CLOUDFLARE

Island: Seamless integration of sandboxing

SSTIC

Mickaël Salaün - Kernel Maintainer

2026-06-05

Island: Demo

Island

Goal:

- Protect users' data access from buggy, malicious, or exploited software by restricting most commands
- Available to everyone using a terminal
- Avoid cognitive load (once configured)

Interesting features:

- Fully unprivileged
- Shell integration
- Flexible configuration

CLOUDFLARE

What about other sandboxers?

	Cross-distro	Fine-grained Control and Logs	Natively Unprivileged	User-controlled	Shell Integration
Docker / Podman	✓	✗	✗	✓	✗
Bubblewrap / Firejail	✓	✗	✗	✓	✗
Flatpak	✓	✗	✗	✗	✗
Snap	✗	✓	✗	✗	✗
Island	✓	✓	✓	✓	✓

Island’s Properties

- Runs existing binaries without modification
- Flexible policies
- Context-aware activation
- Dedicated environments per sandbox: isolated workspaces (XDG directories, TMPDIR)

Island’s Current Limitations

- Work-in-progress
- No full isolation yet: ongoing work to fill the gaps
- Feedback welcome

Island's Configuration

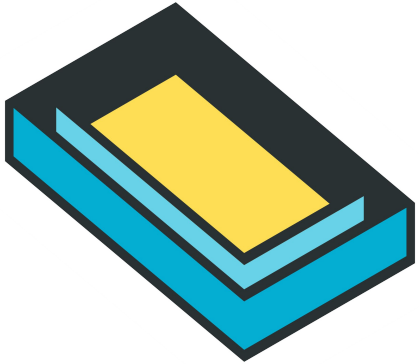
```
# Main system file hierarchies can be read and executed.
[[path_beneath]]
allowed_access = ["abi.read_execute"]
parent = ["/bin", "/lib", "/usr", "/dev", "/proc", "/etc", "/home/user/bin"]

# Only allow writing to some directories.
[[path_beneath]]
allowed_access = ["abi.read_write"]
parent = ["${myvariable}"]
```

Island’s Configuration Properties

- Ease sharing and maintaining security policies
- Declarative, deterministic, idempotent
- Composable: cleanly “merge” a set of standalone files
- Handle variables and compose them commutatively:
  - Variables are a set of values
  - Must be defined when using it, but can be empty

Island leverages Landlock



- Integrated in the Linux kernel
- Complementary to seccomp but for access control:
  - Safe unprivileged sandboxing
  - Ephemeral and one-way restrictions
- Kernel semantic:
  - Filesystem operations control
  - TCP (and soon UDP) control
  - IPC isolation
- Observability interfaces: audit and soon tracepoints/eBPF

CLOUDFLARE

Thank you

Questions?

https://github.com/landlock-lsm/island