LinuxTesting.org

Predicate Analysis with BLAST 2.7.2

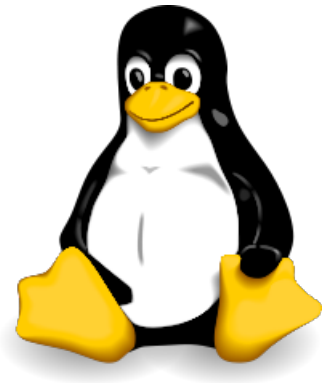
Pavel Shved, Mikhail Mandrykin, and Vadim Mutilin

ISP RAS

Institute for System Programming of the Russian Academy of Sciences

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



BLAST 2.5

Berkeley

Lazy

Abstraction

Software Verification

Tool

BLAST is a software model checker for C programs.

It uses counterexample-driven automatic abstraction refinement to construct an abstract model which is model checked for safety properties.

SV-COMP 2012 – BLAST 2.7

- General
- Program Representation
- Counter Example Analysis
- Refinement
- Pointer Analysis
- Configurable Program Analysis

SV-COMP 2013 – BLAST 2.7.1

SV-COMP 2014 – BLAST 2.7.2

- Bug fixes

- Goal of competing:
  To see how far the other tools improved

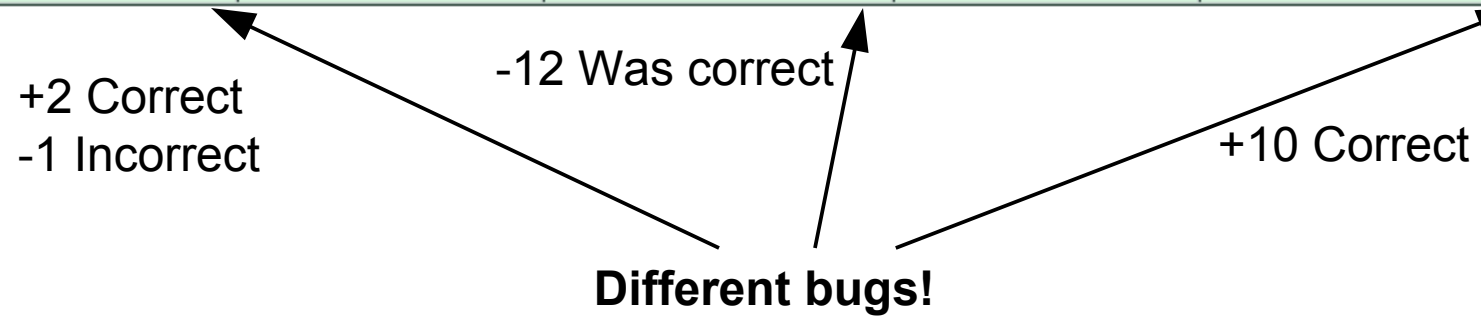
Verification of Linux-3.12-rc1 Device Drivers

Task	Total	Safe	Unsafe	Unknown	Time	Time Ok	Time Fail
Task description **BLAST 2.7.2**	4405	3714	53	638	71 740	32 761	38 979
Task description **UFO**	4405	3443	20	942	49 078	9 759	39 319
Task description **FrankenBit**	4405	3327	31	1047	139 559	7 629	131 929
Task description **CPAchecker (new rev., LDV config)**	4405	3683	54	668	178 002	48 564	129 438

Time is shown in seconds

BLAST → CPAchecker

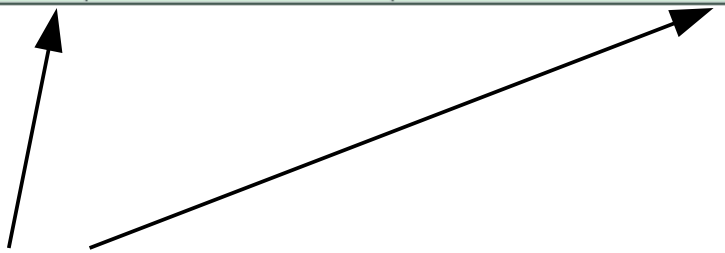
Total changes	Safe → Unsafe	Safe → Unknown	Unsafe → Unknown	Unknown → Safe	Unknown → Unsafe
171	3	87	12	59	10



Total known unsafes – 65
BLAST – 53
CPAcheker – 53

UFO → FrankenBit

Total changes	Safe → Unknown	Unsafe → Unknown	Unknown → Safe	Unknown → Unsafe
169	125	12	9	23



Different bugs!

Conclusion

- Configuration matters
- Tools complement each other
- Ready to be applied for more complex rules
- Require to produce readable verification trace (preferably in a common format)

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