



Kernel Hijacking Is Not an Option: MemoryRanger Comes to the Rescue Again

Igor Korkin

Independent Researcher

HITB **LOCKDOWN** **002**
livestream
2020

WHOAMI

- PhD, speaker at the ADFSL conference since 2014 and the BlackHat
- Windows OS Kernel Security Researcher:
 - Rootkits and anti-rootkits
 - Bare-Metal Hypervisors vs. Attacks on Kernel Memory
- Fan of cross-disciplinary research — igorkorkin.blogspot.com
- Love traveling and powerlifting —  [igor.korkin](https://www.instagram.com/igor.korkin)

AGENDA: ATTACKS ON FILES

- Three attacks on kernel memory data:

Bypass file sharing access control:



1. Handle Table Hijacking
2. Hijacking NTFS structures

AGENDA: ATTACKS ON FILES+TOKENS

- Three attacks on kernel memory data:

Bypass file sharing access control:



1. Handle Table Hijacking
2. Hijacking NTFS structures

Process Privilege Escalation:



3. Token Hijacking

AGENDA: ATTACKS ON FILES+TOKENS & MEMORYRANGER

- Three attacks on kernel memory data:

Bypass file sharing access control:



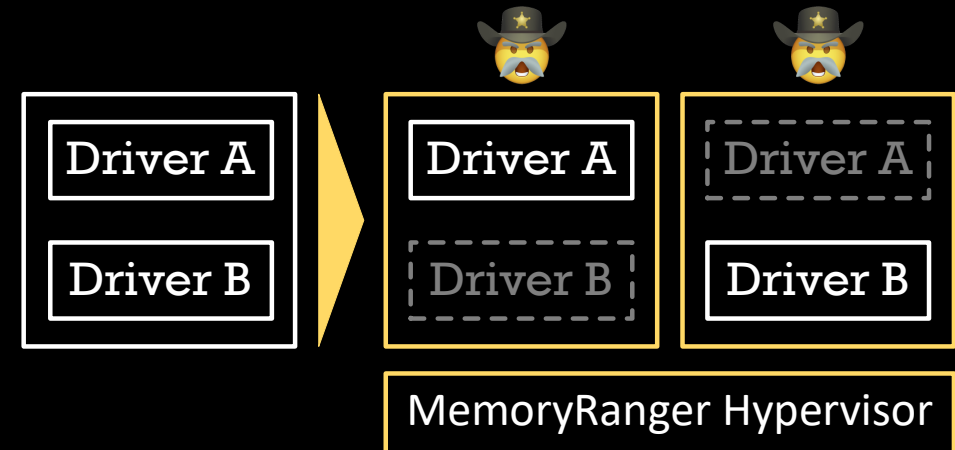
1. Handle Table Hijacking
2. Hijacking NTFS structures

Process Privilege Escalation:

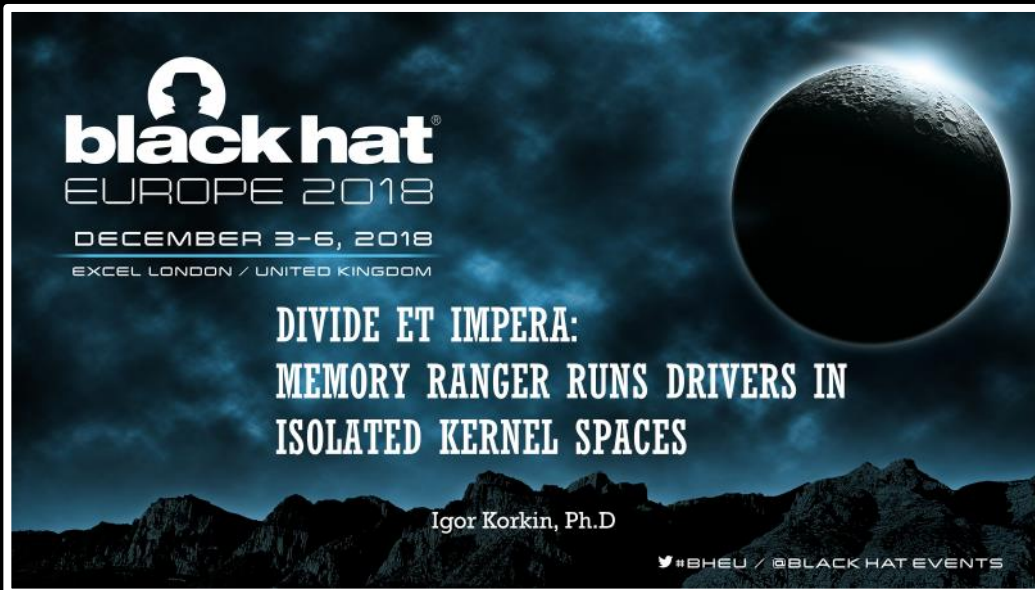


3. Token Hijacking

- MemoryRanger blocks kernel attacks:
 - It runs drivers in isolated kernel enclaves
 - It includes a new feature: Data-Only Enclave

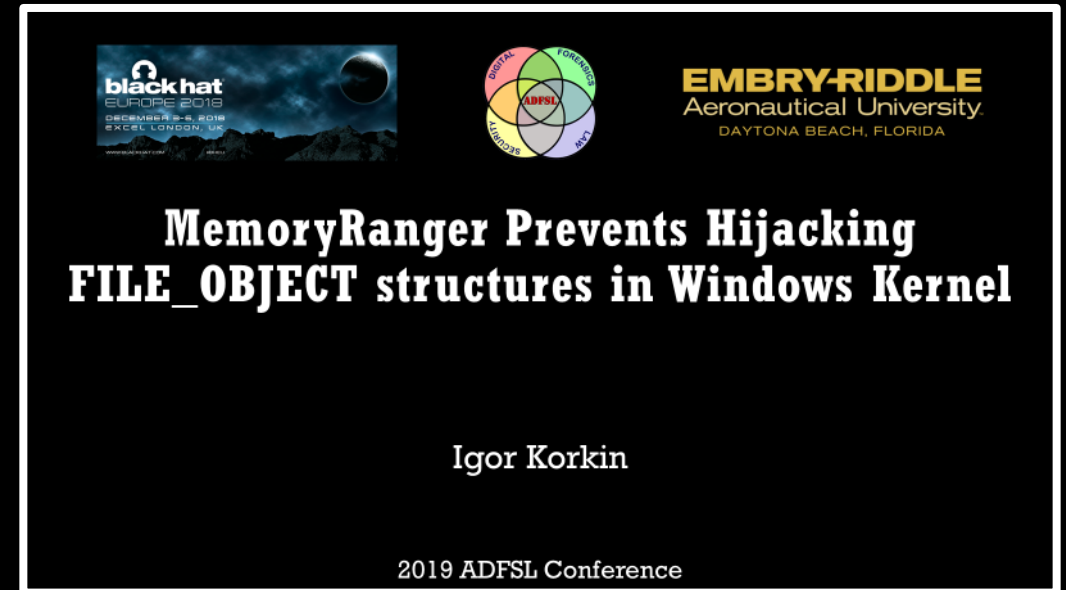


PREVIOUS RESEARCH ON MEMORYRANGER: PAPERS+SLIDES+DEMOS



(2018) Divide et Impera: MemoryRanger
Runs Drivers in Isolated Kernel Spaces

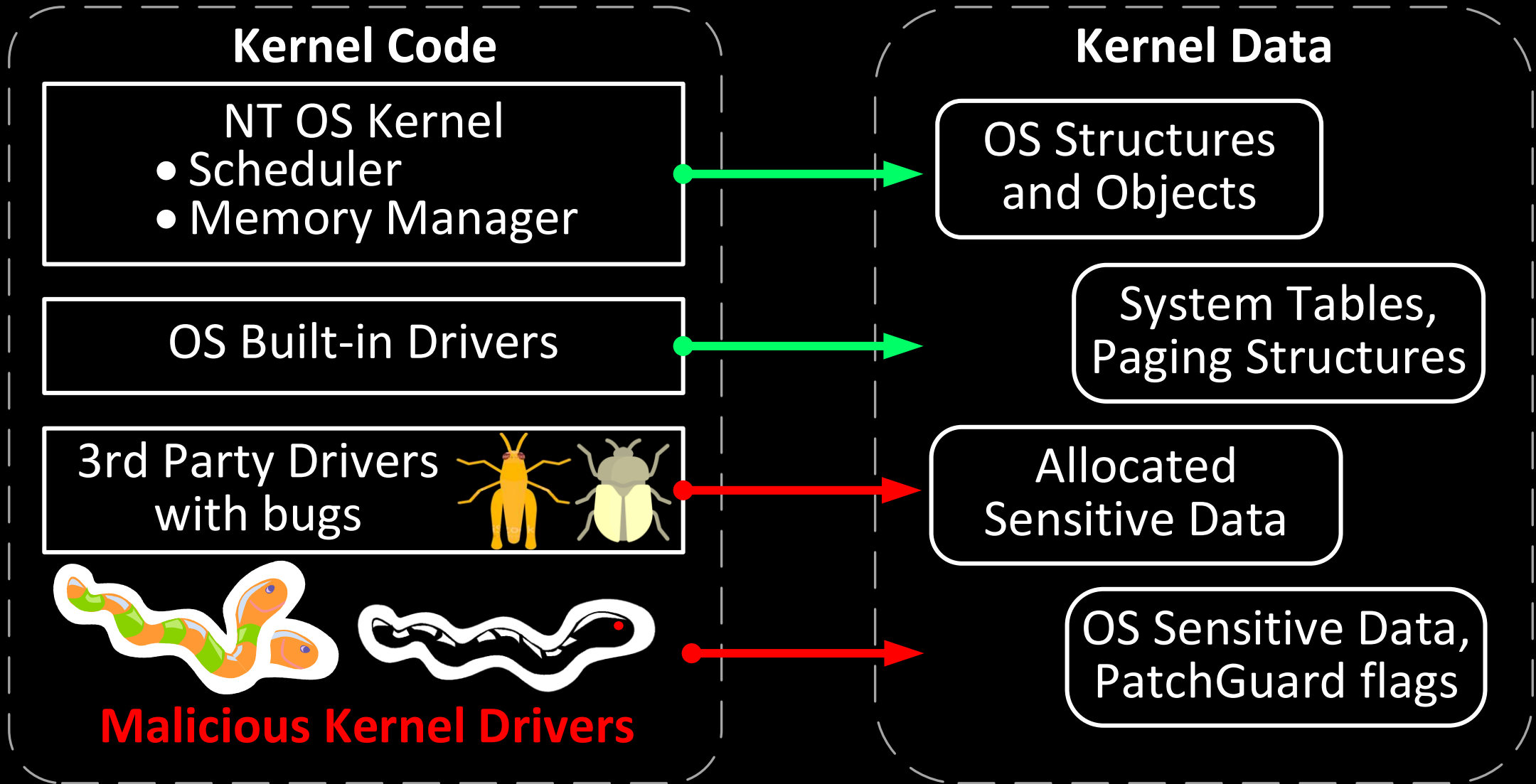
<https://igorkorkin.blogspot.com/2018/12/divide-et-impera-memoryranger-runs.html>



(2019) MemoryRanger Prevents Hijacking
FILE_OBJECT Structures in Windows Kernel

<https://igorkorkin.blogspot.com/2019/04/memoryranger-prevents-hijacking.html>

KERNEL DRIVERS CAN COMPROMISE THE OS SECURITY



KERNEL DRIVERS IN RECENT MALWARE ATTACKS ON WINDOWS

- RobbinHood Ransomware - 2020
 - Exploits a legitimate buggy driver to load a malware driver
 - Malware driver disables endpoint security products

1. Ransomware installs Gigabyte driver to kill antivirus products - <https://www.zdnet.com/article/ransomware-installs-gigabyte-driver-to-kill-antivirus-products/>
2. Nansh0u Miner Attack Infects 50K MS-SQL, PHPMyAdmin Servers - <https://www.guardicore.com/2019/05/nansh0u-campaign-hackers-arsenal-grows-stronger/>
3. Glupteba: Hidden Malware Delivery in Plain Sight - https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final.pdf

KERNEL DRIVERS IN RECENT MALWARE ATTACKS ON WINDOWS

- RobbinHood Ransomware - 2020

- Exploits a legitimate buggy driver to load a malware driver
- Malware driver disables endpoint security products

- Crypto-miner with a signed driver - 2019

- Infected more than 50,000 Windows machines in the world
- Uses a signed malware driver to protect itself from termination

1. Ransomware installs Gigabyte driver to kill antivirus products - <https://www.zdnet.com/article/ransomware-installs-gigabyte-driver-to-kill-antivirus-products/>
2. Nansh0u Miner Attack Infects 50K MS-SQL, PHPMyAdmin Servers - <https://www.guardicore.com/2019/05/nansh0u-campaign-hackers-arsenal-grows-stronger/>
3. Glupteba: Hidden Malware Delivery in Plain Sight - https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final.pdf

KERNEL DRIVERS IN RECENT MALWARE ATTACKS ON WINDOWS

- RobbinHood Ransomware - 2020

- Exploits a legitimate buggy driver to load a malware driver
- Malware driver disables endpoint security products

- Crypto-miner with a signed driver - 2019

- Infected more than 50,000 Windows machines in the world
- Uses a signed malware driver to protect itself from termination

- Glupteba includes rootkit to hide files and processes - 2020

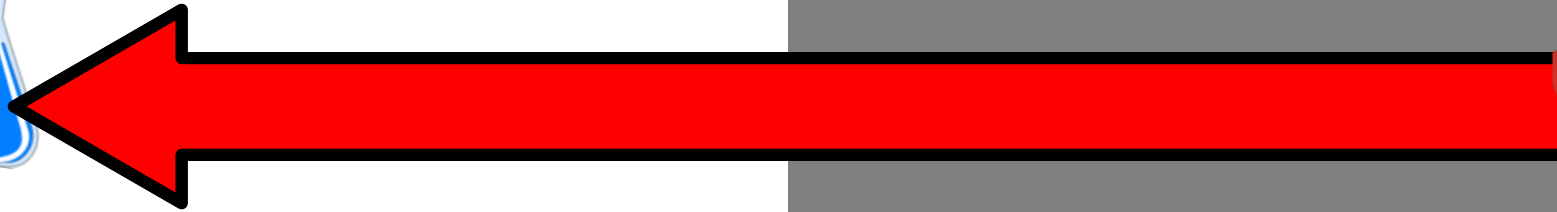
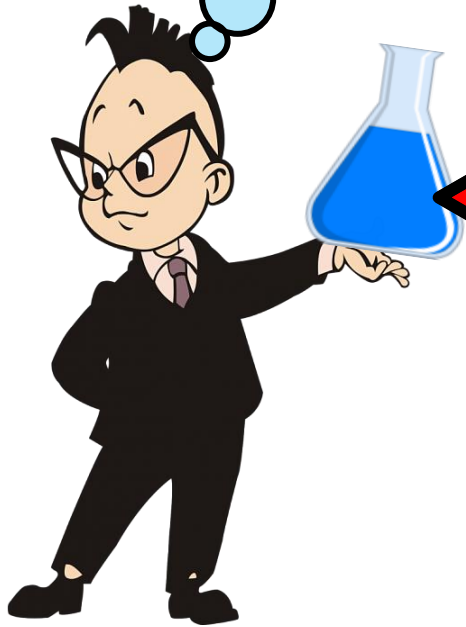
- Exploits a signed vulnerable driver to bypass the Kernel Patch Protection and Driver Signature Enforcement

1. Ransomware installs Gigabyte driver to kill antivirus products - <https://www.zdnet.com/article/ransomware-installs-gigabyte-driver-to-kill-antivirus-products/>
2. Nansh0u Miner Attack Infects 50K MS-SQL, PHPMyAdmin Servers - <https://www.guardicore.com/2019/05/nansh0u-campaign-hackers-arsenal-grows-stronger/>
3. Glupteba: Hidden Malware Delivery in Plain Sight - https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final.pdf











**Don't mess with
kernel data!**



MemoryRanger



Episode 1

Bypass File Sharing Access Control via Hijacking File Structures

SCENARIO OF ATTACKS ON FILES



Researcher's Driver

Open a file in an exclusive mode

NTOS Kernel



Secret Formula

SCENARIO OF ATTACKS ON FILES



Researcher's Driver

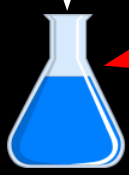
Open a file in an exclusive mode



Attacker's Driver

(1) Try to access the file via ZwCreateFile

NTOS Kernel



Secret Formula

SCENARIO OF ATTACKS ON FILES



Researcher's Driver

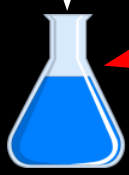
Open a file in an exclusive mode



Attacker's Driver

(1) Try to access the file via ZwCreateFile

NTOS Kernel



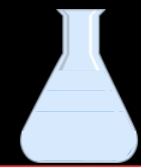
Secret Formula

SCENARIO OF ATTACKS ON FILES



Researcher's Driver

Open a file in an exclusive mode



Leaked Secret Formula

Attacker's Driver

(1) Try to access the file via ZwCreateFile

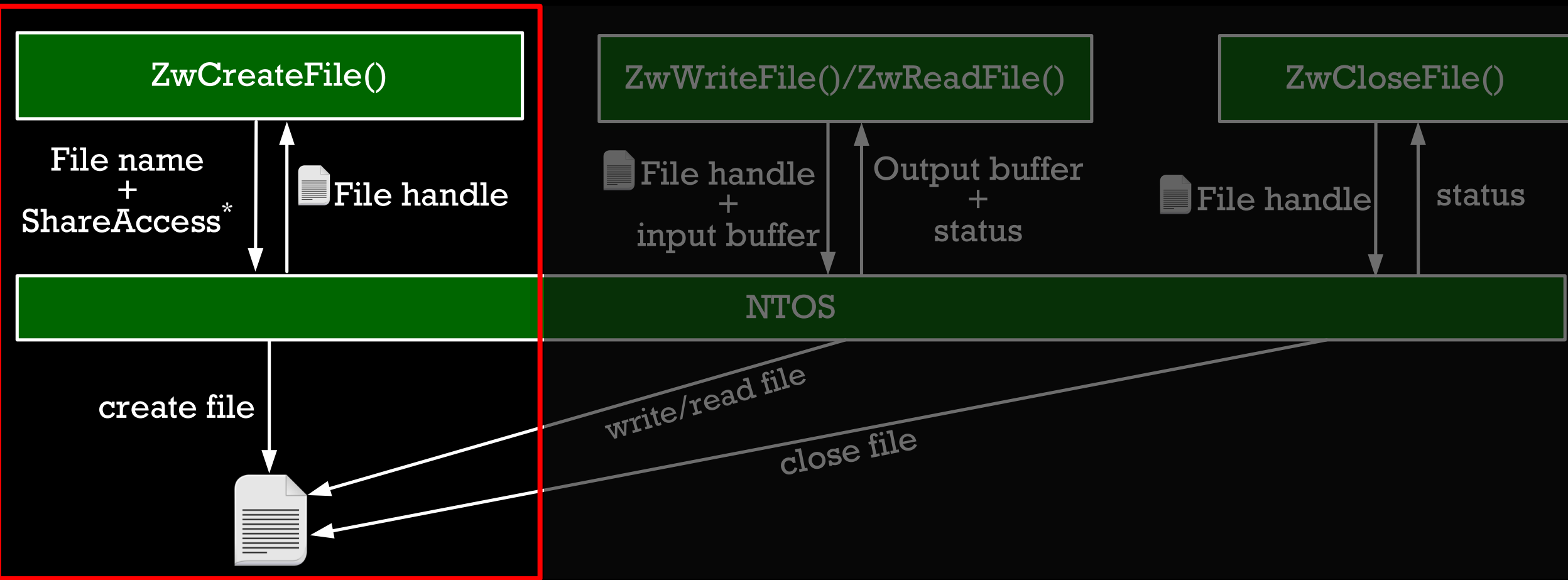
(2) Try to access the file via Hijacking Attacks

NTOS Kernel



Corrupted Data

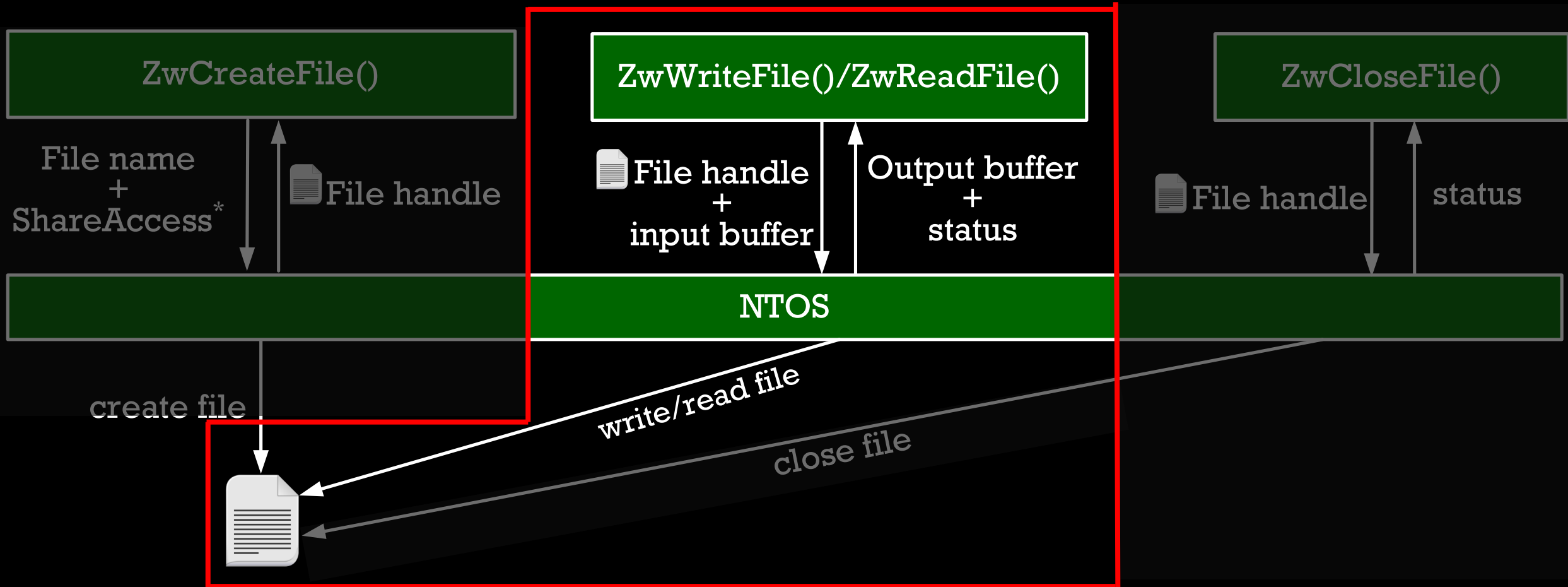
FILE SYSTEM KERNEL API ROUTINES



```
NTSTATUS ZwCreateFile(..., ShareAccess, ...);
```

- ShareAccess flag determines whether other drivers can access the opened file.

FILE SYSTEM KERNEL API ROUTINES

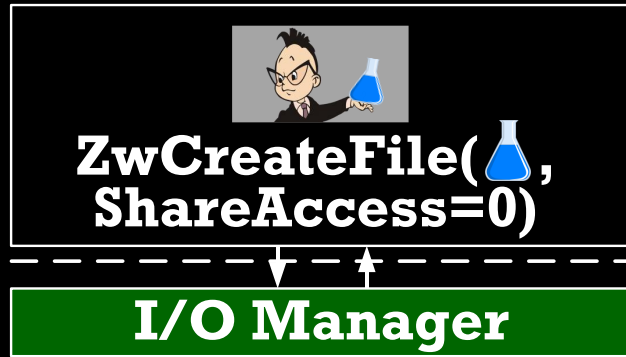


INTERNALS OF ZwCreateFile

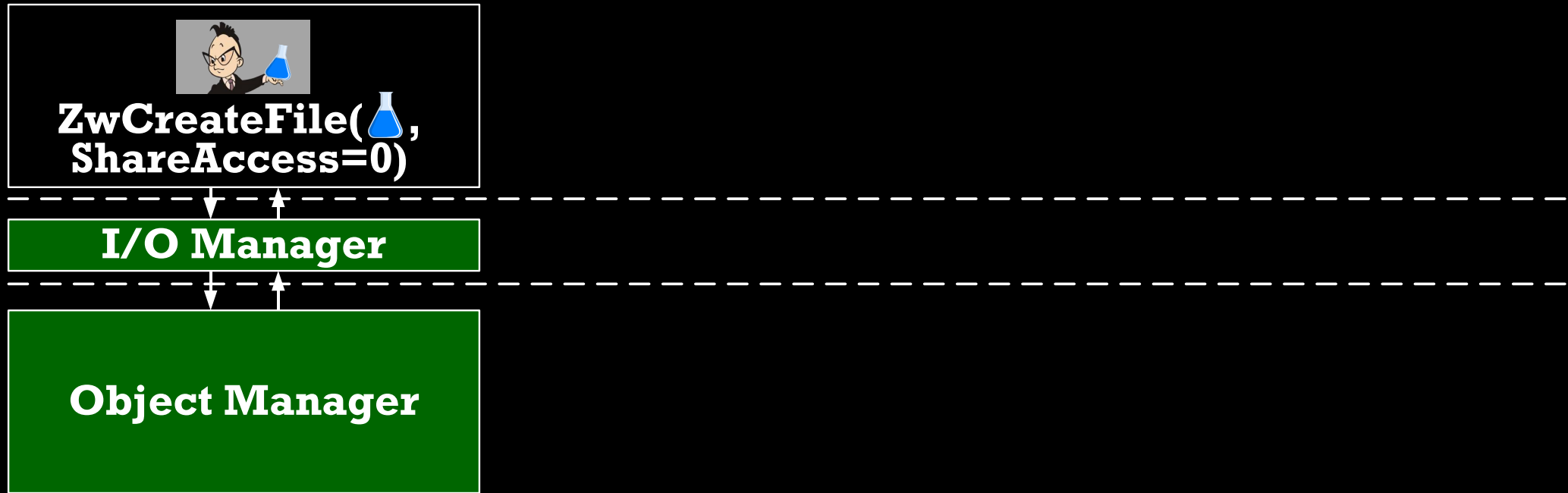


**ZwCreateFile(🧪,
ShareAccess=0)**

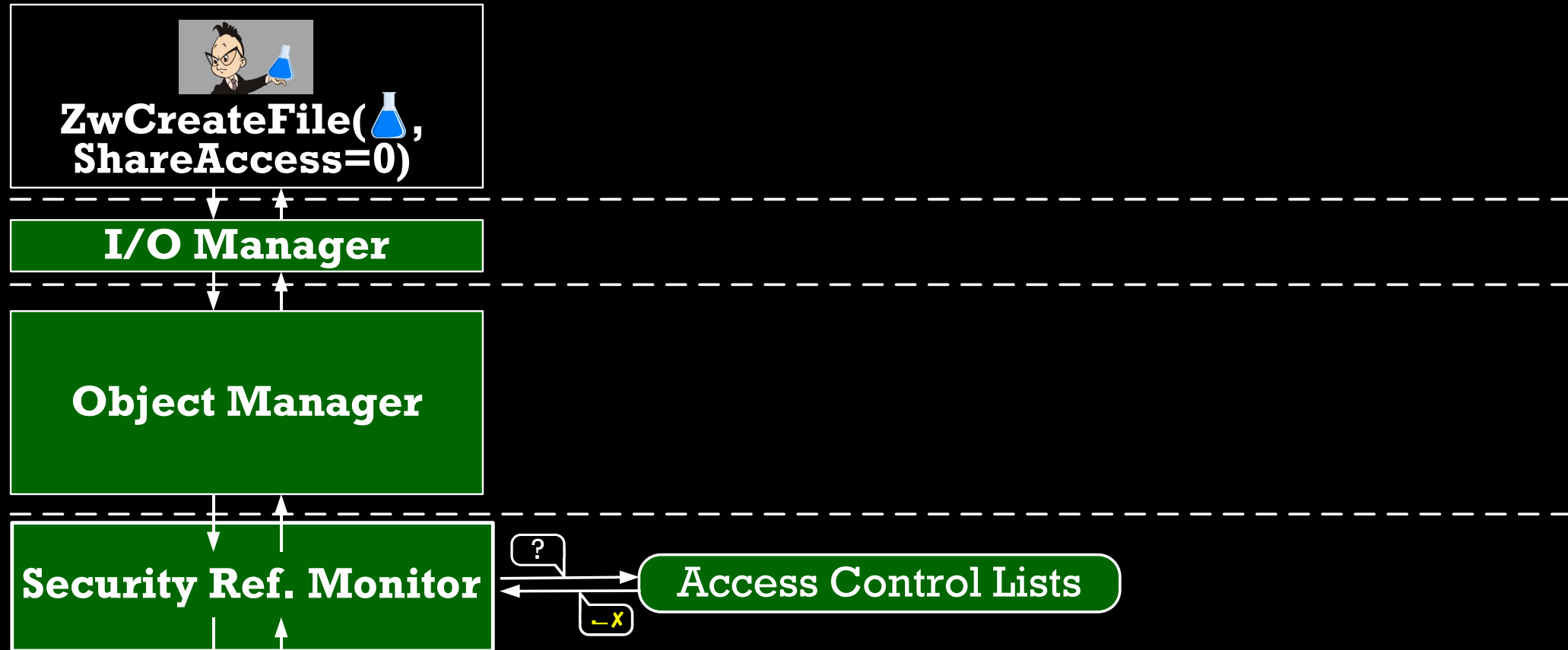
INTERNALS OF ZwCreateFile



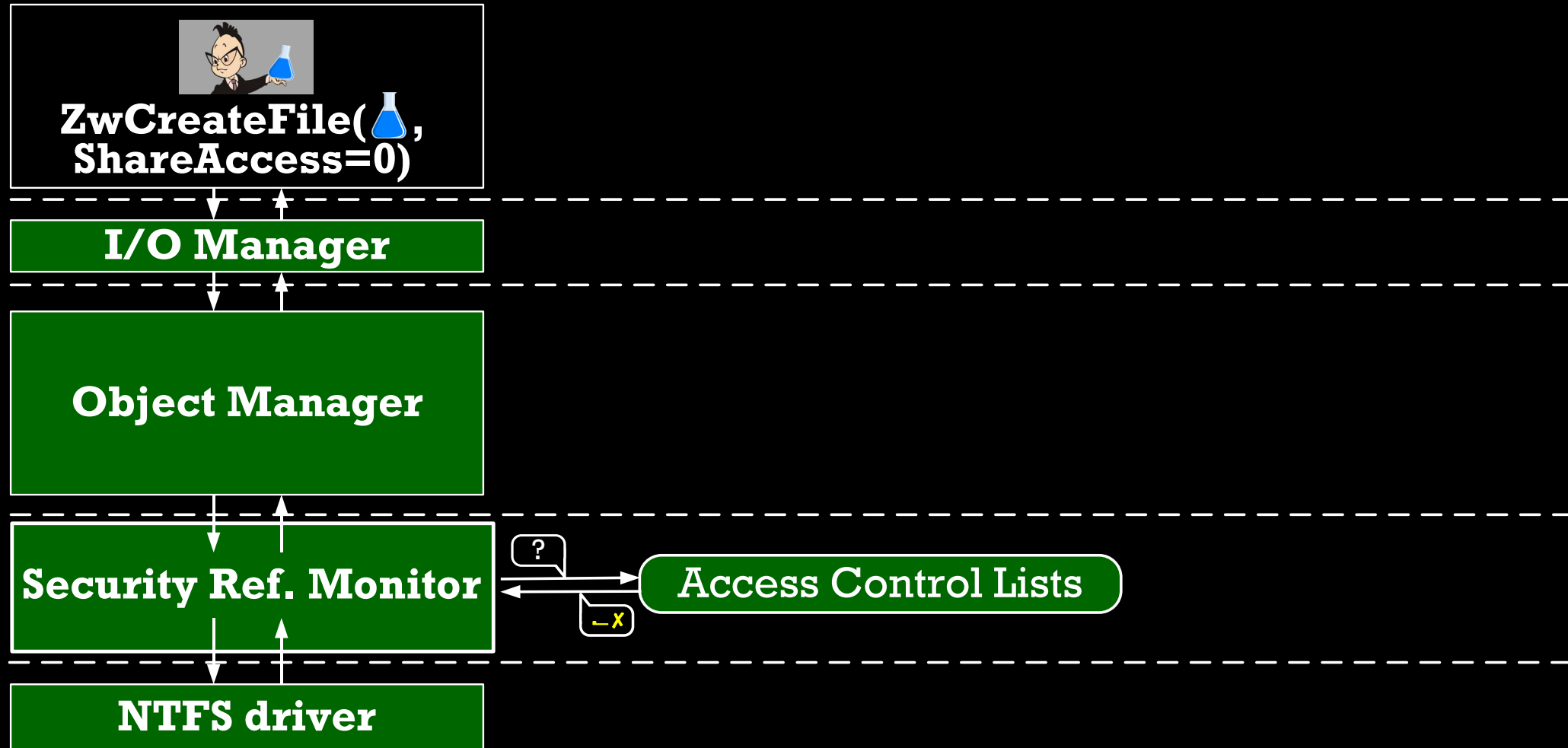
INTERNALS OF ZwCreateFile



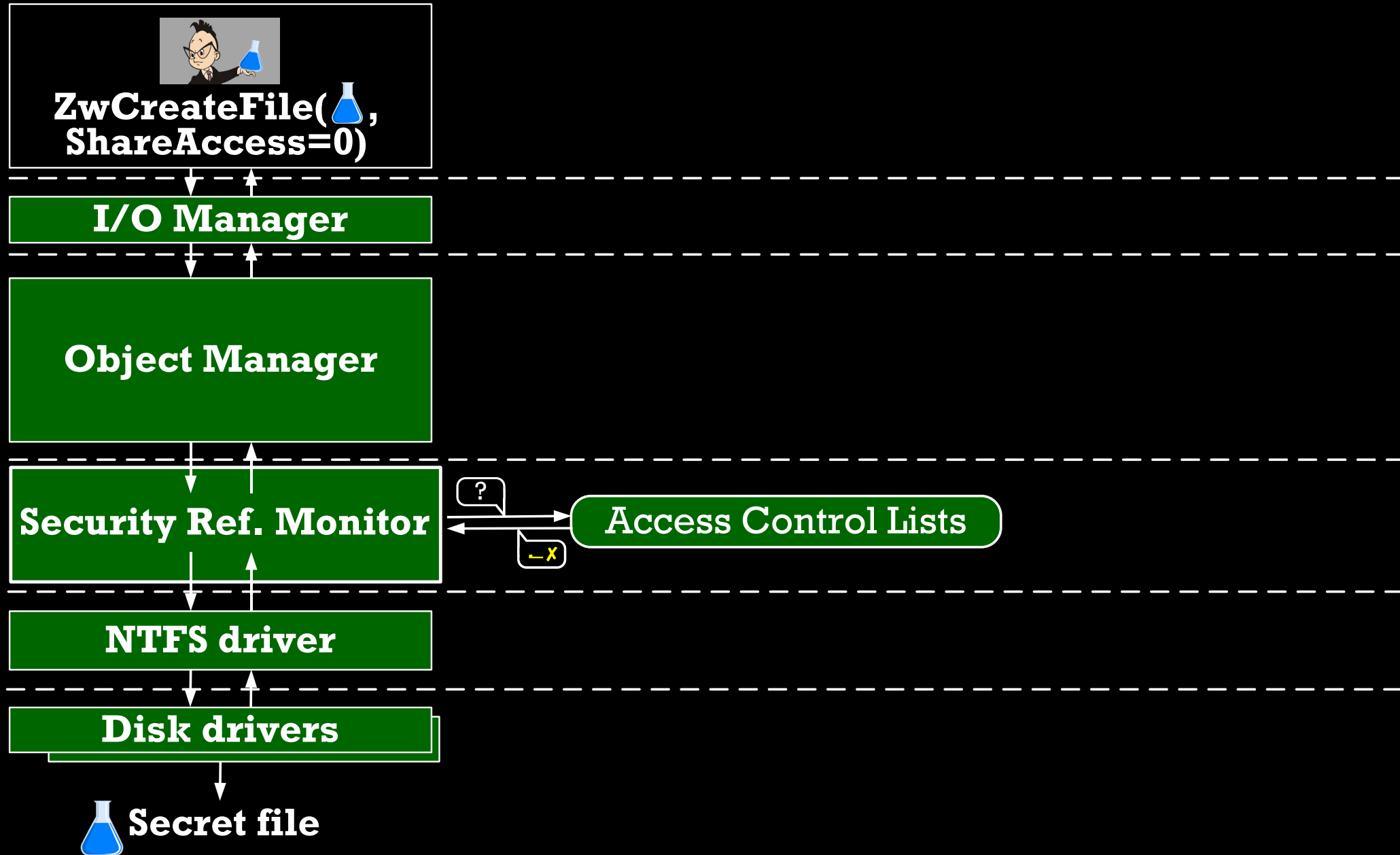
INTERNALS OF ZwCreateFile



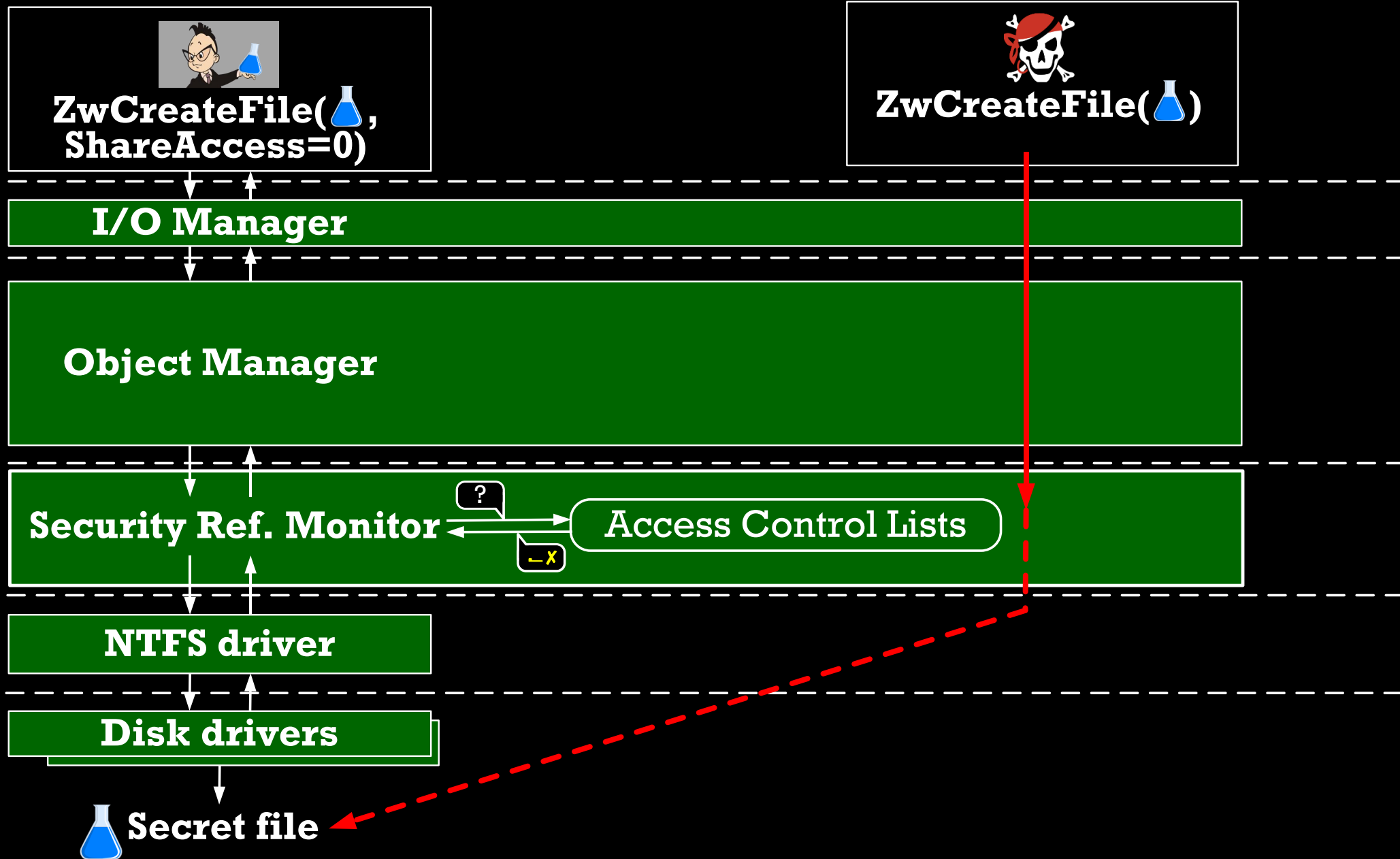
INTERNALS OF ZwCreateFile



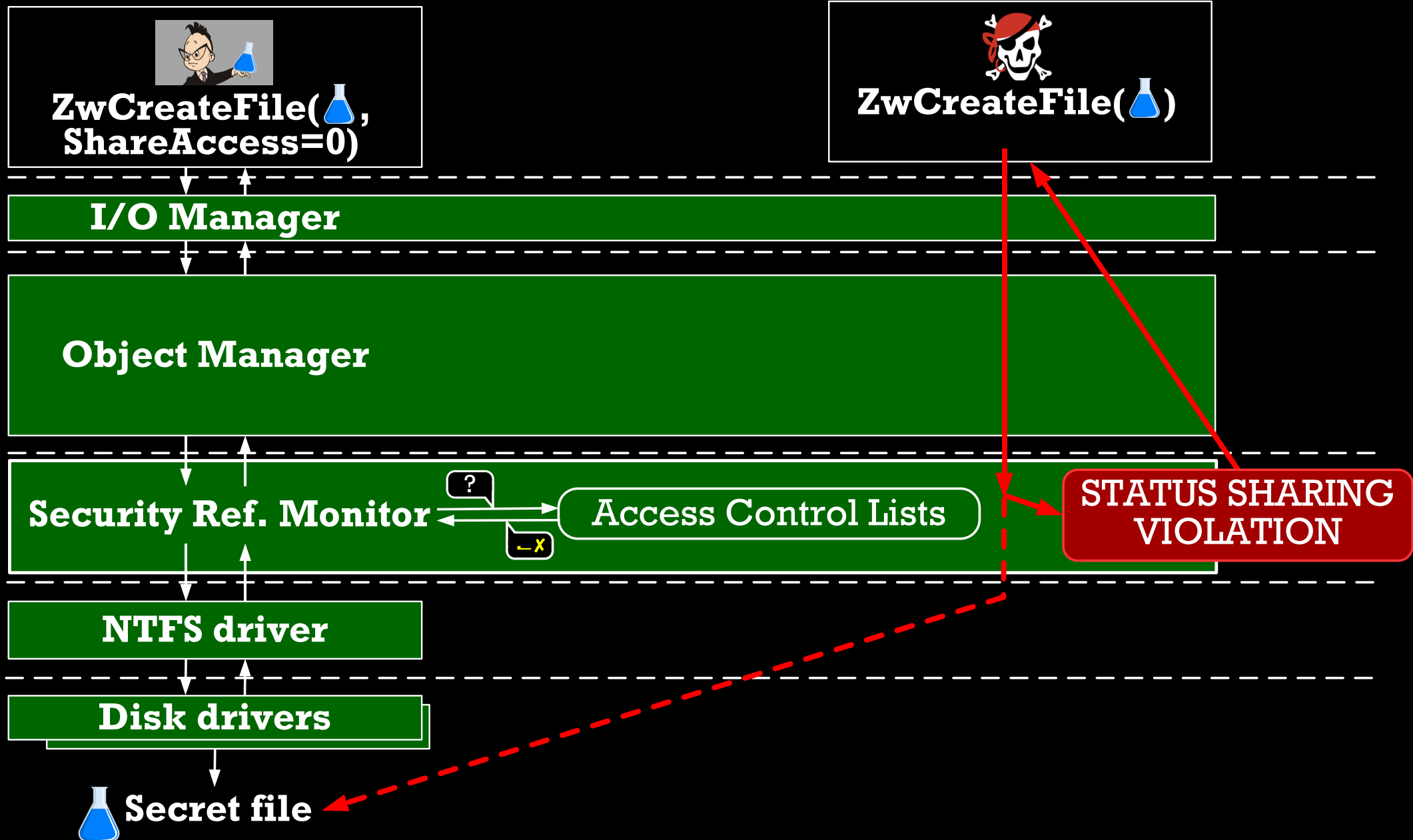
INTERNALS OF ZwCreateFile



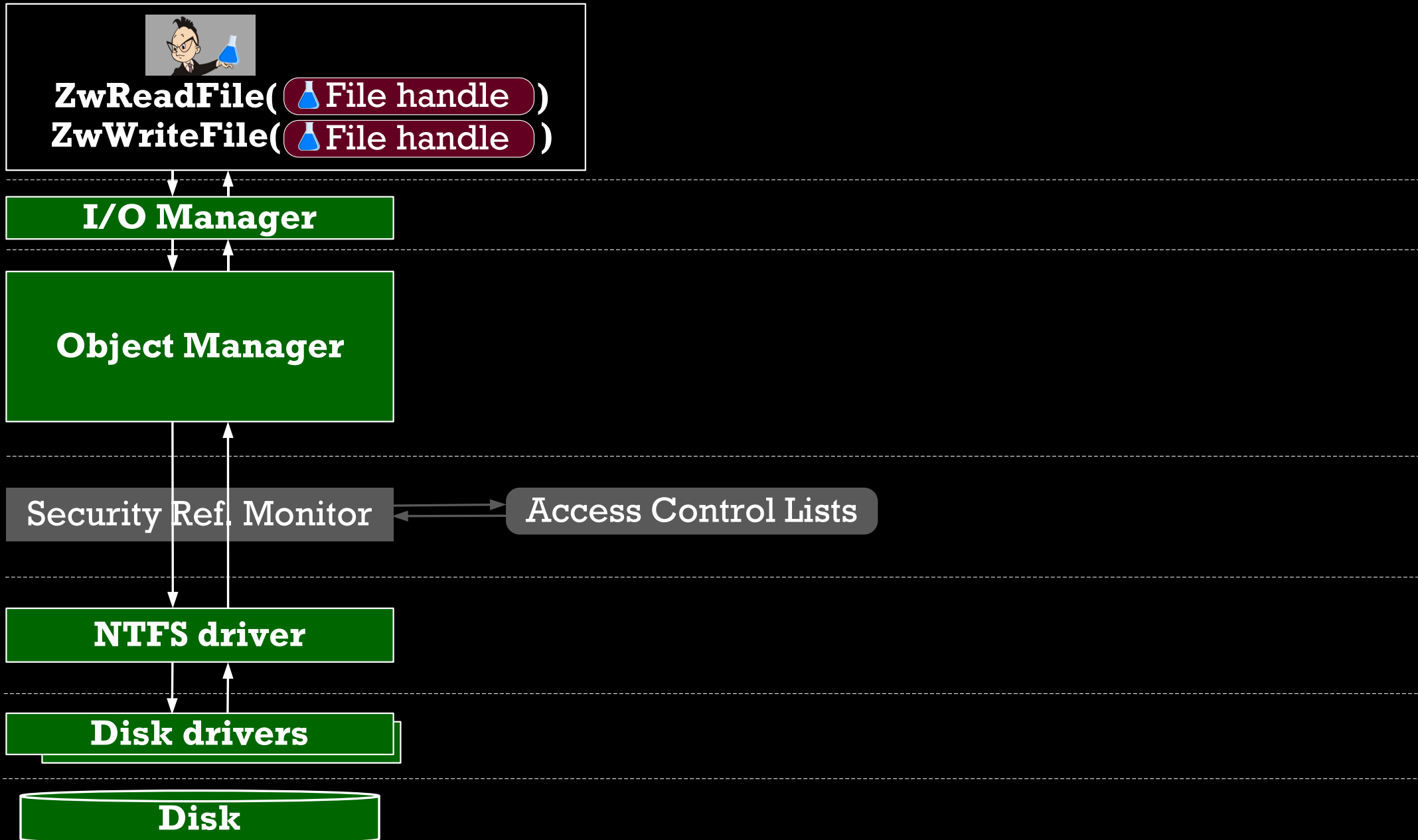
SECURITY REFERENCE MONITOR PREVENTS ILLEGAL ACCESS



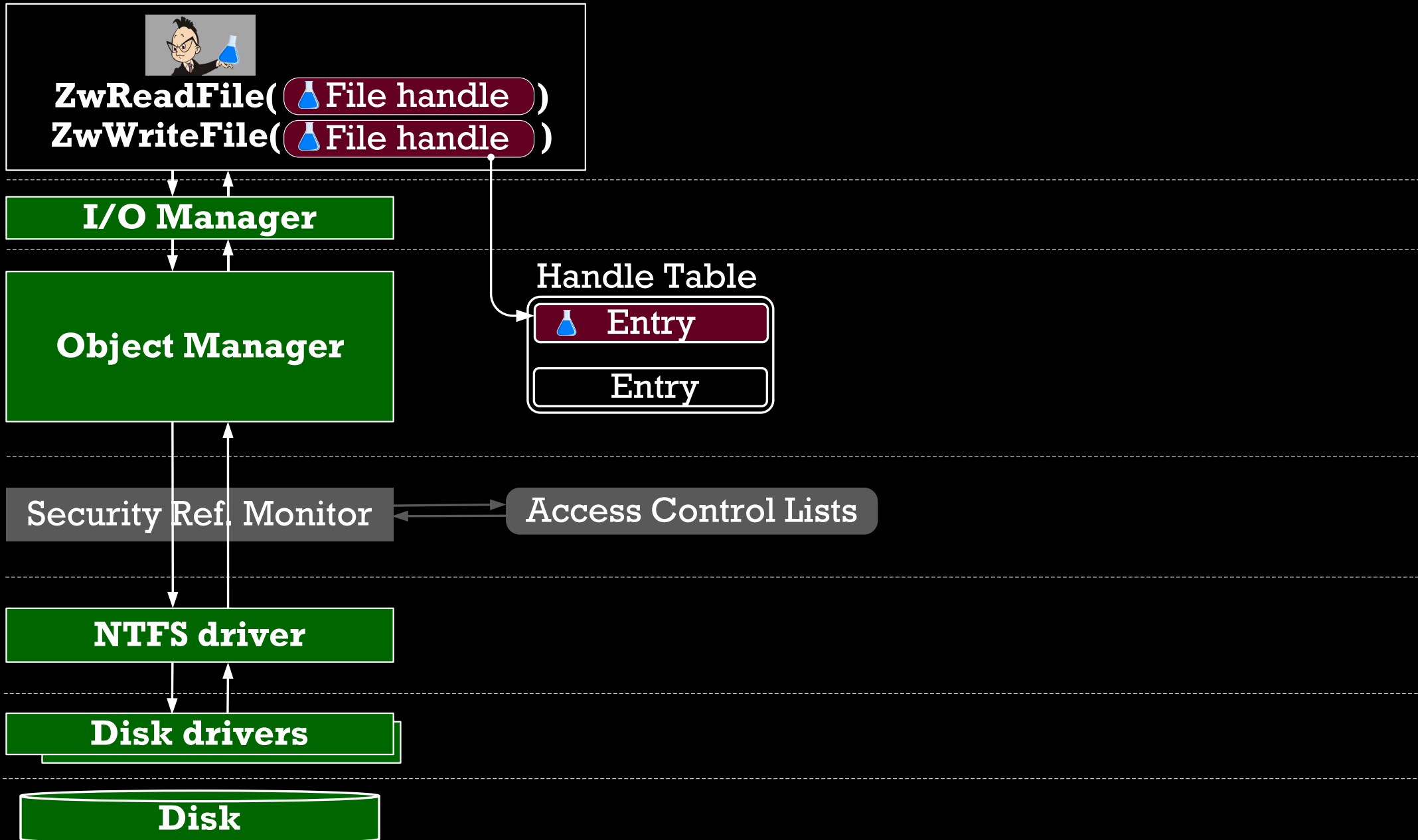
SECURITY REFERENCE MONITOR PREVENTS ILLEGAL ACCESS



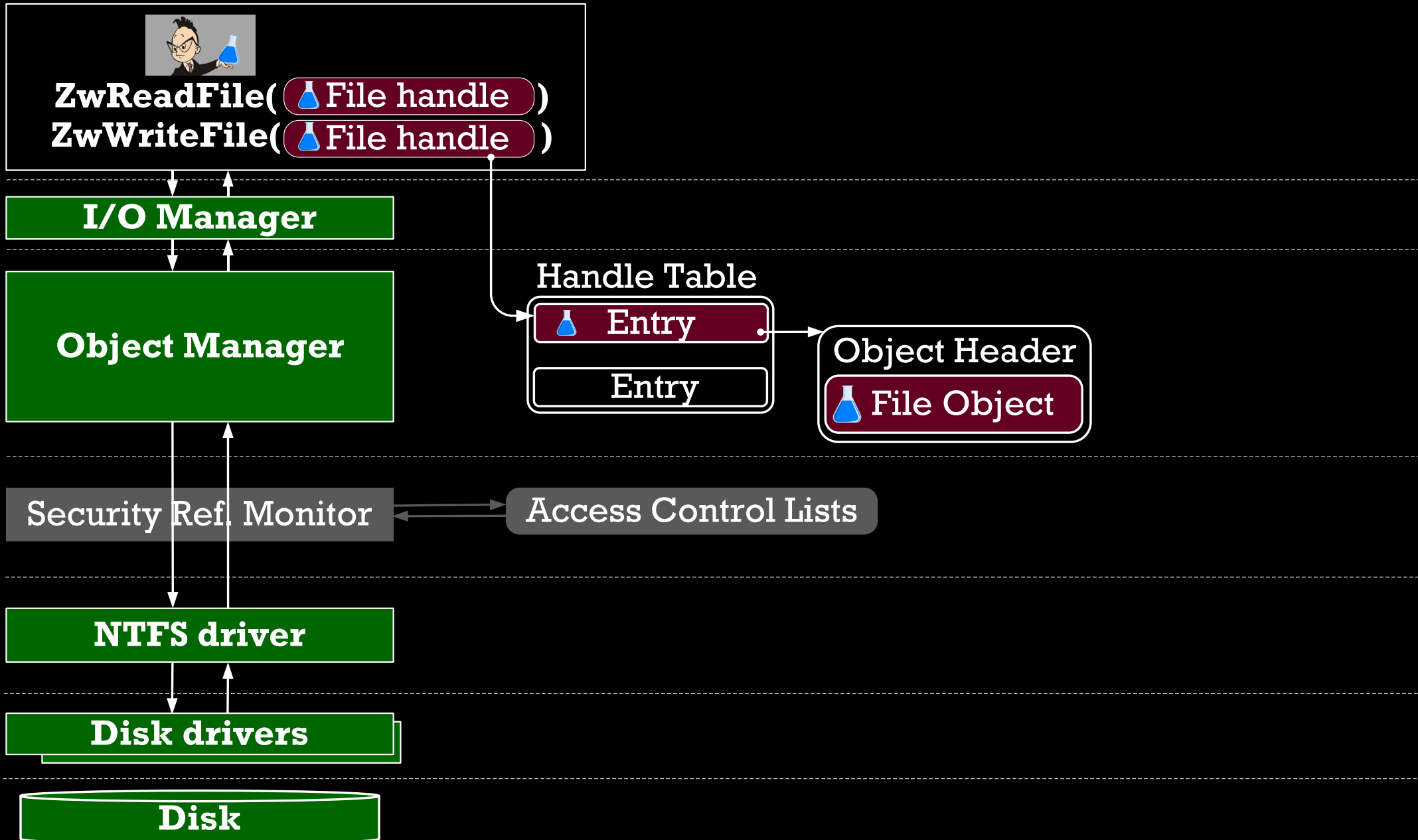
INTERNALS OF ZwReadFile/ZwWriteFile



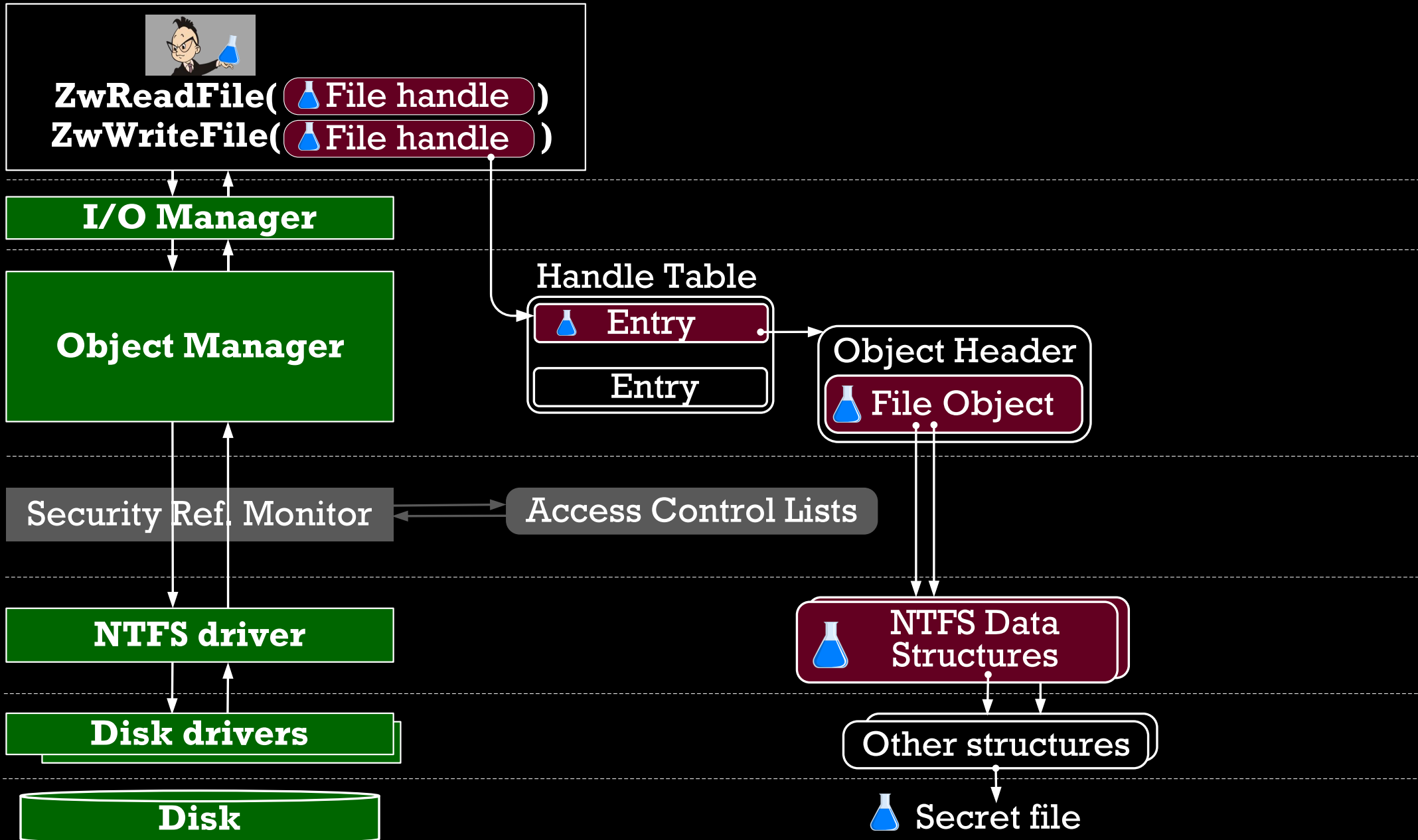
INTERNALS OF ZwReadFile/ZwWriteFile



INTERNALS OF ZwReadFile/ZwWriteFile



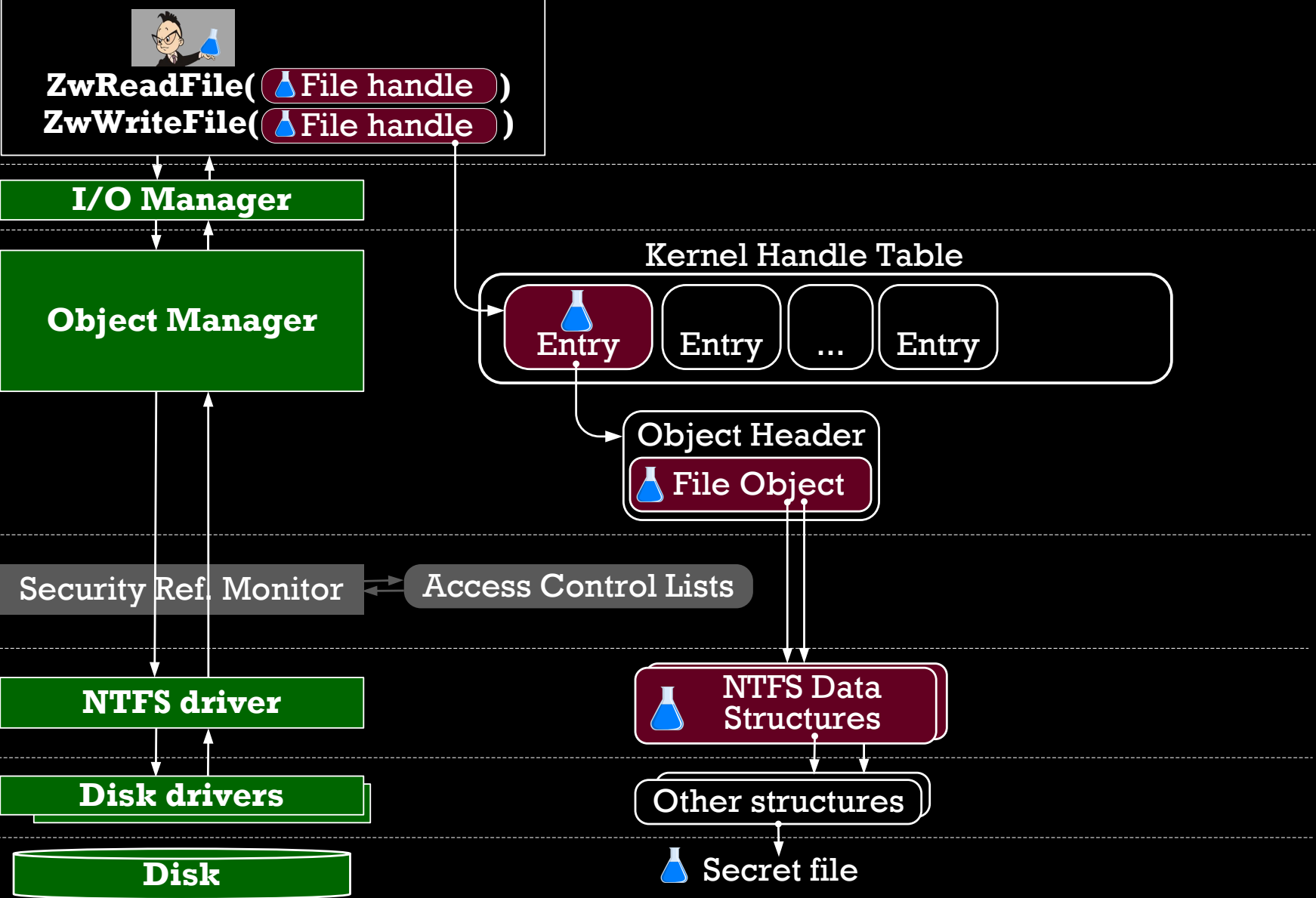
INTERNALS OF ZwReadFile/ZwWriteFile



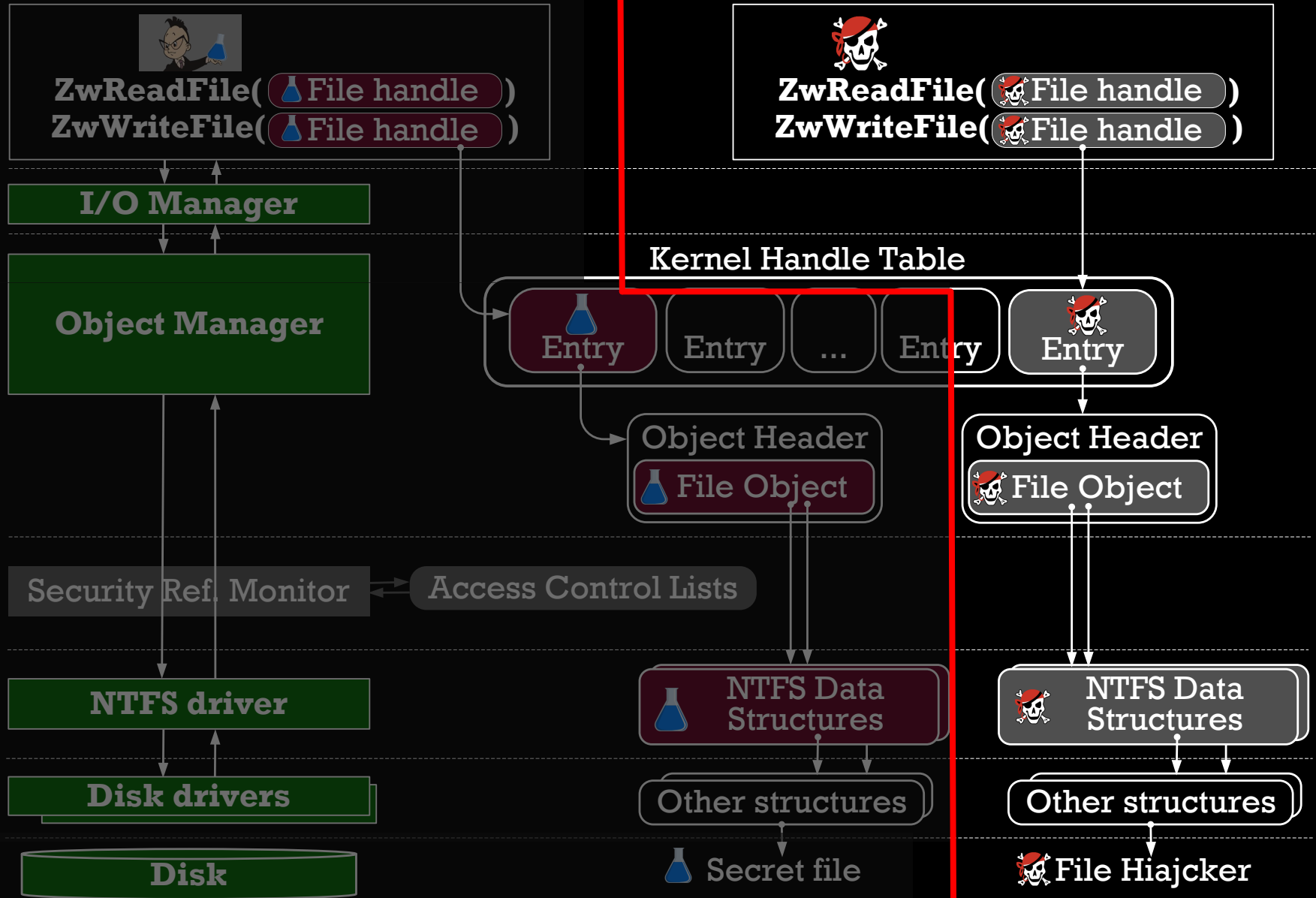
SUMMARY

- ZwCreateFile checks shared access permissions
- ZwWriteFile and ZwReadFile do not bother about access permissions

IDEA OF HIJACKING: CREATE A FILE HIJACKER



IDEA OF HIJACKING: CREATE A FILE HIAJCKER AND COPY STRUCTS



IDEA OF HIJACKING: CREATE A FILE HIAJCKER AND COPY STRUCTS


ZwReadFile( File handle)
ZwWriteFile( File handle)

I/O Manager

Object Manager

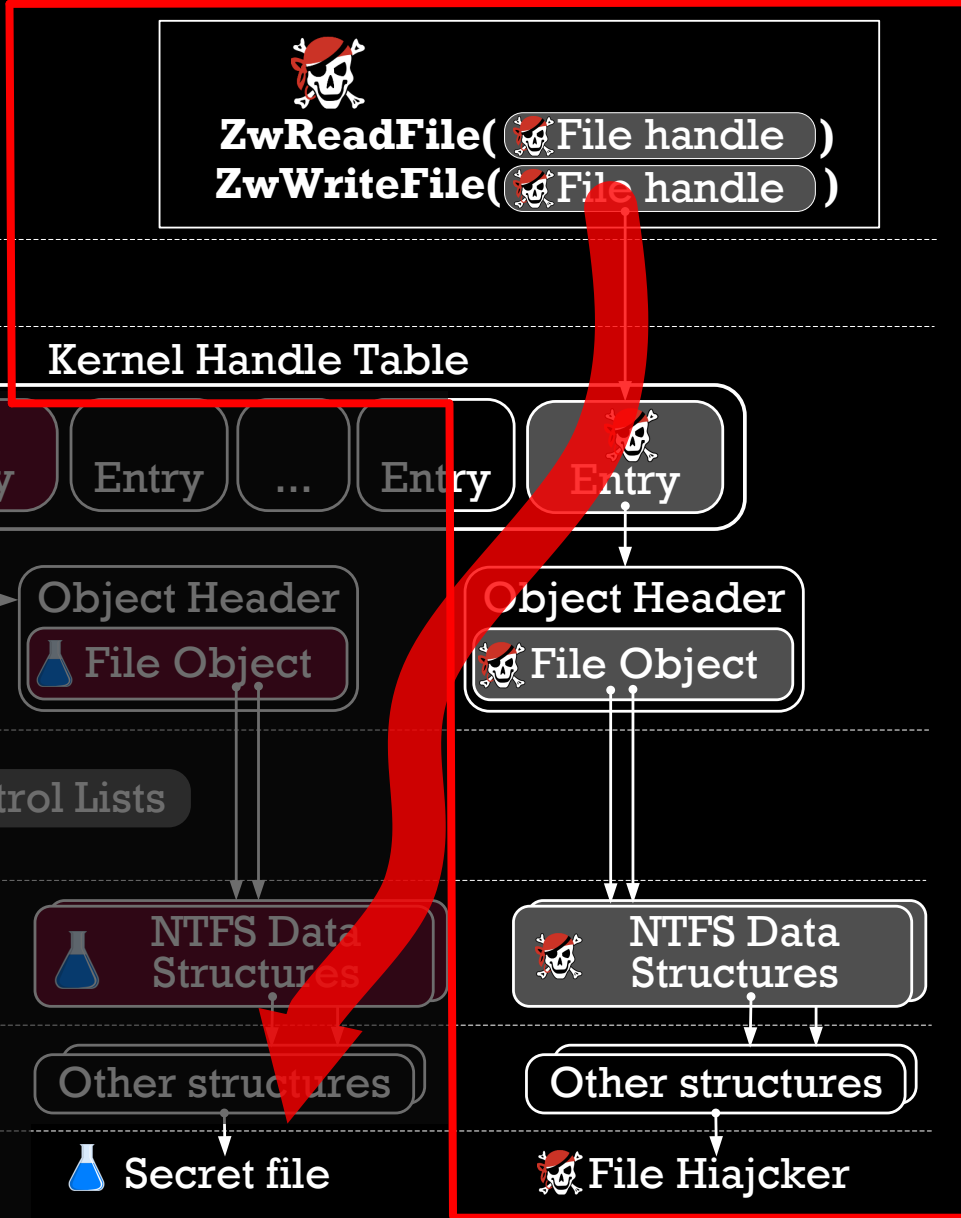
Security Ref. Monitor

Access Control Lists

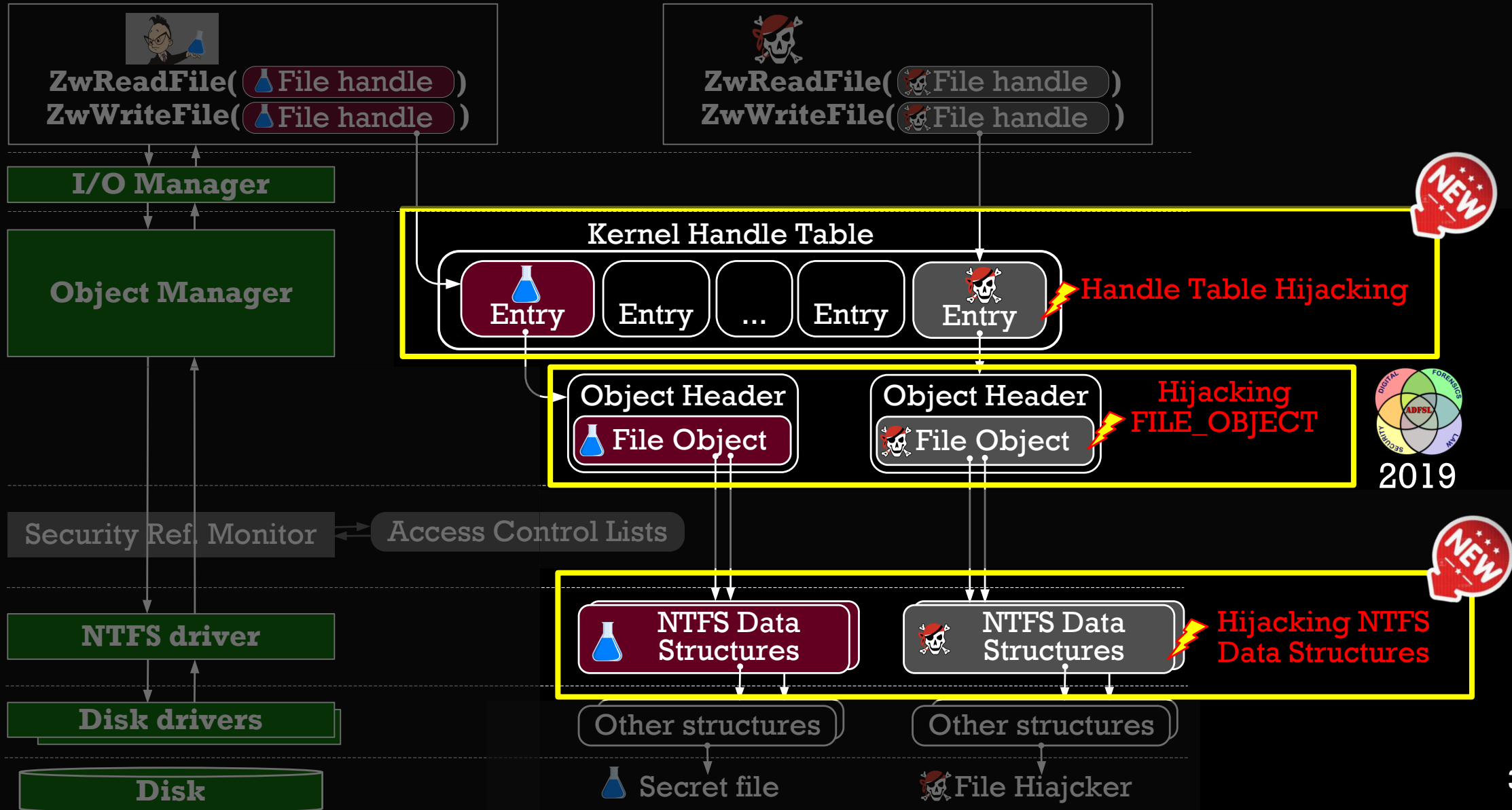
NTFS driver

Disk drivers

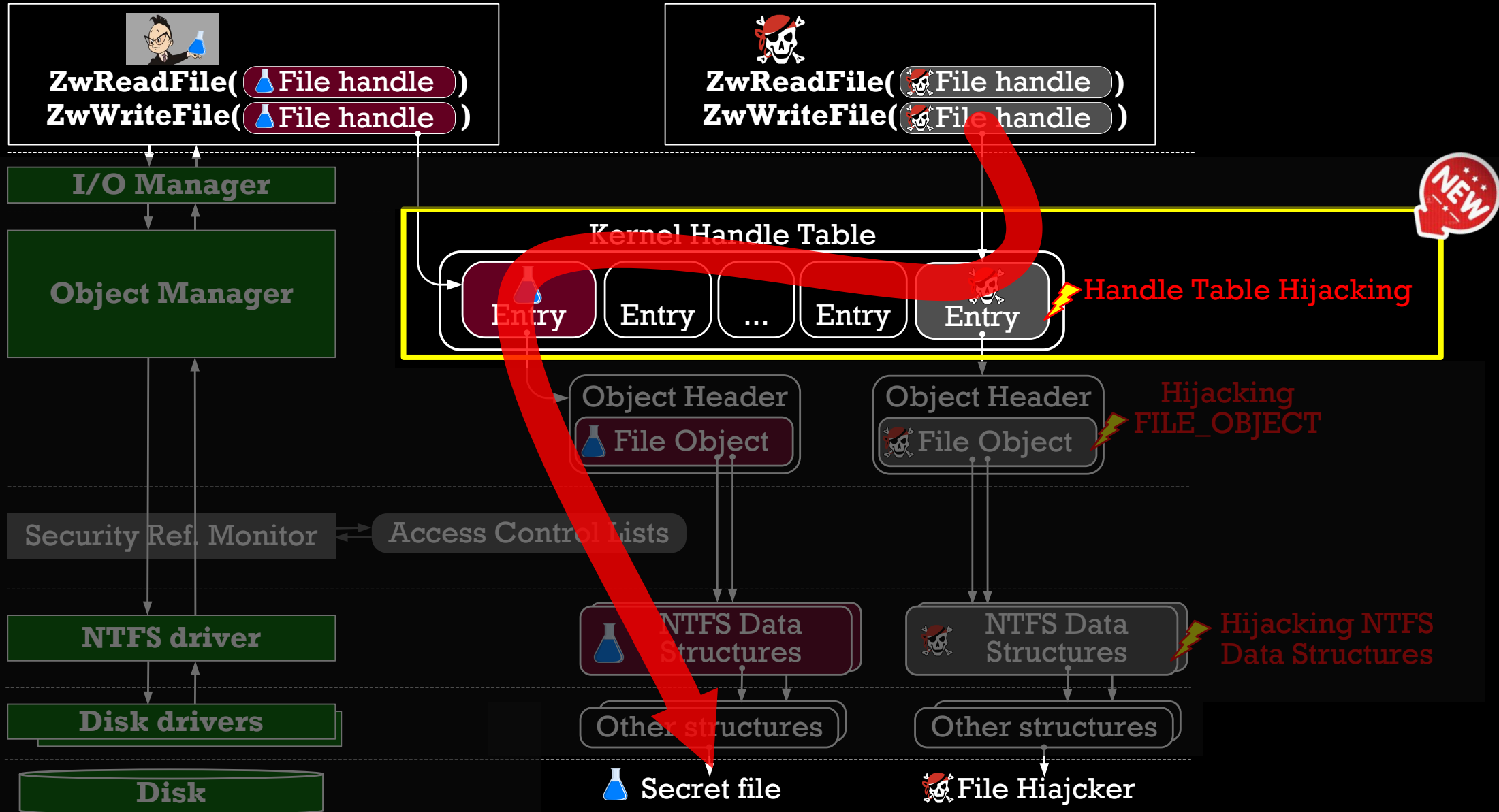
Disk



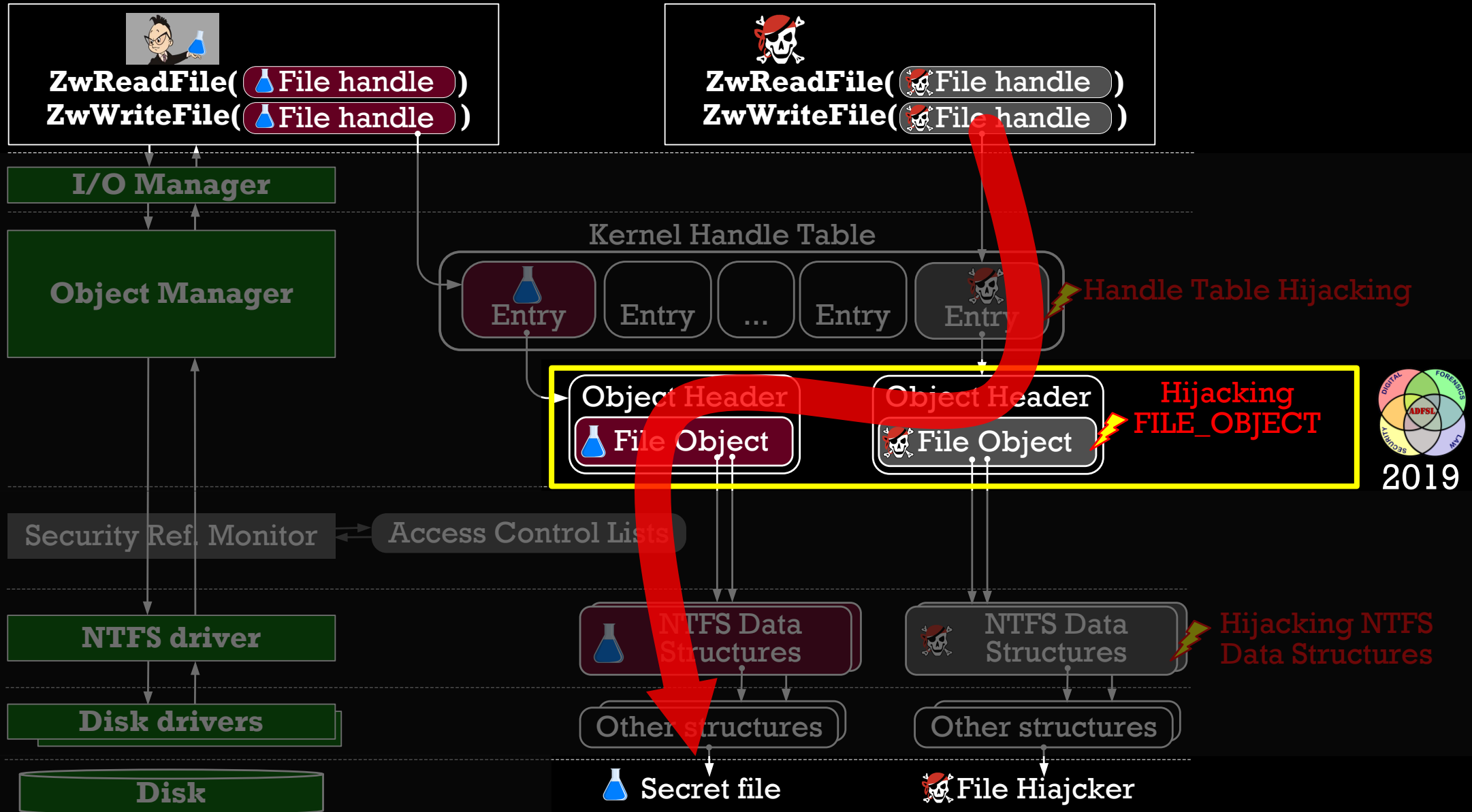
HIJACKING ATTACKS ON FILES STRUCTURES



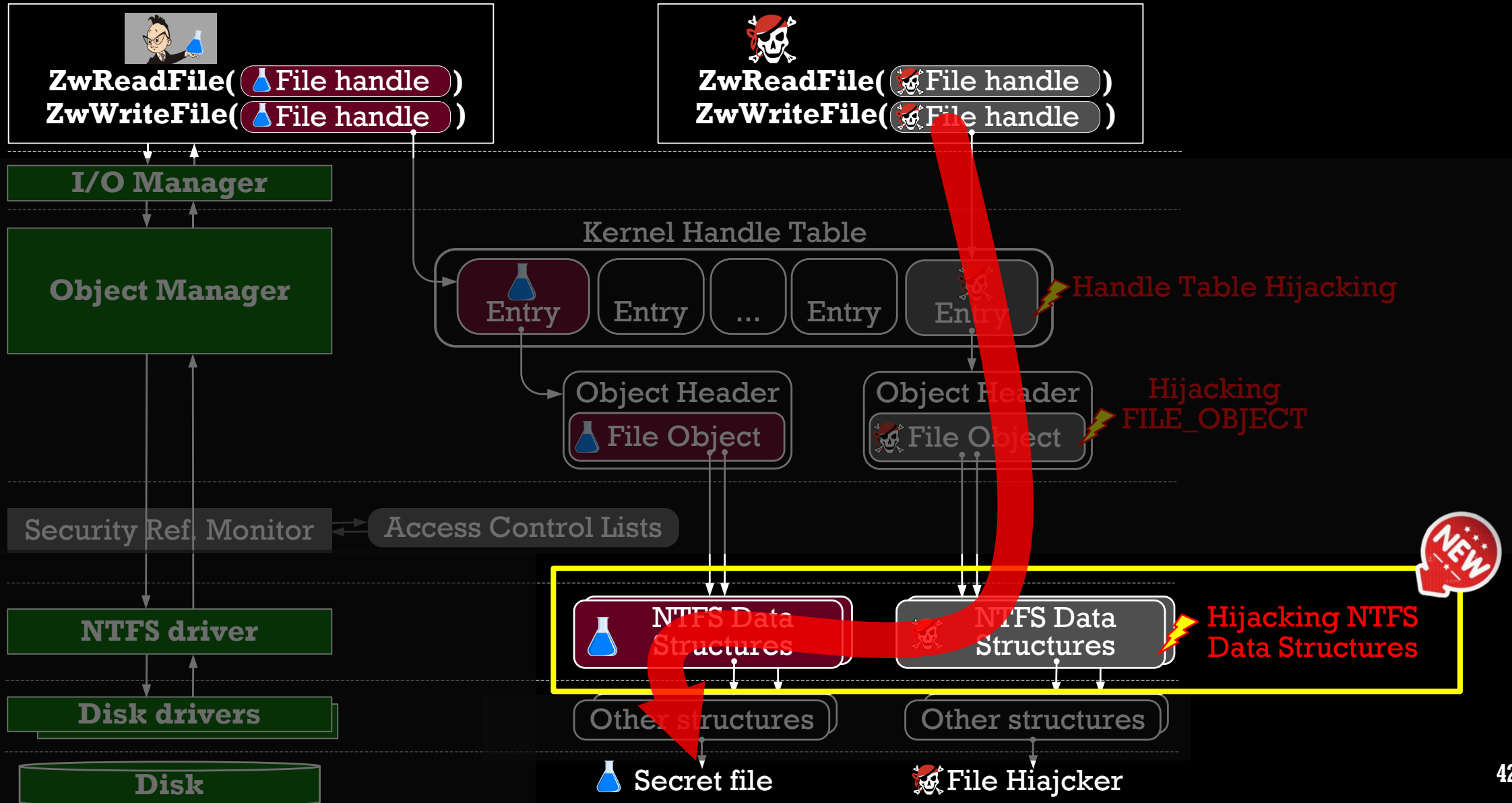
HIJACKING ATTACKS ON FILES STRUCTURES



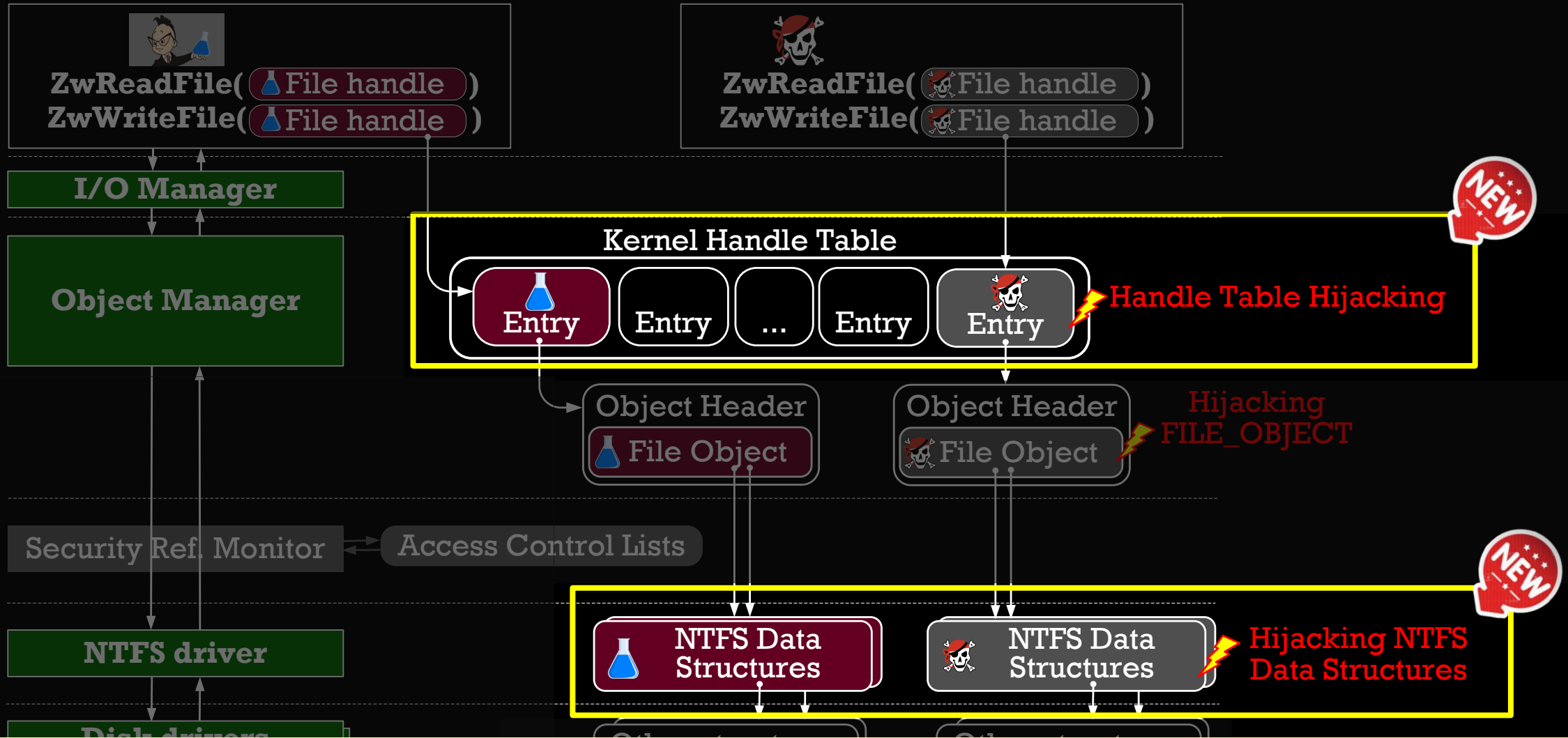
HIJACKING ATTACKS ON FILES STRUCTURES



HIJACKING ATTACKS ON FILES STRUCTURES



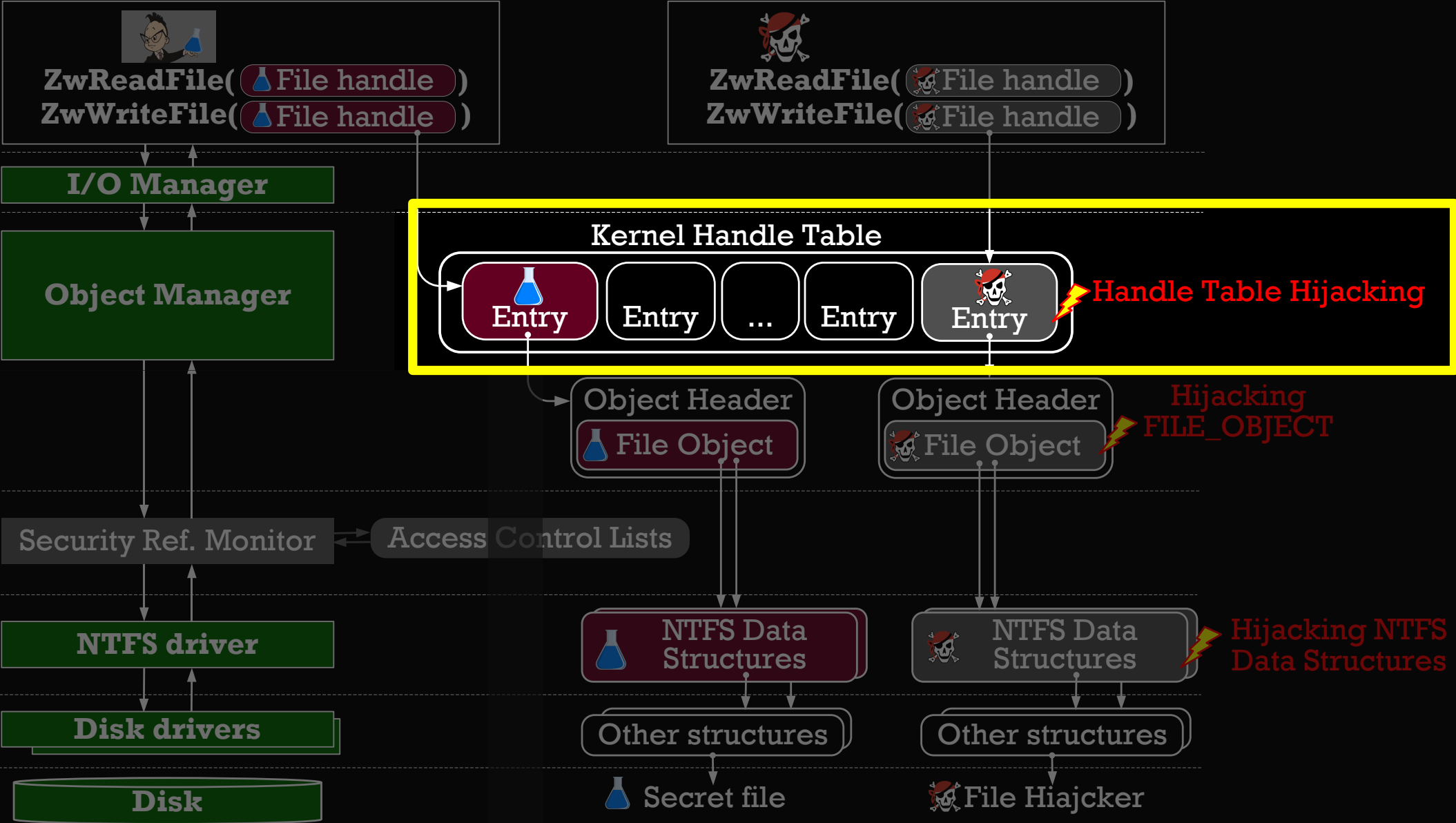
HIJACKING ATTACKS ON FILES STRUCTURES



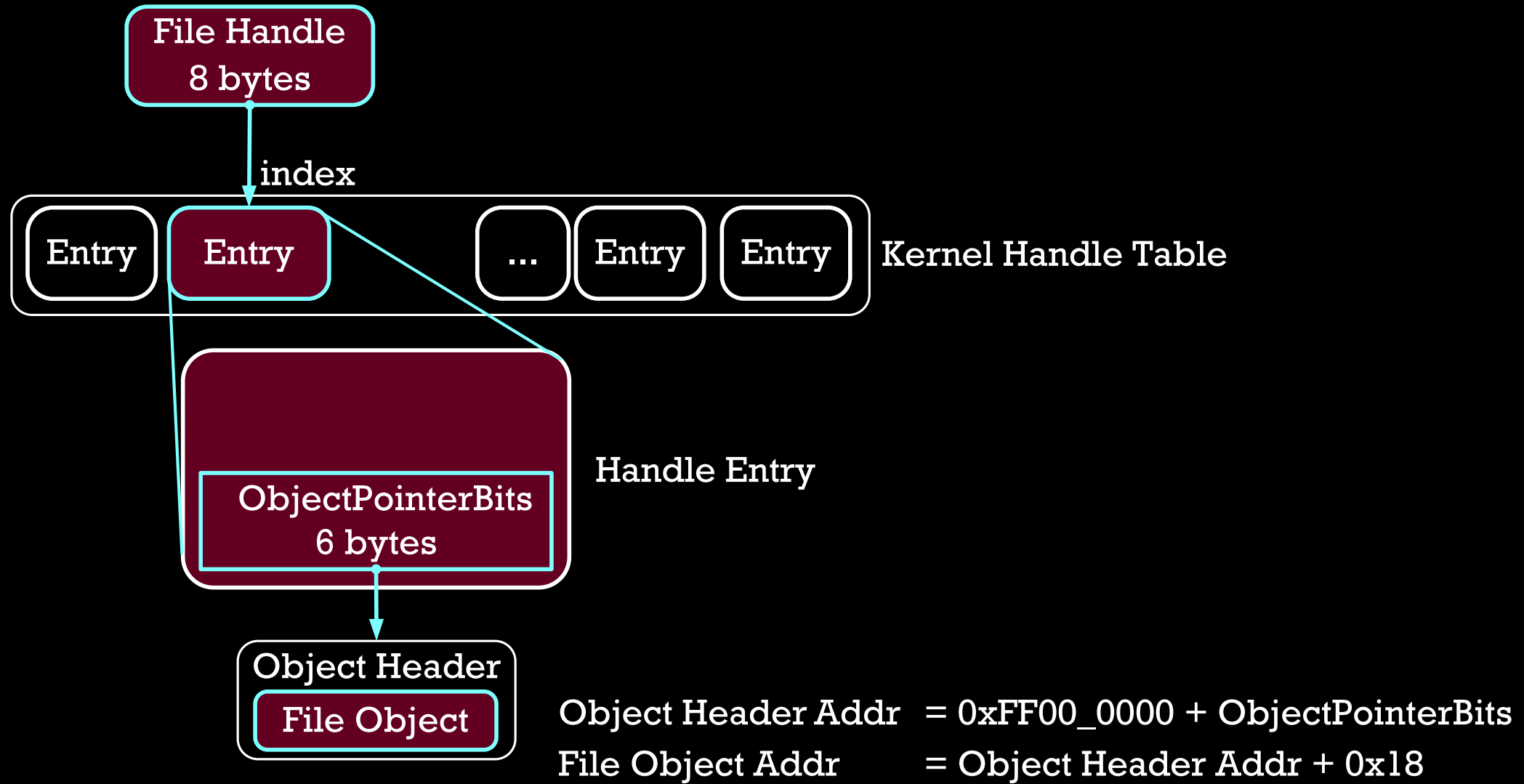
Hijacking FILE_OBJECT → MemoryRanger Prevents Hijacking FILE_OBJECT Structures in Windows Kernel
<https://igorkorkin.blogspot.com/2019/04/memoryranger-prevents-hijacking.html>

HANDLE HIJACKING ATTACK

HANDLE HIJACKING ATTACK



KERNEL HANDLE TABLE



HANDLE TABLE HIJACKING



Researcher's Driver



Attacker's Driver

File handle 

File handle 

Kernel Handle Table

ObjectPointerBits 

Entry

...

ObjectPointerBits 

Object Header 

Object Header 

Secret File 

File Hijacker 

HANDLE TABLE HIJACKING



Researcher's Driver



Attacker's Driver

File handle 

File handle 

Kernel Handle Table

ObjectPointerBits 

Copy content

ObjectPointerBits 

Handle Table Hijacking 

Object Header 

illegal access

Object Header 

Secret File 

File Hijacker 

HANDLE TABLE HIJACKING



Researcher's Driver

File handle 

Kernel Handle Table

ObjectPointerBits 

Object Header 

Secret File 



Attacker's Driver

File handle 

ObjectPointerBits 

Object Header 

File Hijacker 

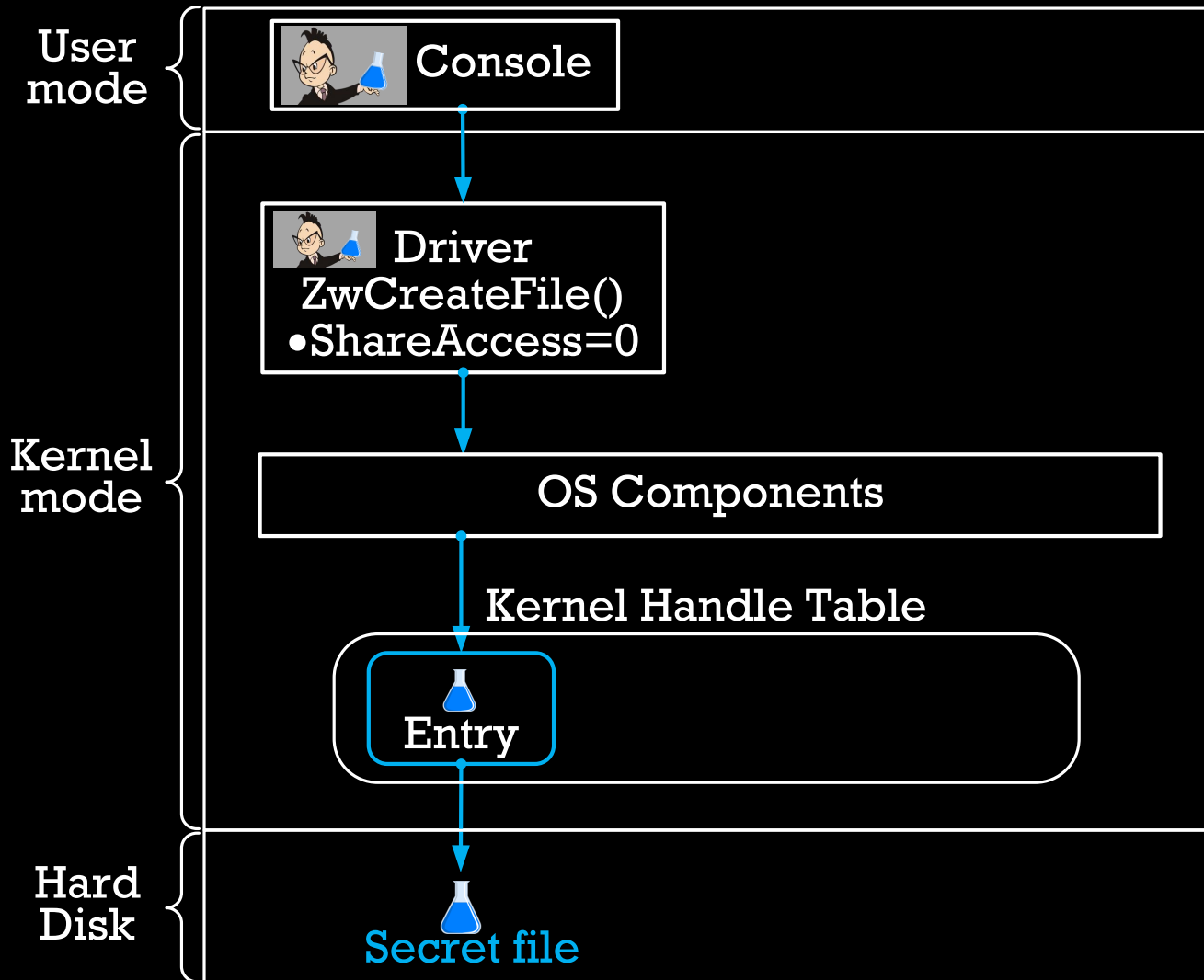
Copy content

illegal access

Handle Table Hijacking

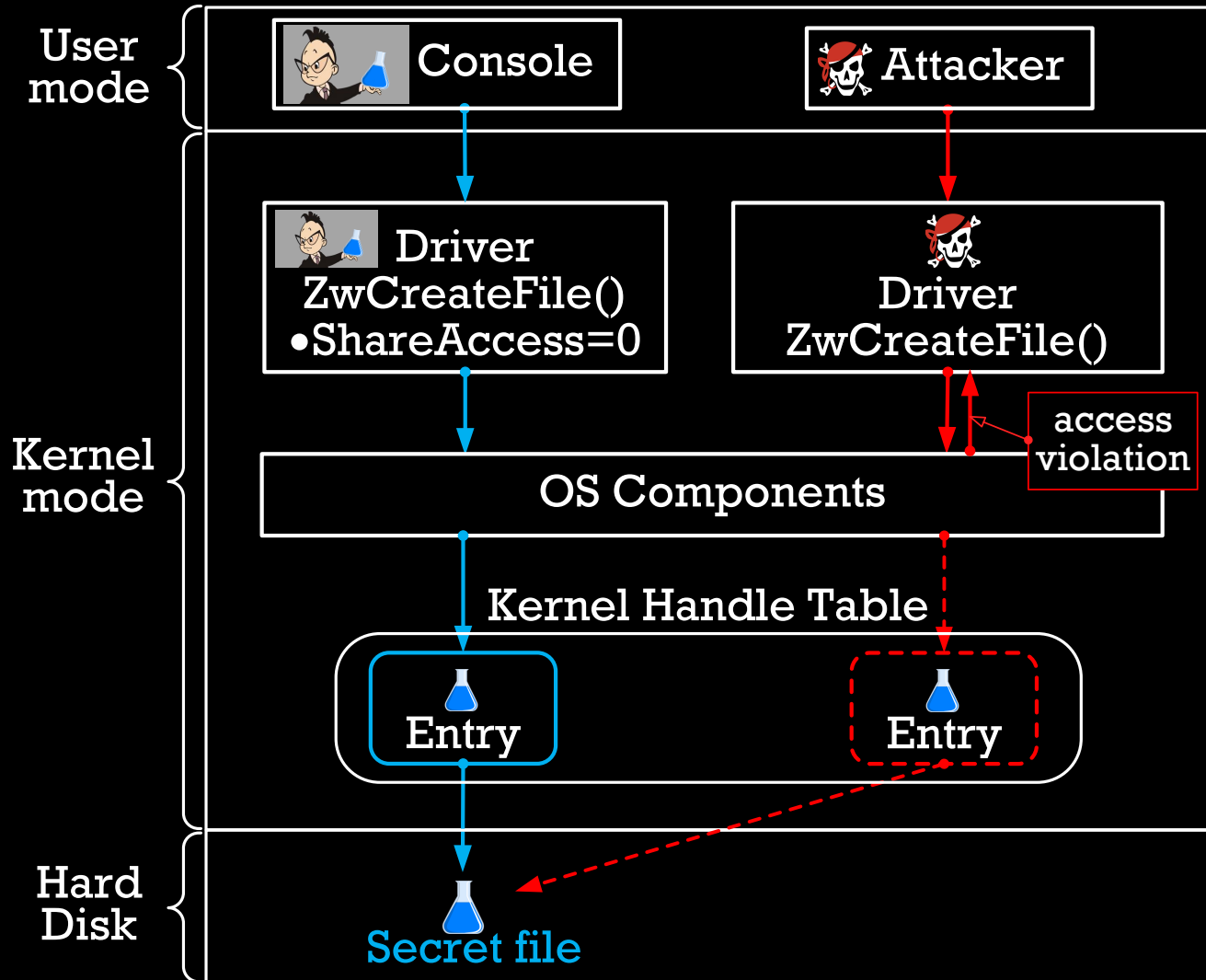
DEMO: HANDLE TABLE HIJACKING

The researcher opens a secret file



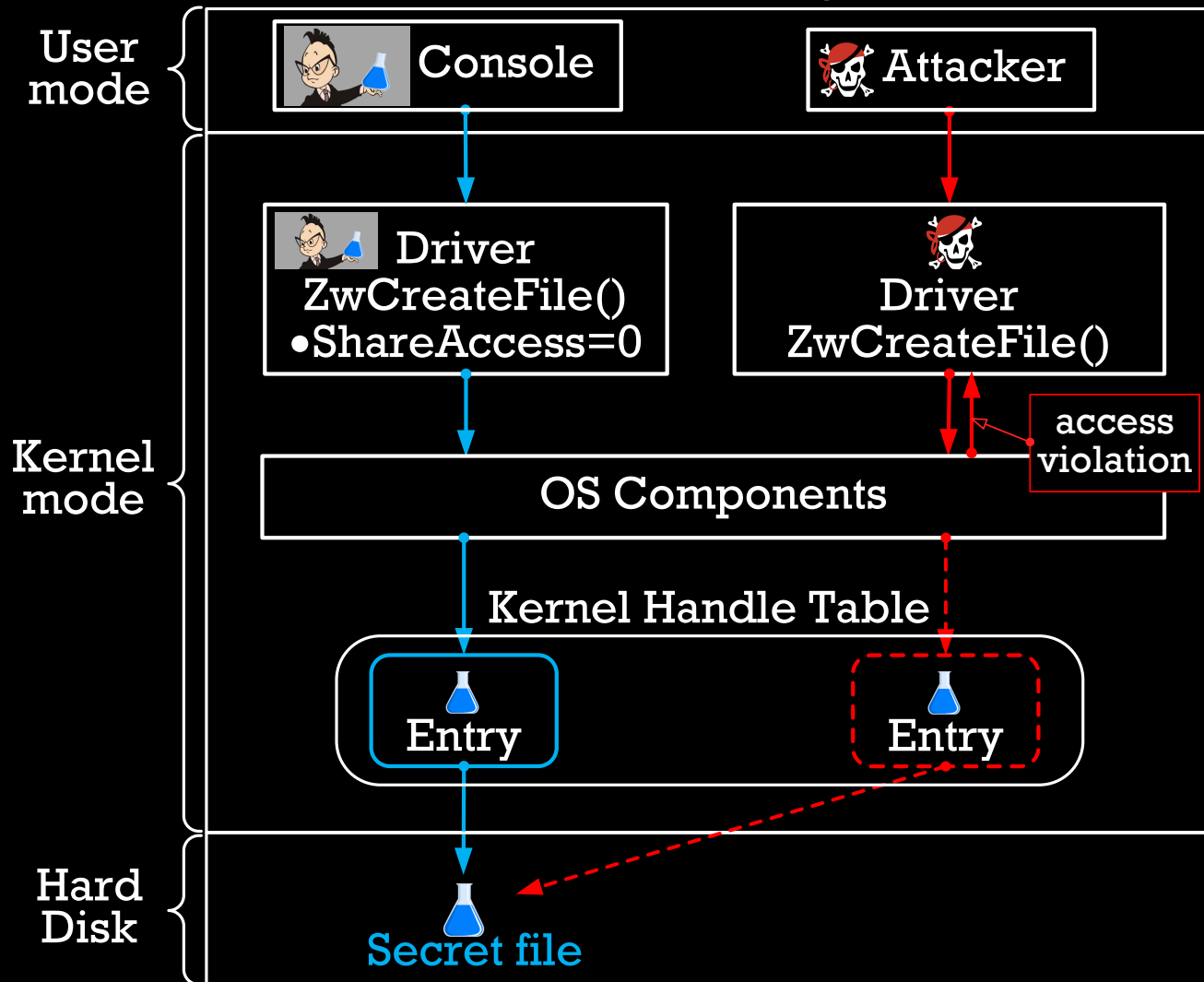
DEMO: HANDLE TABLE HIJACKING

Attempt 1: The Legal Access

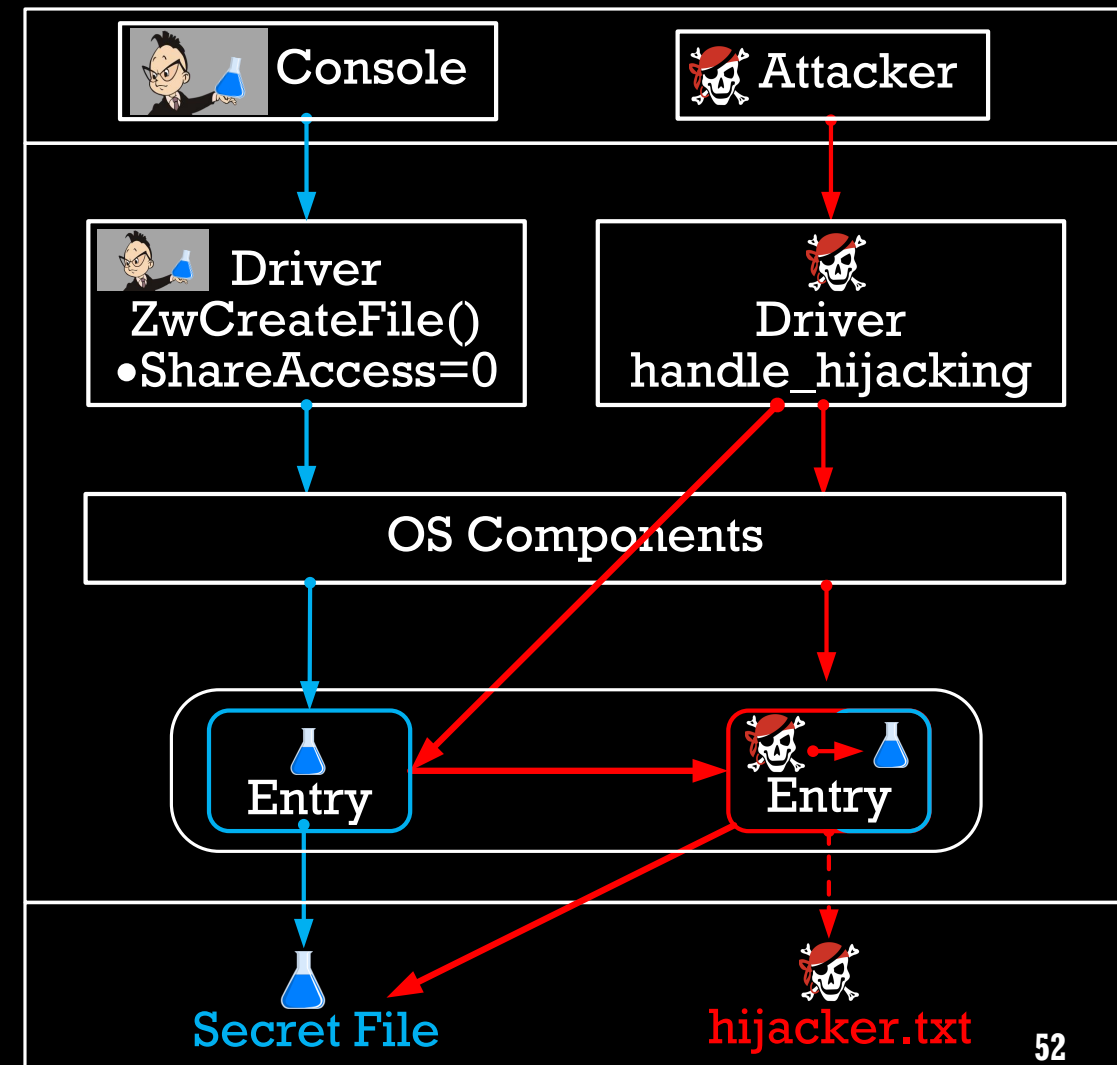


DEMO: HANDLE TABLE HIJACKING

Attempt 1: The Legal Access



Attempt 2: Handle Table Hijacking



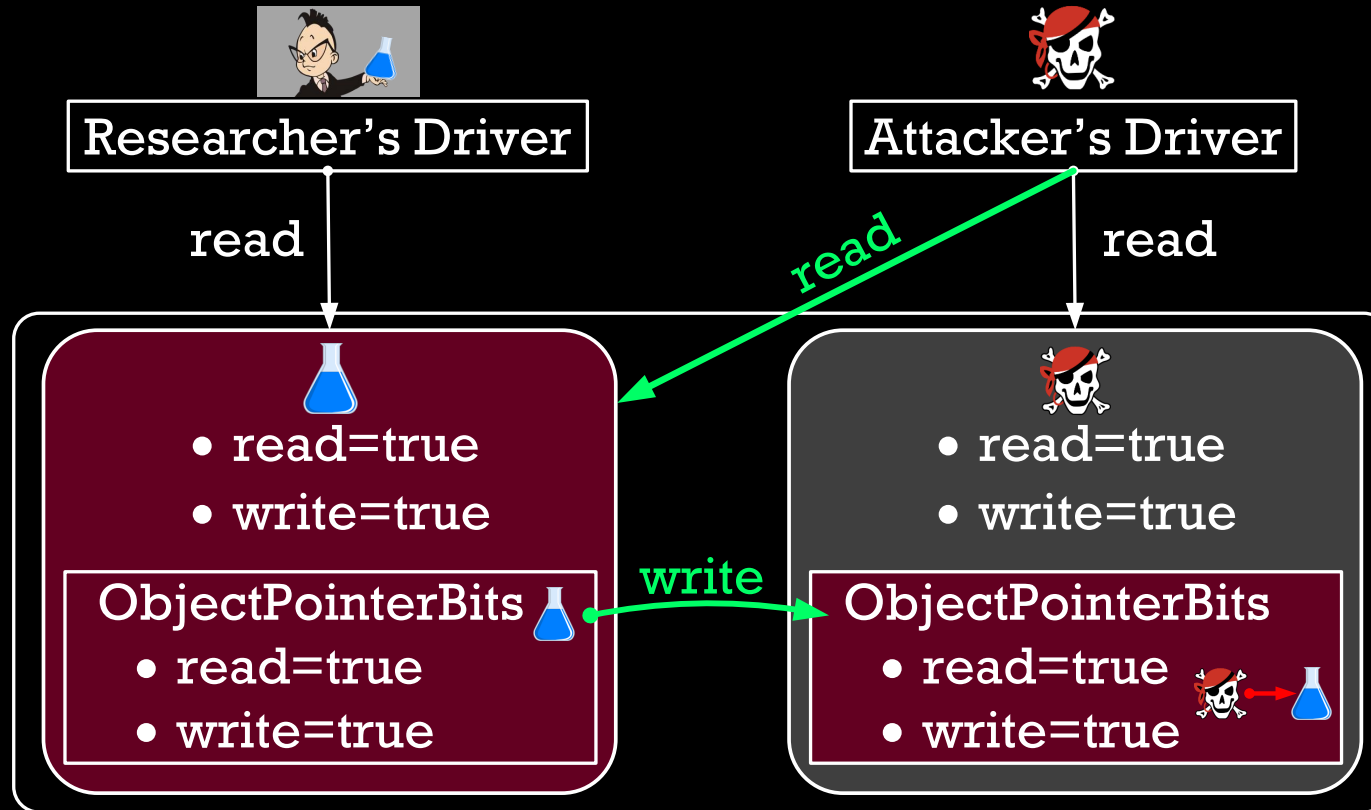
DEMO#1: HANDLE TABLE HIJACKING

The online version is here –

<https://www.youtube.com/embed/5NNSXfTRtiQ?vq=hd1440>

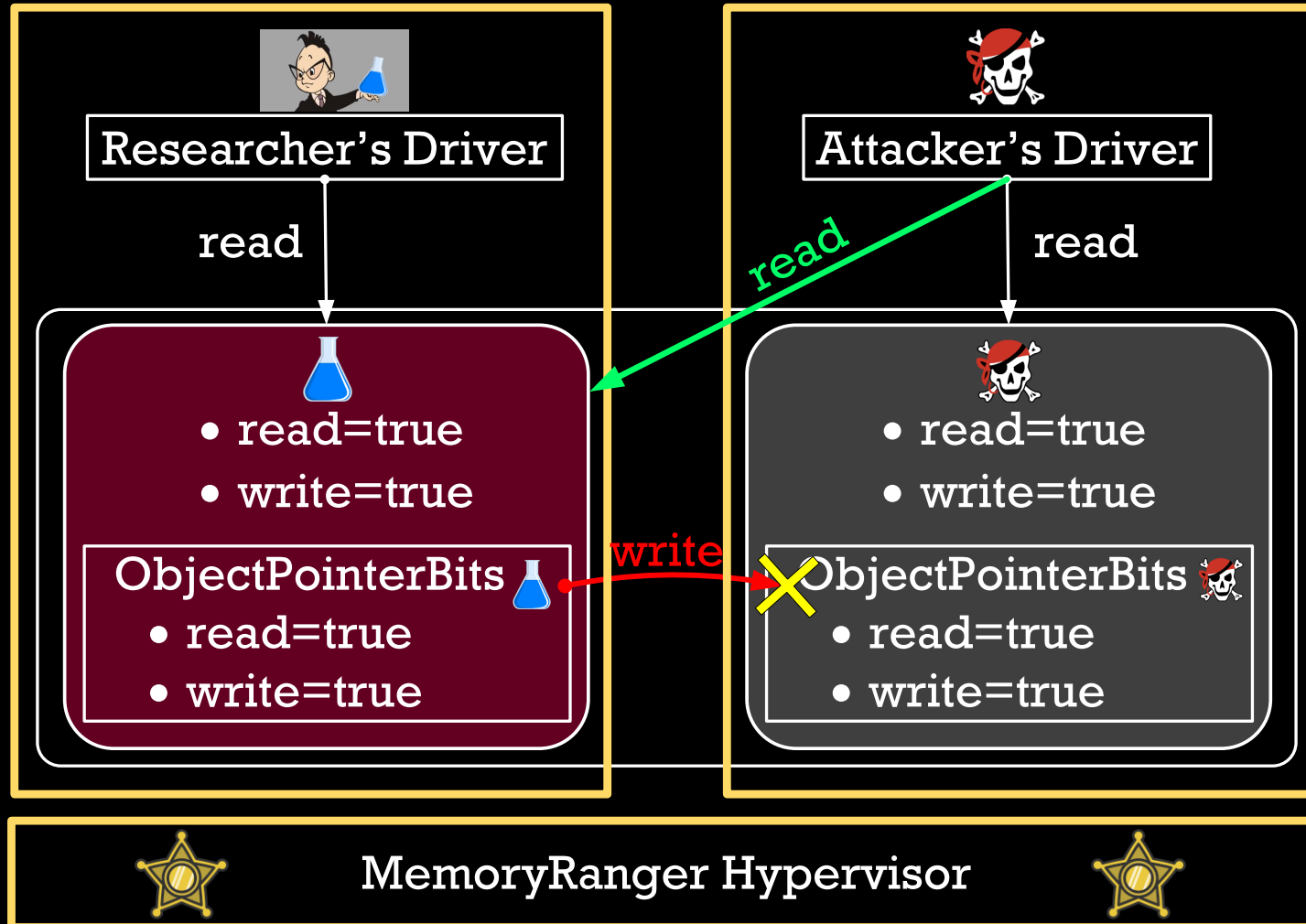
HOW TO PREVENT THE HANDLE HIJACKING?

- We have to block **WRITE** access to the ObjectPointerBits
- We have to grant **READ** access to the whole Handle Table for all drivers

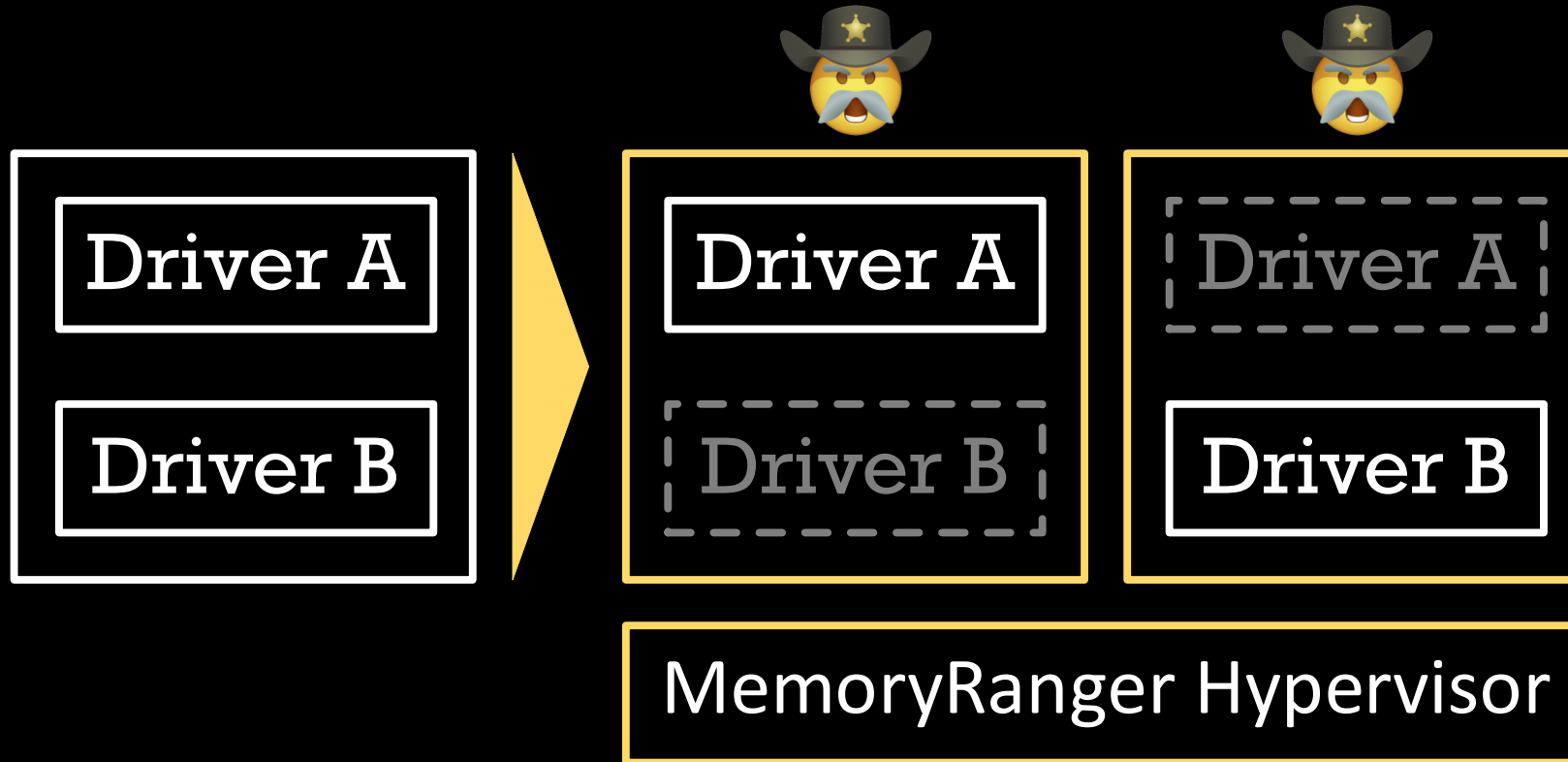


HOW TO PREVENT THE HANDLE HIJACKING?

- We have to block WRITE access to the ObjectPointerBits
- We have to grant READ access to the whole Handle Table for all drivers



MEMORYRANGER ISOLATES DRIVERS BY RUNNING DRIVERS IN SEPARATE KERNEL SPACES

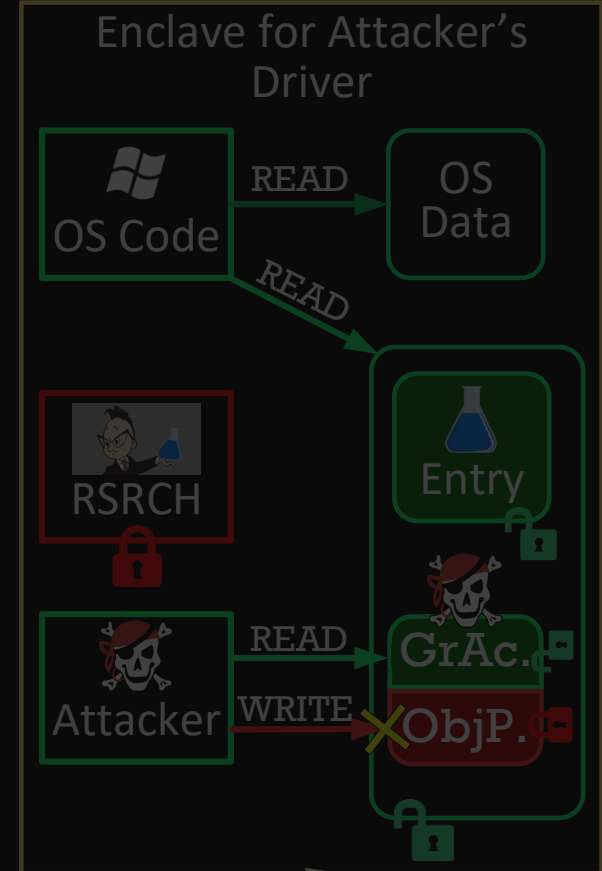
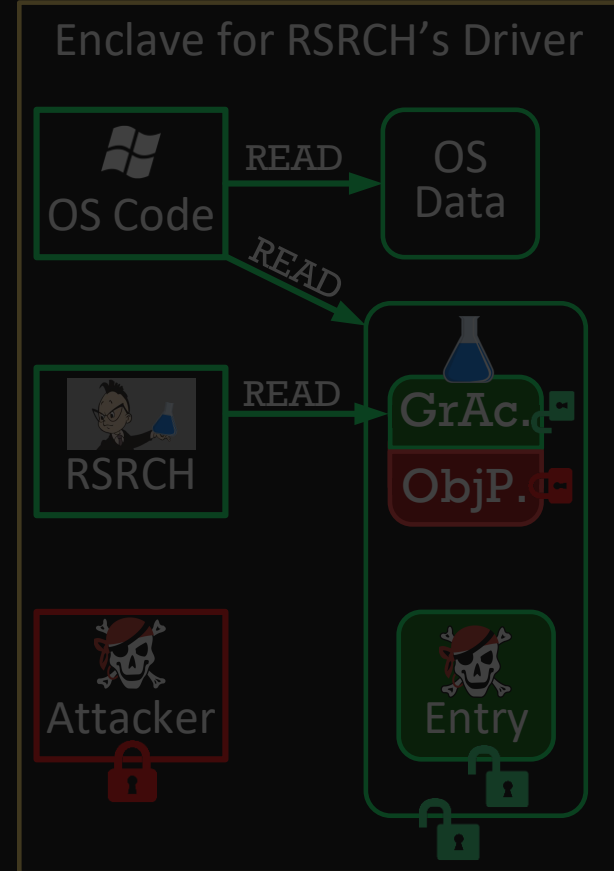
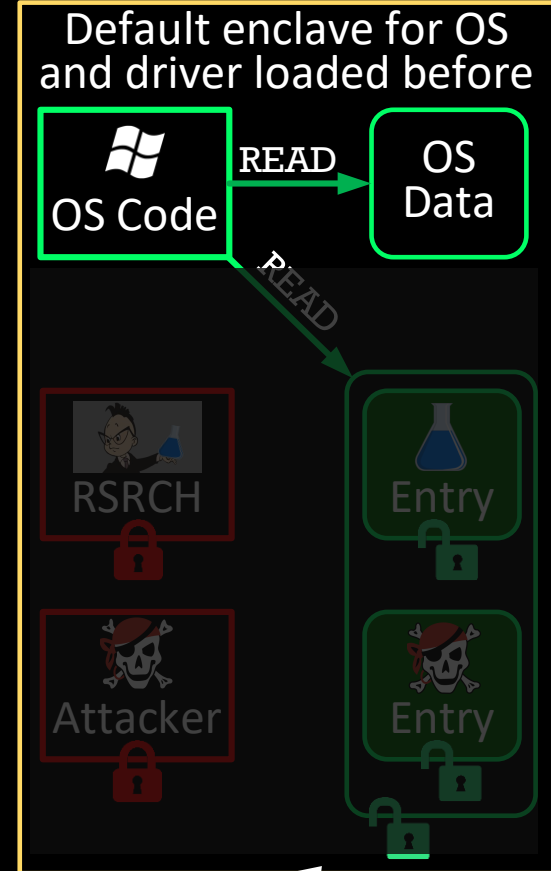
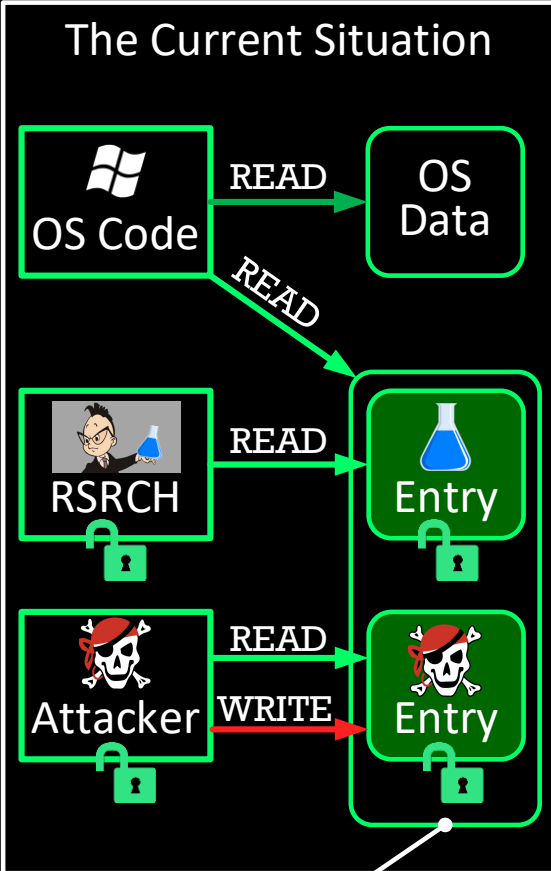


MemoryRanger and Enclaves details are here:

(2019) <https://igorkorkin.blogspot.com/2019/04/memoryranger-prevents-hijacking.html>

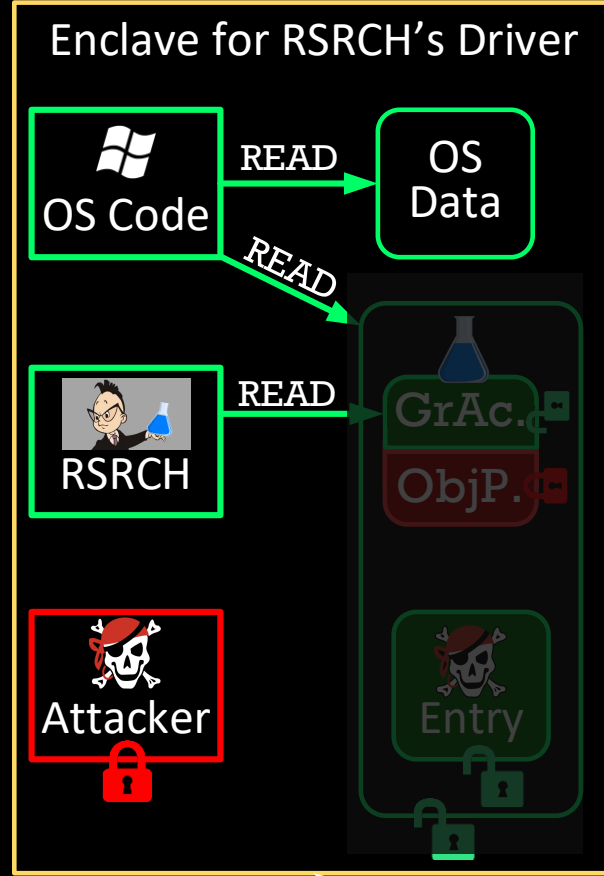
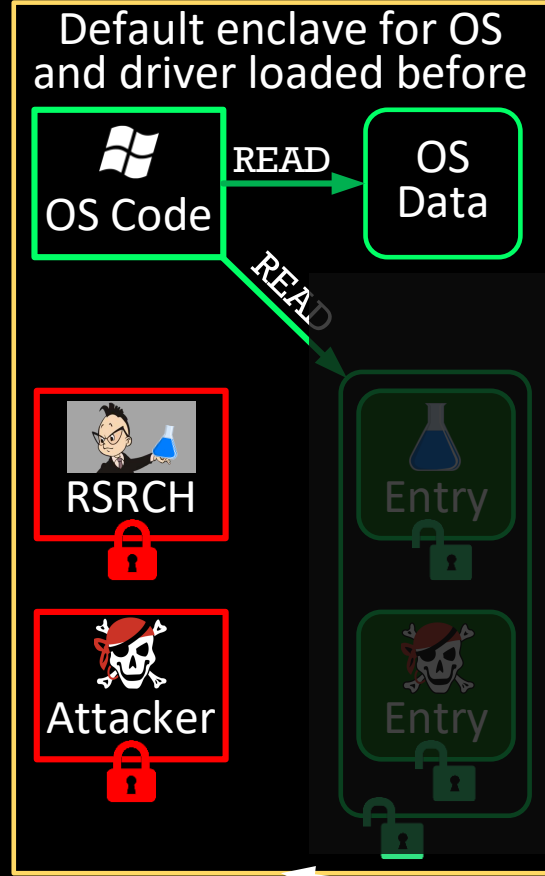
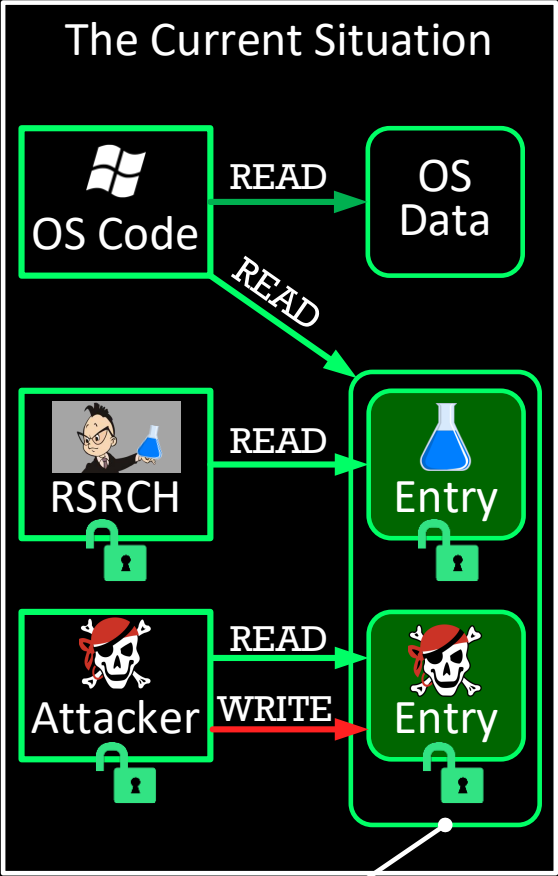
(2018) <https://igorkorkin.blogspot.com/2018/12/divide-et-impera-memoryranger-runs.html>

MEMORY MAP: MEMORYRANGER PREVENTS HANDLE HIJACKING



EPT pointer

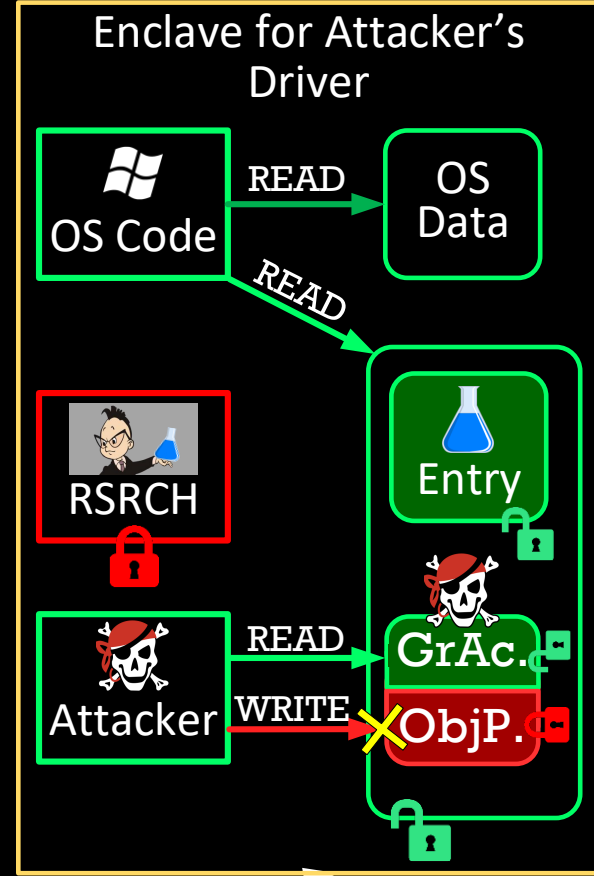
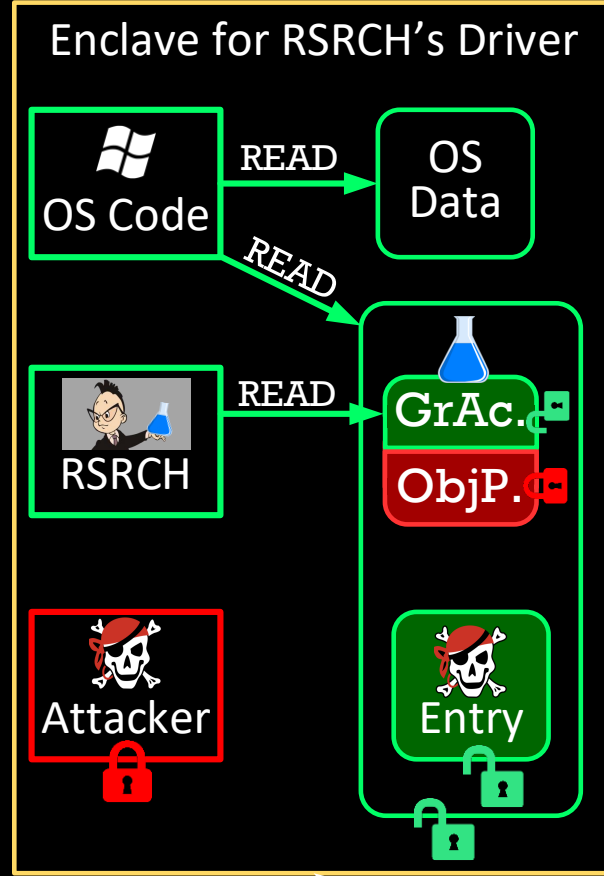
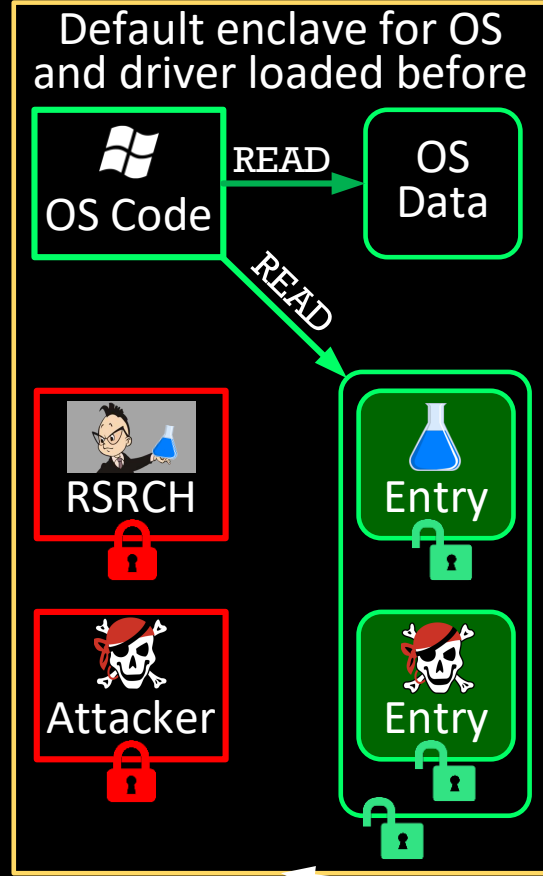
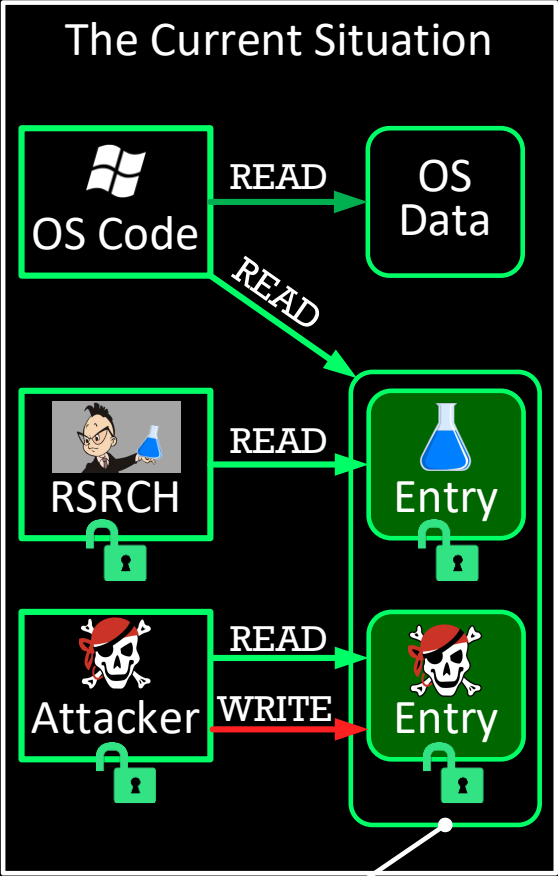
MEMORY MAP: MEMORYRANGER PREVENTS HANDLE HIJACKING



Kernel Handle Table

EPT pointer

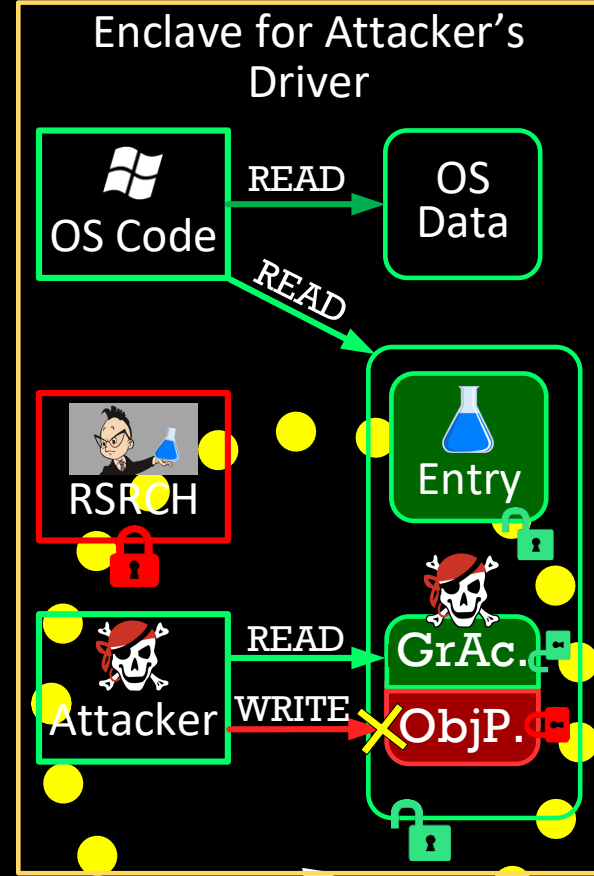
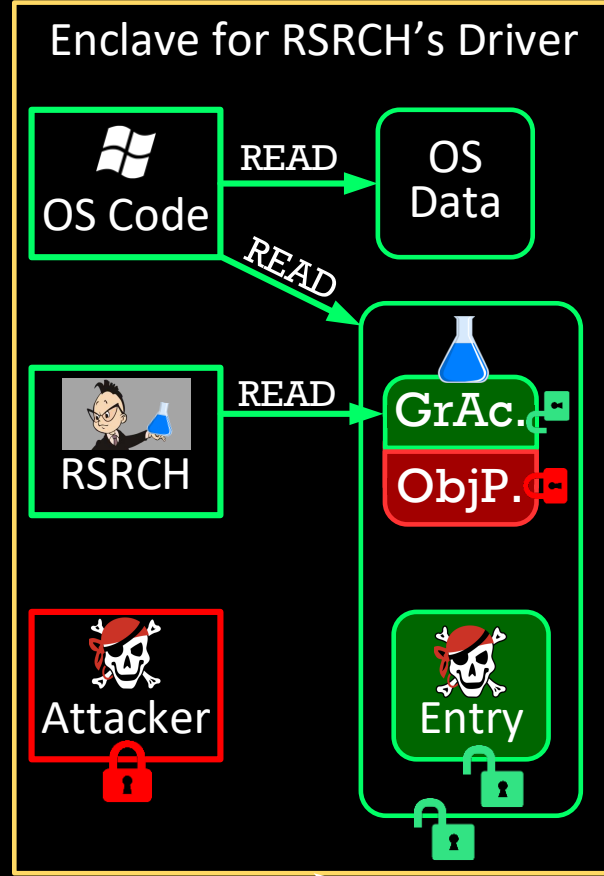
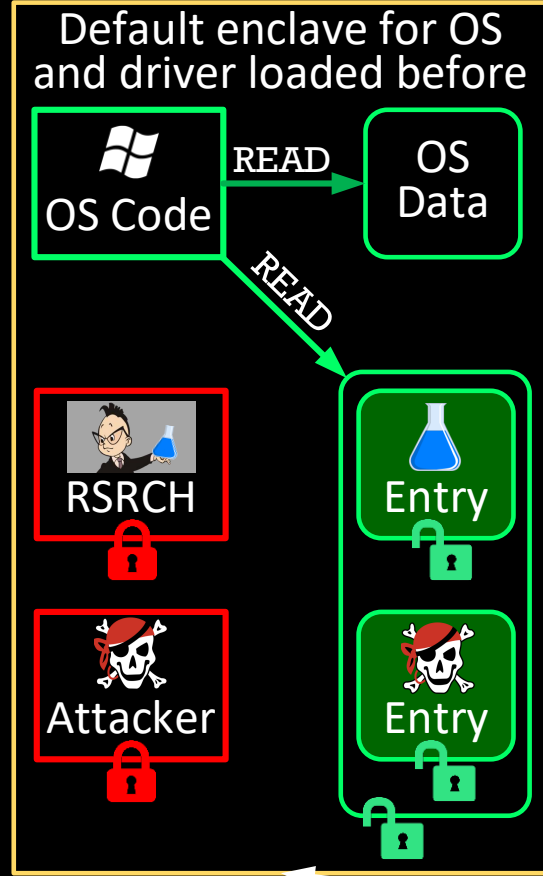
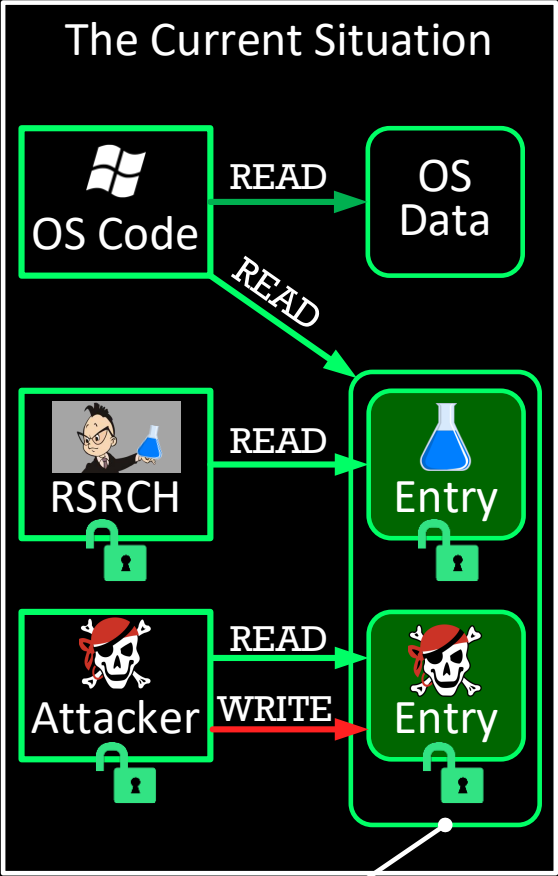
MEMORY MAP: MEMORYRANGER PREVENTS HANDLE HIJACKING



Kernel Handle Table

EPT pointer

MEMORY MAP: MEMORYRANGER PREVENTS HANDLE HIJACKING



Kernel Handle Table

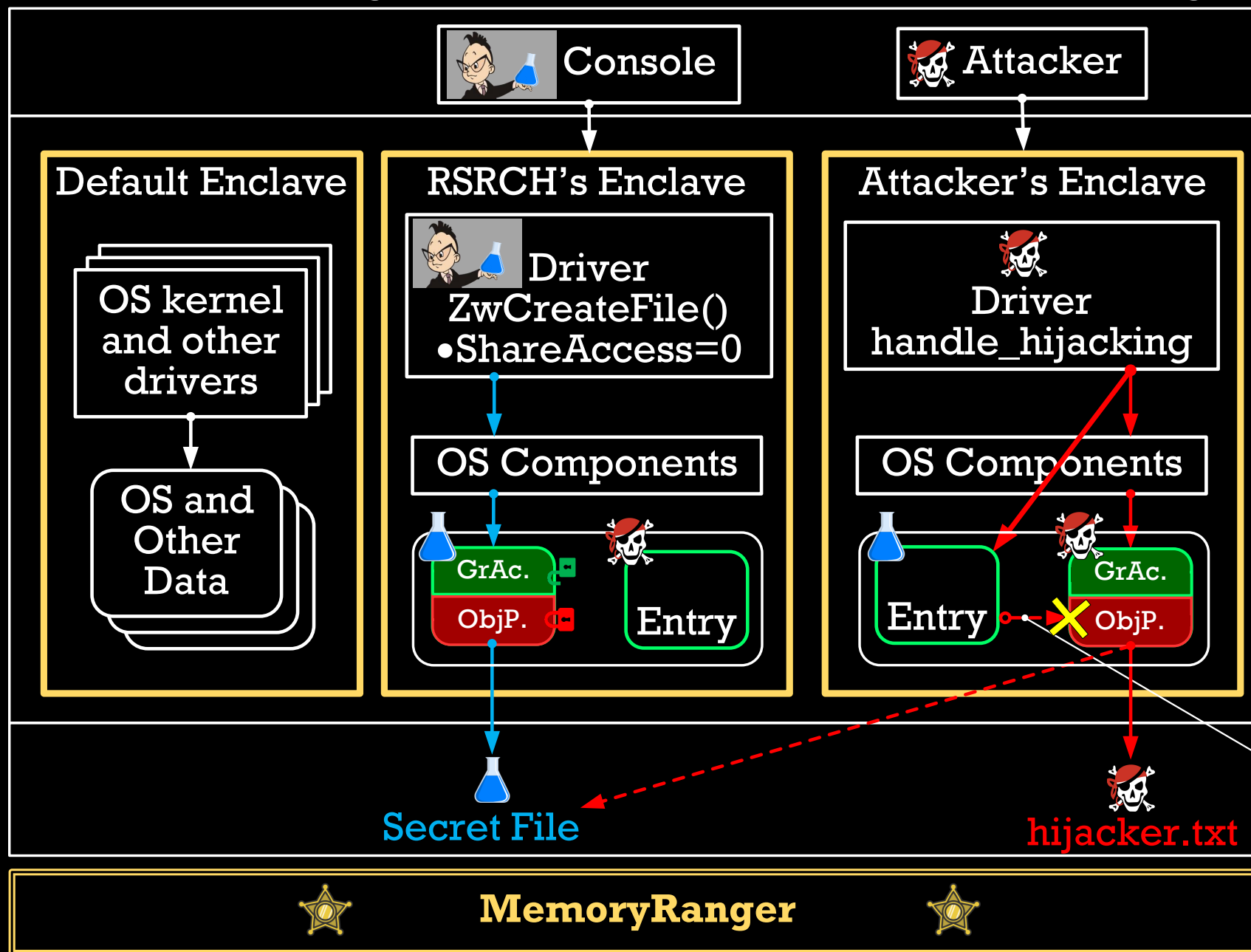
EPT pointer

DEMO#2: PREVENTION OF HANDLE TABLE HIJACKING

The online version is here –

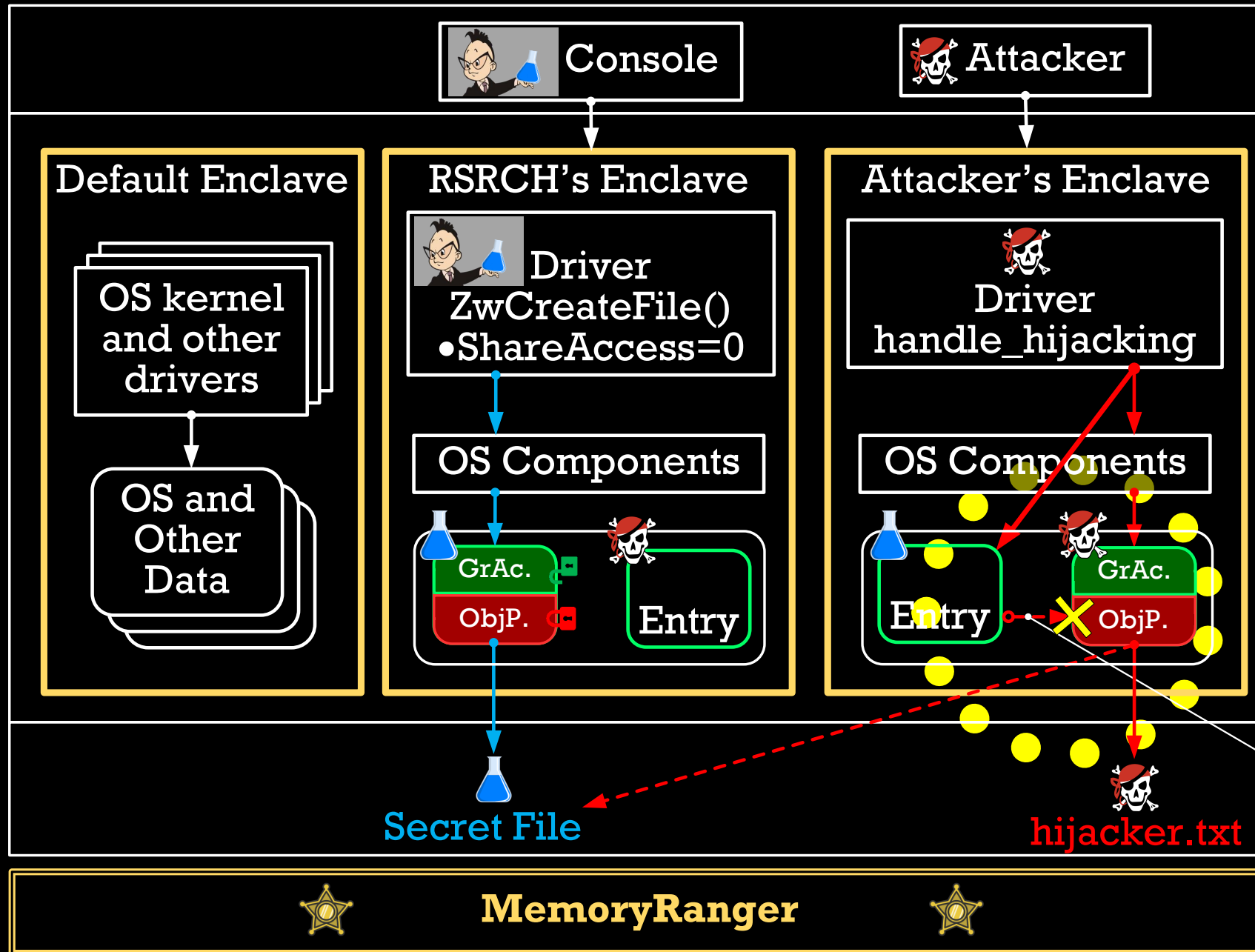
<https://www.youtube.com/embed/5Pz-IXvQDiY?vq=hd1440>

MemoryRanger Prevents the Handle Hijacking



MemoryRanger restricts WRITE access to the ObjectPointerBits field

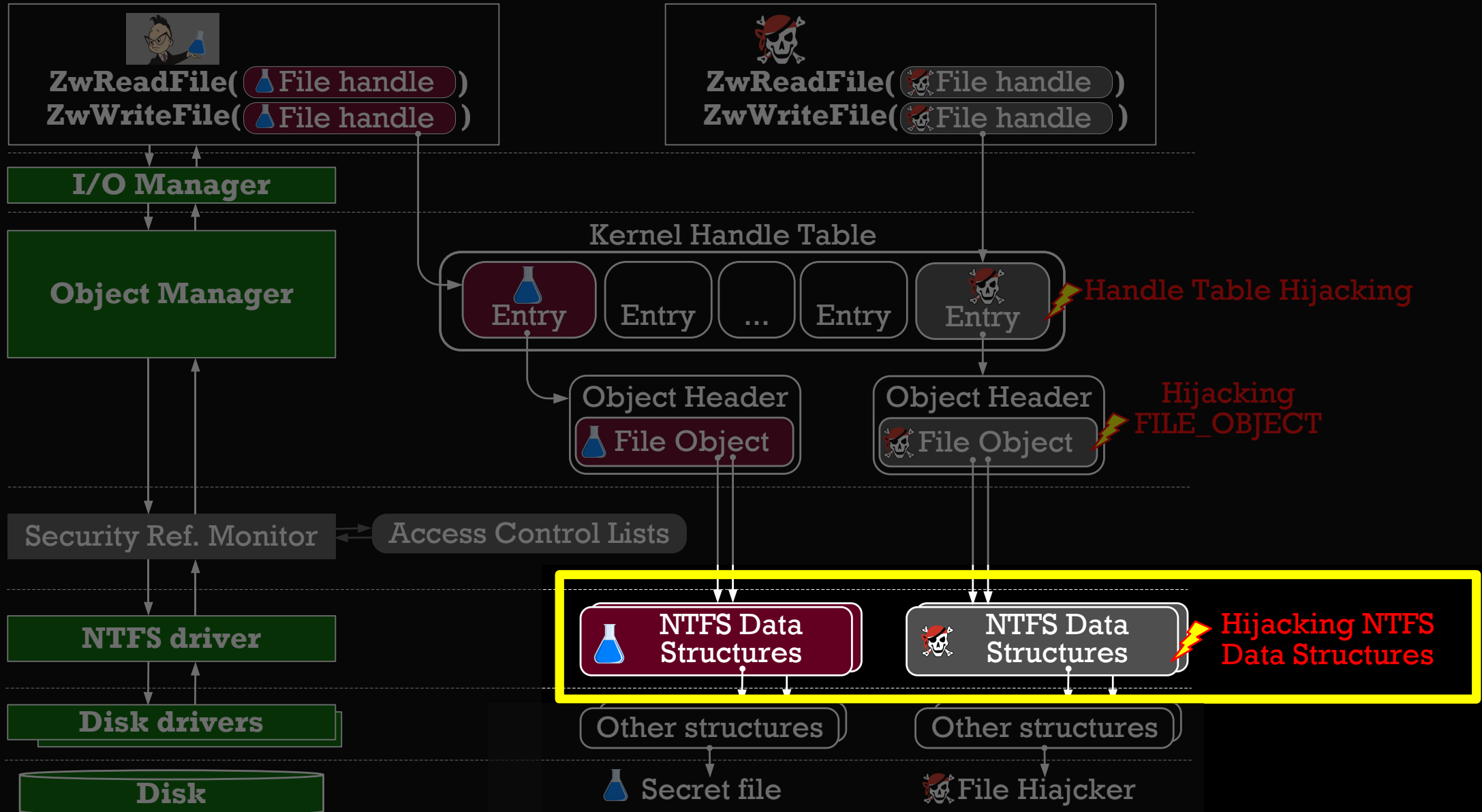
MemoryRanger Prevents the Handle Hijacking



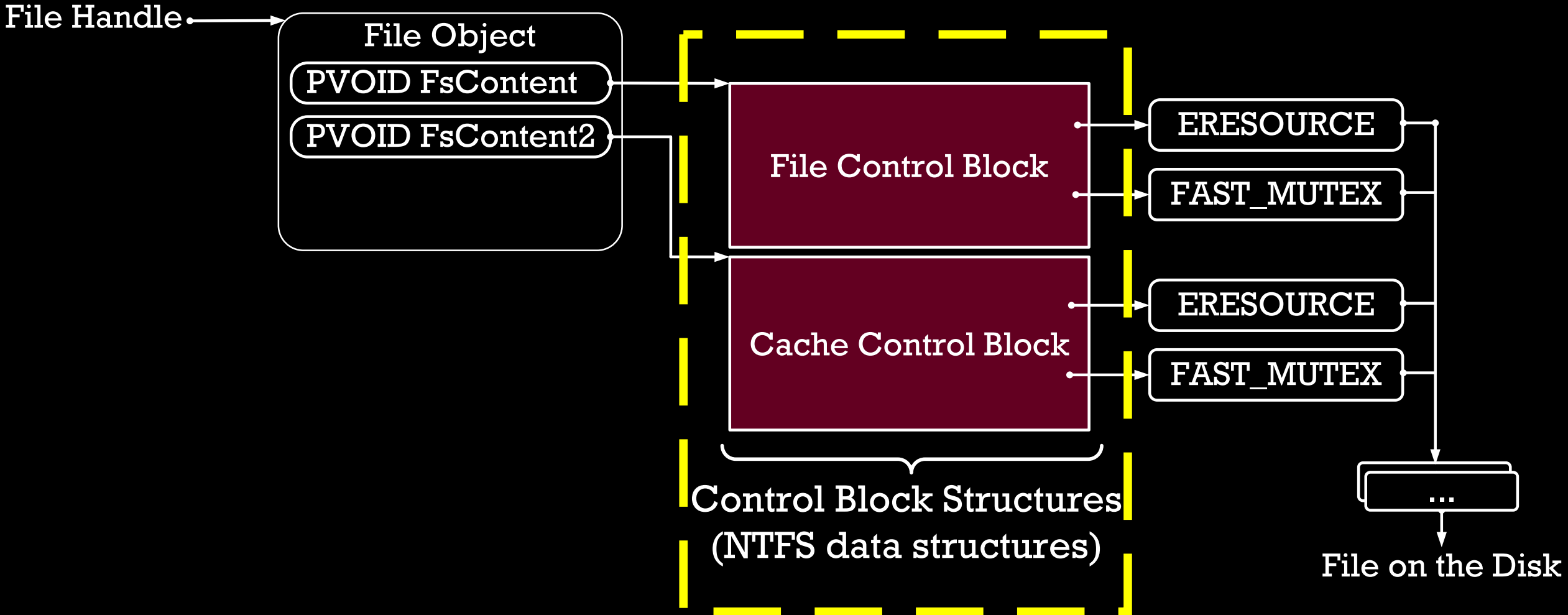
MemoryRanger restricts WRITE access to the ObjectPointerBits field

HIJACKING NTFS DATA STRUCTURES

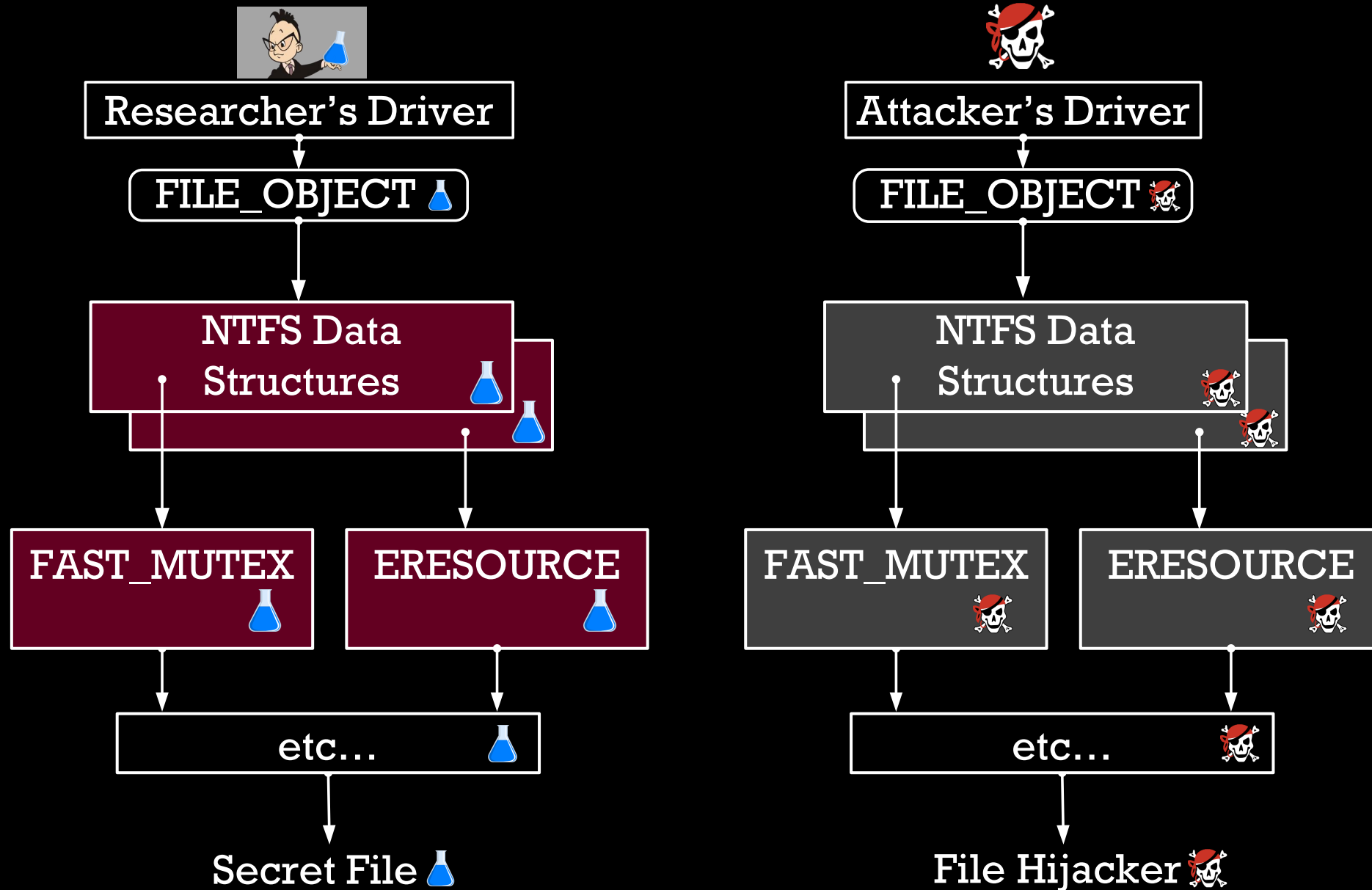
HIJACKING ATTACKS ON FILES STRUCTURES



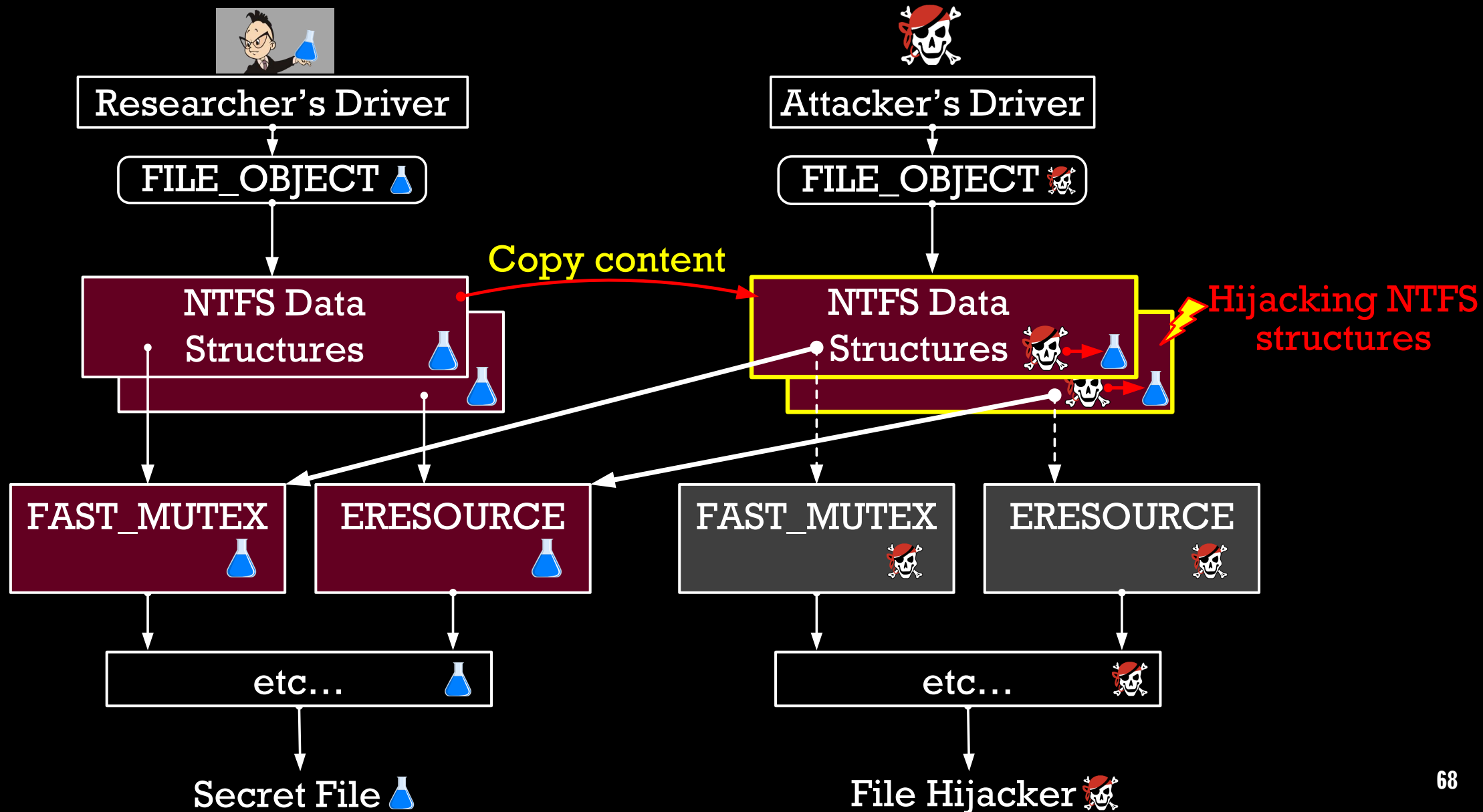
NTFS DATA STRUCTURES



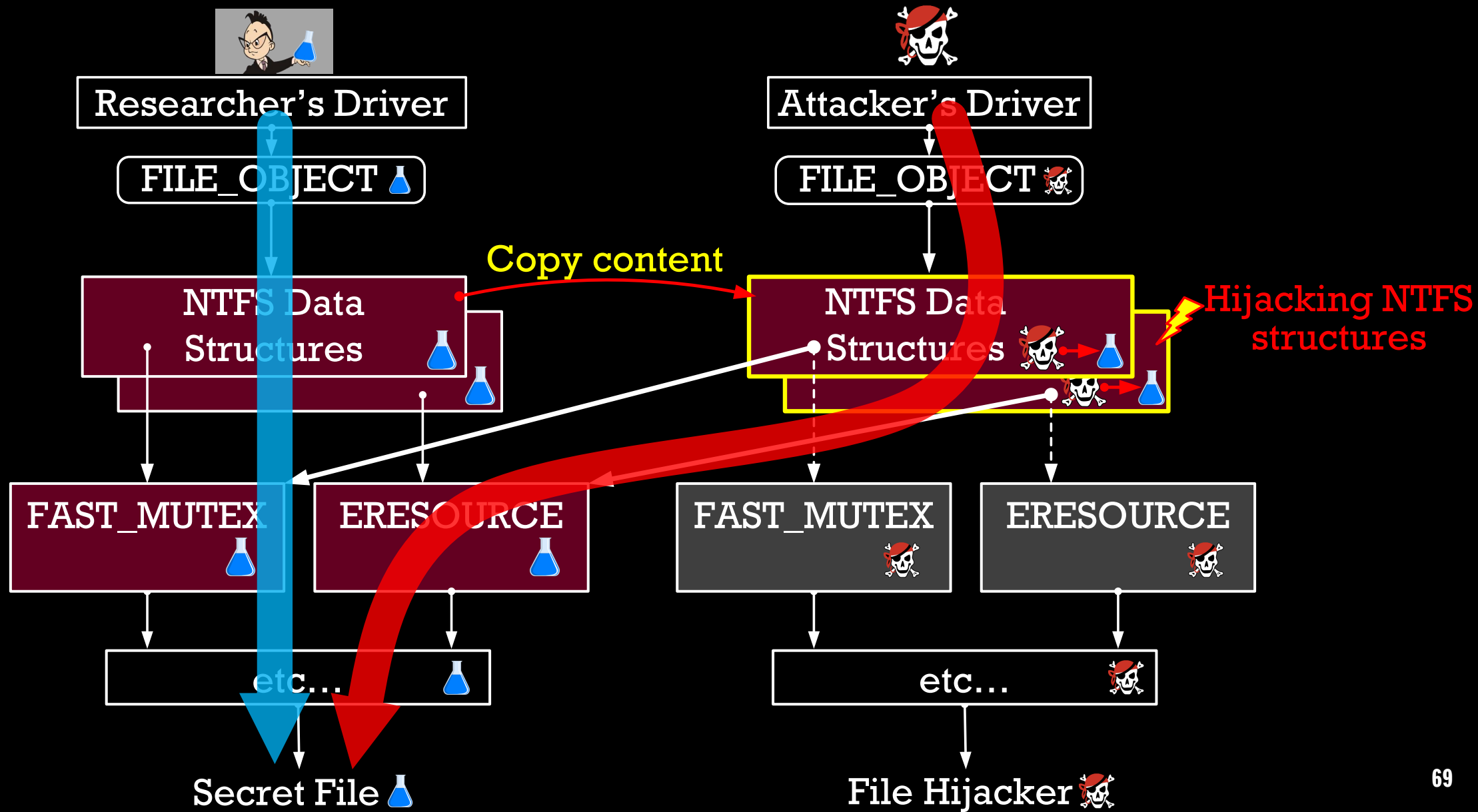
HIJACKING NTFS STRUCTURES



HIJACKING NTFS STRUCTURES



HIJACKING NTFS STRUCTURES



BSOD - RESOURCE_NOT_OWNED (0xE3)



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

60% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:
Stop code: RESOURCE NOT OWNED

BSOD: THE REASON AND THE WAY TO BYPASS

```
void ExReleaseResourceLite(PERESOURCE Resource){  
    ...  
    CurrentThread = KeGetCurrentThread();  
    if (IsOwnedExclusive(Resource)) {  
        if (Resource->OwnerThreads[0].OwnerThread != CurrentThread) {  
            KeBugCheckEx(RESOURCE_NOT_OWNED, ... )  
        }  
    }  
}
```

BSOD: THE REASON AND THE WAY TO BYPASS

```
void ExReleaseResourceLite(PERESOURCE Resource){
```

```
...
```

```
CurrentThread = KeGetCurrentThread();
```

```
if (IsOwnedExclusive(Resource)) {
```

```
    if (Resource->OwnerThreads[0].OwnerThread != CurrentThread) {
```

```
        KeBugCheckEx(RESOURCE_NOT_OWNED, ... )
```

```
    }
```

```
}
```

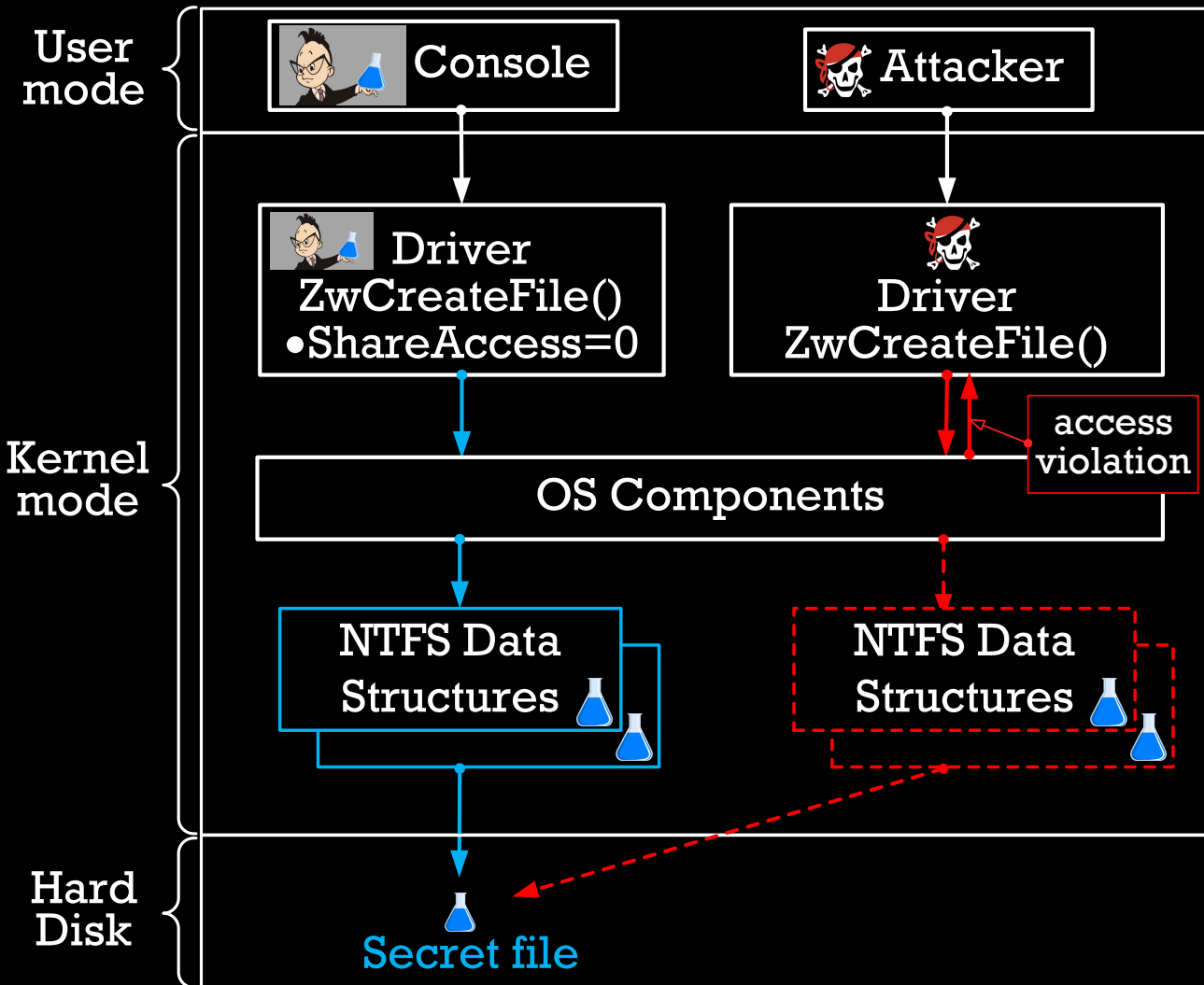
```
}
```


BSOD: THE WAY TO BYPASS (FOR HACKERS ONLY)

1. Overwrite control block structures
2. Patch ThreadID-related fields using attackers ThreadID:
 - `Resource->OwnerEntry.OwnerThread = PsGetCurrentThread();`
 - `PagingIoResource->OwnerEntry.OwnerThread = PsGetCurrentThread();`
3. Repeat steps 1 and 2 before each read and write call

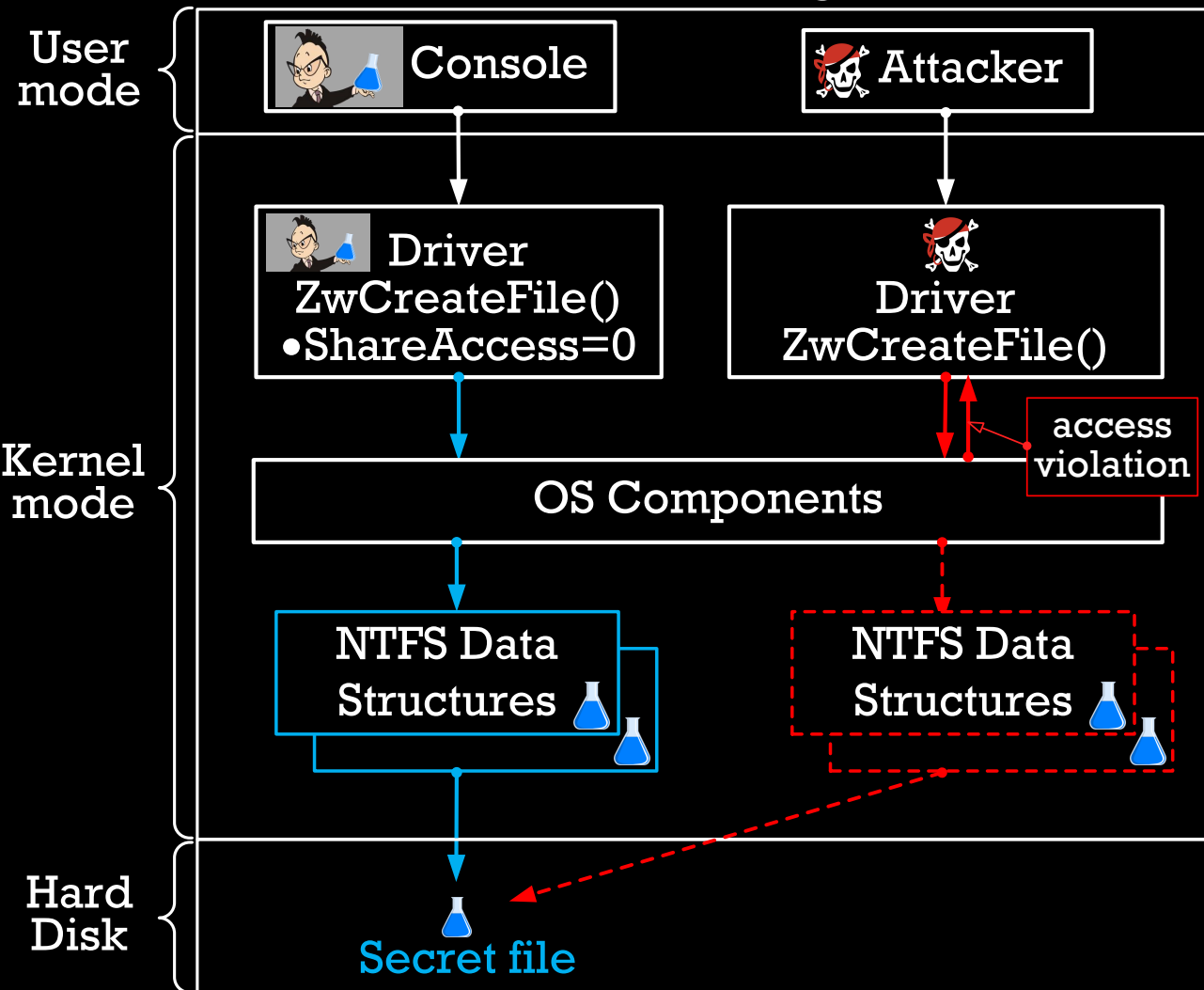
DEMO: HIJACKING NTFS STRUCTURES

Attempt 1: The Legal Access

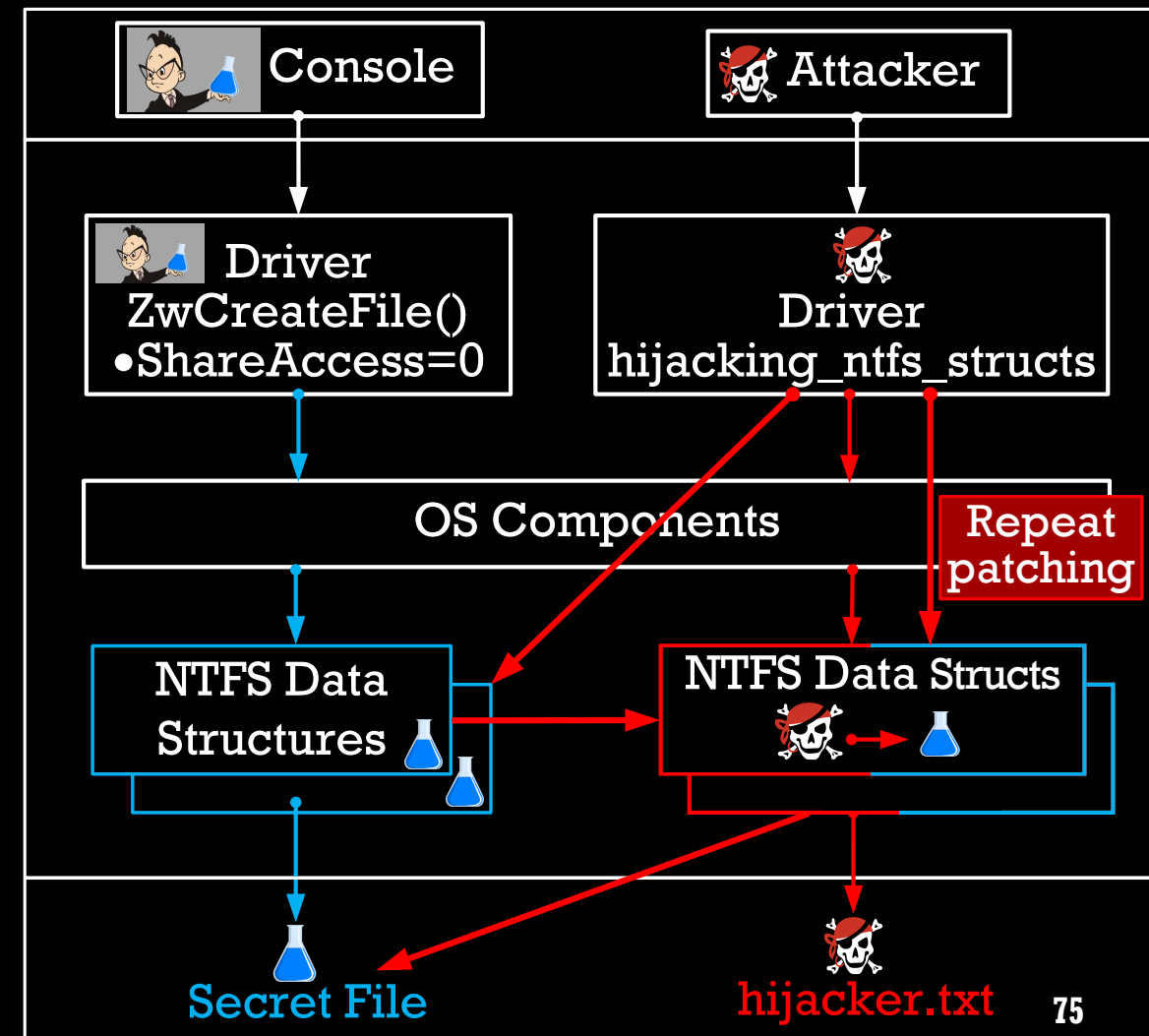


DEMO: HIJACKING NTFS STRUCTURES

Attempt 1: The Legal Access



Attempt 2: Hijacking NTFS structures

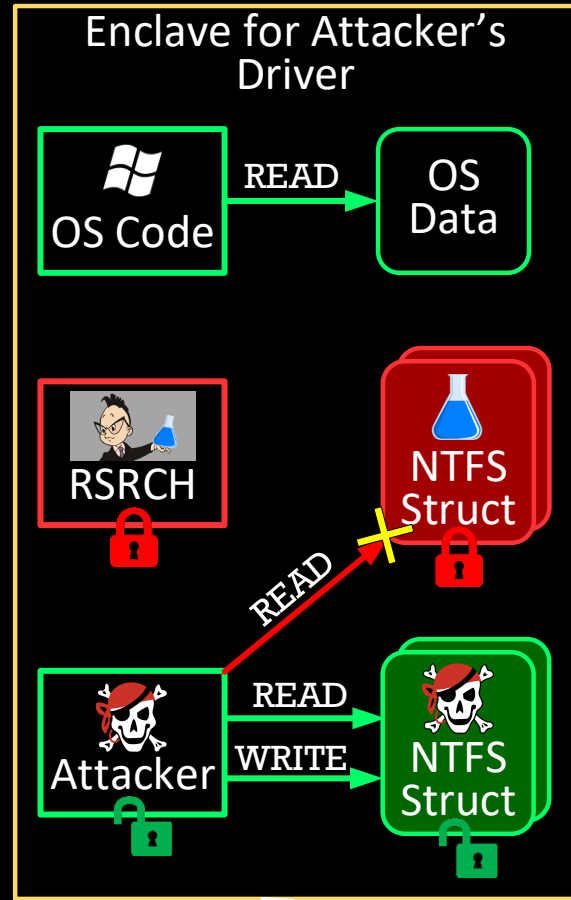
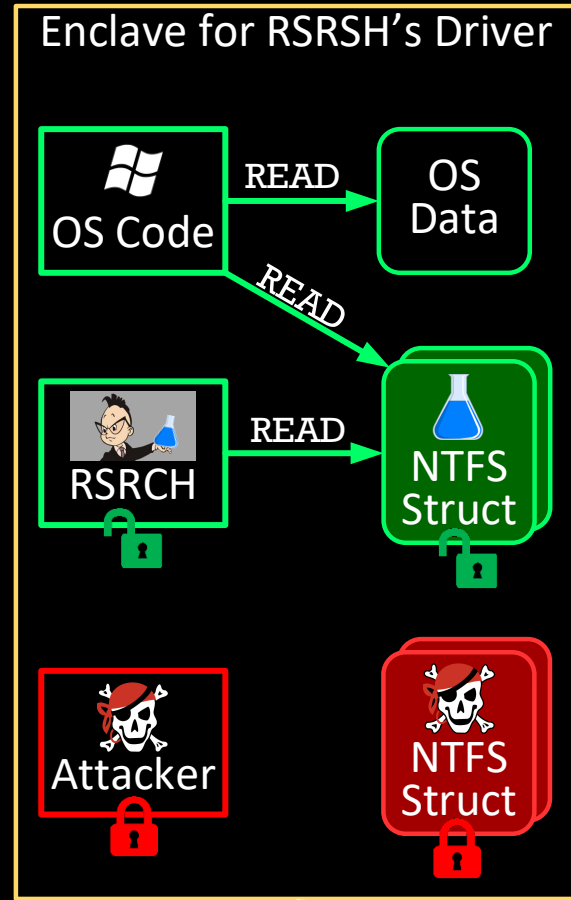
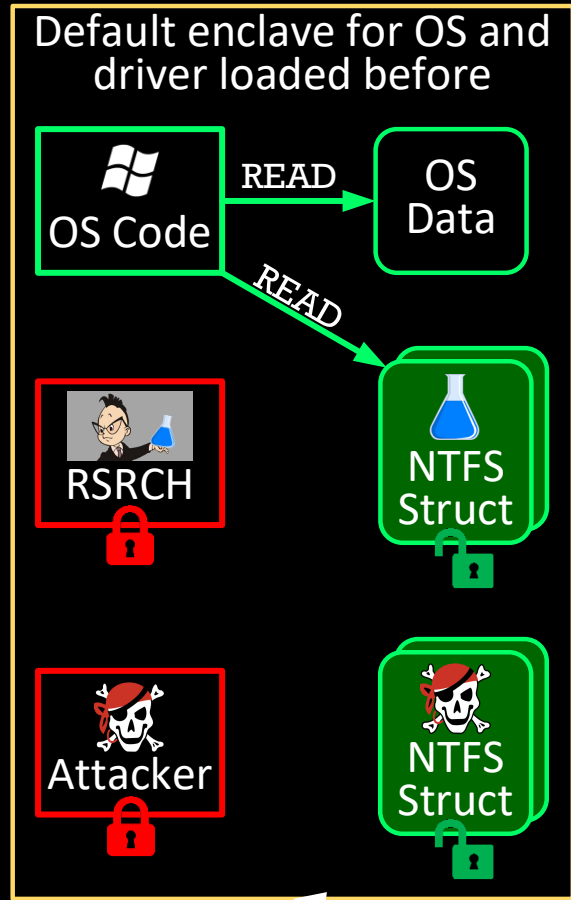
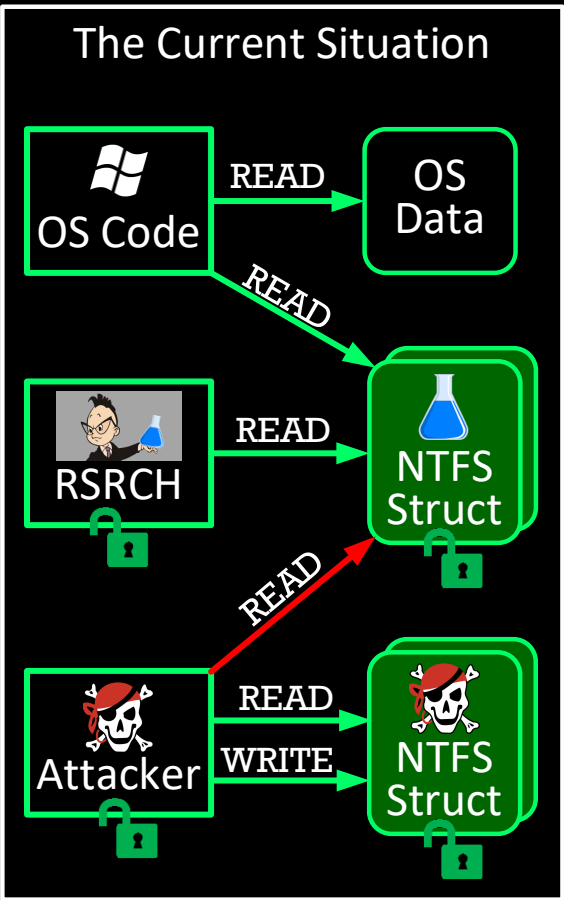


DEMO#3: HIJACKING NTFS STRUCTURES

The online version is here –

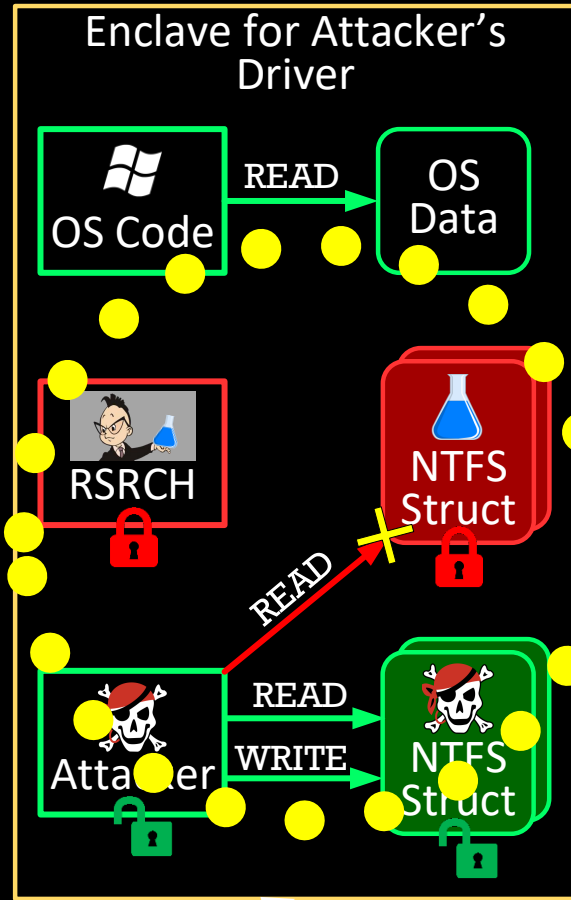
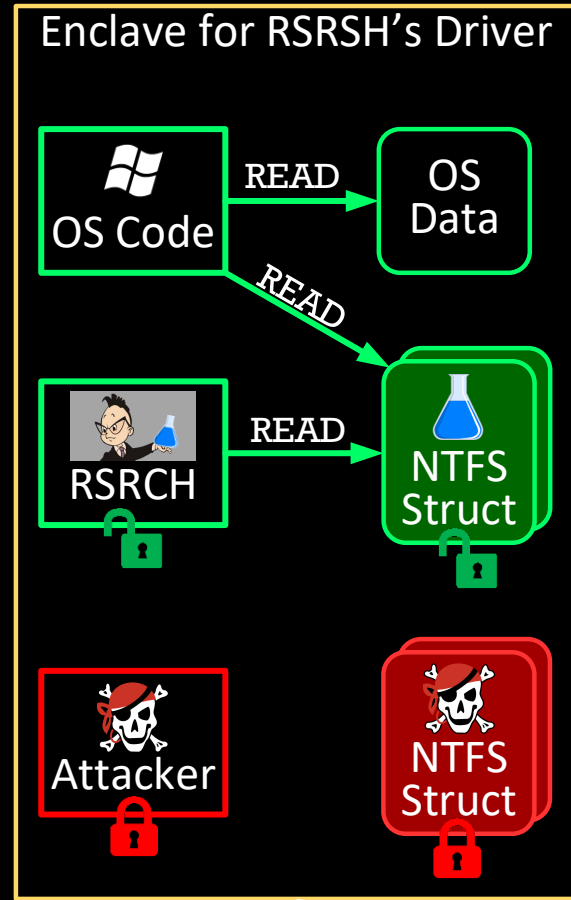
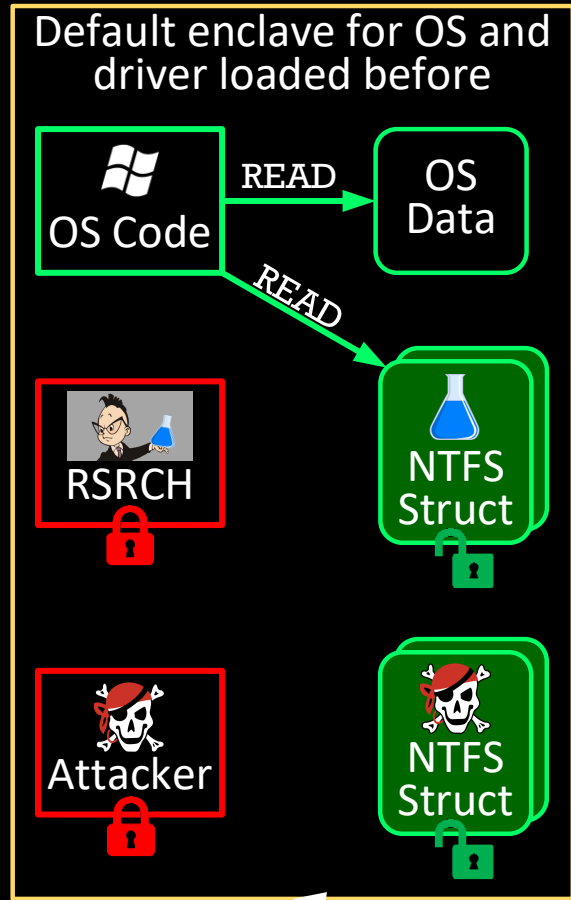
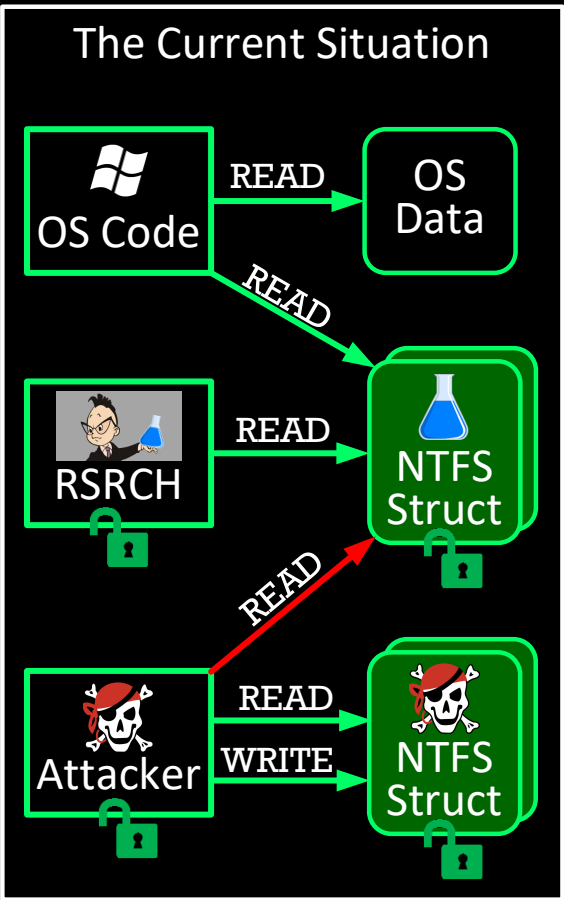
<https://www.youtube.com/embed/bHEf2fNkqbc?vq=hd1440>

MEMORYRANGER PREVENTS HIJACKING NTFS STRUCTS



EPT pointer

MEMORYRANGER PREVENTS HIJACKING NTFS STRUCTS



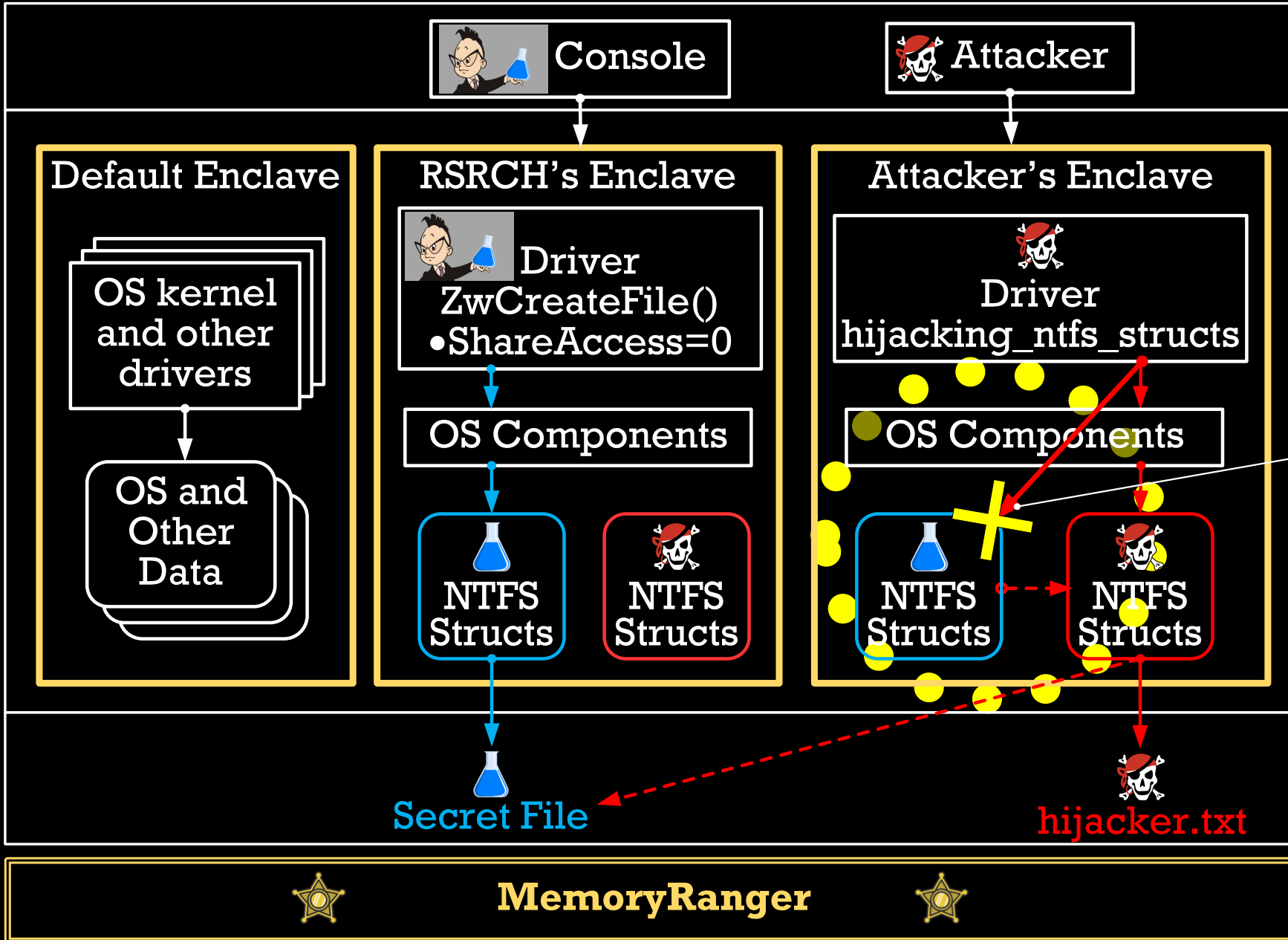
EPT pointer

DEMO#4: PREVENTION OF HIJACKING NTFS STRUCTS

The online version is here –

<https://www.youtube.com/embed/CSvq-VyxFH4?vq=hd1440>

Preventing the Hijacking NTFS structures

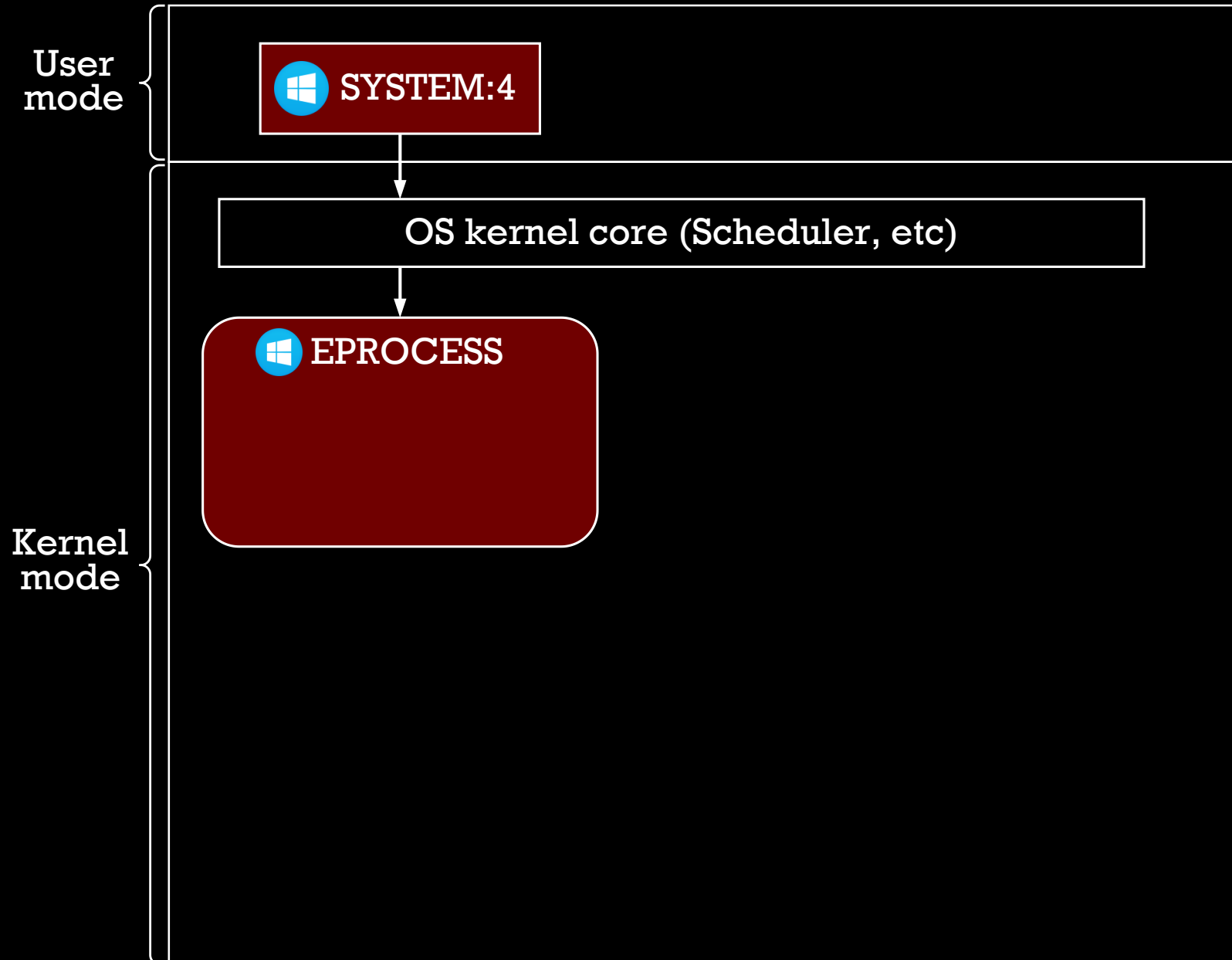


MemoryRanger prevents Hijacking NTFS structures

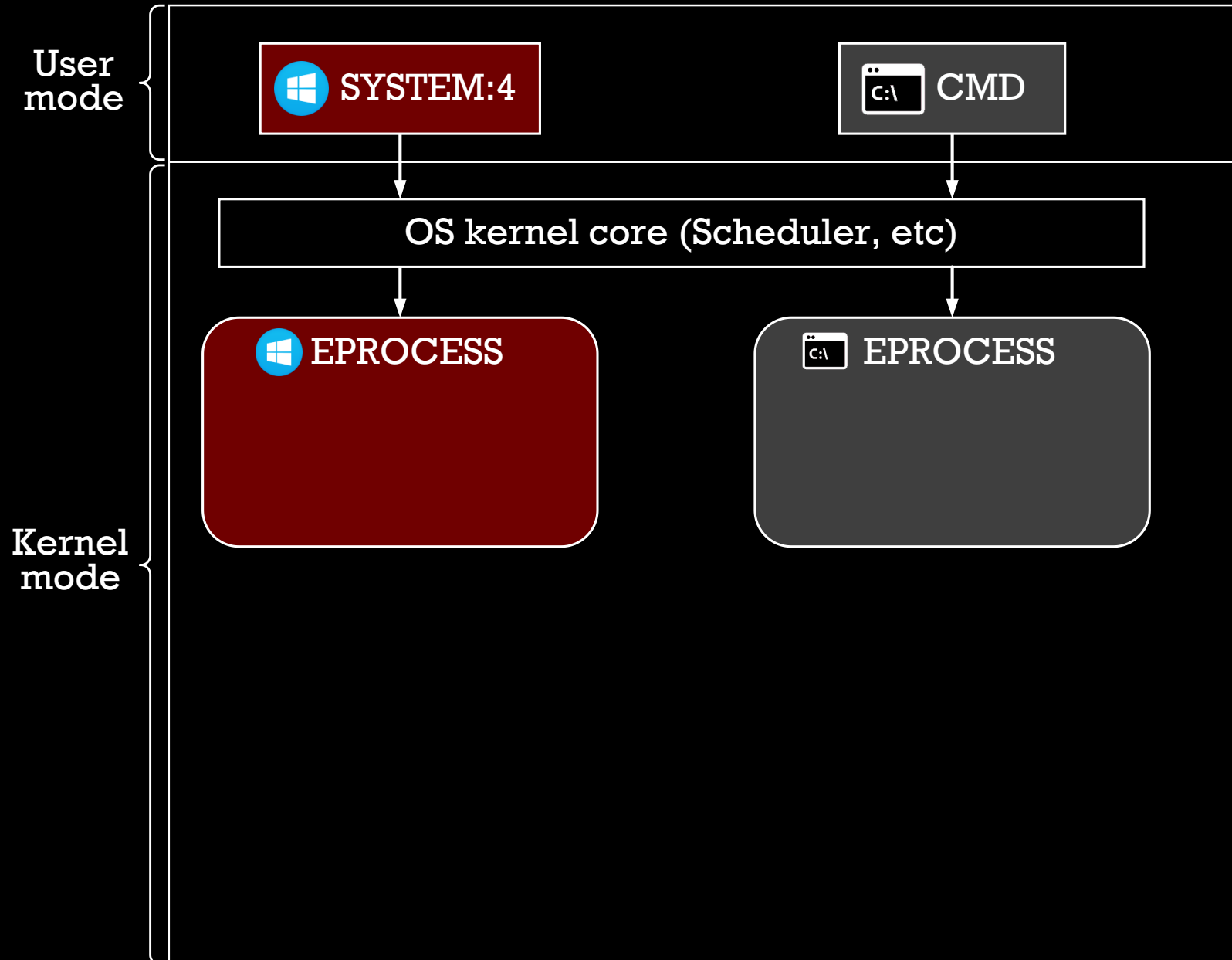
Episode 2

Privilege Escalation via Token Hijacking

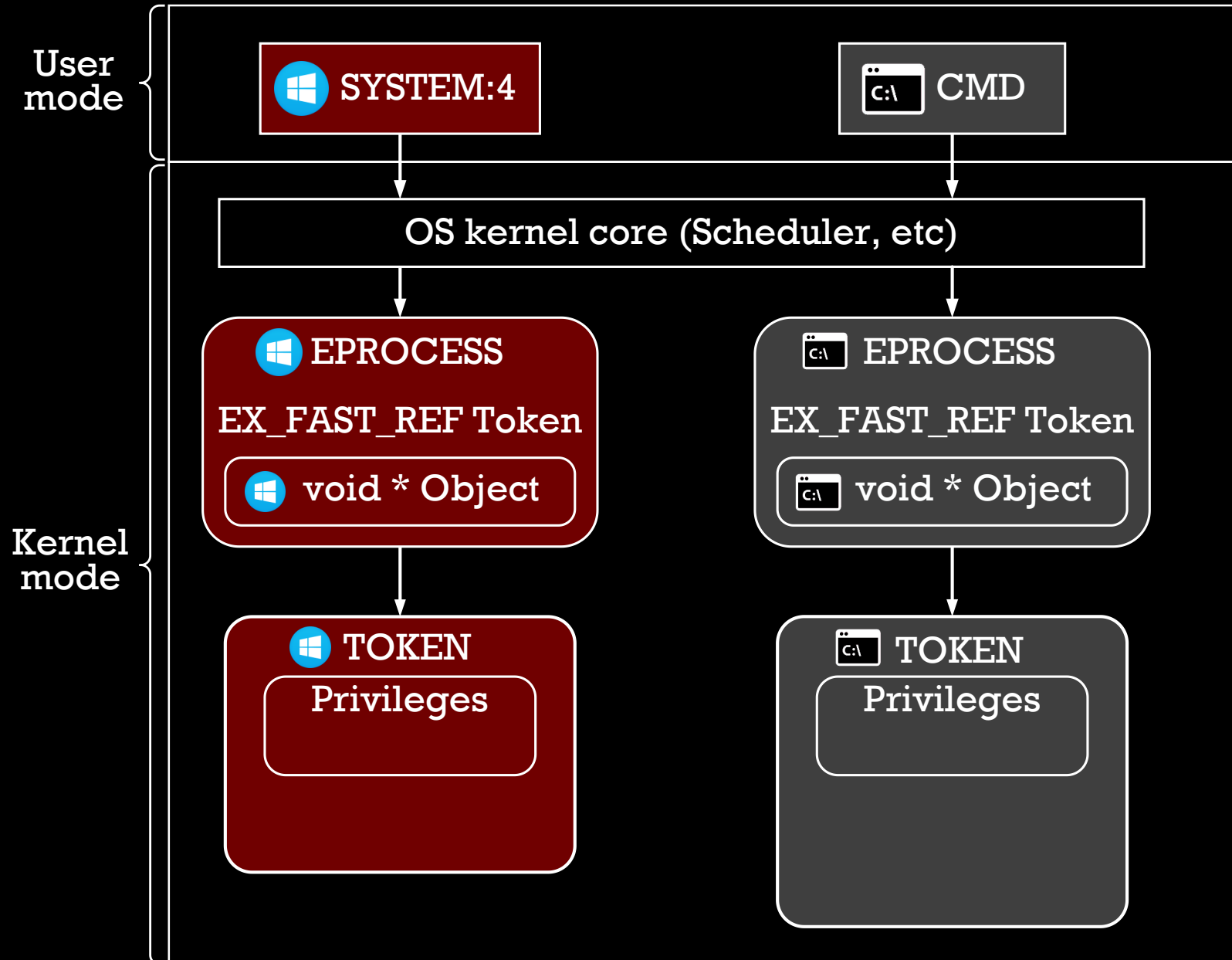
EPROCESS AND TOKEN IN WINDOWS



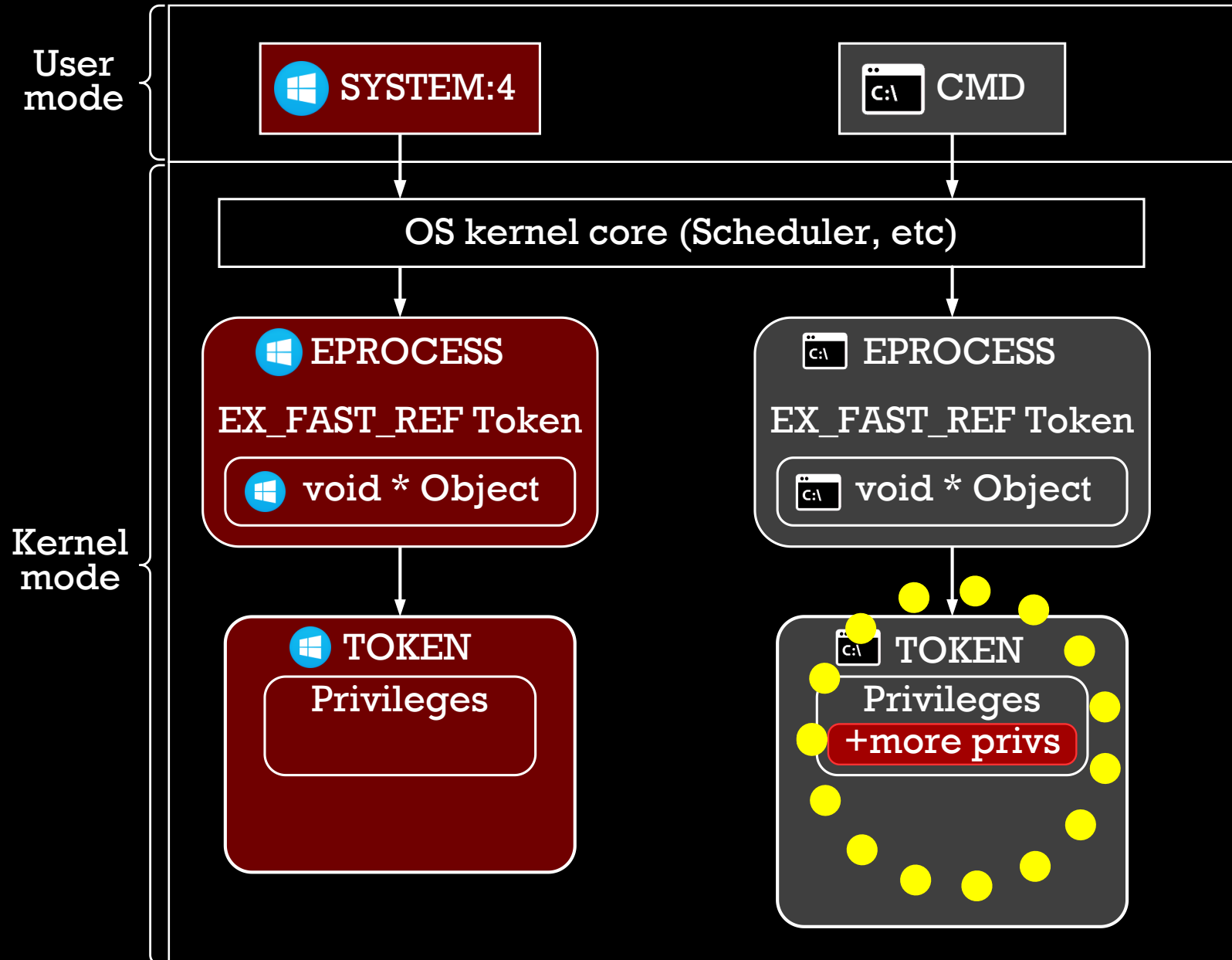
EPROCESS AND TOKEN IN WINDOWS



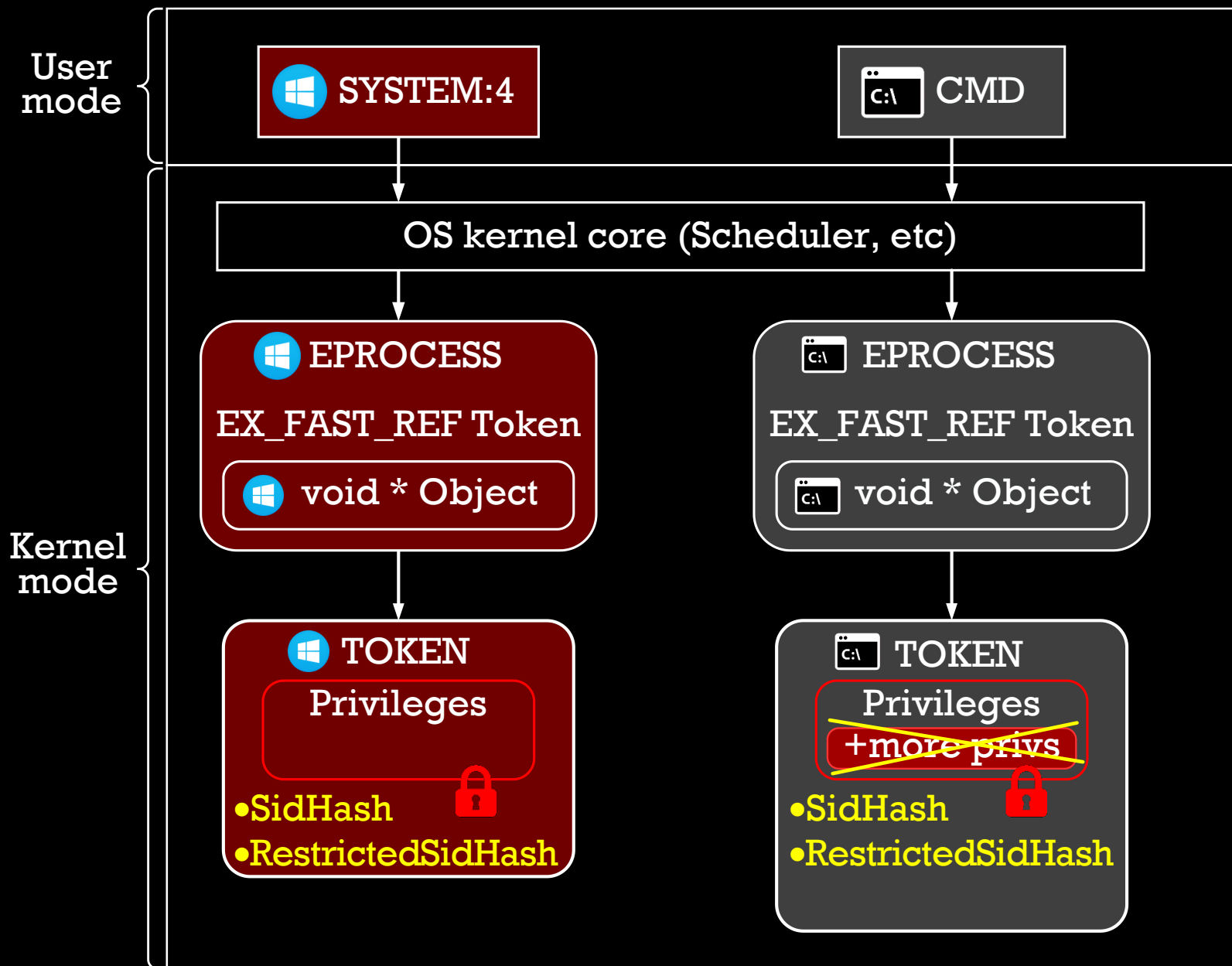
EPROCESS AND TOKEN IN WINDOWS



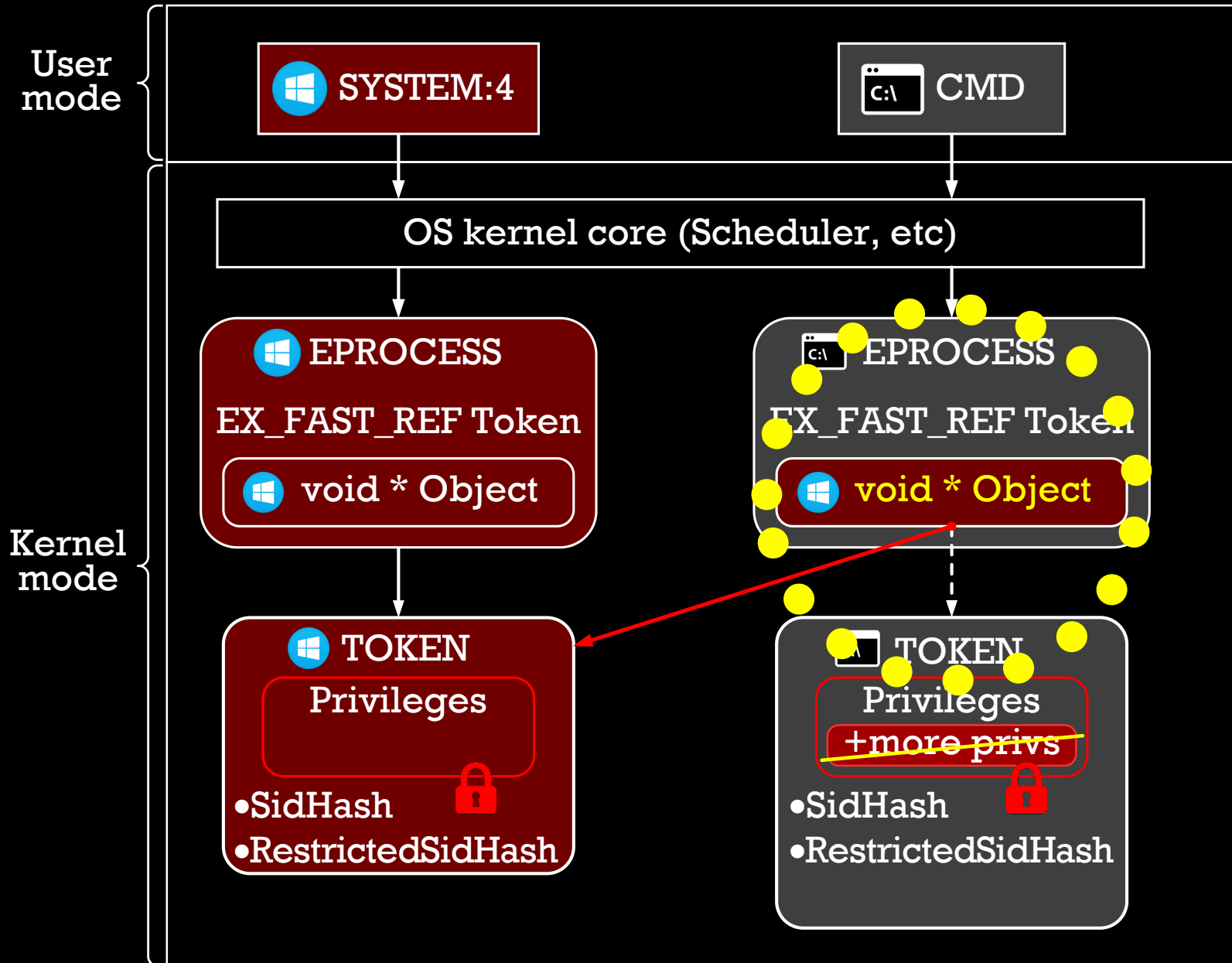
EPROCESS AND TOKEN IN WINDOWS: ADD MORE PRIVILEGES



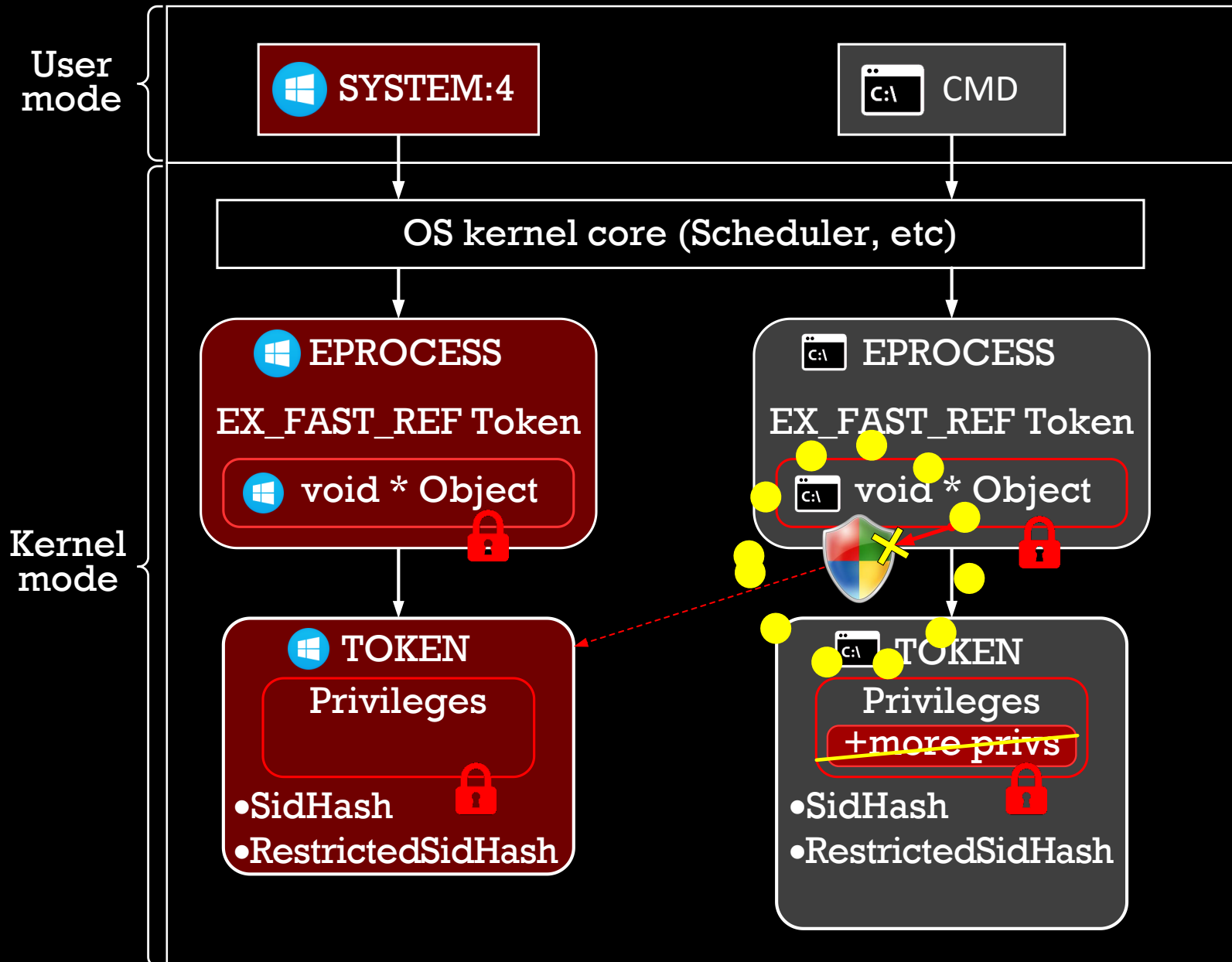
EPROCESS AND TOKEN IN WINDOWS: SidHash field



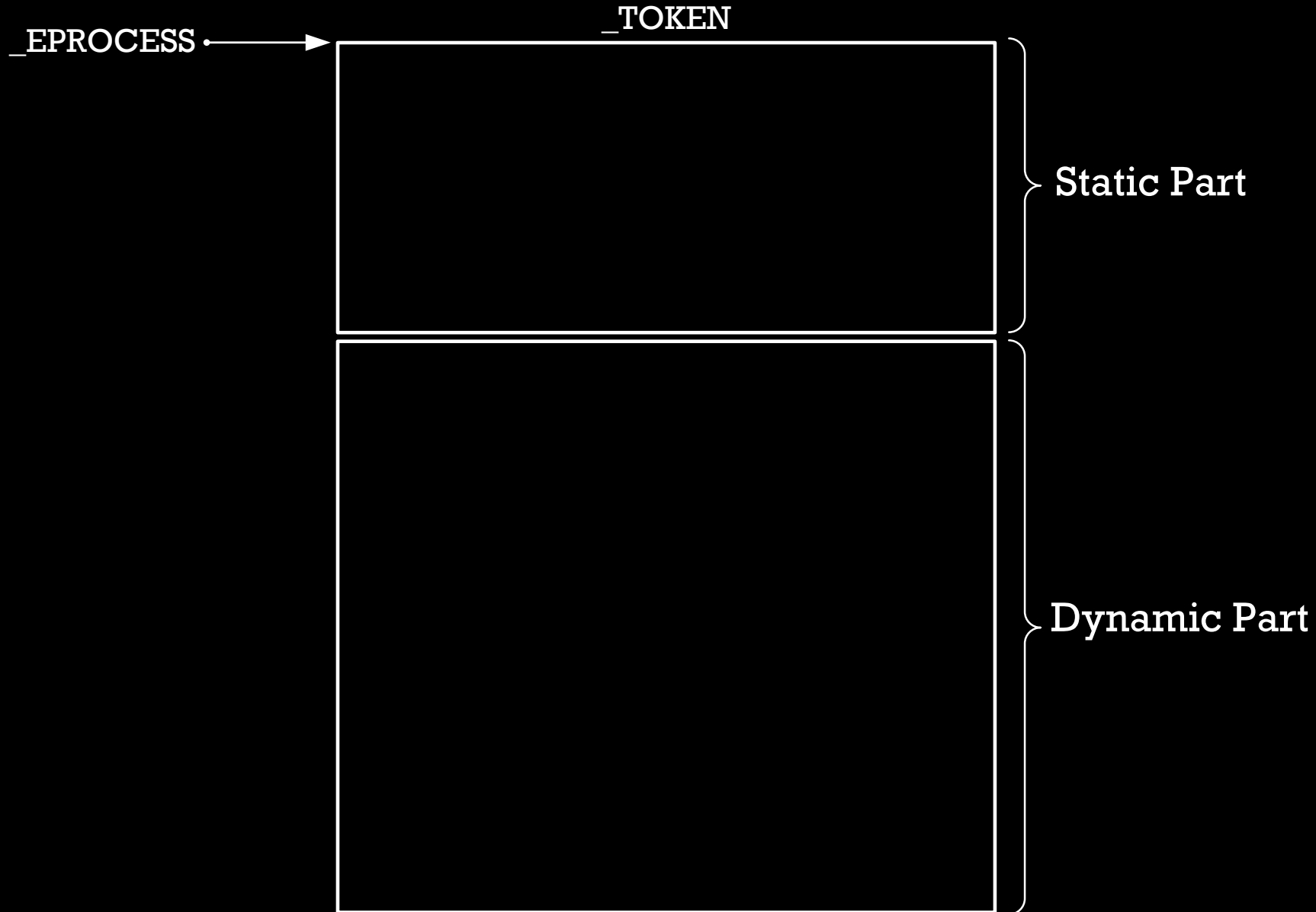
EPROCESS AND TOKEN IN WINDOWS: TOKEN SWAPPING



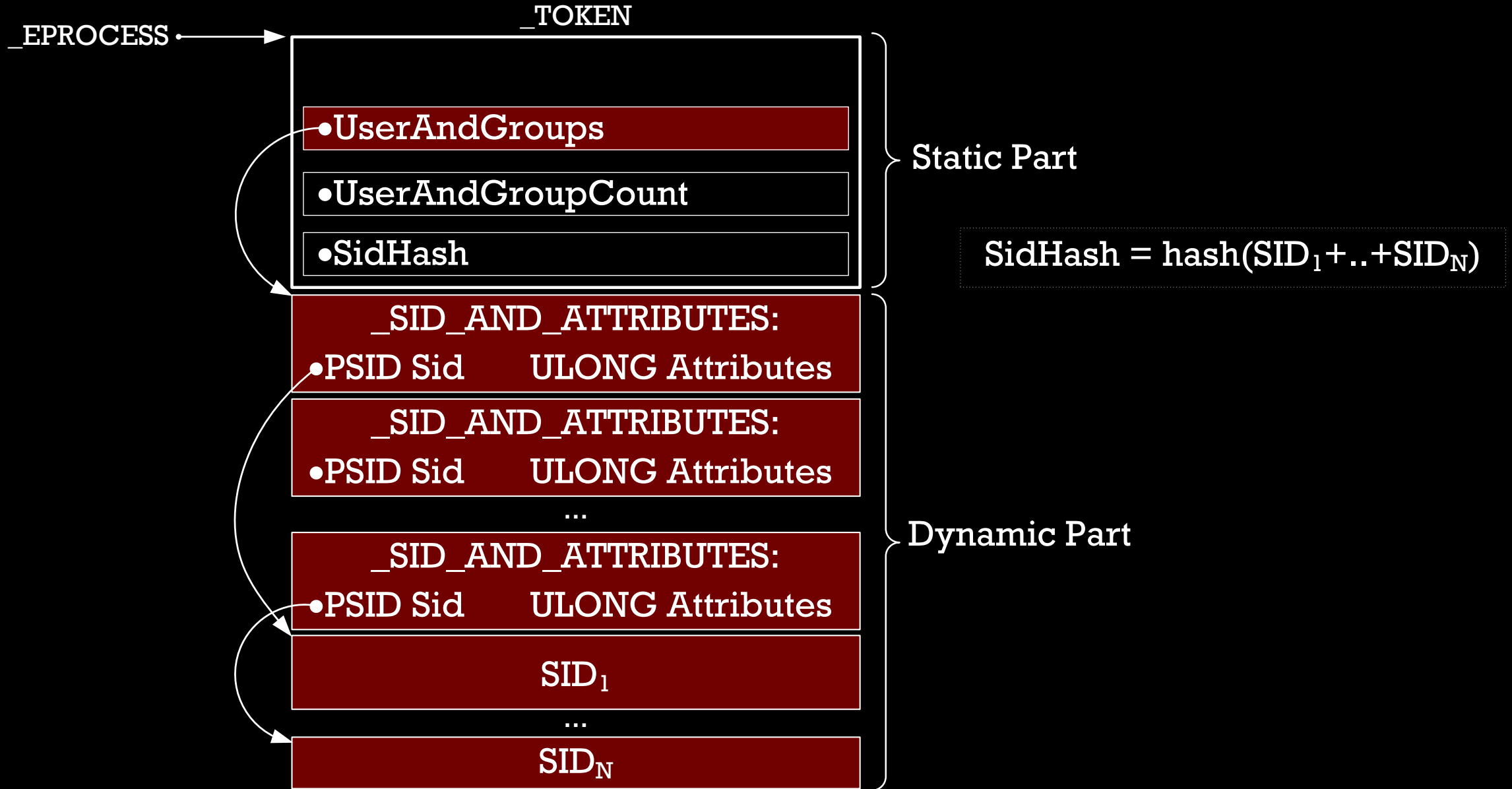
EPROCESS AND TOKEN IN WINDOWS: MSFT Defender



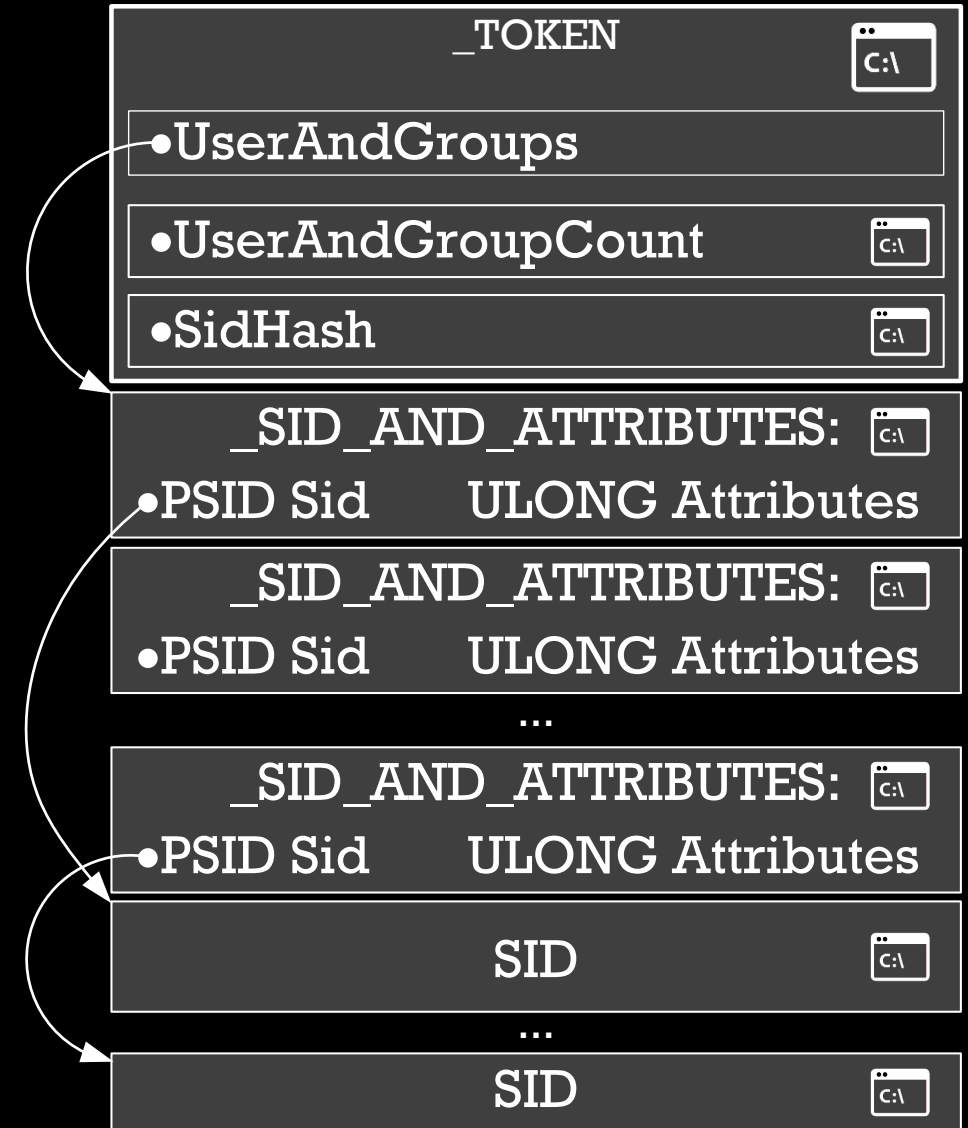
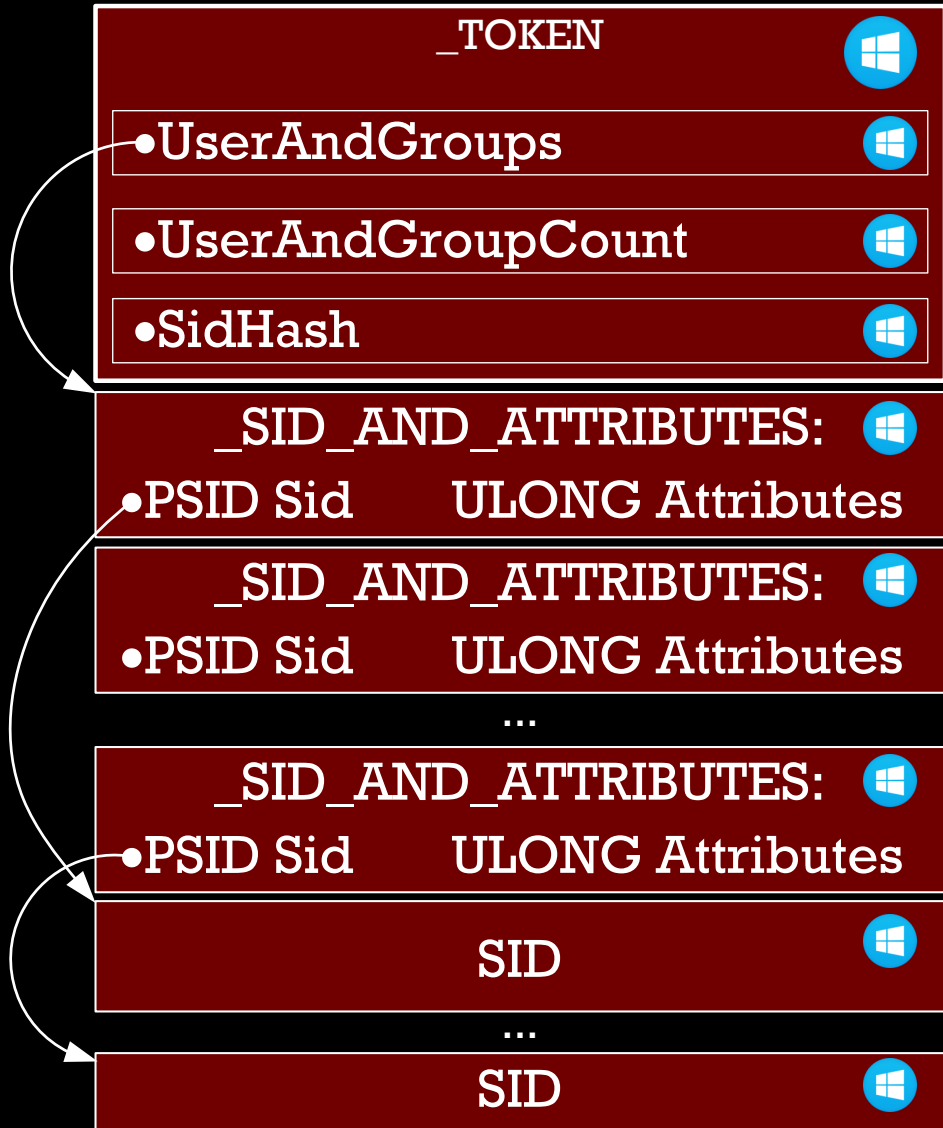
TOKEN INTERNALS



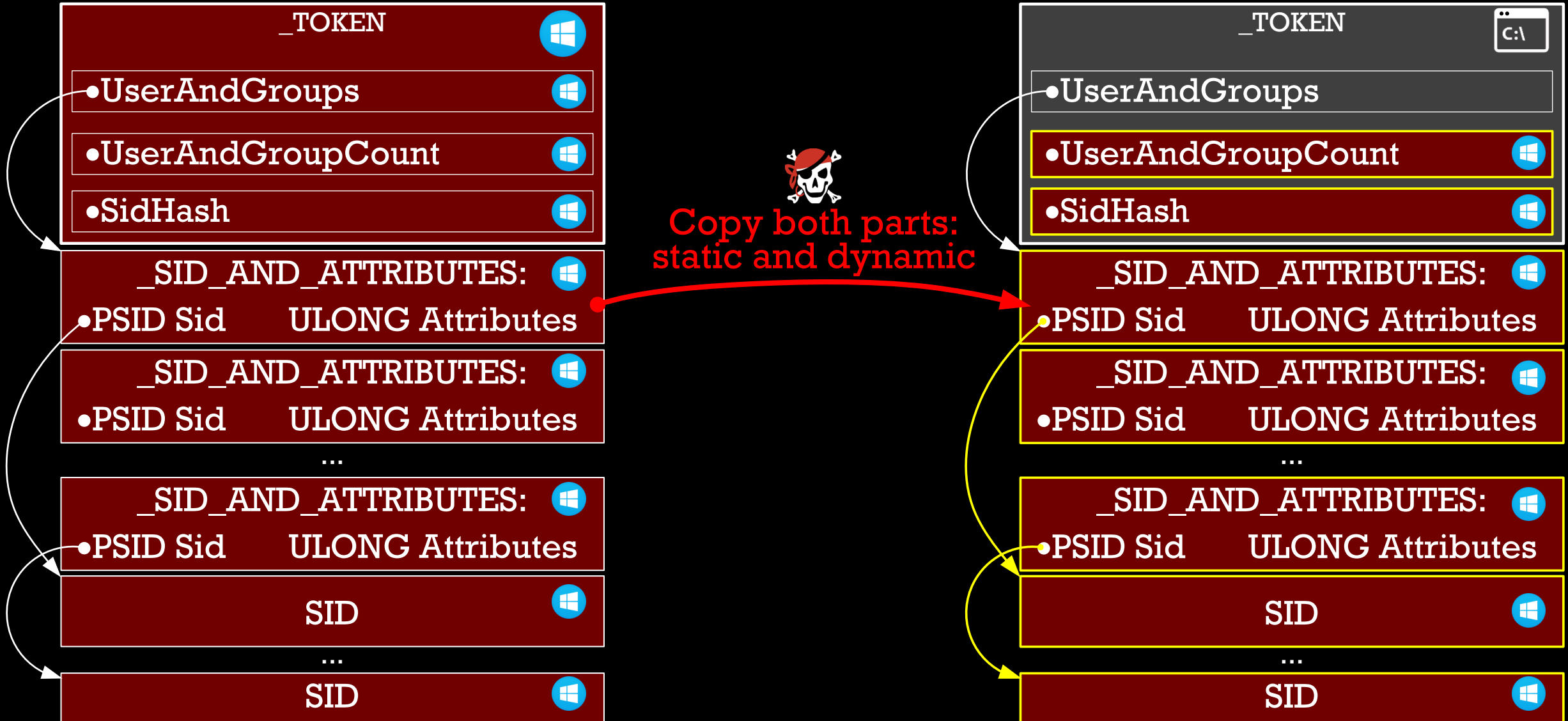
TOKEN INTERNALS



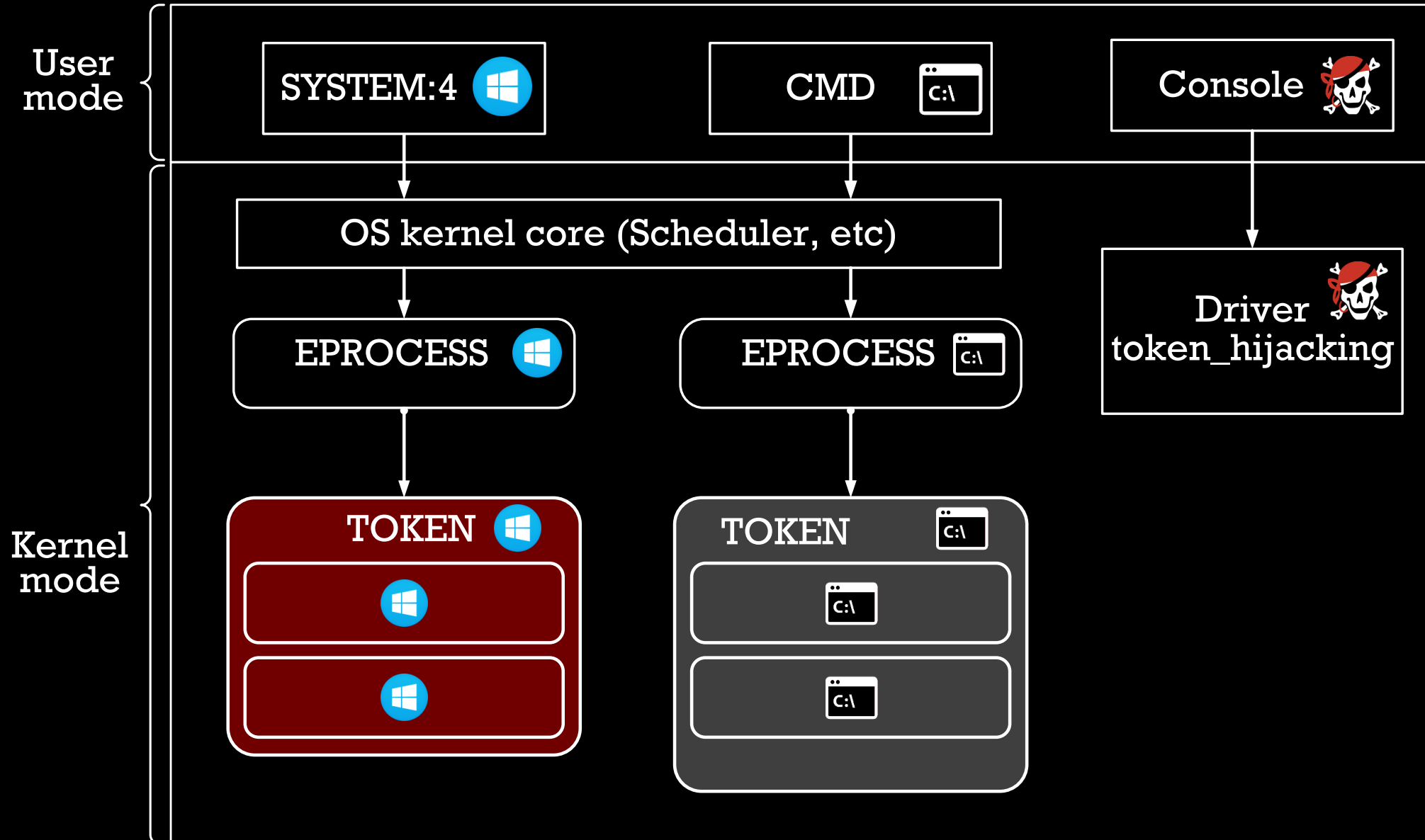
AN IDEA OF TOKEN HIJACKING ATTACK



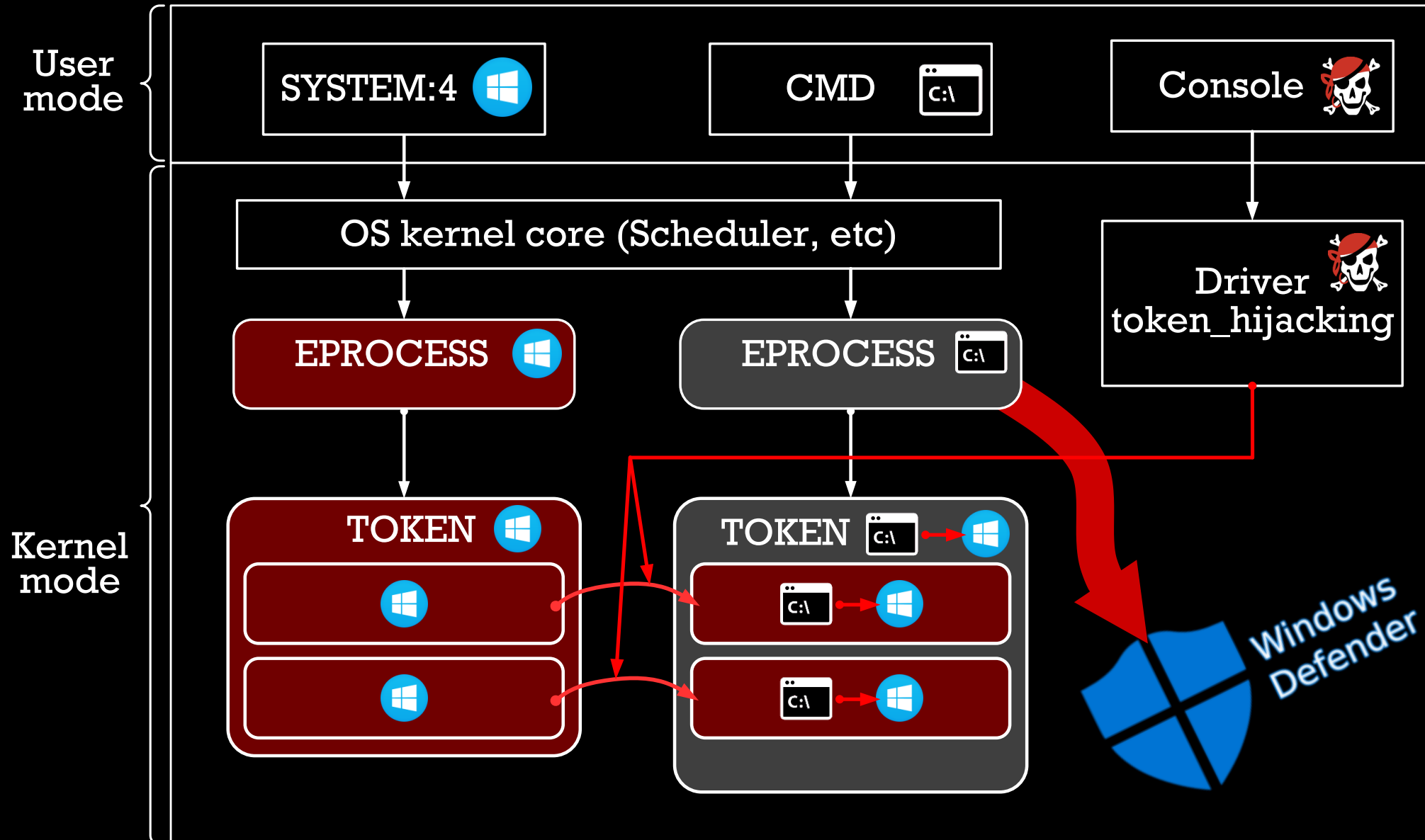
AN IDEA OF TOKEN HIJACKING ATTACK



TOKEN HIJACKING ATTACK



TOKEN HIJACKING ATTACK



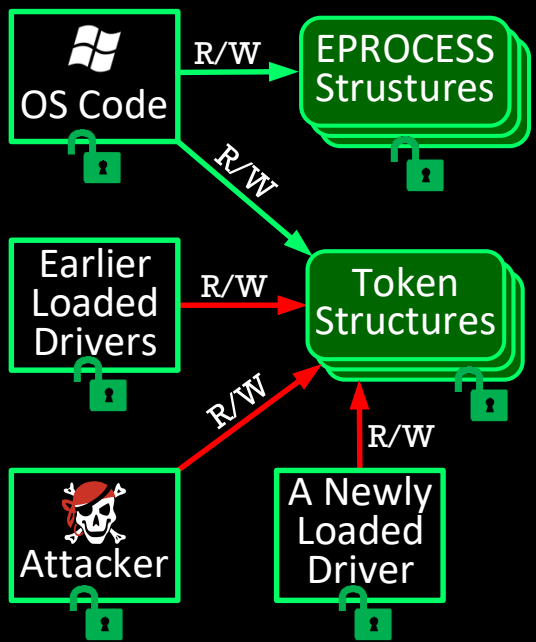
DEMO#5: TOKEN HIJACKING

The online version is here –

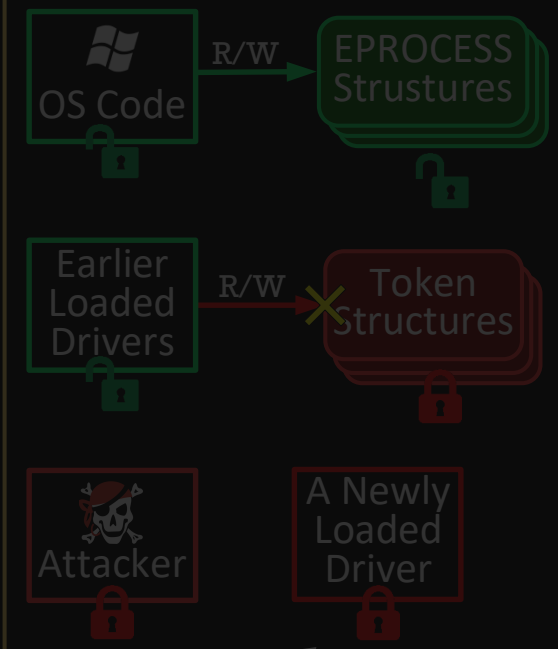
https://www.youtube.com/embed/7Dgtz_2oGJg?vq=hd1440

MEMORY MAP: MEMORYRANGER PREVENTS TOKEN HIJACKING

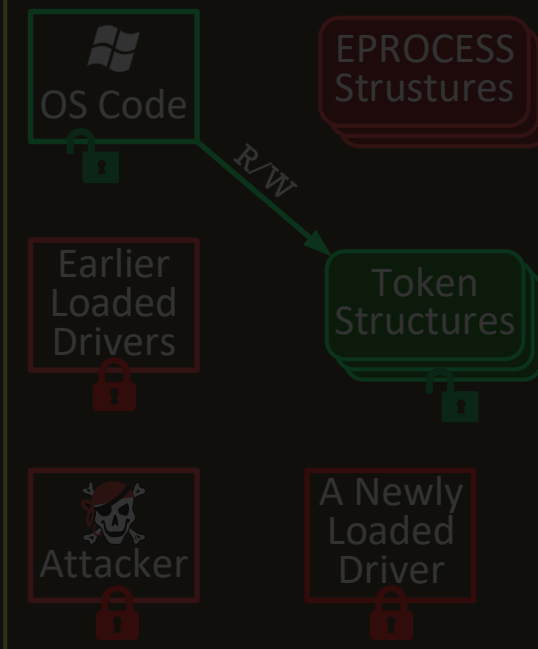
The Current Situation



Default enclave for OS and driver loaded before



The Token Enclave



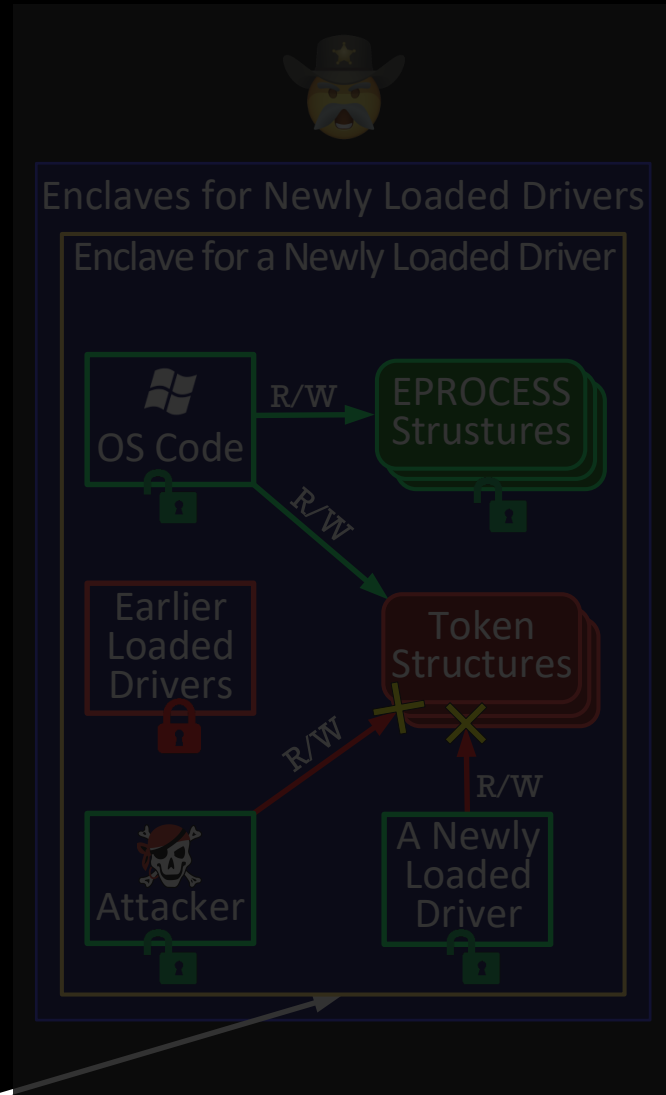
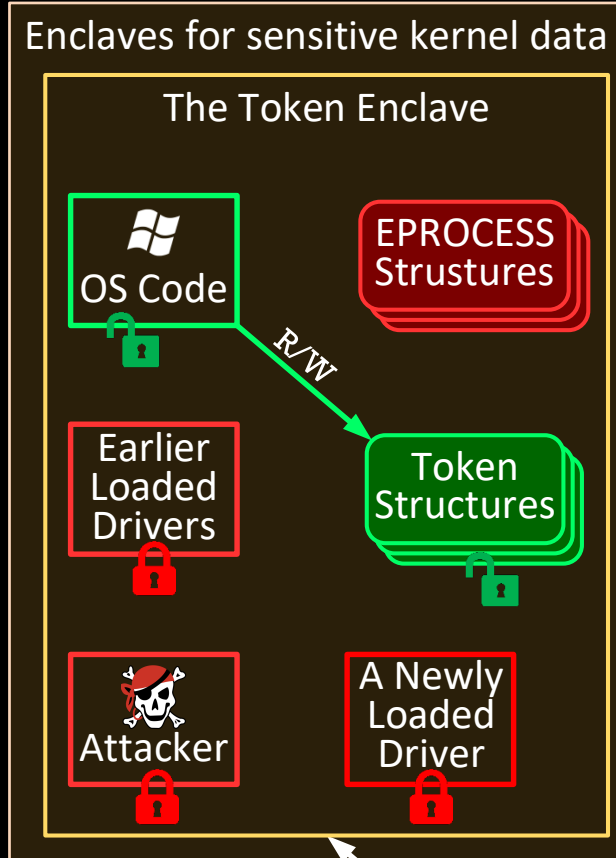
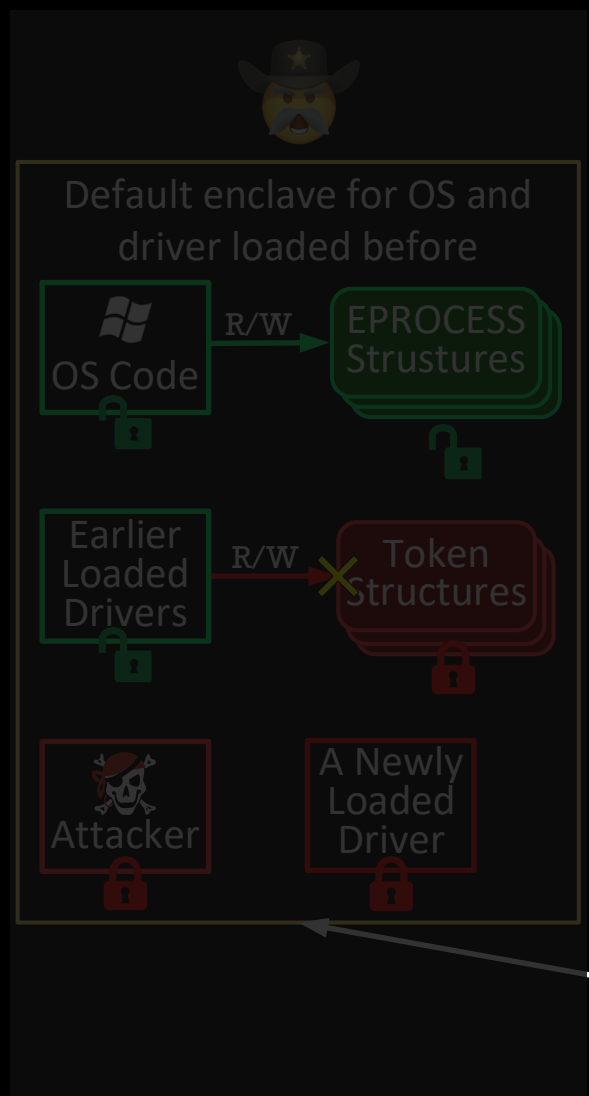
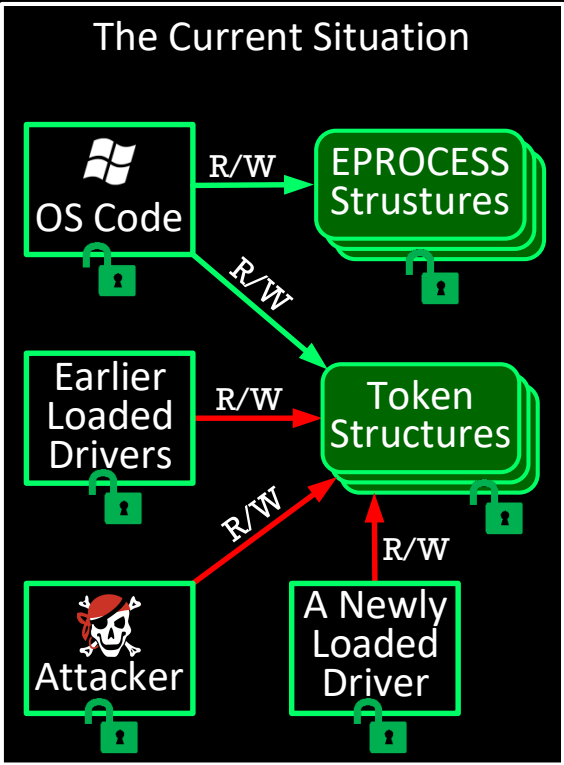
Enclaves for Newly Loaded Drivers

Enclave for a Newly Loaded Driver



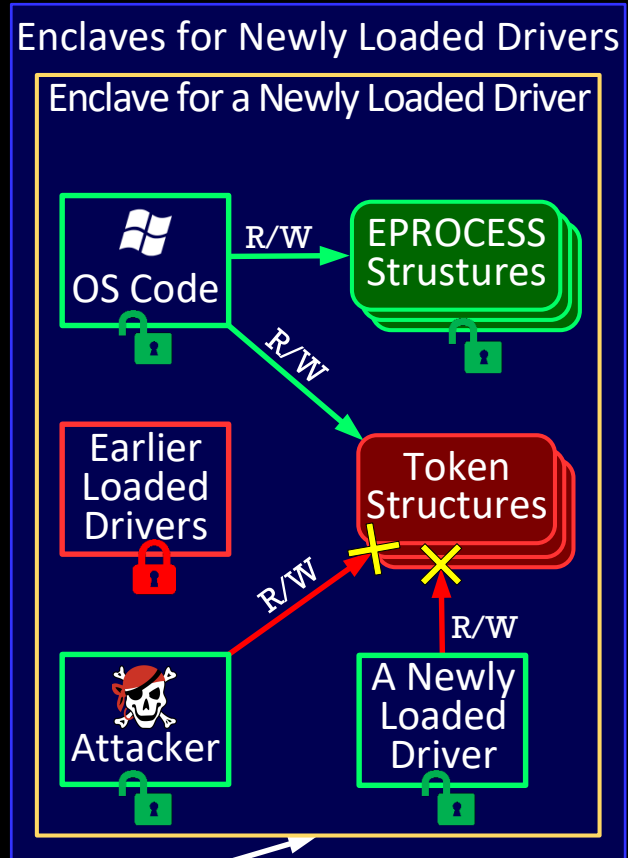
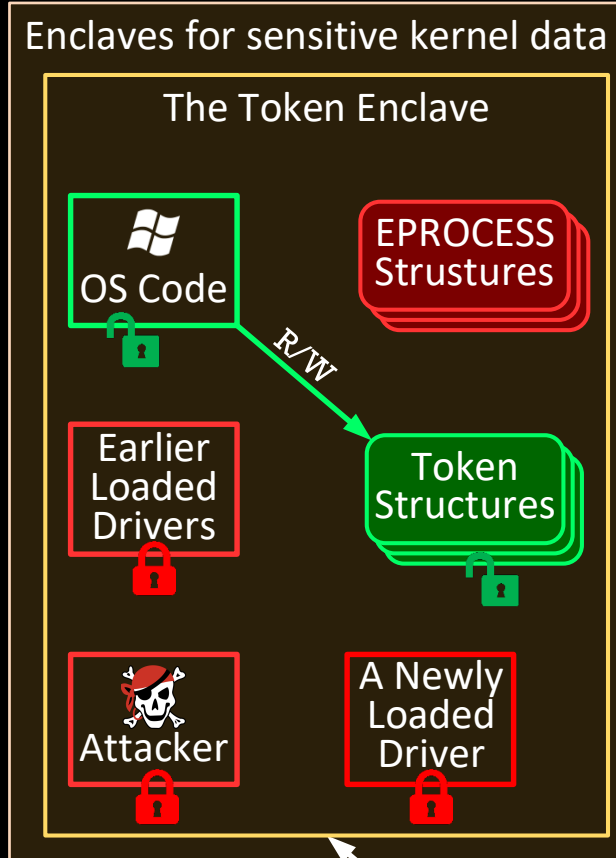
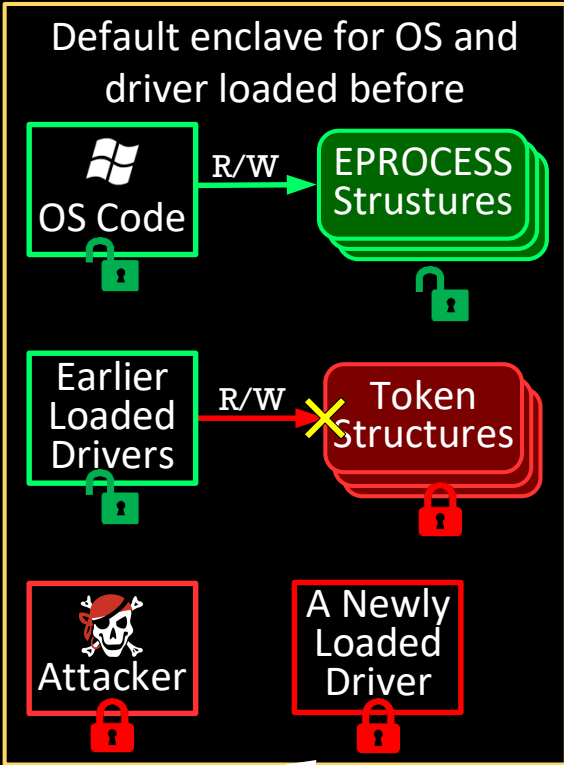
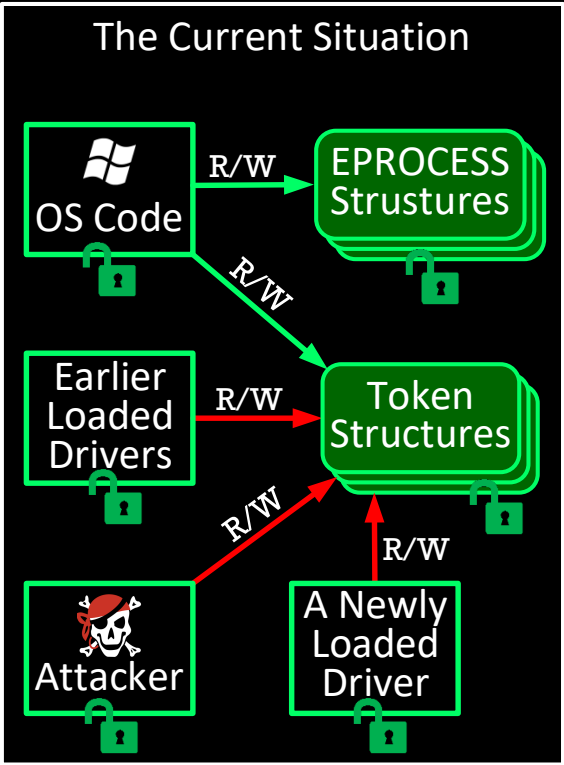
EPT pointer

MEMORY MAP: MEMORYRANGER PREVENTS TOKEN HIJACKING



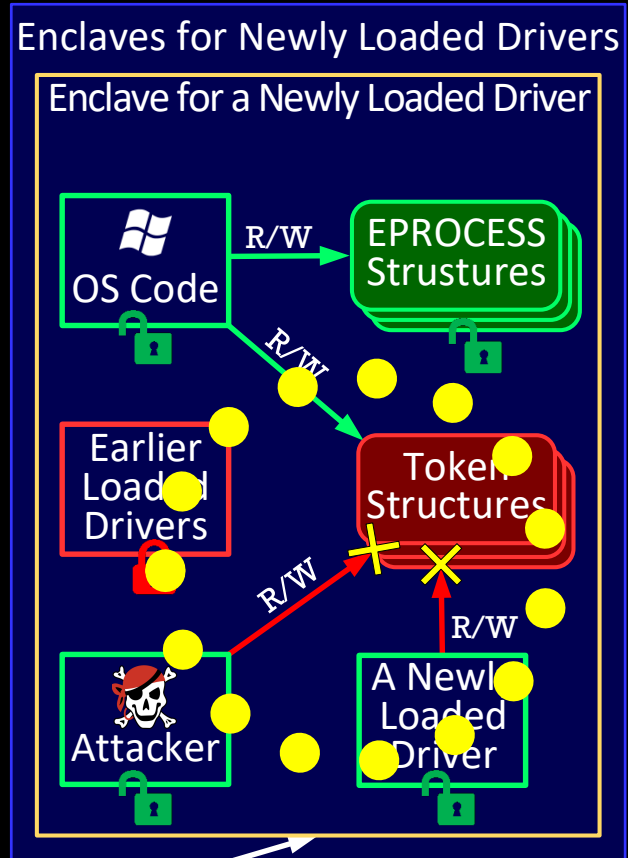
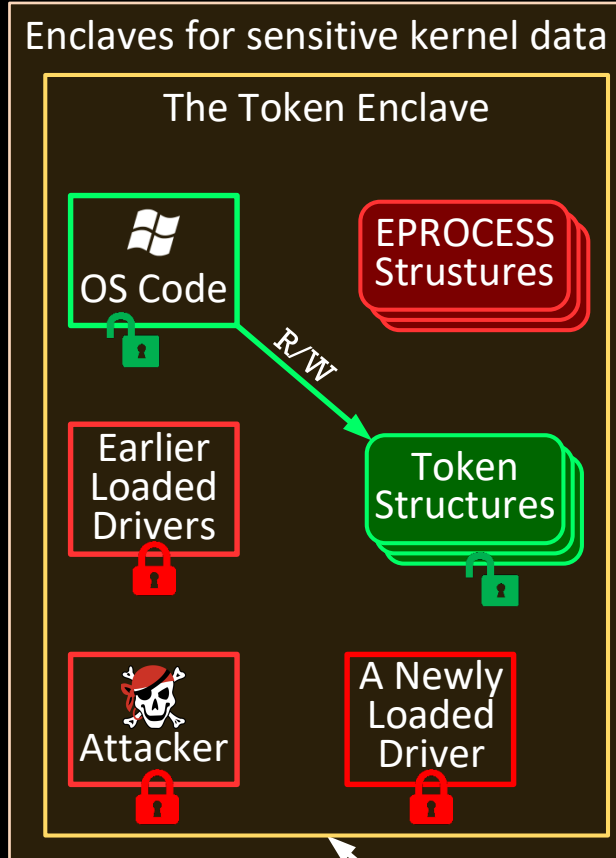
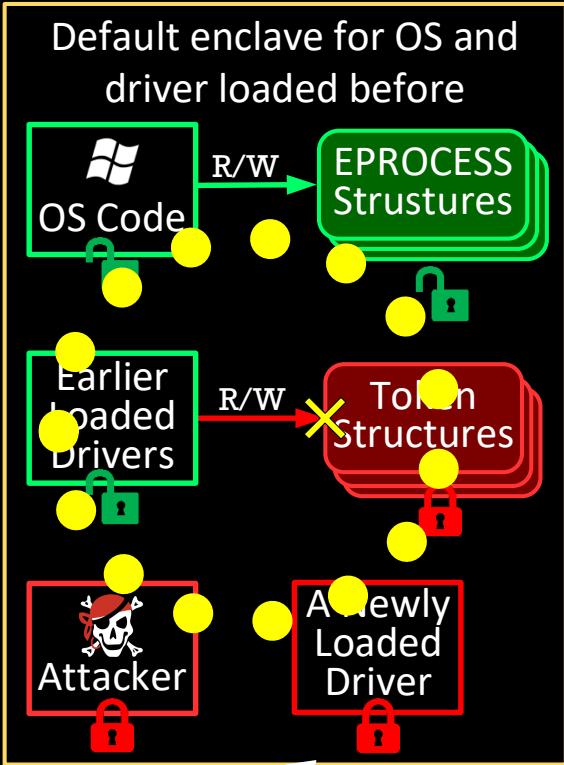
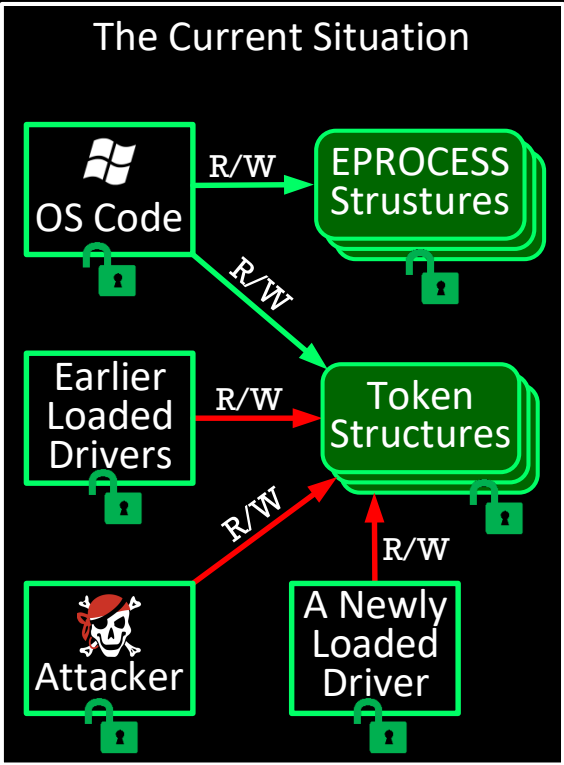
EPT pointer

MEMORY MAP: MEMORYRANGER PREVENTS TOKEN HIJACKING



EPT pointer

MEMORY MAP: MEMORYRANGER PREVENTS TOKEN HIJACKING



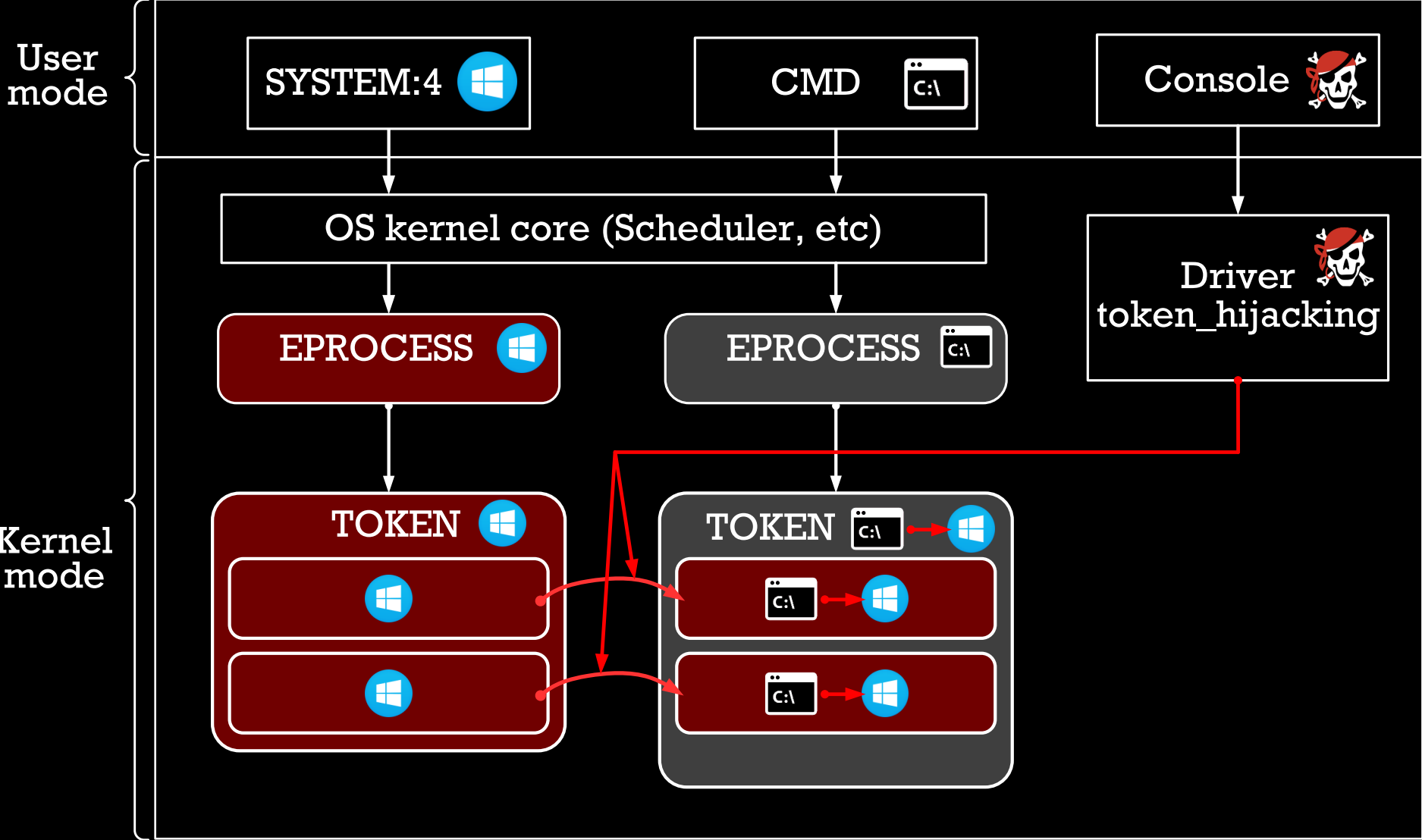
EPT pointer

DEMO#6: PREVENTION OF TOKEN HIJACKING

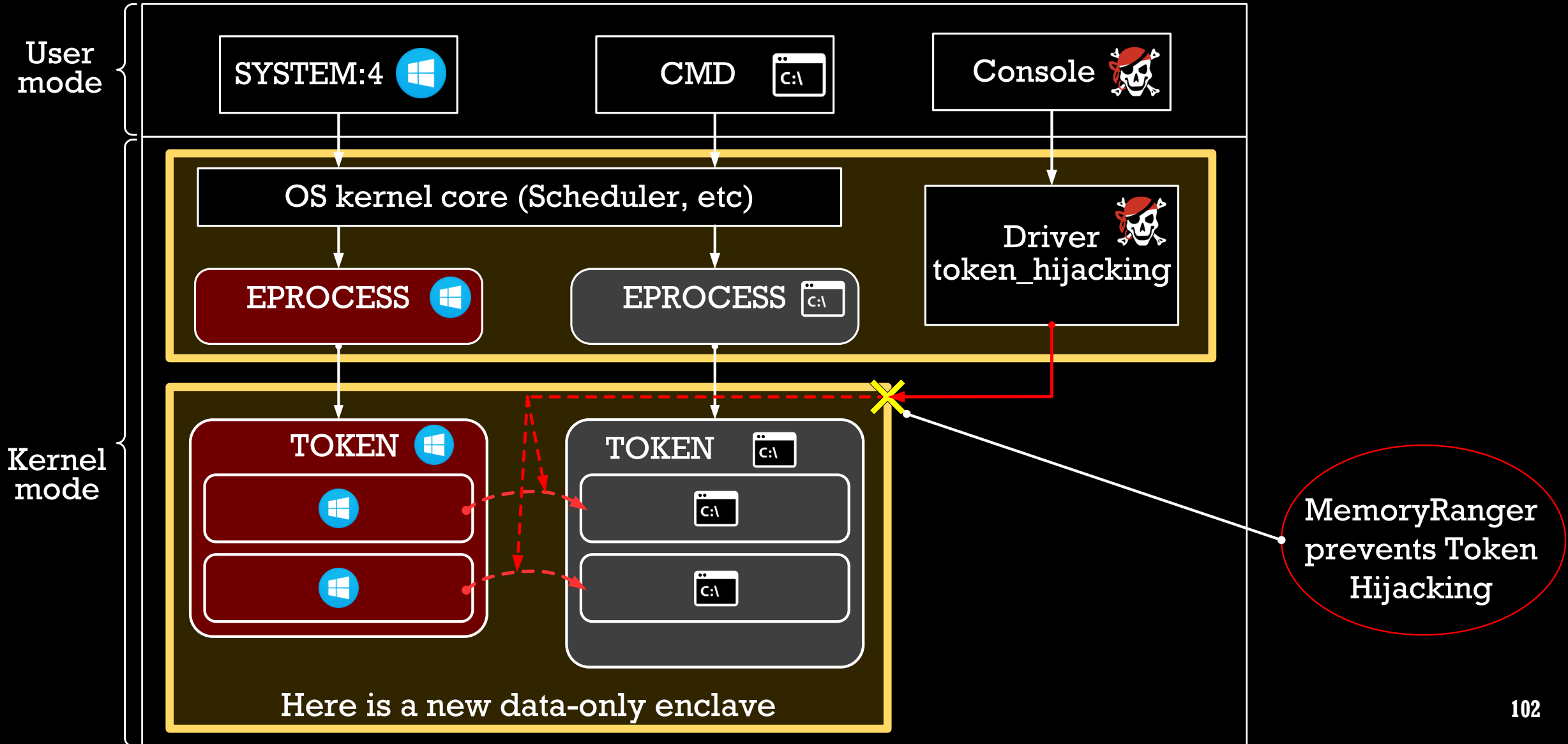
The online version is here –

<https://www.youtube.com/embed/zGAR7wvM4g?vq=hd1440>

TOKEN HIJACKING ATTACK



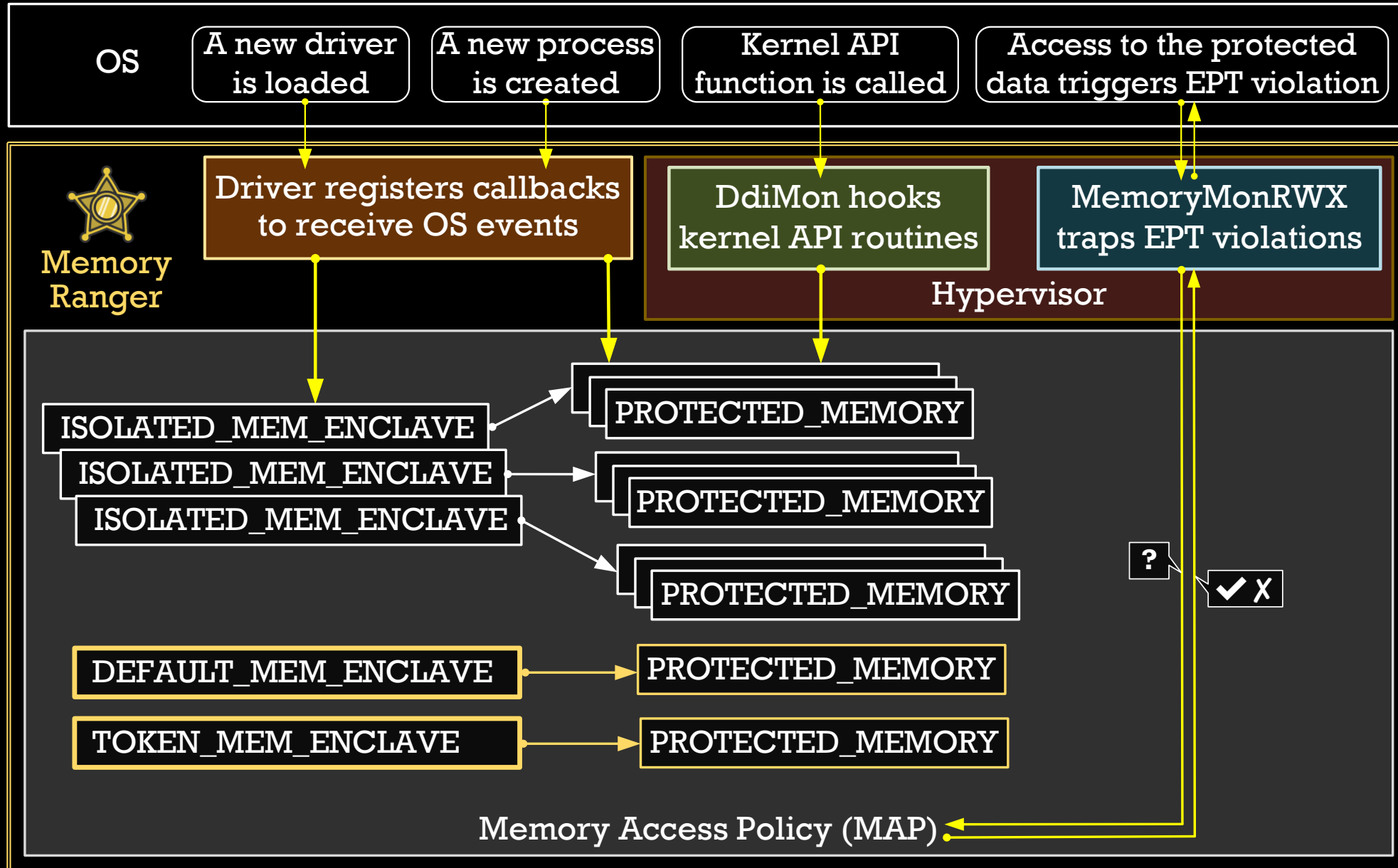
TOKEN HIJACKING IS BLOCKED BY A NEW DATA-ONLY ENCLAVE



Episode 3

MemoryRanger

MEMORY RANGER ARCHITECTURE

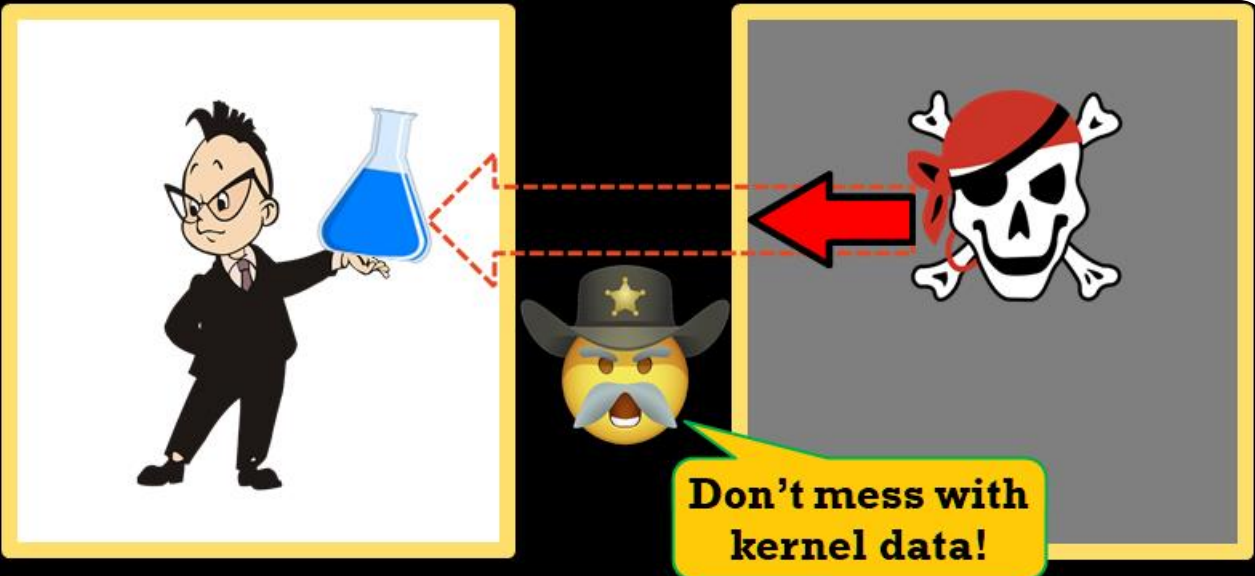
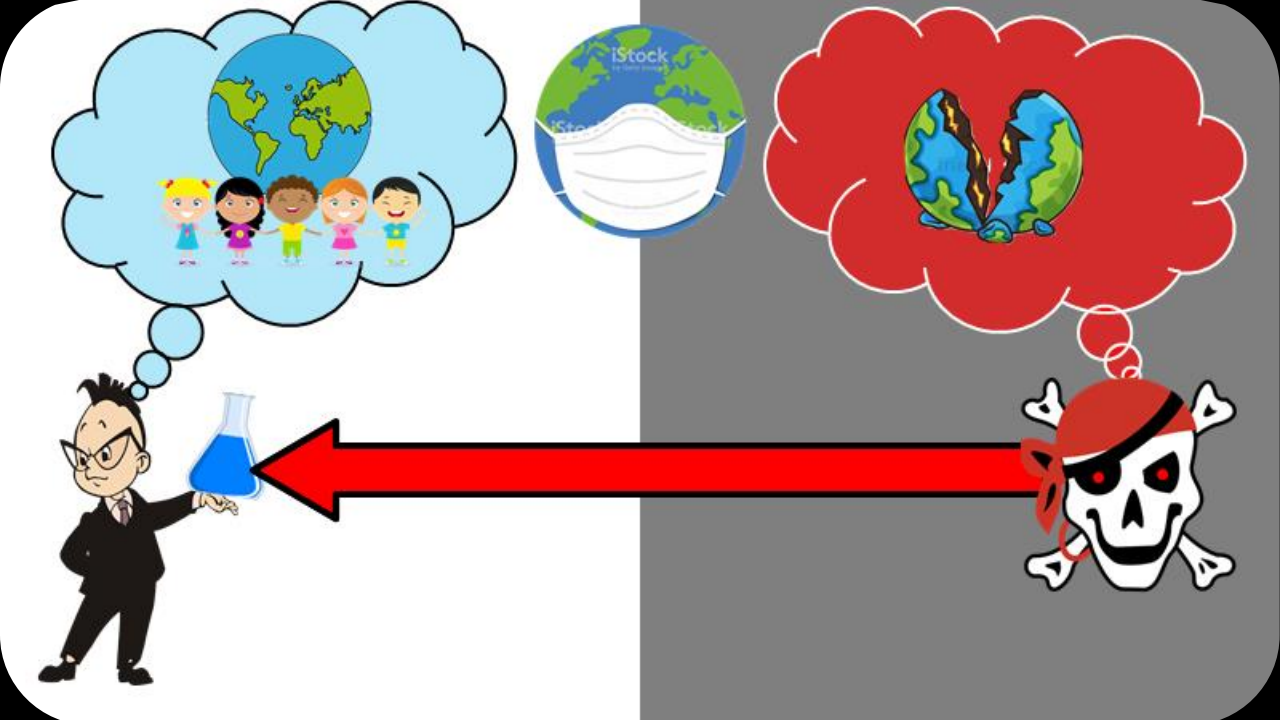


(Further details in the paper)

<https://github.com/IgorKorkin/MemoryRanger>

CONCLUSION

1. Windows OS security features provide limited kernel memory protection
2. **Handle Hijacking** = copy 6 bytes of structure
3. **Hijacking NTFS** = copy data structures & Thread ID
4. **Token Hijacking** = copy structures & their interconnections
5. **Updated MemoryRanger**
 - protects new data structures
 - includes a new data-only enclave to isolate the secret data from all drivers
 - works well on the recent Windows 1003





**MemoryRanger
protects the OS!**



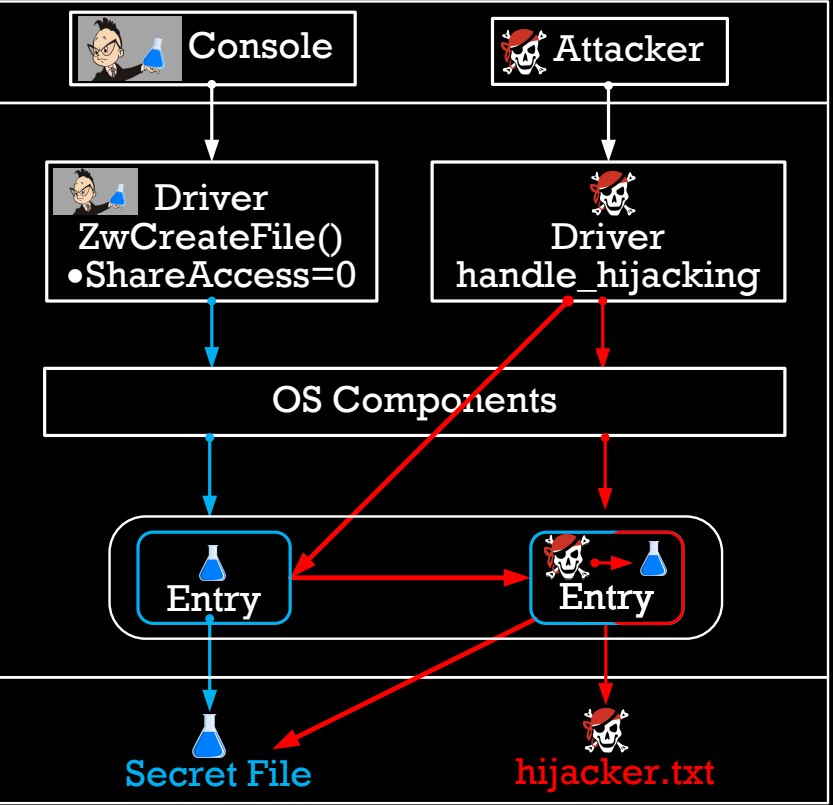
Thank You!

HITB **LOCKDOWN** ⁰⁰²
livestream

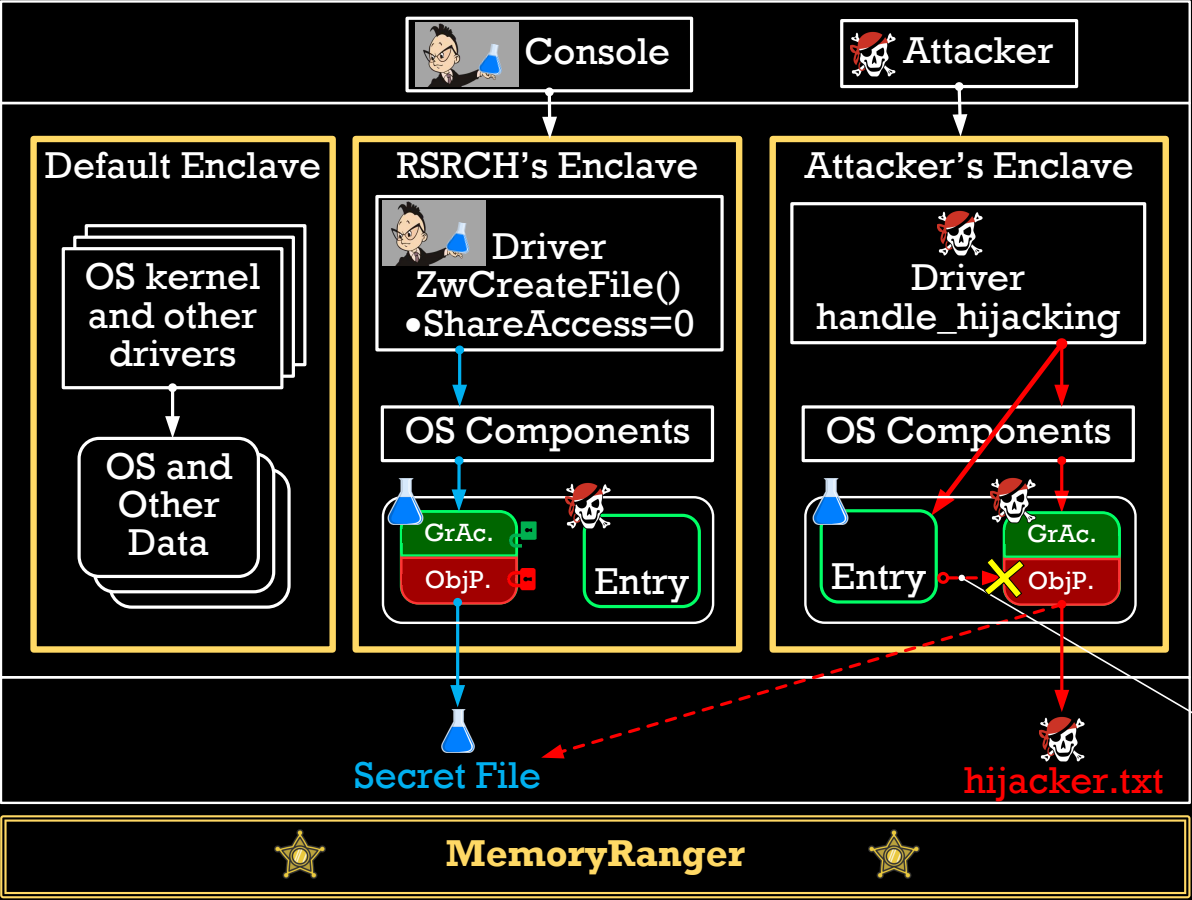
EXTRA SLIDES

DEMO: PREVENTING THE HANDLE HIJACKING ATTACK

Attempt 2: Handle Table Hijacking

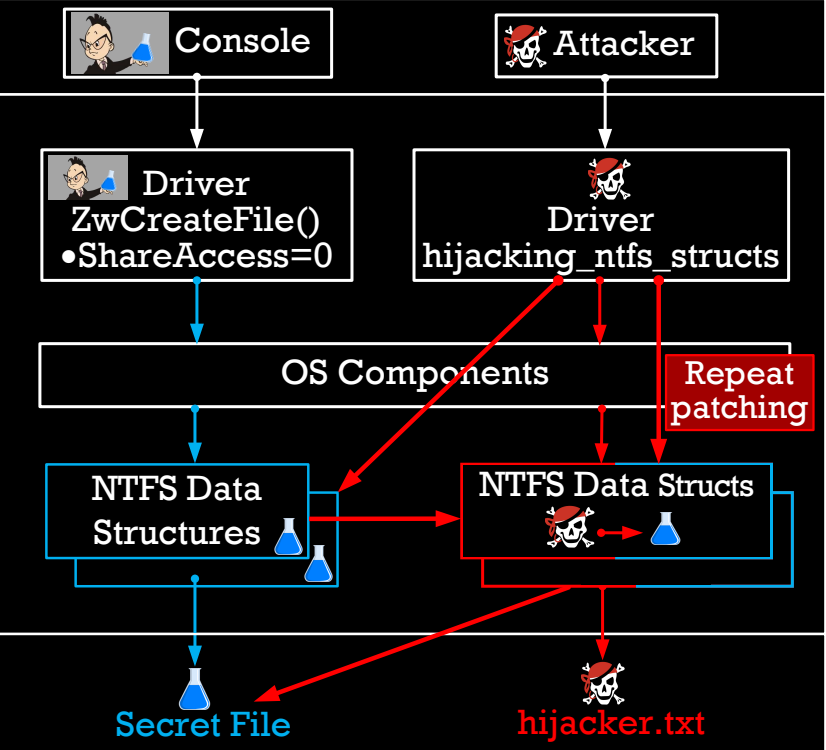


MemoryRanger Prevents the Handle Hijacking

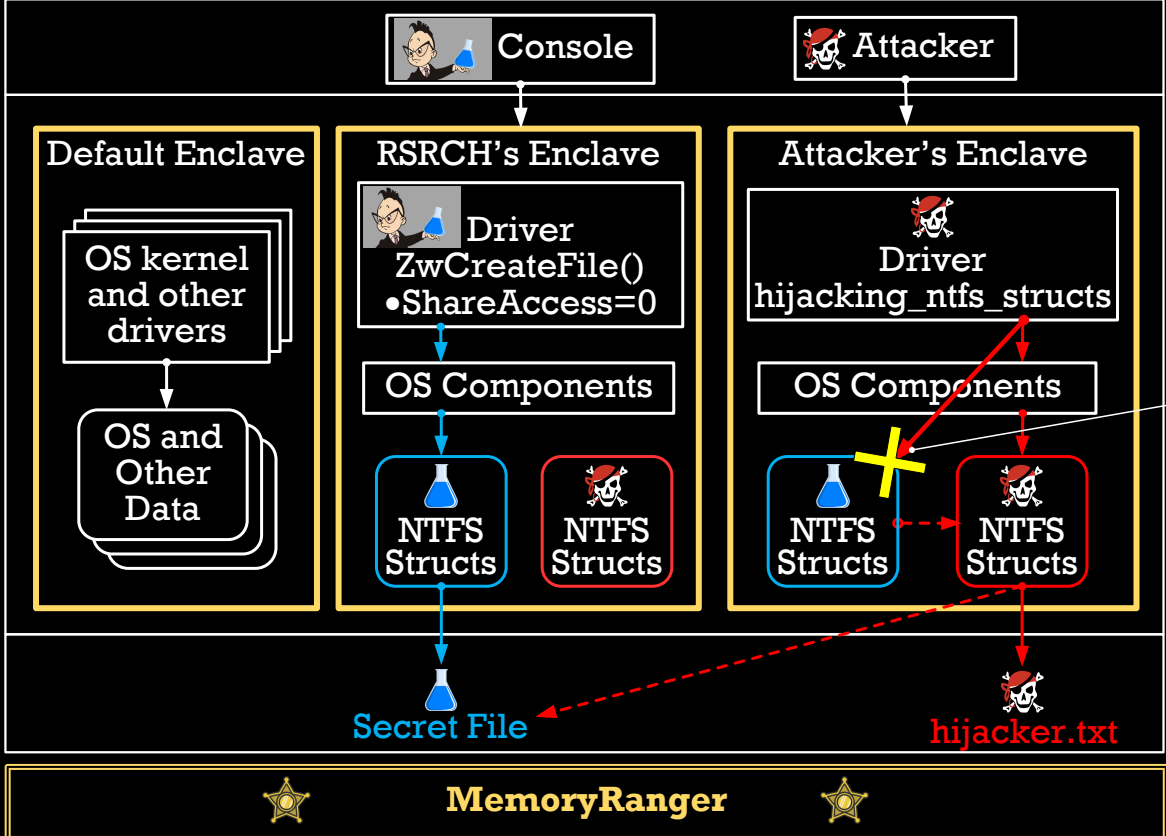


DEMO: PREVENTING THE HIJACKING NTFS STRUCTURES

Attempt 2: Hijacking NTFS structures



Preventing the Hijacking NTFS structures



MemoryRanger prevents Hijacking NTFS structures