Maximizing Patch Coverage for Testing of Highly-Configurable Software without Exploding Build Times

Necip Fazıl Yıldıran, Jeho Oh, Julia Lawall, and **Paul Gazzillo**

May 29th, 2024

To Appear: FSE 2024

Testing the Linux Kernel is Important

Linux Kernel

70% of mobile devices

70% of IoT developers

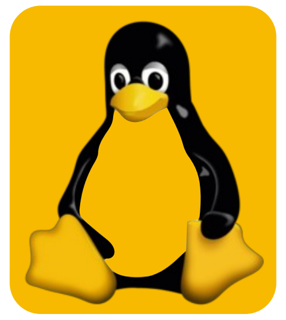
40% of servers

Configurability Makes Testing Hard

- Configuration options allow extensive reuse
- Trillions of kernel variations

Configuration options enable/disable features

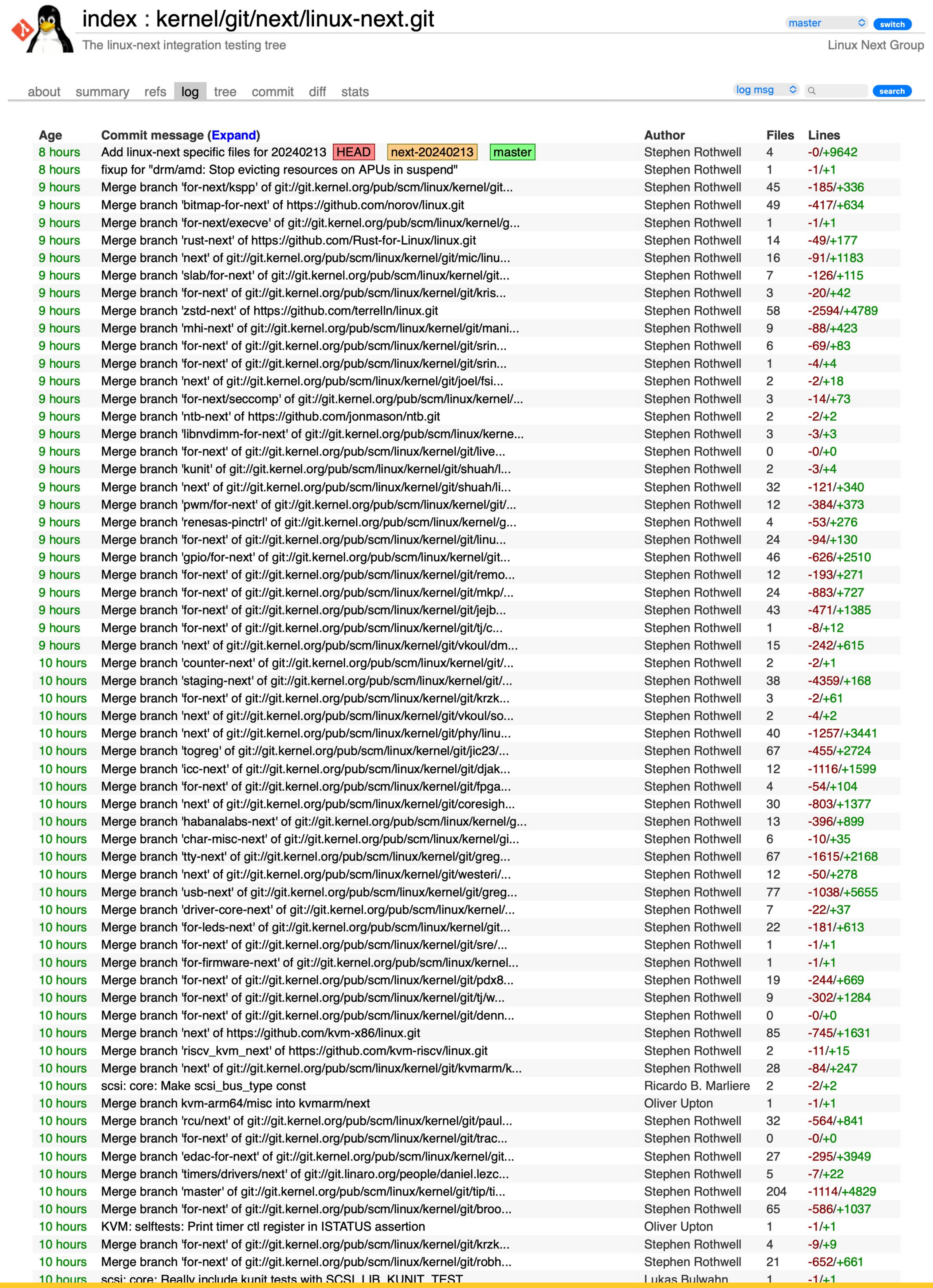
Linux build system generates many variations



Build customized software without reprogramming

Rapid Change Makes Testing Hard

Linux-next commit history



index : kernel/git/next/linux-next.git

The linux-next integration testing tree

Linux Next Group

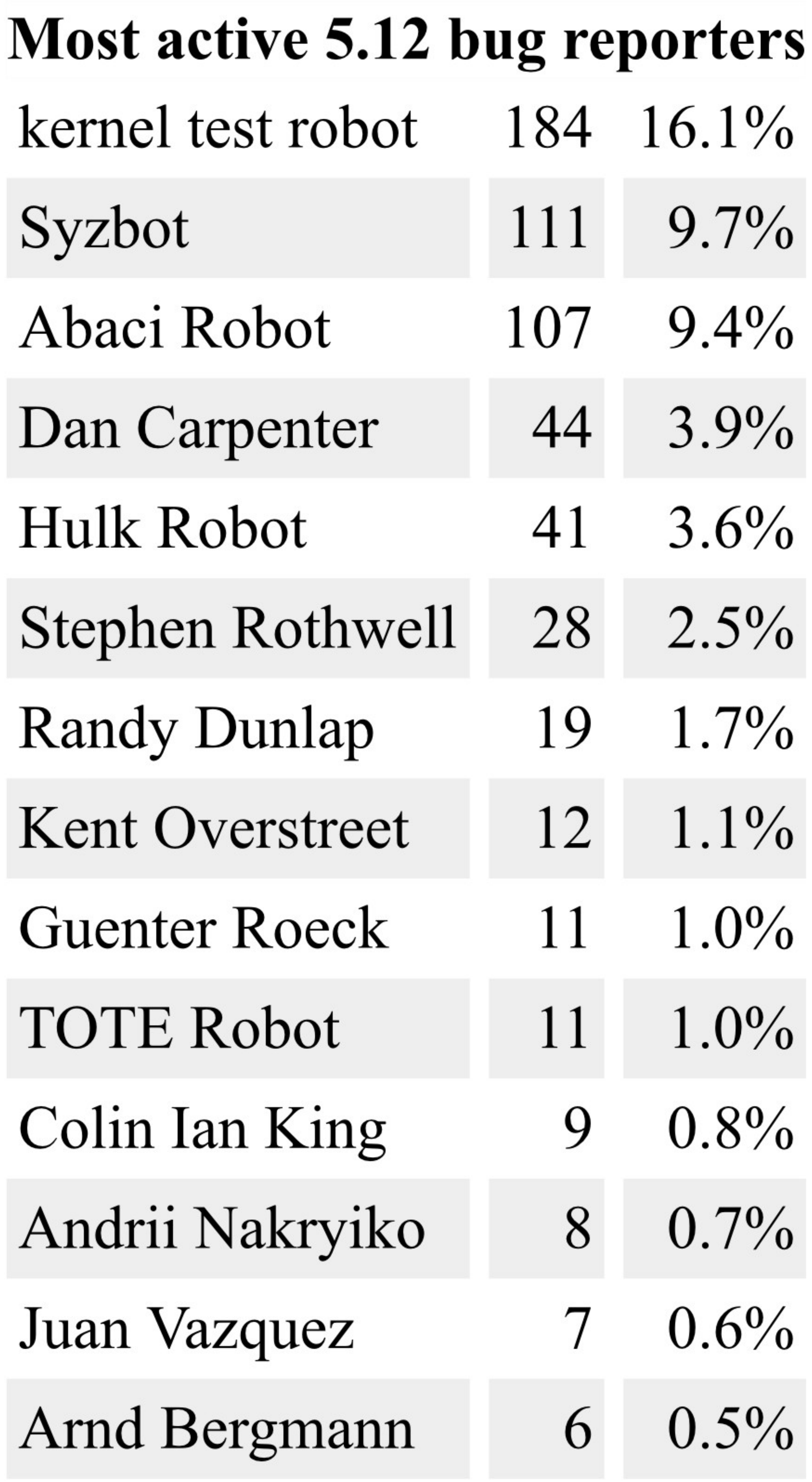
Age	Commit message (Expand)	Author	Files	Lines
8 hours	Add linux-next specific files for 20240213 HEAD next-20240213 master	Stephen Rothwell	4	-0/+9642
8 hours	fixup for "drm/amd: Stop evicting resources on APUs in suspend"	Stephen Rothwell	1	-1/+1
9 hours	Merge branch 'for-next/kspp' of git://git.kernel.org/pub/scm/linux/kernel/git...	Stephen Rothwell	45	-185/+336
9 hours	Merge branch 'bitmap-for-next' of https://github.com/norov/linux.git	Stephen Rothwell	49	-417/+634
9 hours	Merge branch 'for-next/execve' of git://git.kernel.org/pub/scm/linux/kernel/g...	Stephen Rothwell	1	-1/+1
9 hours	Merge branch 'rust-next' of https://github.com/Rust-for-Linux/linux.git	Stephen Rothwell	14	-49/+177
9 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/mic/linu...	Stephen Rothwell	16	-91/+1183
9 hours	Merge branch 'slab/for-next' of git://git.kernel.org/pub/scm/linux/kernel/git...	Stephen Rothwell	7	-126/+115
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/kris...	Stephen Rothwell	3	-20/+42
9 hours	Merge branch 'zstd-next' of https://github.com/terrelln/linux.git	Stephen Rothwell	58	-2594/+4789
9 hours	Merge branch 'mhi-next' of git://git.kernel.org/pub/scm/linux/kernel/git/mani...	Stephen Rothwell	9	-88/+423
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/srin...	Stephen Rothwell	6	-69/+83
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/srin...	Stephen Rothwell	1	-4/+4
9 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/joel/fsi...	Stephen Rothwell	2	-2/+18
9 hours	Merge branch 'for-next/seccomp' of git://git.kernel.org/pub/scm/linux/kernel/...	Stephen Rothwell	3	-14/+73
9 hours	Merge branch 'ntb-next' of https://github.com/jonmason/ntb.git	Stephen Rothwell	2	-2/+2
9 hours	Merge branch 'libnvdimm-for-next' of git://git.kernel.org/pub/scm/linux/kerne...	Stephen Rothwell	3	-3/+3
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/live...	Stephen Rothwell	0	-0/+0
9 hours	Merge branch 'kunit' of git://git.kernel.org/pub/scm/linux/kernel/git/shuah/l...	Stephen Rothwell	2	-3/+4
9 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/shuah/li...	Stephen Rothwell	32	-121/+340
9 hours	Merge branch 'pwm/for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/...	Stephen Rothwell	12	-384/+373
9 hours	Merge branch 'renesas-pinctrl' of git://git.kernel.org/pub/scm/linux/kernel/g...	Stephen Rothwell	4	-53/+276
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/linu...	Stephen Rothwell	24	-94/+130
9 hours	Merge branch 'gpio/for-next' of git://git.kernel.org/pub/scm/linux/kernel/git...	Stephen Rothwell	46	-626/+2510
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/remo...	Stephen Rothwell	12	-193/+271
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/mkp/...	Stephen Rothwell	24	-883/+727
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/jejb...	Stephen Rothwell	43	-471/+1385
9 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/tj/c...	Stephen Rothwell	1	-8/+12
9 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/vkoul/dm...	Stephen Rothwell	15	-242/+615
10 hours	Merge branch 'counter-next' of git://git.kernel.org/pub/scm/linux/kernel/git/...	Stephen Rothwell	2	-2/+1
10 hours	Merge branch 'staging-next' of git://git.kernel.org/pub/scm/linux/kernel/git/...	Stephen Rothwell	38	-4359/+168
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/krzk...	Stephen Rothwell	3	-2/+61
10 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/vkoul/so...	Stephen Rothwell	2	-4/+2
10 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/phy/linu...	Stephen Rothwell	40	-1257/+3441
10 hours	Merge branch 'togreg' of git://git.kernel.org/pub/scm/linux/kernel/git/jic23/...	Stephen Rothwell	67	-455/+2724
10 hours	Merge branch 'icc-next' of git://git.kernel.org/pub/scm/linux/kernel/git/djak...	Stephen Rothwell	12	-1116/+1599
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/fpga...	Stephen Rothwell	4	-54/+104
10 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/coresigh...	Stephen Rothwell	30	-803/+1377
10 hours	Merge branch 'habanalabs-next' of git://git.kernel.org/pub/scm/linux/kernel/g...	Stephen Rothwell	13	-396/+899
10 hours	Merge branch 'char-misc-next' of git://git.kernel.org/pub/scm/linux/kernel/gi...	Stephen Rothwell	6	-10/+35
10 hours	Merge branch 'tty-next' of git://git.kernel.org/pub/scm/linux/kernel/git/greg...	Stephen Rothwell	67	-1615/+2168
10 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/westeri/...	Stephen Rothwell	12	-50/+278
10 hours	Merge branch 'usb-next' of git://git.kernel.org/pub/scm/linux/kernel/git/greg...	Stephen Rothwell	77	-1038/+5655
10 hours	Merge branch 'driver-core-next' of git://git.kernel.org/pub/scm/linux/kernel/...	Stephen Rothwell	7	-22/+37
10 hours	Merge branch 'for-leds-next' of git://git.kernel.org/pub/scm/linux/kernel/git...	Stephen Rothwell	22	-181/+613
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/sre/...	Stephen Rothwell	1	-1/+1
10 hours	Merge branch 'for-firmware-next' of git://git.kernel.org/pub/scm/linux/kernel...	Stephen Rothwell	1	-1/+1
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/pdx8...	Stephen Rothwell	19	-244/+669
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/tj/w...	Stephen Rothwell	9	-302/+1284
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/denn...	Stephen Rothwell	0	-0/+0
10 hours	Merge branch 'next' of https://github.com/kvm-x86/linux.git	Stephen Rothwell	85	-745/+1631
10 hours	Merge branch 'riscv_kvm_next' of https://github.com/kvm-riscv/linux.git	Stephen Rothwell	2	-11/+15
10 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/kvmarm/k...	Stephen Rothwell	28	-84/+247
10 hours	scsi: core: Make scsi_bus_type const	Ricardo B. Marliere	2	-2/+2
10 hours	Merge branch kvm-arm64/misc into kvmarm/next	Oliver Upton	1	-1/+1
10 hours	Merge branch 'rcu/next' of git://git.kernel.org/pub/scm/linux/kernel/git/paul...	Stephen Rothwell	32	-564/+841
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/trac...	Stephen Rothwell	0	-0/+0
10 hours	Merge branch 'edac-for-next' of git://git.kernel.org/pub/scm/linux/kernel/git...	Stephen Rothwell	27	-295/+3949
10 hours	Merge branch 'timers/drivers/next' of git://git.linaro.org/people/daniel.lezc...	Stephen Rothwell	5	-7/+22
10 hours	Merge branch 'master' of git://git.kernel.org/pub/scm/linux/kernel/git/tip/ti...	Stephen Rothwell	204	-1114/+4829
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/broo...	Stephen Rothwell	65	-586/+1037
10 hours	KVM: selftests: Print timer ctl register in ISTATUS assertion	Oliver Upton	1	-1/+1
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/krzk...	Stephen Rothwell	4	-9/+9
10 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/robh...	Stephen Rothwell	21	-652/+661
10 hours	scsi: core: Really include kunit tests with SCSI_LIB_KUNIT_TEST	Lukas Bulwahn	1	-1/+1

~30k mailing list messages per month

~6k commits per month, 100s per day

e.g., ~13k commits between v5.12 and v5.13

Test Robots Are the Most Successful Reporters



Most active 5.12 bug reporters

kernel test robot	184	16.1%
Syzbot	111	9.7%
Abaci Robot	107	9.4%
Dan Carpenter	44	3.9%
Hulk Robot	41	3.6%
Stephen Rothwell	28	2.5%
Randy Dunlap	19	1.7%
Kent Overstreet	12	1.1%
Guenter Roeck	11	1.0%
TOTE Robot	11	1.0%
Colin Ian King	9	0.8%
Andrii Nakryiko	8	0.7%
Juan Vazquez	7	0.6%
Arnd Bergmann	6	0.5%

Intel 0-day kernel test robot

- Suite of static and dynamic testing tools
  - compile, boot, performance, etc.
- continuously runs on new commits in linux-next

Google syzbot

- syzkaller system call fuzz tester
- continuously tests the kernel
- runs on linux-next, other versions

https://lwn.net/Articles/853039/

Typical Configurations Exclude Code Changes

Configuration	Avg. Patch Coverage
defconfig	22%
randconfig	30%
syzbot	42%

Based on 507 randomly-selected C code patches from linux-next between 2021/09/19-2022/09/18
5% margin of error
98% confidence level

Problem: How do we pick configuration files that cover new patches?

Patch Coverage

Percent of C source lines in a patchfile compiled by a configuration file

allyesconfig for Patch Coverage?

Covers 89% of patches ✓

Not bootable, mostly for compile testing ✗

No variation, can miss configuration bugs ✗

Time-consuming to build, hours vs. minutes for defconfig ✗

Very large memory footprint ✗

Still fails to cover 11% of patched lines ✗

Introducing krepair

krepair automatically modifies any configuration file to be patch covering

krepair Benefits

98.5% patch coverage (sample average) ✓

Use any configuration file, maintains variation ✓

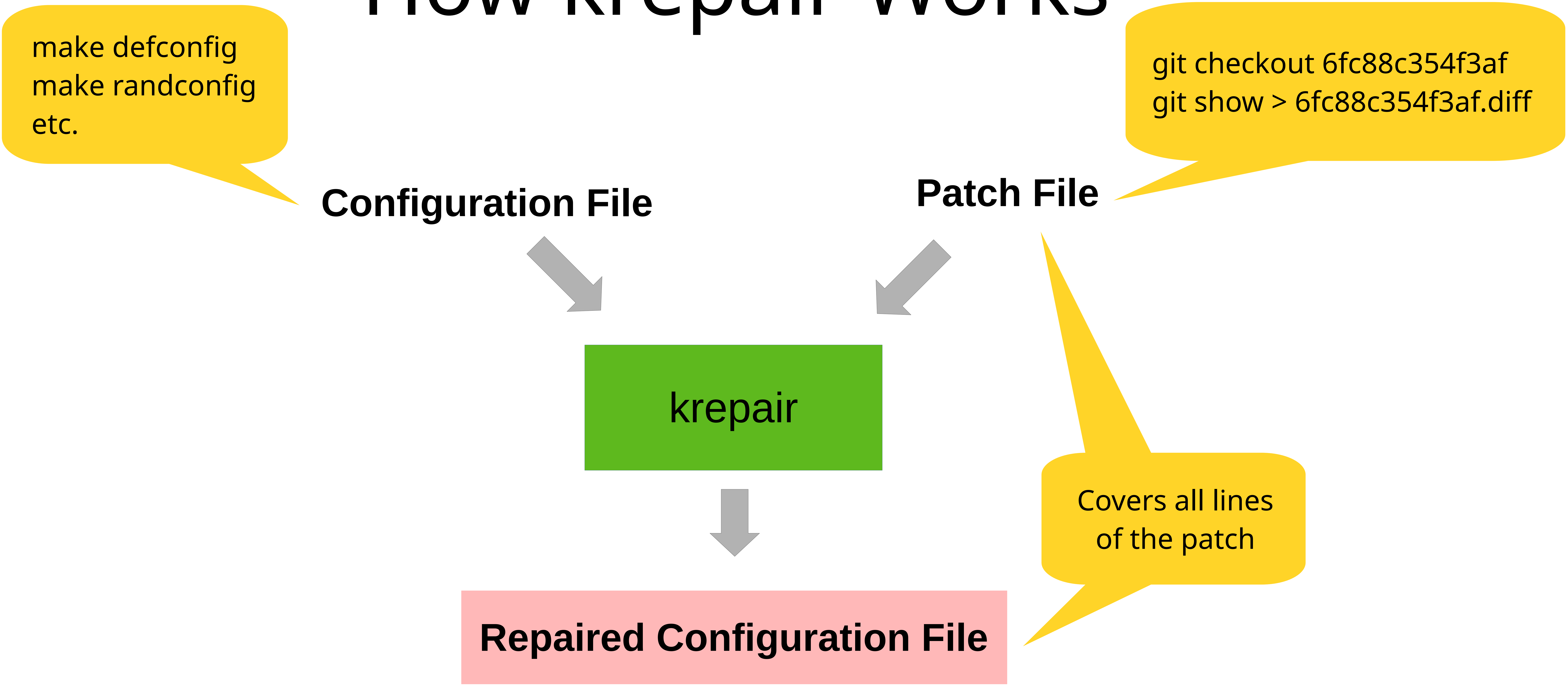
<2% change to most configuration files ✓

Configuration remains bootable ✓

Maintains fast build times ✓

Maintains memory footprint ✓

How krepair Works



```
make defconfig
make randconfig
etc.
```

Configuration File

```
git checkout 6fc88c354f3af
git show > 6fc88c354f3af.diff
```

Patch File

krepair

Covers all lines of the patch

Repaired Configuration File

Evaluating krepair

Random patches

Repair defconfig for each

Measure patch coverage and build time

Compare against unrepaired defconfig and allyesconfig

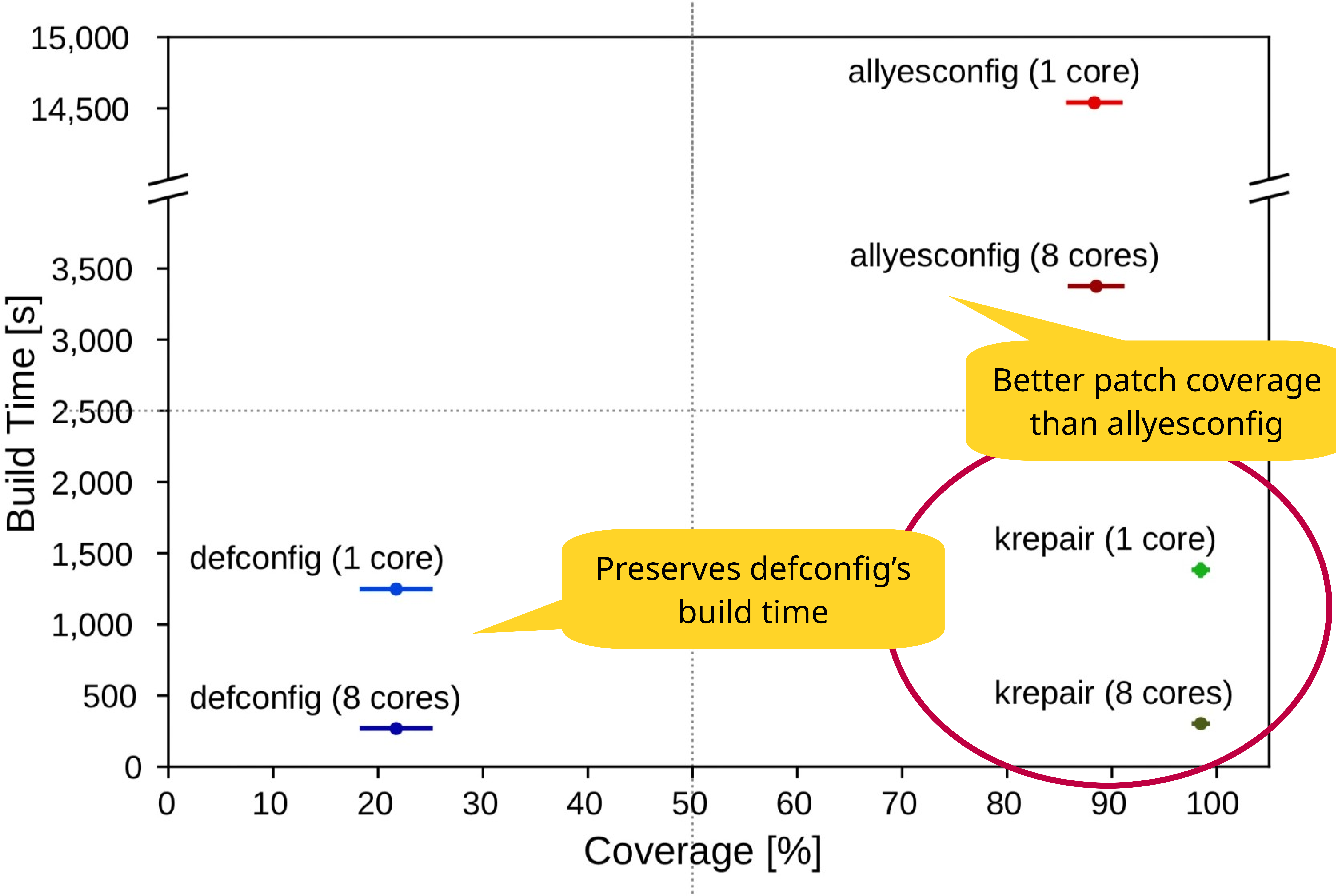
Random Patch Selection

Sample from 71k over a year (2021-2022) from linux-next

5% margin of error and 98% confidence

507 patches

Filter out non-C-source patches (documentation, scripts, etc.)



Better patch coverage than allyesconfig

Preserves defconfig's build time

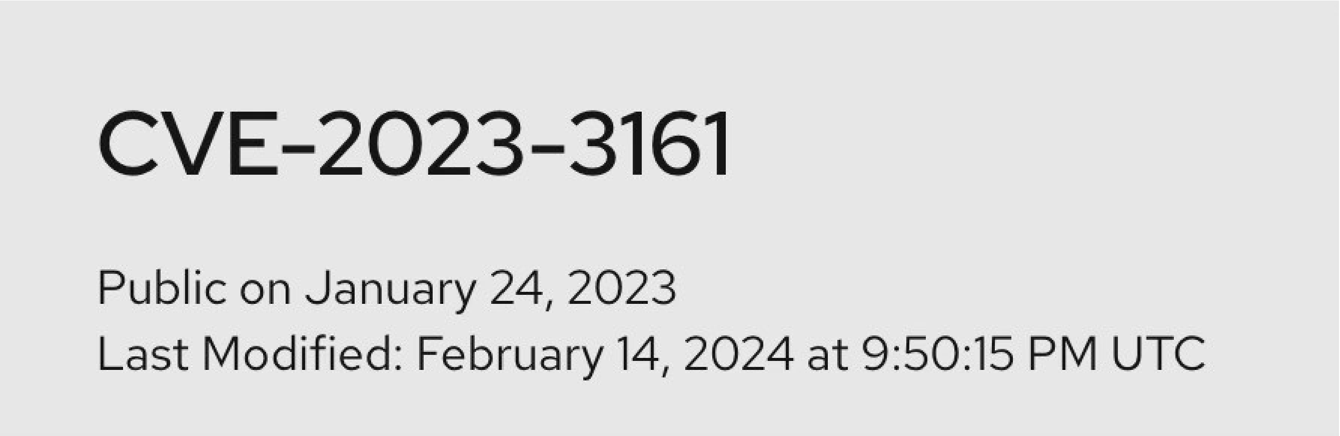
Case Study: Repairing Fuzzer Configurations

Take 40 previous syzkaller runs

Run krepair on run’s configuration file

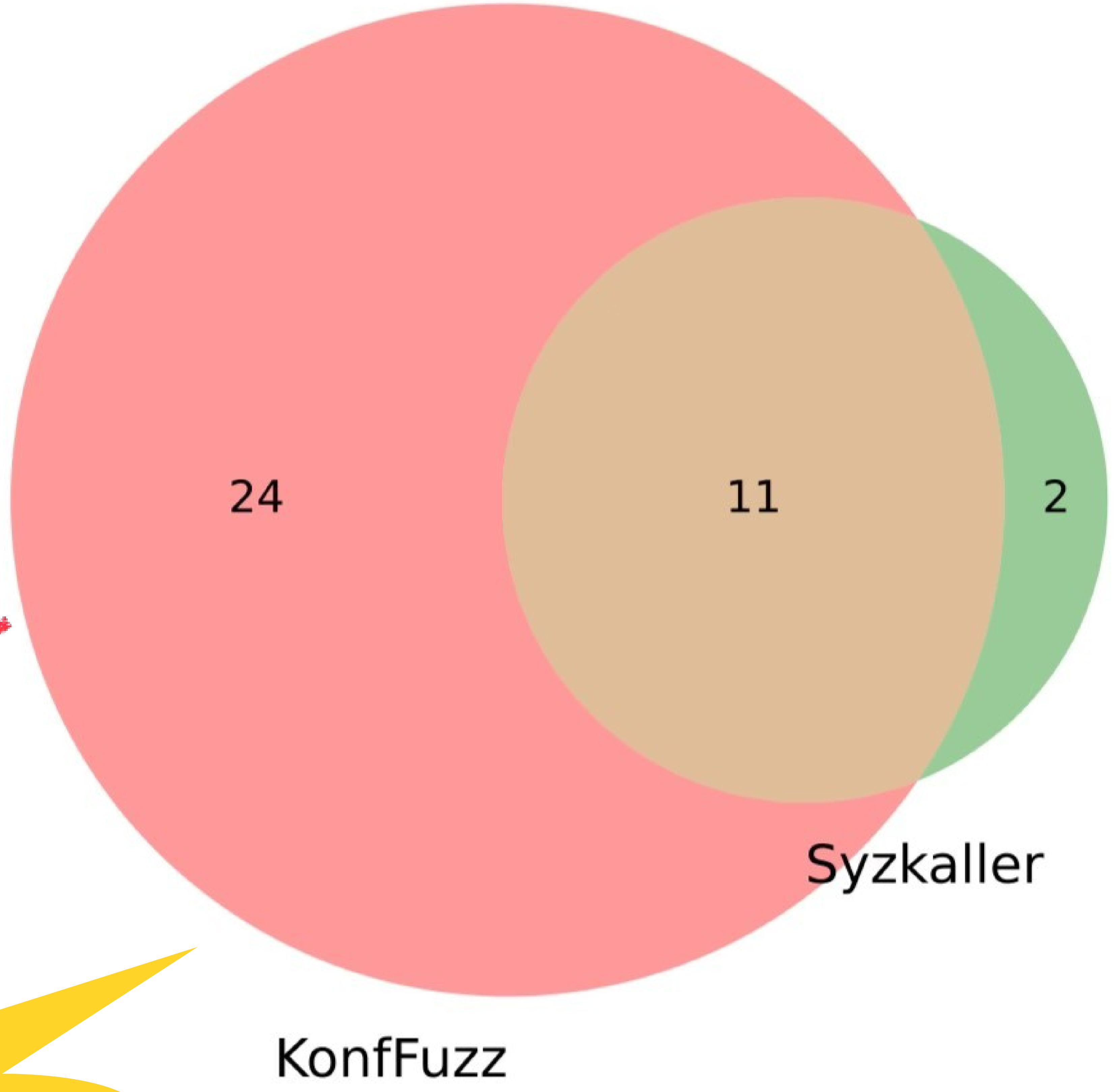
Rerun syzkaller with and without krepair

Preliminary Results



CVE-2023-3161

Public on January 24, 2023
Last Modified: February 14, 2024 at 9:50:15 PM UTC



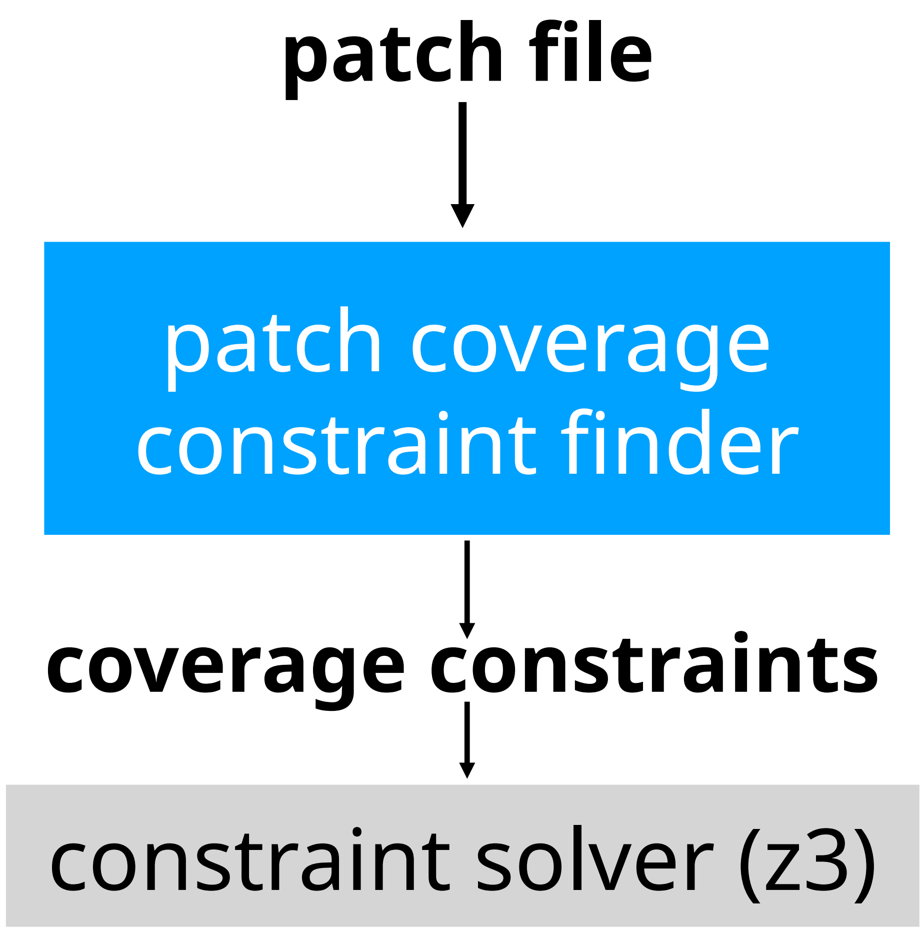
New bugs found with old configuration files

New bugs found with repaired configuration files

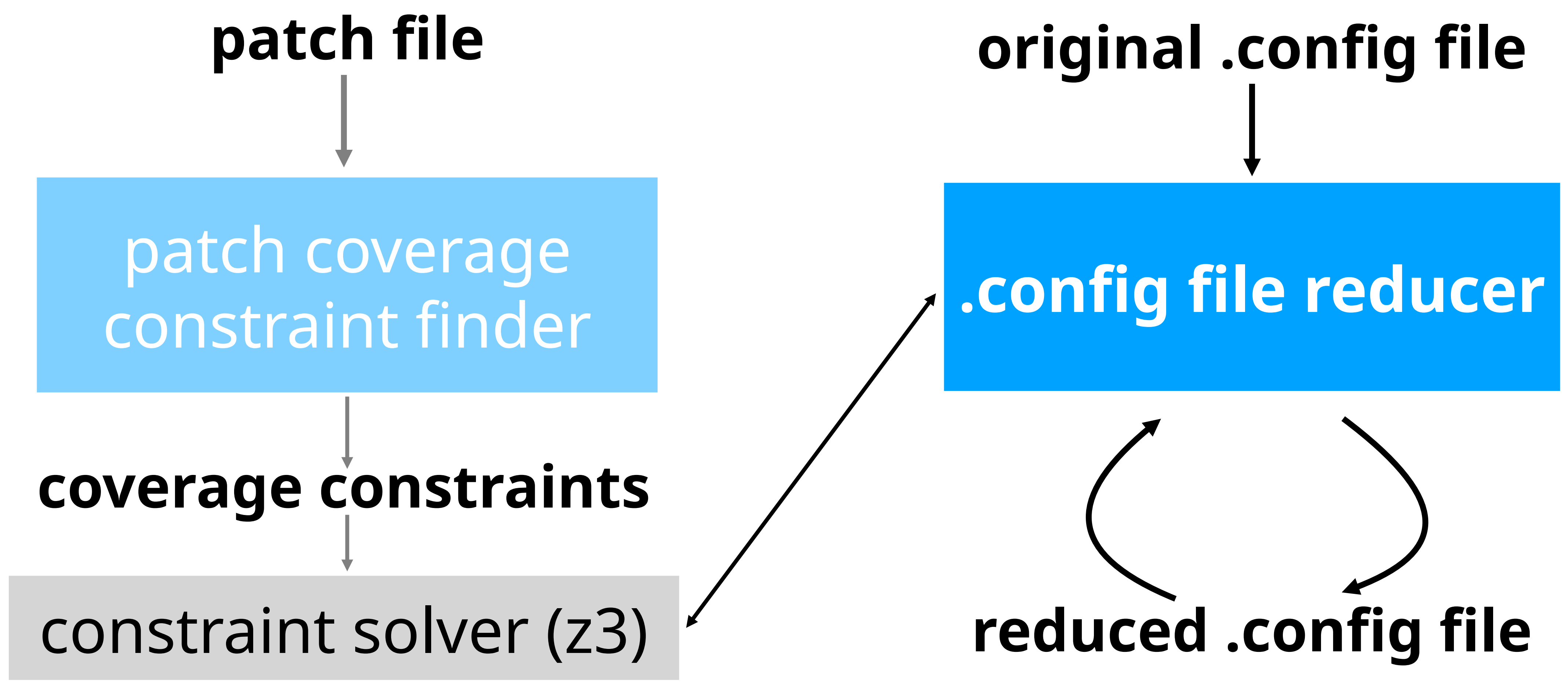
krepair’s Algorithm

1. **Analyze**: find patch covering constraints
2. **Reduce**: remove options preventing patch coverage
3. **Repair**: re-add only settings that satisfy patch coverage constraints

(1) Figure Out Configuration Constraints for the Patch



(2) Remove Options Preventing Patch from Building



patch file

patch coverage constraint finder

coverage constraints

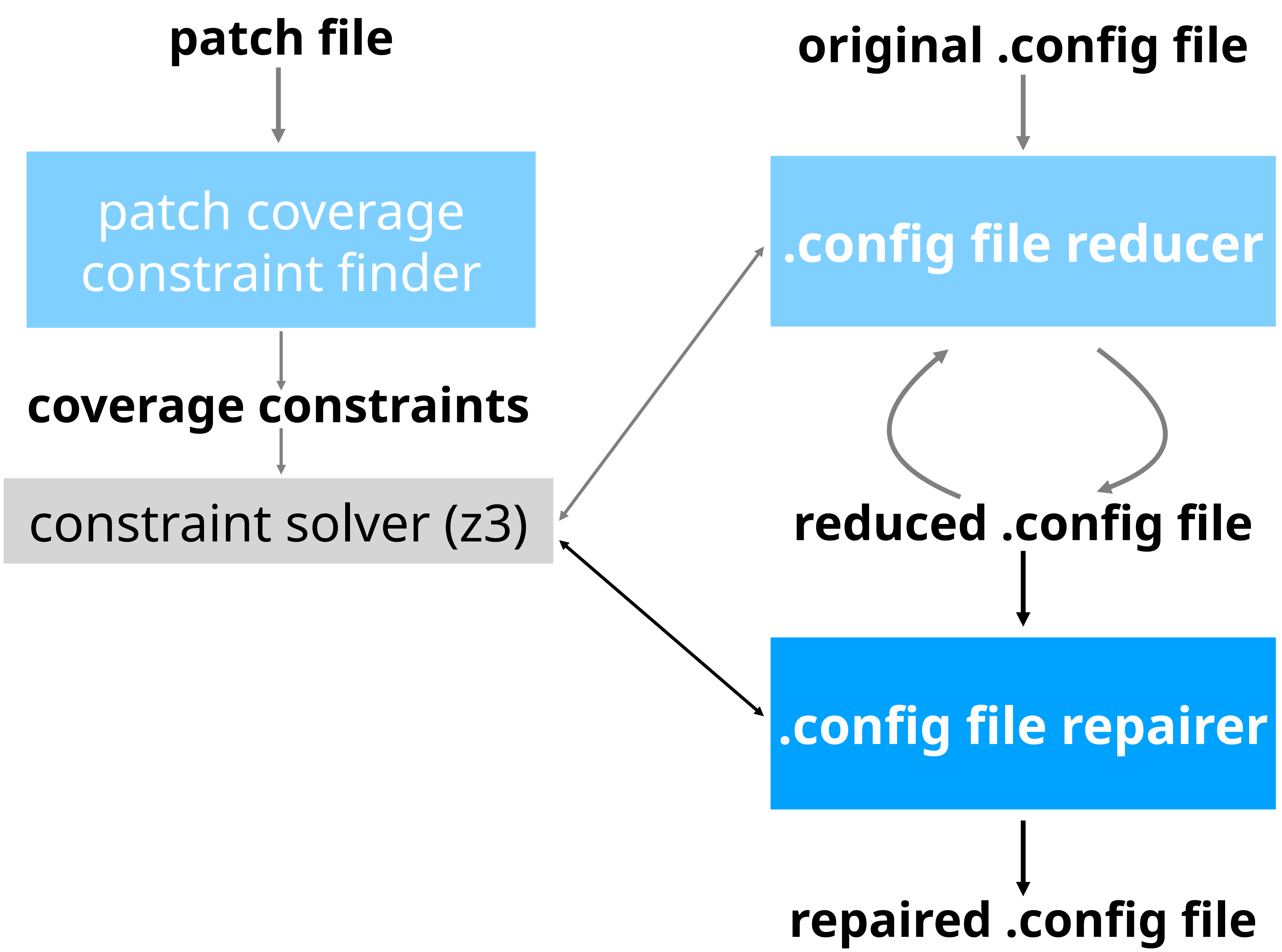
constraint solver (z3)

original .config file

.config file reducer

reduced .config file

(3) Add Back Settings that Satisfy Constraints



patch file

patch coverage constraint finder

coverage constraints

constraint solver (z3)

original .config file

.config file reducer

reduced .config file

.config file repairer

repaired .config file

Conclusion

krepair modifies configuration files for patch coverage

Makes minimal changes, preserving most original settings

Achieves very high patch coverage on average

https://github.com/paulgazz/kmax