THCON 2024

TOULOUSE HACKING CONVENTION

Présentation

- Une conférence sur la cybersécurité
- Rassemble étudiants, pros et chercheurs
- Depuis 2016 à Paul Sabatier
- Plusieurs sponsors et partenaires

THCON

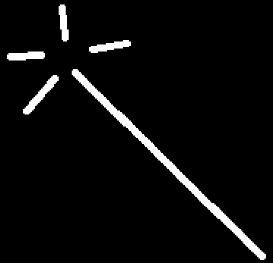
INP N7
ami TOULOUSE
ICO
Gold sponsors
MISC
Orange Cyberdefense
sopra steria
xmco
AIRBUS
iTRUST
Silver sponsors
VIVERIS
squad
LEXFO
Continental
ESNA
Lyra
THALES
ynov CAMPUS
Bronze sponsors
SYNACKTIV
G ECHO cybersécurité

RootMe
PRO
#1
LA VERSION PRO
de LA PLATEFORME
DE RÉFÉRENCE
EN CYBERSÉCURITÉ
ENTRAINEZ & SENSIBILISEZ
IDENTIFIEZ & RECRUTEZ
CHALLENGEZ & FÉDÉREZ
CONTRIBUEZ & COMMUNIQUEZ
REJOIGNEZ LA

Notre sélection :

- Bringing the Science of Cybersecurity out of the Dark Ages
- Vulnérabilitée Ubuntu ShiftFS
- Security analysis of radio water meters
- Exploring OS administratives privileges
- Hunting for Evidence of Malicious Behavior

- Dark ages : ignorance and error
- Age of Enlightment : knowledge and understanding

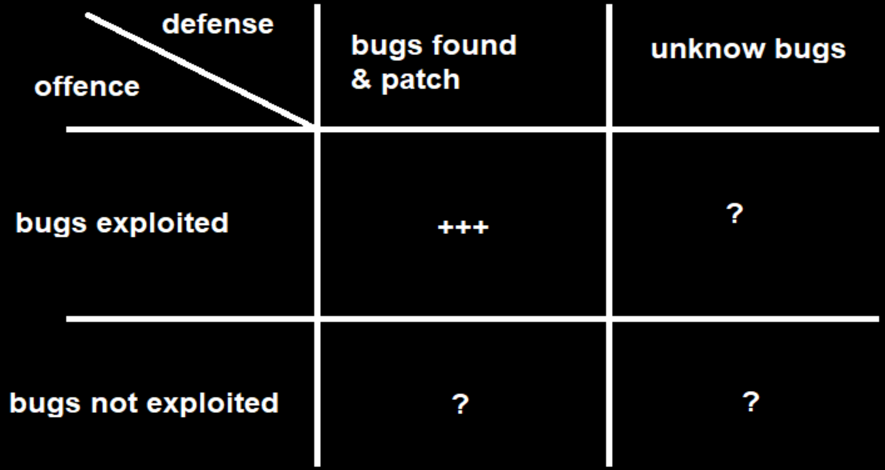


Bringing the Science of Cybersecurity out of the Dark Ages
by Jiska Classen Hasso Plattner Institute, University of Potsdam

- Where are we at the moment ?
- The Philosopher stone <=> unhackable systeme
- Metal to gold <=> bug to CVE

Bringing the Science of Cybersecurity out of the Dark Ages
by Jiska Classen Hasso Plattner Institute, University of Potsdam

- What is happenning rn ? Bluid & break loop



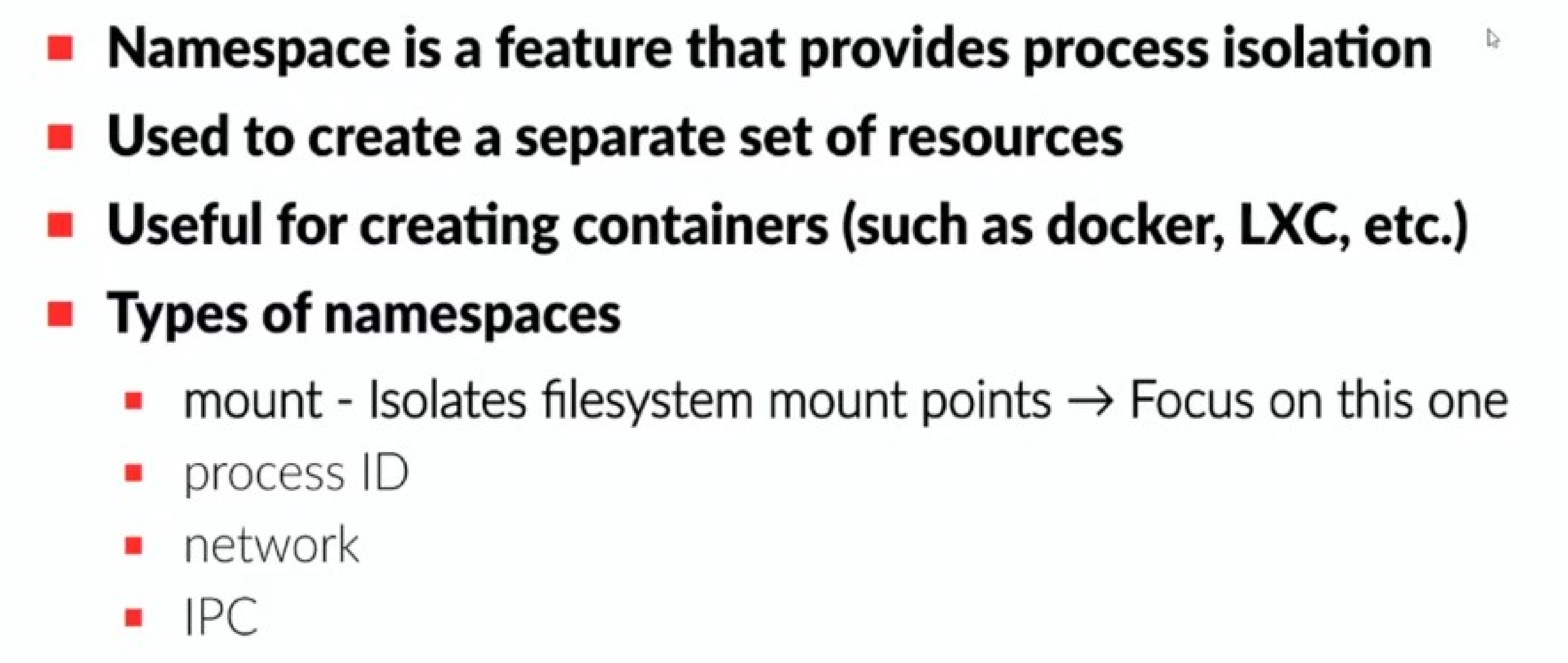
defense offence	bugs found & patch	unknow bugs
bugs exploited	+++	?
bugs not exploited	?	?

- What next ?
- Break to patch loop => kinda ok at the moment
- Open source will help
- Court alchemist = fraud vendor
- IA fussing

Ubuntu ShiftFS :

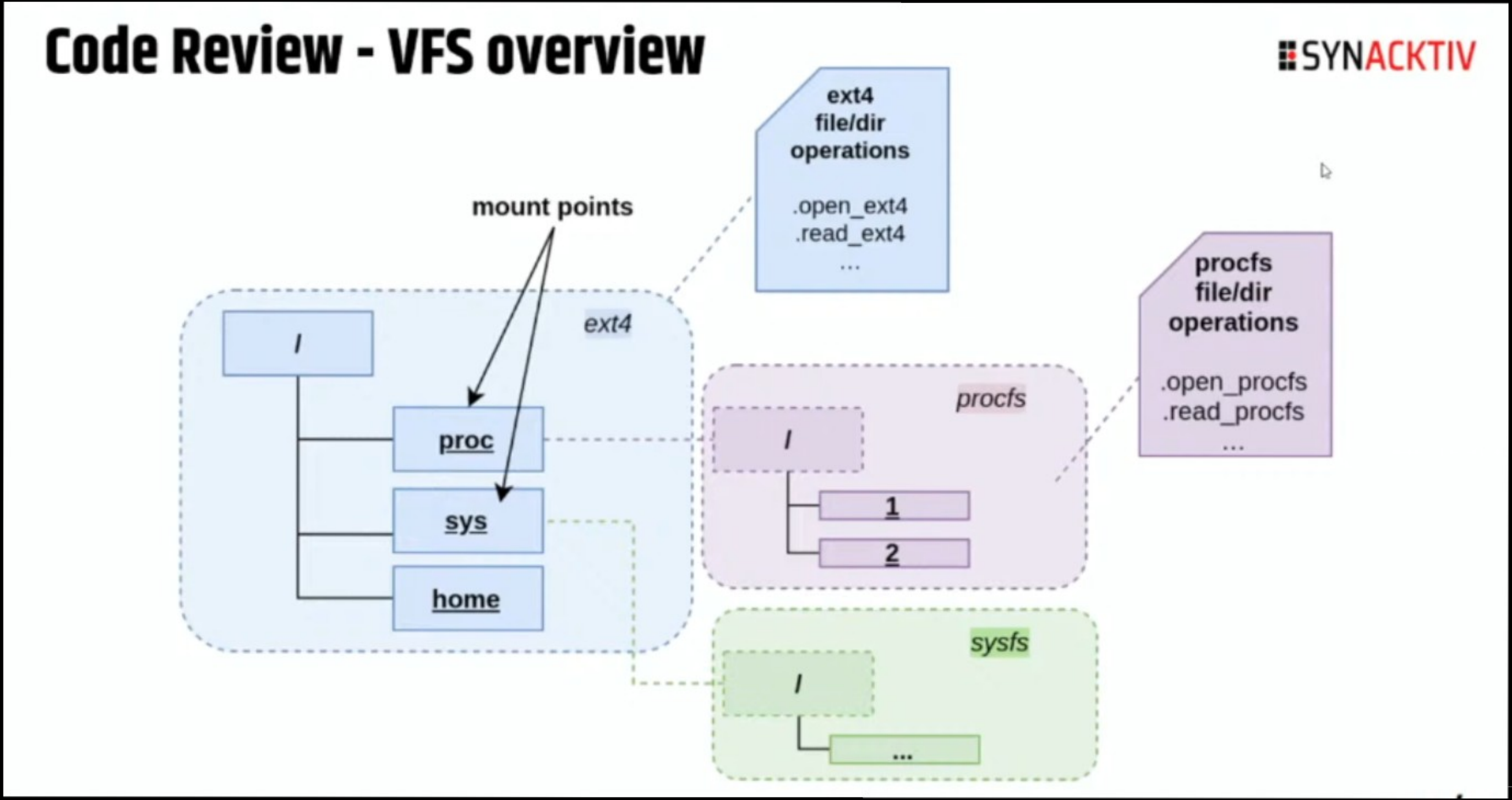
- ShiftFS est un Filesystem présent uniquement sous Ubuntu
- La faille a été remontée dans la CVE-2023-2612
- L’exploit permet d’obtenir des droits root sur un dossier
- Le noyau contenait une condition de concurrence critique lors de la gestion du verrouillage des inodes dans certaines situations
- L’attaquant pourrait ensuite exploiter du code malveillant

Ubuntu ShiftFS :



- **Namespace is a feature that provides process isolation**
- **Used to create a separate set of resources**
- **Useful for creating containers (such as docker, LXC, etc.)**
- **Types of namespaces**
  - mount - Isolates filesystem mount points → Focus on this one
  - process ID
  - network
  - IPC

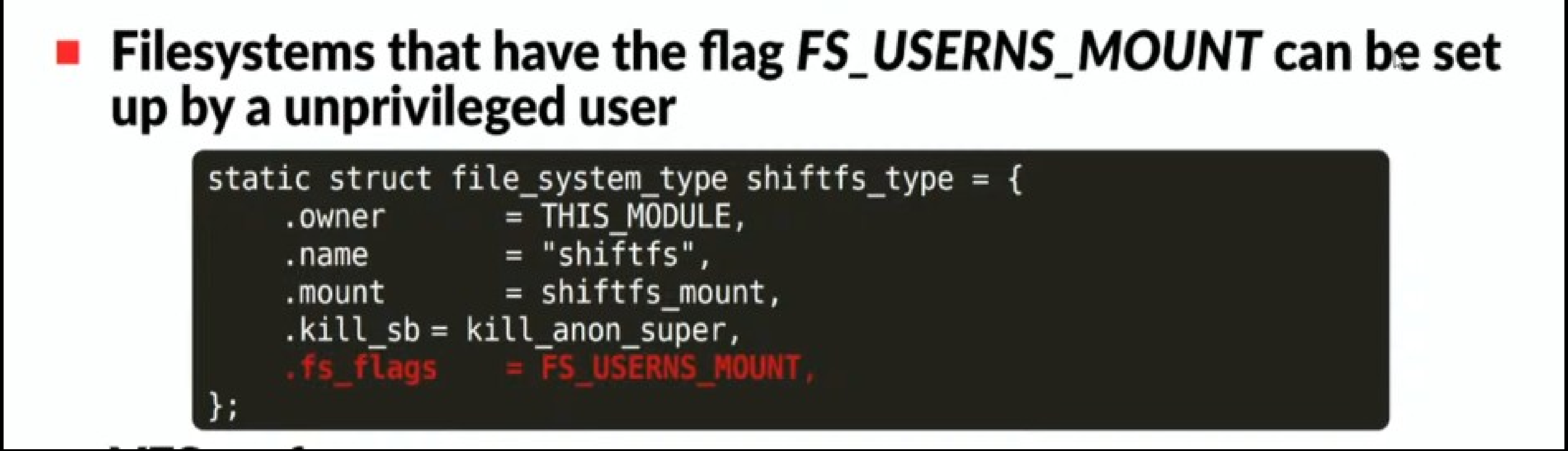
Ubuntu ShiftFS



Code Review - VFS overview

SYNACKTIV

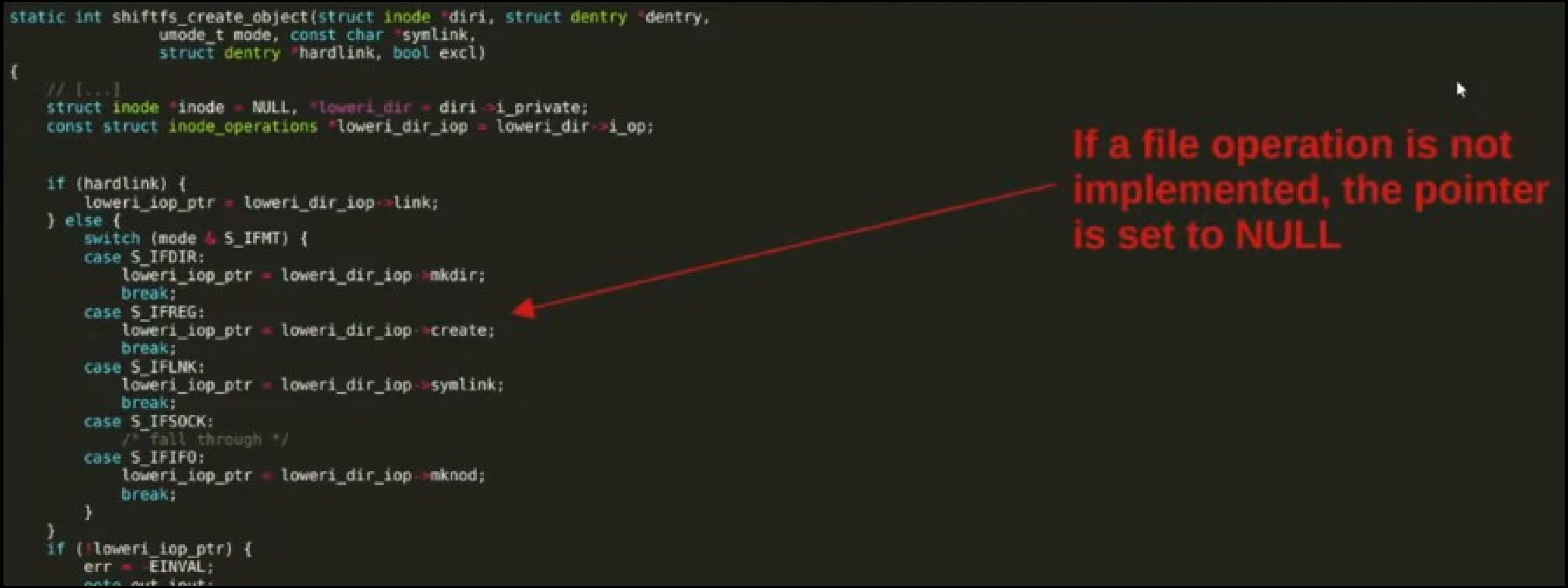
Ubuntu ShiftFS :



- Filesystems that have the flag *FS_USERNS_MOUNT* can be set up by a unprivileged user

```
static struct file_system_type shiftfs_type = {
	.owner		= THIS_MODULE,
	.name		= "shiftfs",
	.mount		= shiftfs_mount,
	.kill_sb = kill_anon_super,
	.fs_flags	= FS_USERNS_MOUNT,
};
```

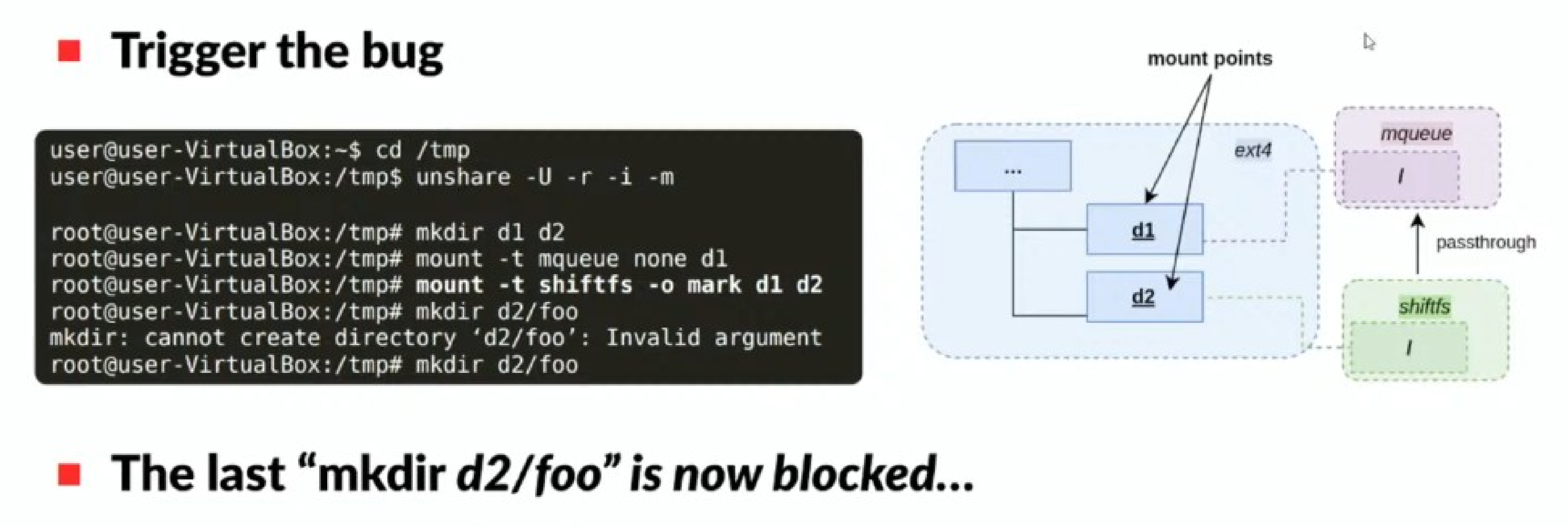
Ubuntu ShiftFS :



```
static int shiftfs_create_object(struct inode *diri, struct dentry *dentry,
                umode_t mode, const char *symlink,
                struct dentry *hardlink, bool excl)
{
    // [...]
    struct inode *inode = NULL, *loweri_dir = diri->i_private;
    const struct inode_operations *loweri_dir_iop = loweri_dir->i_op;


    if (hardlink) {
        loweri_iop_ptr = loweri_dir_iop->link;
    } else {
        switch (mode & S_IFMT) {
        case S_IFDIR:
            loweri_iop_ptr = loweri_dir_iop->mkdir;
            break;
        case S_IFREG:
            loweri_iop_ptr = loweri_dir_iop->create;
            break;
        case S_IFLNK:
            loweri_iop_ptr = loweri_dir_iop->symlink;
            break;
        case S_IFSOCK:
            /* fall through */
        case S_IFIFO:
            loweri_iop_ptr = loweri_dir_iop->mknod;
            break;
        }
    }
    if (!loweri_iop_ptr) {
        err = -EINVAL;
        goto out_iput;
```

If a file operation is not implemented, the pointer is set to NULL

Ubuntu ShiftFS :

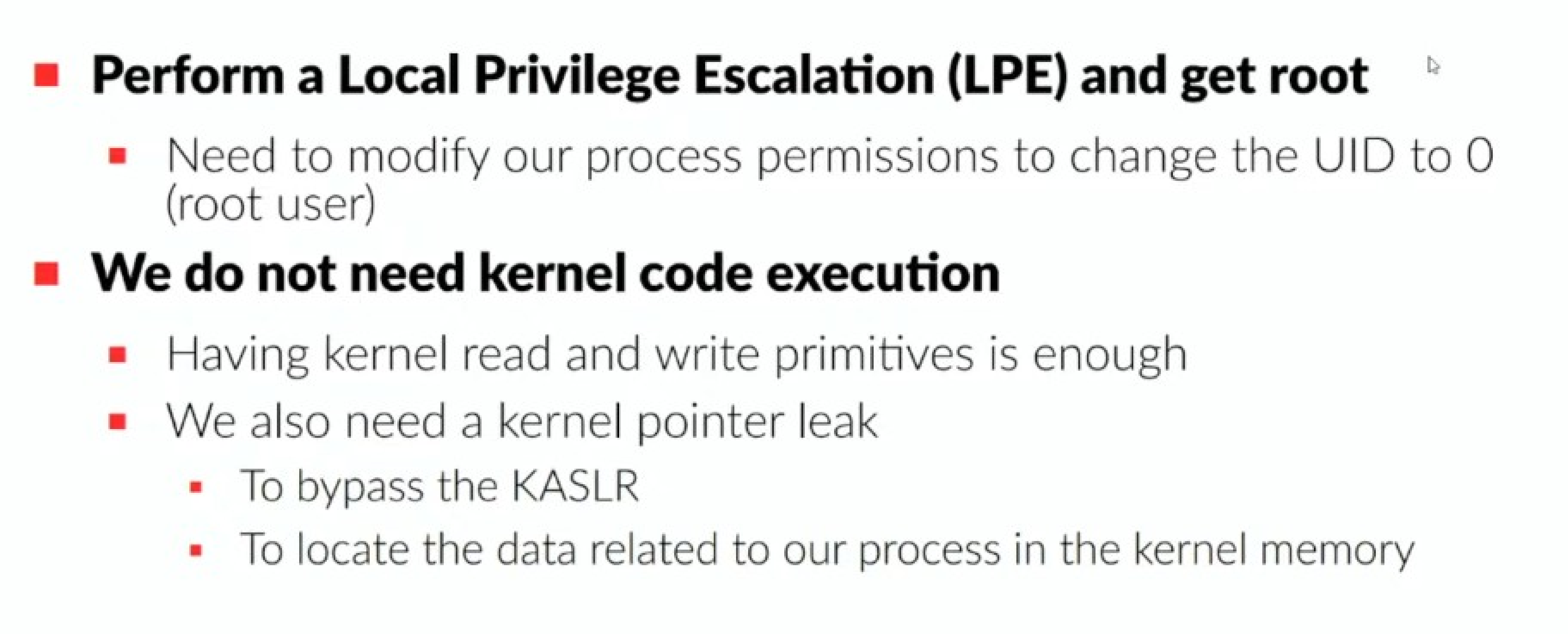


- **Trigger the bug**

```
user@user-VirtualBox:~$ cd /tmp
user@user-VirtualBox:/tmp$ unshare -U -r -i -m

root@user-VirtualBox:/tmp# mkdir d1 d2
root@user-VirtualBox:/tmp# mount -t mqueue none d1
root@user-VirtualBox:/tmp# mount -t shiftfs -o mark d1 d2
root@user-VirtualBox:/tmp# mkdir d2/foo
mkdir: cannot create directory ‘d2/foo’: Invalid argument
root@user-VirtualBox:/tmp# mkdir d2/foo
```

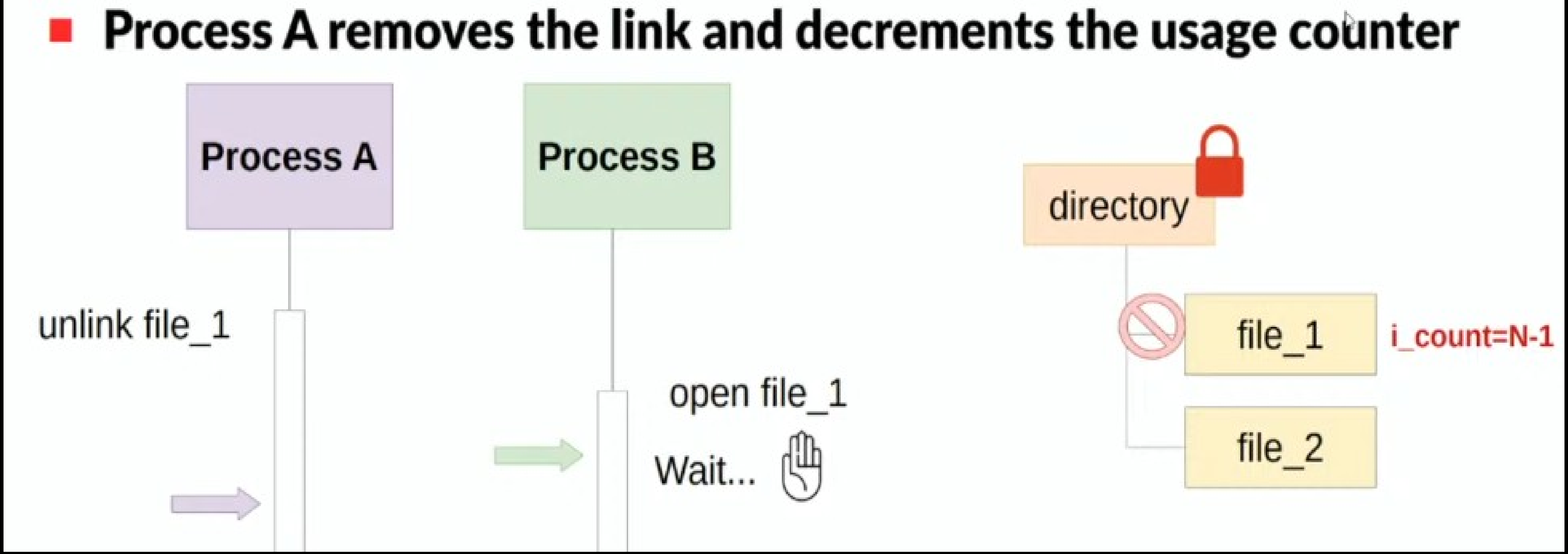
- **The last “mkdir *d2/foo*” *is now blocked...***

Ubuntu ShiftFS :



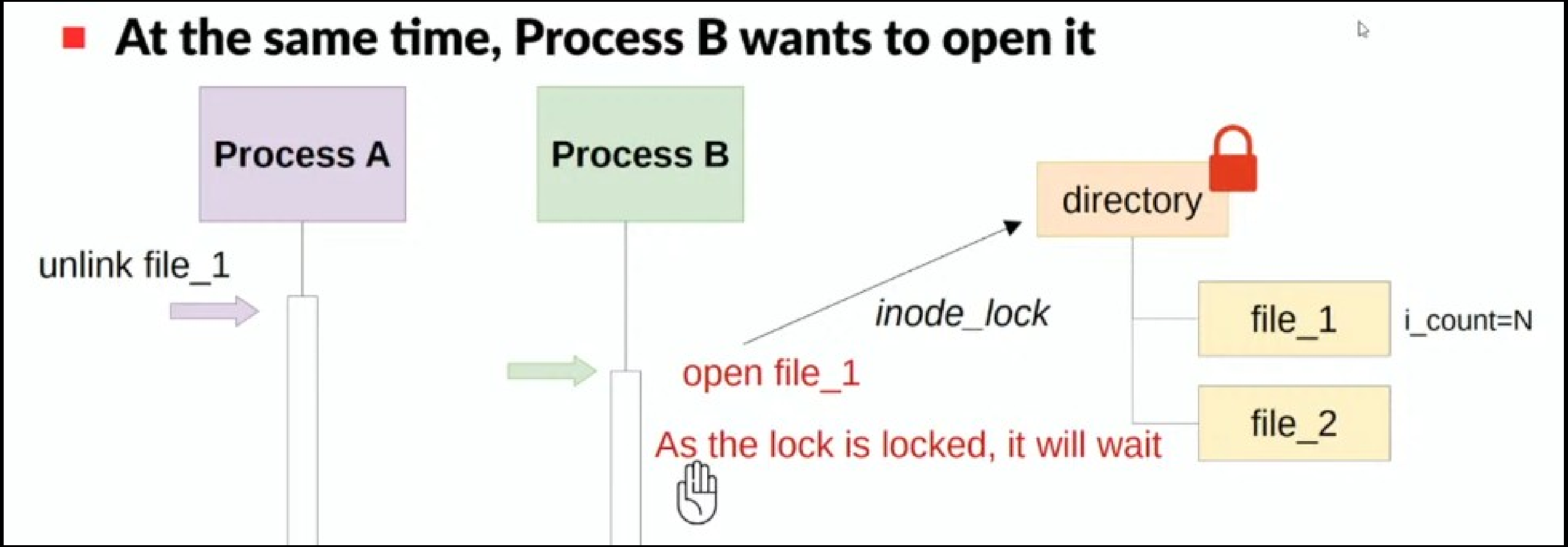
- **Perform a Local Privilege Escalation (LPE) and get root**
  - Need to modify our process permissions to change the UID to 0 (root user)
- **We do not need kernel code execution**
  - Having kernel read and write primitives is enough
  - We also need a kernel pointer leak
    - To bypass the KASLR
    - To locate the data related to our process in the kernel memory

Ubuntu ShiftFS :



- Process A removes the link and decrements the usage counter

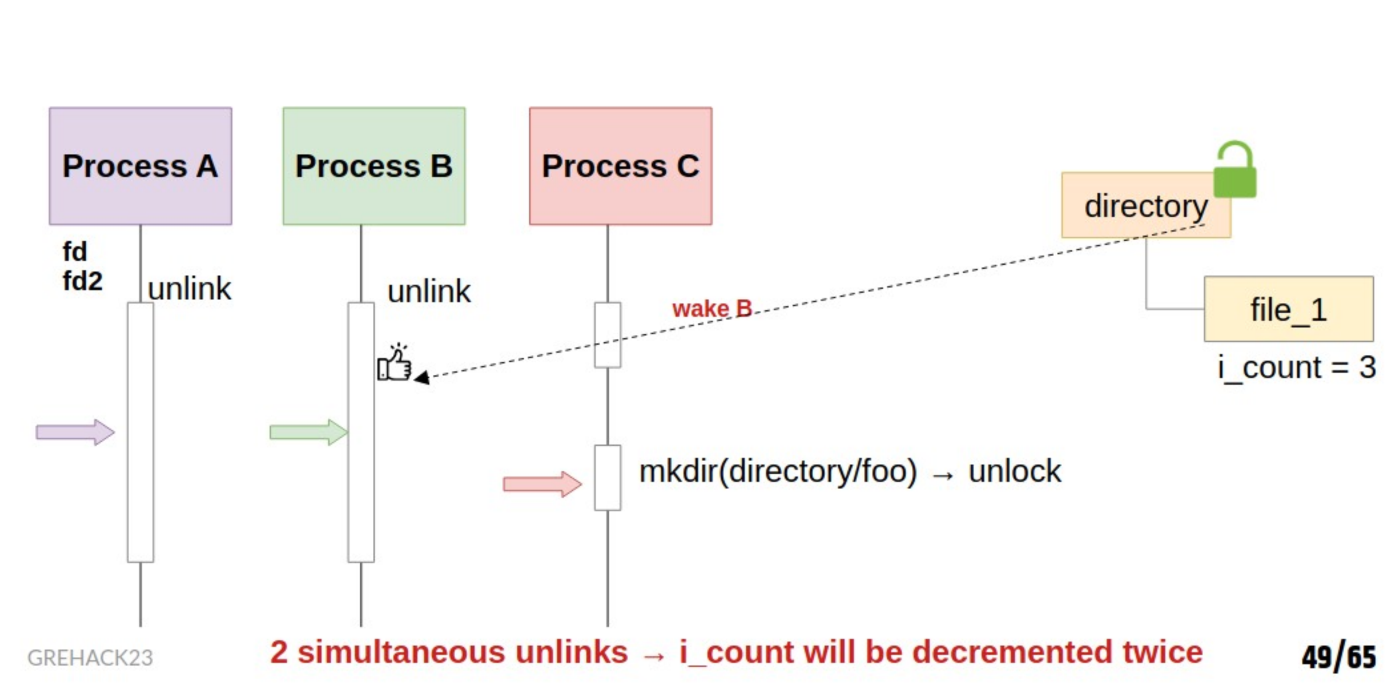
Ubuntu ShiftFS :



- At the same time, Process B wants to open it

As the lock is locked, it will wait

Ubuntu ShiftFS :

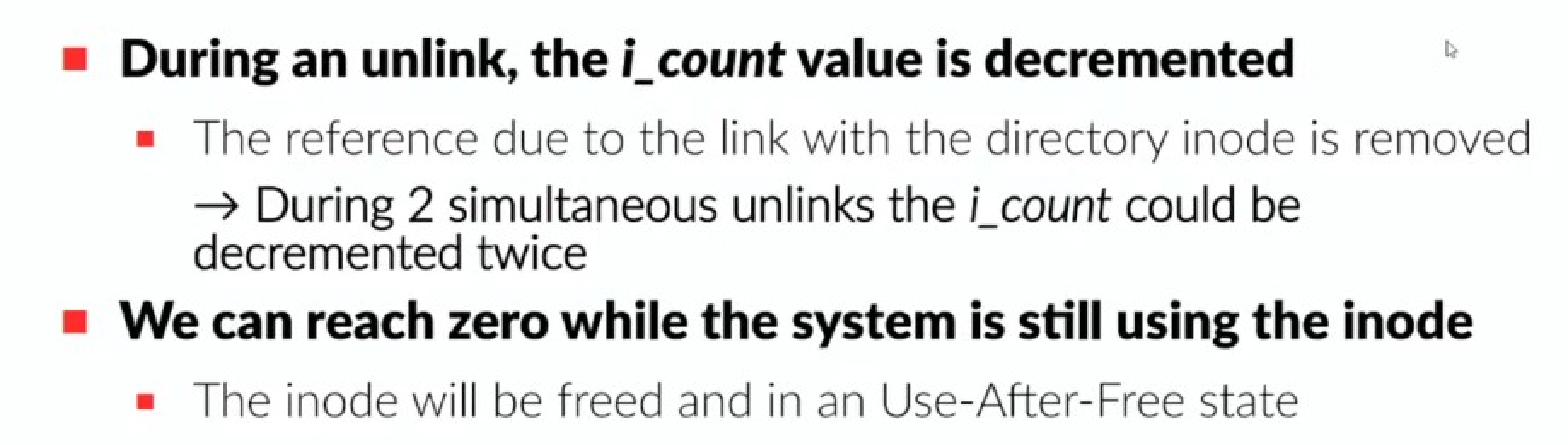


2 simultaneous unlinks → i_count will be decremented twice

GREHACK23

49/65

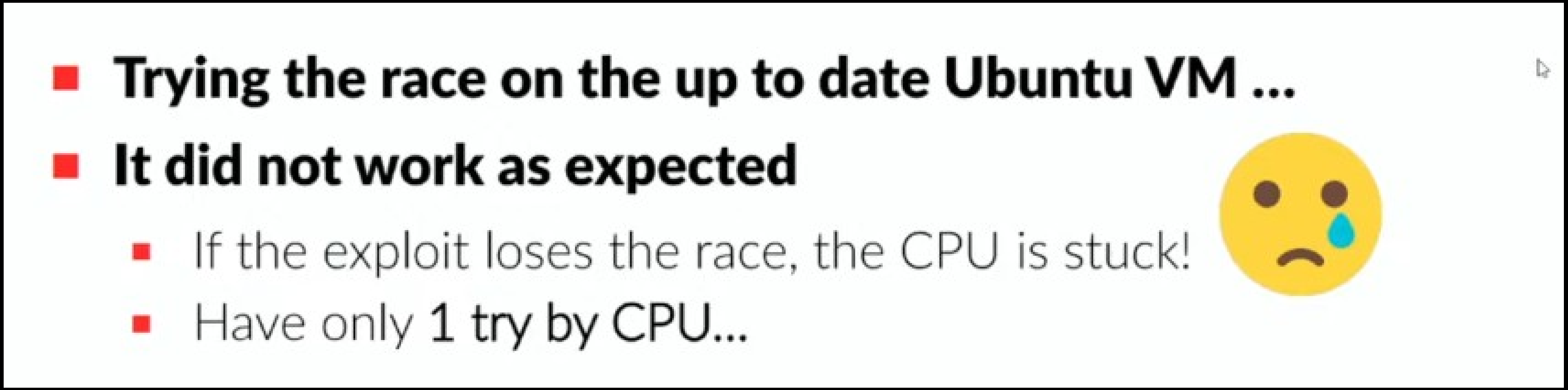
Ubuntu ShiftFS :



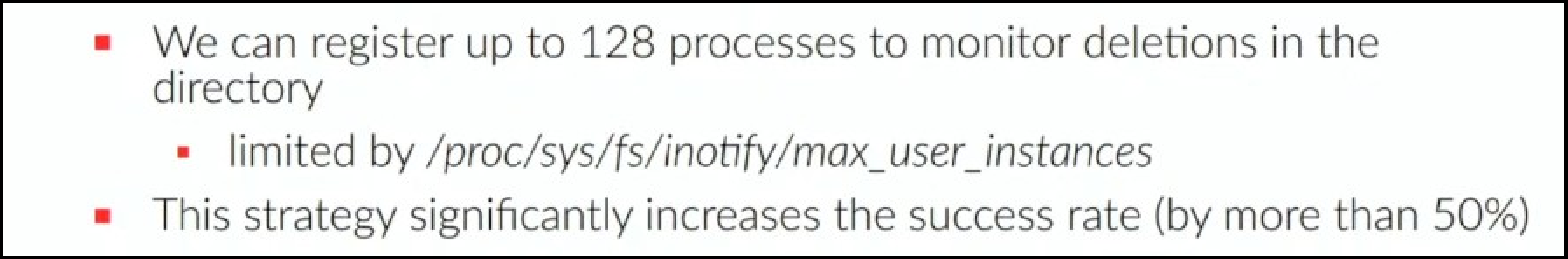
- **During an unlink, the *i_count* value is decremented**
  - The reference due to the link with the directory inode is removed

    → During 2 simultaneous unlinks the *i_count* could be decremented twice
- **We can reach zero while the system is still using the inode**
  - The inode will be freed and in an Use-After-Free state

Ubuntu ShiftFS :

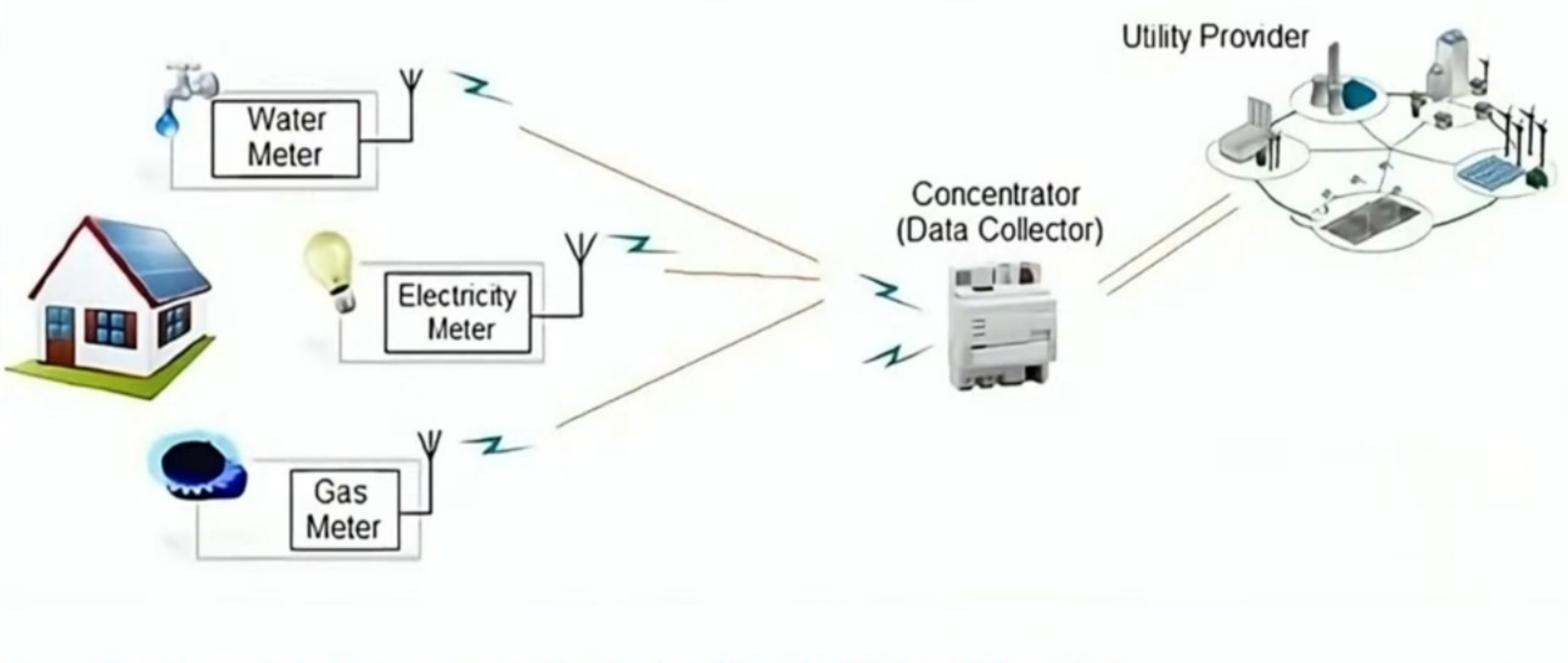


- **Trying the race on the up to date Ubuntu VM ...**
- **It did not work as expected**
  - If the exploit loses the race, the CPU is stuck! 😢
  - Have only **1 try by CPU...**

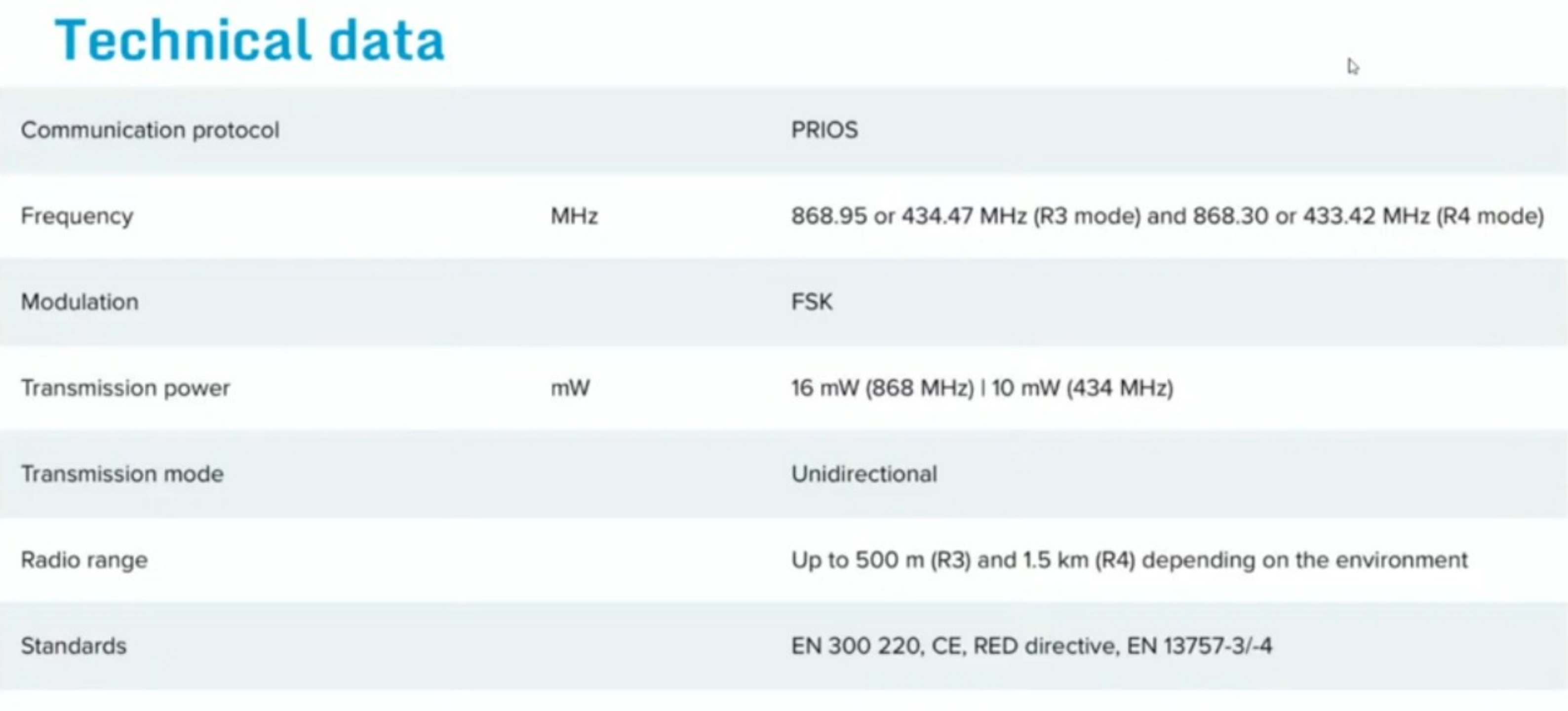


- We can register up to 128 processes to monitor deletions in the directory
  - limited by */proc/sys/fs/inotify/max_user_instances*
- This strategy significantly increases the success rate (by more than 50%)

Security analysis of radio water meters
by Lucas Georget - LAAS-CNRS Toulouse

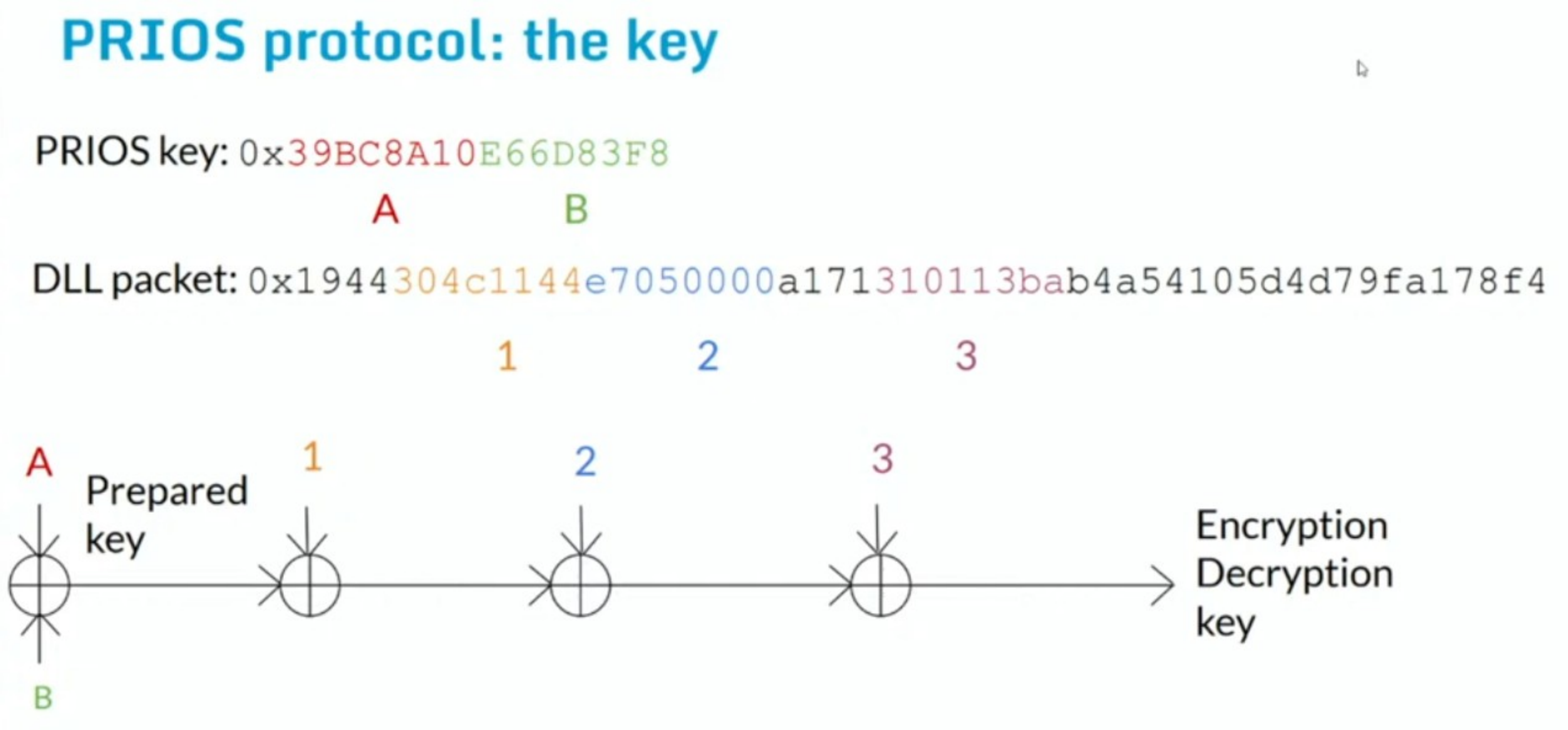


From https://www.rfwireless-world.com/Terminology/What-is-Wireless-M-Bus.html



Technical data

Communication protocol		PRIOS
Frequency	MHz	868.95 or 434.47 MHz (R3 mode) and 868.30 or 433.42 MHz (R4 mode)
Modulation		FSK
Transmission power	mW	16 mW (868 MHz) I 10 mW (434 MHz)
Transmission mode		Unidirectional
Radio range		Up to 500 m (R3) and 1.5 km (R4) depending on the environment
Standards		EN 300 220, CE, RED directive, EN 13757-3/-4



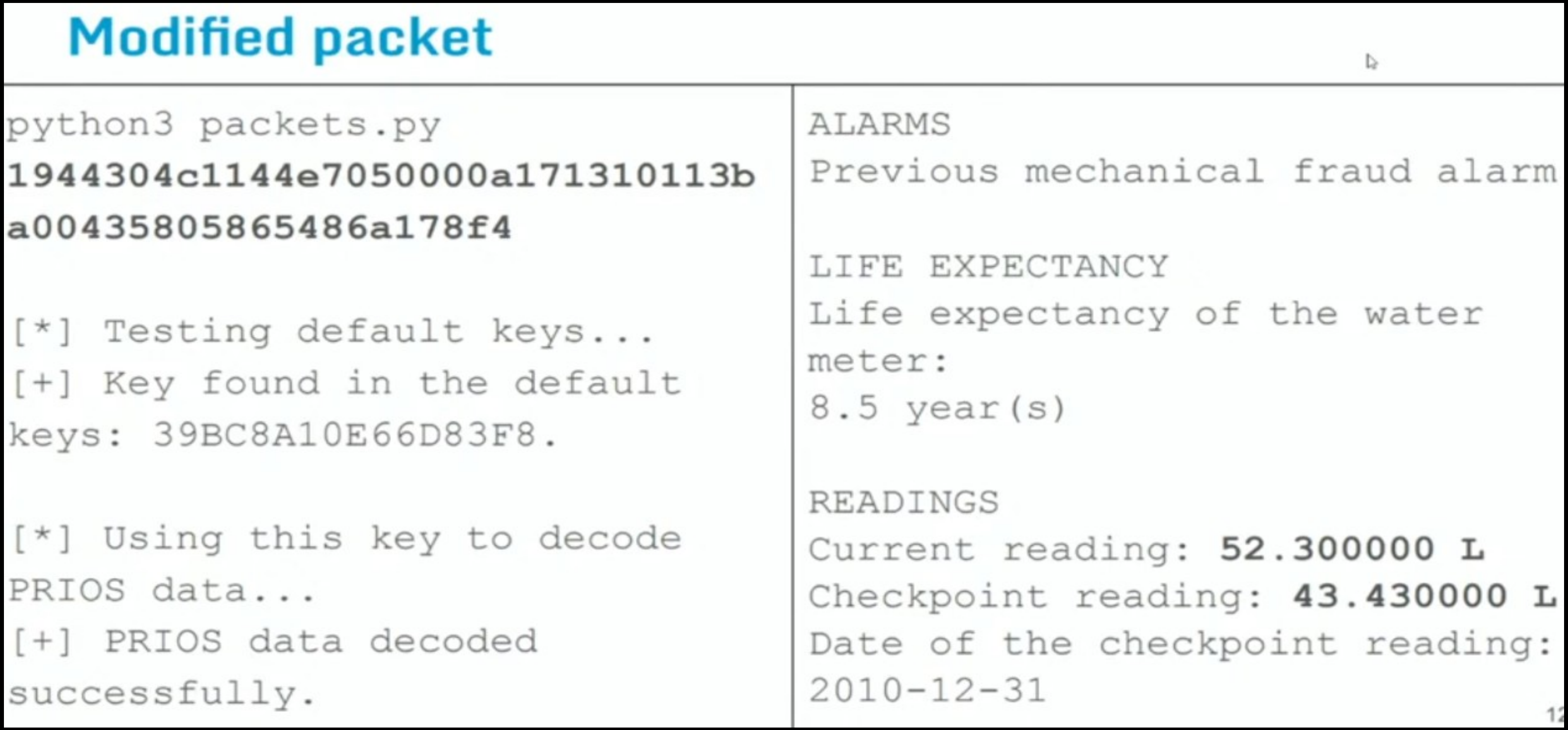
PRIOS protocol: the key

PRIOS key: 0x39BC8A10E66D83F8

A B

DLL packet: 0x1944304c1144e7050000a171310113bab4a54105d4d79fa178f4

1 2 3



Modified packet

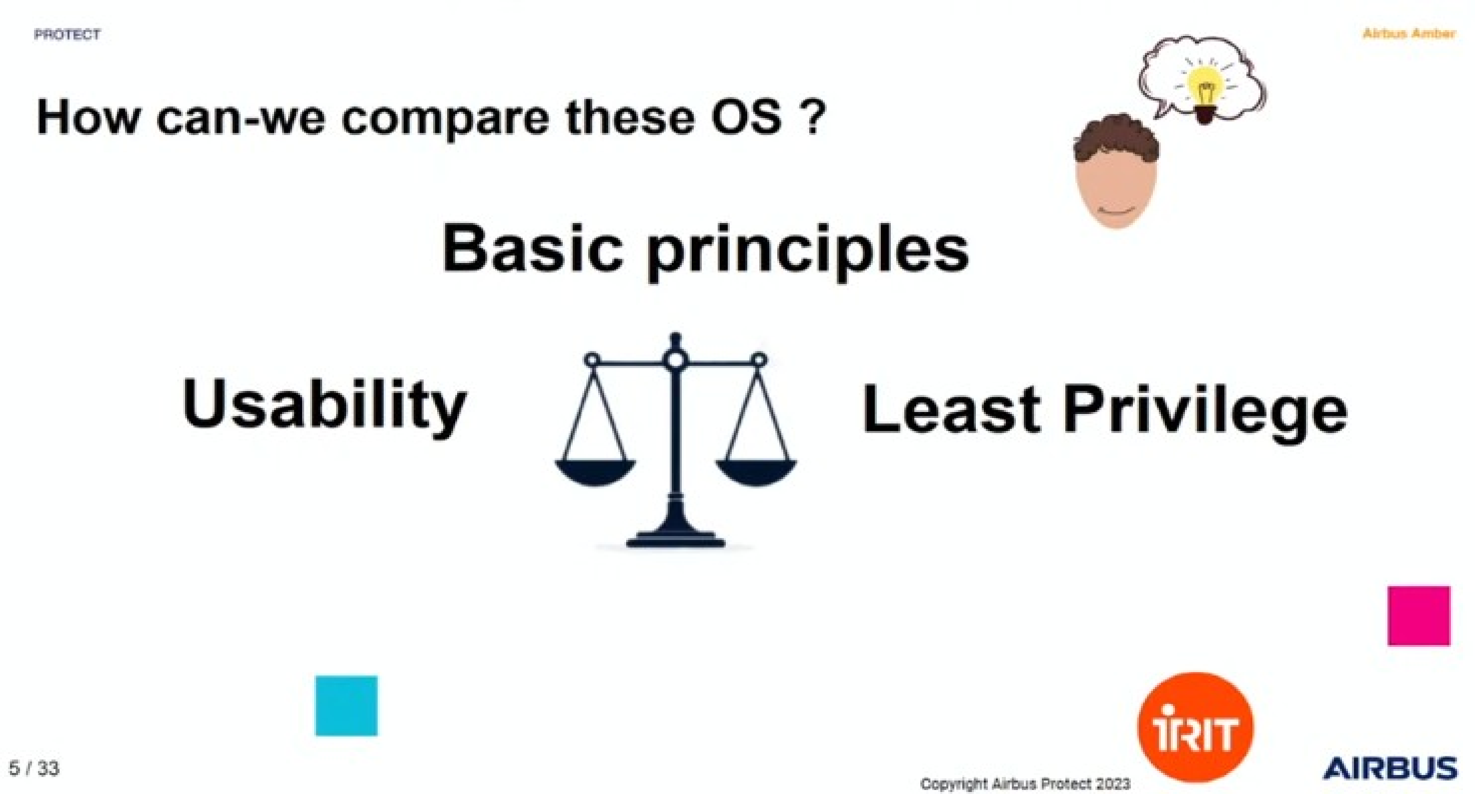
```
python3 packets.py
1944304c1144e7050000a171310113b
a00435805865486a178f4

[*] Testing default keys...
[+] Key found in the default
keys: 39BC8A10E66D83F8.

[*] Using this key to decode
PRIOS data...
[+] PRIOS data decoded
successfully.
```

```
ALARMS
Previous mechanical fraud alarm

LIFE EXPECTANCY
Life expectancy of the water
meter:
8.5 year(s)

READINGS
Current reading: 52.300000 L
Checkpoint reading: 43.430000 L
Date of the checkpoint reading:
2010-12-31
```

OS administratives privileges

- Explication de l’évolution de l’administration des privilèges
- Linux est le premier OS à avoir implémenté une séparation
- La recherche porte sur la capacité des autres OS à séparer
- Le but est de savoir lequel est le meilleur pour manager les privilèges

OS administratives privileges



PROTECT

Airbus Amber

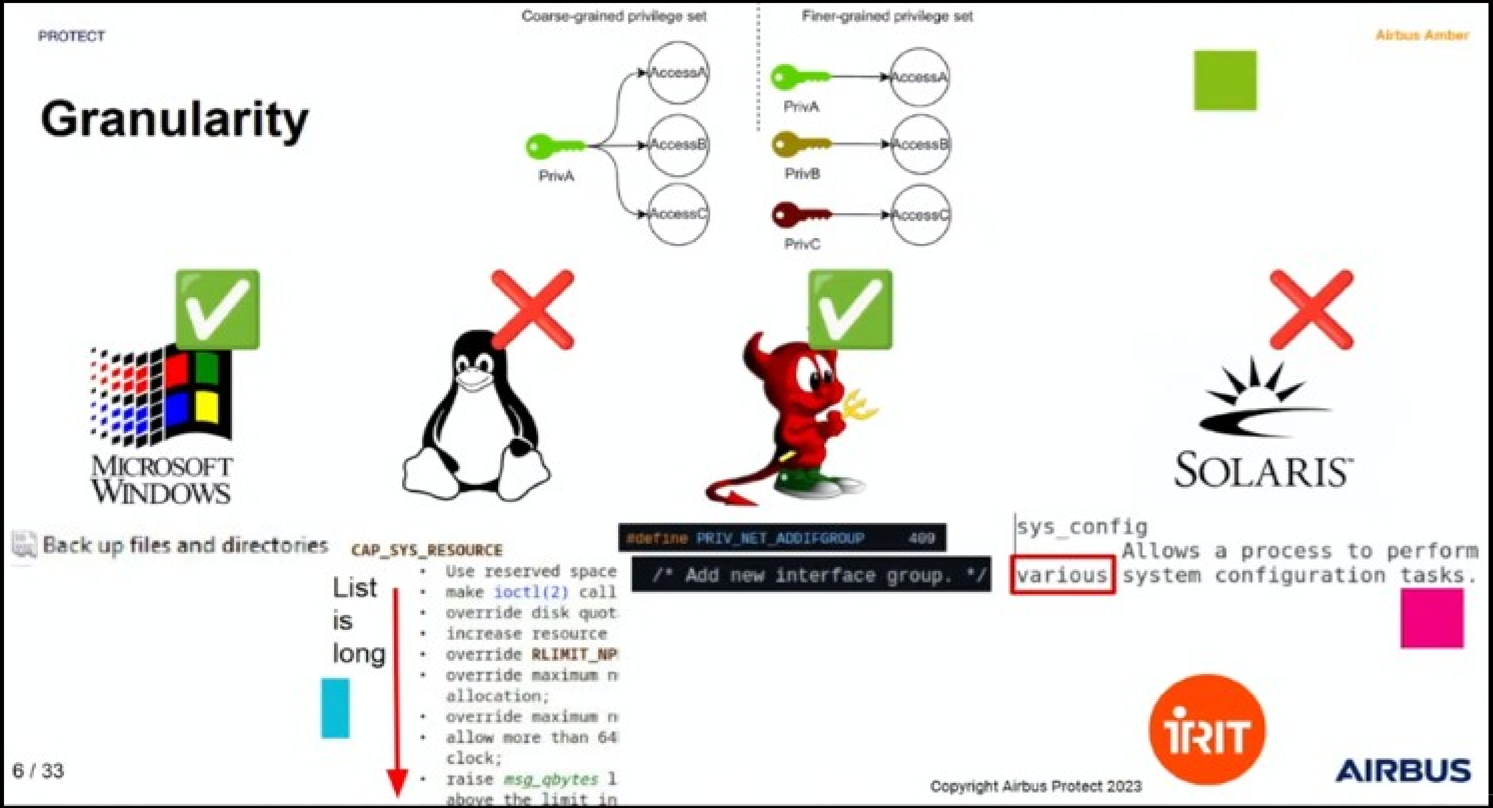
How can-we compare these OS ?

Basic principles

Usability

Least Privilege

OS administratives privileges



PROTECT

Airbus Amber

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. */
```

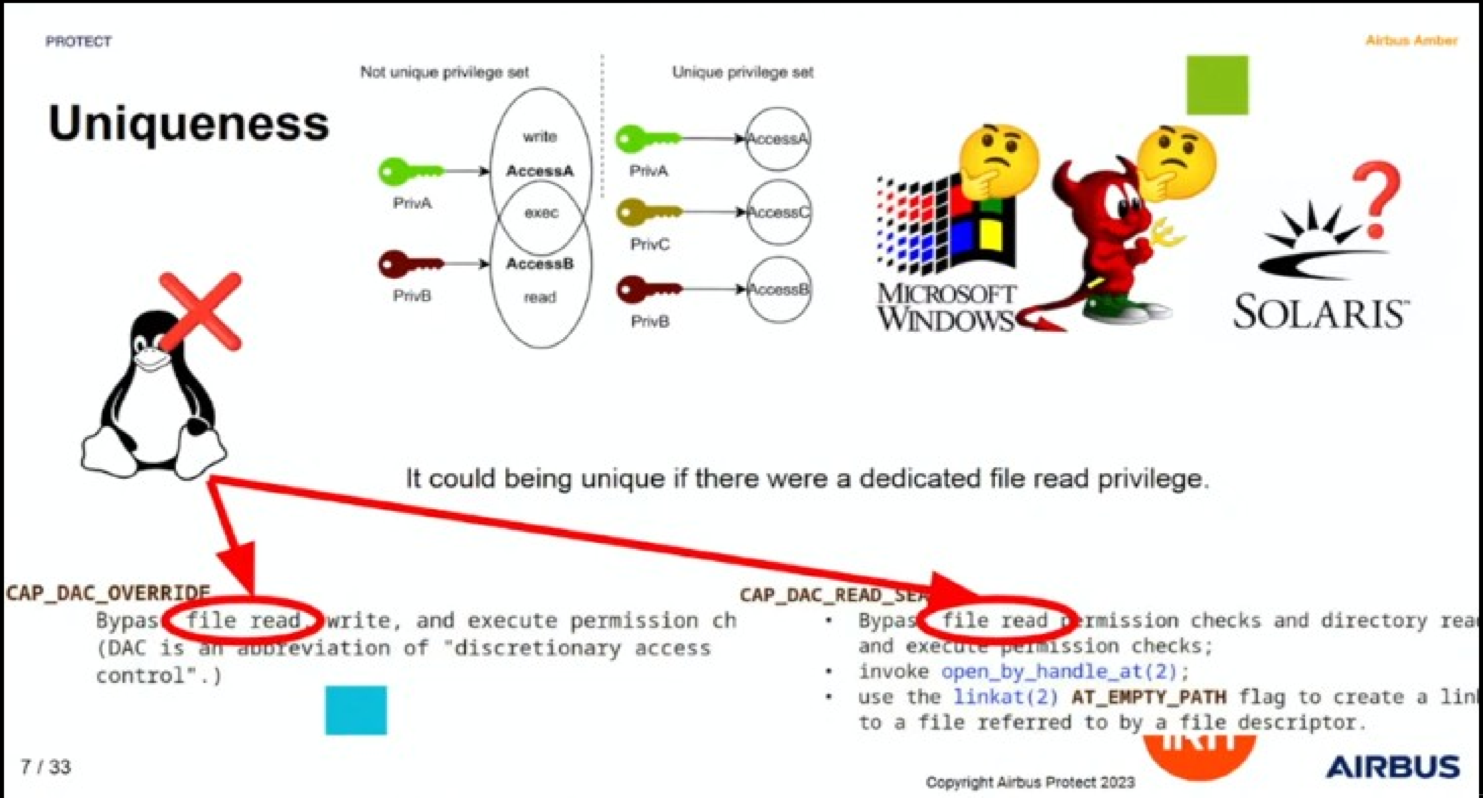
```
sys_config
        Allows a process to perform
various system configuration tasks.
```

6 / 33

IRIT

AIRBUS

OS administratives privileges



PROTECT

Airbus Amber

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".)
```

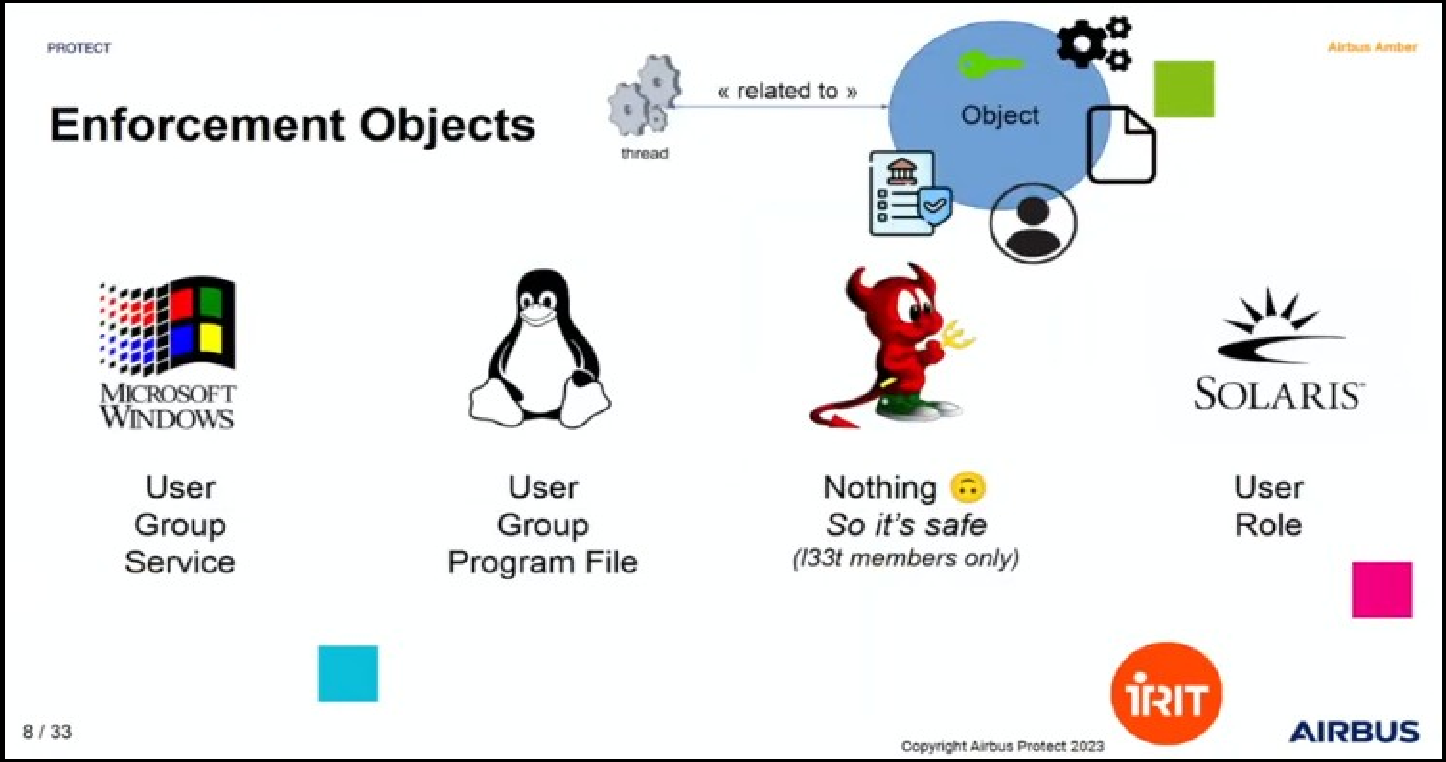
```
CAP_DAC_READ_SEA
       •  Bypass file read permission checks and directory rea
          and execute permission checks;
       •  invoke open_by_handle_at(2);
       •  use the linkat(2) AT_EMPTY_PATH flag to create a lin
          to a file referred to by a file descriptor.
```

7 / 33

Copyright Airbus Protect 2023

AIRBUS

OS administratives privileges



Enforcement Objects

thread « related to » Object

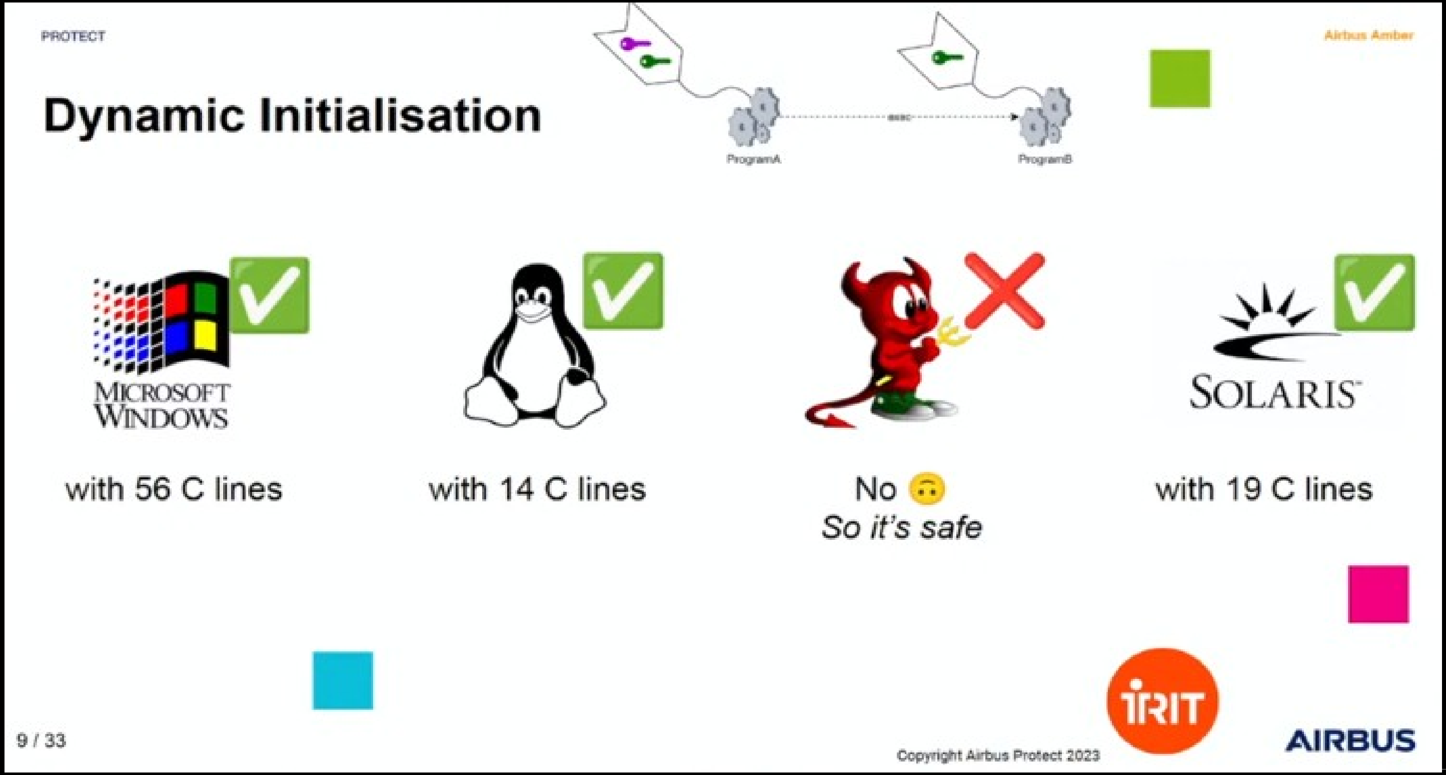
User
Group
Service

User
Group
Program File

Nothing 🙃
So it's safe
(l33t members only)

User
Role

OS administratives privileges



PROTECT

Airbus Amber

Dynamic Initialisation

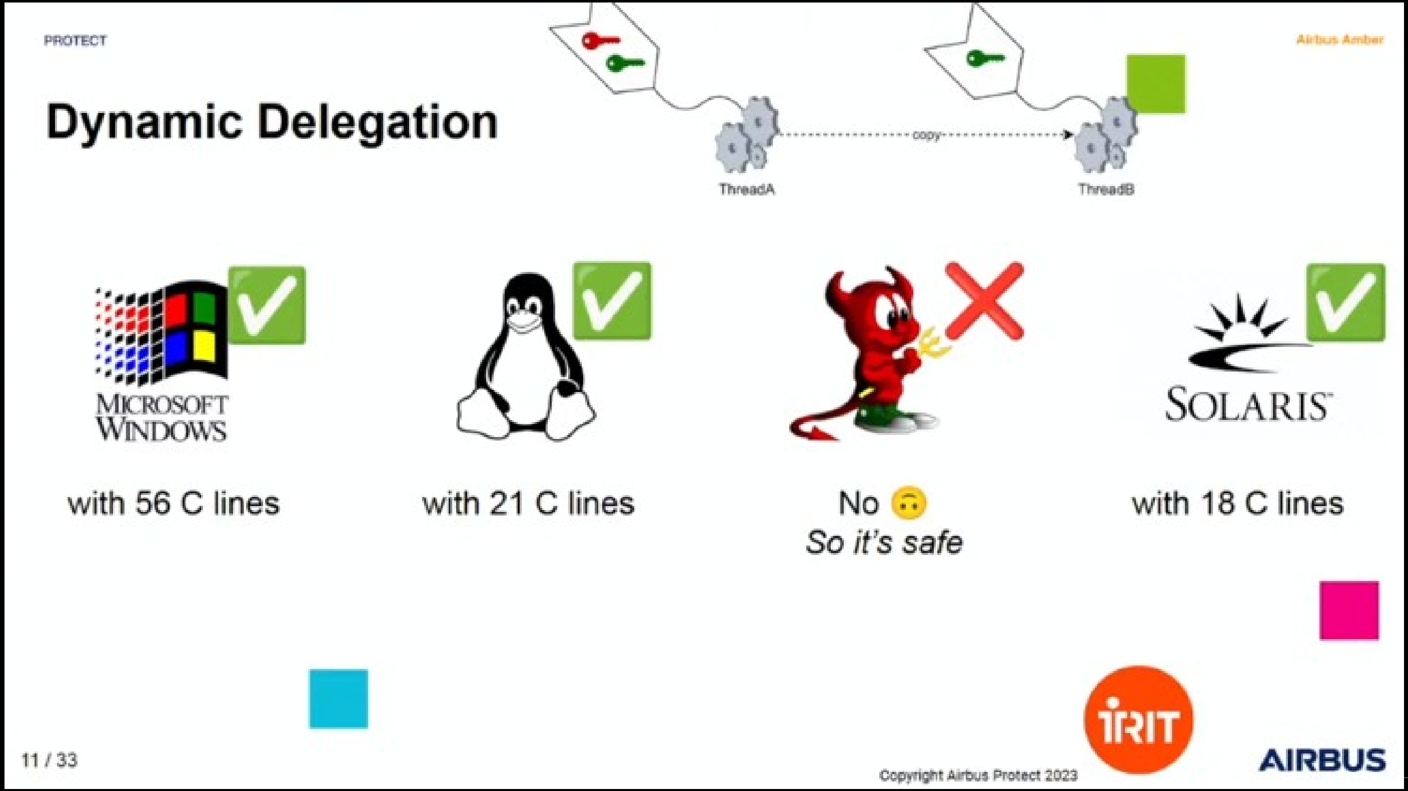
with 56 C lines ✅

with 14 C lines ✅

No 🙃 ❌
So it's safe

with 19 C lines ✅

OS administratives privileges



PROTECT

Airbus Amber

Dynamic Delegation

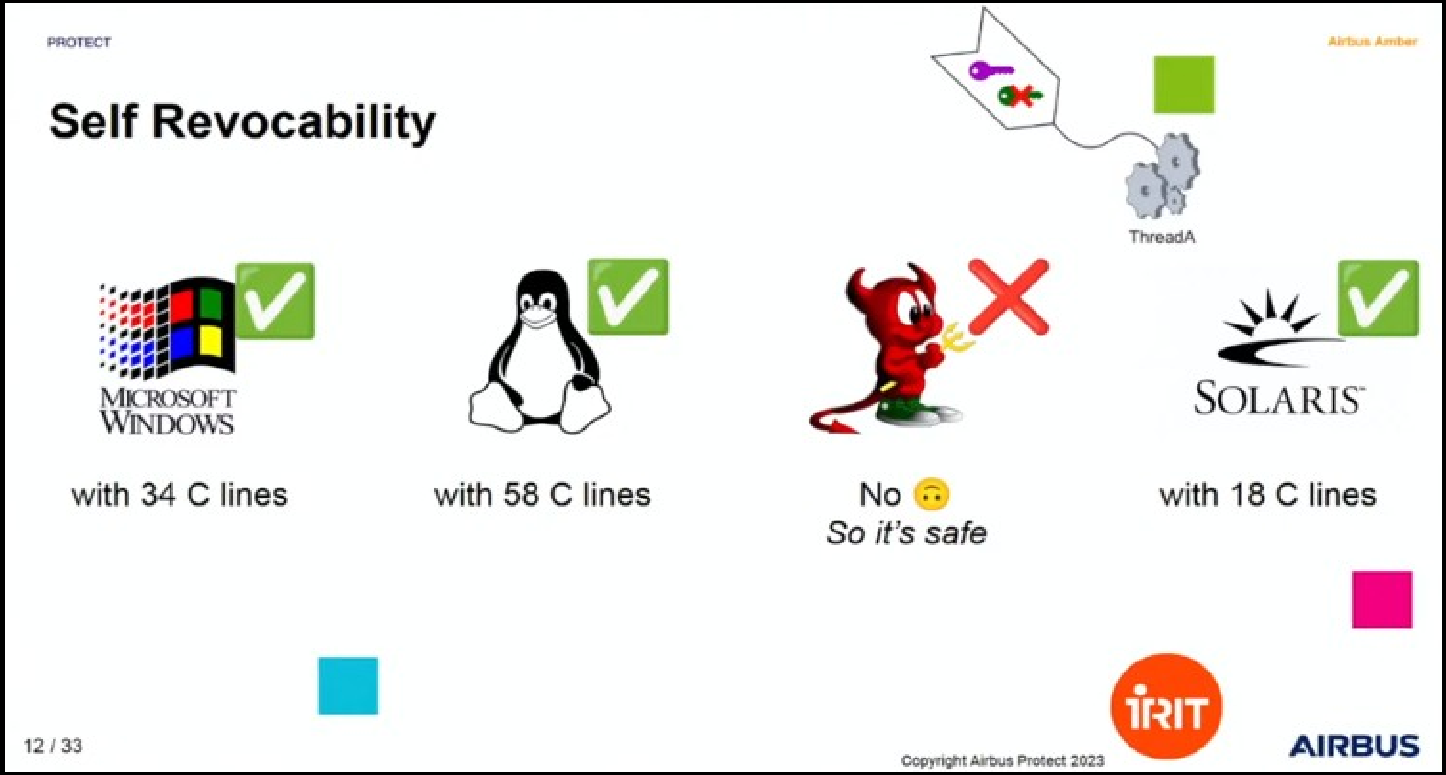
✓ with 56 C lines

✓ with 21 C lines

✗ No 🙃
So it's safe

✓ with 18 C lines

OS administratives privileges



PROTECT

Airbus Amber

Self Revocability

ThreadA

✓ with 34 C lines

✓ with 58 C lines

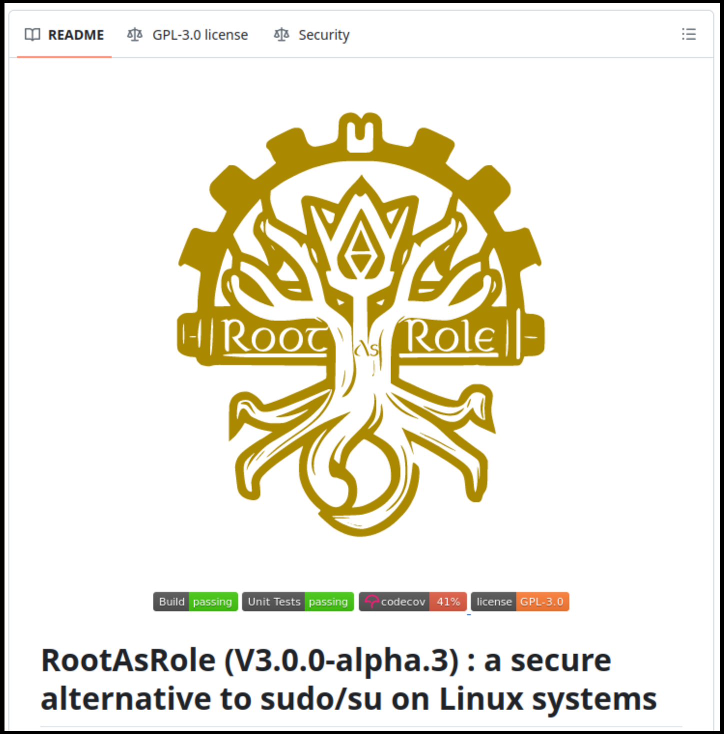
✗ No 🙃
So it's safe

✓ with 18 C lines

OS administratives privileges

- Conclusion, lequel est donc safe ?
- Aucun ne propose un compromis parfait entre sécurité et usabilité
- Freebsd reste le plus sécure
- Mais l’intervenant nous a présenté une solution alternative, avec Linux et le projet RooAsRole.

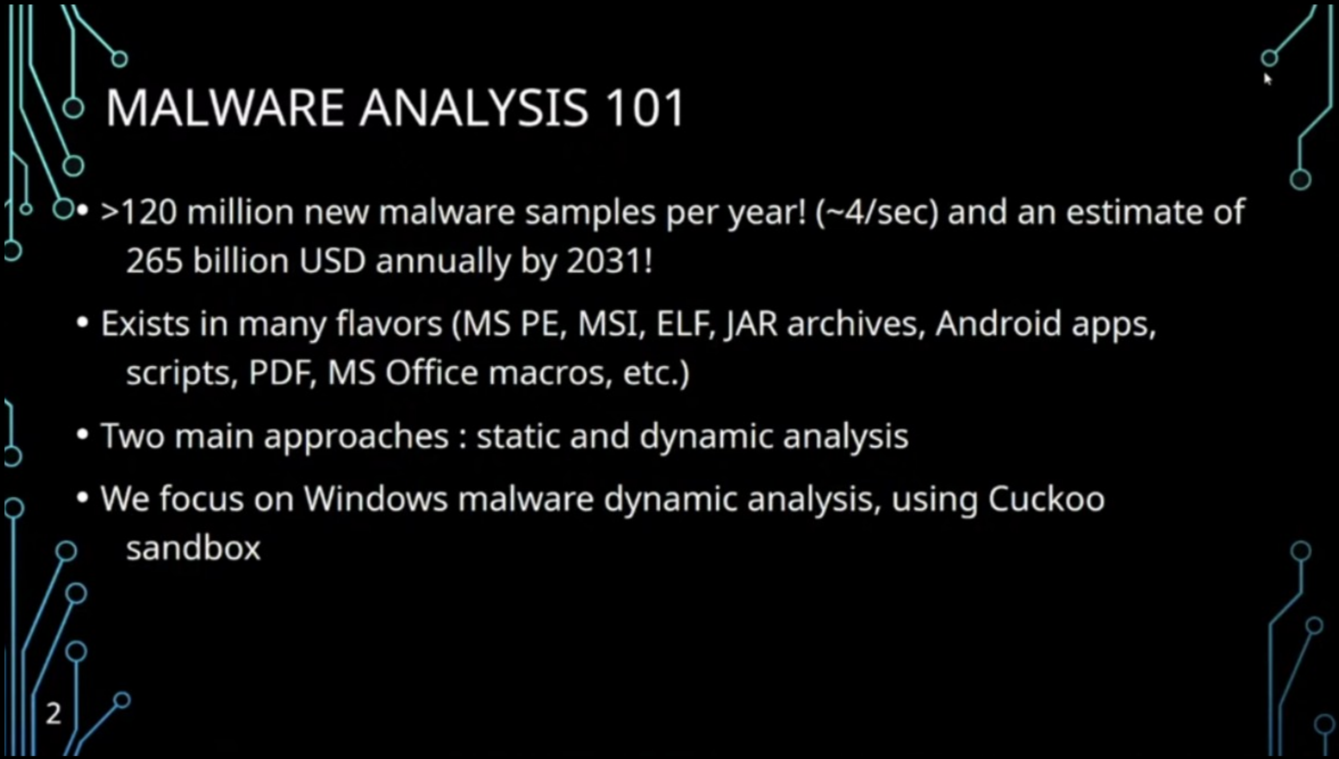
OS administratives privileges



RootAsRole (V3.0.0-alpha.3) : a secure alternative to sudo/su on Linux systems

- Gestion sécure des accès
- Alternative à sudo avec du « least privileges »
- Modèle RBAC
- Les privileges sont réduits pour chaque tache
- Prévient les « privileges escalation »

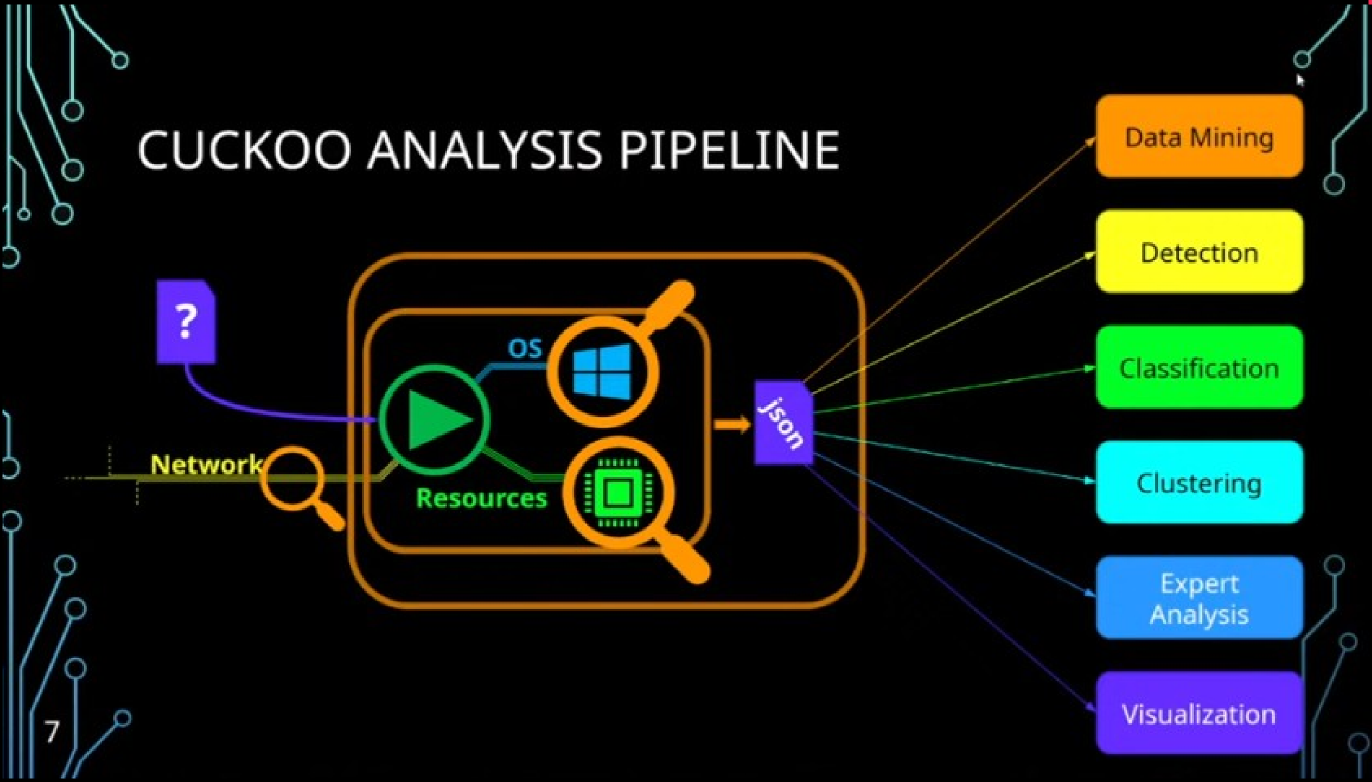
BAGUETTE: Hunting for Evidence of Malicious Behavior
by Pierre-François Gimenez - INRIA Rennes



MALWARE ANALYSIS 101

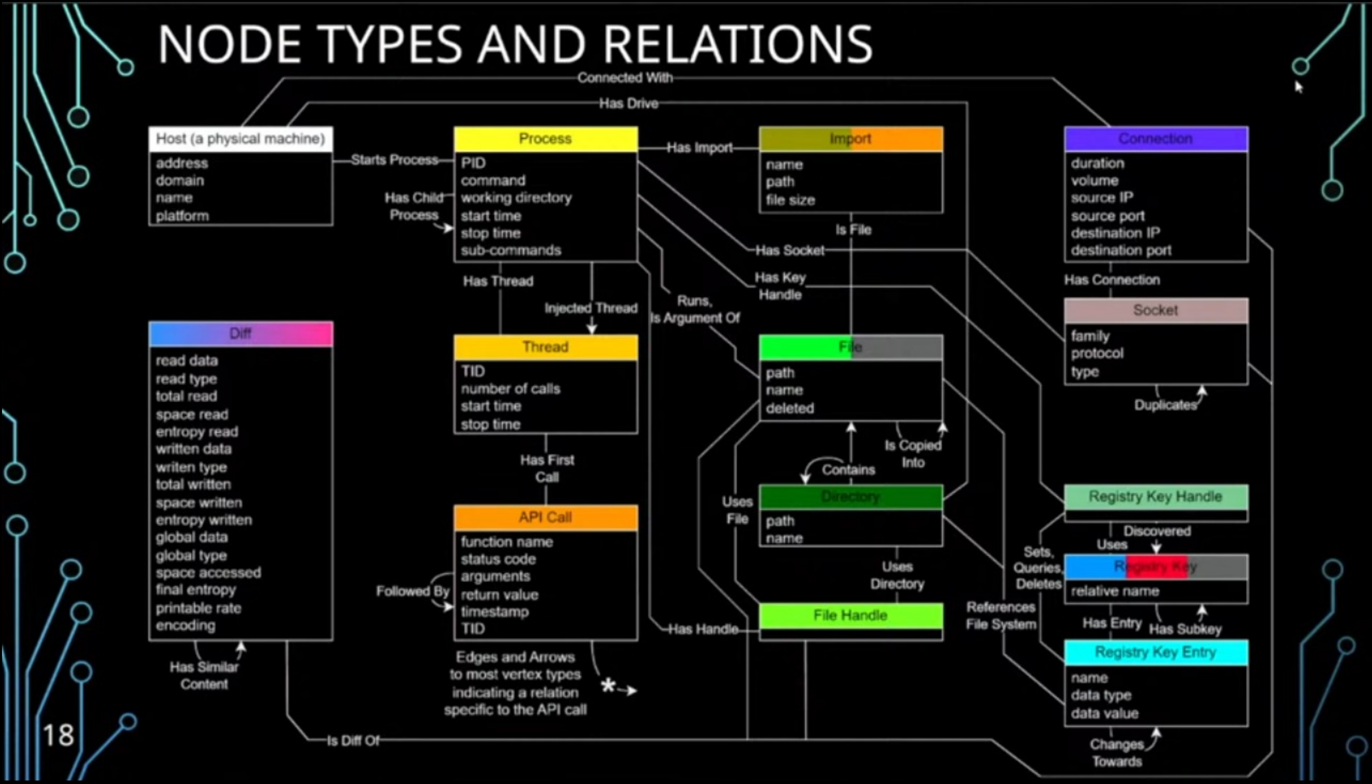
- >120 million new malware samples per year! (~4/sec) and an estimate of 265 billion USD annually by 2031!
- Exists in many flavors (MS PE, MSI, ELF, JAR archives, Android apps, scripts, PDF, MS Office macros, etc.)
- Two main approaches : static and dynamic analysis
- We focus on Windows malware dynamic analysis, using Cuckoo sandbox

BAGUETTE: Hunting for Evidence of Malicious Behavior
by Pierre-François Gimenez - INRIA Rennes



CUCKOO ANALYSIS PIPELINE

BAGUETTE: Hunting for Evidence of Malicious Behavior by Pierre-François Gimenez - INRIA Rennes



NODE TYPES AND RELATIONS

Host (a physical machine)
- address
- domain
- name
- platform

Process
- PID
- command
- working directory
- start time
- stop time
- sub-commands

Import
- name
- path
- file size

Connection
- duration
- volume
- source IP
- source port
- destination IP
- destination port

Socket
- family
- protocol
- type

Diff
- read data
- read type
- total read
- space read
- entropy read
- written data
- writen type
- total written
- space written
- entropy written
- global data
- global type
- space accessed
- final entropy
- printable rate
- encoding

Thread
- TID
- number of calls
- start time
- stop time

File
- path
- name
- deleted

Directory
- path
- name

API Call
- function name
- status code
- arguments
- return value
- timestamp
- TID

File Handle

Registry Key Handle

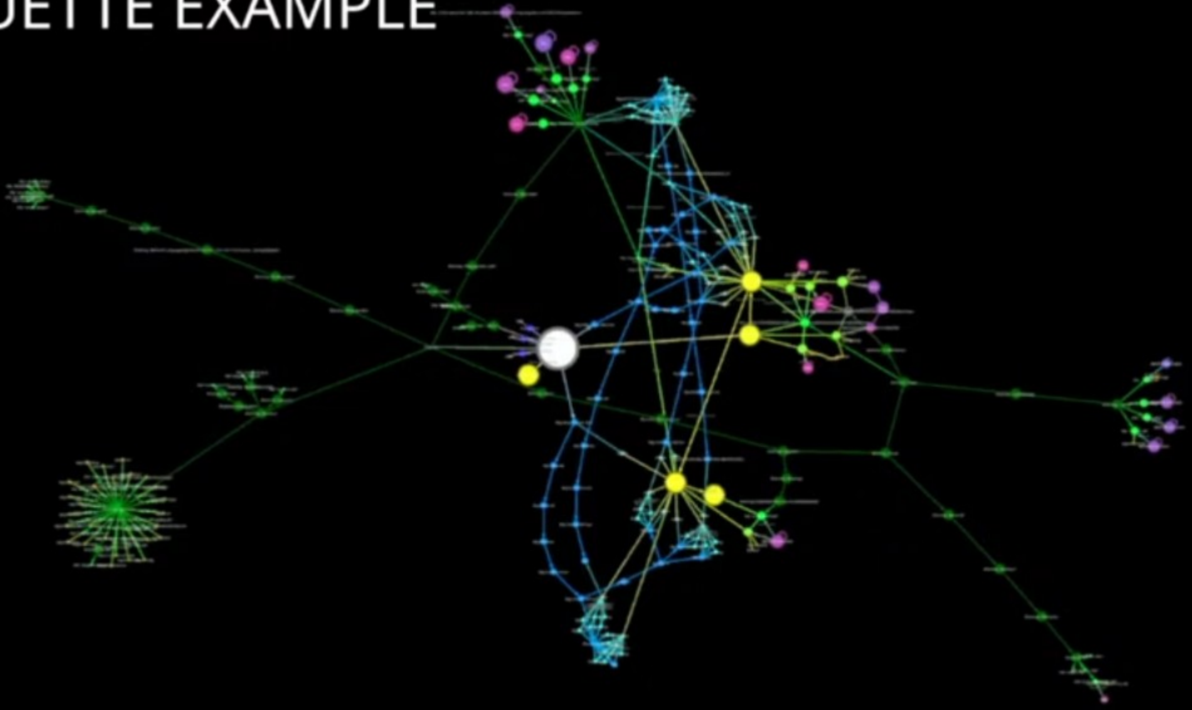
Registry Key
- relative name

Registry Key Entry
- name
- data type
- data value

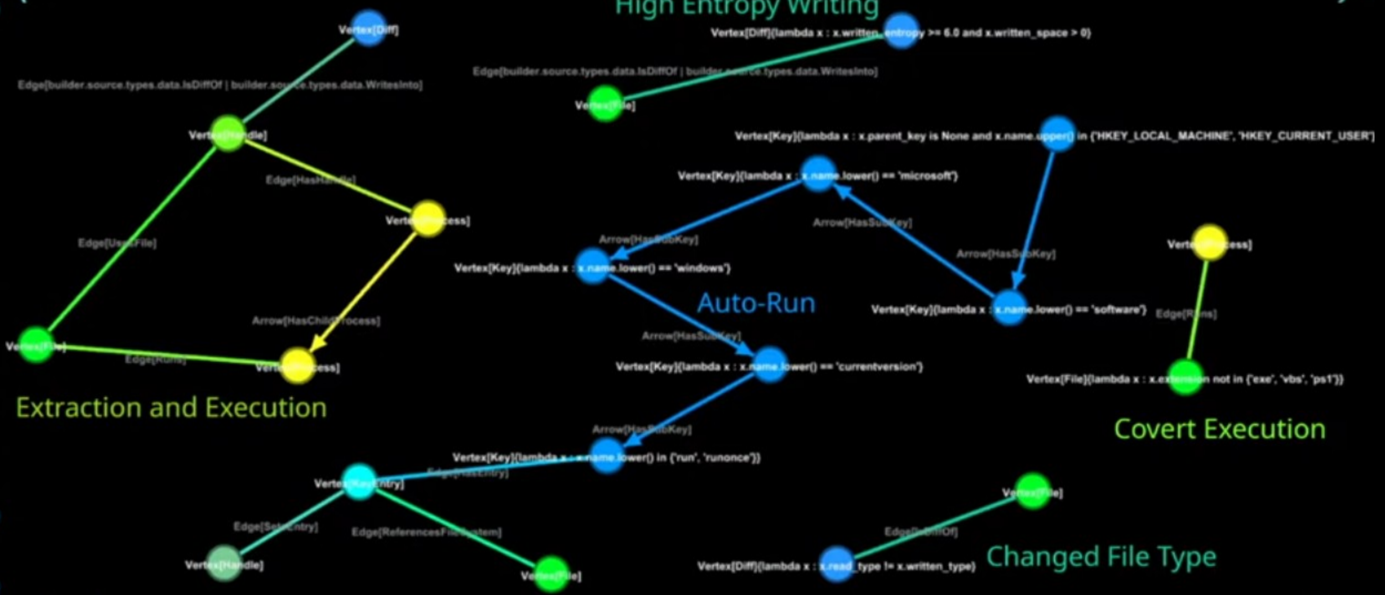
Edges and Arrows to most vertex types indicating a relation specific to the API call *→

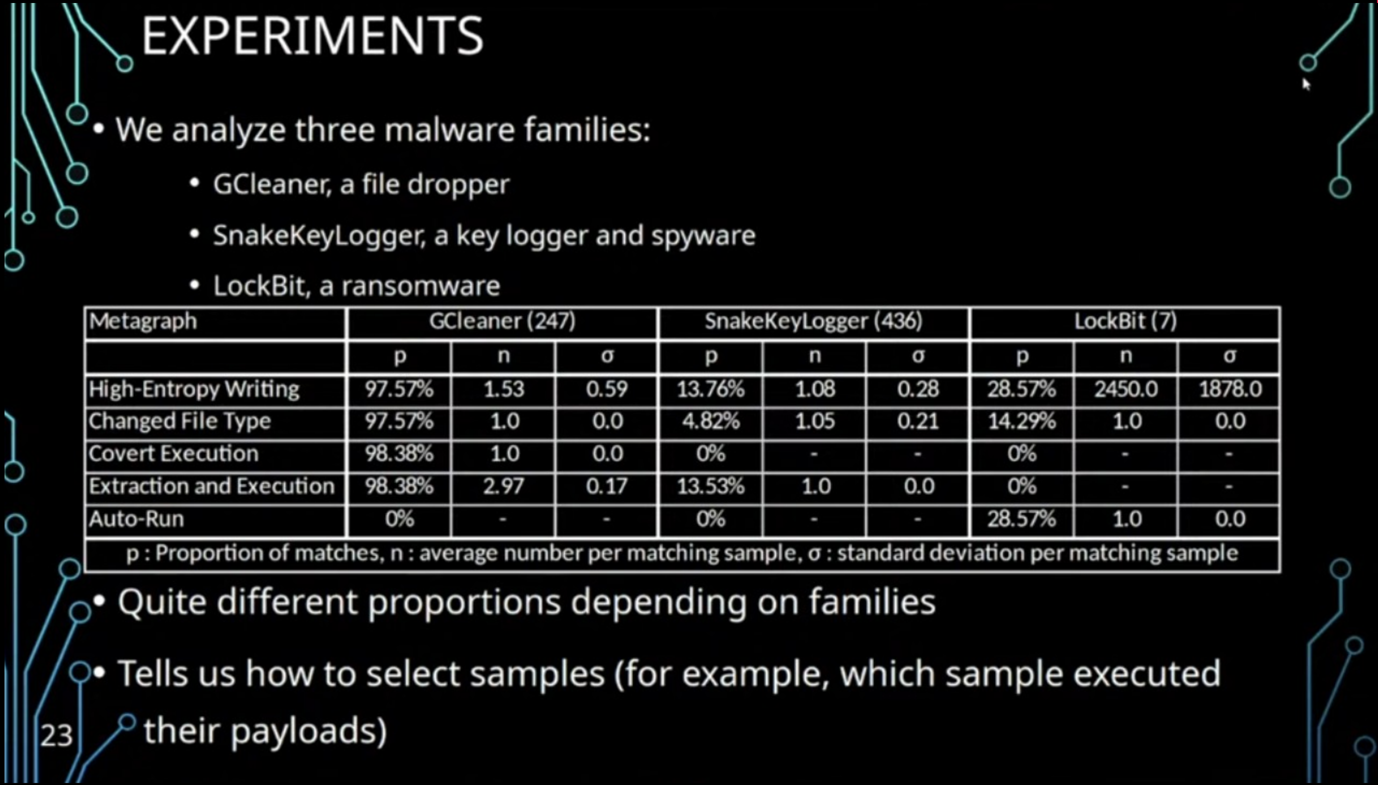
BAGUETTE: Hunting for Evidence of Malicious Behavior
by Pierre-François Gimenez - INRIA Rennes

BAGUETTE EXAMPLE



METAGRAPH EXAMPLES


High Entropy Writing
Vertex[Diff](lambda x : x.written_entropy >= 6.0 and x.written_space > 0)
Edge[builder.source.types.data.IsDiffOf | builder.source.types.data.WritesInto]
Vertex[File]
Vertex[Diff]
Edge[builder.source.types.data.IsDiffOf | builder.source.types.data.WritesInto]
Vertex[Handle]
Edge[HasHandle]
Vertex[Process]
Edge[UsesFile]
Arrow[HasChildProcess]
Vertex[File]
Edge[Runs]
Vertex[Process]
Extraction and Execution
Vertex[Key](lambda x : x.parent_key is None and x.name.upper() in ('HKEY_LOCAL_MACHINE', 'HKEY_CURRENT_USER'))
Vertex[Key](lambda x : x.name.lower() == 'microsoft')
Arrow[HasSubKey]
Arrow[HasSubKey]
Arrow[HasSubKey]
Vertex[Key](lambda x : x.name.lower() == 'windows')
Auto-Run
Vertex[Key](lambda x : x.name.lower() == 'software')
Arrow[HasSubKey]
Vertex[Key](lambda x : x.name.lower() == 'currentversion')
Arrow[HasSubKey]
Vertex[Key](lambda x : x.name.lower() in ('run', 'runonce'))
Edge[HasEntry]
Vertex[KeyEntry]
Edge[SetsEntry]
Edge[ReferencesFileSystem]
Vertex[Handle]
Vertex[File]
Vertex[Process]
Edge[Runs]
Vertex[File](lambda x : x.extension not in ('exe', 'vbs', 'ps1'))
Covert Execution
Vertex[File]
Edge[IsDiffOf]
Vertex[Diff](lambda x : x.read_type != x.written_type)
Changed File Type



EXPERIMENTS

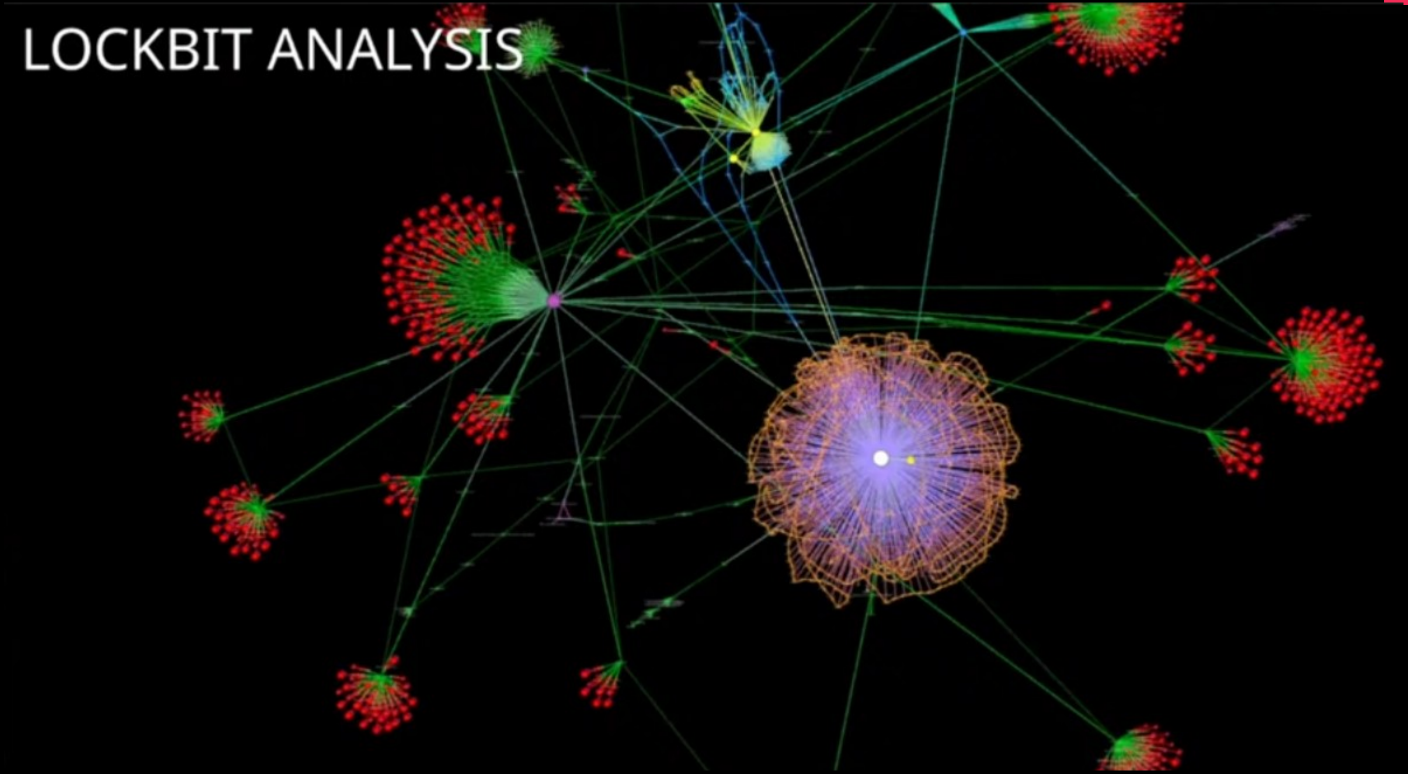
- We analyze three malware families:
  - GCleaner, a file dropper
  - SnakeKeyLogger, a key logger and spyware
  - LockBit, a ransomware

Metagraph	GCleaner (247)			SnakeKeyLogger (436)			LockBit (7)		
	p	n	σ	p	n	σ	p	n	σ
High-Entropy Writing	97.57%	1.53	0.59	13.76%	1.08	0.28	28.57%	2450.0	1878.0
Changed File Type	97.57%	1.0	0.0	4.82%	1.05	0.21	14.29%	1.0	0.0
Covert Execution	98.38%	1.0	0.0	0%	-	-	0%	-	-
Extraction and Execution	98.38%	2.97	0.17	13.53%	1.0	0.0	0%	-	-
Auto-Run	0%	-	-	0%	-	-	28.57%	1.0	0.0

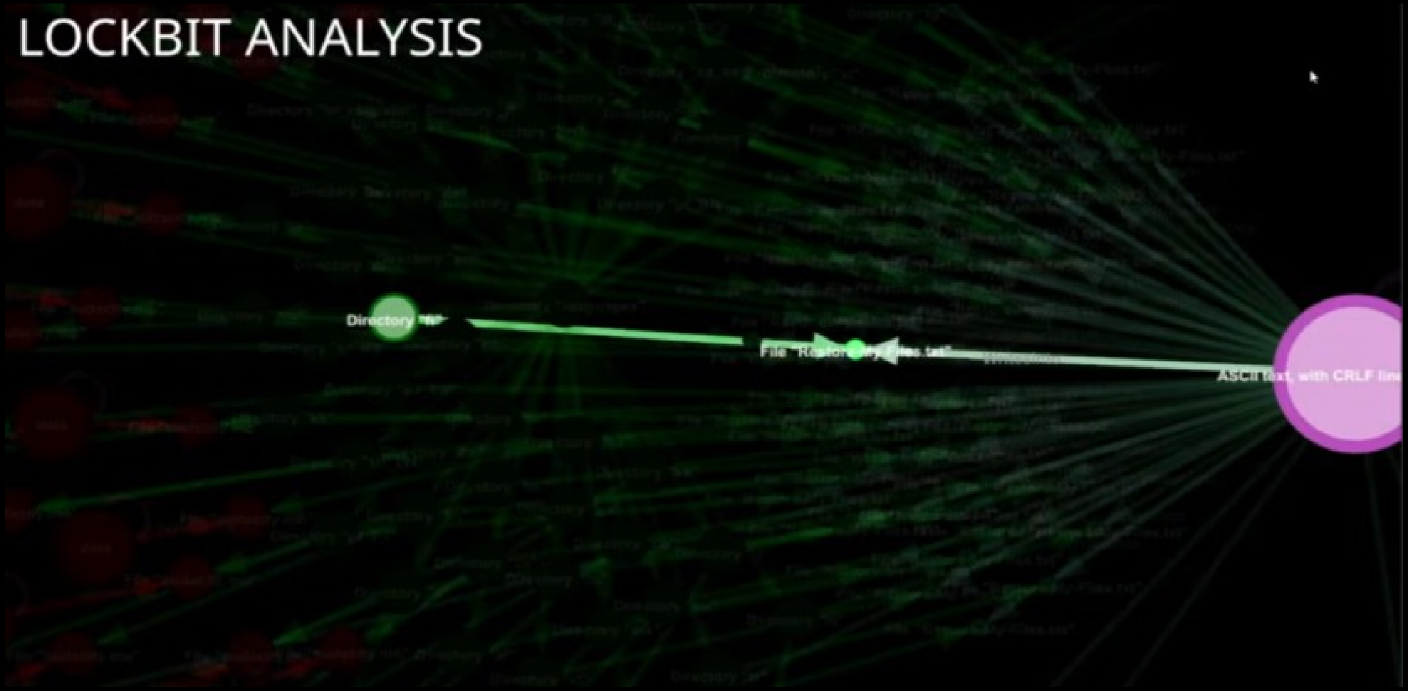
p : Proportion of matches, n : average number per matching sample, σ : standard deviation per matching sample

- Quite different proportions depending on families
- Tells us how to select samples (for example, which sample executed their payloads)

BAGUETTE: Hunting for Evidence of Malicious Behavior
by Pierre-François Gimenez - INRIA Rennes


LOCKBIT ANALYSIS

BAGUETTE: Hunting for Evidence of Malicious Behavior
by Pierre-François Gimenez - INRIA Rennes



Conclusion

Points positifs :

- Permet de rencontrer des passionnés et pros du domaine
- Des intervenants de qualité
- Accessibilité

Points négatifs :

- L’organisation était moyenne (peu de capacité d’accueil)
- Certaines conférences peu claires (issues de la recherche)
- Qualité des conférences disparates

Ressources complémentaires

Baguette :

https://hal.science/hal-04102144/file/SECRYPT_2023%20%284%29.pdf

RootAsRole :

https://github.com/LeChatP/RootAsRole

Replay conférences :

https://www.youtube.com/@THCon/streams