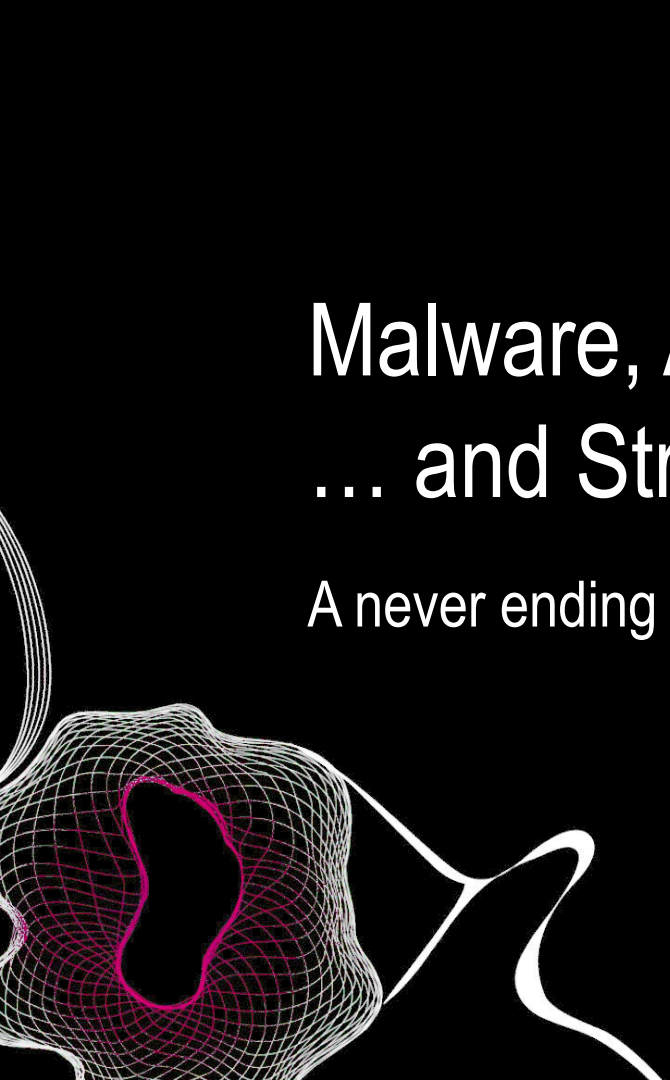
Malware, Anti-Malware … and Street Fighter V

A never ending cat-and-mouse game



Jerre Starink - j.a.l.starink@utwente.nl

UNIVERSITY OF TWENTE.

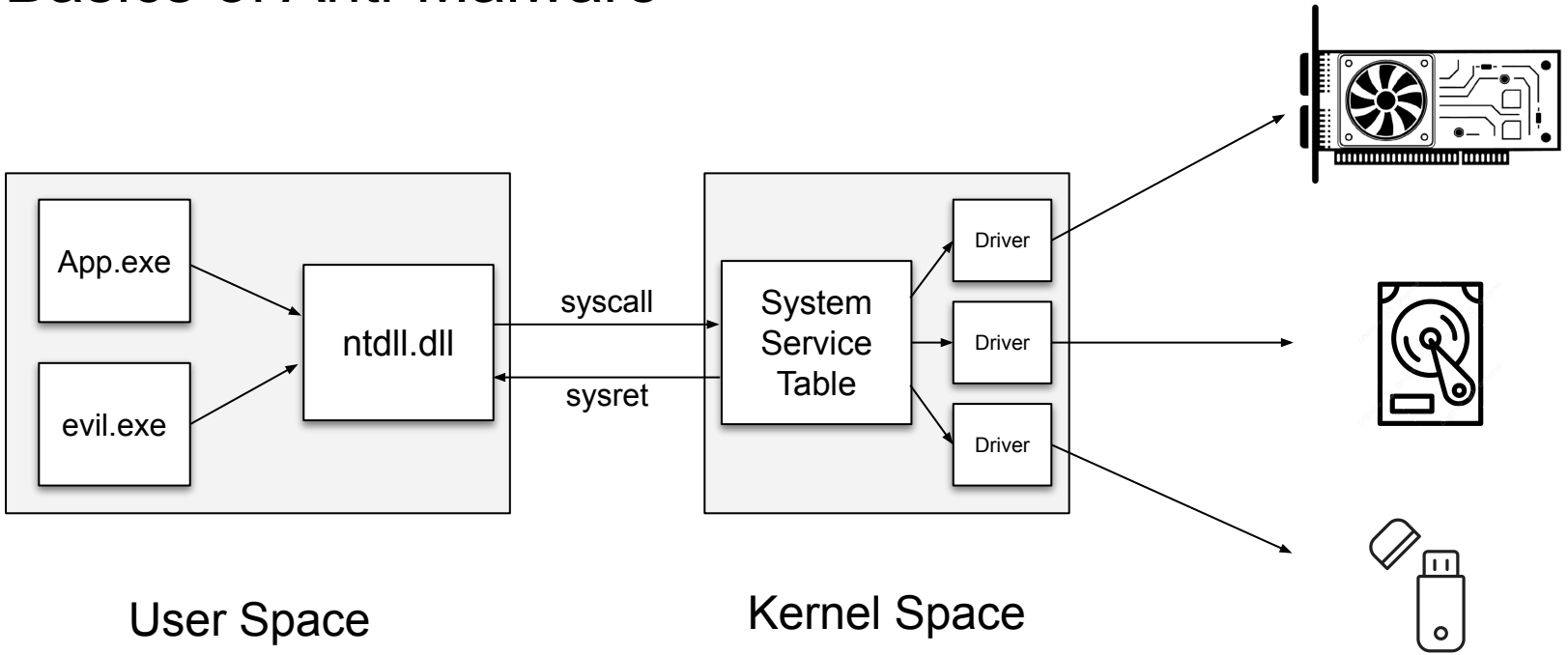
Agenda

- The Basics of Anti-Malware
- Why is it hard on modern operating systems
- Street Fighter V
- Moving Forward

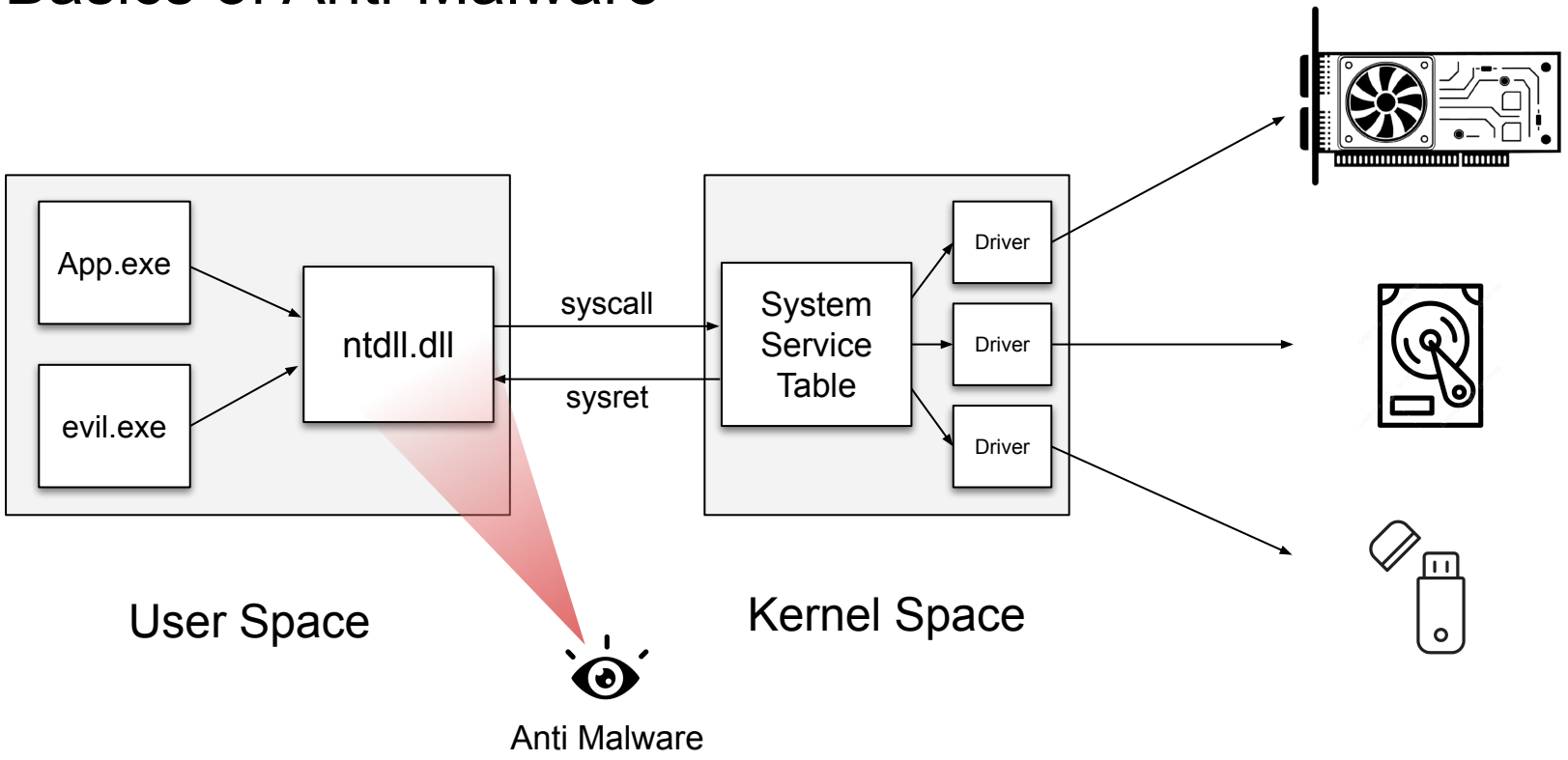
The Basics of Anti-Malware

- Typically based on Dynamic Analysis.
- Allow the program to run, but stop it in its tracks when it does something bad.

The Basics of Anti-Malware



The Basics of Anti-Malware



Userspace Inline Hooking

```
18009d5df    ...
ntdll.dll!NtWriteFile:
18009d5e0    MOV     R10, RCX
18009d5e3    MOV     EAX, 0x8
18009d5e8    TEST    byte ptr [0x7ffe0308], 0x1
18009d5f0    JNZ     0x18009d5f5
18009d5f2    SYSCALL
18009d5f4    RET
18009d5f5    INT     0x2e
18009d5f7    RET
18009d5f8    ...
```

ntdll.dll (in memory)

Userspace Inline Hooking

```
18009d5df     ...
ntdll.dll!NtWriteFile:
18009d5e0     JMP      antimalware!MyNtWriteFile
18009d5e3     MOV      EAX, 0x8
18009d5e8     TEST     byte ptr [0x7ffe0308], 0x1
18009d5f0     JNZ      0x18009d5f5
18009d5f2     SYSCALL
18009d5f4     RET
18009d5f5     INT      0x2e
18009d5f7     RET
18009d5f8     ...
```

ntdll.dll (in memory)

Redirection
to Anti-Malware

```
// antimalware.c

int MyNtWriteFile(...) {
     print("NtWriteFile was called");
     // ...
     return NtWriteFile(...);
}
```

Userspace Inline Hooking

- Pros:
  - Practical, easy to implement.
  - You can place them anywhere on any function.
  - You have a lot of freedom.

Userspace Inline Hooking

```
18009d5df    ...
ntdll.dll!NtWriteFile:
18009d5e0    JMP     antimalware!MyNtWriteFile
18009d5e3    MOV     EAX, 0x8
18009d5e8    TEST    byte ptr [0x7ffe0308], 0x1
18009d5f0    JNZ     0x18009d5f5
18009d5f2    SYSCALL
18009d5f4    RET
18009d5f5    INT     0x2e
18009d5f7    RET
18009d5f8    ...
```

ntdll.dll (in memory)

Userspace Inline Hooking

```
18009d5df     ...
ntdll.dll!NtWriteFile:
18009d5e0     JMP      antimalware!MyNtWriteFile
18009d5e3     MOV      EAX, 0x8
18009d5e8     TEST     byte ptr [0x7ffe0308], 0x1
18009d5f0     JNZ      0x18009d5f5
18009d5f2     SYSCALL
18009d5f4     RET
18009d5f5     INT      0x2e
18009d5f7     RET
18009d5f8     ...
```

ntdll.dll (in memory)

```
def NtWriteFile(...)
  MOV     R10, RCX
  MOV     EAX, 0x8
  TEST    byte ptr [0x7ffe0308],0x1
  JNZ     0x18009d5f5
  SYSCALL
  RET
  INT     0x2e
  RET
```

ntdll.dll (on disk)

Userspace Inline (Un)Hooking

```
18009d5df    ...
ntdll.dll!NtWriteFile:
18009d5e0    MOV     R10, RCX
18009d5e3    MOV     EAX, 0x8
18009d5e8    TEST    byte ptr [0x7ffe0308], 0x1
18009d5f0    JNZ     0x18009d5f5
18009d5f2    SYSCALL
18009d5f4    RET
18009d5f5    INT     0x2e
18009d5f7    RET
18009d5f8    ...
```

ntdll.dll (in memory)

Write back original removes hook

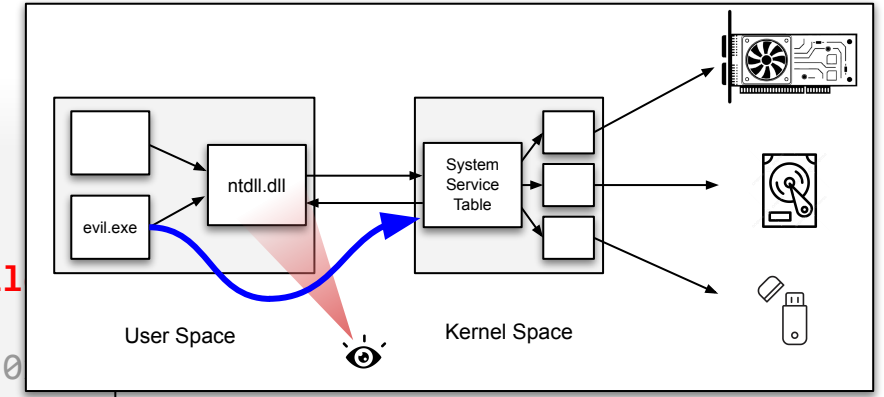
```
def NtWriteFile(...)
  MOV     R10, RCX
  MOV     EAX, 0x8
  TEST    byte ptr [0x7ffe0308],0x1
  JNZ     0x18009d5f5
  SYSCALL
  RET
  INT     0x2e
  RET
```

ntdll.dll (on disk)

Userspace Inline Hook Bypass

```
18009d5df     ...
ntdll.dll!NtWriteFile:
18009d5e0     JMP      antimalware!MyNtWriteFil
18009d5e3     MOV      EAX, 0x8
18009d5e8     TEST     byte ptr [0x7ffe0308], 0
18009d5f0     JNZ      0x18009d5f5
18009d5f2     SYSCALL
18009d5f4     RET
18009d5f5     INT      0x2e
18009d5f7     RET
18009d5f8     ...
```

ntdll.dll (in memory)



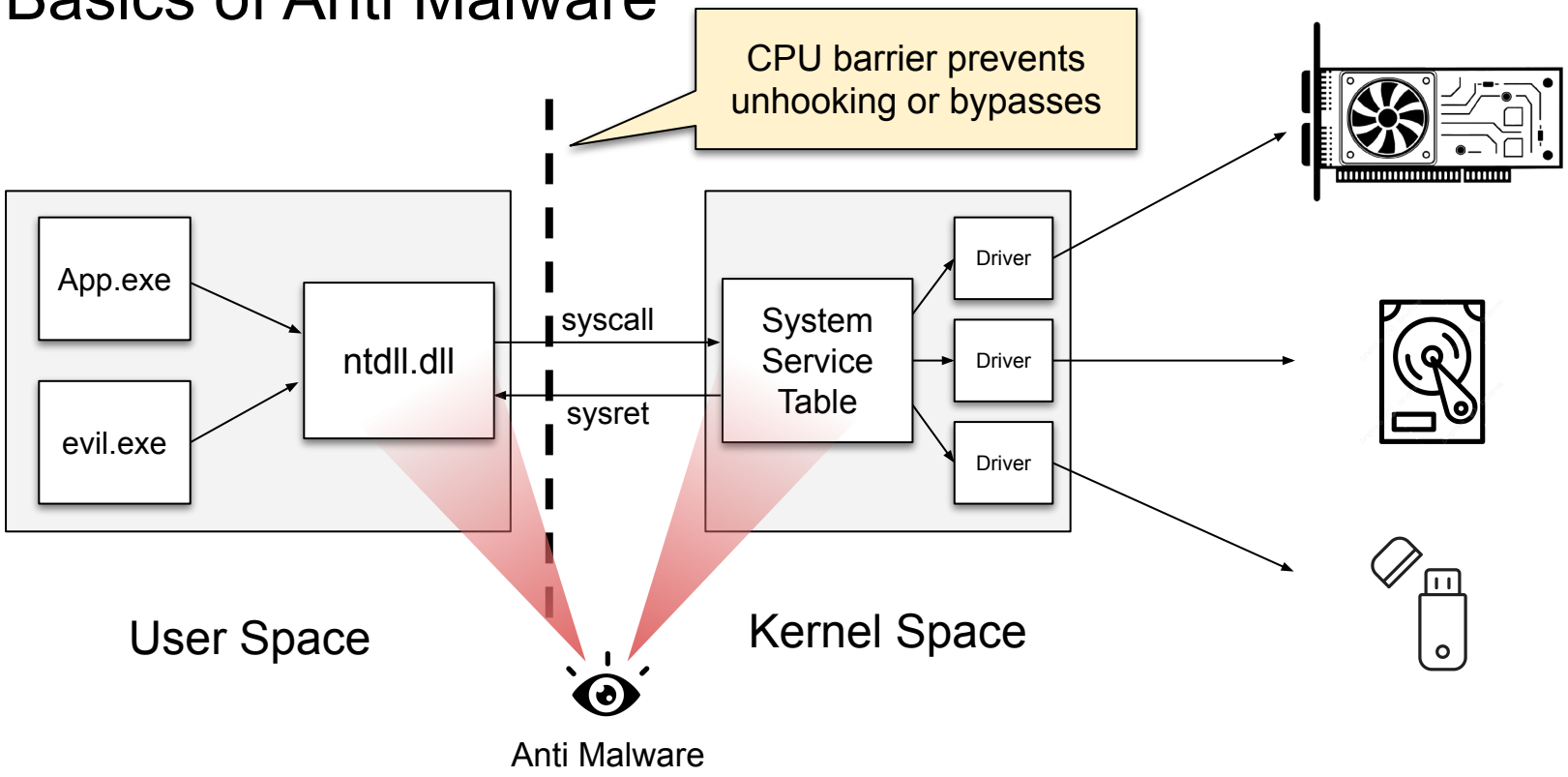

```
// evil.c

int main(...) {
   NtWriteFile("C:\\foo.txt", ...)
   __syscall(0x8, "C:\\foo.txt", ...);
}
```

Userspace Inline Hooking

- Pros:
  - Practical, easy to implement.
  - You can place them anywhere on any function.
  - You have a lot of freedom.

- Cons:
  - Hooks also reside in userspace.
  - Malware can just remove the hook again.
  - Malware can do direct system calls instead.

The Basics of Anti Malware



A NEW FOE HAS APPEARED!

CHALLENGER APPROACHING

UNIVERSITY
OF TWENTE.


Windows Vista™

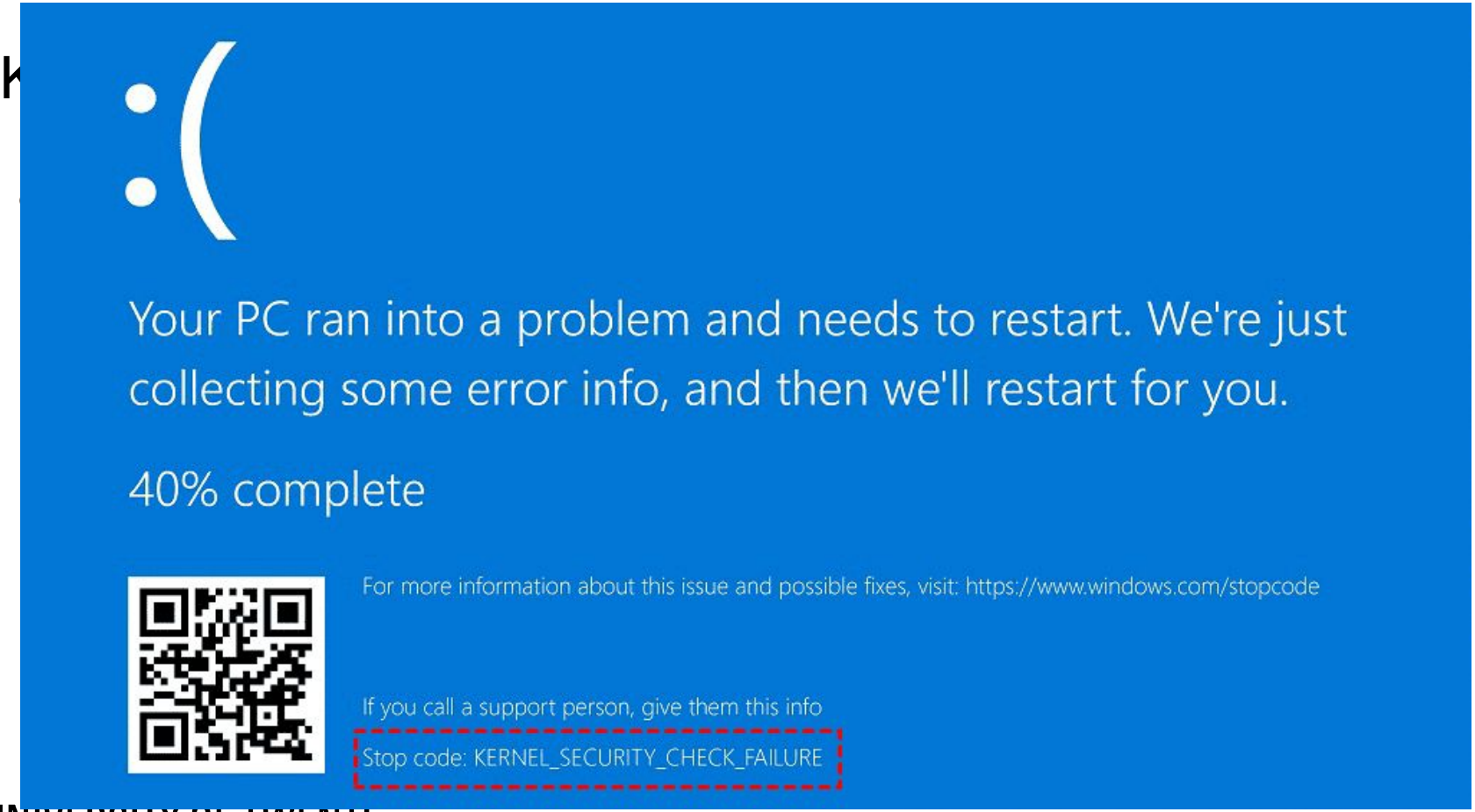

61°
Redmond, WA
Tokyo
January 2007
29
Monday
Eggs
Milk
Bread
Windows Media Center
10:10 AM
Now Playing
TV + Movies
recorded tv
play dvd
set up tv
more tv
Sports
Tokyo Photos
Control Panel
Documents
Windows Photo ...
Windows Media ...
Calculator
Internet Explorer ...
10:10 AM

UNIVE

Kernel Patch Protection (PatchGuard)

Kernel Patch Protection (PatchGuard)

- Periodically monitor critical code and data structures in the kernel.
  - If a change is detected, trigger a bugcheck.


:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
40% 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: KERNEL_SECURITY_CHECK_FAILURE

Kernel Patch Protection (PatchGuard)

- Periodically monitor critical code and data structures in the kernel.
  - If a change is detected, trigger a bugcheck.

- Great for Security!
  - Prevention of Out-of-Bound Write Vulnerabilities etc.

Kernel Patch Protection (PatchGuard)

- Periodically monitor critical code and data structures in the kernel.
  - If a change is detected, trigger a bugcheck.

- Great for Security!
  - Prevention of Out-of-Bound Write Vulnerabilities etc.

- Terrible for Security!
  - No more kernel changes = No more inline hooks = No more monitoring!

Microsoft's Answer

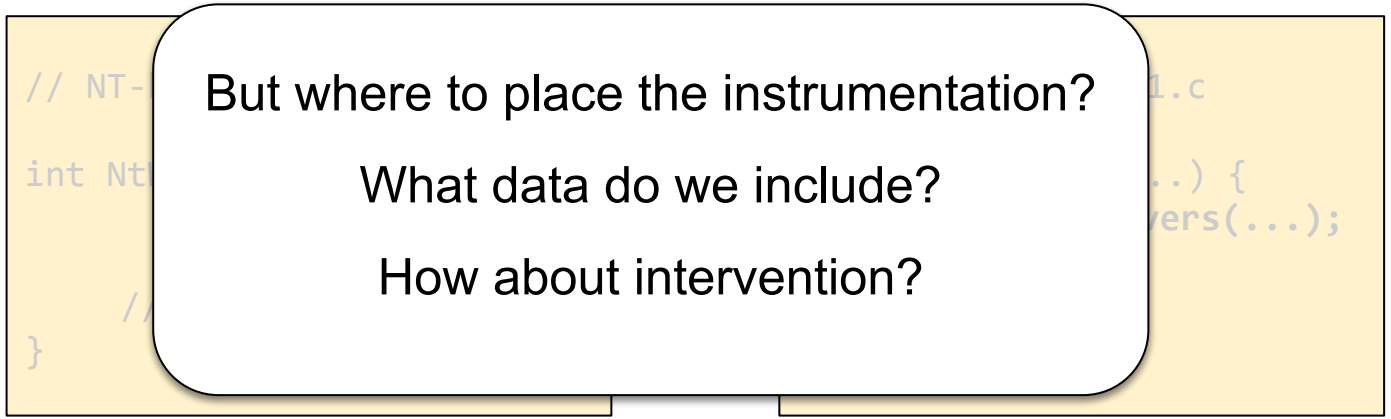
- Preemptively instrument important kernel code to prevent patches:

```
// NT-kernel-winxp.c

int NtWriteFile(...) {


     // ...
}
```

```
// NT-kernel-win11.c

int NtWriteFile(...) {
     notify_observers(...);

     // ...
}
```

Microsoft's Answer

- Preemptively instrument important kernel code to prevent patches:



“That’s just an engineering problem”

So… Problems Solved?


STREET FIGHTER V
UNIVERSITY OF TWENTE.

Sidestep: CAPCOM Street Fighter V

- In 2016 CAPCOM released Street Fighter V.

CAPCOM®

Sidestep: CAPCOM Street Fighter V

- In 2016 CAPCOM released Street Fighter V.
- Tournaments in user space call for Anti-Cheat.

CAPCOM®

Sidestep: CAPCOM Street Fighter V

- In 2016 CAPCOM released Street Fighter V.
- Tournaments in user space call for Anti-Cheat.
- Anti-Cheat cannot live in userspace,
  so CAPCOM made a kernel space Anti-Cheat.

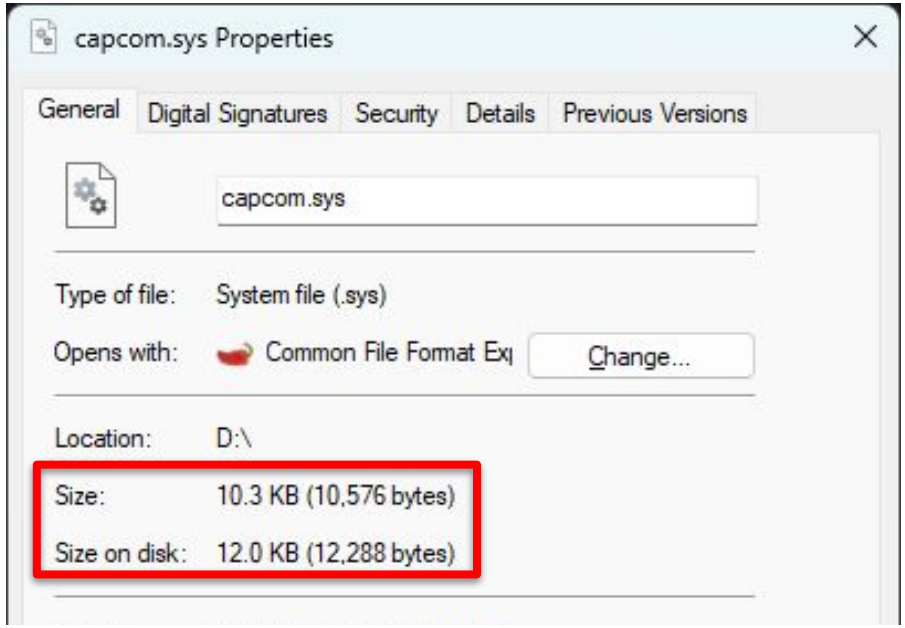
CAPCOM®

Sidestep: CAPCOM Street Fighter V

- In 2016 CAPCOM released Street Fighter V.
- Tournaments in user space call for Anti-Cheat.
- Anti-Cheat cannot live in userspace,
  so CAPCOM made a kernel space Anti-Cheat.
- However, they were a bit… practical.

CAPCOM®

CAPCOM's Anti-Cheat Driver



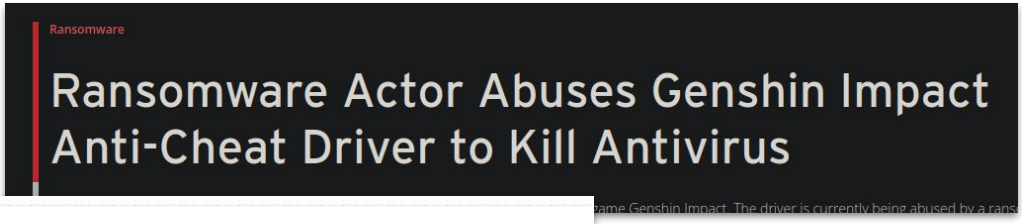
CAPCOM's Anti-Cheat Driver

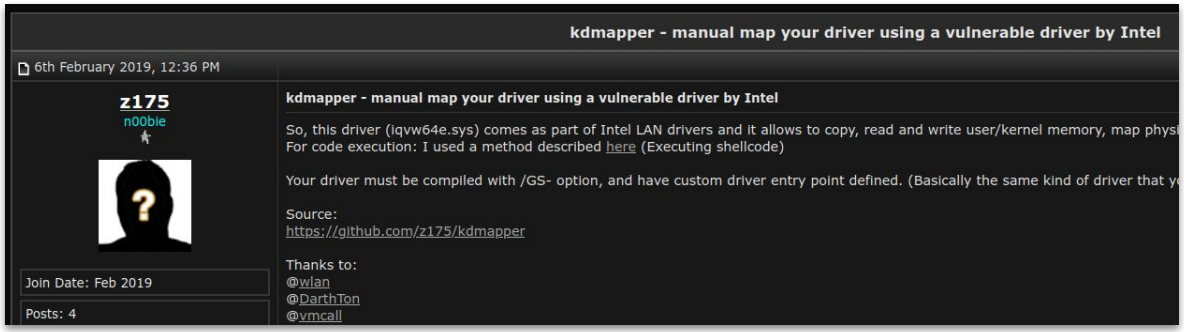
Decompile: IoCtl_Handler - (Capcom.sys)

```
1
2  bool IoCtl_Handler(byte *data_passed_in_from_userspace)
3  {
4    ulonglong old_cr4;
5    code *function_pointer;
6    MmGetSystemRoutineAddress *pMmGetSystemRoutineAddress;
7    byte *magic_value;
8
9    magic_value = *(byte **)(data_passed_in_from_userspace + -8);
10   if (magic_value == data_passed_in_from_userspace) {
11     pMmGetSystemRoutineAddress = MmGetSystemRoutineAddress_exref;
12     old_cr4 = 0;
13     function_pointer = (code *)data_passed_in_from_userspace;
14
15     (*function_pointer)(pMmGetSystemRoutineAddress);
16
17   }
18   return magic_value == data_passed_in_from_userspace;
19 }
20
```

Out of scope of Thread Model?

Out of scope of Thread Model?





Moving forward

- Hook/instrument deeper?
  - The lower level you place the hooks, the less interpretable the information gets.
  - Is it really helping at this point?

Moving forward

- Hook/instrument deeper?
  - The lower level you place the hooks, the less interpretable the information gets.
  - Is it really helping at this point?

- Fully banish all kernel space code unless absolutely system critical.
  - Microsoft is starting to do this more in Win10-11.

Moving forward

- Hook/instrument deeper?
  - The lower level you place the hooks, the less interpretable the information gets.
  - Is it really helping at this point?

- Fully banish all kernel space code unless absolutely system critical.
  - Microsoft is starting to do this more in Win10-11.

- Shift to a different paradigm on how software is installed on Windows.
  - App Stores, Package managers, etc.


Thanks!
UNIVERSITY
OF TWENTE.