Hypervisor-Based Active Data Protection for Integrity and Confidentiality of Dynamically Allocated Memory in Windows Kernel

Igor Korkin

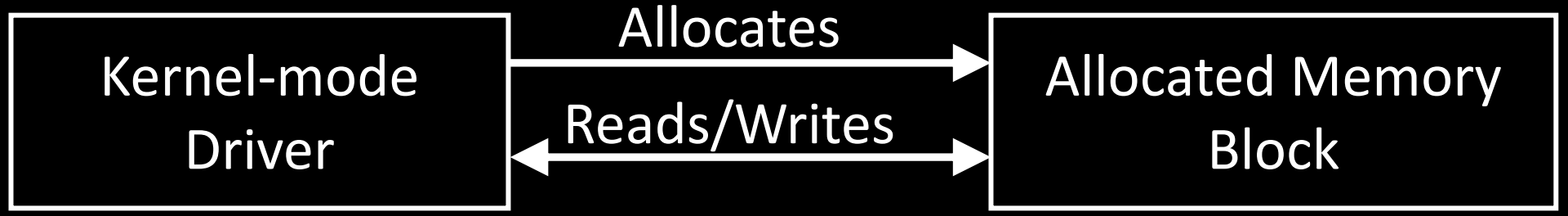
2018 ADFSL Conference

1) Dynamically Allocated Memory in Windows Kernel

Dynamically Allocated Memory in Windows Kernel

The function `ExAllocatePoolWithTag(NumberOfBytes)` —

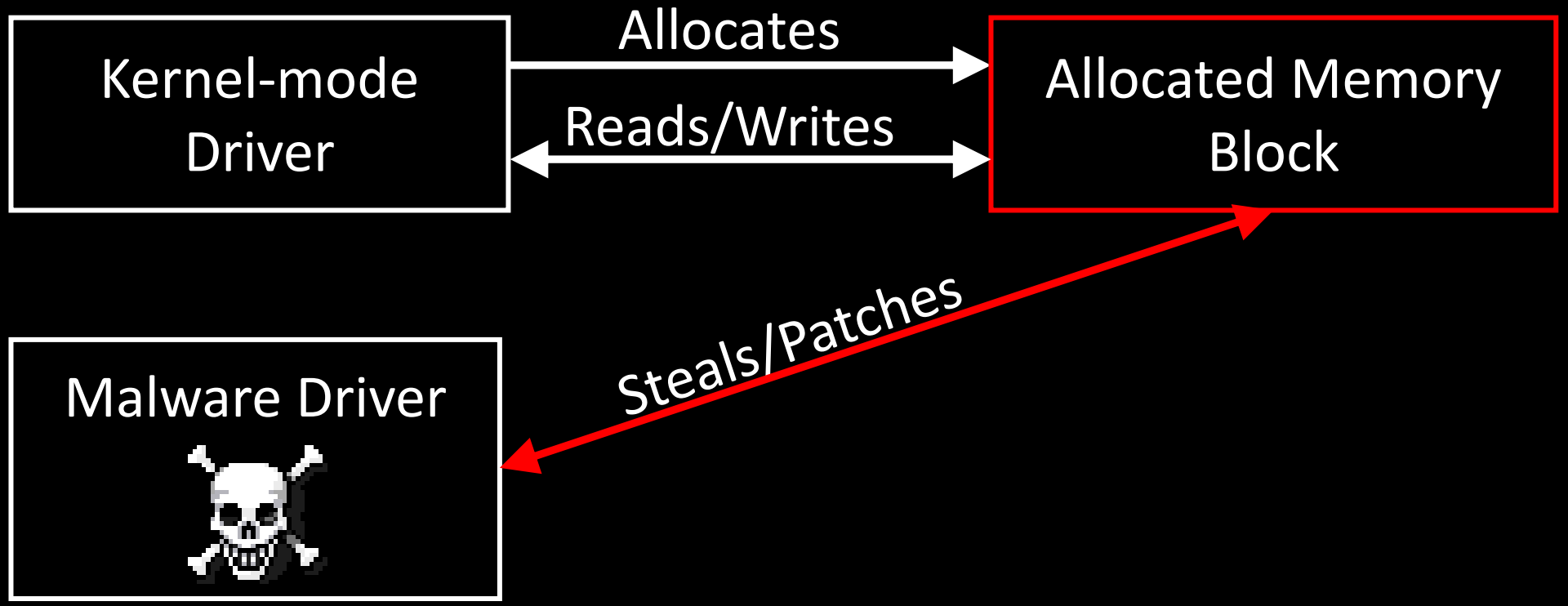
allocates memory block of the specified size and returns a pointer to it



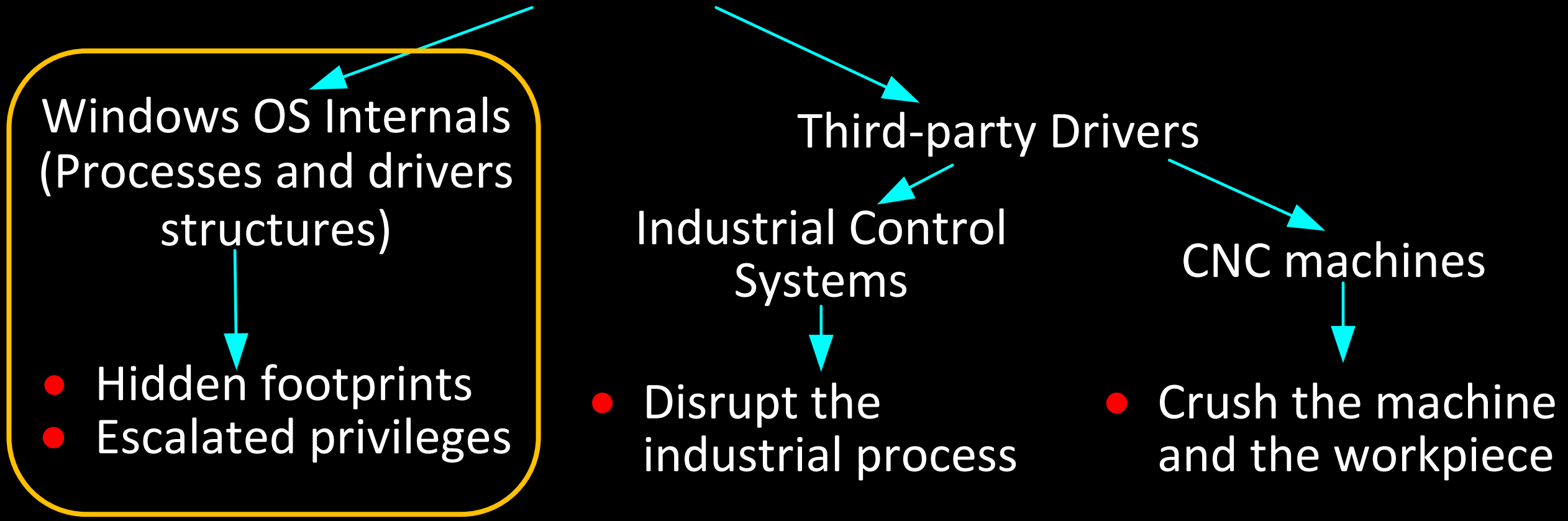
Dynamically Allocated Memory in Windows Kernel

The function `ExAllocatePoolWithTag(NumberOfBytes)` —

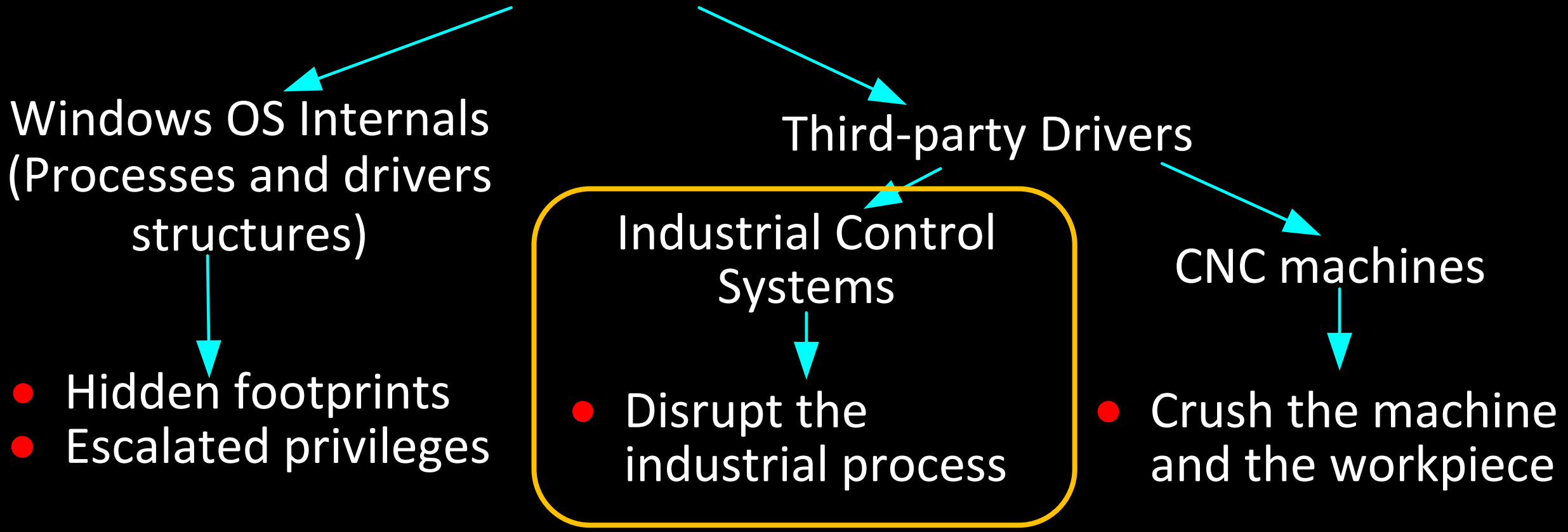
allocates memory block of the specified size and returns a pointer to it



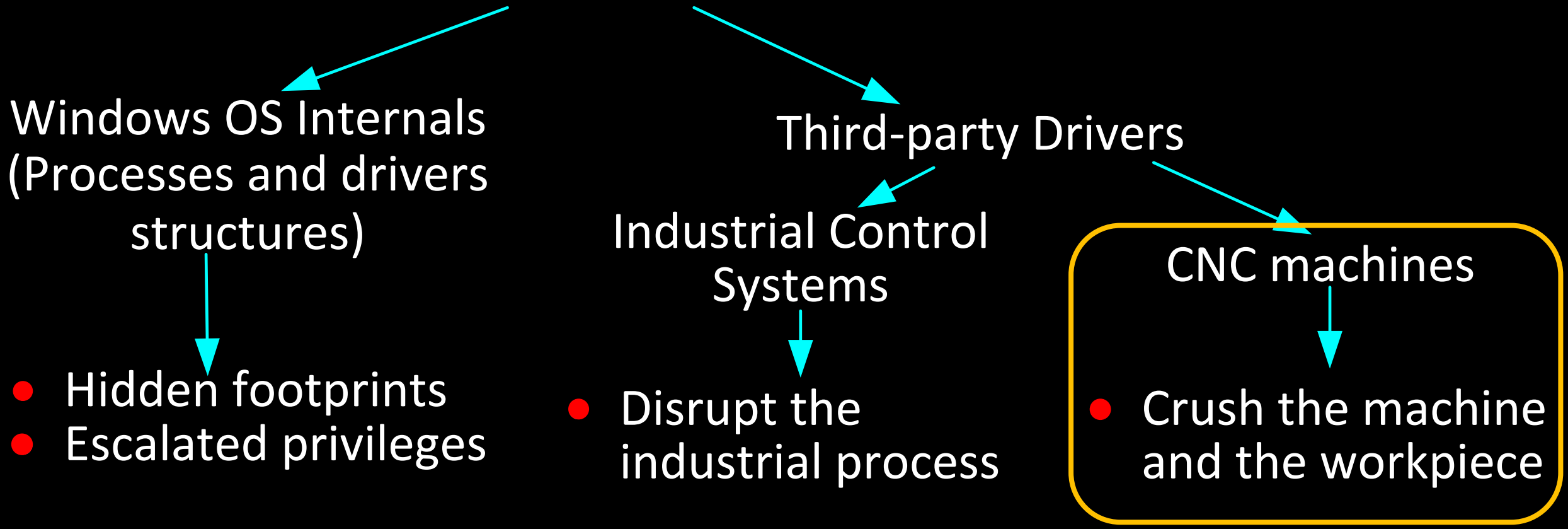
Consequences of Allocated Data Attacks



Consequences of Allocated Data Attacks

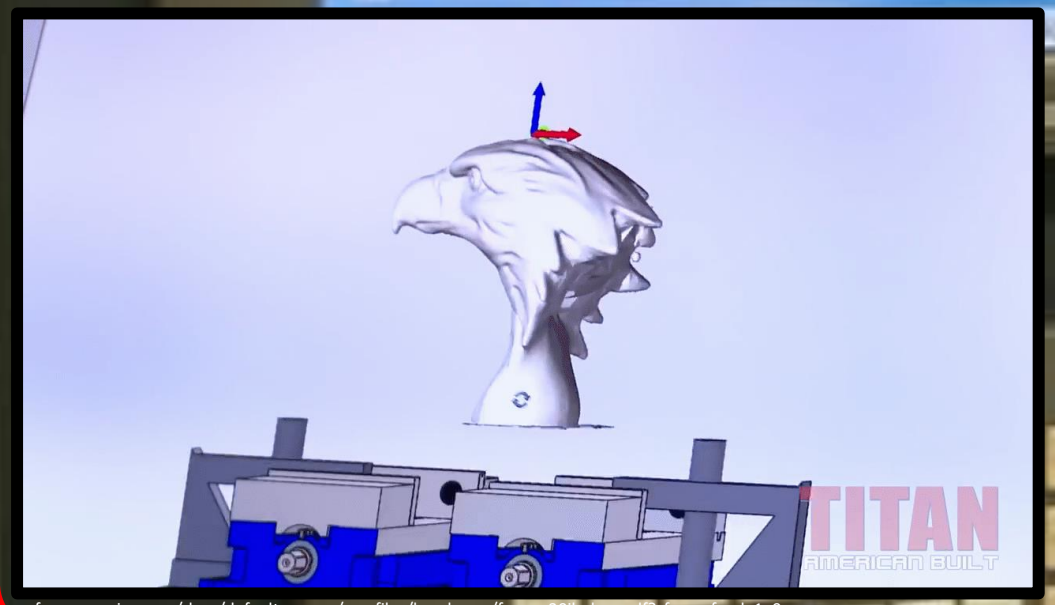


Consequences of Allocated Data Attacks

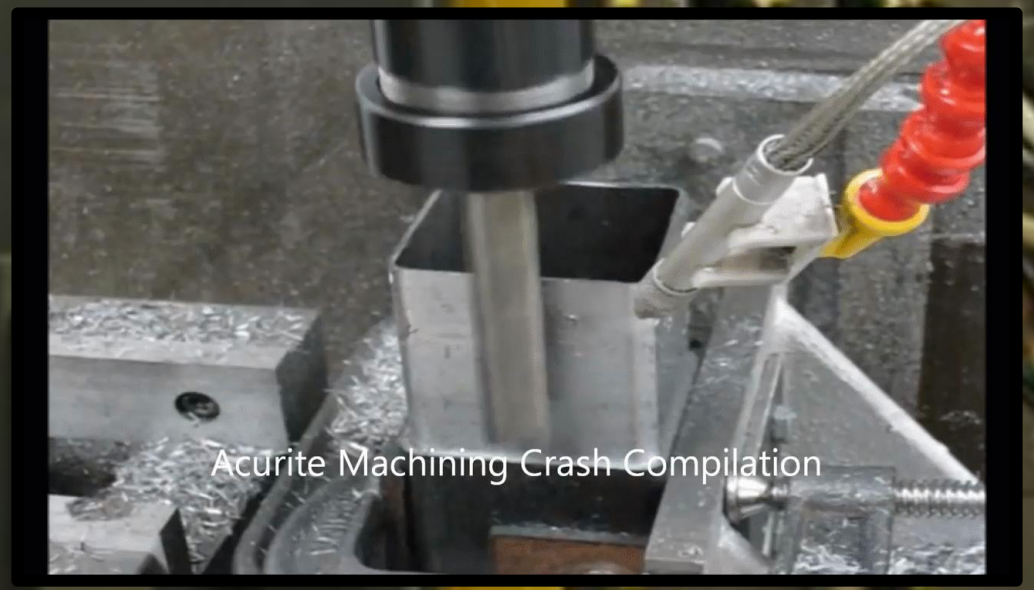


Windows-based CNC can be attacked like a PC

CNC machines make everything!



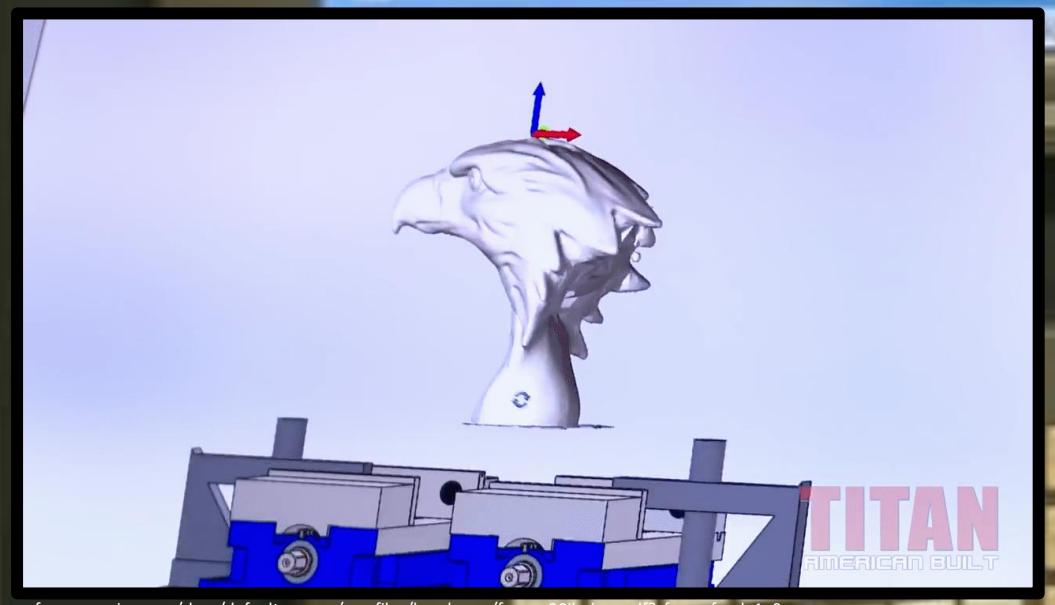
CNC machine crashes!



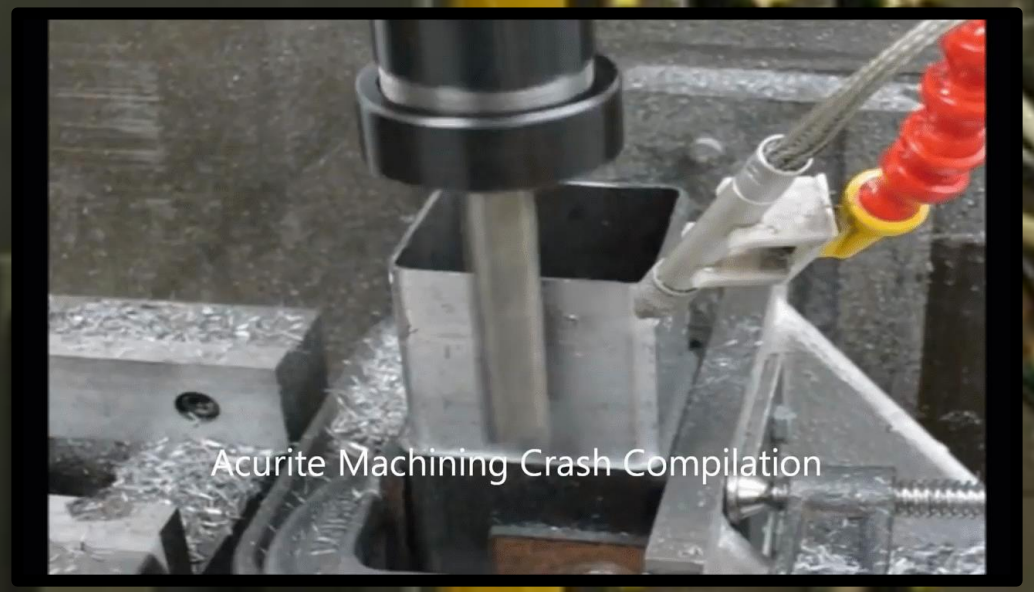
https://www.fanucamerica.com/docs/default-source/cnc-files/brochures/fanuc_30ib_low.pdf?sfvrsn=feeda1_0
https://www.youtube.com/watch?v=8CSwOebmb0A

Windows-based CNC can be attacked like a PC

CNC machines make everything!



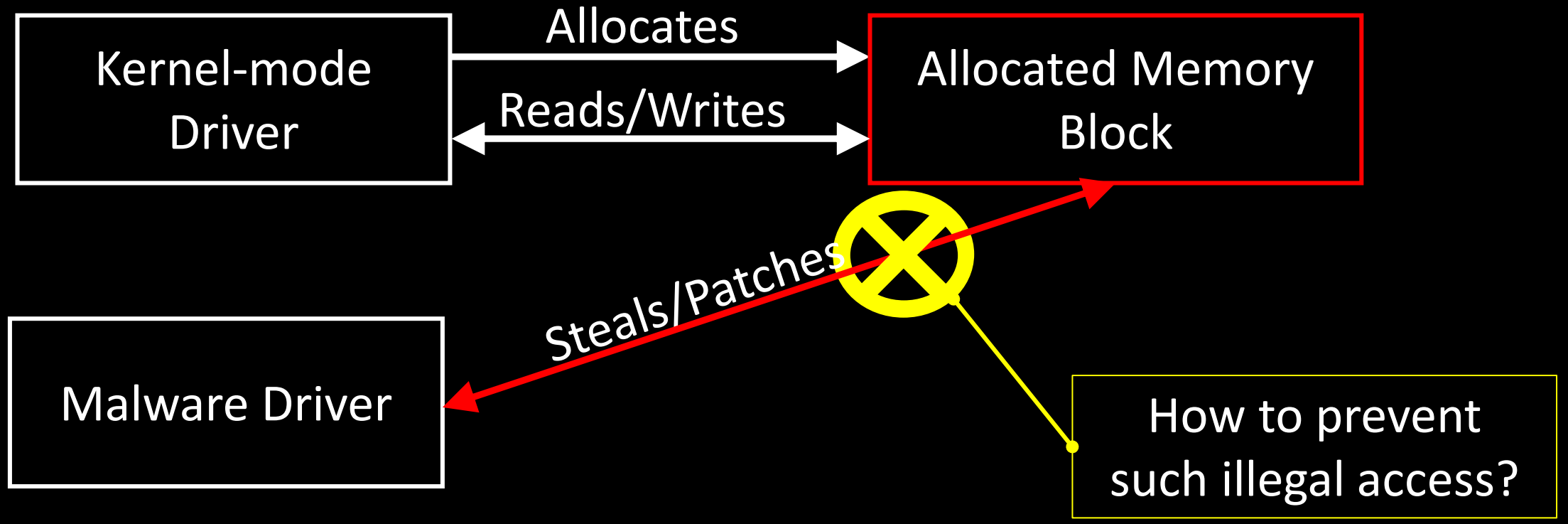
CNC machine crashes!



https://www.fanucamerica.com/docs/default-source/cnc-files/brochures/fanuc_30ib_low.pdf?sfvrsn=feeda1_0
https://www.youtube.com/watch?v=jHbl_B2sPA0
https://www.youtube.com/watch?v=8CSwOebmb0A

2) Protection for Integrity and Confidentiality of Dynamically Allocated Memory in Windows Kernel

Protection for Integrity and Confidentiality of Dynamically Allocated Memory in Windows Kernel



Analysis of Allocated Data Protection Projects

Title, year	OS data Integrity	Third-Party Drivers Data		OS
		Integrity	Confidentiality	
Patch Guard in Windows 10 1709, 2017	+–*	–	–	Windows
HUKO, 2011	+	+–**	–	Windows, Linux
LKMG, 2018	+	+–**	+–**	Linux
LKRG, 2018	+	–	–	Linux
AllMemPro, 2018	+	+	+	Windows

* — Windows security does not reveal the privilege escalation

** — HUKO and LKMG systems do not restrict the OS kernel

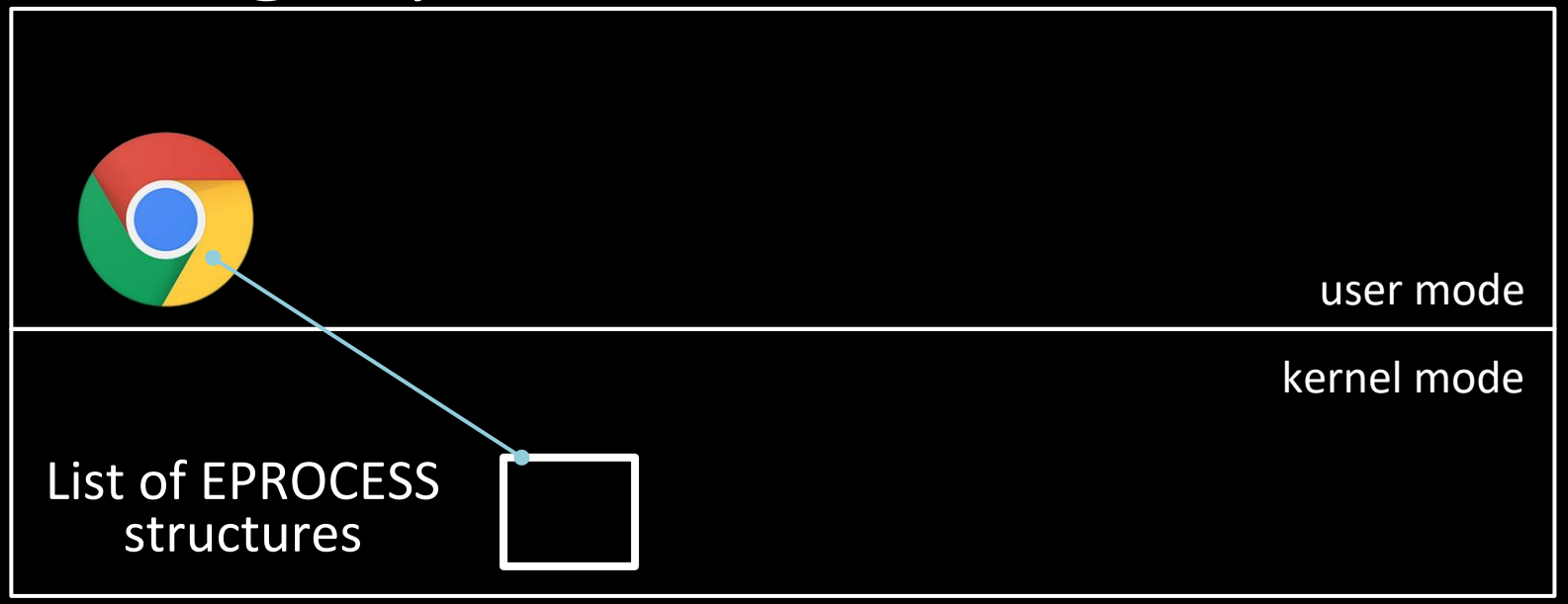
Analysis of Allocated Data Protection Projects

Title, year	OS data Integrity	Third-Party Drivers Data		OS
		Integrity	Confidentiality	
Patch Guard in Windows 10 1709, 2017	+–*	–	–	Windows
HUKO, 2011	+	+–**	–	Windows, Linux
LKMG, 2018	+	+–**	+–**	Linux
LKRG, 2018	+	–	–	Linux
AllMemPro, 2018	+	+	+	Windows

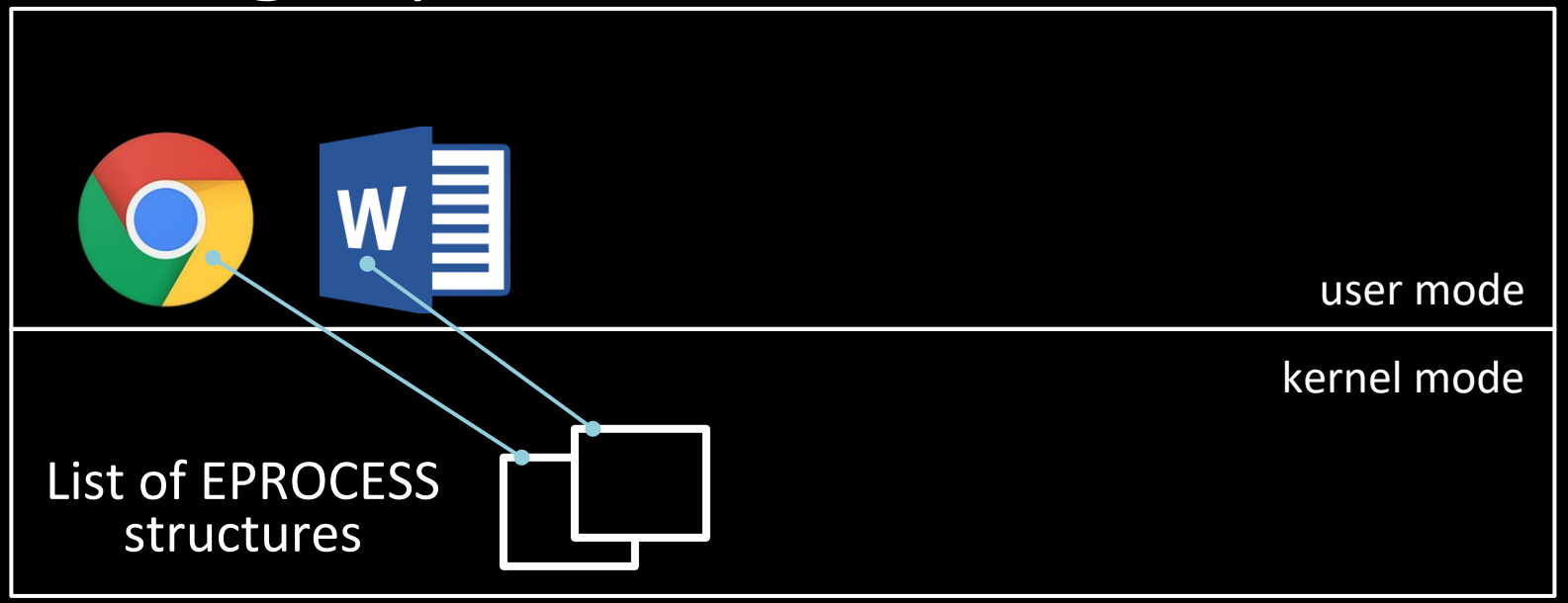
* — Windows security does not reveal the privilege escalation

** — HUKO and LKMG systems do not restrict the OS kernel

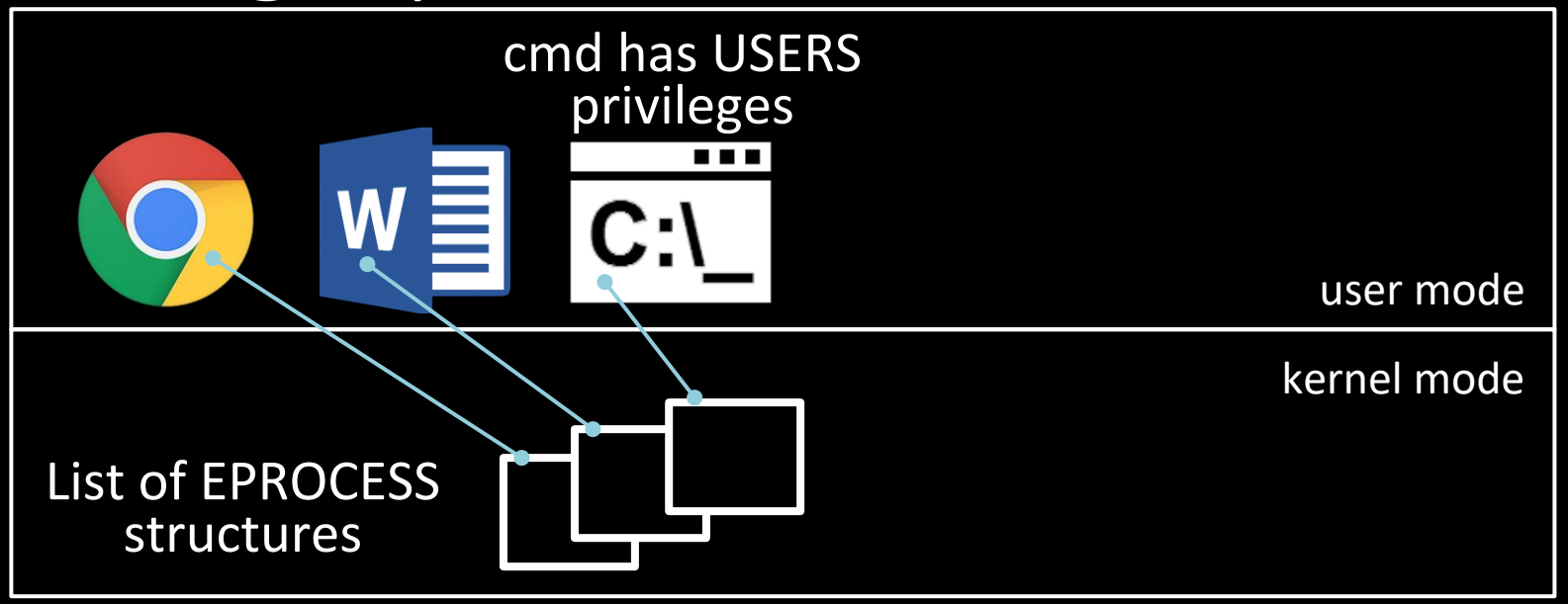
Integrity of Windows Internals



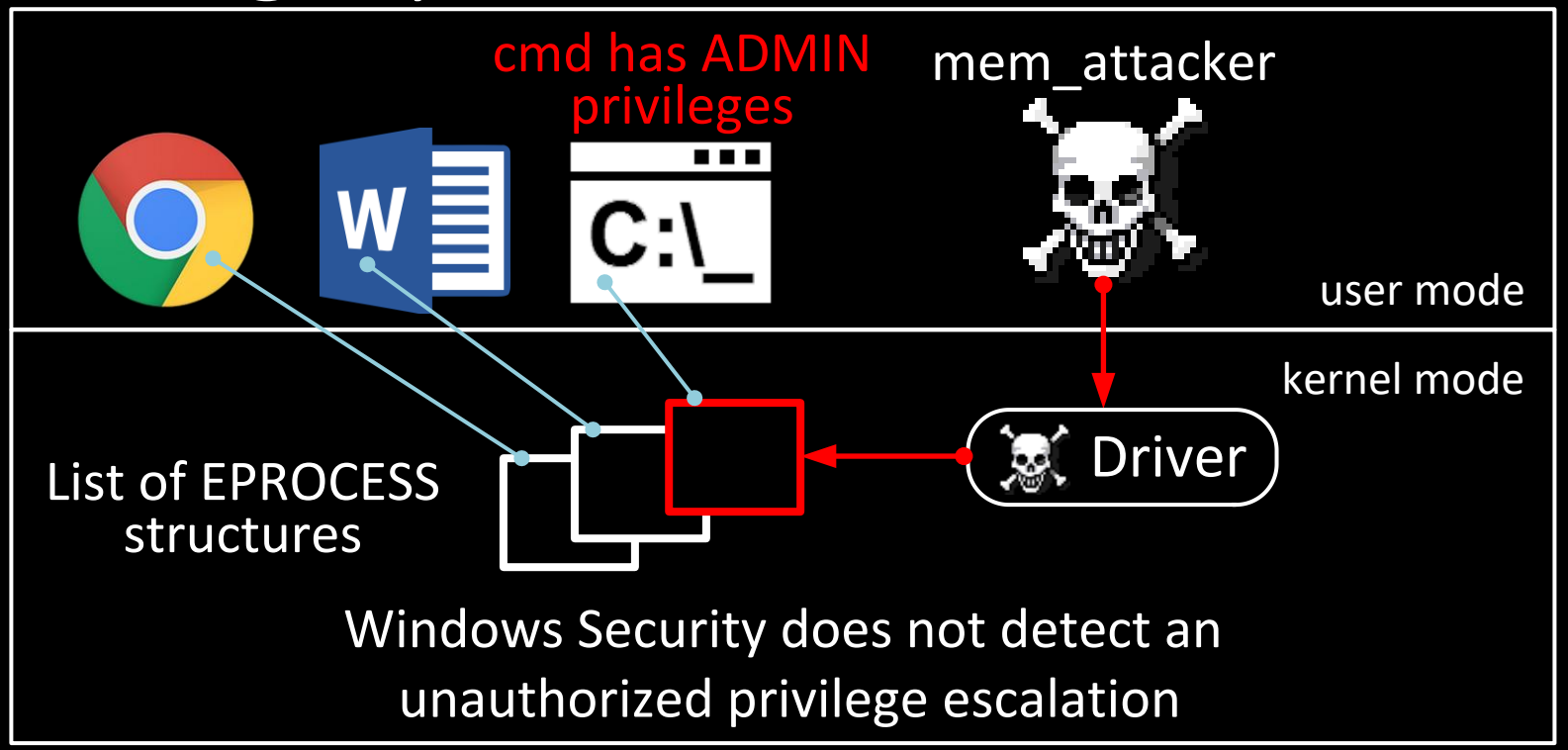
Integrity of Windows Internals



Integrity of Windows Internals



Integrity of Windows Internals



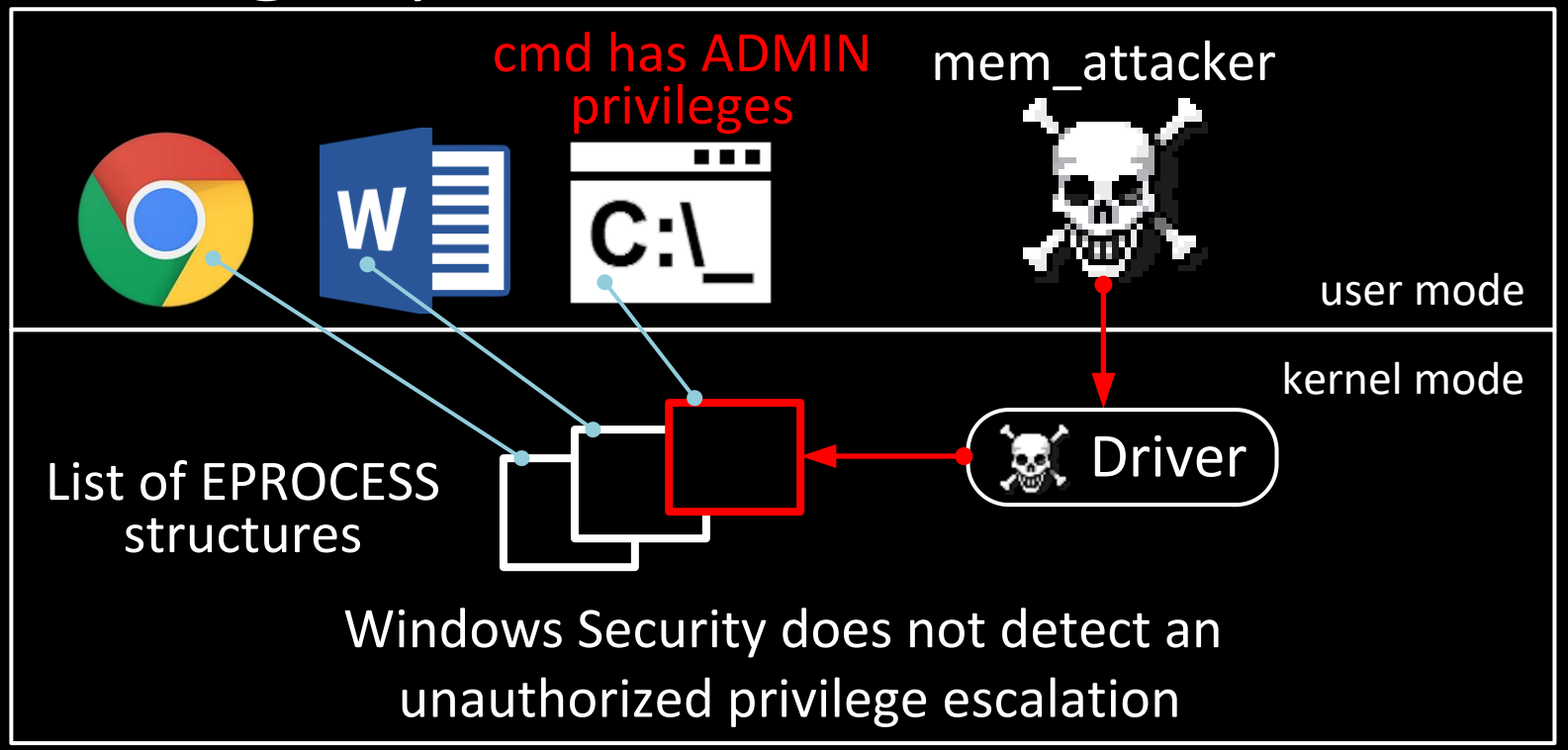
Fields of EPROCESS	Hackers Goals	Reaction of Security Service
ActiveProcessLinks	Hide a process	Demo A

Part 1/3 - Hiding a Process

Demo A

The online version is here – https://www.youtube.com/embed/GZ8HlgNDBms?vq=hd1440

Integrity of Windows Internals



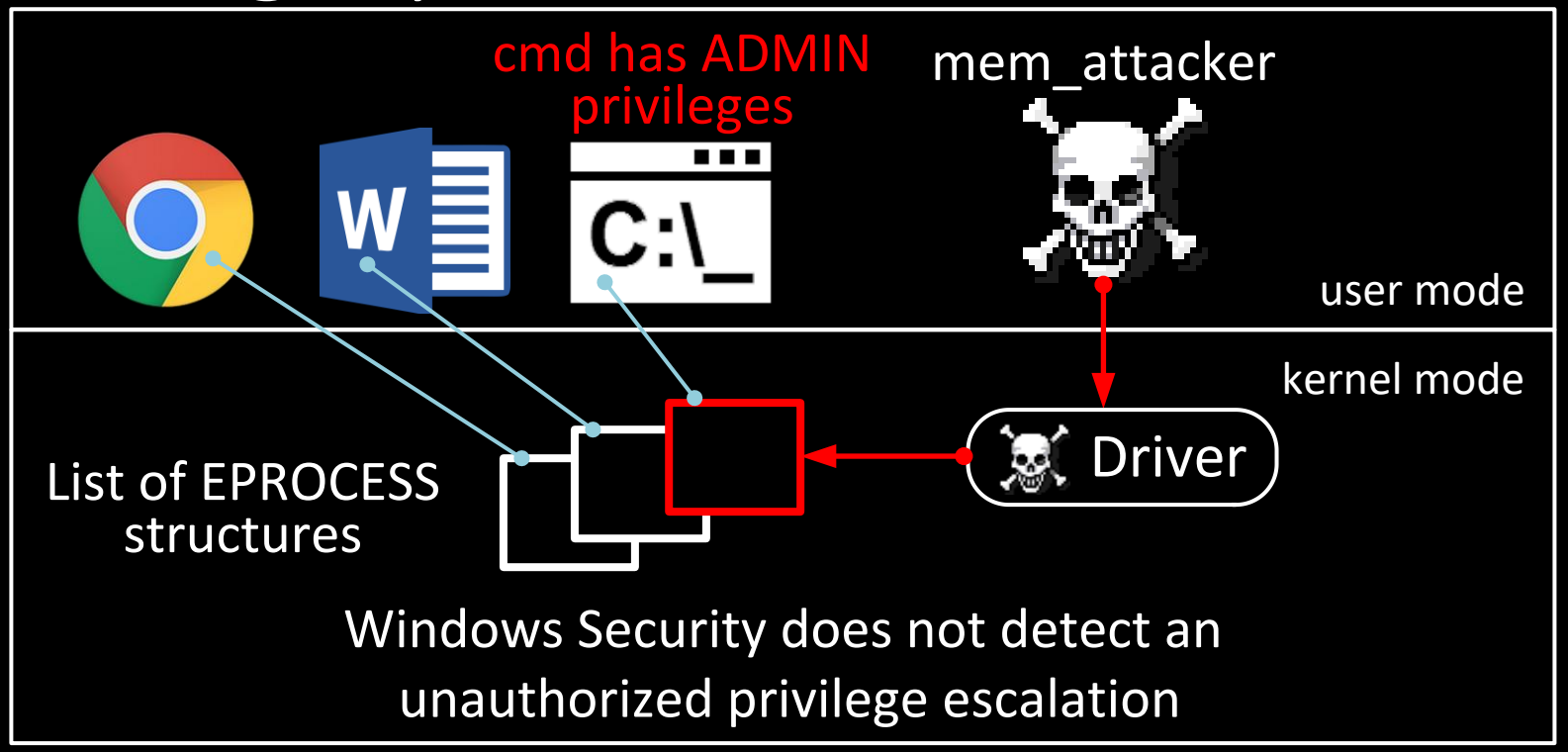
Fields of EPROCESS	Hackers Goals	Reaction of Security Service
ActiveProcessLinks	Hide a process	PatchGuard crashes the OS ✔
Token	Elevate process privileges	Demo B

Part 2/3 - Escalating Process Privileges

Demo B

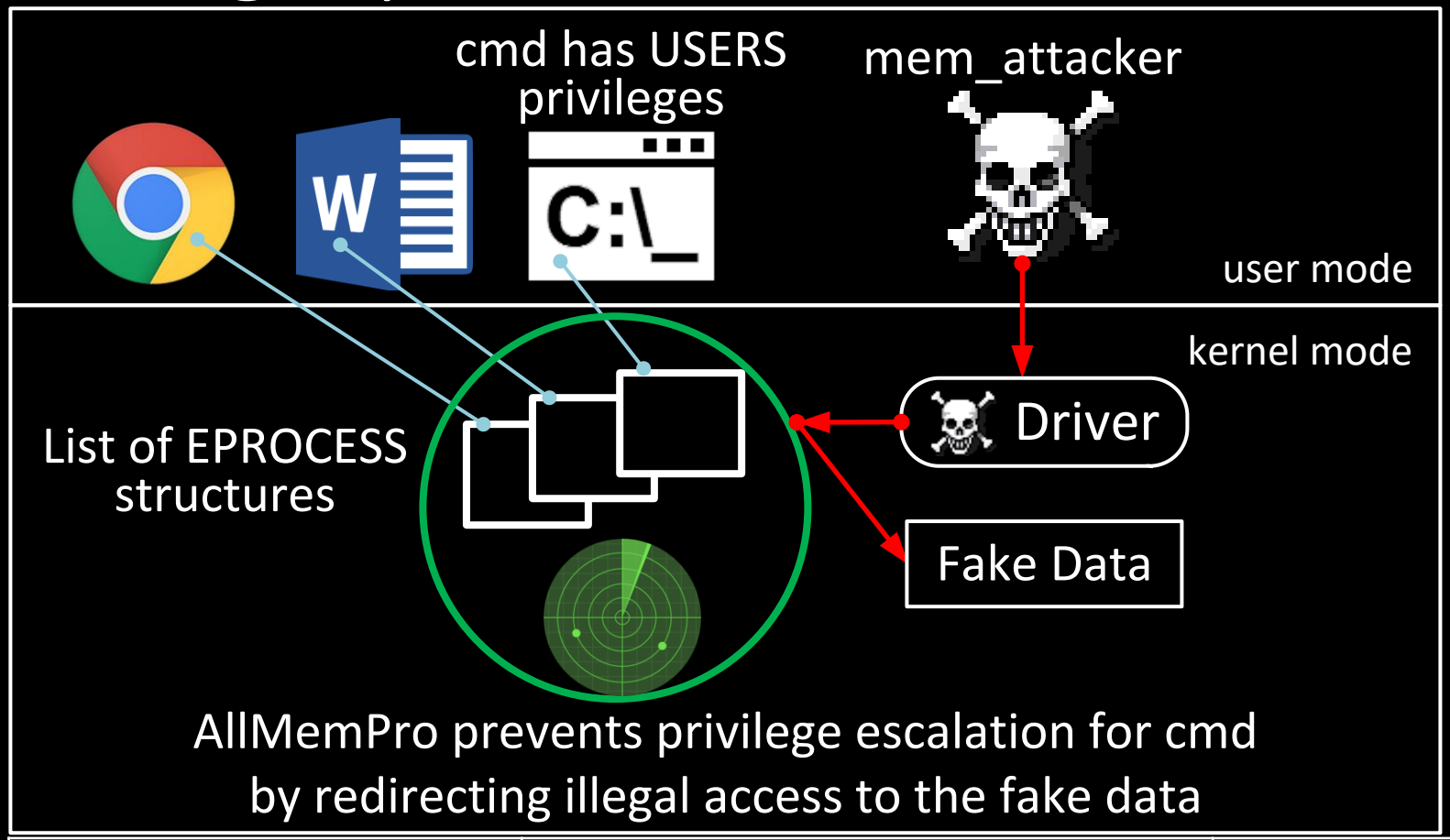
The online version is here – https://www.youtube.com/embed/ngMsY9ixtGw?vq=hd1440

Integrity of Windows Internals



Fields of EPROCESS	Hackers Goals	Reaction of Security Service
ActiveProcessLinks	Hide a process	PatchGuard crashes the OS ✔
Token	Elevate process privileges	OS has been infected

Integrity of Windows Internals



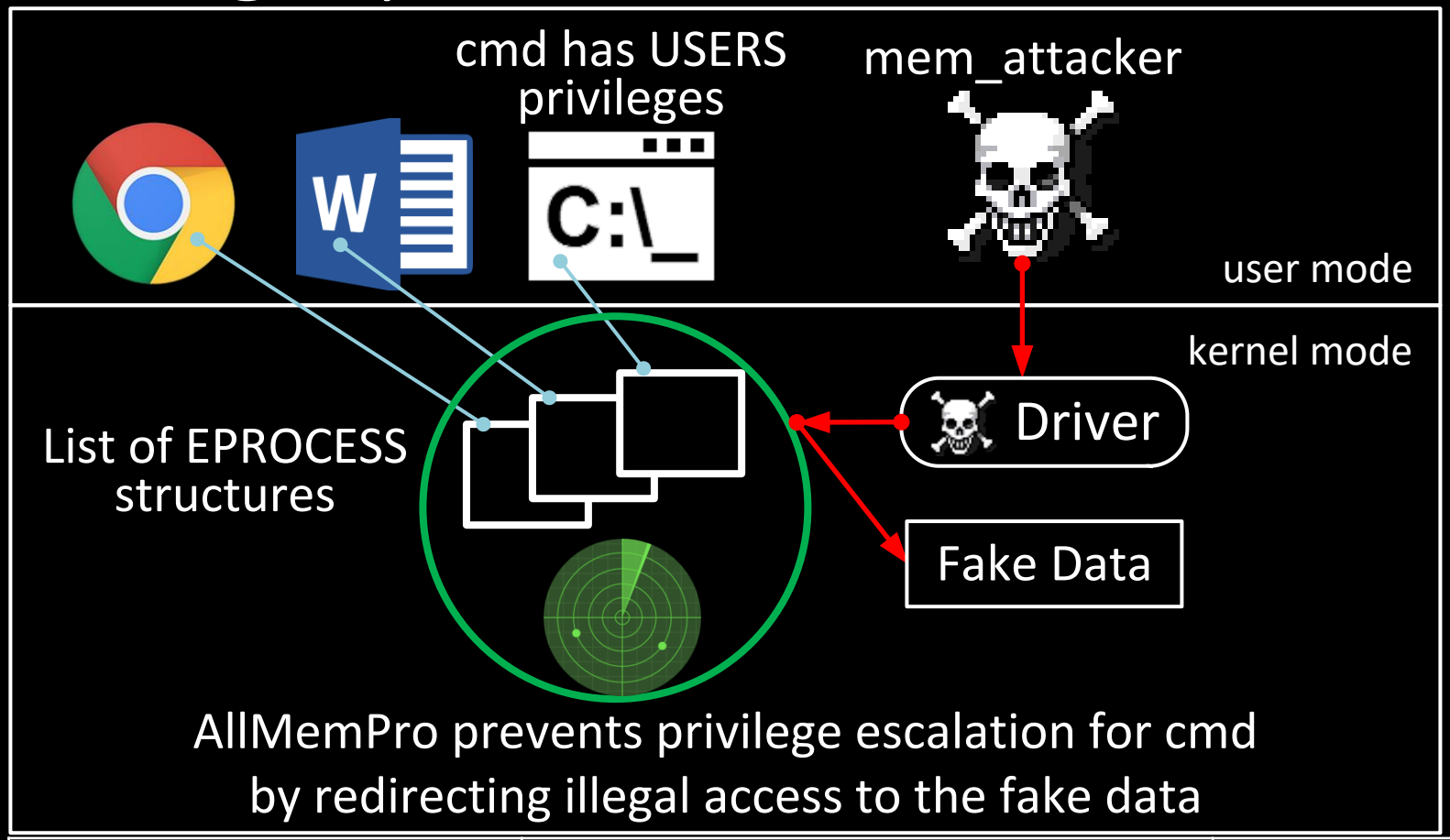
Fields of EPROCESS	Hackers Goals	Reaction of Security Service
ActiveProcessLinks	Hide a process	PatchGuard crashes the OS ✔
Token	Elevate process privileges	Demo C

Part 3/3 - AllMemPro Prevents Escalation of Process Privileges

Demo C

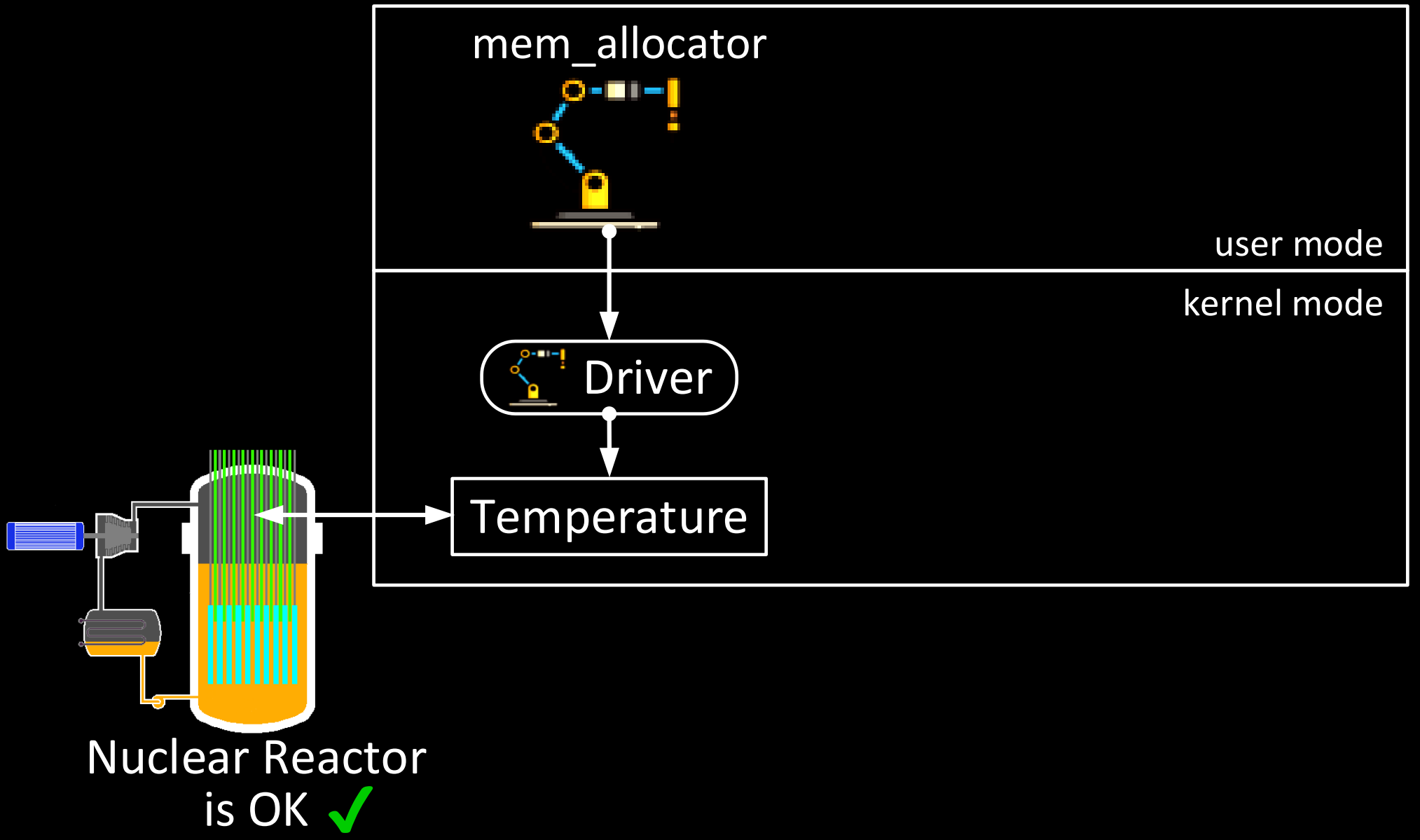
The online version is here – https://www.youtube.com/embed/EEoTkQn7qFk?vq=hd1440

Integrity of Windows Internals

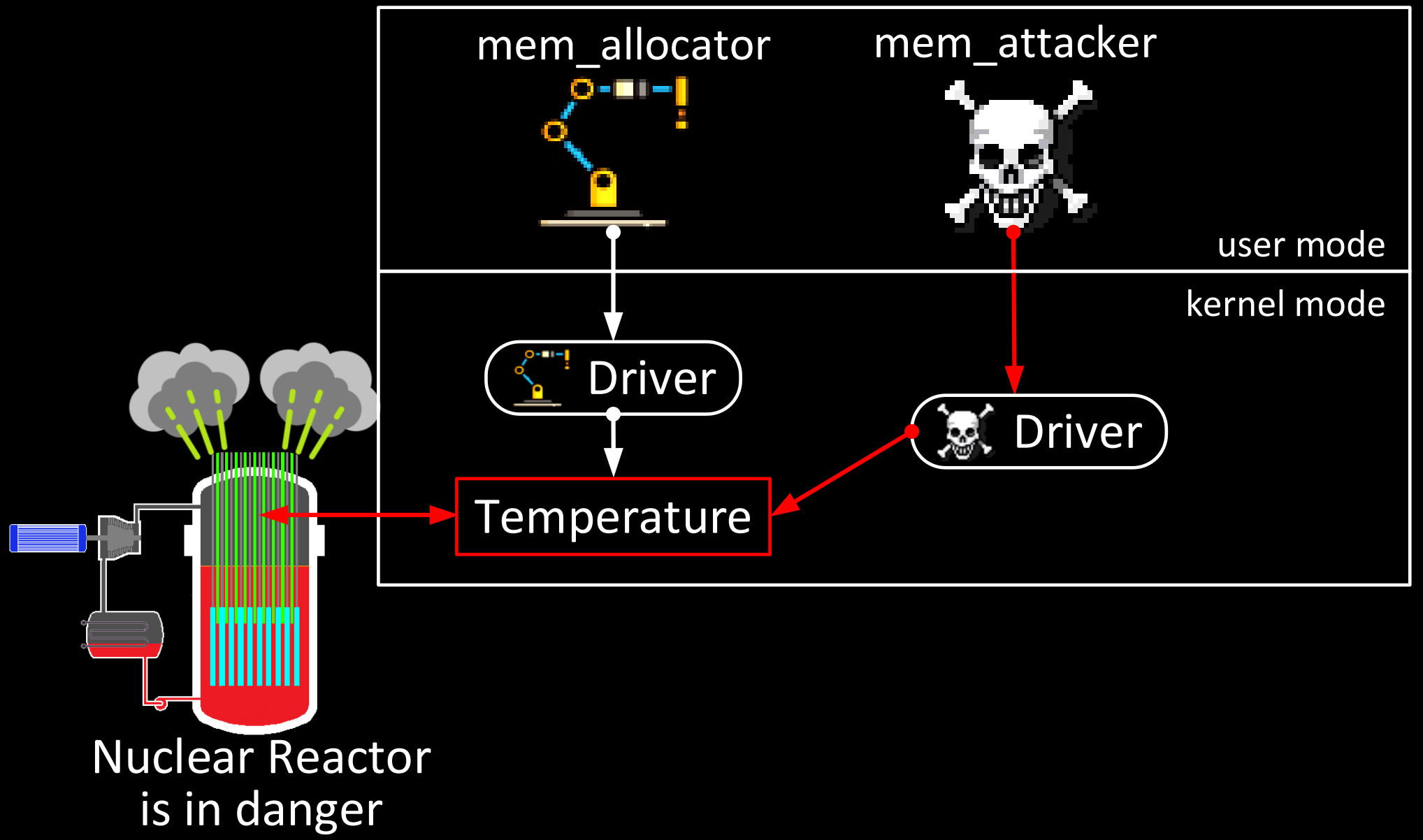


Fields of EPROCESS	Hackers Goals	Reaction of Security Service
ActiveProcessLinks	Hide a process	PatchGuard crashes the OS ✔
Token	Elevate process privileges	AllMemPro prevents access ✔

Protection of Industrial Control Systems



Protection of Industrial Control Systems – Demo D

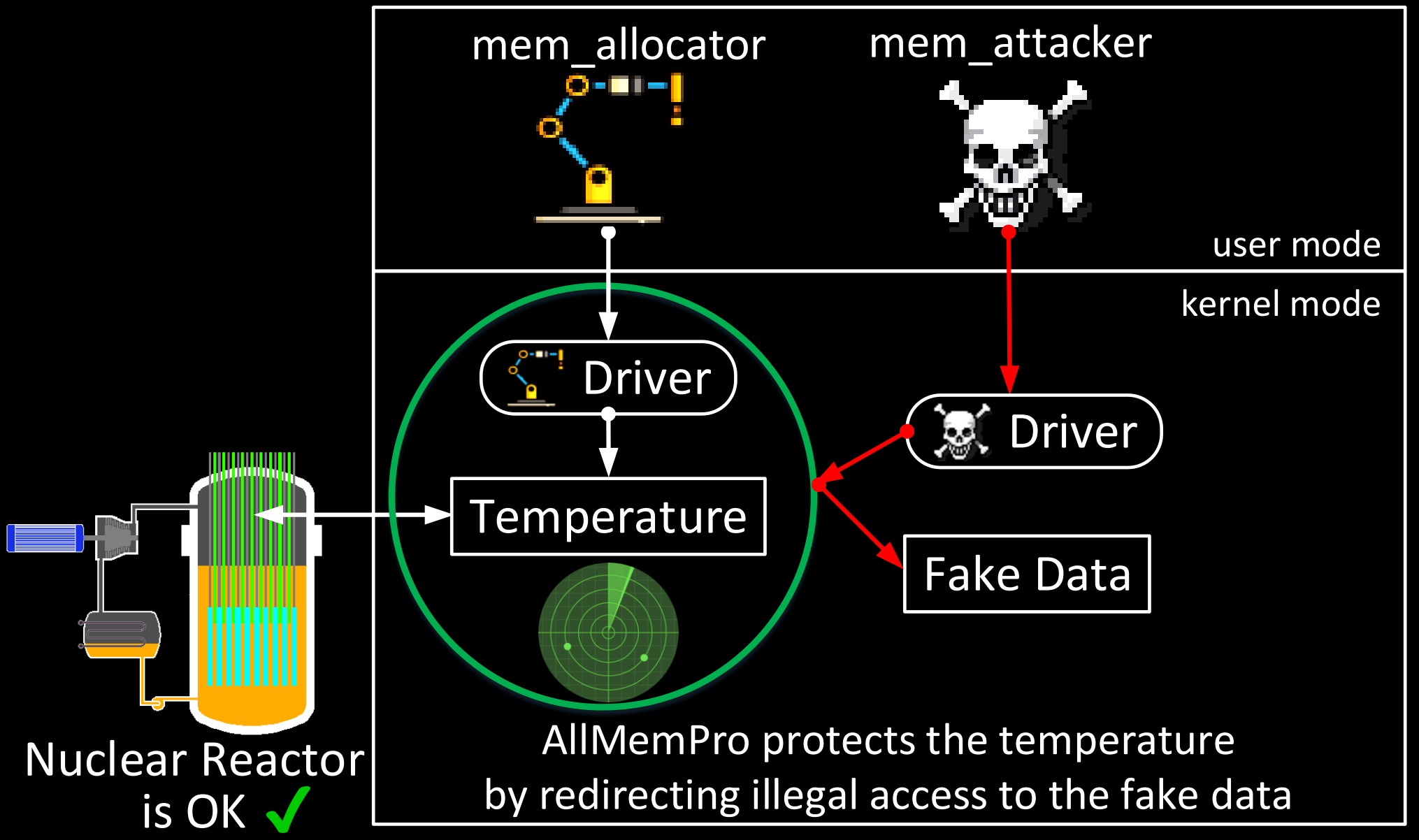


Part 1/2 - Unauthorized Modification of Dynamically Allocated Memory

Demo D

The online version is here – https://www.youtube.com/embed/K3lPb7Zv4Zg?vq=hd1440

Protection of Industrial Control Systems – Demo E



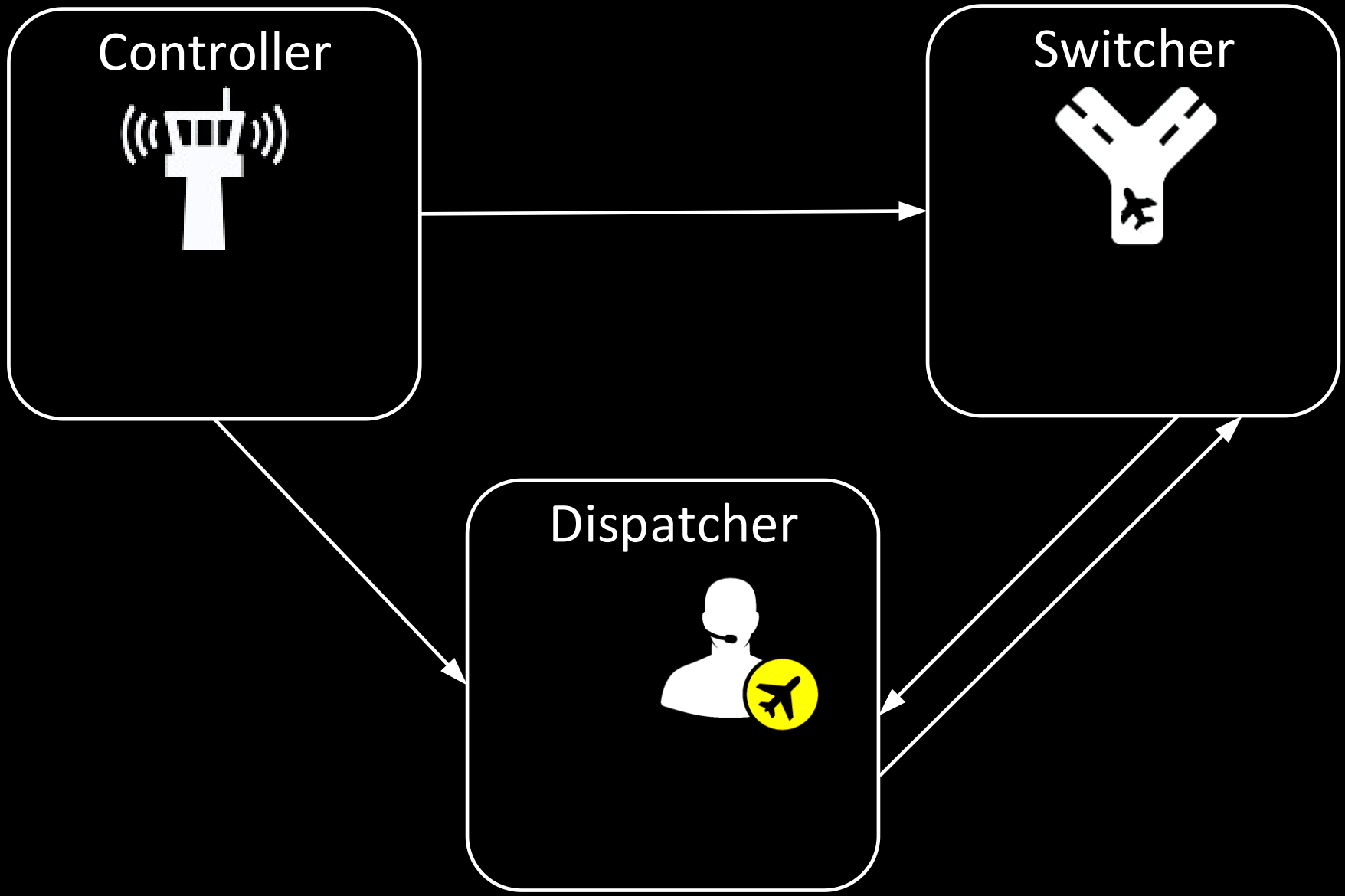
Part 2/2 - AllMemPro Prevents Illegal Access to the Allocated Memory

Demo E

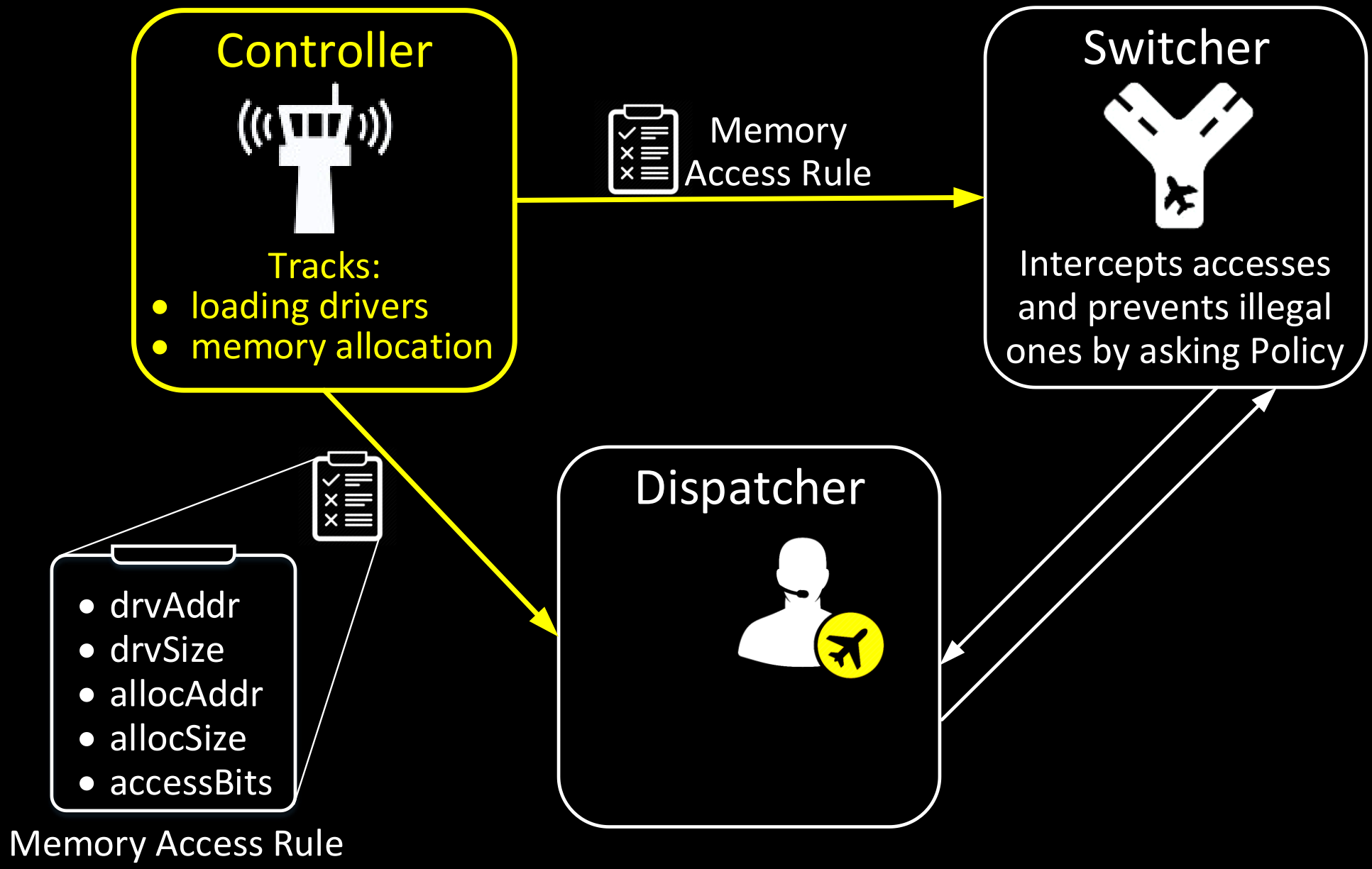
The online version is here – https://www.youtube.com/embed/yytIUX9fzqw?vq=hd1440

3) Hypervisor-Based Active Data Protection for Integrity and Confidentiality of Dynamically Allocated Memory in Windows Kernel

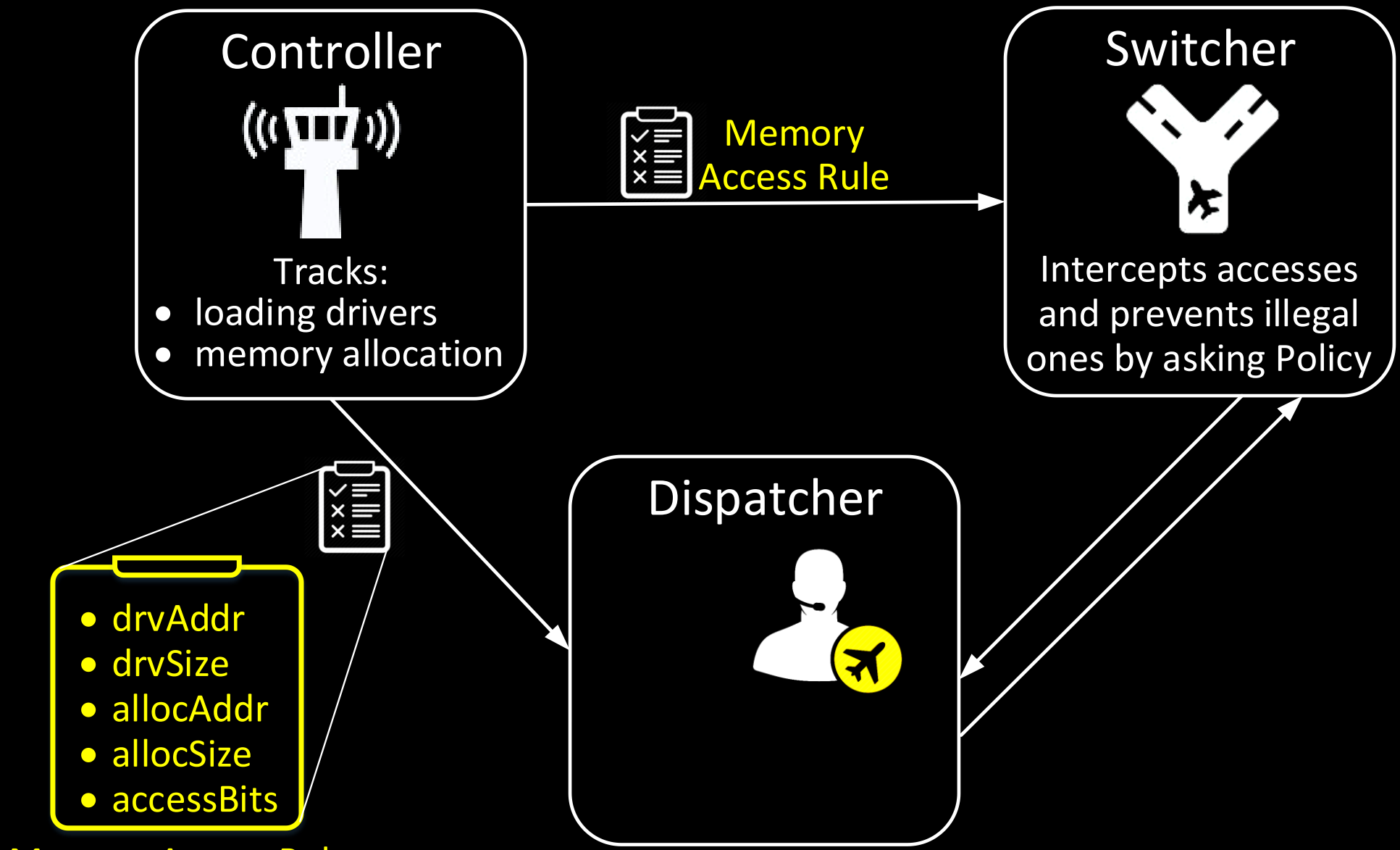
Architecture of AllMemPro - Allocated Memory Protection



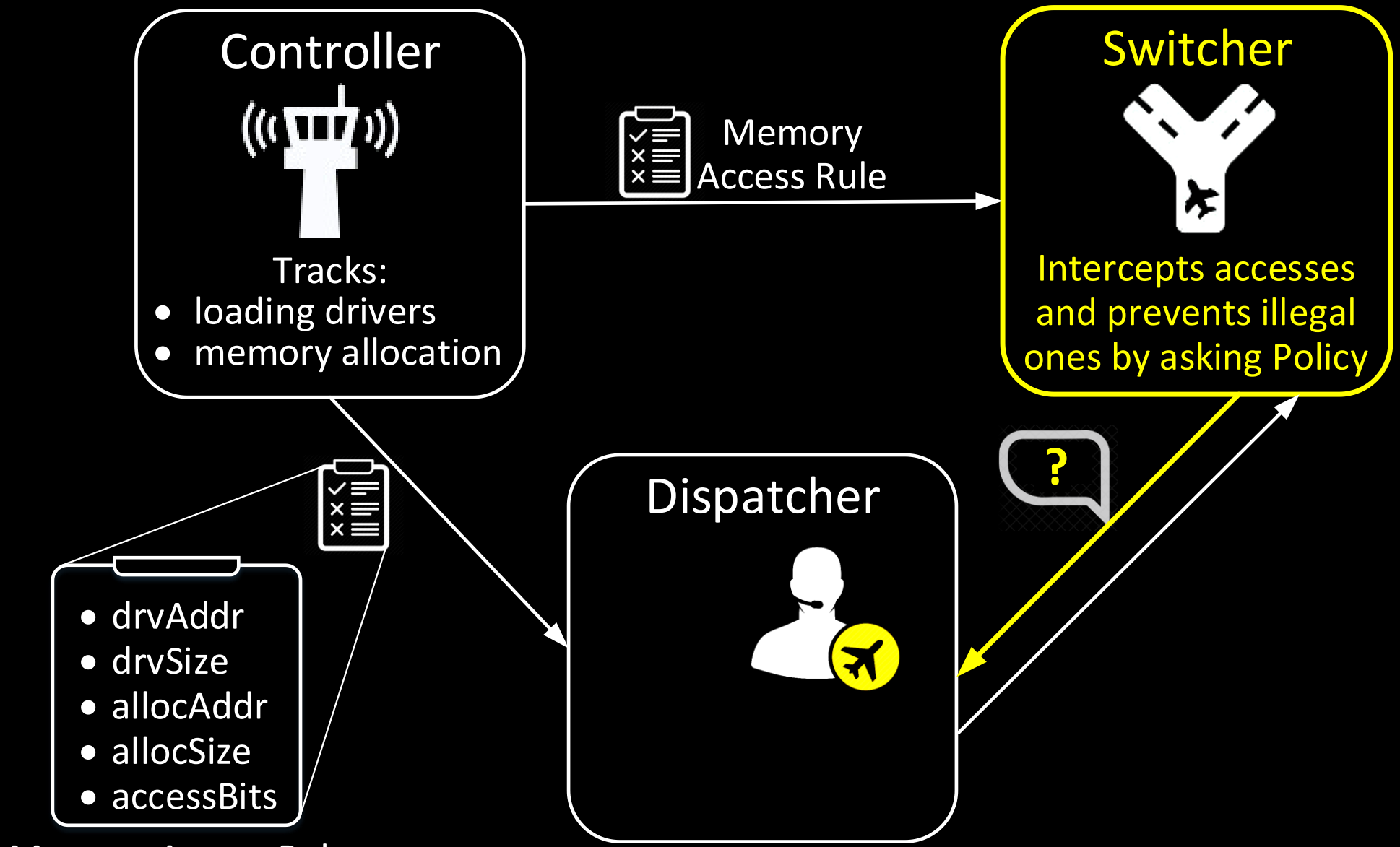
Architecture of AllMemPro - Allocated Memory Protection



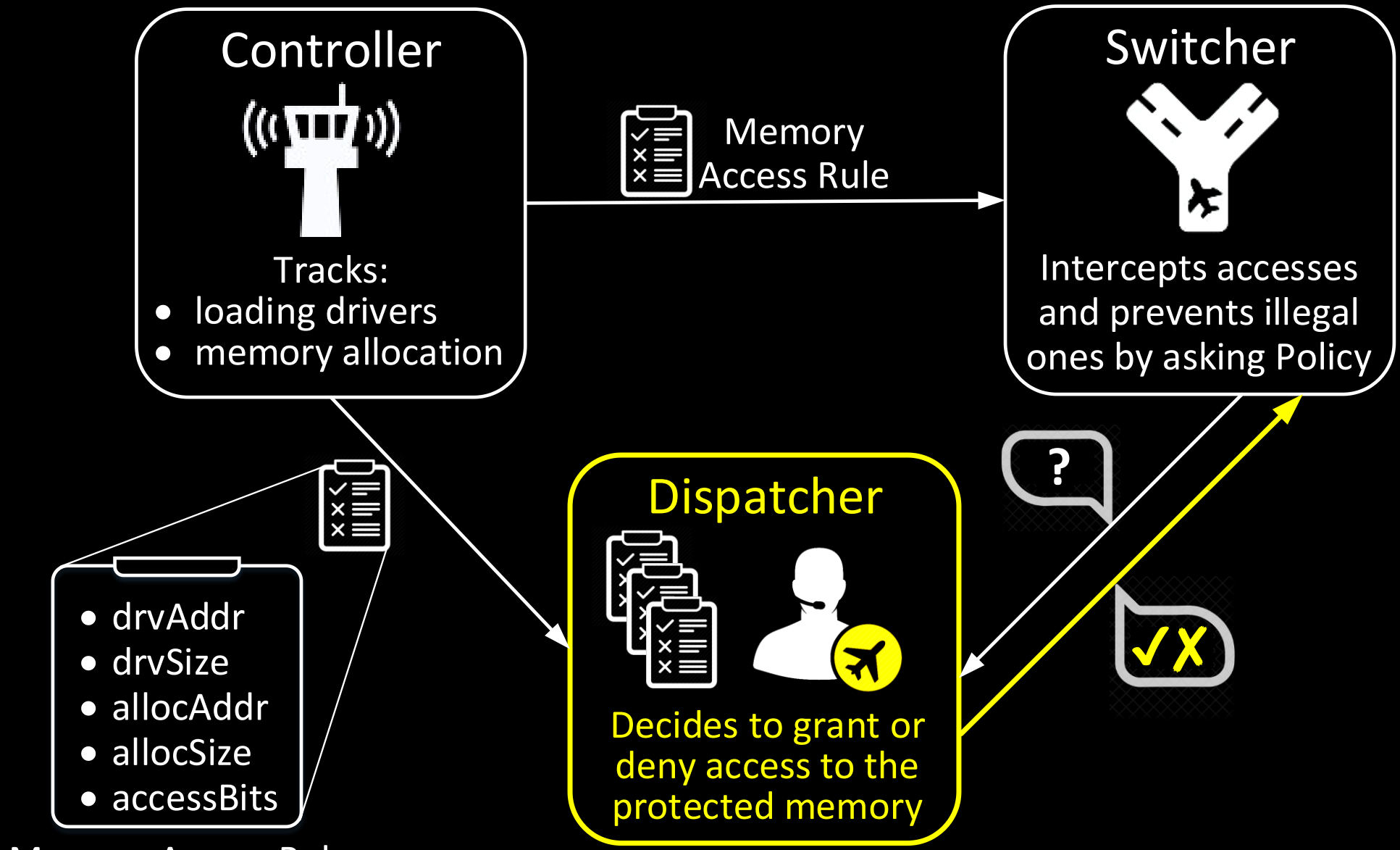
Architecture of AllMemPro - Allocated Memory Protection



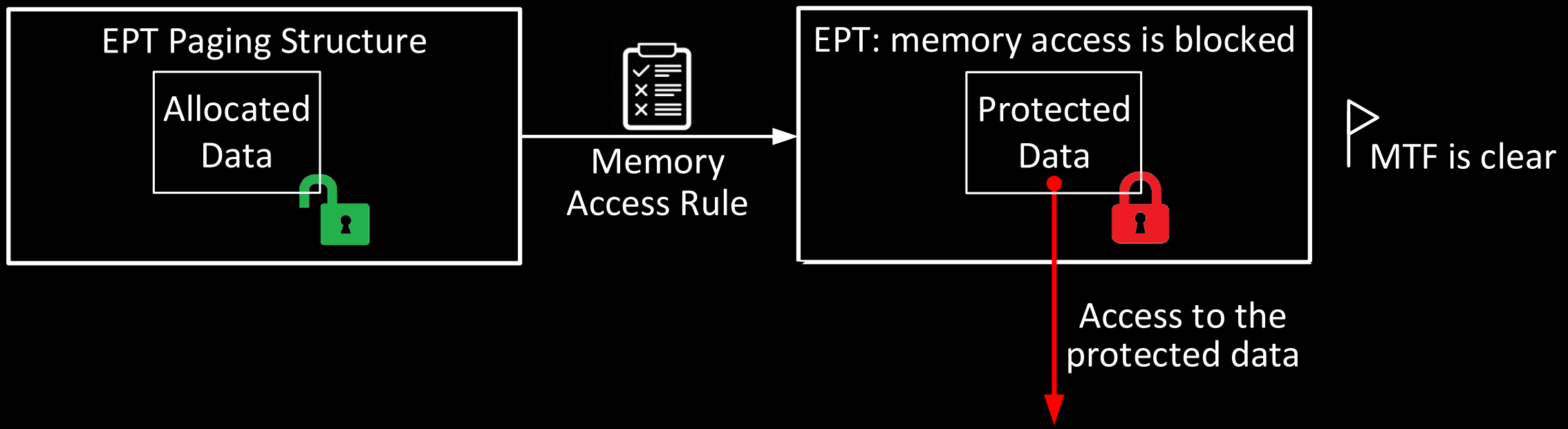
Architecture of AllMemPro - Allocated Memory Protection



Architecture of AllMemPro - Allocated Memory Protection



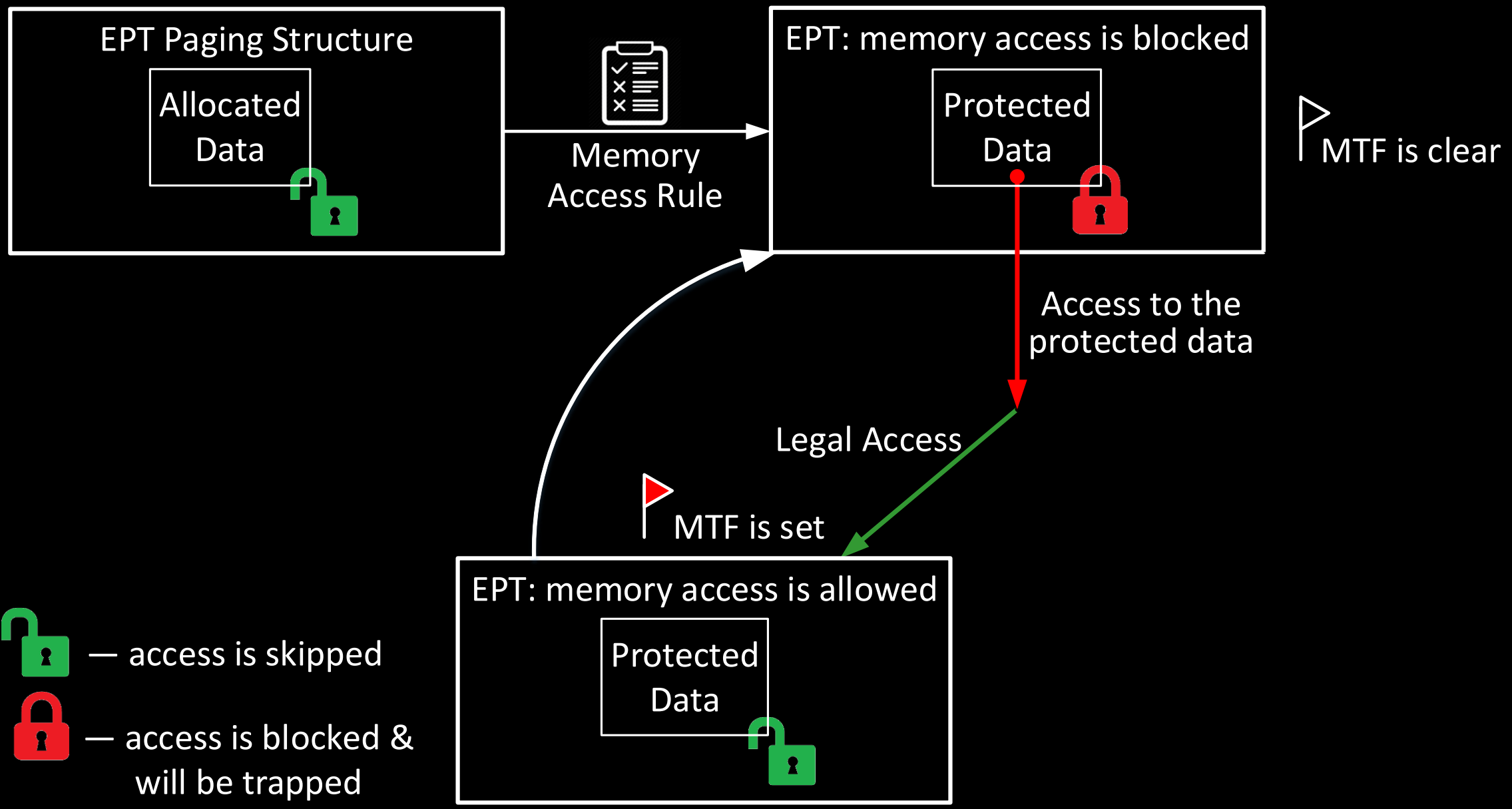
The Switcher Controls Memory Access via EPT



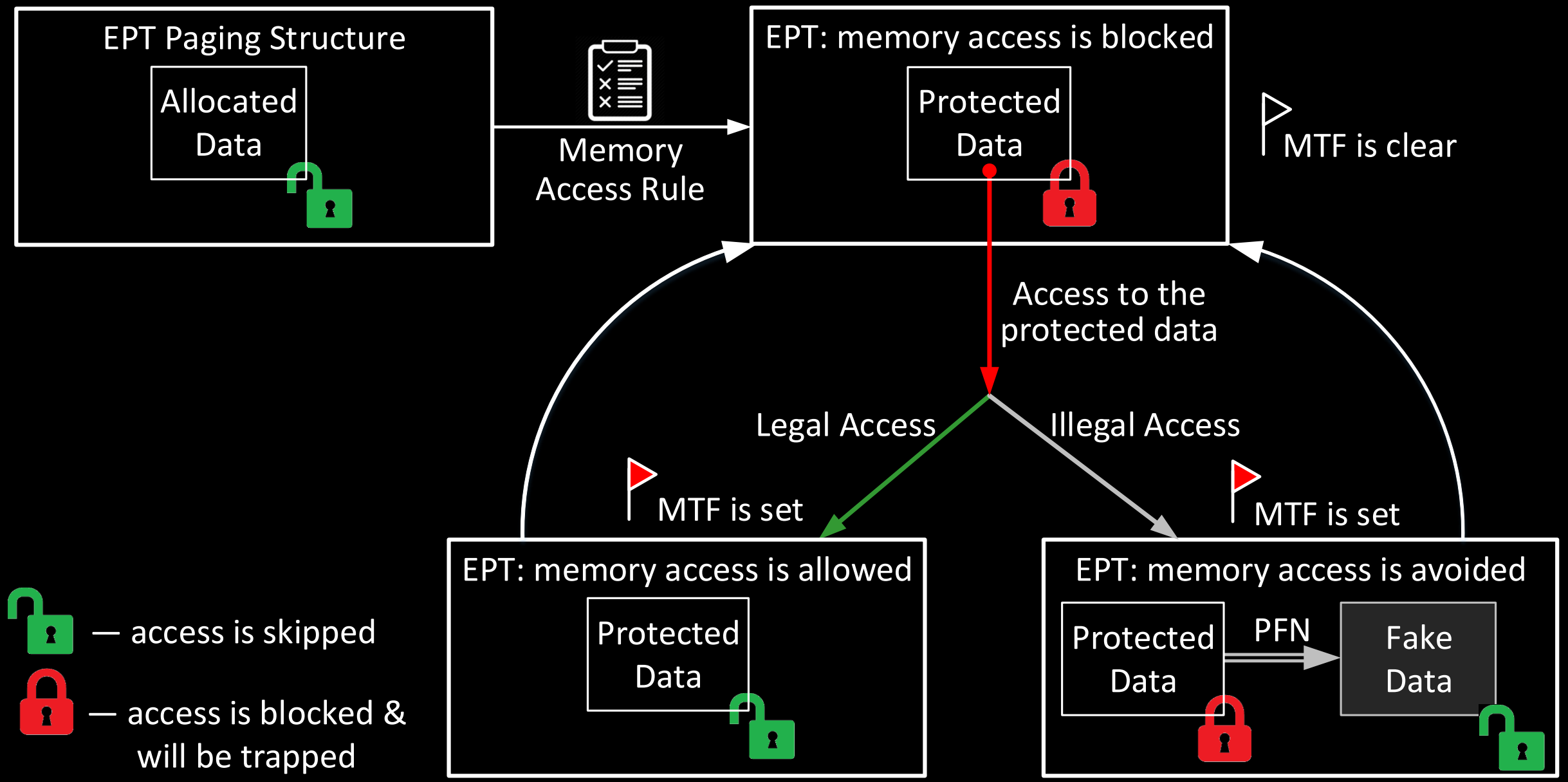
— access is skipped

— access is blocked & will be trapped

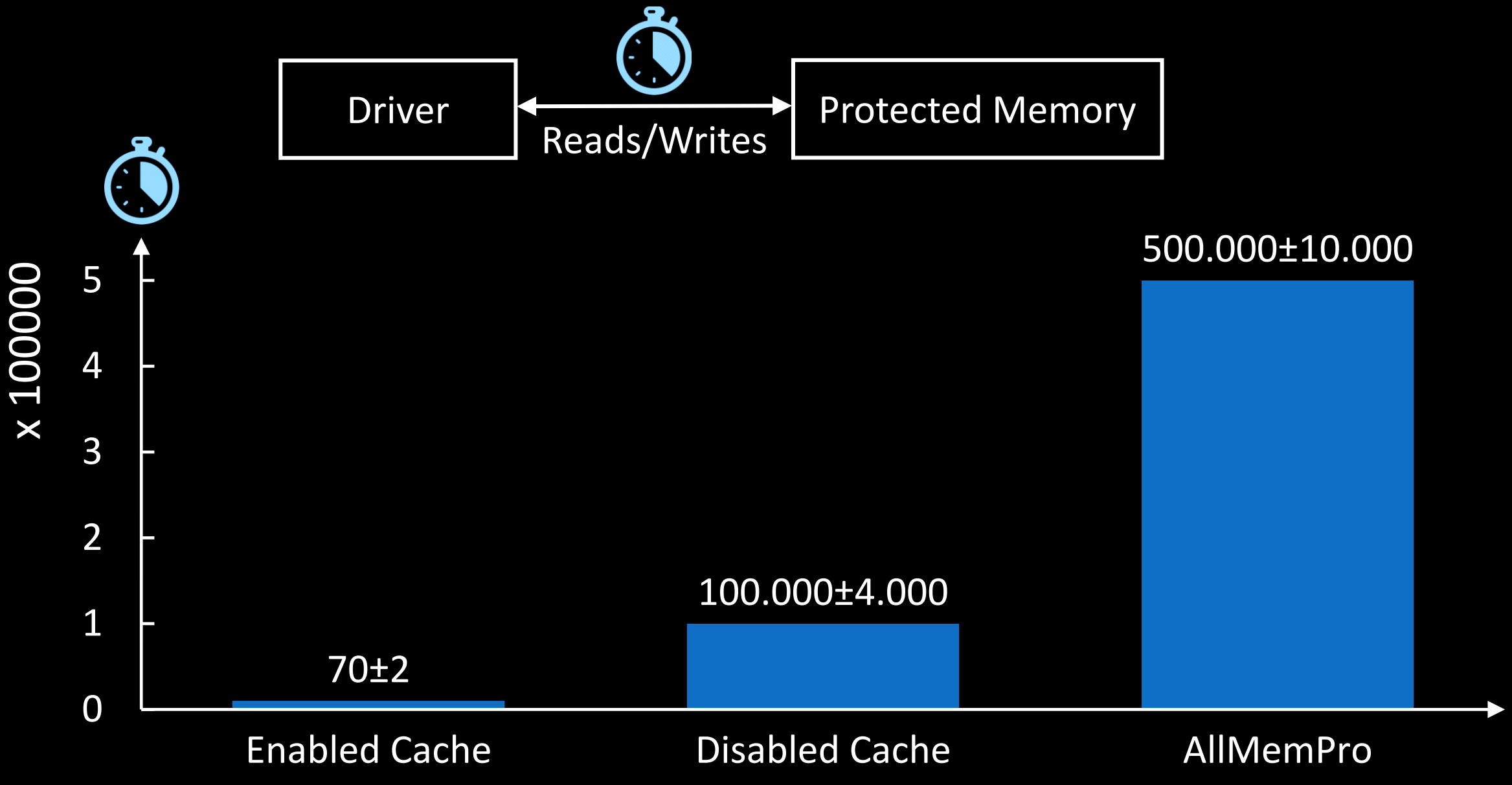
The Switcher Controls Memory Access via EPT



The Switcher Controls Memory Access via EPT



AllMemPro benchmarks: memory access time



AllMemPro Summary

- restricts the OS kernel
- protects each byte of the allocated memory
- is hypervisor-based and does not modify the OS
- protects memory with not so frequent access attempts
- seems to prevent Spectre and Meltdown CPU attacks: research is ongoing

Thank you!

Igor Korkin igor.korkin@gmail.com

All the details are here igorkorkin.blogspot.com