

Automatic Seccomp Syscall Policy Generator

Marek Tamaskovic

Brno University of Technology, Faculty of Information Technology
Božetěchova 1/2, 602 00 Brno - Královo Pole
xtamas01@fit.vutbr.cz



August 22, 2018

- Ing. Lenka Turoňová
- Bc. Daniel Kopeček
- Cooperation with RedHat Inc.
- Motivation?



Input:

- `strace` log

Output:

- C\C++ code template
- `libseccomp`

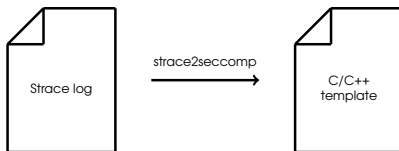


Figure: Transformation

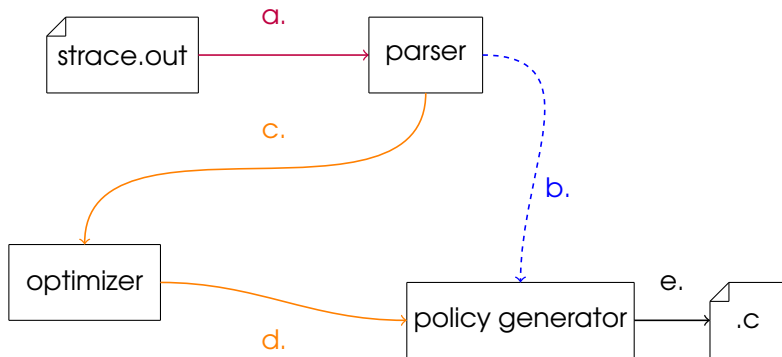


Figure: Pipe&Filter Architecture

- Three optimization levels
 - Strict:
 - 1:1
 - input \rightarrow output
 - MinMax:
 - allowed intervals
 - border values are extremes
 - DBSCAN¹:
 - implemented DBSCAN(1, 2)

¹Density-based spatial clustering of applications with noise

- Designed program architecture
- Implemented:
 - IDS²
 - 3 algorithms
- Created `testsuite`
- *"It is on good way to appear in production"*
- $\sim 2.8\text{K LOC}^3$ +

²Intermediate Data Structure

³Lines of Code



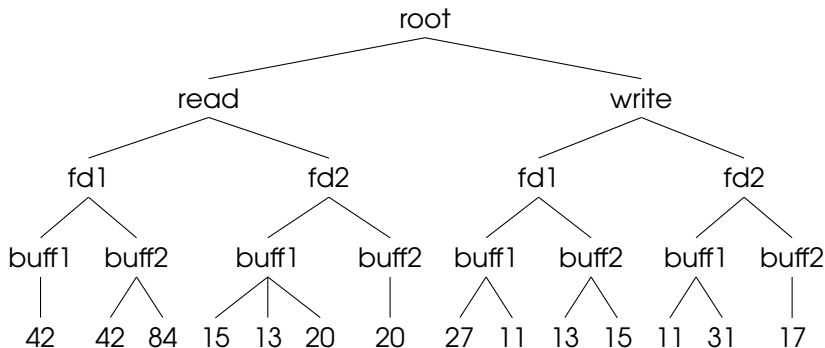
K. Mahesh Kumar and A. Rama Mohan Reddy. "A fast DBSCAN clustering algorithm by accelerating neighbor searching using Groups method". In: *Pattern Recognition* 58 (2016), pp. 39–48. ISSN: 0031-3203. DOI: [10.1016/j.patcog.2016.03.008](https://doi.org/10.1016/j.patcog.2016.03.008).



Erich Schubert et al. "DBSCAN Revisited, Revisited: Why and How You Should (Still) Use DBSCAN". In: *ACM Trans. Database Syst.* 42.3 (July 2017), 19:1–19:21. ISSN: 0362-5915. DOI: [10.1145/3068335](https://doi.org/10.1145/3068335). URL: <http://doi.acm.org.ezproxy.lib.vutbr.cz/10.1145/3068335>.

Any questions?

Název vašeho algoritmu je Minmax nebo Minimax? (V BP je toto nekonzistentní, i ve zdrojových kódech). Dokážete vysvětlit rozdíl oproti existujícímu algoritmu Minimax?



- Go support
- ASLR⁴ turned off
- Customizable template
- Packaging
- More algorithms

⁴Address Space Layout Randomization