Exploring modern OS Administrative Privileges

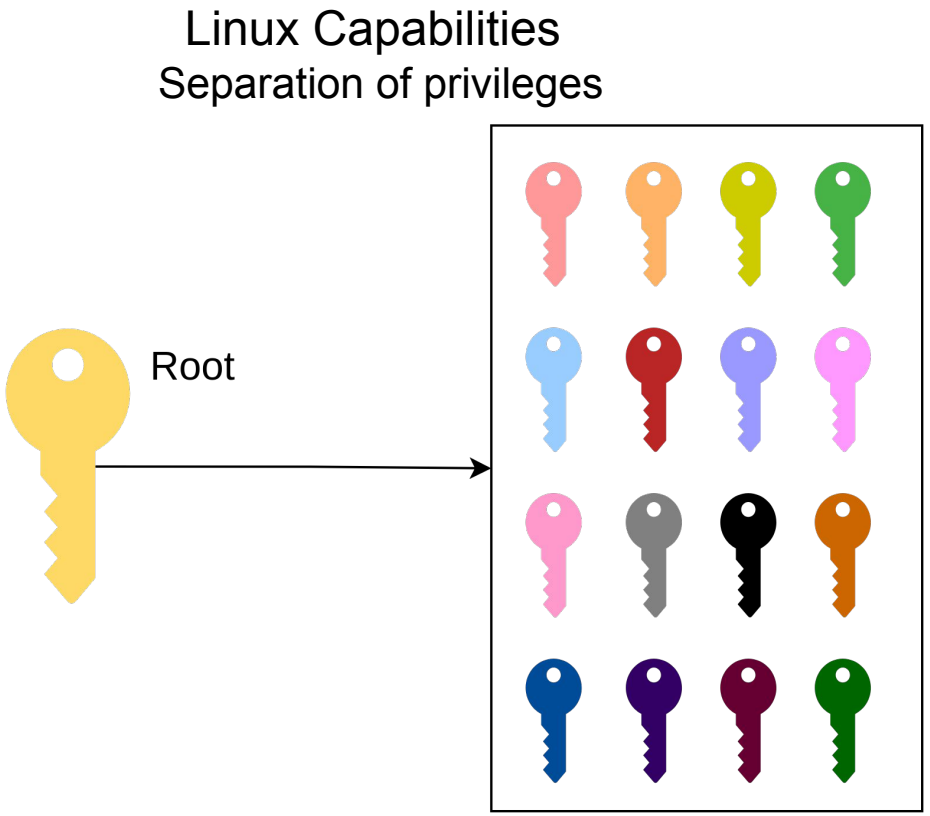
Eddie Billoir,
Romain Laborde,
Ahmad Samer Wazan,
Yves Rütschlé,
Abdelmalek Benzekri

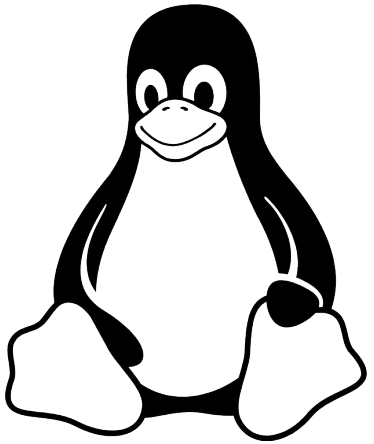
PROTECT

ANRT ASSOCIATION NATIONALE RECHERCHE TECHNOLOGIE
Cifre
UNIVERSITÉ TOULOUSE III PAUL SABATIER
Admitt
IRIT
AIRBUS

Why do we need Administrative Privileges on OS ?

How can we apply Zero-Trust on Administrator ?



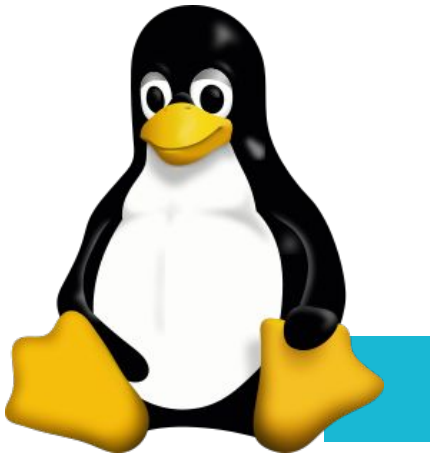


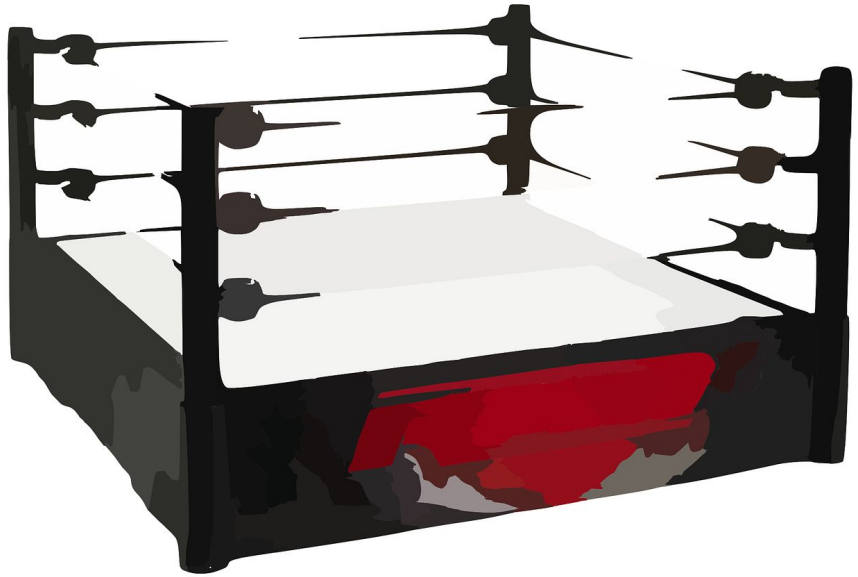
What about other brand new OS?

MICROSOFT® WINDOWS

http://www.freebsd.org
FreeBSD
FreeBSD:The Power To Serve

Let's make a battle ! Who is going to win ?



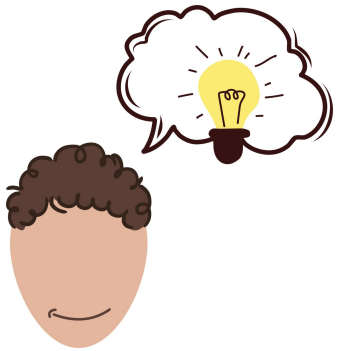


SOLARIS™

Institut de Recherche en Informatique de Toulouse

AIRBUS

How can-we compare these OS ?

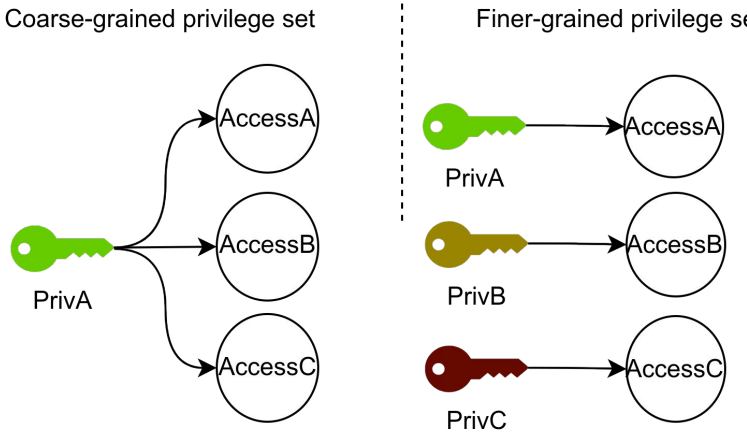


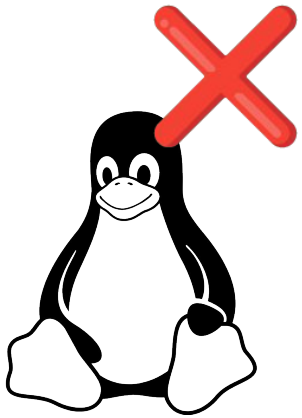
Basic principles

Usability

Least Privilege

Granularity





Back up files and directories

List is long

```
CAP_SYS_RESOURCE
 • Use reserved space
 • make ioctl(2) call
 • override disk quot
 • increase resource
 • override RLIMIT_NP
 • override maximum n
   allocation;
 • override maximum n
 • allow more than 64
   clock;
 • raise msg_qbytes l
   above the limit in
```

```
#define PRIV_NET_ADDIFGROUP     409
```

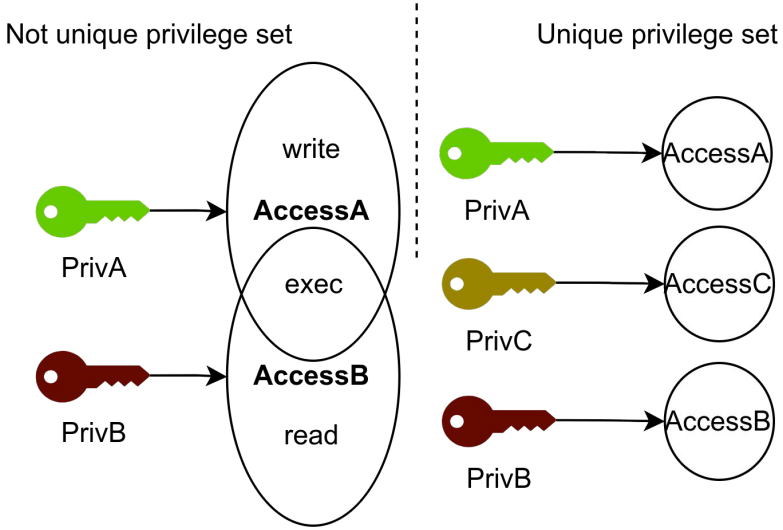
```
/* Add new interface group. */
```

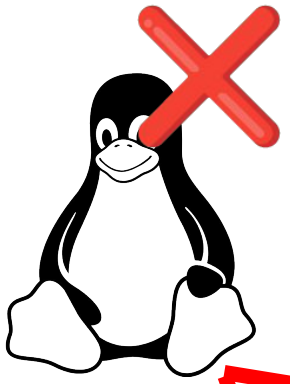
```
sys_config
        Allows a process to perform
various system configuration tasks.
```


IRIT

AIRBUS

Uniqueness





It could being unique if there were a dedicated file read privilege.

CAP_DAC_OVERRIDE

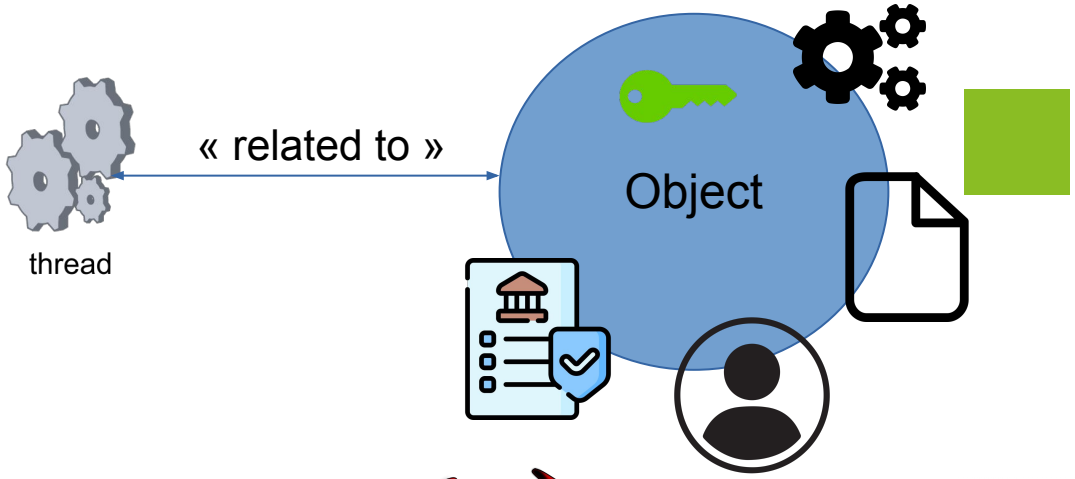
Bypass file read, write, and execute permission ch
(DAC is an abbreviation of "discretionary access
control".)

CAP_DAC_READ_SEA

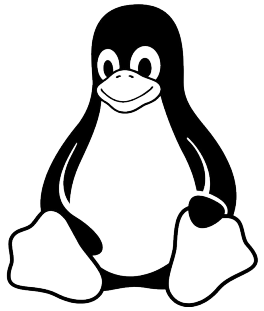
- Bypass file read permission checks and directory read and execute permission checks;
- invoke `open_by_handle_at(2)`;
- use the `linkat(2)` **`AT_EMPTY_PATH`** flag to create a link to a file referred to by a file descriptor.

AIRBUS

Enforcement Objects

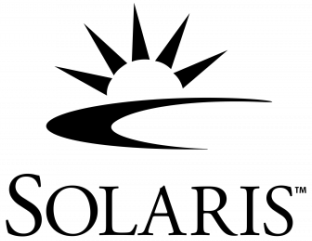


User
Group
Service



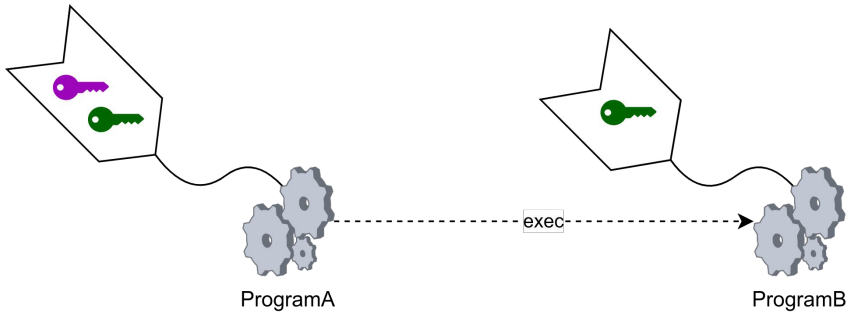
User
Group
Program File

Nothing 🙃
So it's safe
(I33t members only)



User
Role

Dynamic Initialisation



with 56 C lines

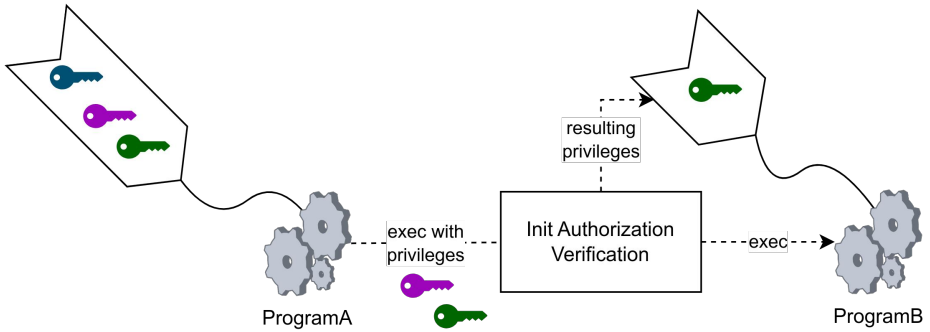
with 14 C lines

No 🙃

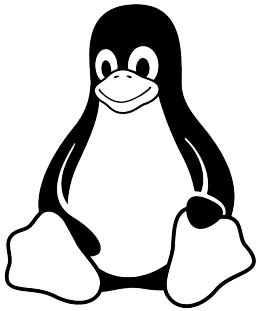
So it's safe

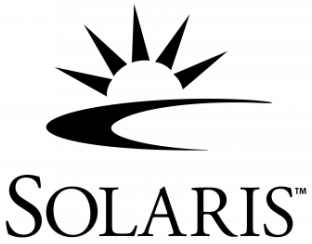
with 19 C lines

Init Authorization Verification

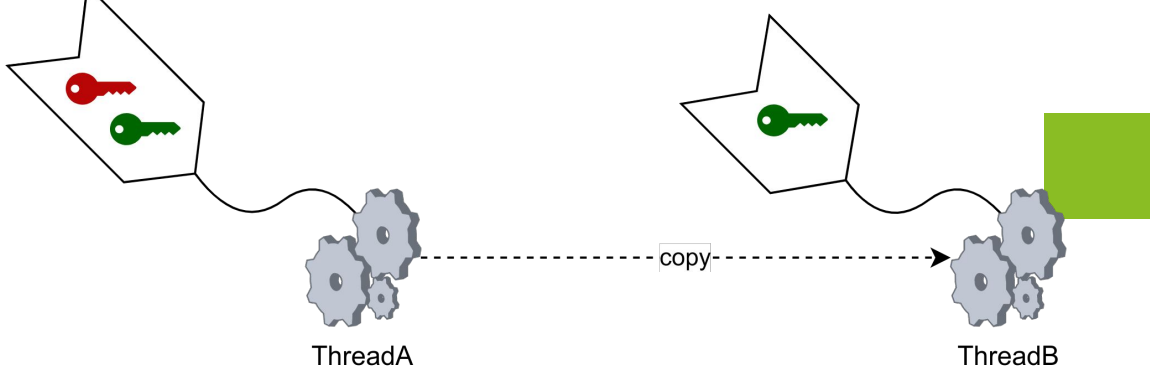


No one does.





Dynamic Delegation



with 56 C lines

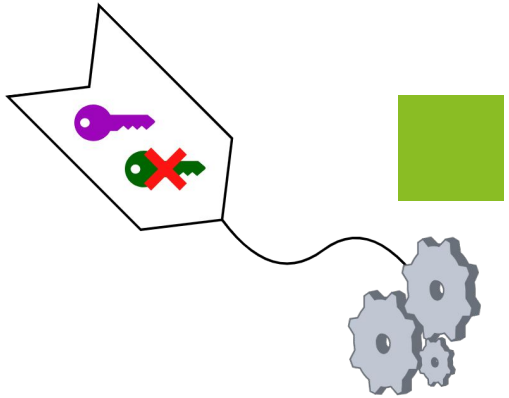
with 21 C lines

No 🙃

So it's safe

with 18 C lines

Self Revocability



with 34 C lines

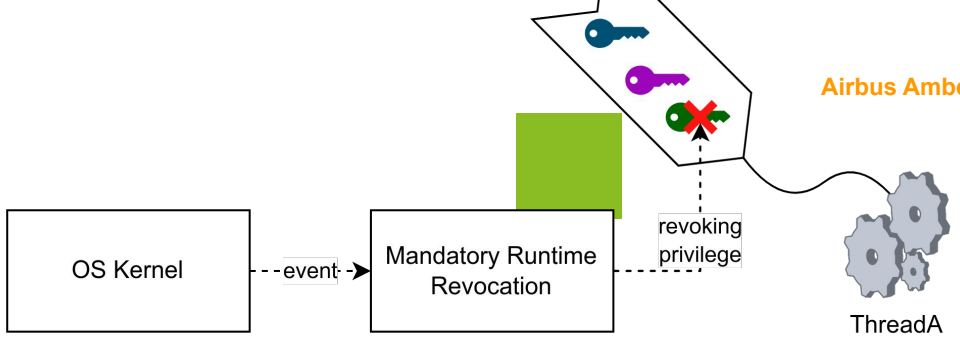
with 58 C lines

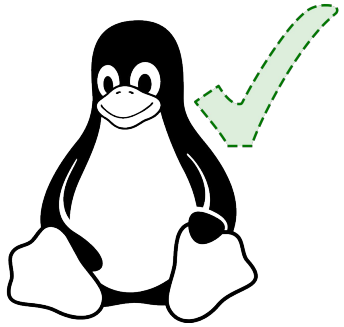
No 🙃

So it's safe

with 18 C lines

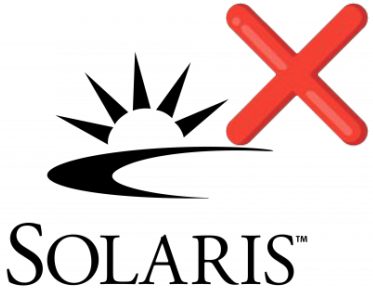
Mandatory Runtime Revocation



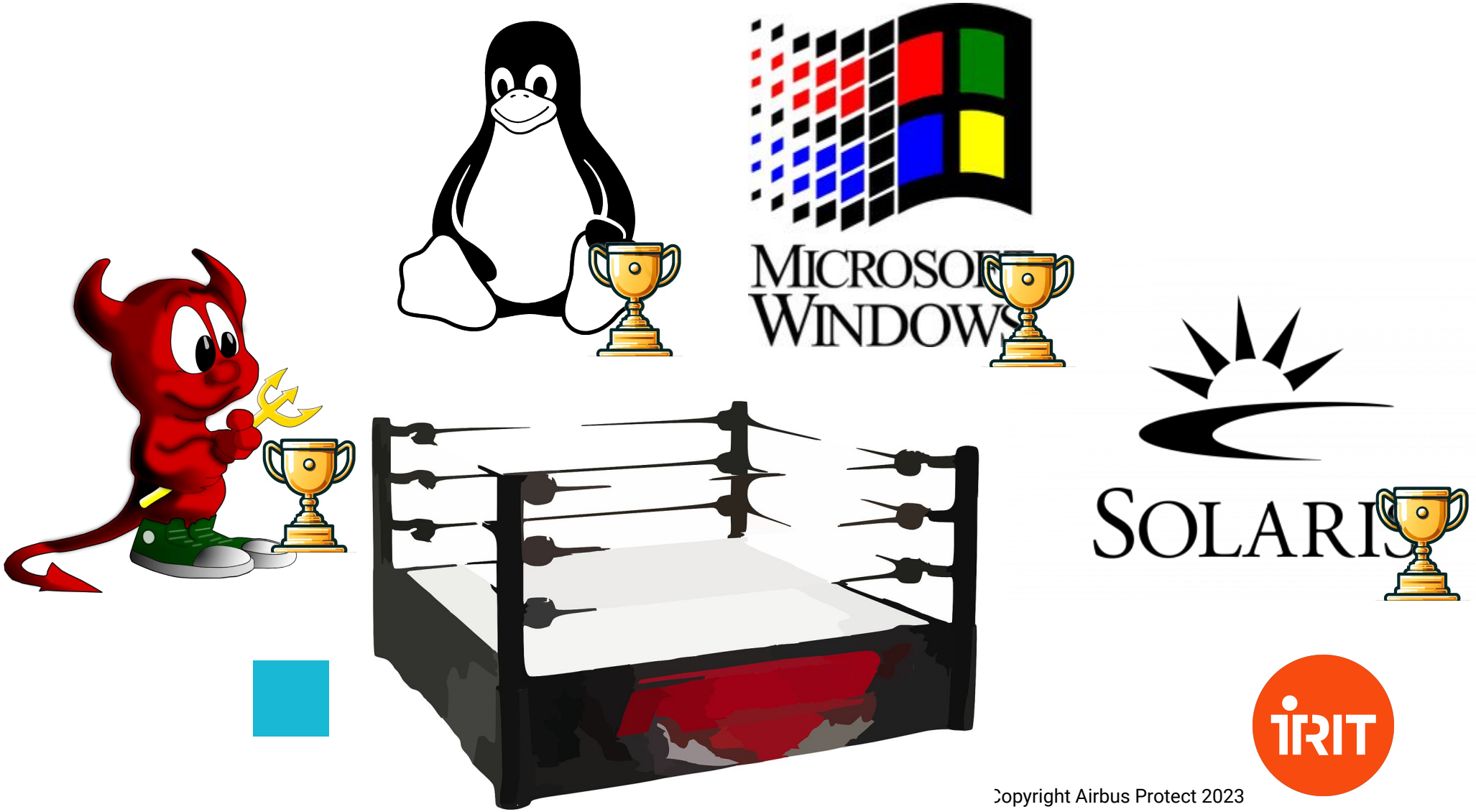


Partial,
with LSM

🎉**YES**🎉
So it's safe



Which one is winning ?



IRIT

AIRBUS

What could-we do next ?

Make Linux the real winner because

…

we need a winner

RootAsRole project

- Find out which capability is requested for a program.
- And many more incoming features !

	setcap	sudo	sr
change user		✅	✅
change groups		✅	✅
set capabilities	✅		✅
strict command		✅	✅
prevent direct privilege escalation			✅
unknown features that nobody knows		⚠️✅⚠️	

Give us a star 🌟

Let's talk !

Root as Role

Give us a star

THCON 2024
TOULOUSE HACKING CONVENTION

Questions ?

Eddie Billoir,
Romain Laborde,
Ahmad Samer Wazan,
Yves Rütschlé,
Abdelmalek Benzekri

ANRT ASSOCIATION NATIONALE RECHERCHE TECHNOLOGIE
Cifre
UNIVERSITÉ TOULOUSE III PAUL SABATIER
Admitt
IRIT
AIRBUS