

Bubblewrap, jednoduše sandbox

Sandbox jednoduše?

LinuxDays 2025

Stanislav Lukeš

Bubblewrap?

- Zjednodušuje používání Linuxových namespaces
- Jeden příkaz (s hodně parametry 😊)
- Rootless

Bubblewrap?

- Zjednodušuje používání Linuxových namespaces
- Jeden příkaz (s hodně parametry 😊)
- Rootless
- Původ jako součást Flatpacku
- Dnes široce využívaný aplikacemi k izolaci komponent

Bubblewrap není sandbox

- Bubblewrap je nástroj na konstrukci sandboxu
... a bez parametrů má prázdný filesystem

- `# df`

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
tmpfs	31697892	1272	31696620	0%	/

Bubblewrap není sandbox

- Bubblewrap je nástroj na konstrukci sandboxu
... a bez parametrů má prázdný filesystem

- `# df`

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
tmpfs	31697892	1272	31696620	0%	/

Mount namespace

- Konfigurace kde jsou které soubory/adresáře
- Propojit složku z mého systému dovnitř kontejneru
 - `--bind /from /target`
- To samé, jen pro čtení
 - `--ro-bind /from /target`

Root filesystem

- Pouze pro čtení:
 - `/bin`, `/sbin`, `/usr`, `/lib`, `/lib64`, `/opt`, `/nix`
 - `/etc`
- Vyrobíme prázdné:
 - `/tmp`
 - `/run/user/$UID`, tedy `$XDG_RUNTIME_DIR`
 - `/home/$USER`
- `/proc` a `/dev` jsou speciální
- Ignorujeme:
 - `/boot`, `/mnt`, `/var`

Mount namespace

- Konfigurace kde jsou které soubory/adresáře
- `--bind /from /target`
- `--ro-bind /from /target`
- Nové speciální filesystemy:
 - `--proc /proc --dev /dev`
- Nové prázdné složky:
 - `--dir /tmp --dir $XDG_RUNTIME_DIR`

Další namespacey

- to co není soubor, například procesy
- `--unshare-all`
 - `--unshare-pid`: izoluje process tree
 - `--unshare-ipc`: izoluje POSIX message queue apod
 - `--unshare-uts`: izoluje hostname
 - `--hostname BWRAP`: poznám kde jsem!
 - `--unshare-net`: vyrobí izolovanou síť

Další namespacey

- to co není soubor, například procesy
- `--unshare-all`
 - `--unshare-pid`: izoluje process tree
 - `--unshare-ipc`: izoluje POSIX message queue apod
 - `--unshare-uts`: izoluje hostname
 - `--hostname BWRAP`: poznám kde jsem!
 - `--unshare-net`: vyrobí izolovanou síť
- `--share-net`
 - zruší izolaci sítě

Další namespacey

- to co není soubor, například procesy
- `--unshare-all`
 - `--unshare-pid`: izoluje process tree
 - `--unshare-ipc`: izoluje POSIX message queue apod
 - `--unshare-uts`: izoluje hostname
 - `--hostname BWRAP`: poznám kde jsem!
 - `--unshare-net`: vyrobí izolovanou síť
- `--share-net`
 - zruší izolaci sítě
- nemáme moc prostoru k další konfiguraci

--new-session

- `--new-session`
 - vyrobí virtuální tty, ochrana před ioctl TIOCSTI a TIOCLINUX
 - často ale rozbíjí CLI tooly

--new-session

- `--new-session`
 - vyrobí virtuální tty, ochrana před ioctl TIOCSTI a TIOCLINUX
 - často ale rozbíjí CLI tooly
 - nemělo by být nutné na Linuxu 6.7+, když

```
$ cat /proc/sys/dev/tty/legacy_tiocsti
0
```

--new-session

- `--new-session`
 - vyrobí virtuální tty, ochrana před ioctl TIOCSSTI a TIOCLINUX
 - často ale rozbíjí CLI tooly
 - nemělo by být nutné na Linuxu 6.7+, když

```
$ cat /proc/sys/dev/tty/legacy_tiocsti
0
```

- `--die-with-parent`
 - prevence zombie apokalypsy

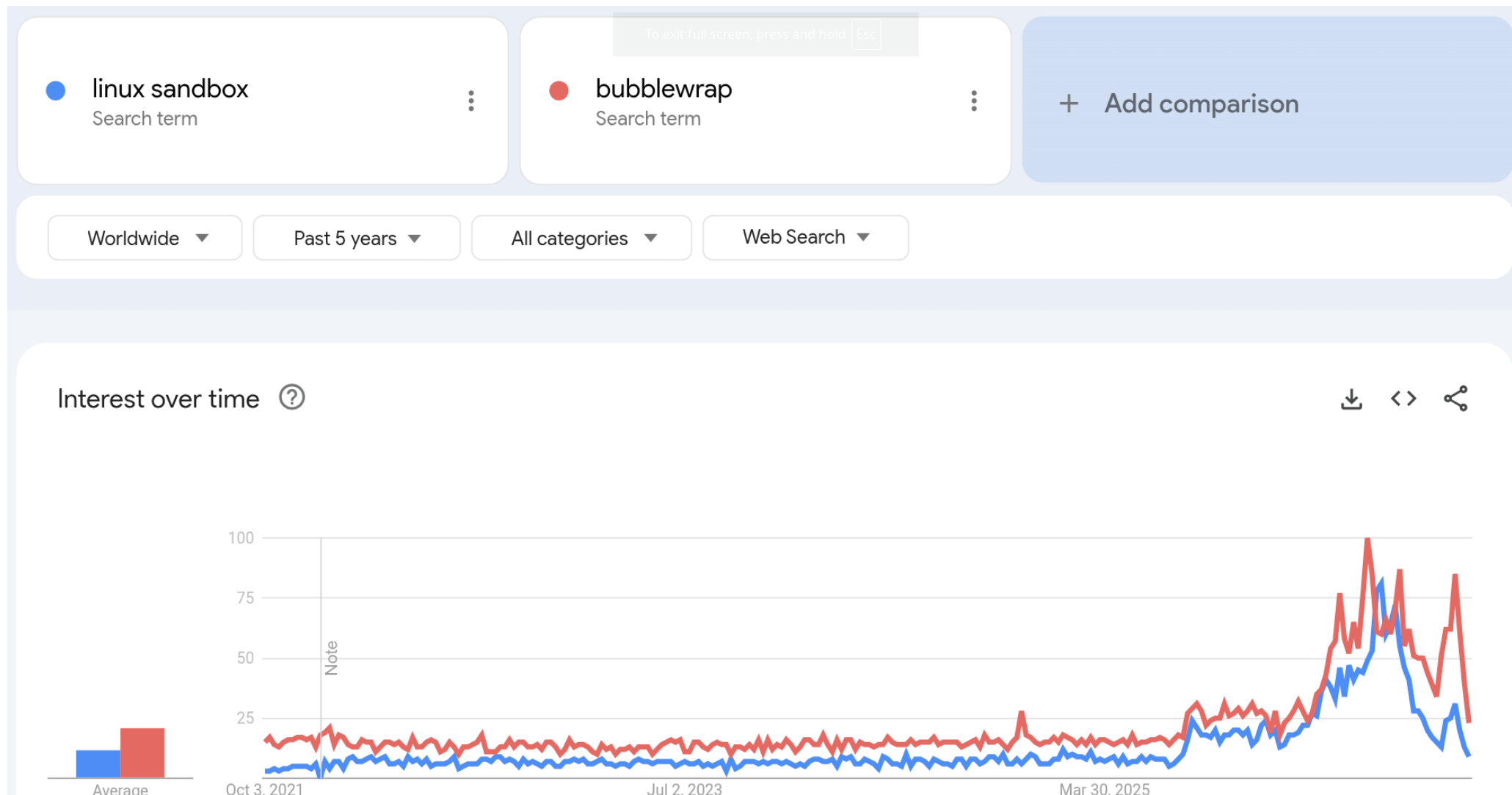
Příklad: LibreOffice v bubblewrapu

- Motivace: chceme v rámci webové aplikace konvertovat docx/odt na PDF
- LibreOffice umí `--convert-to pdf`

Příklad: LibreOffice v bubblewrapu

- Motivace: chceme v rámci webové aplikace konvertovat docx/odt na PDF
- LibreOffice umí `--convert-to pdf`
- ```
bwrap --unshare-all --new-session --die-with-parent \
 $rootdirs \
 --ro-bind ~/TextDocument.odt /tmp/doc.odt \
 --bind ~/output_dir /tmp/out \
 libreoffice --convert-to pdf \
 --outdir /tmp/out \
 /tmp/doc.odt
```

# Proč všechny najednou zajímá sandboxing?



# OpenCode

- [OpenCode #10939](#)
- Ale chceme přece vibekódit

auth login <url> should confirm before running well-known auth.command #10939

✓ Closed

Assignees



Labels

windows



MaxMiksa opened on Jan 28

Contributor



## Description

opencode auth login <url> fetches <url>/well-known/opencode and runs the returned auth.command immediately to obtain a token.

This executes a remote-provided command without an explicit confirmation step and without validating the payload shape.



github-actions

bot

on Mar 30 – with [GitHub Actions](#)

Contributor



To stay organized issues are automatically closed after 90 days of no activity. If the issue is still relevant please open a new one.



4



2



github-actions closed this as [completed](#) on Mar 30

# OpenCode

- `bwrap --unshare-all --die-with-parent $rootdirs \`  
`--share-net \`  
`--bind . /tmp/project \`  
`--chdir /tmp/project \`  
`/bin/opencode --standalone`

# Overlay

- Fake modifikovatelný adresář
  - `--overlay-src /from --overlay-tmp /target`
  - například (vidí konfiguraci, může jí měnit pro sebe)  
`--overlay-src ~/.config --overlay-tmp ~/.config`

# Overlay

- Fake modifikovatelný adresář
  - `--overlay-src /from --overlay-tmp /target`
  - například (vidí konfiguraci, může jí měnit pro sebe)  
`--overlay-src ~/.config --overlay-tmp ~/.config`
- Modifikace jsou jinde než zdrojáky
  - `--overlay-src /from`  
`--overlay ~/.changes ~/.workdir /target`

# OpenCode

- Změny udělané agentem jsou separátně v ~/my\_changes

- `mkdir ~/my_changes ~/workdir`

```
bwrap --unshare-all --die-with-parent ... \
 --share-net \
 --overlay-src . \
 --overlay ~/my_changes ~/workdir /tmp/project \
 --chdir . /tmp/project \
 /bin/opencode --standalone
```

# OpenCode

- Změny udělané agentem jsou separátně v ~/my\_changes
- ```
mkdir ~/my_changes ~/workdir
bwrap --unshare-all --die-with-parent ... \
      --share-net \
      --overlay-src . \
      --overlay ~/my_changes ~/workdir /tmp/project \
      --chdir . /tmp/project \
      /bin/opencode --standalone
```
- TODO:
 - chcete přidat ~/.config, část ~/.local s OpenCode autentifikací, atd
 - workflow jak pracovat se změněnými soubory

Cheatsheet

- **boilerplate:** `--unshare-all --die-with-parent [--new-session]`
- **povolit síť:** `--share-net`
- **pouze pro čtení:** `--ro-bind /from /target`
- **i pro zápis:** `--bind /from /target`
- **overlay fake zápis:** `--overlay-src /from --tmp-overlay /target`
- **prázdný temp:** `--tmpfs /target`
- **reset proměnných:** `--clearenv --setenv PATH /bin ...`
- **working directory:** `--chdir /`

Zdroje / kam dál?

- **Dokumentace dostupných parametrů:**

man bwrap, <https://github.com/containers/bubblewrap>

- **Další (komplikovanější) příklady:**

Arch Wiki: <https://wiki.archlinux.org/title/Bubblewrap>

plus examples: <https://wiki.archlinux.org/title/Bubblewrap/Examples>

- **Další speciality**

Julia Evans: Notes on running containers with bubblewrap

<https://jvns.ca/blog/2022/06/28/some-notes-on-bubblewrap/>

- **Včerejší přednáška Michala Vyskočila:**

[Moderní izolace procesů v Linuxu: namespaces, seccomp a další](#)