Recent Advances of CPAchecker within Klever

Evgeny Novikov
ISP RAS, Linux Verification Center

CPA&LDV'20, Online, September 28, 2020

Target Programs

Linux loadable kernel modules			
Linux kernel		Loadable modules	
Version	5.5	Number	**~2000** (27%)
Release date	**January 26, 2020**	C source files	~3400
Configuration	allmodconfig	Total size	**~2.7 MLOC**
Architecture	x86_64	Average module size	**~1.3 KLOC**

Tools and Settings

- Klever
  - version: git 54182dd1d released on September 18, 2020
  - default settings and specifications
- CPAchecker
  - version: svn trunk:31140 released on May 6, 2019
  - main configurations: *ldv-bam* (reachability) and *smg-ldv* (memory safety)
- Computational resource limits
  - 5 minutes of CPU time
  - 5 GB of memory
- OpenStack virtual machine with 8 vCPUs (Intel Xeon E312xx) and 64 GB of memory

Code Coverage

Directory	Line coverage, KLOC	Function coverage, thousands
hid	20/36 (54%)	1.1/2.1 (50%)
hwmon	33/63 (52%)	1.5/3.9 (38%)
media	100/330 (31%)	5.2/18 (29%)
mtd	18/51 (35%)	0.79/2.8 (28%)
platform	11/29 (37%)	0.67/2.1 (31%)
staging	49/140 (34%)	2.2/7.5 (29%)
usb	58/150 (40%)	3.0/7.9 (38%)
video	34/75 (46%)	1.4/3.9 (36%)
Total	**320/870 (37%)**	**16/48 (33%)**

Verification Results (Memory Safety)

Unsafes: 242 (12%)	Safes: 857 (42%)	Unknowns: 960 (46%)
Bugs: 21 (9%)		CPAchecker: 643 (67%)
False alarms: 209 (86%)		• Timeout: 536 (83%)
• Verifier: 124 (59%)		• Others: 107 (17%)
• Models: 83 (40%)		Others: 317 (33%)
• Others: 2 (1%)		
To be assessed: 12 (5%)		

- Wall time: 11 hours
- CPU time (just CPAchecker): 54 hours

Verification Results
(14 Requirements Expressed as Reachability)

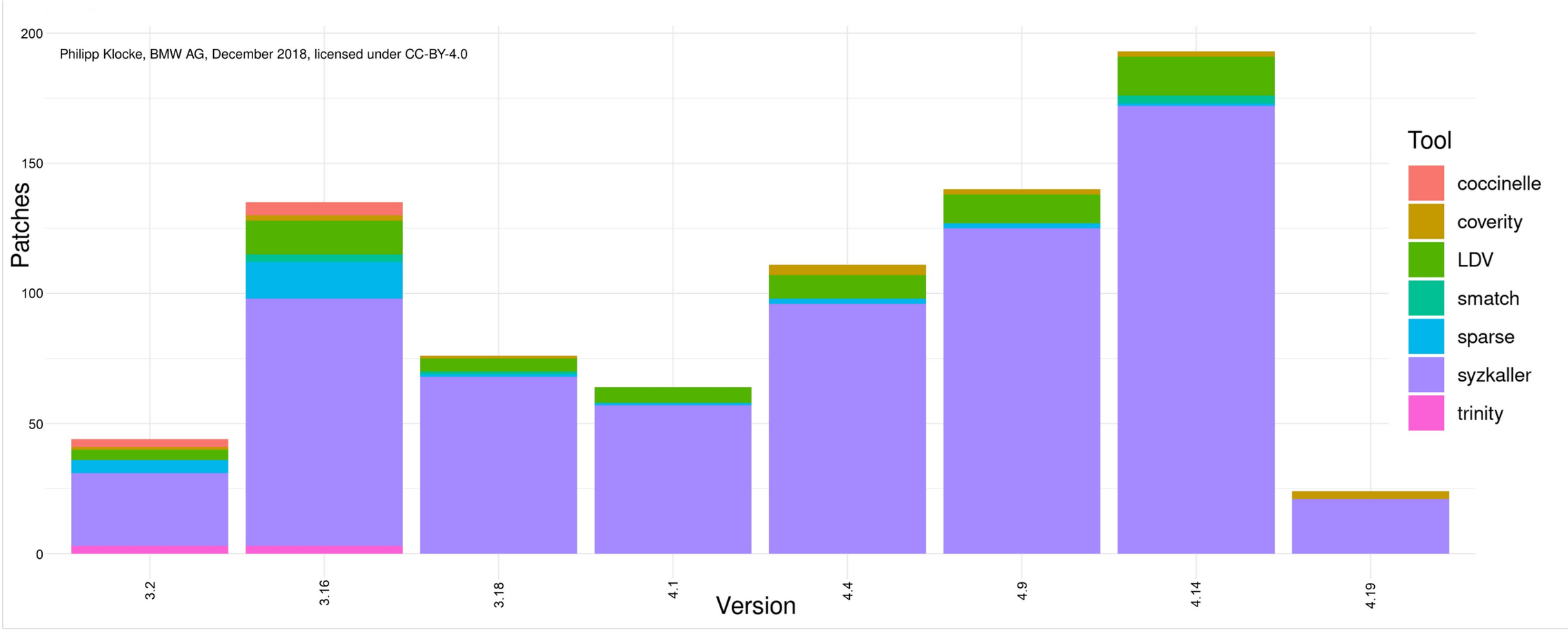
Unsafes: 90 (0.3%)	Safes: 23547 (89%)	Unknowns: 2962 (11%)
Bugs: 44 (49%)		CPAchecker: 771 (26%)
False alarms: 33 (37%)		• Timeout: 430 (56%)
• Verifier: 12 (36%)		• Others: 341 (44%)
• Models: 20 (61%)		Others: 2155 (74%)
• Others: 1 (3%)		
To be assessed: 13 (14%)		

- Wall time: ~58 (several invocations of Klever)
- CPU time (just CPAchecker): 165 hours

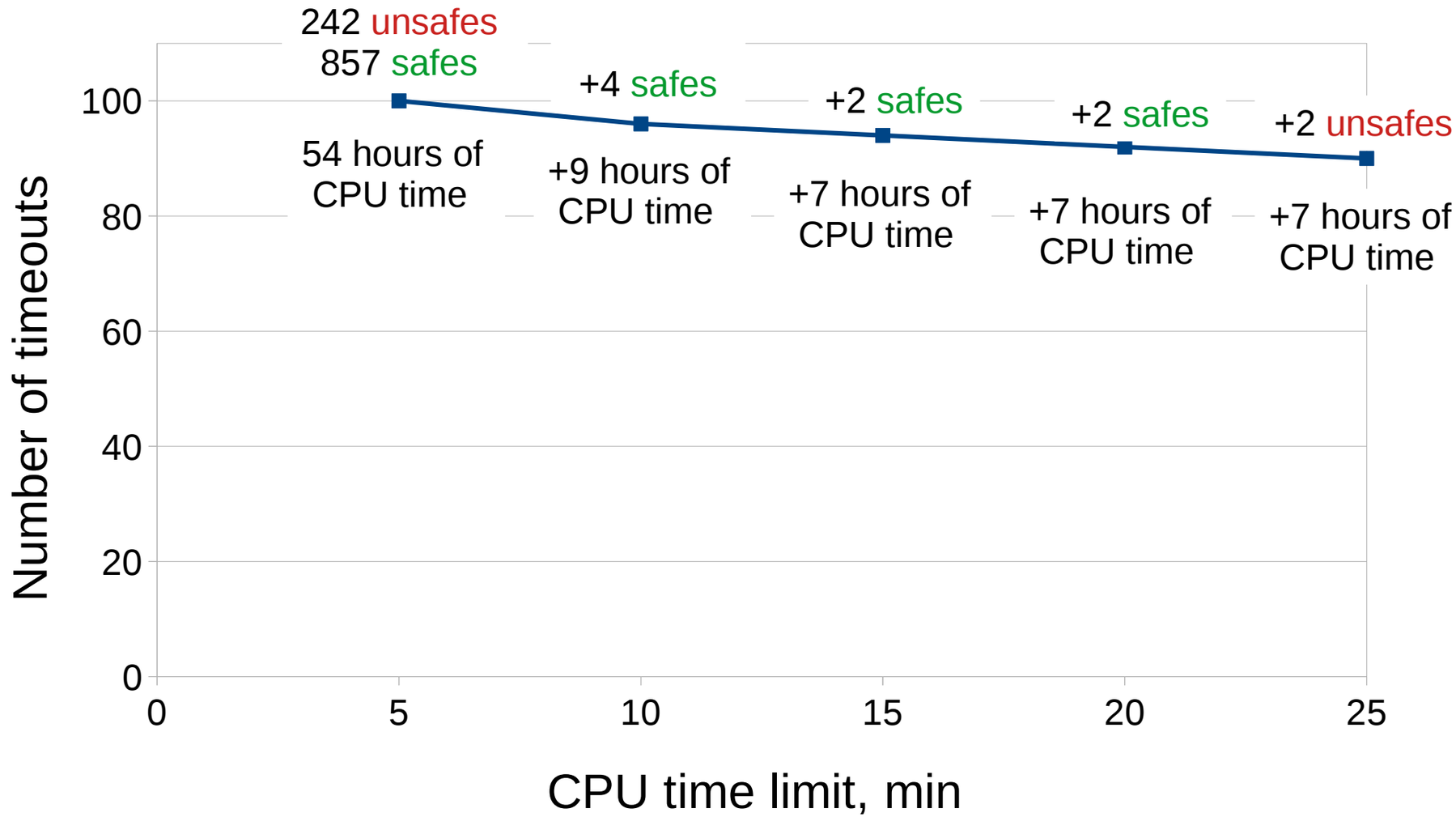
Bug Reports

- 22 patches and 3 messages
  - 15 commits are in the mainline already
  - 4 patches were accepted but they are not in the mainline yet
  - 2 bug reports were rejected due to corresponding execution paths are not possible on practice (inaccurate model)
- 10 commits were backported to stable branches
- 1 discussion resulted in considerable changes in the USB Device Controller framework

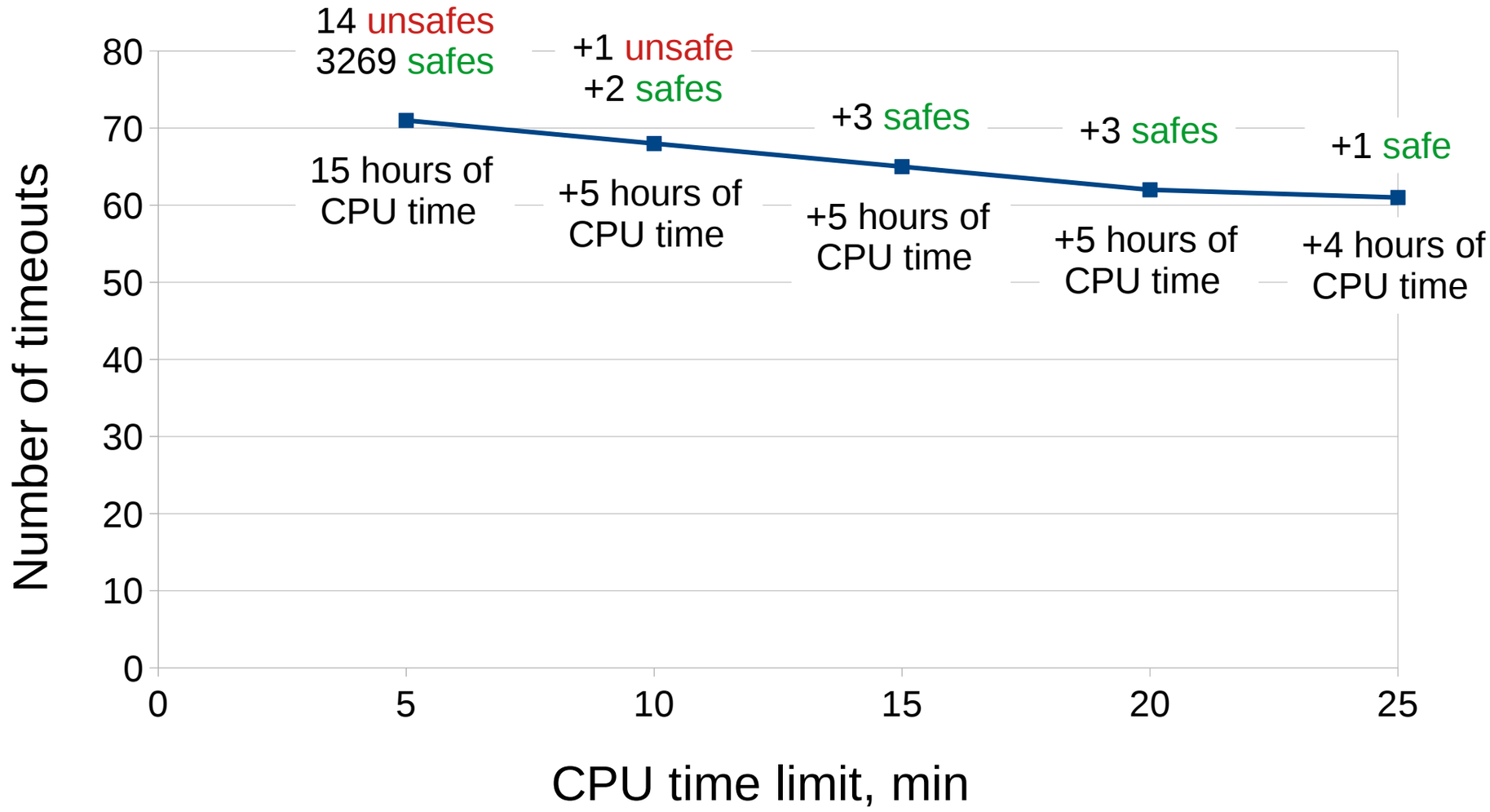
Patch Backports



Increasing CPU Time Limit (Memory Safety, 100 of 536 timeouts)



Increasing CPU Time Limit (Requirement Specification *drivers:clk1*)



Comparison of Verification Results (Memory Safety, CPAchecker 35003)

Previous verdict	New verdict	Number of changes
Unknown timeouts, parsing failures, exceptions	Safe	33
Unknown timeouts, parsing failures, exceptions	Unsafe false alarms (verifier), bugs	36
Safe	Unsafe false alarms (verifier), bugs	7
Safe	Unknown timeouts, exceptions	6
Unsafe	Unknown exceptions, timeouts	11

- CPU time (just CPAchecker): 54 hours → 52 hours

Comparison of Verification Results (*drivers:clk1*, CPAchecker 35003)

Previous verdict	New verdict	Number of changes
Unknown parsing failures, timeouts	Safe	22
Unknown timeouts, exceptions	Unsafe bugs, false alarms	3
Safe	Unknown timeouts	6
Unsafe false alarm (model)	Unknown timeout	1

- CPU time (just CPAchecker): 17 hours → 20 hours

New CPAchecker Test Suite

- Based on the Klever integrity regression test suite
  - 1309 verification tasks that are used to track regressions within Klever primarily
  - verification tasks correspond to different models, requirements, programs and configurations of CPAchecker
  - most of verification tasks need several dozens of seconds of CPU time and several hundreds of megabytes of memory, but some are rather complicated
- Concurrency safety verification tasks are not included into the BuildBot job

Conclusion

- CPAchecker within Klever finds severe bugs in industrial software
- Improving models shift the false alarm rate from Klever to CPAchecker
- Increasing the CPU time limit almost does not help to solve complicated verification tasks
- More frequent updates of CPAchecker within Klever are necessary