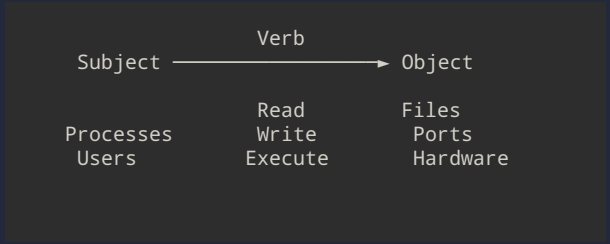
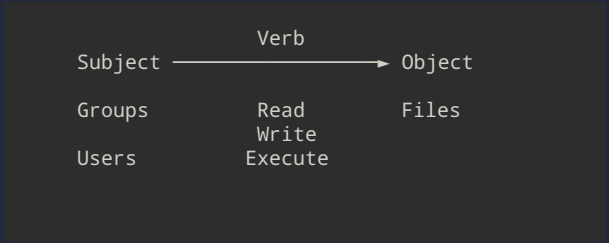
Intro to Landlock LSM

Nihaal (https://nihaal.me)


Verb
Subject
Object
Read
Write
Execute
Processes
Users
Files
Ports
Hardware

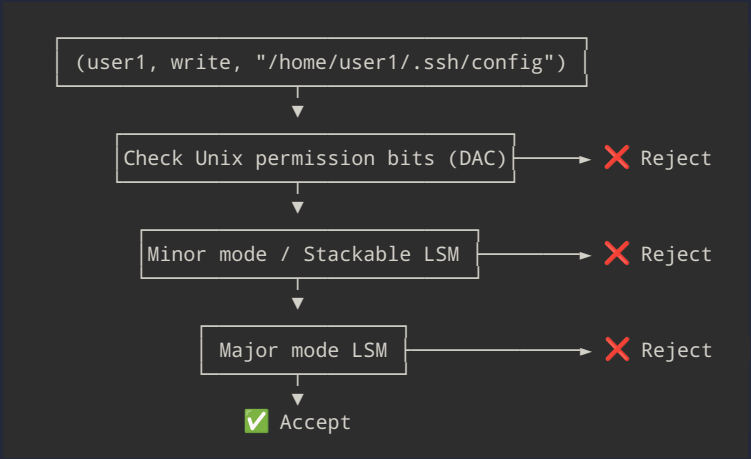
Unix Permissions




```
.rwxrwxr-x  16k nihaal 13 Feb 16:12 a.out
.rw-rw-r-- 1.6k nihaal 13 Feb 19:54 recat.c
.rw-rw-r--  11k nihaal 13 Feb 15:53 sandboxer.c
.rw-rw-r-- 3.5k nihaal 13 Feb 19:56 Session.vim
```

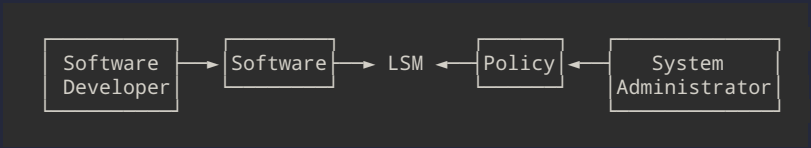
▒▒ Linux Security Module

- Adds additional checks to enforce stricter security policies
- Hooks in the kernel code before accessing objects
- Major vs Minor/Stackable modes



Popular LSMs

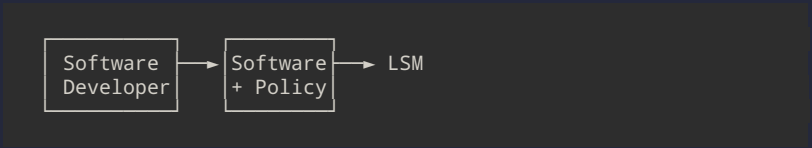
- SELinux : Based on Attributes to enable fine grained access control
- AppArmor : Based on Task profiles and Path based restrictions



- Policy issues
  - Restrictive policy ==> Application won't function
  - Relaxed policy ==> May not guarentee security
  - How to find out the exact (file/network) resources an application needs?

Landlock LSM

- Stackable (minor) LSM
- Allows applications to specify policy to be enforced



- Developed by Mickael Salaun & other FOSS contributors
- Since Linux 5.13
- Principles
  - Unprivileged: Works without superuser permission
  - Dynamic policy composition
    - Can keep on restriciting access for different threads
    - One-way: Restrictions cannot be undoed
    - Child threads inherit restrictions
  - Deny-by-default

▒▒ Landlock LSM

- Applications
  - Build sandboxes (eg: island)
  - Add security guardrails to your application
- Resources that can be restricted
  - Filesystems
  - Networking Connect/Bind to TCP ports
  - Sockets, Signals
- Implemented using 3 system calls
  - `landlock_create_ruleset`
  - `landlock_add_rule`
  - `landlock_restrict_self`

References

- Landlock website (https://landlock.io)
- Documentation (https://docs.kernel.org/security/landlock.html)
- Landlock has library bindings for Rust, Go, Python

Thank you ! Questions ?