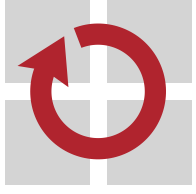
Dateisystemsandboxing

Zugriffskontrolle für Verzeichnisse mit stapelbaren Dateisystemen

March 13, 2020

Ole Wiedemann, Sebastian Scherbel

Friedrich-Alexander-Universität Erlangen-Nürnberg



Lehrstuhl für Verteilte Systeme
und Betriebssysteme

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

TECHNISCHE FAKULTÄT

Sandboxing (recap)

Overlayfs (recap)

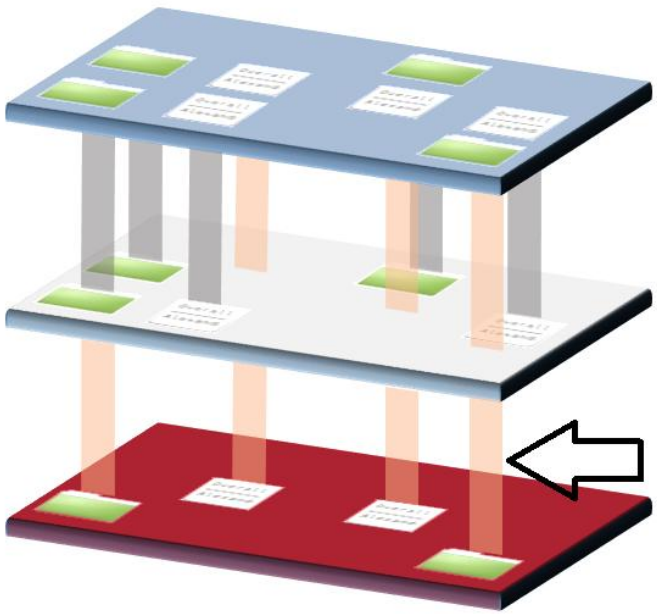
Overlay

=

Upper
changes

+

Lower
read only



LSM hook
allowed?!

Ziele

funktionale Anforderungen

- Regeln dynamisch anpassbar (x)
- feingranular (x)
- Black- und Whitelisting (x)
- nutzbar von unpriviligieren Nutzern (x)
- optionale GUI (x)

nicht funktionale Anforderungen

- sicher (x)
- performanter als bestehende Lösungen (x)
- wartbar (x)

erfüllt, mit kleineren Einschränkungen, nicht erfüllt

Architektur

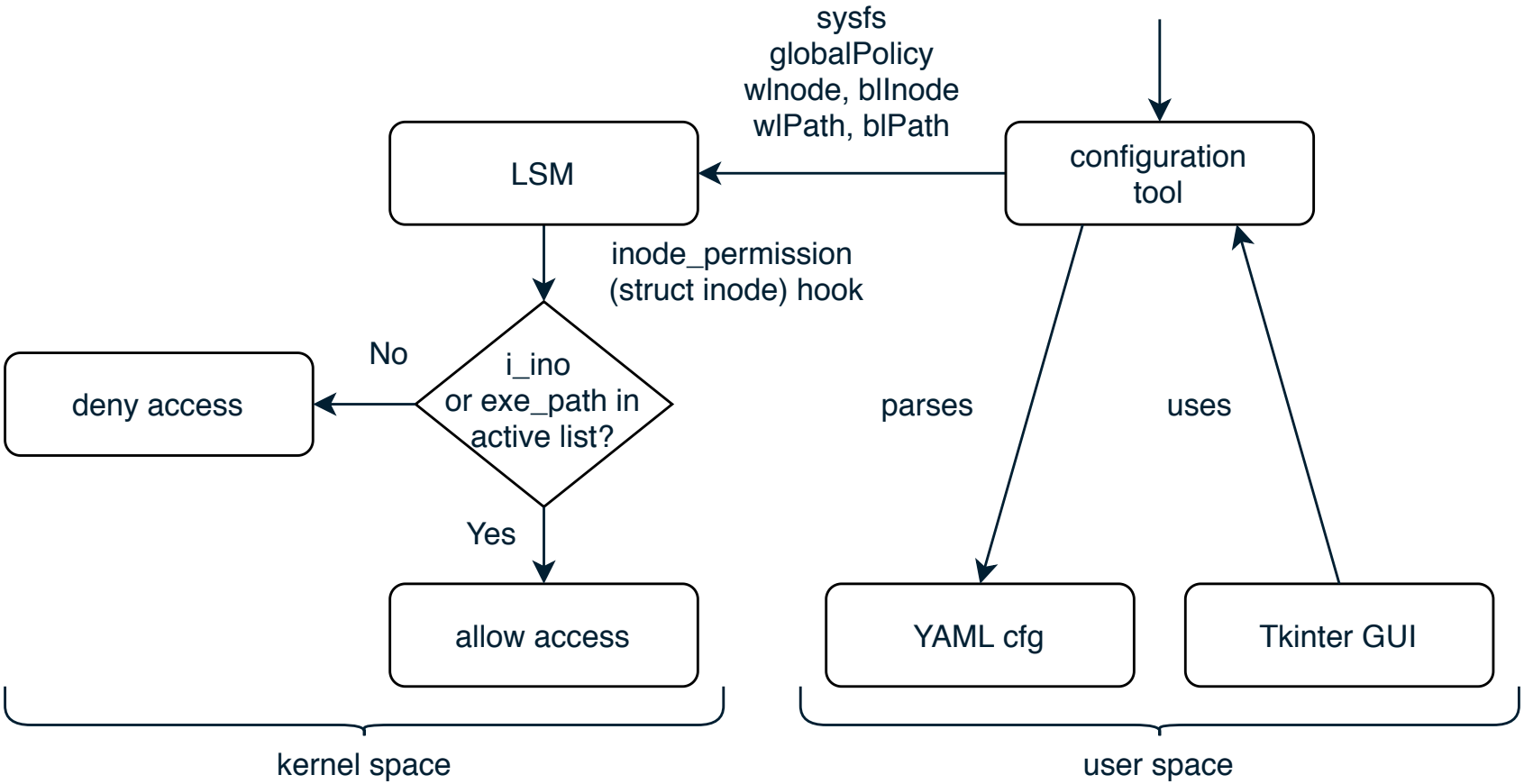
Modul (C)

- Linux Security Modul (LSM)
- nutzt inode_permission hook

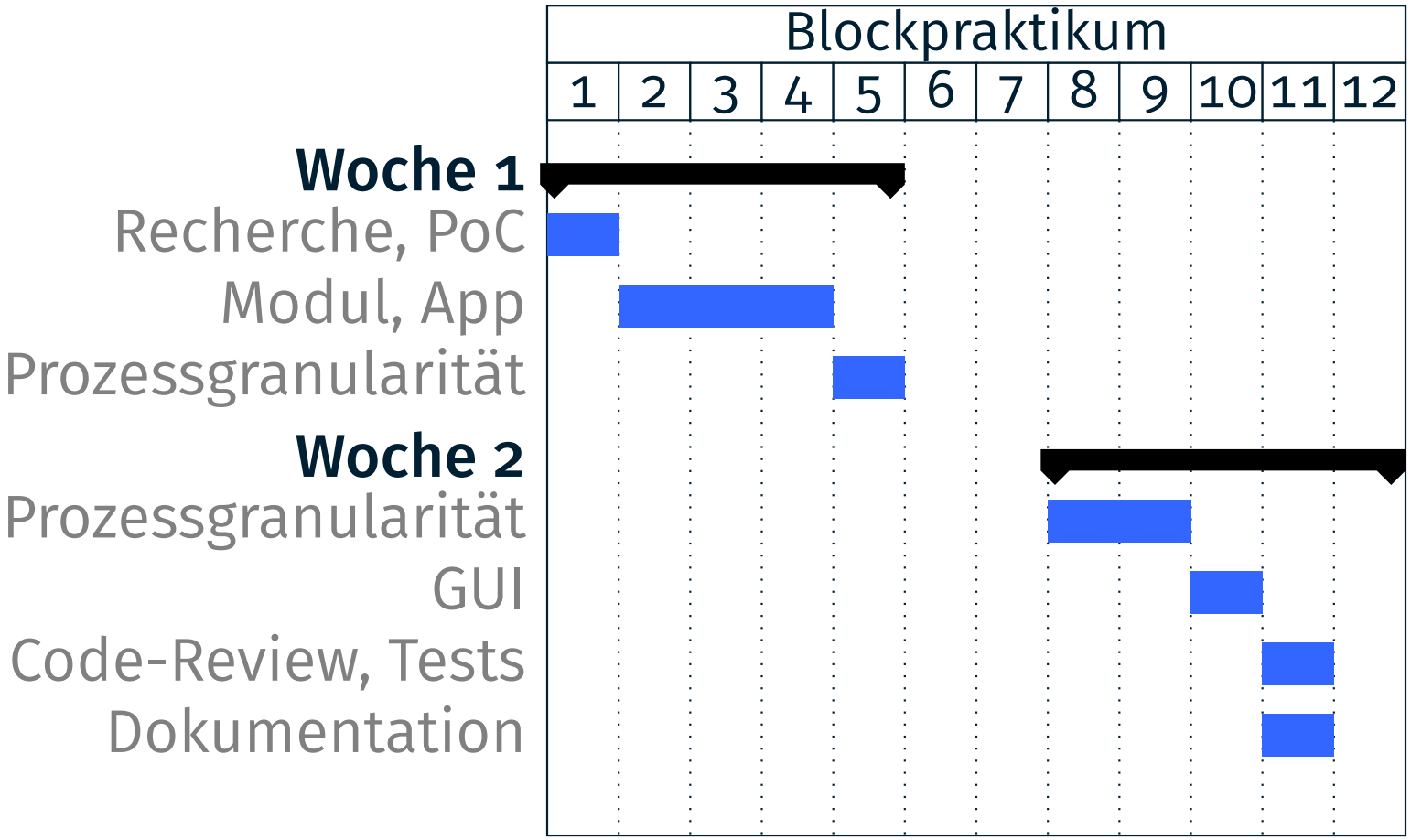
Applikation (Python, Shellscript zum Mounten)

- parst YAML-Konfiguration
- bedienbar über Kommandozeile oder Tkinter-GUI
- kommuniziert mit Modul über sysfs

Architektur



Ablauf


Blockpraktikum
1
2
3
4
5
6
7
8
9
10
11
12
Woche 1
Recherche, PoC
Modul, App
Prozessgranularität
Woche 2
Prozessgranularität
GUI
Code-Review, Tests
Dokumentation

Schwierigkeit: LSM

kein dynamischer Modulsupport mehr

- es existieren mehrere Patchsets
- Änderungen minimal gehalten

frühe Intitialisierung

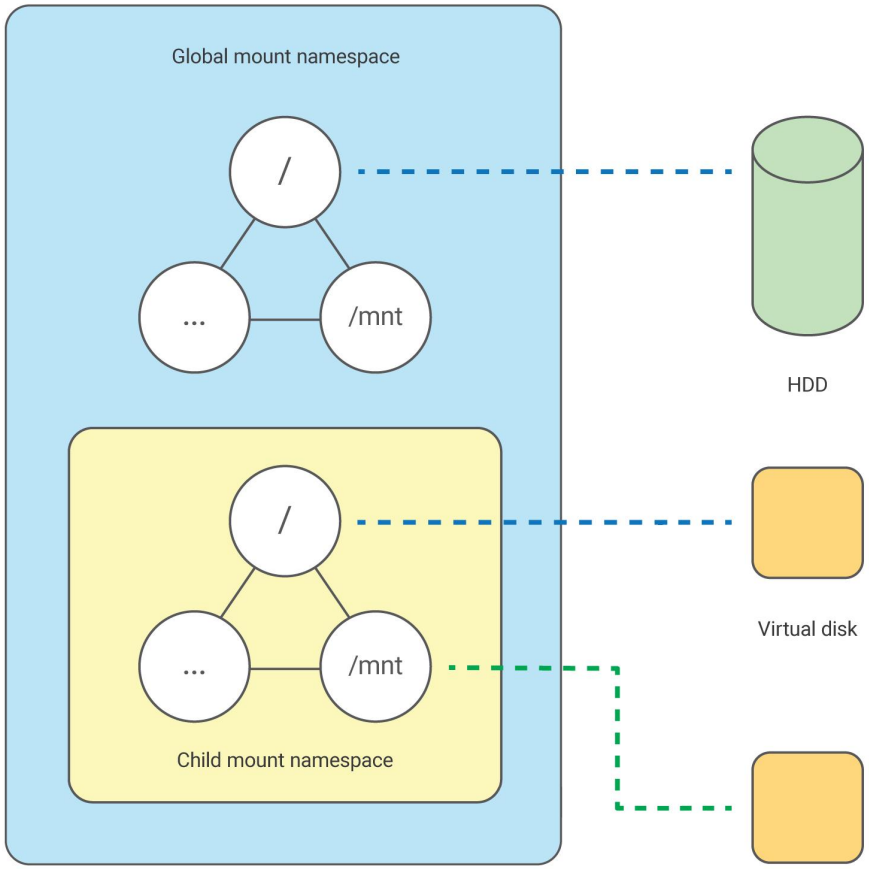
- sysfs existiert noch nicht
- Einträge werden erst beim ersten hook angelegt

Schwierigkeit: Prozessgranularität

Overlay soll nur von einem Prozess gesehen werden

- erzeugen eines eigenen namespaces
- mounten als root
- droppen von Privilegien
- starten einer gesandboxten Shell

Namespaces


Global mount namespace
/
...
/mnt
HDD
/
...
/mnt
Child mount namespace
Virtual disk

Fragen

Abbildungen (1)

- Sevantio.
  File:malicious-software-application-code-development-600w-363729896.jpg, 2016.

  [Online; accessed 13-March-2020].
- Datalight Thom Denholm.
  File:overlayfsimage.png with own modifications, 2016.
  [Online; accessed 13-March-2020].

Abbildungen (2)

Selectel Andrej Yemelianov.
File:pr-3854-2.png with own modifications, 2017.
[Online; accessed 13-March-2020].