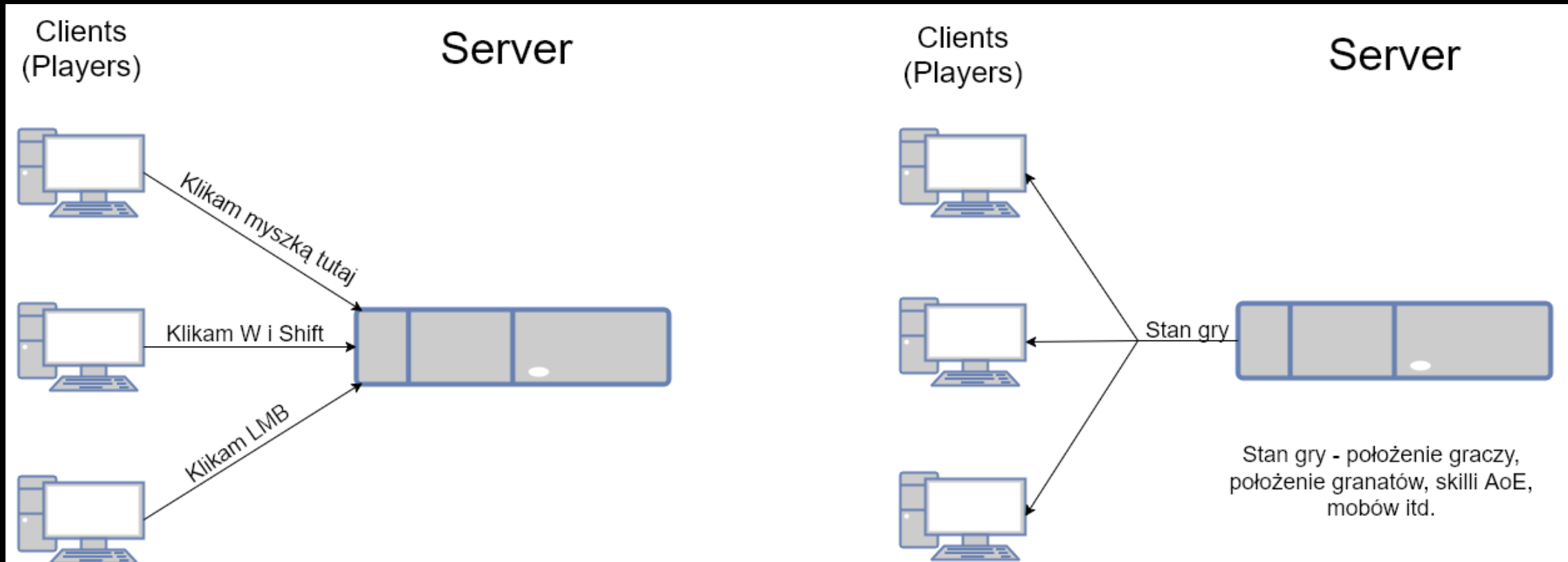


Anti-cheats vs cheats

Kacper Müller

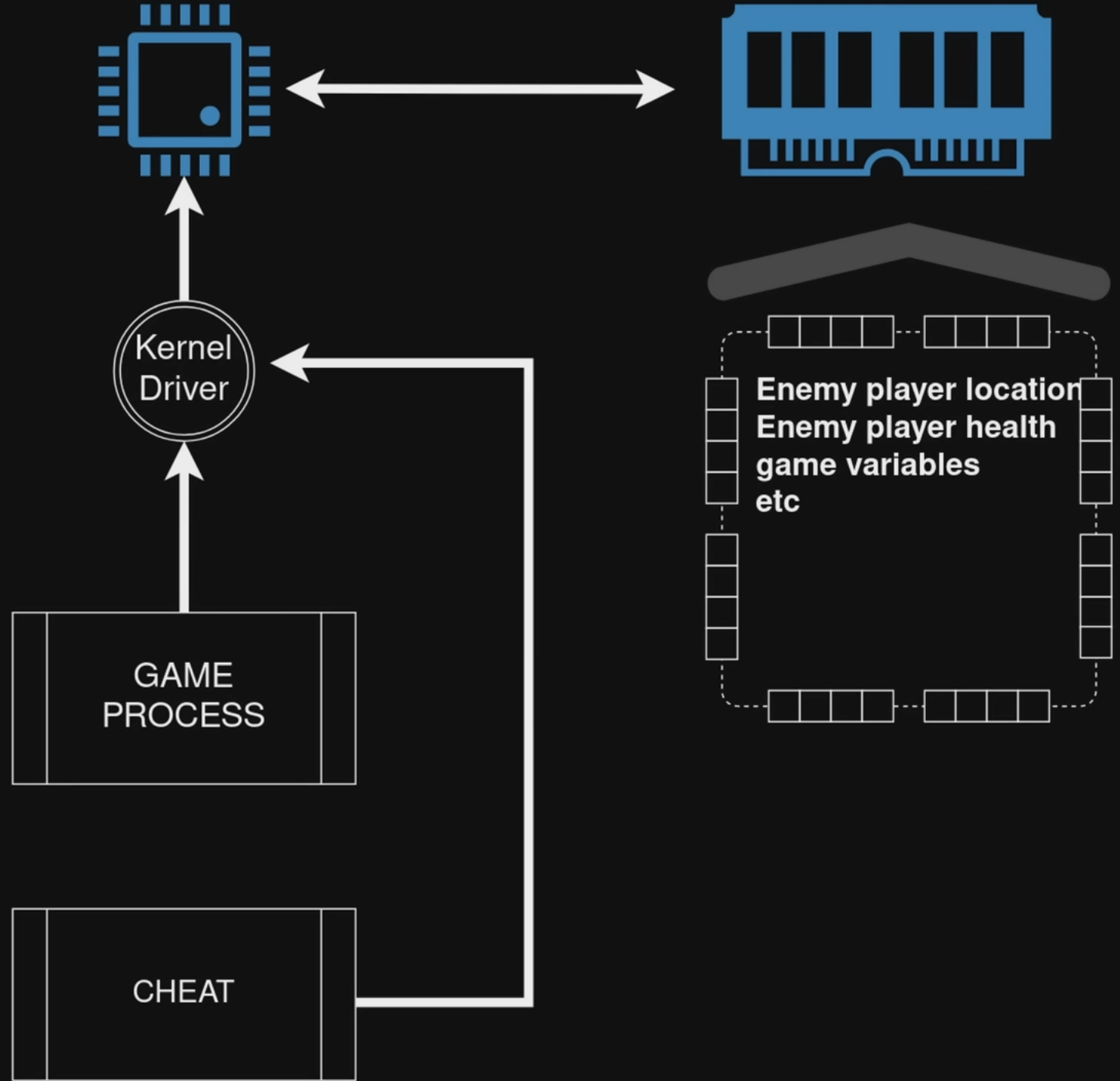


How do online games work?

Can you just read
it from RAM?

Memory read cheats – reading
memory and then presenting this
information on screen.

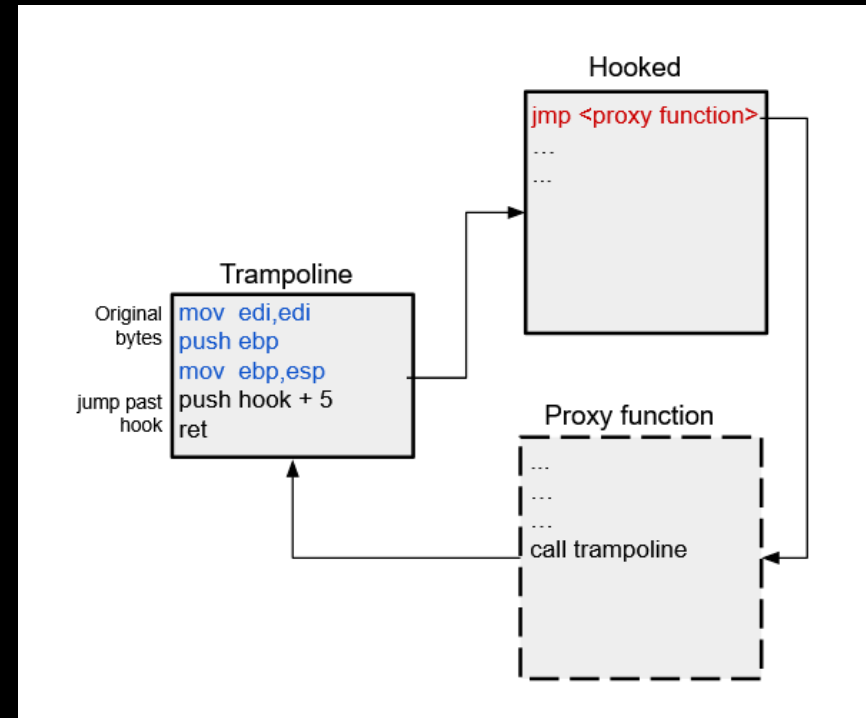
ESP – extra sensory perception e.g.
wallhack, radar

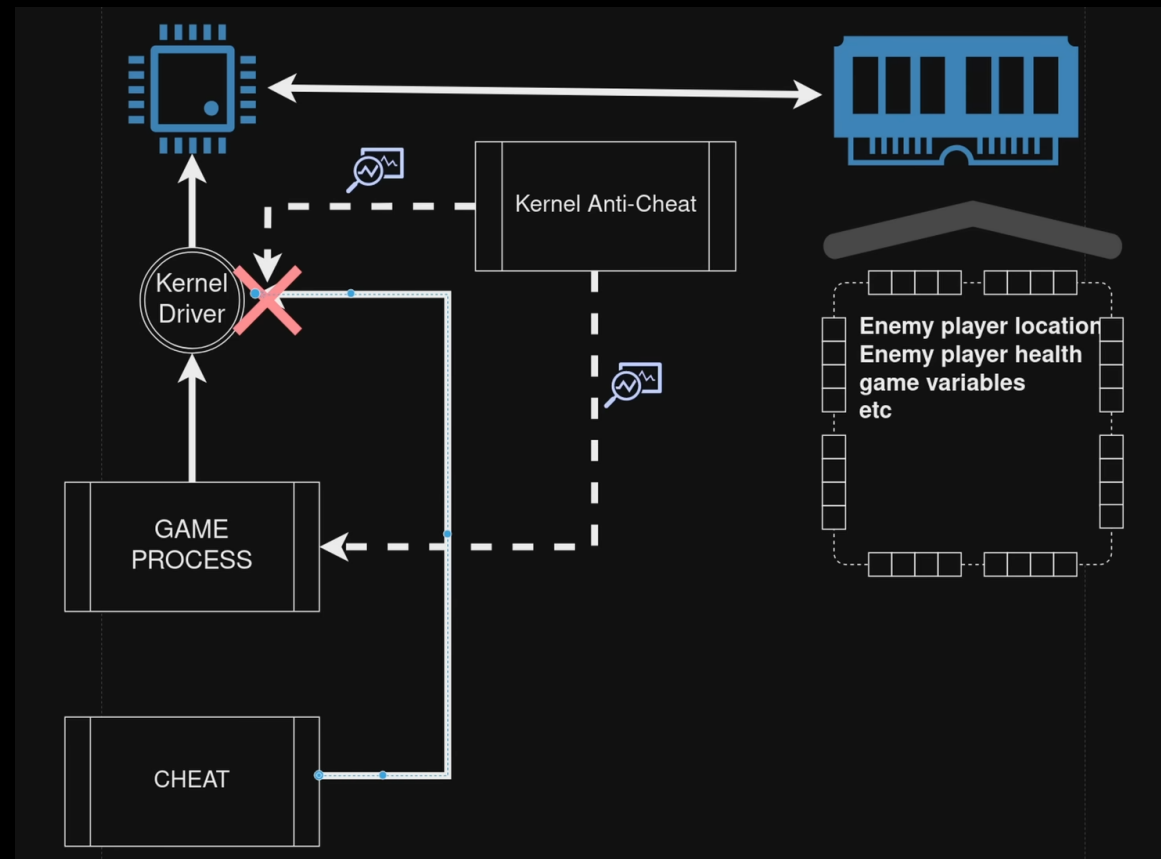
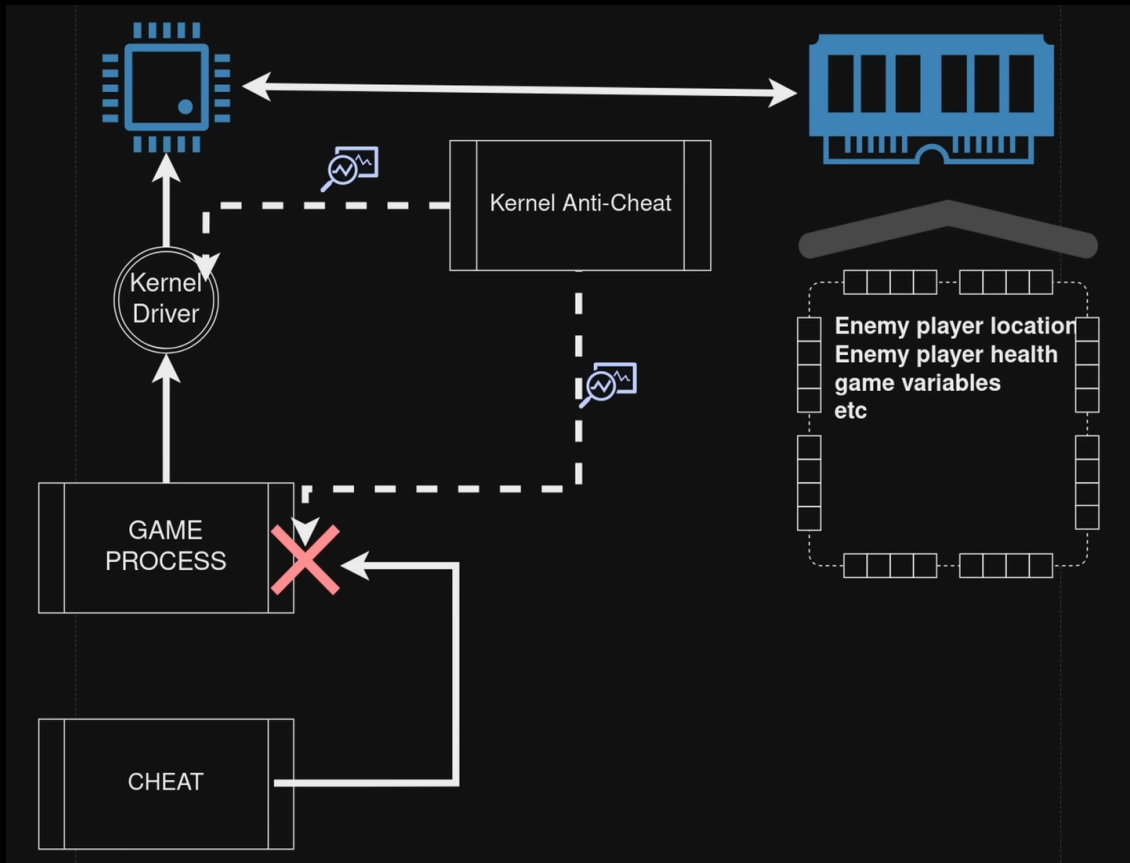


Ways of reading memory

- **External cheat** – separate process, makes system's API calls to read into the game memory space and resolve players locations, their HP...
- **Internal cheats** – injected, mapped DLL into game client, reading and writing to app memory through game instance by **hooking** function calls, which means less latency.

To **hook** a function means intercepting or redirecting a function to run your code. It can be done by adding jump in machine code

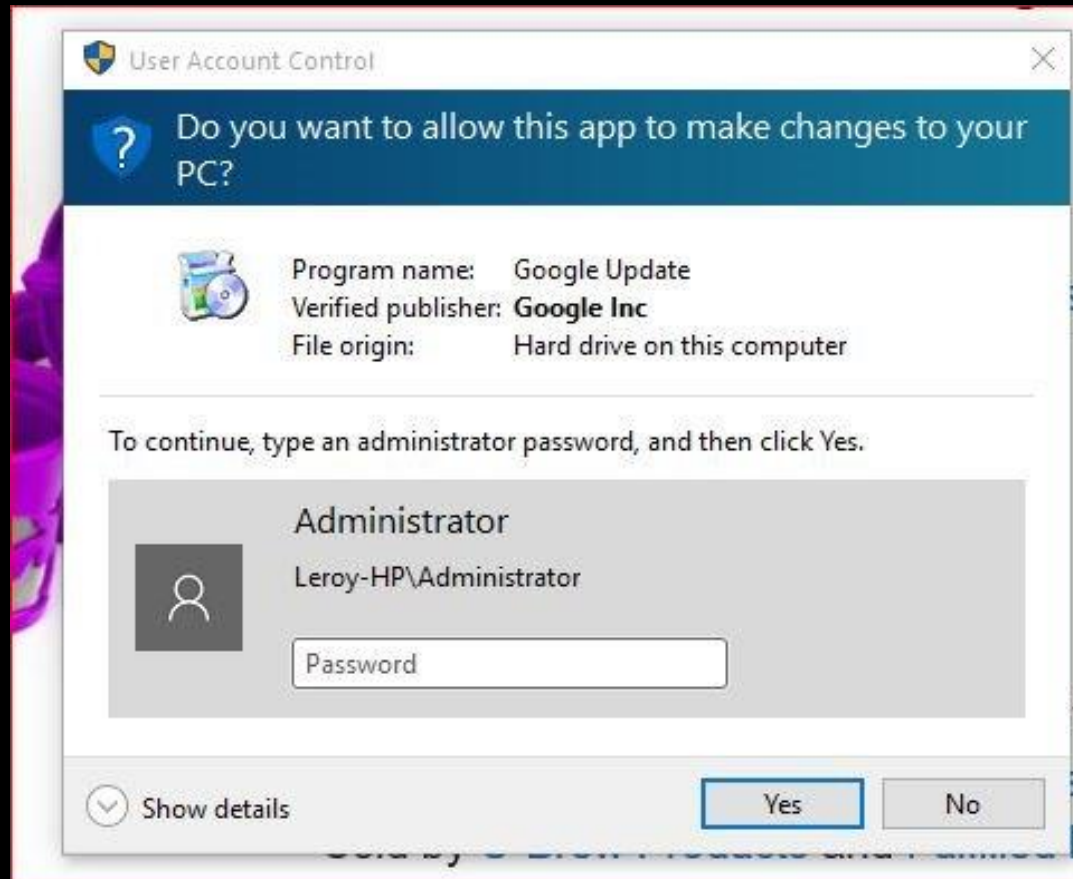




Internal vs external
cheats

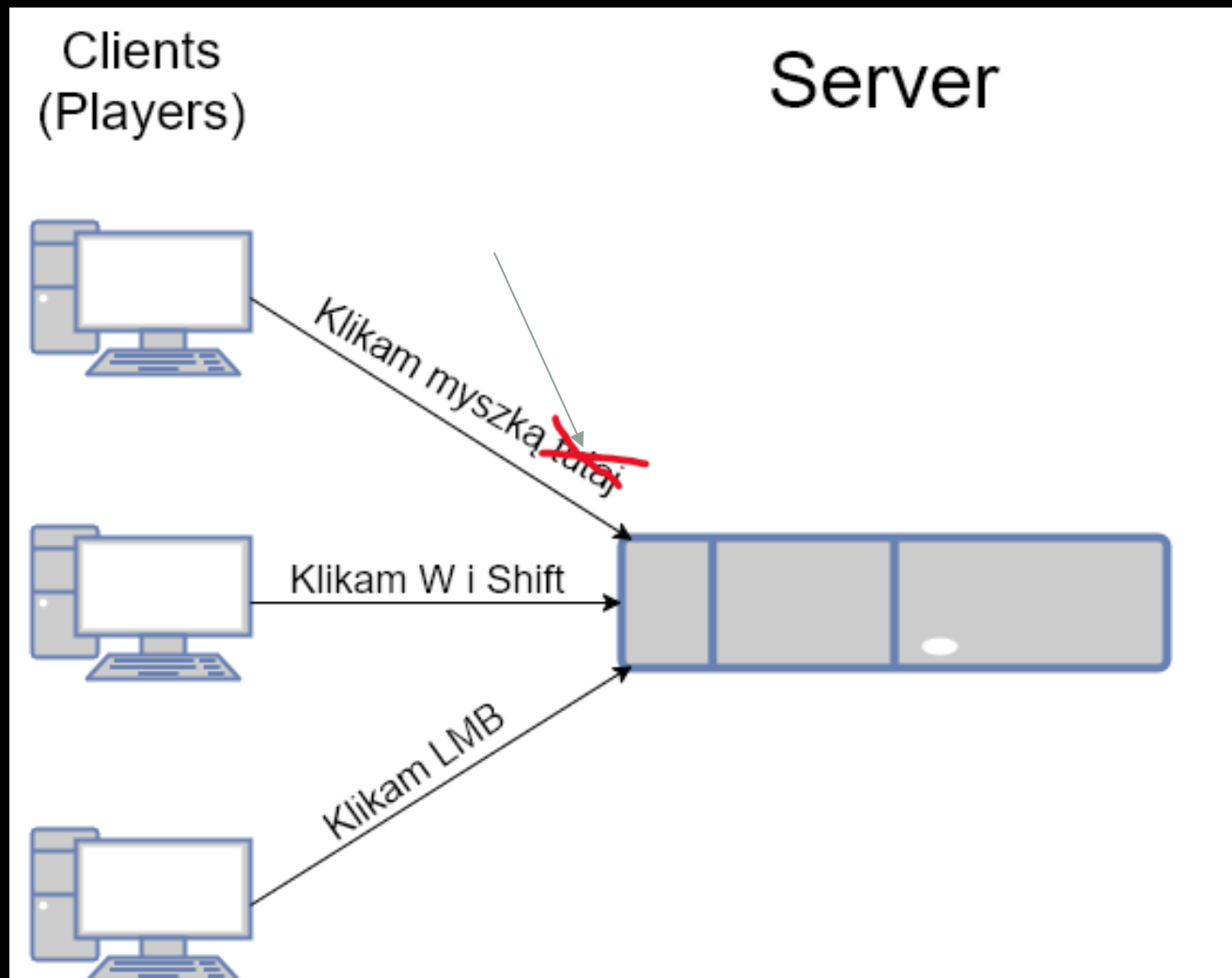
Functions of Windows API: `OpenProcess()`, `ReadProcessMemory()`.

But can't processes only use their memory? Well, you can just give extra permission to the cheat via a UAC prompt



Controlling input

- Aimbots, trigger bots etc.
- Taking actions based on what was read
- Correcting mouse movement

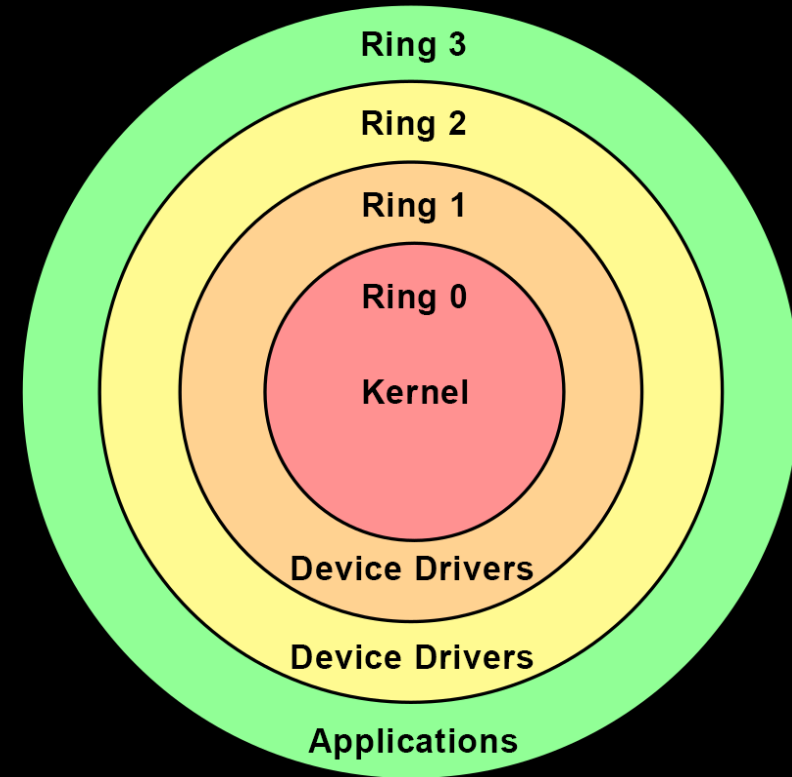


Historic cheats countering

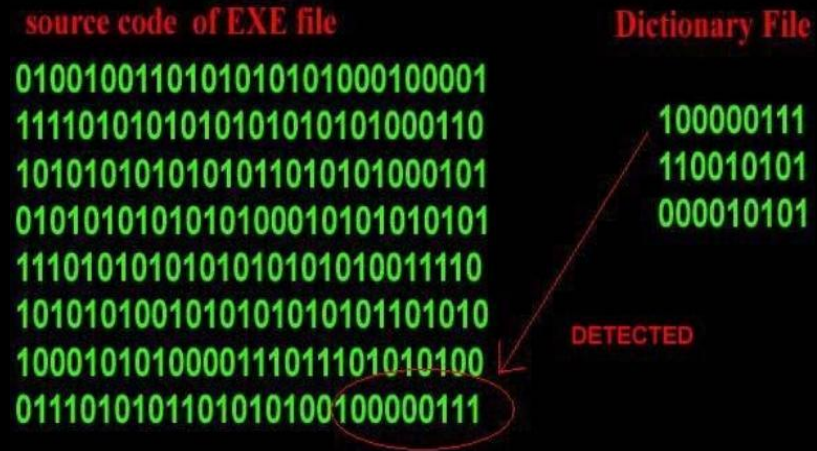
- Servers were community driven (CS 1.6 times).
- If someone was clearly using cheats, they were reported and admins had to block them manually, or it could be automated, but still based on player's reports.
- Special Hack vs hack (HvH) servers, only for cheating players
- Now: overwatch

VAC

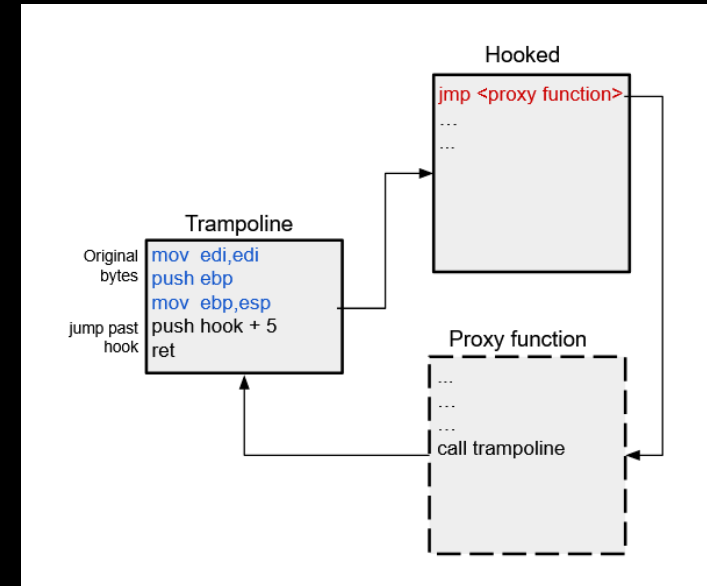
- Runs in user mode – ring 3, not kernel (same as previously mentioned cheats)
- Uses delayed bans, so it's harder to reverse engineer vac
- Misses: kernel cheats, **manual mapping** (changing load library function so that we can inject DLL without adding it to module list), DMA



How does VAC detect cheats?



Application's signature
(byte patterns in DLLs, modules)



Hooking functions, like
ReadProcessMemory

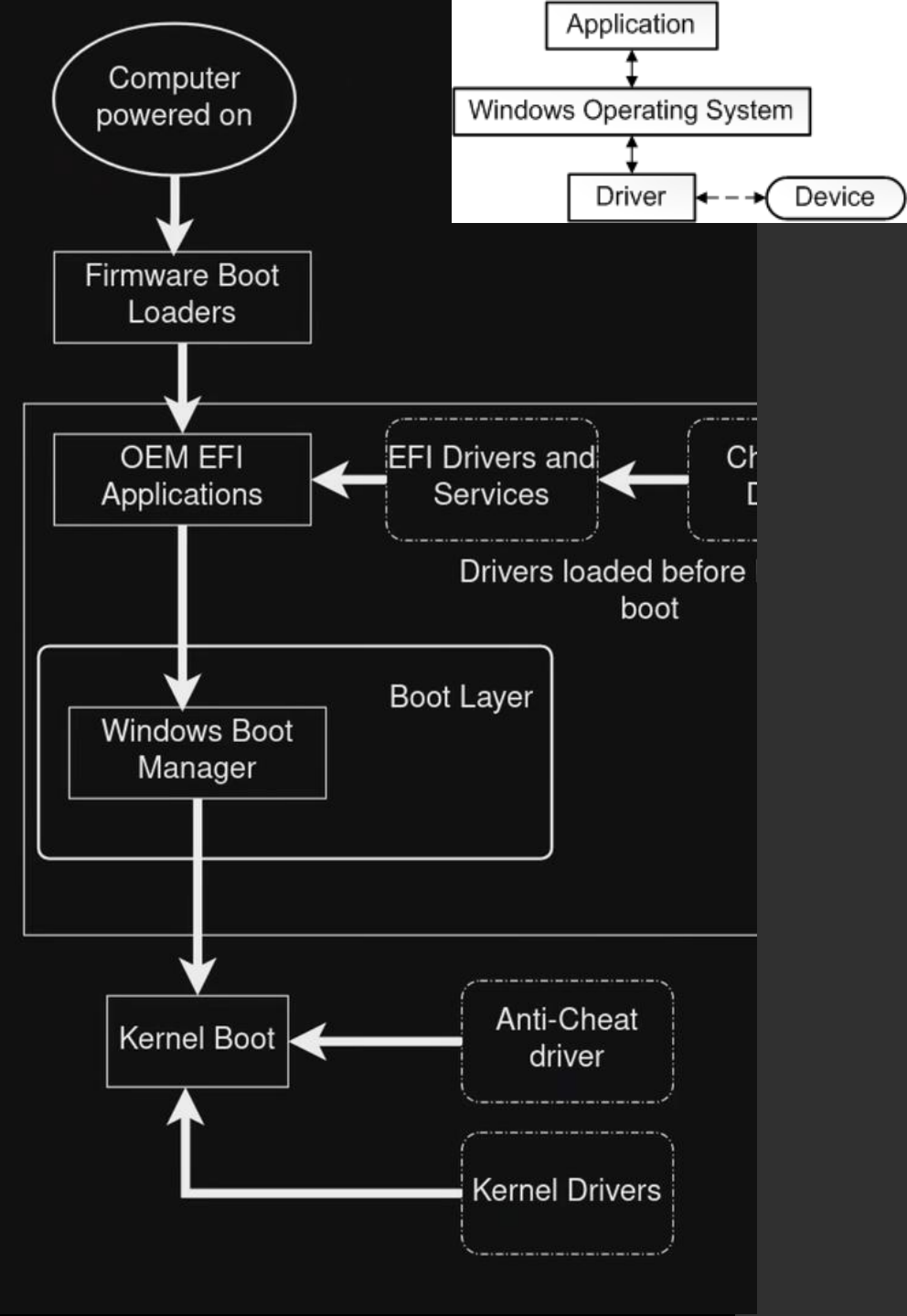
Forsaken cheating

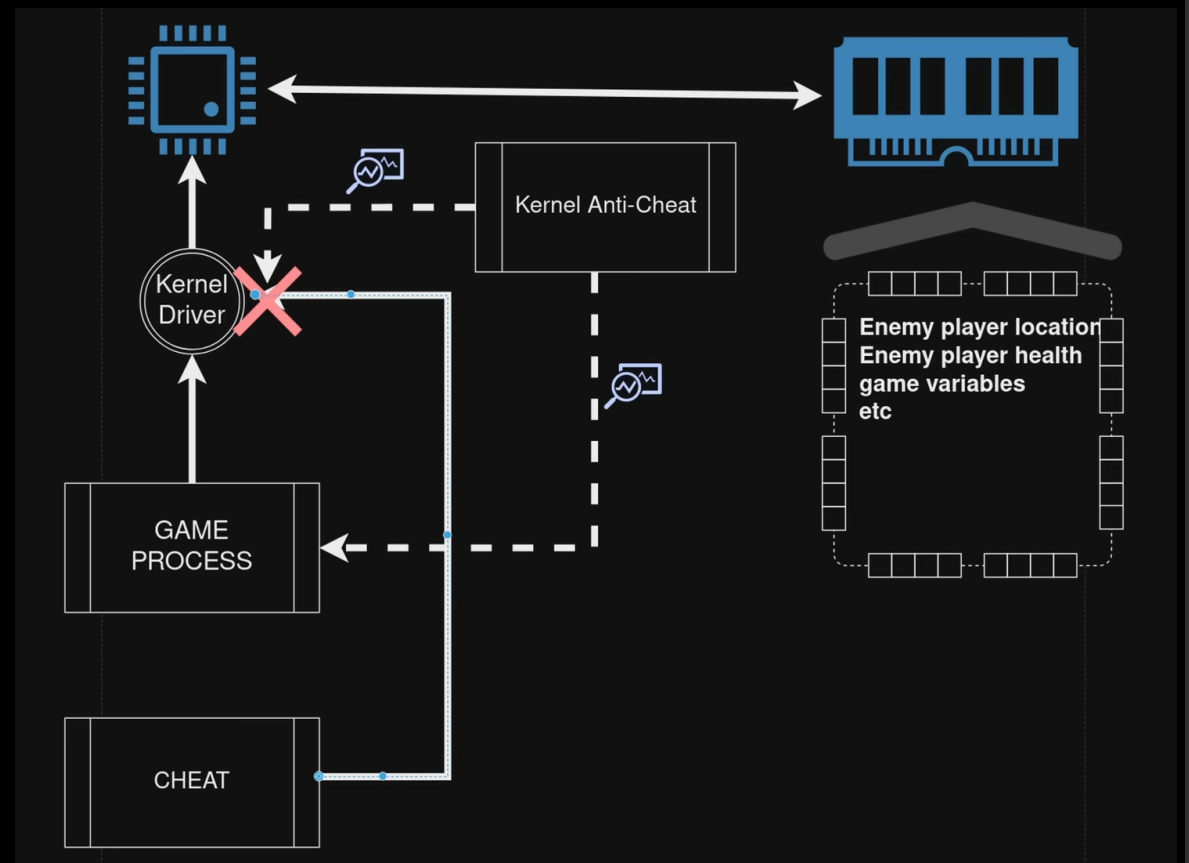
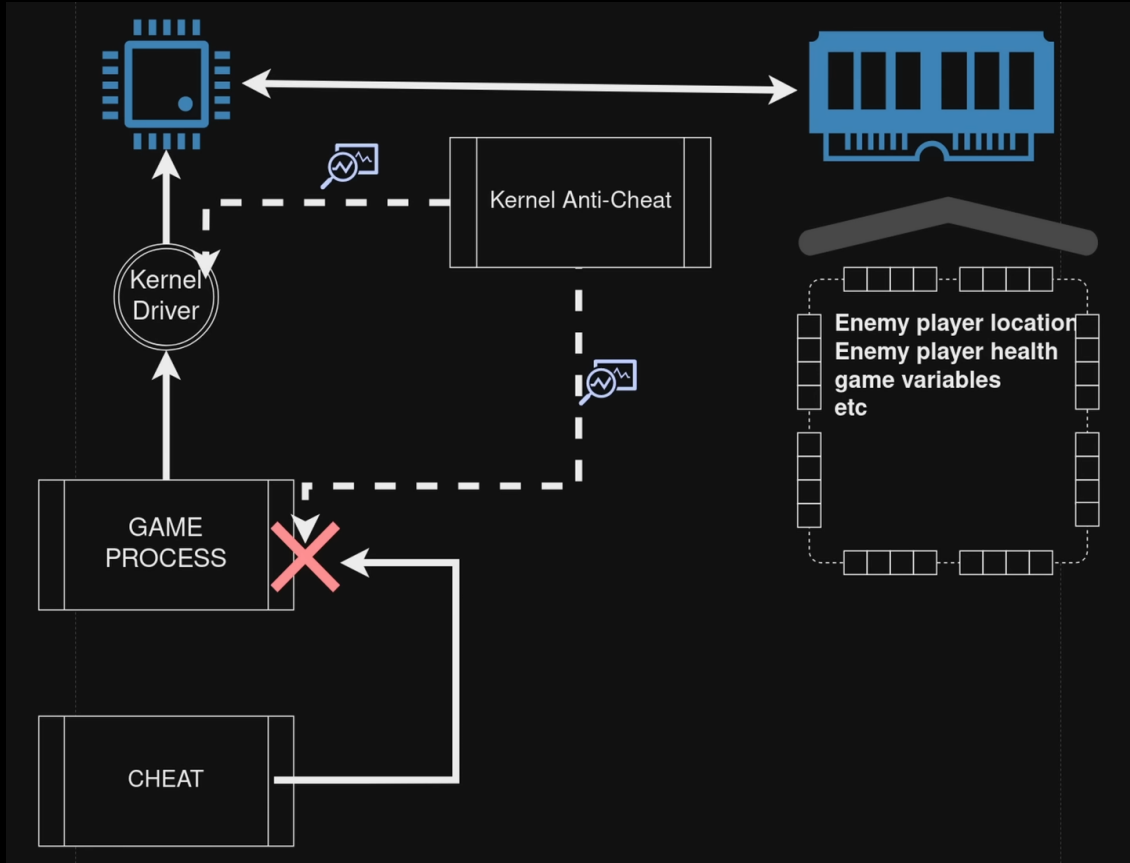


Layout		
ch Results in Administrator > Local > Temp > Rar\$EXa3508.40620 > og		
Name	Date modified	Type
word.bak	10/5/2018 2:53 PM	BAK File
word.exe	10/17/2018 6:38 PM	Application
word.exe.log	10/5/2018 2:54 PM	Text Document

Kernel anti-cheats

- Faceit, ESEA, Easy Anti Cheat, Vanguard
- System that monitors whole PC, but focuses on the game.
- Loads during system boot in ring 0.
- It can detect cheats a lot easier (OB register callback). In some cases, it's the only way.
- Still can be bypassed...
- ESEA used players' GPUs to mine Bitcoin





Internal vs external
cheats and their detection

Kernel cheats

Driver that makes client-level anti-cheats useless (using OB register callback).

When it comes to kernel anti-cheats, it's a battle. Fighting fire with fire.

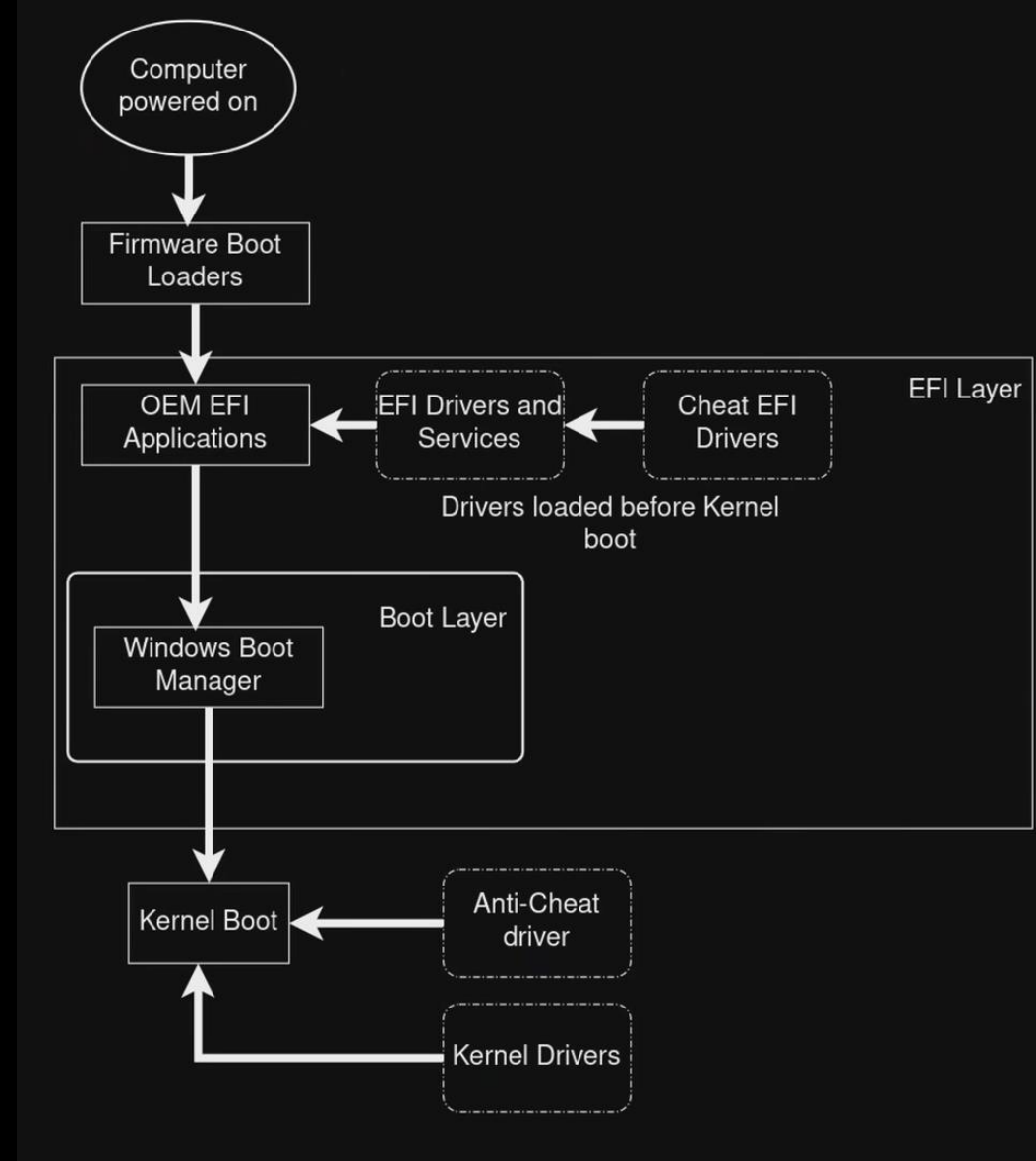
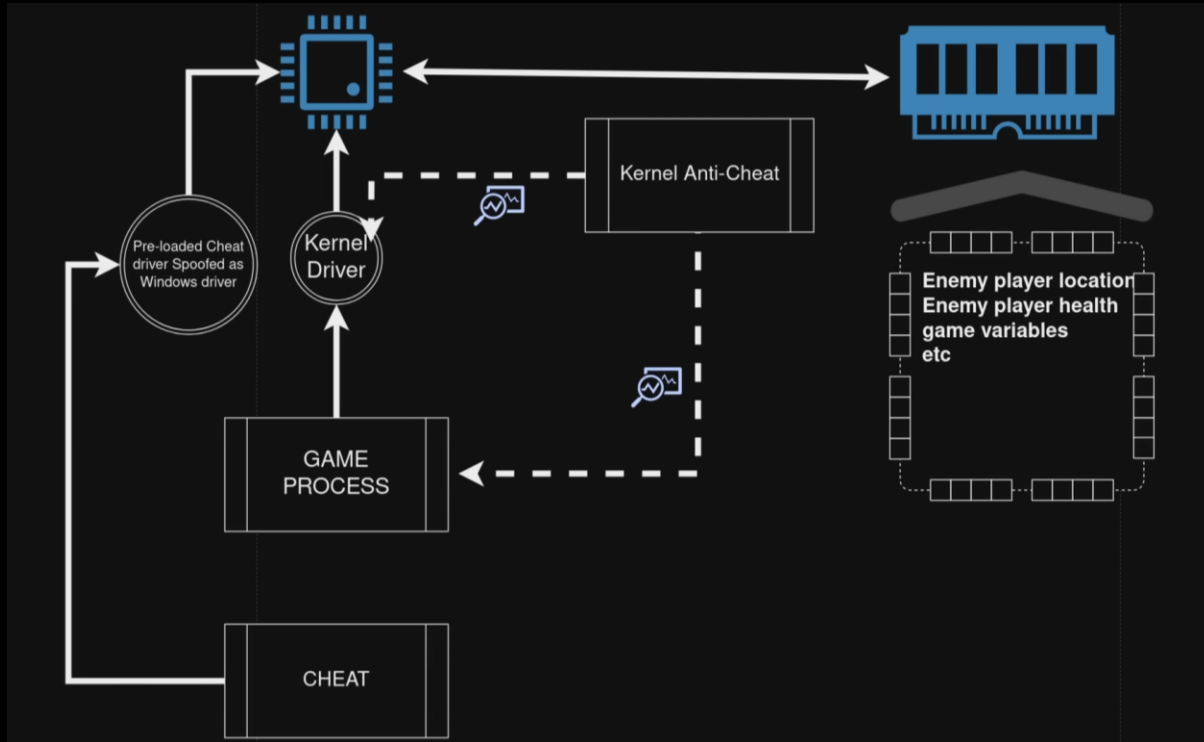
"Now, while most players might find the idea of a corrupted Windows installation objectionable, a disturbing number of cheaters have shown themselves to be *downright enthusiastic about the opportunity to jump onto some guy's botnet in exchange for the ability to orbwalk.*"

"/dev/null: Anti-Cheat Kernel Driver", mirageofpenguins

<https://www.leagueoflegends.com/en-gb/news/dev/dev-null-anti-cheat-kernel-driver/>

EFI cheats

- Using drivers that load before kernel - EFI mapping
- EFI mapping - using the UEFI boot process to manually map a kernel-mode driver (or shellcode) into system memory before Windows boots, so that it's active when the OS starts — but never loaded via standard Windows APIs.
- It can hook kernel functions without being detected



To write such cheat you need to know low-level C and x86/64 assembly, knowledge of UEFI spec, memory layout, boot process.

Defending against EFI cheats

Vanguard requires Windows 11 machines to use secure boot (checks signatures of drivers, so they can only come from Original Equipment Manufacturer - OEM). It enforces clean EFI boot. Doesn't enforce that on Windows 10, so such cheats can still be used there.

Then TPM 2.0 was enforced, but again cheaters found a way to bypass that via USB booting.

DMA cheats

Installing DMA – direct memory access controller into PCI slot, accessing memory directly and processing it on another PC



Bypass any Anti-Cheats

Gaming PC



FACEIT
CHALLENGE YOUR GAME

Memory



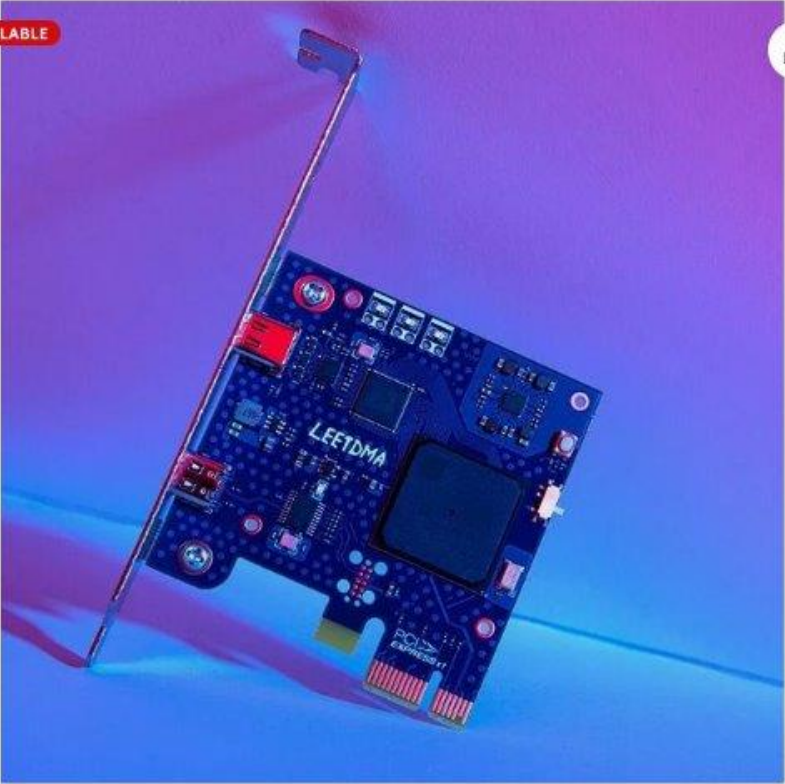
DMA card







Second PC




LAST ITEM AVAILABLE





DMA Board Direct Memory Access Clutch-Solution Enigma Ranger SCREAMER

 **Fancytech Inc** (1849)
99% positive · [Seller's other items](#) · [Contact seller](#)

US \$373.81
or Best Offer

No Interest if paid in full in 6 mo on \$149+ with [PayPal Credit](#)*

Condition: **New** ⓘ

Quantity: **Last one - 4 sold**

Buy It Now

Add to cart

Make offer

♥ Add to Watchlist

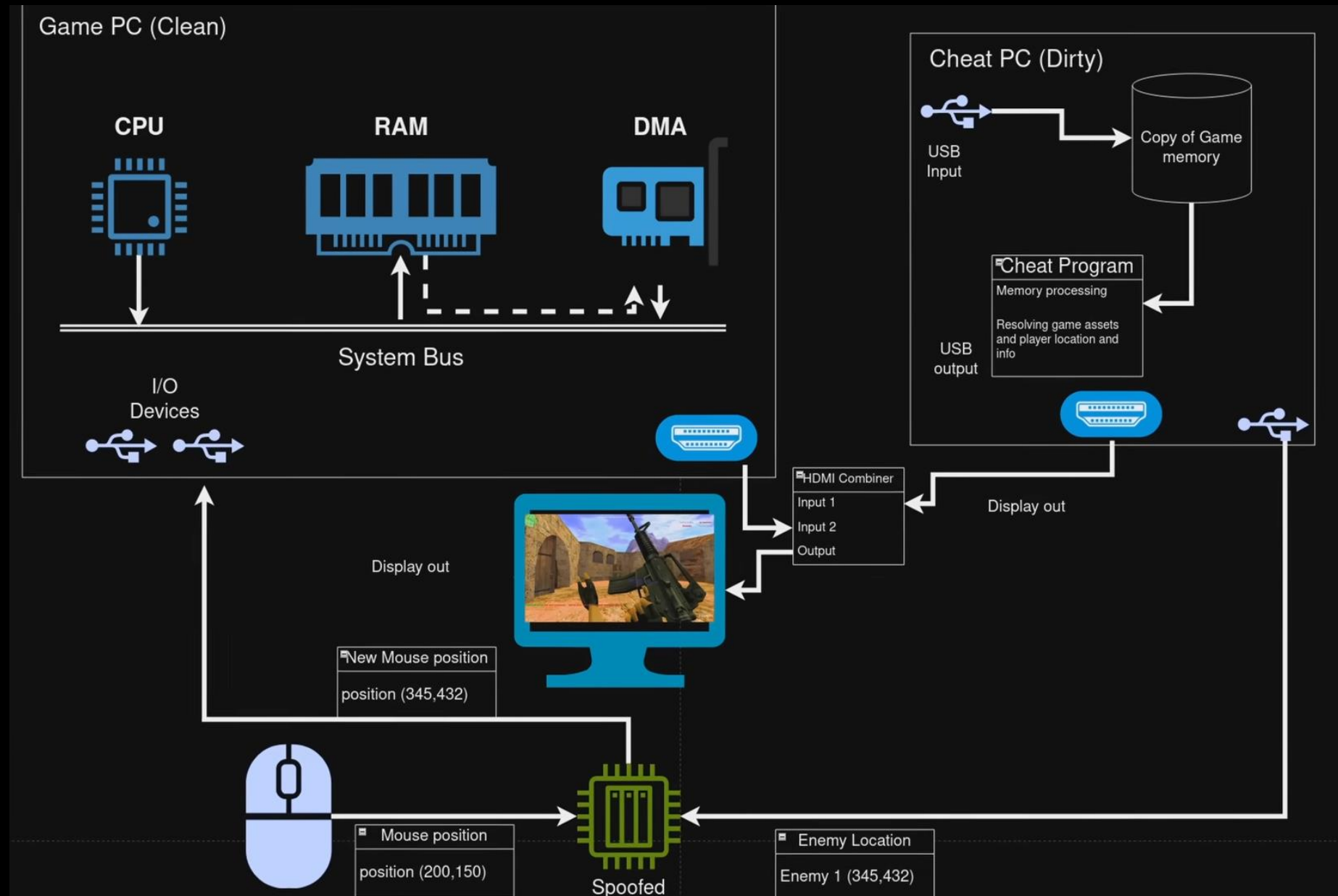
DMA cheats

DMA cheats

Video overlay box – Takes inputs from two PCs and the feeds are combined.



DMA Aimbots



DMA counting

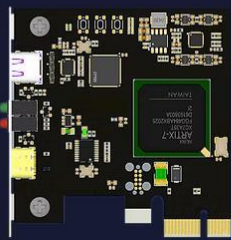
Vanguard is trying to detect DMA devices.

Though attackers are spoofing those into like network card...

DMA cheats are expensive. You need a separate computer, microcontrollers and *monthly subscriptions* for cheat developer.

DMA Hardware Store

In our DMA Store you can buy DMA devices, firmware and computer peripherals.
The best accessories for gamers.



DMA Card



Fuser



Kmbox



Firmware



Mini PC



Monitor



Xim for controller



Cable

DMA cheat for Fortnite

Only cheat



\$45

✓ Fortnite cheat for 1 month ⓘ

* you should have DMA Card with
Firmware to use this cheat

Buy now

Cheat and DMA card



\$320

✓ Fortnite cheat for 1 month ⓘ
✓ DMA PCIe Card 35T ⓘ
✓ Custom 1:1 Firmware ⓘ

* with this package you will be able to
use only radar hack on second PC

Buy now

Full package



\$530

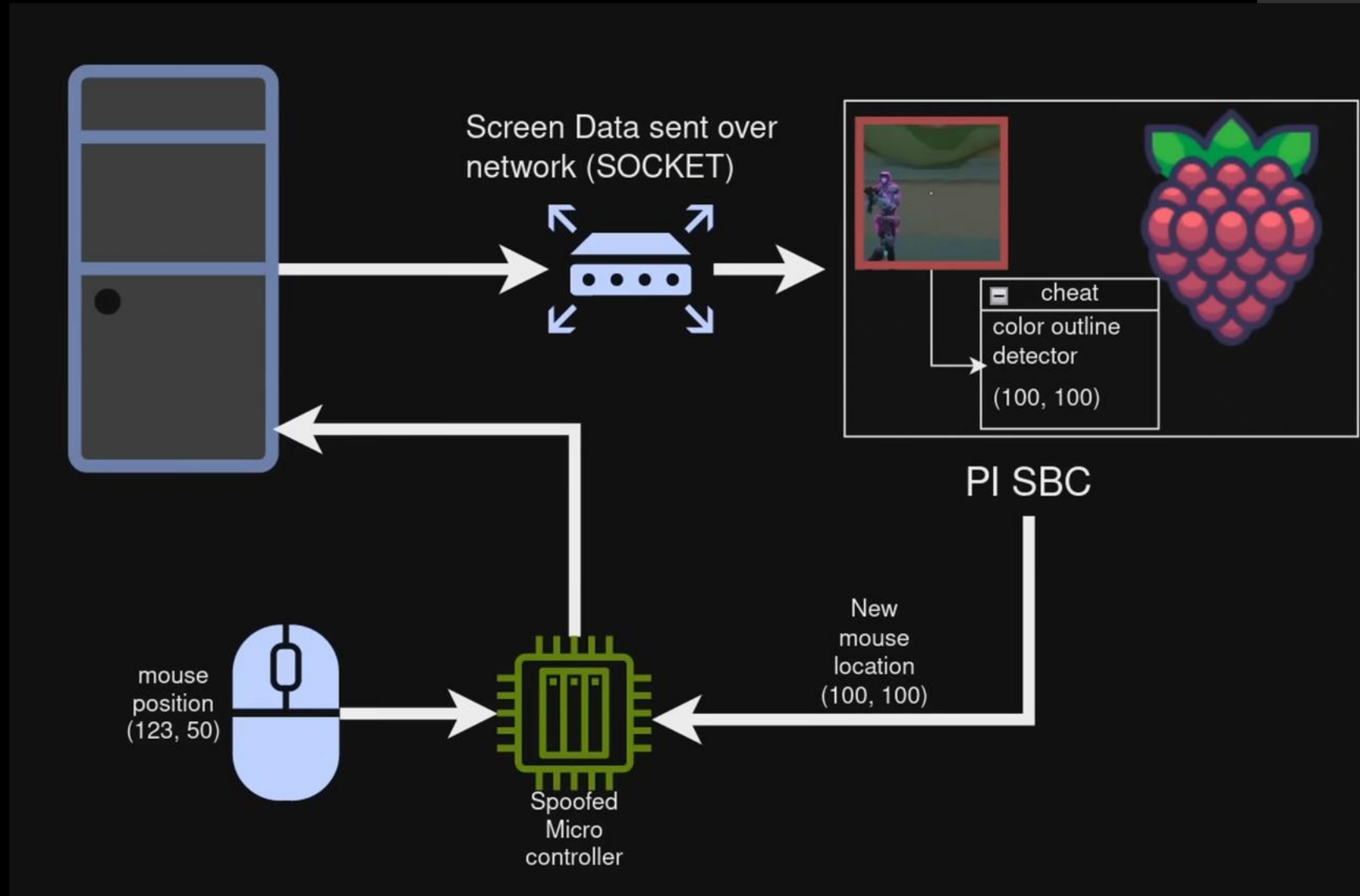
✓ Fortnite cheat for 1 month ⓘ
✓ DMA PCIe Card 35T ⓘ
✓ Custom 1:1 Firmware ⓘ
✓ Kmbox Net for Aimbot ⓘ
✓ Fuser for ESP on monitor ⓘ

Buy now

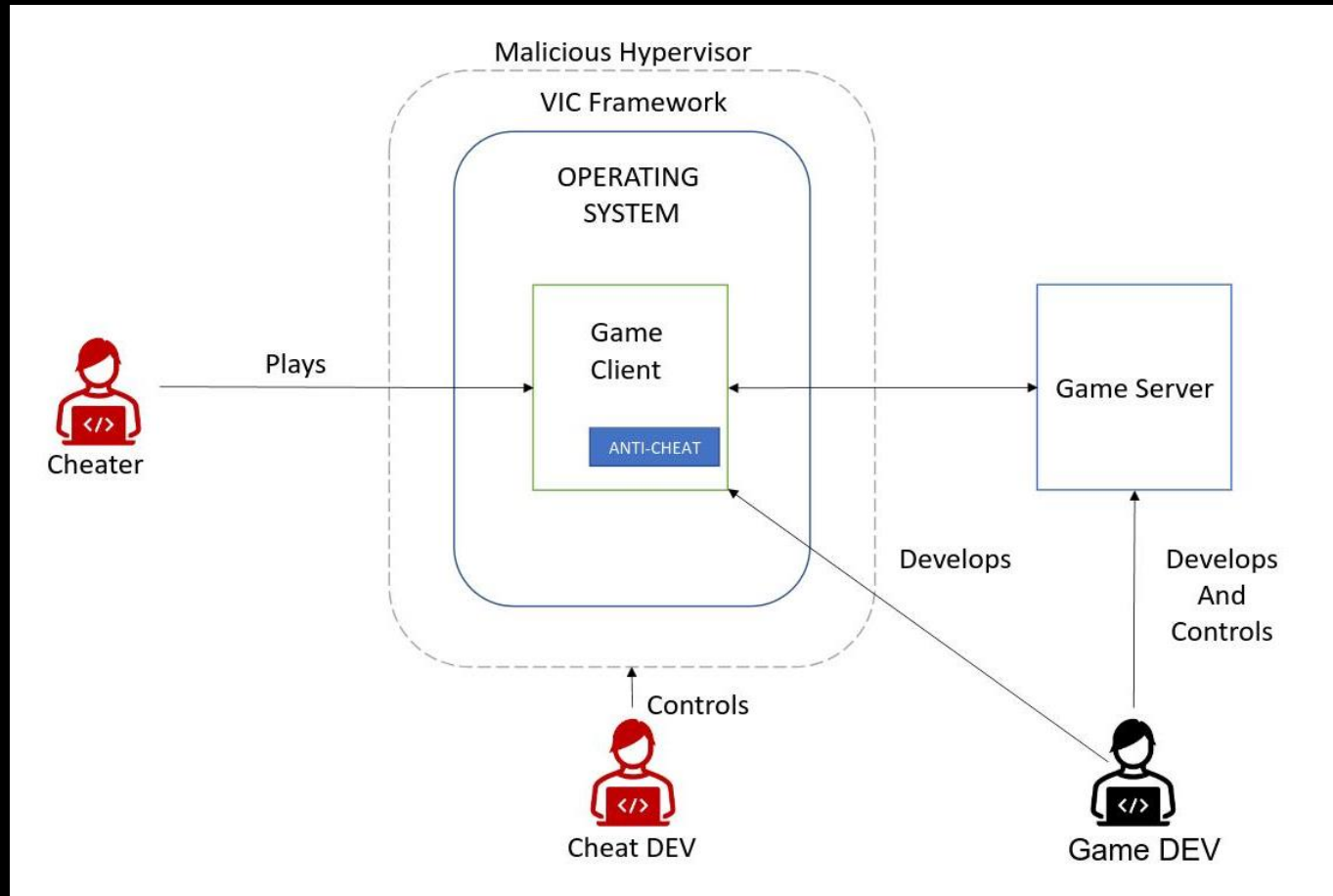
Visual cheats

Using screen output. They don't access memory, just pixels values.

Pixelbots – programs that capture screen output and correct mouse movement. Can use AI for that.



VIC - virtual machine introspection cheats



Panicos Karkallis, Jorge Blasco,

"VIC: Evasive Video Game Cheating via Virtual Machine Introspection"

Bibliography

- Panicos Karkallis, Jorge Blasco, "VIC: Evasive Video Game Cheating via Virtual Machine Introspection", <https://arxiv.org/abs/2502.12322>
- Sam Collins, Alex Pouloupoulos, Marius Muench, Tom Chothia "Anti-Cheat: Attacks and the Effectiveness of Client-Side Defences"
<https://tomchothia.gitlab.io/Papers/AntiCheat2024.pdf>
- "/dev/null: Anti-Cheat Kernel Driver", mirageofpenguins
<https://www.leagueoflegends.com/en-gb/news/dev/dev-null-anti-cheat-kernel-driver/>
- **"Hacking into Kernel Anti-Cheats: How cheaters bypass Faceit, ESEA and Vanguard anti-cheats"** by Unity Research
<https://youtu.be/RwzIq04vd0M?si=6WAOJvvF9SRWBLKc>

