LinuxTesting.org

Predicate Analysis with BLAST 2.7.3

Pavel Shved, Mikhail Mandrykin, and Vadim Mutilin

ISP RAS

Institute for System Programming of the Russian Academy of Sciences

BLAST 2.5

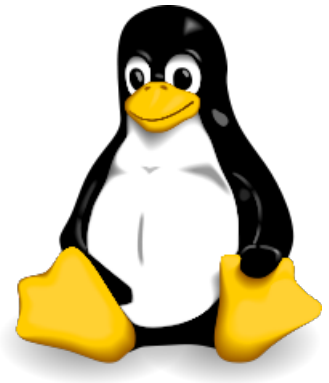
BLAST 2.7.3

ISP RAS

Berkeley
Lazy
Abstraction
Software
Verification
Tool

Linux Driver Verification Project Goals

- Provide infrastructure for application of verification tools to Linux device drivers
- Research new verification approaches in the industrial settings
- Improve quality of the Linux device drivers



New Benchmarks

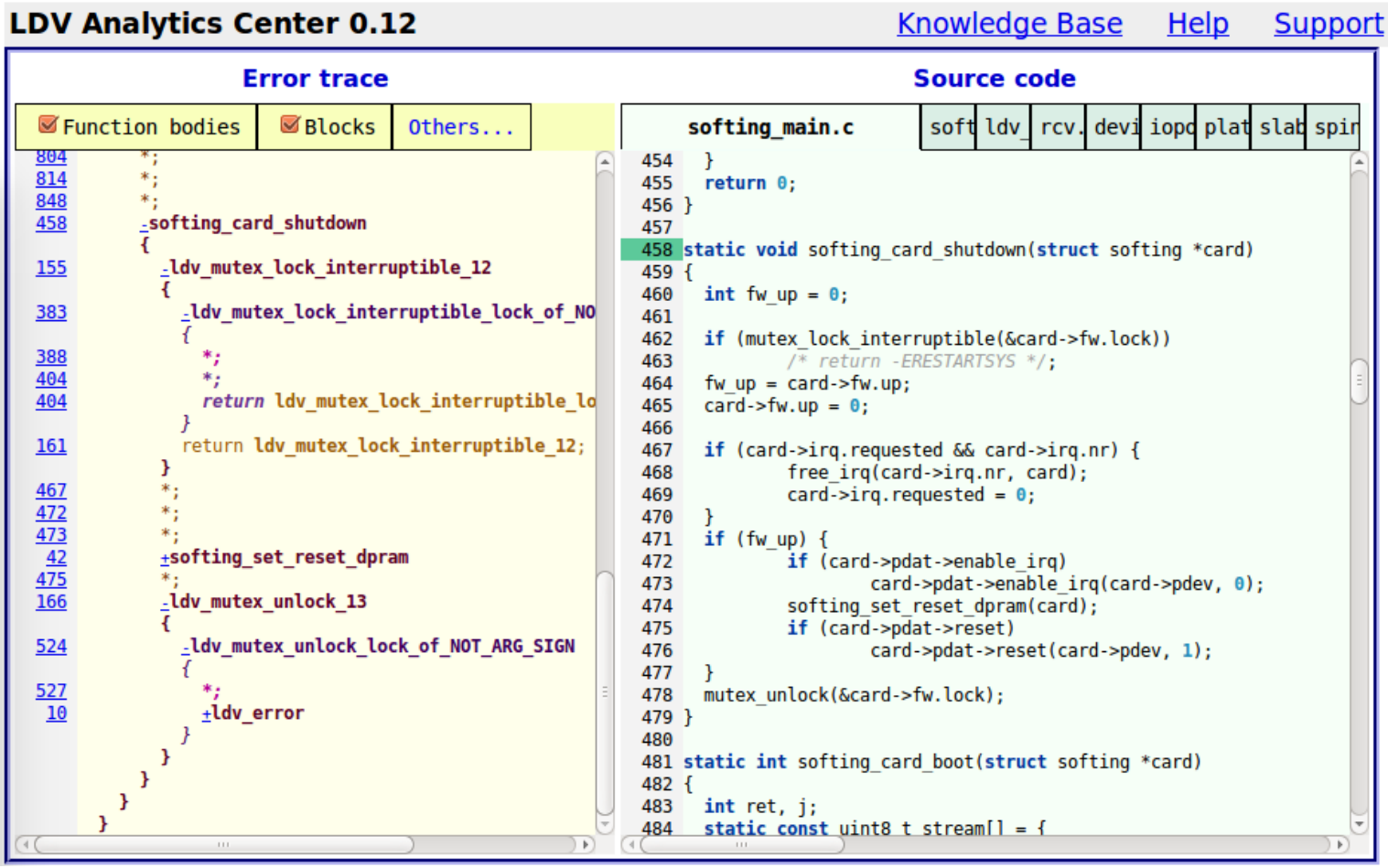
Based on Linux kernels 3.12 and 3.16

- Pointers
- Arrays
- Bitvectors
- Bugs found in Linux kernel

Results Excerpt for Arrays (DeviceDrivers64)

BLAST	CPAchecker	Seahorn
witness confirmed	unknown	out of memory
witness ignored (recursion)	unknown	witness ignored (recursion)
true	true	true
true	true	timeout
witness timeout	witness timeout	out of memory
true	true	true
true	true	timeout
true	true	timeout
true	true	timeout
out of memory	out of memory	timeout
exception (gremlins)	timeout	timeout
timeout	timeout	timeout
out of memory	timeout	timeout
exception (gremlins)	timeout	timeout
timeout	timeout	witness timeout
exception (gremlins)	unknown	witness confirmed
timeout	unknown	timeout
witness timeout	unknown	timeout
witness timeout	witness timeout	witness timeout
witness timeout	out of memory	timeout
exception (gremlins)	unknown	timeout
witness timeout	witness timeout	witness timeout
witness timeout	witness timeout	witness timeout
true	true	timeout

Seahorn Error Witness in LDV Error Trace Visualizer



Suggestions for Error Witnesses

- Better support for single path witnesses
- Cope with/extend timelimits for witness checking

LinuxTesting.org

Thank you!

Vadim Mutilin
mutilin@ispras.ru
http://linuxtesting.org/project/ldv

ISP RAS
Institute for System Programming of the Russian Academy of Sciences