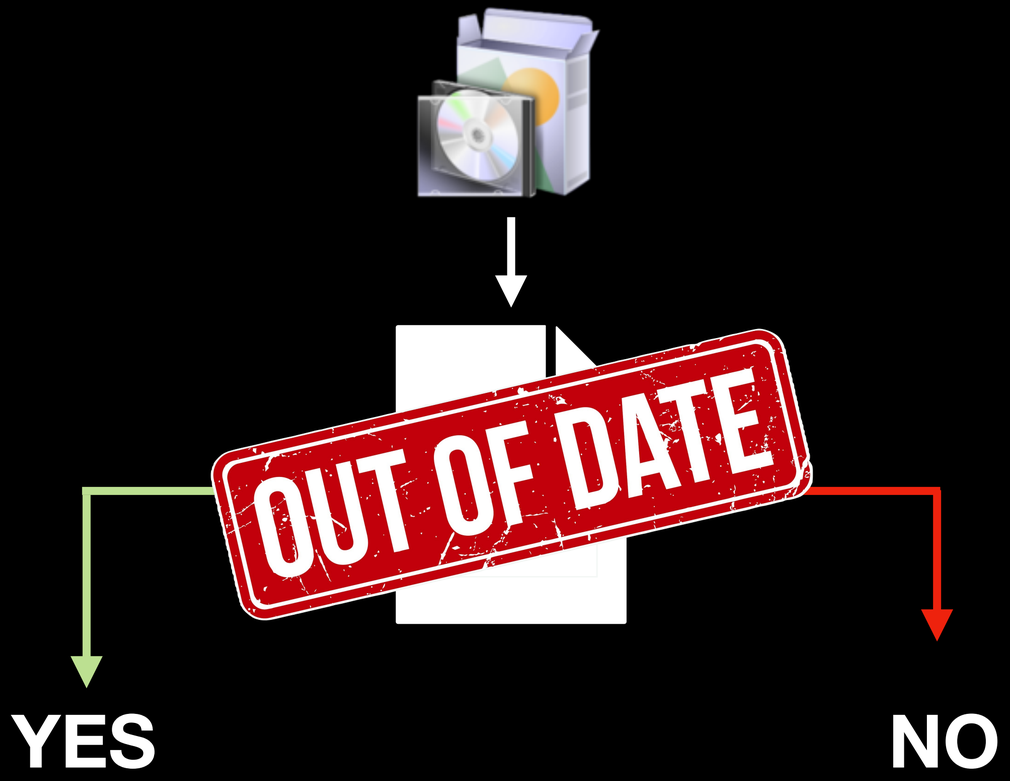
HVCI Blocklist

Block list of vulnerable drivers



HVCI Blocklist

Block list of vulnerable drivers



Intel CET

```
func (){
    a = 1 + 1;
    anotherFunc();
    b = 2 - 1;
}
```

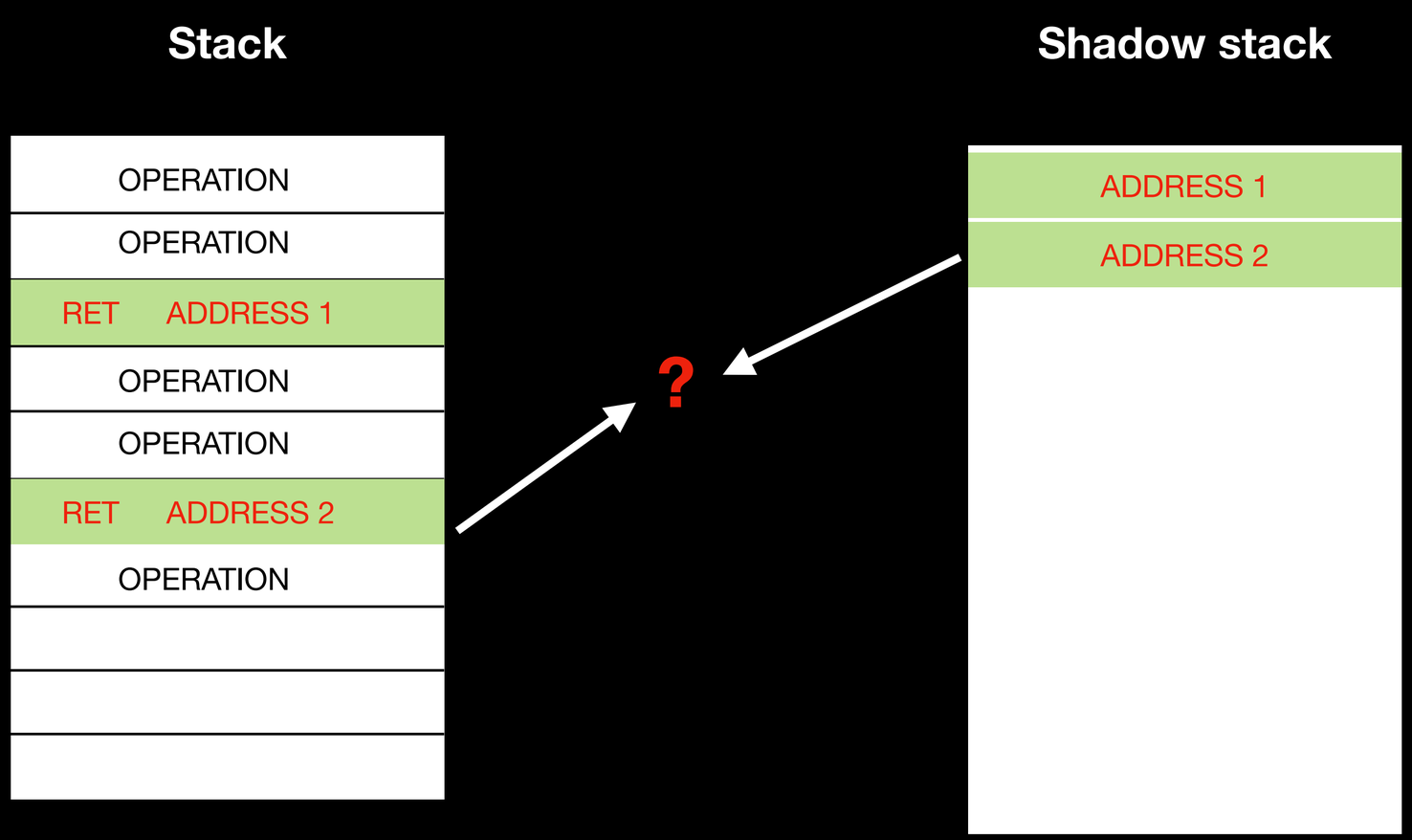
CET - Control-flow Enforcement Technology

Intel CET

70% of all security bugs are memory safety issues
Because of C, C++

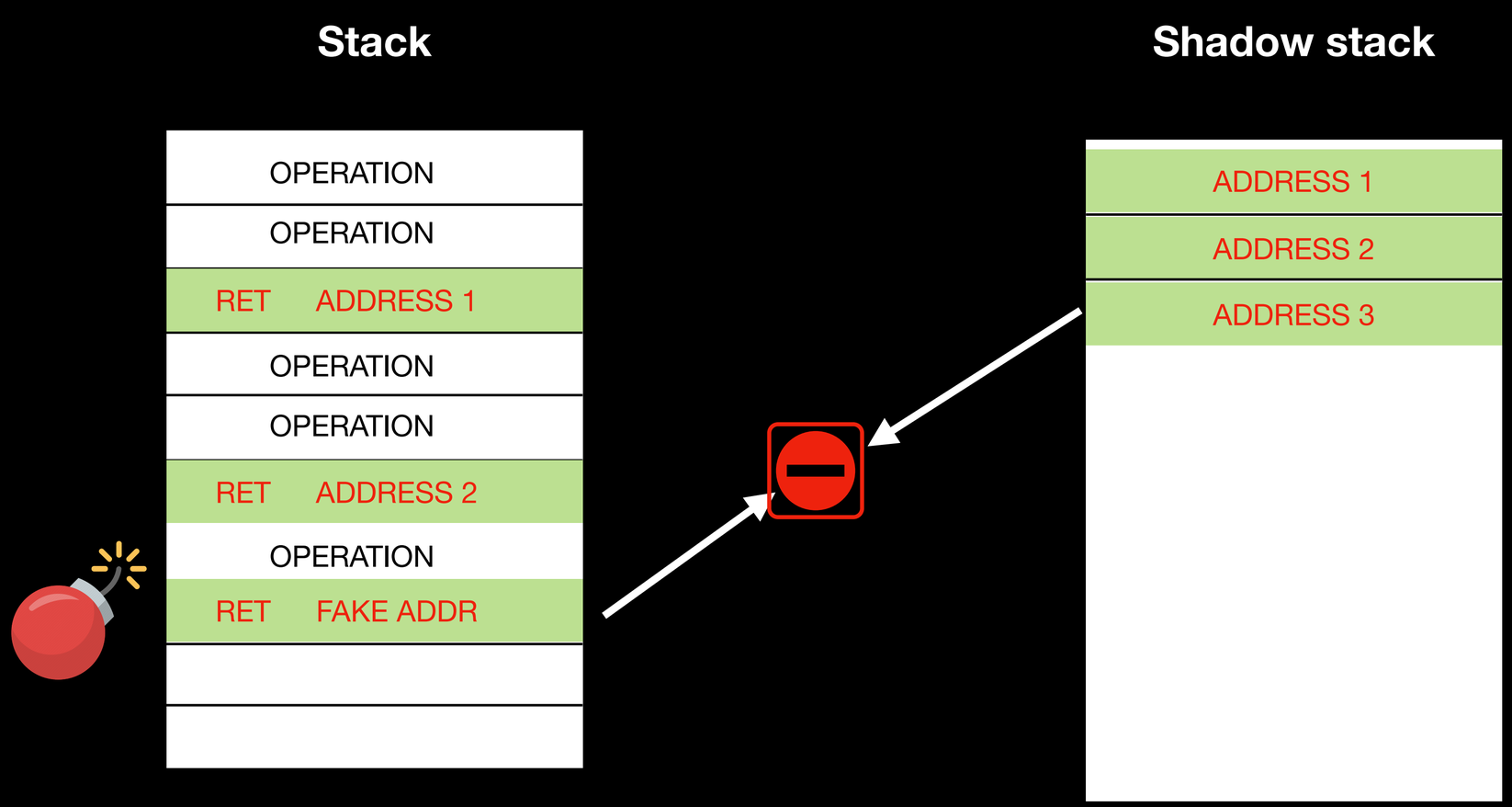
CET - Control-flow Enforcement Technology

Intel CET



CET - Control-flow Enforcement Technology

Intel CET



CET - Control-flow Enforcement Technology

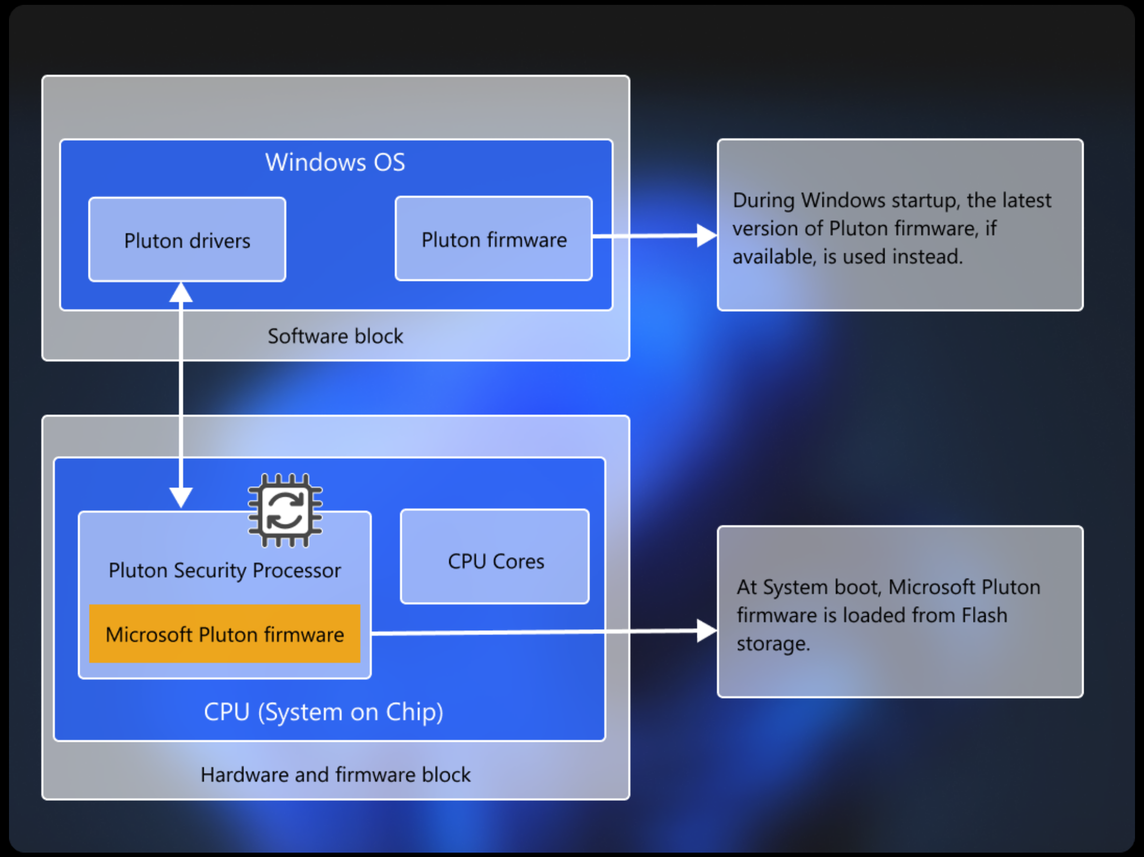
Intel CET

- Developers still not aware about CET
- Misuse

CET - Control-flow Enforcement Technology

Root of Trust

Pluton security processor



Wake up, Neo...