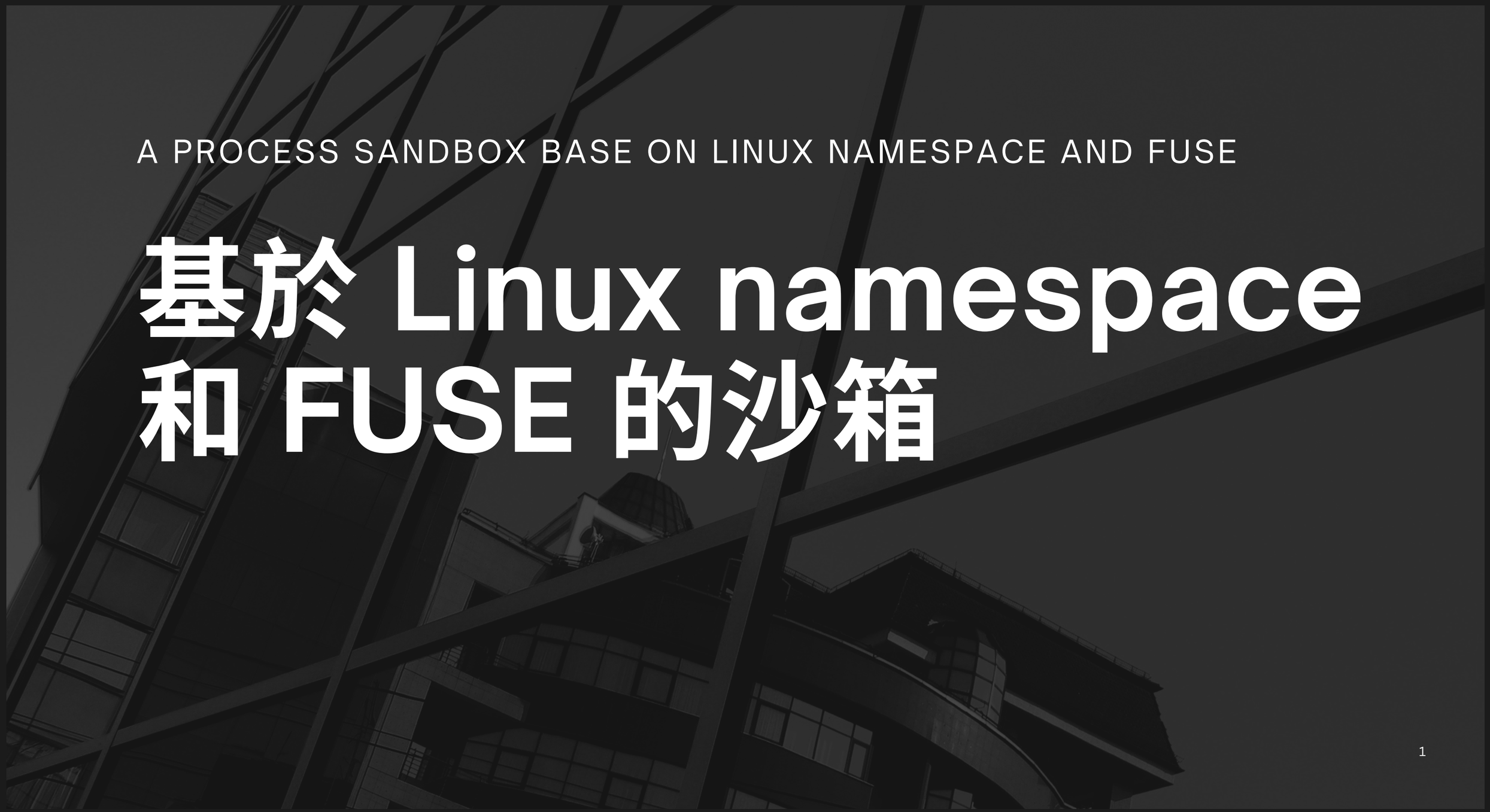


A PROCESS SANDBOX BASE ON LINUX NAMESPACE AND FUSE

基於 Linux namespace 和 FUSE 的沙箱

海報不是 AI 直接生的

用繪圖軟體(Krita)

動機

有了 AI 後，寫的程式有點多
現有的方案都要妥協

方案	缺點
run in docker	opencode 有 bug(#14194)
devcontainer	需要維護額外環境
opencode內建機制	只防止 agent 跑 bash command 時直接存取外部檔案

用到的技術

1

LINUX 命名空間

Abstraction that each namespace own resource.

2

SECCOMP BPF

Set secure computing mode with BPF

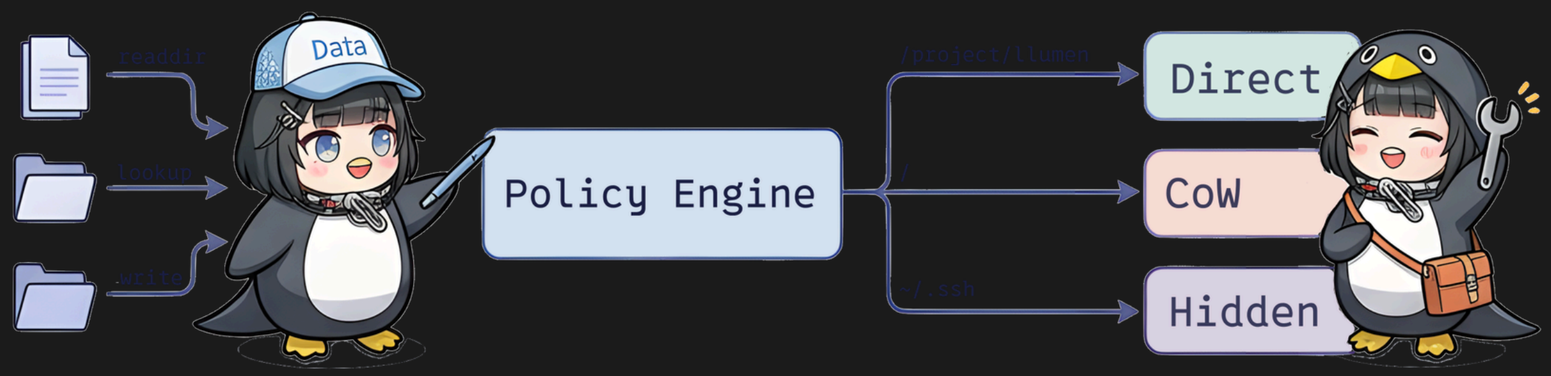
3

FILESYSTEM IN USERSPACE

Run custom filesystem with lower risk

assets/policy.rhai

```
fn decide(path) {
    let sandbox = pwd() + "/.sandbox";
    if path == sandbox || path.starts_with(sandbox + "/") {
        return #{ access: "fuse_only", recursive: true };
    }
    if path.starts_with(pwd()) {
        return #{ access: "passthrough", recursive: true };
    }
    #{}
}
```



檔案系統

用程式化的設定提供檔案系統的權限

記住沙箱內部的變更，僅內部看的到

Direct: 例如專案資料夾
CoW: 外部工具安裝位置(例如 gcc)
Hidden: 放 key 的地方，對 AI 不可見

Demo