Securing Software Configurations

Bringing Analysis and Testing to the Entire Software Ecosystem

Paul Gazzillo Assistant Professor of Computer Science University of Central Florida 04/03/2024



Expand the scope of software analysis beyond the programming language to the entire software ecosystem to further strengthen and secure software.

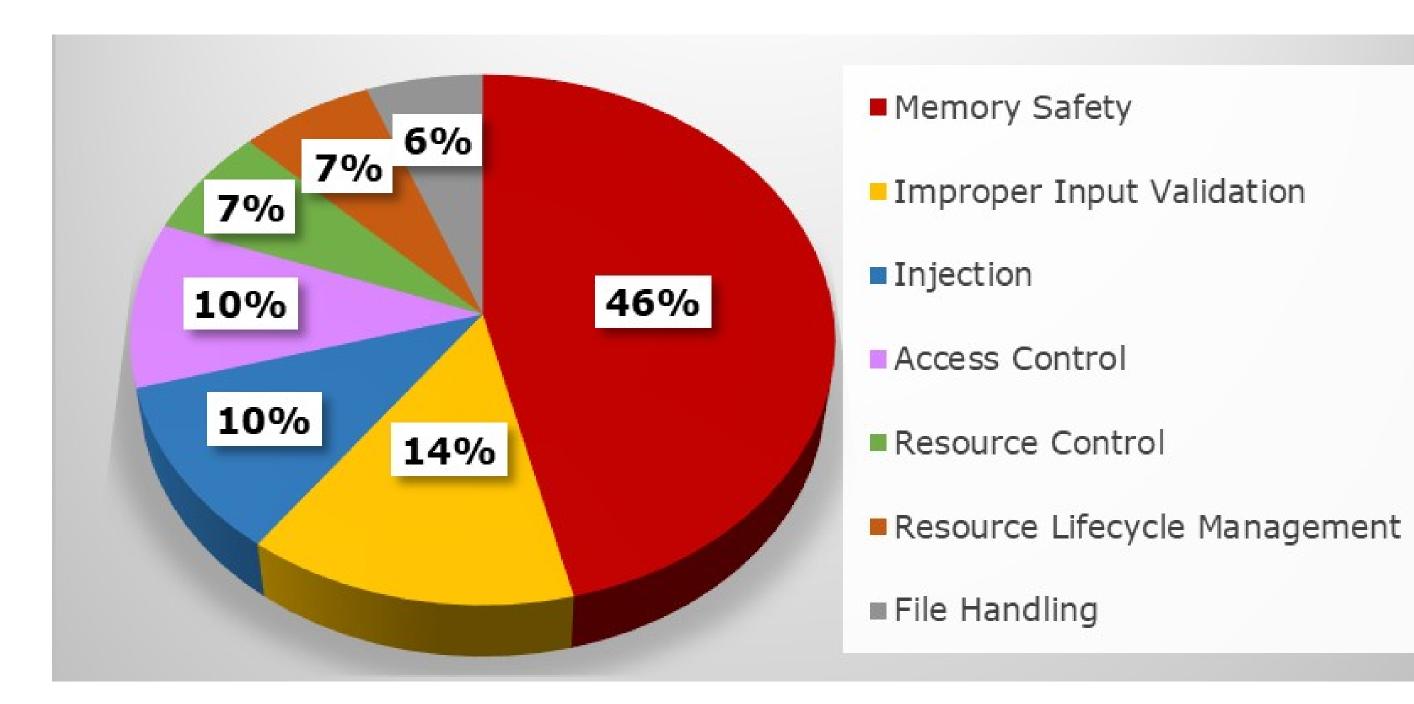
Vision







Memory Safety Dominates Exploits



Source: 2023 CWE Top 10 KEV Weaknesses List Insights







C/C++ Is the Origin

ENOUGH ROPE TO SHOOT YOURSELF IN THE FOOT Rules for C and C++ **Programming**



Memory Safe Programming is Solved





CYCLONE Checked C











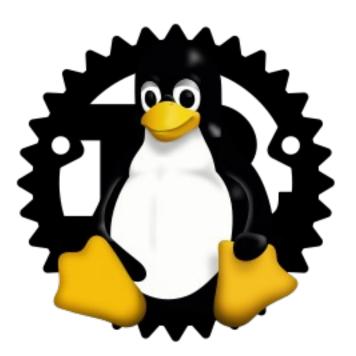
Just a Matter of Time



THE WHITE HOUSE

PRESS RELEASE: Future Software Should Be Memory Safe

FEBRUARY 26, 2024



Swift

Rust for Linux

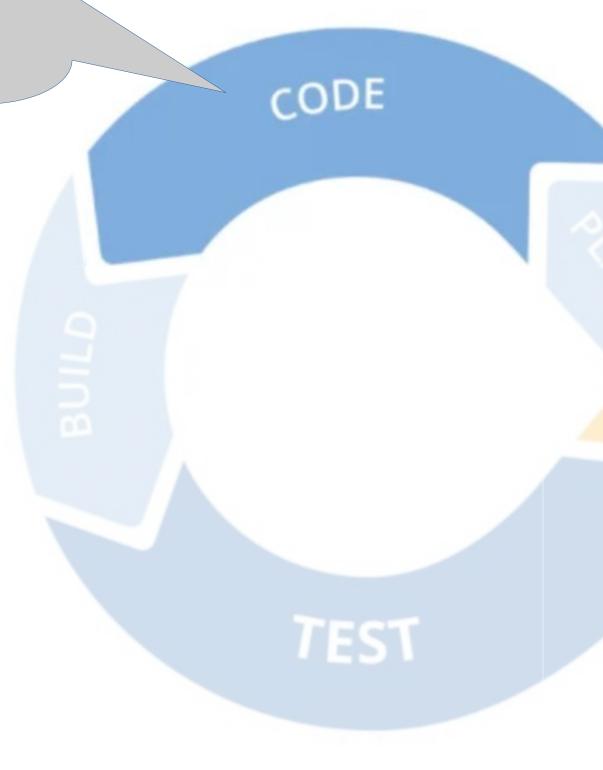
Swift for Apple

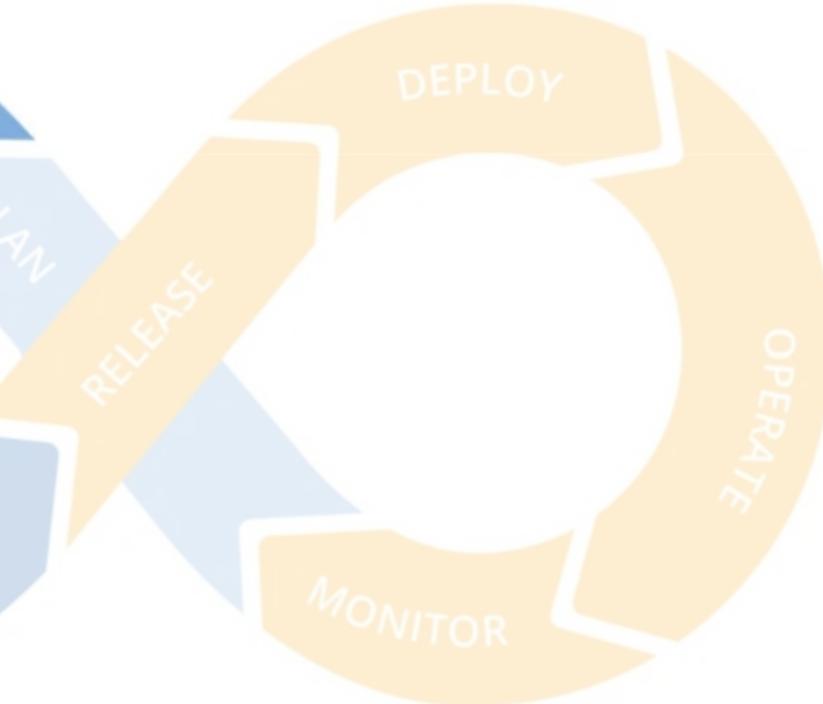




What's Left After Memory-Based Exploits?

Memory bugs happen here



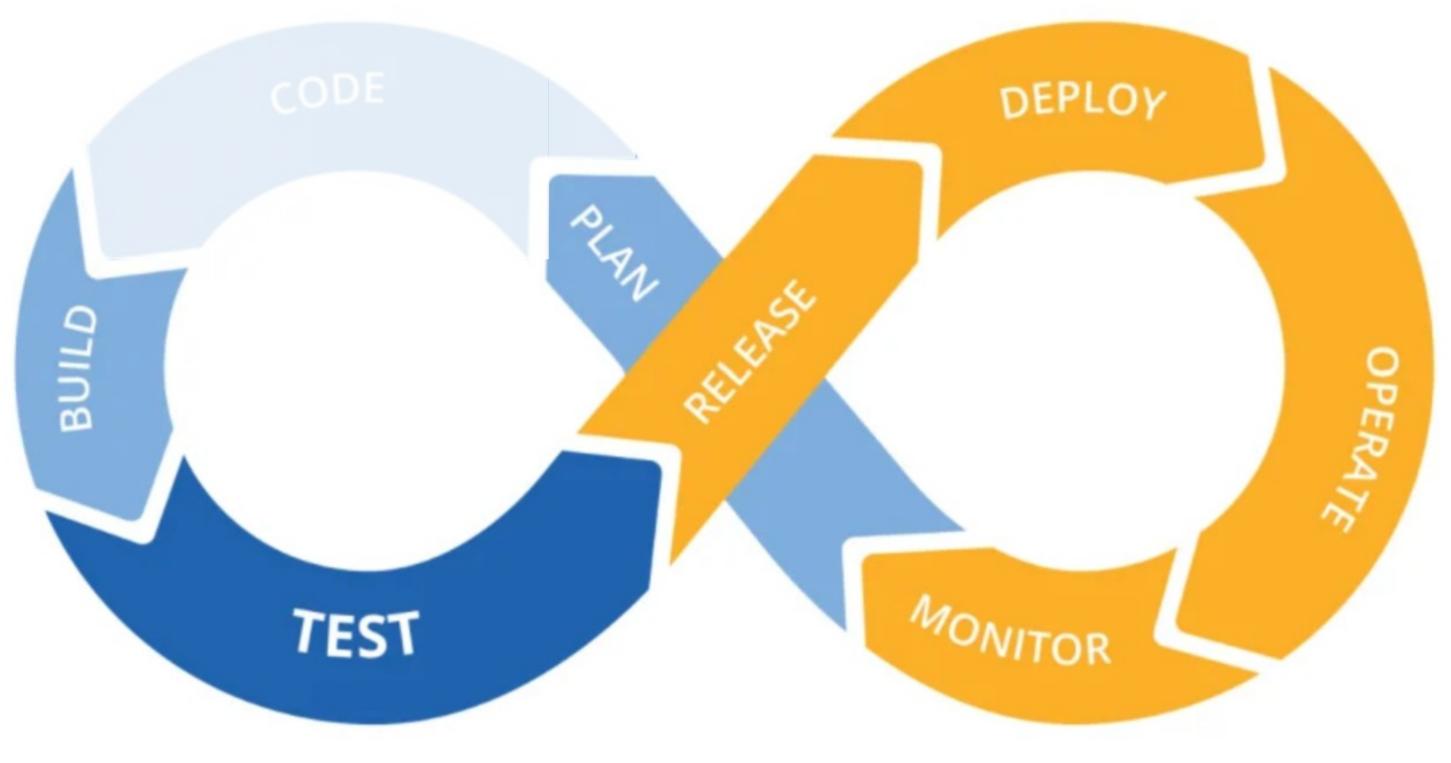


DevOps Phases





Other Phases of Development and Operations



DevOps Phases





- Hacked build system
- Malware in signed code
- "More than 200 victims"

https://www.bloomberg.com/news/articles/2020-12-19/at-least-200-victims-identified-in-suspected-russian-hacking https://www.theguardian.com/technology/2021/dec/10/software-flaw-most-critical-vulnerability-log-4-shell



• Feature, not bug

- Disable with configuration setting
- "Most critical vulnerability"



TURING AWARD LECTURE

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON





Why Bother Breaking In?







Inferring and Securing Software Configurations





Misconfiguration Vulnerabilities Are Prevalent

Wednesday, September 26, 2018

A cache invalidation bug in Linux memory management

Posted by Jann Horn, Google Project Zero

"This exploit shows how much impact the kernel configuration can have on how easy it is to write an exploit for a kernel bug."

#6 in OWASP top ten most critical security risks most common risk reported





Highly-Configurable Software is Widespread



Linux kernel

- 70% of mobile devices
- 70% of IoT developers
- 40% of servers



Apache web server

40% of servers

billions of devices





UCF

Misconfiguration Vulnerabilities are Rooted in Software Configuration Management

- Manages *change* to a software system
- Allows customizing software without reprogramming
 - Falls outside of classic program analysis





Goal: a world without misconfigurations





Solution approach: formal methods to validate and generate software configurations



Challenges: a lack of existing specifications, an enormous state space



Research Goals

Create a rigorous definition of configuration specifications

Mechanize the generation of valid configurations

Automatically discover secure configurations





Motivating Example: OptionsBleed





A Limit Directive Restricts Access to HTTP Methods in an Apache Webserver

</Limit>

<Limit PUT DELTE BIND>



OptionsBleed Leaks Arbitrary Memory Contents of an Apache Webserver

</Limit>

invalid http method exposes a use-after-free bug







Subtle Interactions Between Configuration Mechanisms Influence OptionsBleed's Occurrence

<Limit PUT DELTE </Limit>



BIND is only valid with the WebDAV HTTP extension

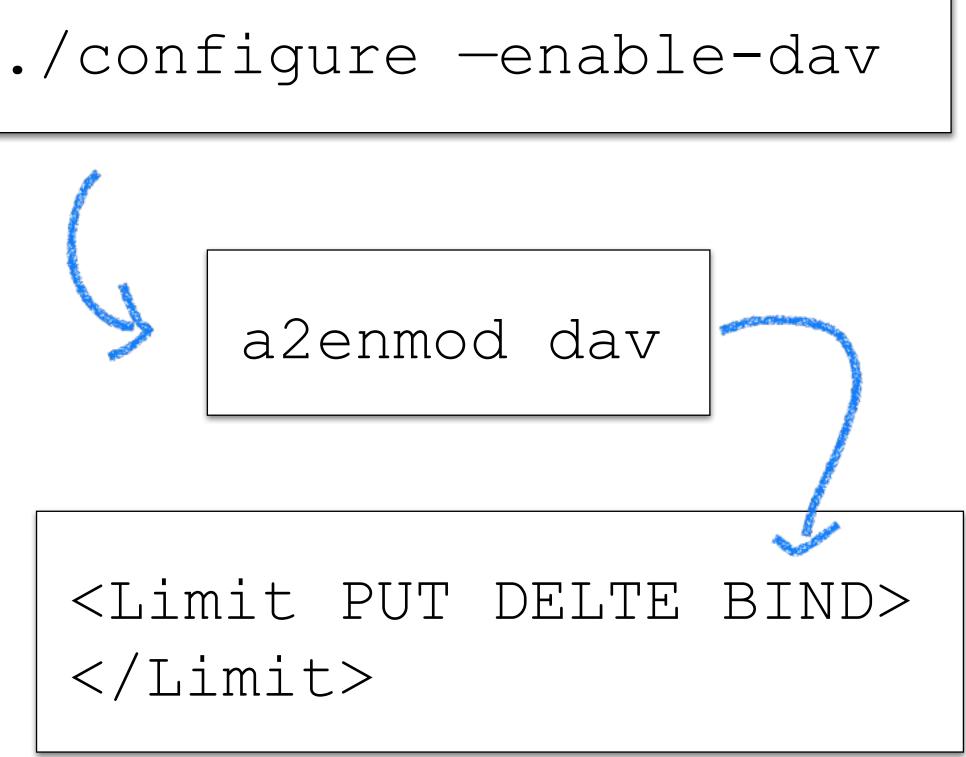


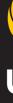


Subtle Interactions Between Configuration Mechanisms Influence OptionsBleed's Occurrence

</Limit>

WebDAV is enabled only with a compile-time flag and run-time module loader







Solution approach: automatically validate and generate software configurations



Automation needs a unified global view of configuration specifications



Configuration options are long-lived values, global to an entire software system





Formalize Valid Configurations as Constraints Among All Configuration Options

limit.method = PUT
or limit.method = DELETE
or (limit.method = BIND
 and build.enable-dav =
True
and module.dav = True)



configuration validity is satisfiability

build

./configure -enable-dav

module

a2enmod dav

limit

<Limit PUT DELTE BIND> </Limit>





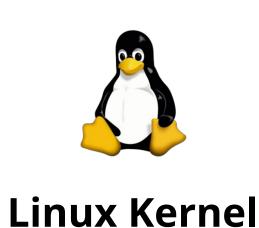


Formalizing the Linux Build and **Configuration System**



The Linux Kernel Build System







Example: Linux Kernel

70% of mobile devices 70% of IoT developers 40% of servers





The Kernel is Ultra-Configurable

*** Compiler: gcc (Ubuntu 9.2.1-9ubuntu2) 9.2.1 20191008 *** General setup ---> [*] 64-bit kernel Processor type and features --->

Bus options (PCI etc.) ---> Binary Emulations ---> Firmware Drivers --->

- [*] Virtualization ---> General architecture-dependent options --->
- [*] Enable loadable module support --->
- [*] Enable the block layer ---> IO Schedulers ---> Executable file formats ---> Memory Management options ---> [*] Networking support ---> v(+)



```
Linux/x86 5.4.0 Kernel Configuration
```

```
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus
----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc> to exit, <?> for Help, </> for
Search. Legend: [*] built-in [] excluded <M> module < > module capable
```

```
Power management and ACPI options --->
                                              < Load >
                         < Help >
                                     < Save >
```

Configurability Makes Maintenance Harder

given a patch, what configurat given a bug, what configurat what's a minimal configuration th what code is no longer configura

- given a patch, what configurations does it affect? (jmake, lawall et al)
 - given a bug, what configurations does it appear in? (config-bisect)
- what's a minimal configuration that includes specific source? (config-bisect)
- what code is no longer configurable in the kernel? (undertaker, tarlet et al)

There's About 15,000 Configuration Options

General setup ---> [*] 64-bit kernel Processor type and features ---> Power management and ACPI options ---> Bus options (PCI etc.) ---> Binary Emulations ---> Firmware Drivers ---> [*] Virtualization ---> General architecture-dependent options ---> [*] Enable loadable module support ---> [*] Enable the block layer ---> IO Schedulers ---> Executable file formats ---> Memory Management options ---> [*] Networking support --->



```
Linux/x86 5.4.0 Kernel Configuration
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus
----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc> to exit, <?> for Help, </> for
Search. Legend: [*] built-in [] excluded <M> module < > module capable
```

```
*** Compiler: gcc (Ubuntu 9.2.1-9ubuntu2) 9.2.1 20191008 ***
```

```
< Load >
< Help >
            < Save >
```



Written in about 150,000 Lines of Kconfig

there's around 1,500 Kconfig files

arch/arm/mach-exynos/Kconfig	./drivers/char/ipvi/Kconfig	./drivers/lio/temperature/Kconfig	./drivers/net/calf/Kc
arch/arm/mach-footbridge/Kconfig	./drivers/char/Kconfig	./drivers/lio/trigger/Kconfig	./drivers/net/can/cc7
arch/arm/mach-gemini/Kconfig	/drivers/char/pcmcia/Kconfig	./drivers/infiniband/hs/boxt_re/Kconfig	./drivers/net/can/c_c
arch/arn/mach-highbank/Kconfig	./drivers/char/tpn/Kconfig	./drivers/infiniband/hw/cxgb4/Kconfig	./drivers/net/can/ifi
arch/arm/mach-hisi/Kconfig	./drivers/char/tpn/st33zp24/Kconfig	./drivers/infiniband/he/efa/Kconfig	./drivers/net/can/Kco
arch/arm/mach-inx/devices/Kconfig	./drivers/char/xillybus/Kconfig	./drivers/infiniband/he/hfil/Kconfig	./drivers/net/can/m_c
arch/arm/mach-inx/Kconfig	/drivers/clk/actions/Kconfig	./drivers/infiniband/hs/hns/Kconfig	./drivers/net/can/msc
arch/arm/mach-integrator/Kconfig	./drivers/clk/analogbits/Kconfig	/drivers/infiniband/hs/1401s/Kconfig	./drivers/net/can/pea
arch/arm/mach-lop32x/Kconfig	./drivers/clk/baikal-t1/Kconfig	./drivers/infiniband/hs/vix4/Kconfig	./drivers/net/can/rca
arch/arm/mach-txp4xx/Kconfig arch/arm/mach-keystone/Kconfig	./drivers/clk/bcm/Kconfig ./drivers/clk/hisilicon/Kconfig	./drivers/infiniband/hw/mlx5/Kconfig ./drivers/infiniband/hw/mthca/Kconfig	./drivers/net/can/sja ./drivers/net/can/sof
arch/arm/nach-1pc32xx/Kconf1g	./drivers/clk/ingtec/Kconfig	./drivers/infiniband/hw/ocrdma/Kconfig	./drivers/net/can/spi
arch/arm/mach-mediatek/Kconfig	./drivers/clk/ins/Kconfig	./drivers/infiniband/hw/gedr/Kconfig	./drivers/net/can/usb
arch/arm/mach-meson/Kconfig	./drivers/clk/ingenic/Kconfig	./drivers/infiniband/hw/gib/Kconfig	./drtvers/net/das/b53
arch/arm/mach-wilbeaut/Kconfig	/drivers/clk/Kconfig	./drivers/infiniband/he/usnic/Kconfig	./drivers/net/dss/Kco
arch/arn/mach-mmp/Kconfig	./drivers/clk/keystone/Kconfig	./drivers/infiniband/hs/vms_pvrdma/Kconfig	./drivers/net/dss/wic
arch/arm/mach-moxart/Kconfig	./drivers/clk/mediatek/Kconfig	./drivers/infiniband/Kconfig	./drtvers/net/daa/ev8
arch/arm/mach-matar/Econfig	./drivers/clk/neson/Kconfig	./drivers/infiniband/ss/rdnavt/Kconfig	./drivers/net/dss/oce
arch/arm/mach-mv78xx8/Kconfig	./drivers/clk/wwebu/Kconfig	/drivers/infiniband/sw/rxe/Kconfig	./drivers/net/dsa/qca
arch/arm/mach-nvebu/Kconfig	./drivers/clk/qcon/Kconfig	./drivers/infiniband/ss/sis/Kconfig	./drivers/net/dss/sja
arch/arm/mach-mox/Kconfig arch/arm/mach-nomadik/Kconfig	./drivers/clk/renesas/Kconfig ./drivers/clk/samsung/Kconfig	./drivers/infiniband/ulp/ipoib/Kconfig ./drivers/infiniband/ulp/iser/Kconfig	./drivers/net/etherne ./drivers/net/etherne
arch/arn/nach-npcn/Kconfig	./drivers/clk/sifive/Kconfig	./drivers/infiniband/ulp/isert/Kconfig	./drivers/net/etherne
arch/arm/mach-mapire/Kconfig	./drivers/clk/sprd/Kconfig	./drivers/infiniband/ulp/ops_vnic/Kconfig	./drivers/net/etherne
arch/arm/mach-onap1/Kconfig	./drivers/clk/sunxi/Kconfig	./drivers/infiniband/ulp/rtrs/Kconfig	./drtvers/net/etherne
arch/arm/mach-onap2/Kconfig	./drivers/clk/sunsi-ng/Kconfig	./drivers/infiniband/ulp/srp/Kconfig	./drivers/net/etherne
arch/arn/mach-orion5x/Roonfig	./drivers/clk/tegrs/Kconfig	./drivers/infiniband/ulp/srpt/Kconfig	./drivers/net/etherne
arch/arn/mach-oxnas/Kconfig	./drivers/clk/ti/Kconfig	./drivers/input/gameport/Kconfig	./drivers/net/etherne
arch/arm/mach-picoxcs/ll/Kconfig	./drivers/clk/uniphier/Kconfig	./drivers/input/joystick/iforce/Kconfig	./drtvers/net/etherne
arch/arn/mach-prima2/Kconfig	./drivers/clk/versatile/Kconfig	./drivers/input/joystick/Kconfig	./drivers/net/etherne
arch/arn/mach-pxa/Kconfig	./drivers/clk/x86/Kconfig	./drivers/input/Kconfig	./drivers/net/etherne
arch/arm/mach-ocom/Kconfig	./drivers/clk/zyngnp/Kconfig	/drivers/input/keyboard/Kconfig	./drivers/net/etherne
arch/arm/mach-rda/Kconfig	./drivers/clocksource/Kconfig	./drivers/input/wisc/Kconfig	./drivers/net/etherne
arch/arm/mach-realtek/Kconfig arch/arm/mach-realview/Kconfig	./drivers/connector/Kconfig ./drivers/counter/Kconfig	./drivers/input/nouse/Kconfig ./drivers/input/rwi4/Kconfig	./drivers/net/etherne ./drivers/net/etherne
arch/arm/wach-rockchip/Kconfig	./drivers/cpufreg/Kconfig	./drivers/input/serio/Kconfig	./drivers/net/etherne
arch/arn/nach-13c24xx/Kconfig	./drivers/cpufreg/Kconfig.arm	./drivers/input/tablet/Kconfig	./drivers/net/etherne
arch/arn/nach-s3c64xx/Kconfig	./drivers/cpufreg/Kconfig.powerpc	./drivers/input/touchscreen/Kconfig	./drivers/net/etherne
arch/arn/mach-s5pv210/Kconfig	/drivers/cpufreg/Kconfig.x86	./drivers/interconnect/inx/Kconfig	./drivers/net/etherne
arch/arm/mach-sal108/Kconfig	./drivers/cpuidle/Kconfig	./drivers/interconnect/Kconfig	./drivers/net/etherne
arch/arm/mach-shmobile/Kconfig	./drivers/cpuidle/Kconfig.arm	./drivers/interconnect/gcom/Kconfig	./drivers/net/etherne
arch/arm/mach-socfpga/Kconfig	/drivers/cpuidle/Kconfig.wips	./drivers/ionnu/and/Kconfig	./drivers/net/etherne
arch/arm/mach-spear/Kconfig	./drivers/cpuidle/Kconfig.powerpc	/drivers/ionmu/intel/Kconfig	./drivers/net/etherne
arch/arm/mach-sti/Kconfig	./drivers/crypto/allarinner/Kconfig	./drivers/ionnu/Kconfig	./drivers/net/etherne
arch/arm/wach-stn32/Kconfig	./drivers/crypto/anlogic/Kconfig	./drivers/ipack/carriers/Kconfig ./drivers/ipack/devices/Kconfig	./drivers/net/etherne ./drivers/net/etherne
arch/arn/nach-sunxt/Kconfig arch/arn/nach-tango/Kconfig	./drivers/crypto/caan/Kconfig ./drivers/crypto/caviun/cpt/Kconfig	./drivers/ipack/Kconfig	./drivers/net/etherne
arch/arm/wach-tegra/Kconftg	./drivers/crypto/caviam/nitrox/Kconfig	./drivers/irgchip/Kconfig	./drtvers/net/etherne
arch/arm/wach-u300/Kconfig	./drivers/crypto/ccp/Kconfig	./drivers/isdn/capi/Kconfig	./drivers/net/etherne
arch/arm/mach-uniphier/Kconfig	./drivers/crypto/chelsio/Kconfig	/drivers/isdn/hardware/wiSDN/Kconfig	./drivers/net/etherne
arch/arn/nach-ux500/Kconfig	/drivers/crypto/hisilicon/Kconfig	./drivers/isdn/Kconfig	./drivers/net/etherne
arch/arm/mach-versatile/Kconfig	./drivers/crypto/Kconfig	./drivers/isdn/wISDN/Kconfig	./drivers/net/etherne
arch/arm/mach-vexpress/Kconfig	./drivers/crypto/marvell/Kconfig	./drivers/Kconfig	./drivers/net/etherne
arch/arm/wach-vt8500/Kconfig	/drivers/crypto/nx/Kconfig	./drivers/leds/Kconfig	./drivers/net/etherne
arch/arm/mach-zx/Kconfig	./drivers/crypto/gat/Kconfig	./drivers/leds/trigger/Kconfig	./drivers/net/etherne
arch/arm/mach-zyng/Kconfig	./drivers/crypto/str/32/Kconfig	./drivers/lightnvm/Kconfig	./drivers/net/etherne
arch/arm/wm/Kconfig arch/arm/plat-omap/Kconfig	./drivers/crypts/ux500/Kconfig ./drivers/crypts/virtio/Kconfig	./drivers/wacintosh/Kconfig ./drivers/wailbox/Kconfig	./drivers/net/etherne ./drivers/net/etherne
arch/arm/plat-pxa/Kconfig	./drivers/crypto/ves/Kconfig	./drivers/mcb/Kconfig	./drtvers/net/etherne
arch/arm/plat-samsung/Kconfig	./drivers/dax/Kconfig	/drivers/md/bcache/Kconfig	./drivers/net/etherne
arch/c6x/Kconfig	./drivers/dcs/Kconfig	./drivers/wd/Kconfig	./drivers/net/etherne
arch/ctx/Kconfig.debug	/drivers/devfreg/event/Kconfig	./drivers/wd/persistent-data/Kconfig	./drivers/net/etherne
arch/c6x/platforms/Kconfig	./drivers/devfreg/Kconfig	./drivers/media/cec/12c/Kconfig	./drtvers/net/etherne
arch/caky/Kconflg	./drivers/dns/bestconn/Kconfig	./drivers/media/cec/Kconfig	./drivers/net/etherne
arch/csky/Kconfig.debug	./drivers/dna-buf/heaps/Kconfig	./drivers/media/cec/platform/Kconfig	./drivers/net/etherne
arch/caky/Kconfig.platforms	/drivers/dws-buf/Kconfig	./drivers/media/cec/usb/Kconfig	./drivers/net/etherne
arch/h6300/Kconfig	./drivers/dma/dw-edma/Rconfig	/drivers/wedia/cec/usb/pulses/Kconfig	./drivers/net/etherne
arch/h8388/Kconfig.cpu	./drivers/dns/ds/Kconfig	./drivers/media/cec/usb/rainshadow/Kconfig	./drivers/net/etherne
arch/h8366/Kconfig.debug	./drivers/dns/fs1-dpss2-gdns/Kconfig	./drivers/media/common/b2c2/Kconfig ./drivers/media/common/Kconfig	./drivers/net/etherne
arch/hexagon/Kconfilg arch/hexagon/Kconfilg.debug	./drivers/dms/ksu/Kconfig ./drivers/dms/Kconfig	./drivers/media/common/sconfig ./drivers/media/common/saa7146/Kconfig	./drivers/net/etherne ./drivers/net/etherne
arch/ta64/Kconftg	./drivers/dna/wediatek/Kconfig	./drivers/wedia/common/stano/Kconfig	./drtvers/net/etherne
arch/1a64/Kconfig.debug	./drivers/dna/gcon/Kconfig	./drivers/media/common/v412-tpg/Kconfig	./drtvers/net/etherne
arch/Kconfig	./drivers/dna/sf-pdna/Kconfig	./drivers/media/common/videobuf2/Kconfig	./drivers/net/etherne
arch/mblik/Kconfig	./drivers/dma/sh/Kconfig	./drivers/media/dvb-core/Kconfig	./drivers/net/etherne
arch/w68k/Kconfig.bus	./drivers/dns/ti/Kconfig	./drivers/media/dvb-frontends/cxd2880/Kconfig	./drivers/net/etherne
arch/m68k/Kconfig.cpu	./drivers/edac/Kconfig	./drivers/media/dvb-frontends/drx59xyj/Kconfig	./drivers/net/etherne
arch/nölik/Kconfig.debug	./drivers/eisa/Kconfig	./drivers/media/dvb-frontends/Kconfig	./drivers/net/etherne
arch/m68k/Kconfig.devices	./drivers/extcon/Kconfig	./drivers/media/firewire/Kconfig	./drivers/net/etherne
arch/m68k/Kconfig.machine	./drivers/firewire/Kconfig	./drivers/media/12c/cx25848/Kconfig	./drivers/net/etherne
arch/wicroblaze/Kconfig	./drivers/firmware/broadcon/Kconfig	./drivers/media/i2c/etBekB/Kconfig	./drivers/net/etherne
arch/wicroblaze/Kconfig.debug	./drivers/fireware/efi/Kconfig	./drivers/media/12c/Kconfig	./drivers/net/etherne
arch/wicroblaze/Kconfig.platform arch/wicroblaze/Kconfig.platform	./drivers/firmware/google/Kconfig ./drivers/firmware/ins/Kconfig	. /drivers/media/i2c/nSnois/Kconfig Detwars/media/i2c/antans/Kconfig	./drivers/net/etherne /drivers/net/etherne
arch/wips/alcheny/Rconfig arch/mips/ath25/Rconfig	deixers (Firmare/Wewfin	./drivers/media/12c/smiapp/Kconfig /drivers/media/Kconfig	./drivers/net/etherne

. /drivers/usb/wisc/itsusby . /drivers/usb/mon/Kconfig . /drivers/usb/musb/Kconfig . /drivers/usb/musb/Kconfig mediatek/Kconfig mellanox/Kconfig ./drtvers/platform/x86/Kconft ./drivers/pnp/isapnp/Kconfig ./drivers/pnp/Kconfig ./drivers/pnp/pnpacpi/Kconfig ./drivers/pnp/pnpbios/Kconfig ./drivers/pnp/pnpbios/Kconfig ./drivers/power/avs/Kconfig ellanox/wlx4/Kconfig ellanox/wlx5/core/Kc ./drivers/usb/phy/Kconfig ./drivers/usb/renesas_usbhs/N ./drivers/usb/roles/Kconfig Lanox /alx fa /Kconfig crel/Kconfig

./net/wirelean/Kconfig ./net/x25/Kconfig ./net/xdp/Kconfig /scripts/gcc-plugins/Kconfig /scripts/Kconfig.include

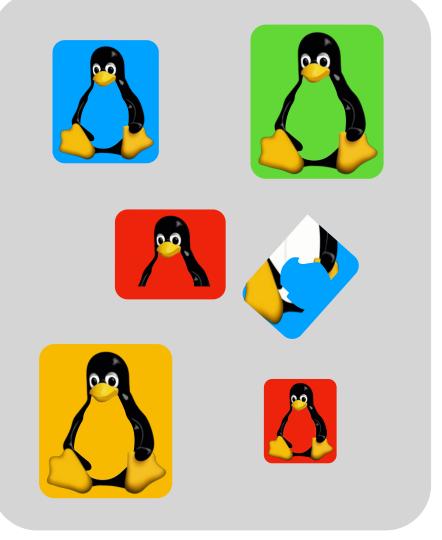


Can Have Trillions of Program in One Codebase

Allows system builders to reuse existing software



Configuration options enable/disable features



Linux build system generates many variations



Build customized software without reprogramming

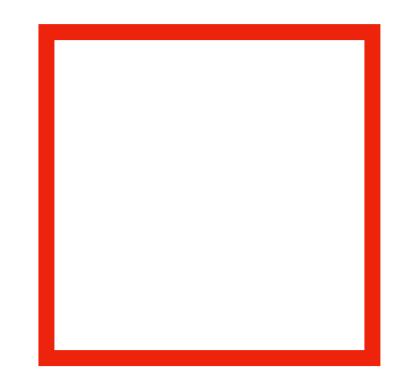


Configurability Complicates Maintenance



Linux source code

Testing infrastructure



- Even if one variant program is correct, another might be broken
- Have to test all variations that might be used
- Automated testing typically works on one variant at a time





The Linux Kernel has a Very Active Codebase

Linux-next commit history

	ndex : kernel/git/next/linux-next.git		(in	aster 🗢 💽 Linux Next
out sur	nmary refs log tree commit diff stats	log	msg ≎	Q
Jut Sul	innary fold log too commit an state			
ge	Commit message (Expand)	Author	Files	Lines
hours	Add linux-next specific files for 20240213 HEAD next-20240213 master	Stephen Rothwell	4	-0/+9642
hours	fixup for "drm/amd: Stop evicting resources on APUs in suspend"	Stephen Rothwell	1	-1/+1
hours	Merge branch 'for-next/kspp' of git://git.kernel.org/pub/scm/linux/kernel/git	Stephen Rothwell	45	-185/+336
hours	Merge branch 'bitmap-for-next' of https://github.com/norov/linux.git	Stephen Rothwell	49	-417/+634
hours	Merge branch 'for-next/execve' of git://git.kernel.org/pub/scm/linux/kernel/g	Stephen Rothwell	1	-1/+1
hours hours	Merge branch 'rust-next' of https://github.com/Rust-for-Linux/linux.git Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/mic/linu	Stephen Rothwell Stephen Rothwell	14	-49/+177
hours	Merge branch 'slab/for-next' of git://git.kernel.org/pub/scm/linux/kernel/git	Stephen Rothwell	16 7	-91/+1183 -126/+115
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/kris	Stephen Rothwell	3	-20/+42
hours	Merge branch 'zstd-next' of https://github.com/terrelln/linux.git	Stephen Rothwell	58	-2594/+4789
hours	Merge branch 'mhi-next' of git://git.kernel.org/pub/scm/linux/kernel/git/mani	Stephen Rothwell	9	-88/+423
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/srin	Stephen Rothwell	6	-69/+83
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/srin	Stephen Rothwell	1	-4/+4
hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/joel/fsi	Stephen Rothwell	2	- <mark>2/</mark> +18
hours	Merge branch 'for-next/seccomp' of git://git.kernel.org/pub/scm/linux/kernel/	Stephen Rothwell	3	-14/+73
hours	Merge branch 'ntb-next' of https://github.com/jonmason/ntb.git	Stephen Rothwell	2	- <mark>2</mark> /+2
hours	Merge branch 'libnvdimm-for-next' of git://git.kernel.org/pub/scm/linux/kerne	Stephen Rothwell	3	-3/+3
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/live	Stephen Rothwell	0	-0/+0
hours	Merge branch 'kunit' of git://git.kernel.org/pub/scm/linux/kernel/git/shuah/l	Stephen Rothwell	2	-3/+4
hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/shuah/li	Stephen Rothwell	32	-121/+340
hours	Merge branch 'pwm/for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/	Stephen Rothwell	12	-384/+373
hours	Merge branch 'renesas-pinctrl' of git://git.kernel.org/pub/scm/linux/kernel/g	Stephen Rothwell	4	-53/+276
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/linu	Stephen Rothwell	24	- <mark>94/+13</mark> 0
hours	Merge branch 'gpio/for-next' of git://git.kernel.org/pub/scm/linux/kernel/git	Stephen Rothwell	46	- <mark>626/+2510</mark>
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/remo	Stephen Rothwell	12	-193/+271
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/mkp/	Stephen Rothwell	24	-883/+727
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/jejb	Stephen Rothwell	43	-471/+1385
hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/tj/c	Stephen Rothwell	1	- <mark>8/</mark> +12
hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/vkoul/dm	Stephen Rothwell	15	-242/+615
0 hours	Merge branch 'counter-next' of git://git.kernel.org/pub/scm/linux/kernel/git/	Stephen Rothwell	2	- <mark>2/</mark> +1
0 hours	Merge branch 'staging-next' of git://git.kernel.org/pub/scm/linux/kernel/git/	Stephen Rothwell	38	-4359/+168
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/krzk	Stephen Rothwell	3	-2/+61
0 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/vkoul/so	Stephen Rothwell	2	-4/+2
0 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/phy/linu Merge branch 'togreg' of git://git.kernel.org/pub/scm/linux/kernel/git/jic23/	Stephen Rothwell	40	-1257/+3441 -455/+2724
0 hours 0 hours		Stephen Rothwell	67	
0 hours	Merge branch 'icc-next' of git://git.kernel.org/pub/scm/linux/kernel/git/djak Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/fpga	Stephen Rothwell Stephen Rothwell	12 4	-1116/+1599 -54/+104
0 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/coresigh	Stephen Rothwell	30	-803/+1377
0 hours	Merge branch 'habanalabs-next' of git://git.kernel.org/pub/scm/linux/kernel/git/vigit.kernel.org/pub/scm/linux/kernel/g	Stephen Rothwell	13	-396/+899
0 hours	Merge branch 'char-misc-next' of git://git.kernel.org/pub/scm/linux/kernel/gi	Stephen Rothwell	6	-10/+35
0 hours	Merge branch 'tty-next' of git://git.kernel.org/pub/scm/linux/kernel/git/greg	Stephen Rothwell	67	-1615/+2168
0 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/westeri/	Stephen Rothwell	12	-50/+278
0 hours	Merge branch 'usb-next' of git://git.kernel.org/pub/scm/linux/kernel/git/greg	Stephen Rothwell	77	-1038/+5655
0 hours	Merge branch 'driver-core-next' of git://git.kernel.org/pub/scm/linux/kernel/	Stephen Rothwell	7	-22/+37
0 hours	Merge branch 'for-leds-next' of git://git.kernel.org/pub/scm/linux/kernel/git	Stephen Rothwell	22	-181/+613
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/sre/	Stephen Rothwell	1	-1/+1
0 hours	Merge branch 'for-firmware-next' of git://git.kernel.org/pub/scm/linux/kernel	Stephen Rothwell	1	-1/+1
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/pdx8	Stephen Rothwell	19	-244/+669
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/tj/w	Stephen Rothwell	9	-302/+1284
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/denn	Stephen Rothwell	0	<mark>-0/+</mark> 0
0 hours	Merge branch 'next' of https://github.com/kvm-x86/linux.git	Stephen Rothwell	85	-745/+1631
0 hours	Merge branch 'riscv_kvm_next' of https://github.com/kvm-riscv/linux.git	Stephen Rothwell	2	-11/+15
0 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/kvmarm/k	Stephen Rothwell	28	- <mark>84</mark> /+247
) hours	scsi: core: Make scsi_bus_type const	Ricardo B. Marliere	2	-2/+2
) hours	Merge branch kvm-arm64/misc into kvmarm/next	Oliver Upton	1	-1/+1
) hours	Merge branch 'rcu/next' of git://git.kernel.org/pub/scm/linux/kernel/git/paul	Stephen Rothwell	32	-564/+841
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/trac	Stephen Rothwell	0	-0/+0
0 hours	Merge branch 'edac-for-next' of git://git.kernel.org/pub/scm/linux/kernel/git	Stephen Rothwell	27	-295/+3949
0 hours	Merge branch 'timers/drivers/next' of git://git.linaro.org/people/daniel.lezc	Stephen Rothwell	5	-7/+22
0 hours	Merge branch 'master' of git://git.kernel.org/pub/scm/linux/kernel/git/tip/ti	Stephen Rothwell	204	-1114/+4829
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/broo	Stephen Rothwell	65	-586/+1037
0 hours	KVM: selftests: Print timer ctl register in ISTATUS assertion	Oliver Upton	1	-1/+1
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/krzk	Stephen Rothwell	4	-9/+9
0 hours	Merge branch 'for-next' of git://git.kernel.org/pub/scm/linux/kernel/git/robh	Stephen Rothwell	21	-652/+661
0 hours	scsi: core: Really include kunit tests with SCSI_LIB_KUNIT_TEST	Lukas Bulwahn	1	-1/+1
0 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/pcmoore/	Stephen Rothwell	2	-4/+2
0 hours 0 hours	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/joro/iom	Stephen Rothwell	9	-483/+457
UNDURS	Merge branch 'next' of git://git.kernel.org/pub/scm/linux/kernel/git/jarkko/l	Stephen Rothwell	1	- <mark>3/+3</mark>

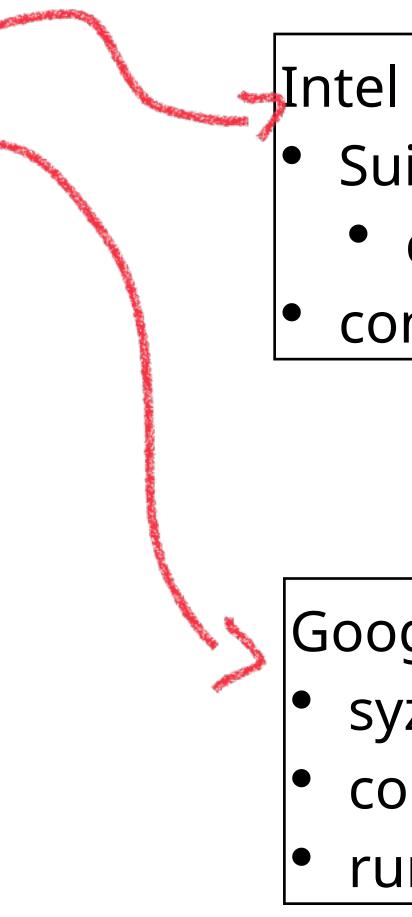
~30k mailing list messages per month

~6k commits per month, 100s per day

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

All These Code Changes Need Testing

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%			
C					



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

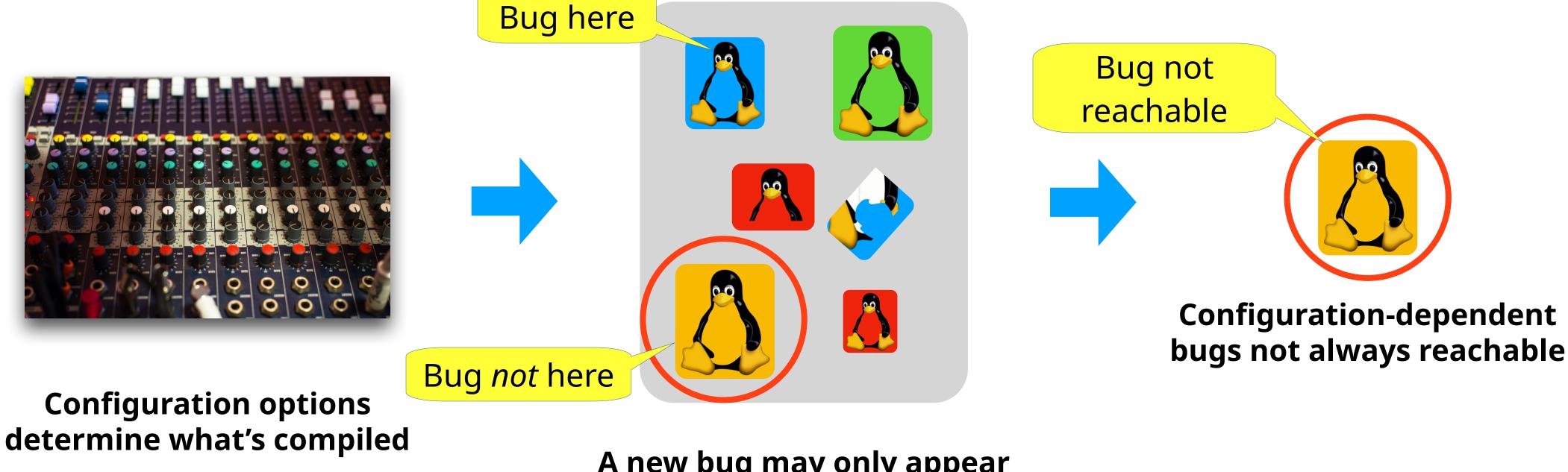
Intel 0-day kernel test robot
Suite of static and dynamic testing tools
compile, boot, performance, etc.
continuously runs on new commits in linux-next

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

The Build System Causes Blindspots in Testing



Code Hidden by the Build System

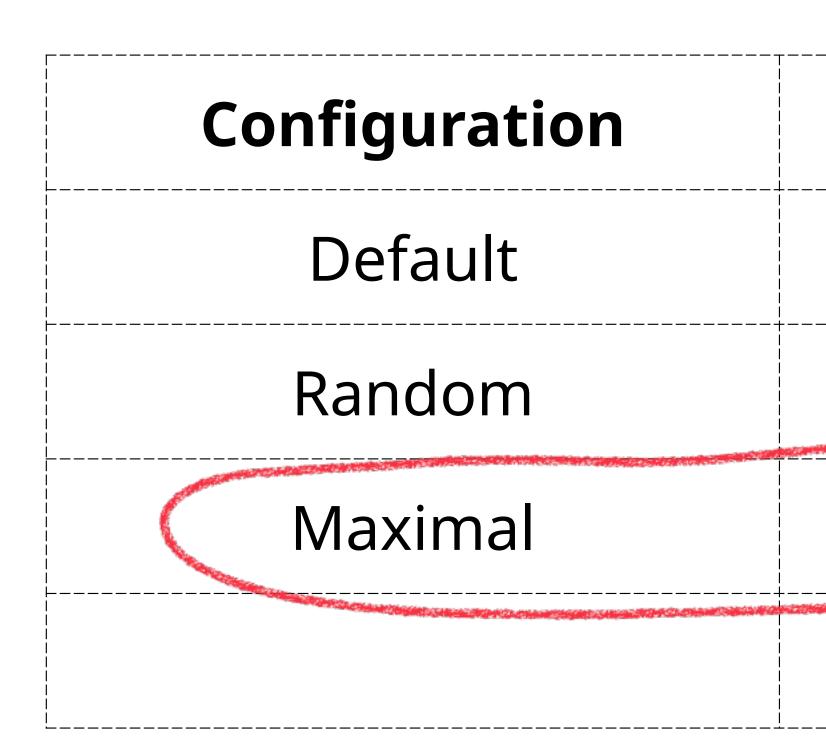


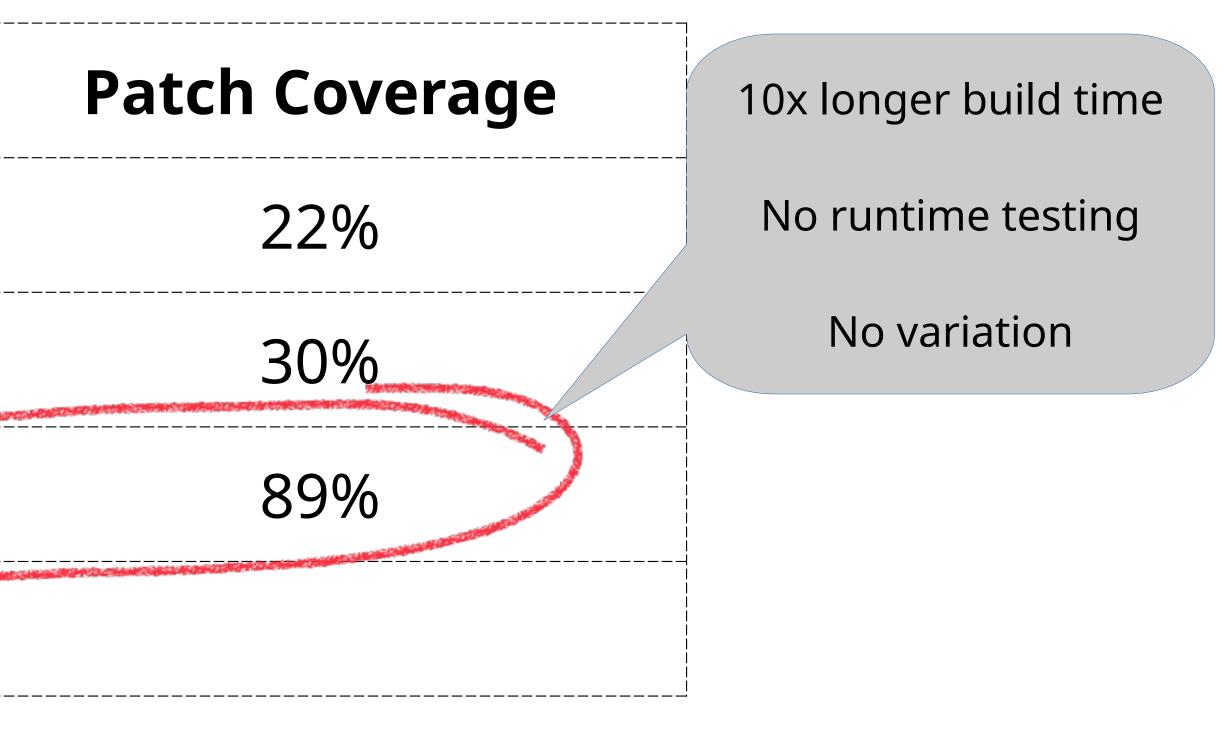
A new bug may only appear in some configurations





Test Robots Miss Most Code Changes

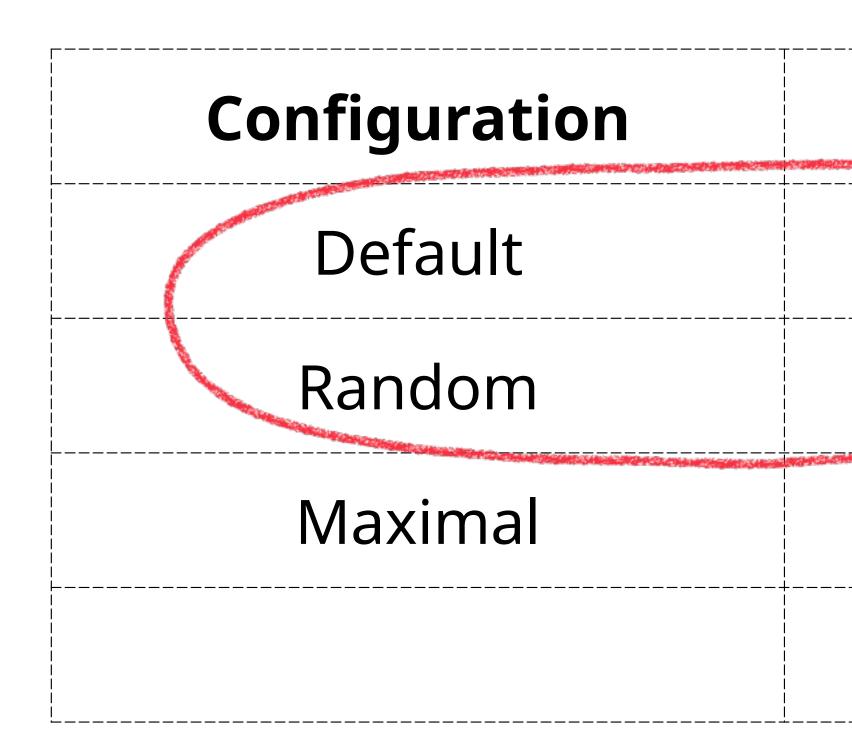


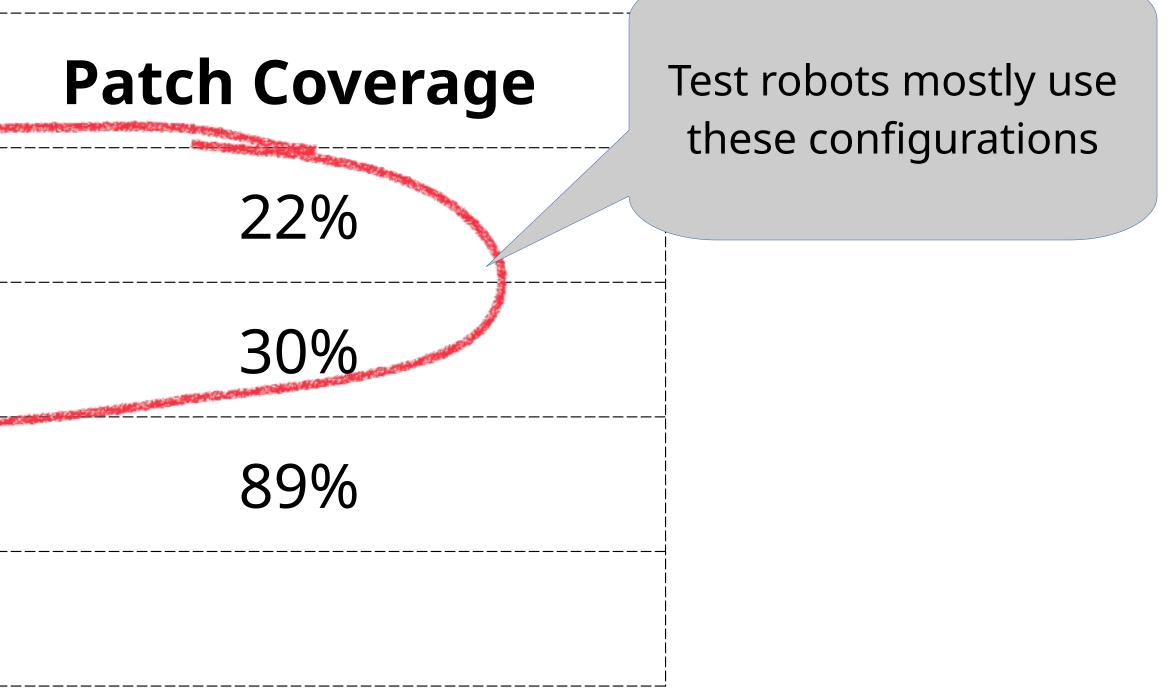






Test Robots Miss Most Code Changes



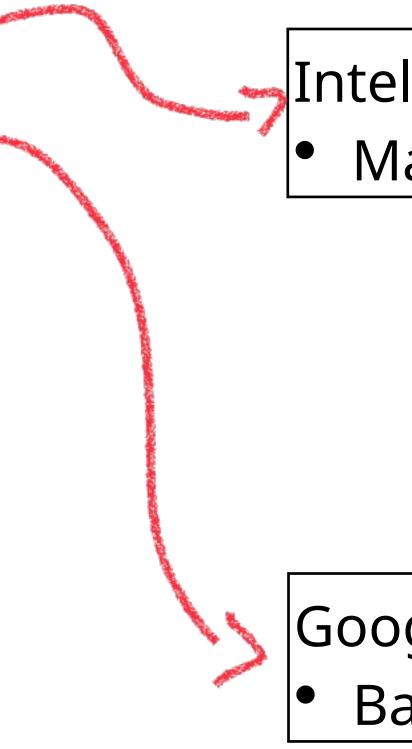






Maximal Testing is Limited

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%				



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

Intel 0-day kernel test robotMaximal only for build test

Google syzbotBased on default configuration

Build System Turns Configurations into Binaries

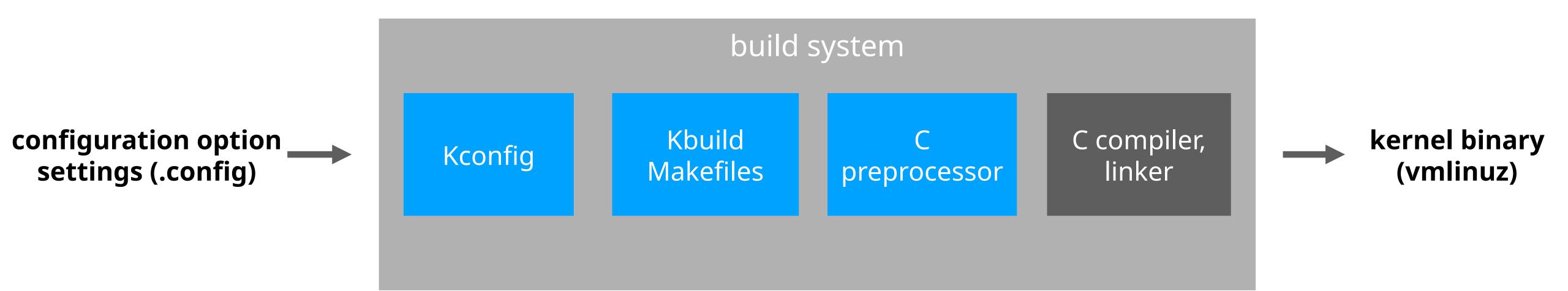
configuration option _____ settings (.config)

build system

kernel binary (vmlinuz)



Build System Comprises Several Tools

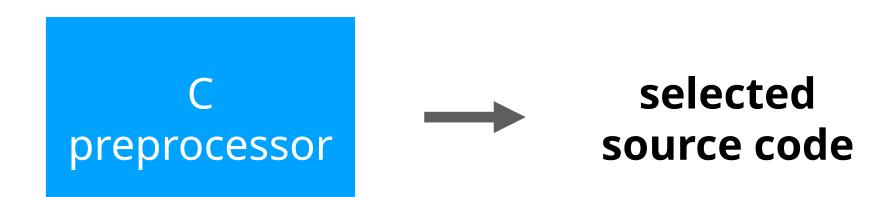


Build System Comprises Several Tools

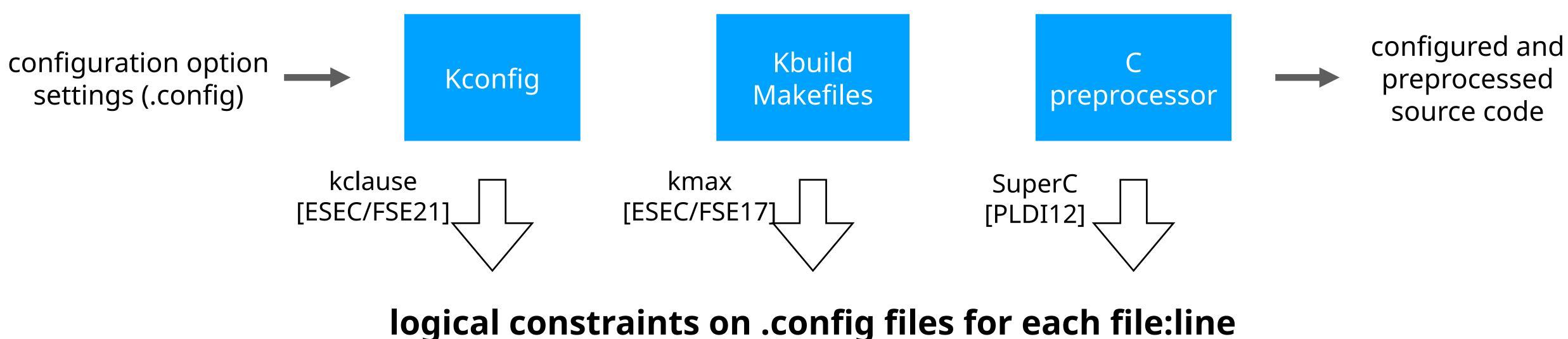
configuration option _____ K settings (.config)

Kconfig

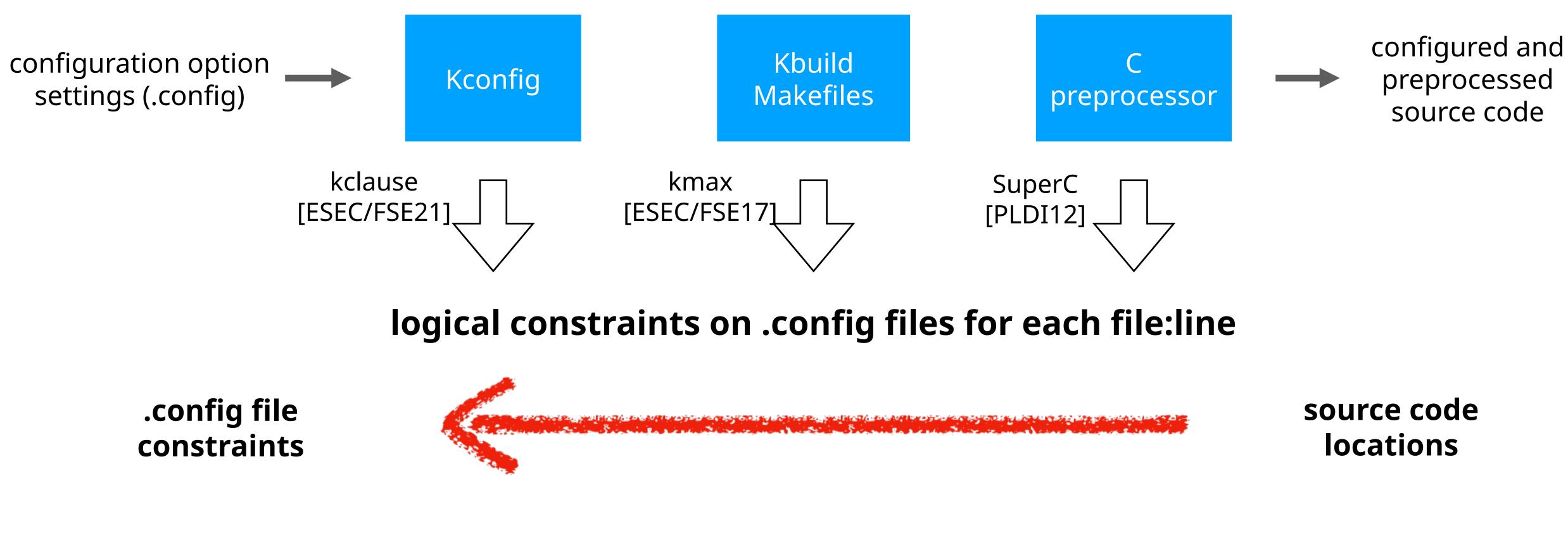




Use Program Analysis on Build Tools



Formally Model Build System Behavior



Applications

- kismet [ESEC/FSE21] -Automatically find Linux Kconfig bugs
- krepair [FSE24]

-Automatically change configuration files to cover patched code





Conclusion

- Current testing and analysis focuses on program code
- The software ecosystem broadens the attack surface beyond code
- Misconfigurations are one of the most critical vulnerabilities
- Our approach: formal model and test configurations
- Applications: find configuration bugs, improve testing



