16 Мая 2012, Москва

LinuxTesting.org

Верификация драйверов устройств ядра Linux

Вадим Мутилин
mutilin@ispras.ru

ISP RAS

Institute for System Programming of the Russian Academy of Sciences

Статистика ядра Linux (1)

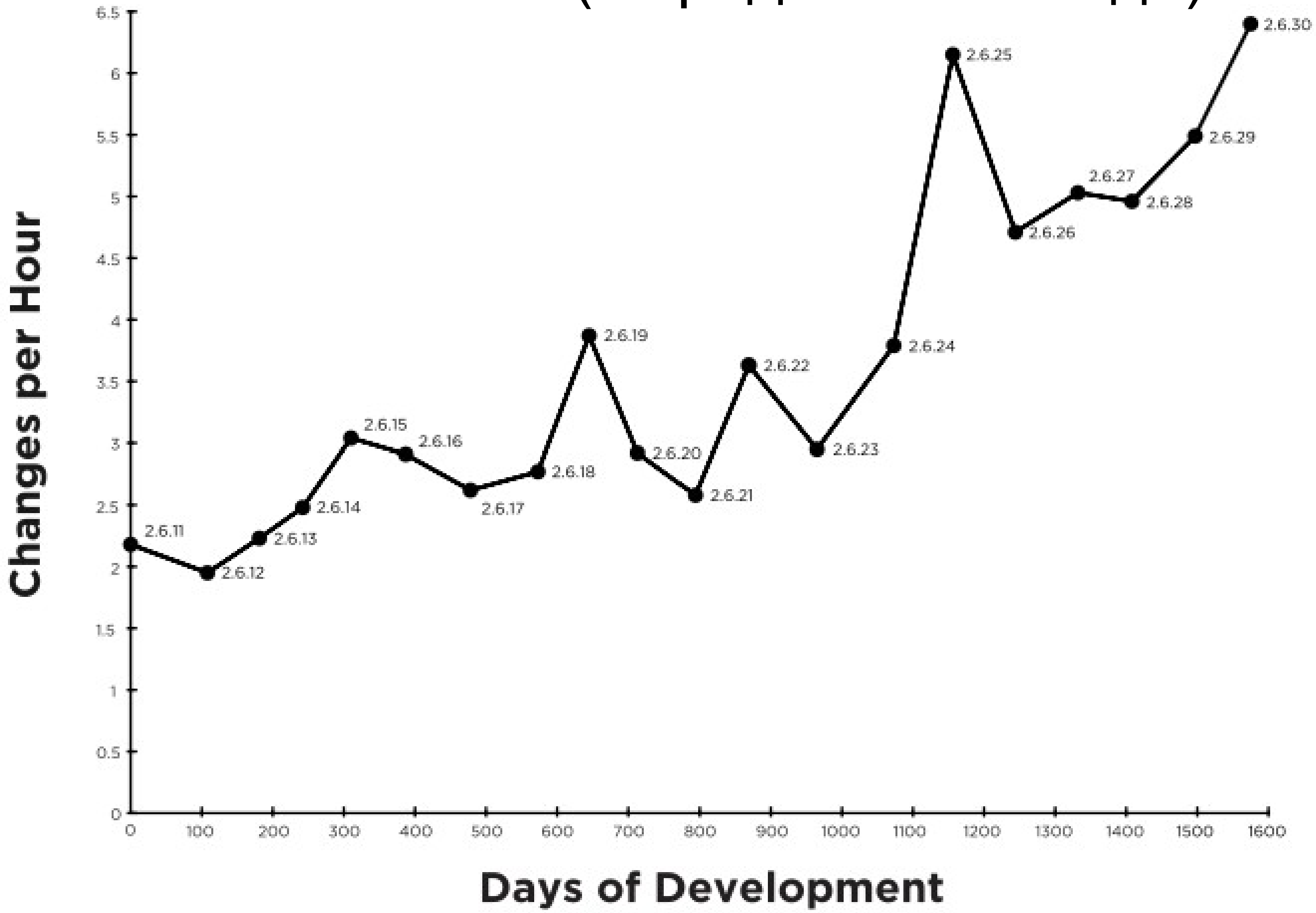
- Более 1000 активных разработчиков

Kernel Version	Number of Developers	Number of Known Companies
2.6.11	389	68
2.6.12	566	90
2.6.13	545	94
2.6.14	553	90
2.6.15	612	108
2.6.16	709	111
2.6.17	726	120
2.6.18	815	133
2.6.19	801	128
2.6.20	673	138
2.6.21	767	143
2.6.22	870	180
2.6.23	912	181
2.6.24	1,057	194
2.6.25	1,123	228
2.6.26	1,027	203
2.6.27	1,021	188
2.6.28	1,075	213
2.6.29	1,180	230
2.6.30	1,150	240
All	4,910	532

[*] Kroah-Hartman G, Corbet J, McPherson A (December 2010) Linux Kernel Development https://www.linuxfoundation.org/sites/main/files/lf_linux_kernel_development_2010.pdf

Статистика ядра Linux (2)

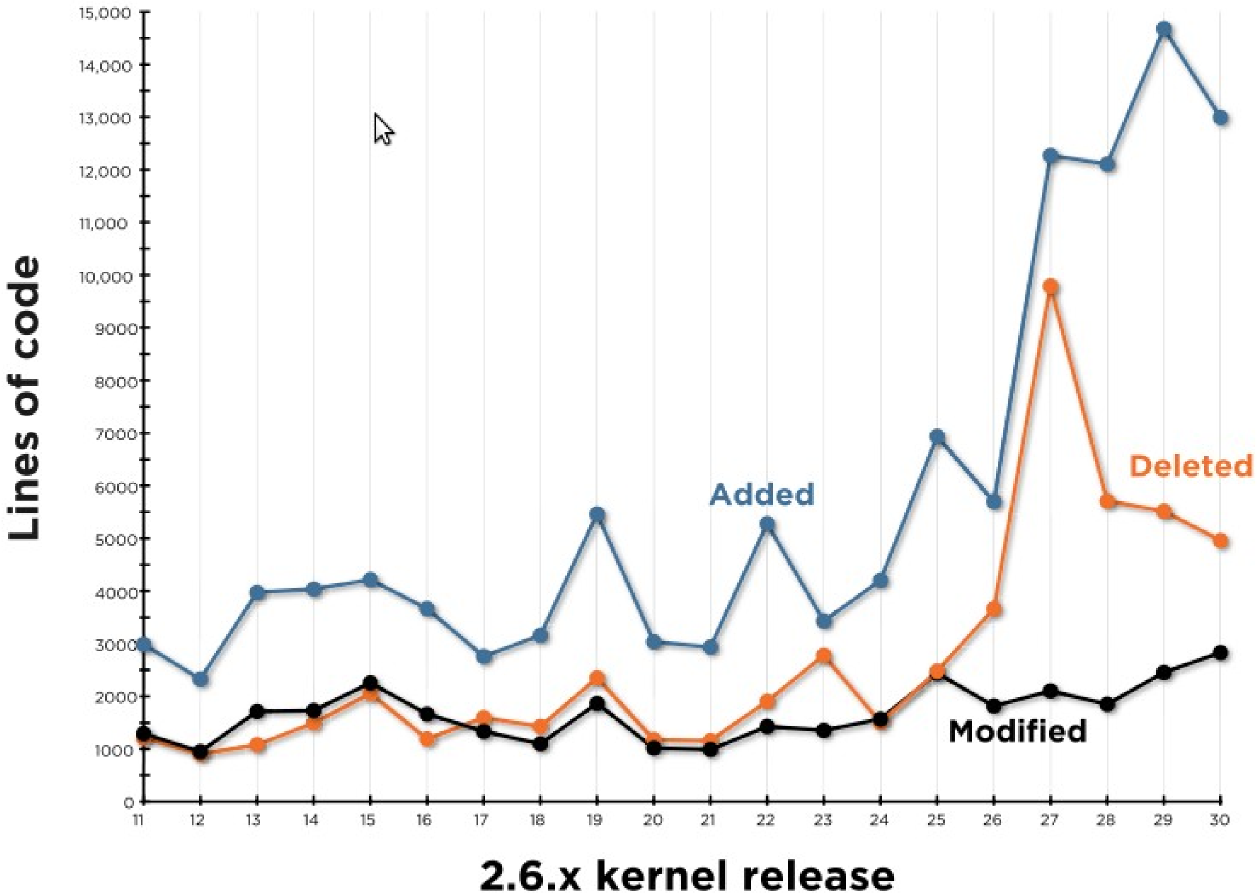
- 3.83 патчей в час (в среднем за 4 года)



[*] Kroah-Hartman G, Corbet J, McPherson A (2009) Linux Kernel Development
http://www.linux-foundation.org/publications/whowriteslinux.pdf

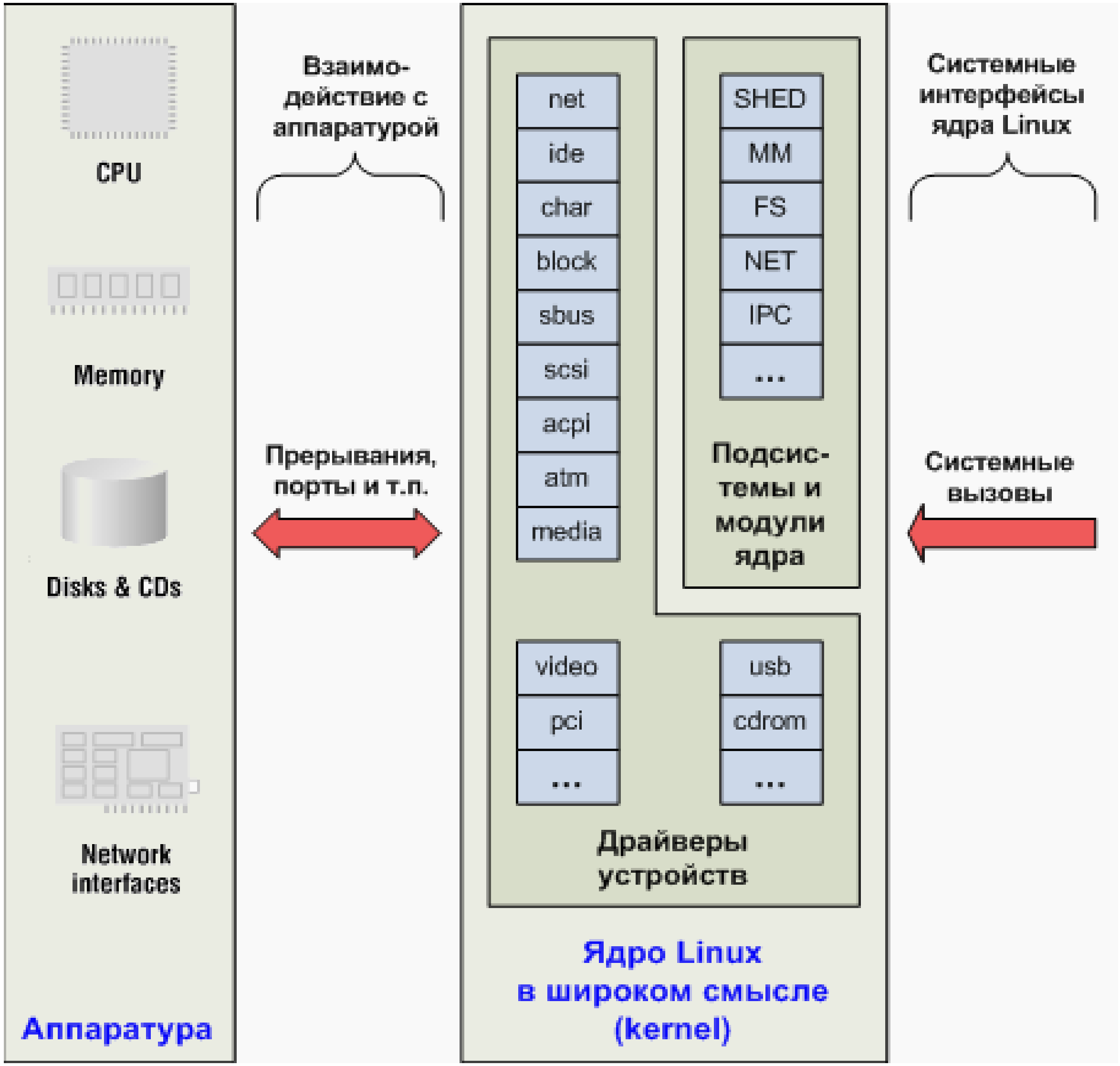
Статистика ядра Linux (3)

- 6422 добавл./3285 удал./1687 измен. ежедневно



[*] Kroah-Hartman G, Corbet J, McPherson A (2009) Linux Kernel Development
http://www.linux-foundation.org/publications/whowriteslinux.pdf

Ядро Linux


CPU
Memory
Disks & CDs
Network interfaces
Аппаратура
Взаимо-действие с аппаратурой
Прерывания, порты и т.п.
net
ide
char
block
sbus
scsi
acpi
atm
media
SHED
MM
FS
NET
IPC
...
Подсис-темы и модули ядра
video
pci
...
usb
cdrom
...
Драйверы устройств
Ядро Linux в широком смысле (kernel)
Системные интерфейсы ядра Linux
Системные вызовы

Драйверы устройств

- Составляют до 70% исходных кодов ядра
- 85% падений происходит из-за драйверов

[1] A. Chou et al. (2001) An Empirical Study of Operating System Errors, In Proc. of the 18-th ACM Symp. Operating System Principles, ACM Press.

[2] Swift M, Bershad B, Levy H. (2003) Improving the reliability of commodity operating systems. In SOSP’03: Symposium on Operating System Principles.

Анализ изменений в стабильных ветках ядра

с версии 2.6.35 по 3.0
за время с 26.10.10 по 26.10.11

Изменения в драйверах (1503)		
Расширение функциональности (321 - 21%)	Исправление ошибок (1182 – 79%)	
	Нетиповые ошибки (786 – 52%)	**Типовые ошибки (396 – 27%)**

Типовые ошибки

Класс и 1-й подкласс	Количество	% от общего
sync:race	60	17.2%
specific:resource	32	9.2%
generic:null_ptr_deref	31	8.9%
specific:check_params	25	7.2%
generic:resource	24	6.9%
specific:context	19	5.4%
...		

Мир инструментов статической верификации

```
int main(int argc,char* argv[])
{
  ...
  other_func(var);
  ...
}
```

```
void other_func(int v)
{
   ...
   assert( x != NULL);
}
```

Мир драйверов устройств

```
static struct pci_driver DAC960_pci_driver = {
        .name           = "DAC960",
        .id_table       = DAC960_id_table,
        .probe          = DAC960_Probe,
        .remove         = DAC960_Remove,
};

static int DAC960_init_module(void)
{
        int ret;
        ret = pci_register_driver(&DAC960_pci_driver)
#ifdef DAC960_GAM_MINOR
        if (!ret)
                DAC960_gam_init();
#endif
        return ret;
}
...
module_init(DAC960_init_module);
module_exit(DAC960_cleanup_module);
```

Регистрация функций обработчиков

Нет явных вызовов функций инициализации и выхода

Генерация псевдо-main

```
int main(int argc,char* argv[])
{
  init_module()
  for(;;) {
    switch(*) {
     case 0: driver_probe(*,*,*);break;
     case 1: driver_open(*,*);break;
     ...
    }
  }
  exit_module();
}
```

Генерация псевдо-main (2)

- Ограничения на порядок
  - Для одного типа
    - file_operations:
      read() только если вызов open() успешен
  - Между типами
    - (usb_driver и file_operations)
      open() после probe(), но перед remove()
- Виды воздействий
  - Последовательные
  - Параллельные

Rule Instrumentor

```
mutex x;
int f(int y)
{
   lock(x);
   ...
   unlock(x);
   return y;
}
```

```
int x_locked = 0;
int f(int y)
{
   assert(x_locked == 0);
   x_locked = 1;
   ...
   assert(x_locked == 1);
   x_locked = 0;
   return y;
}
```

Аспектно-ориентированный подход

```
mutex x;
int f(int y)
{
   lock(x);
   ...
   unlock(x);
   return y;
}
```

```
Аспект:
around:
call(int lock(mutex x)
{
 assert(x_locked == 0);
 x_locked = 1;
}
```

Rule Instrumentor

```
mutex x;
int f(int y)
{
   lock(x);
   ...
   unlock(x);
   return y;
}
```

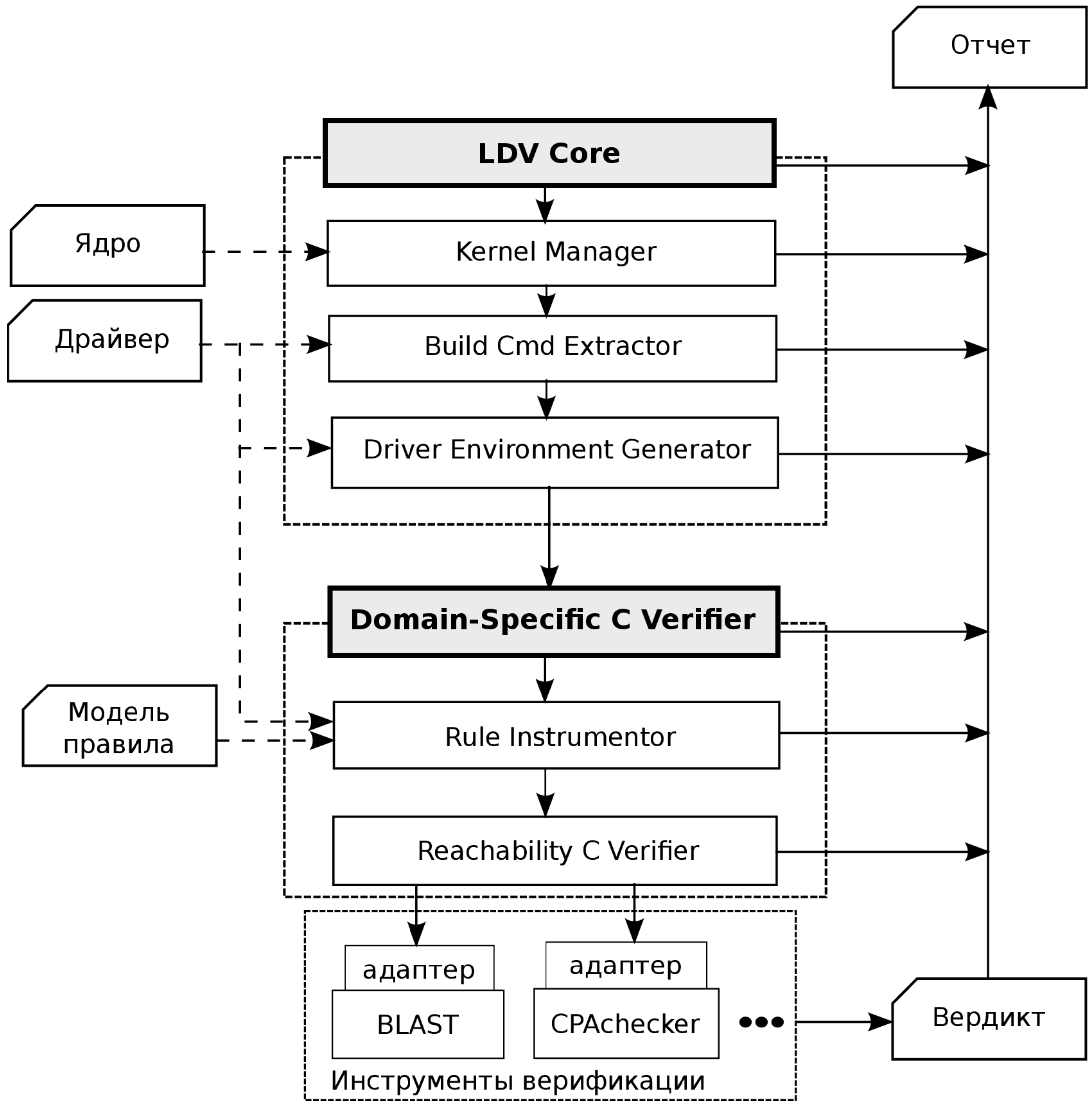
```
int x_locked = 0;
int f(int y)
{
   assert(x_locked == 0);
   x_locked = 1;
   ...
   assert(x_locked == 1);
   x_locked = 0;
   return y;
}
```

Реализация Rule Instrumentor:

- **CIF** – C Instrumentation Framework
  - Основаный на GCC
    инструмент для языка C
  - Доступен на forge.ispras.ru
    под лицензией GPLv3

Результаты SVCOMP'12

Competition candidate	BLAST 2.7	CPAchecker ABE 1.0.10	CPAchecker Memo 1.0.10	ESBMC 1.17	FShell 1.3	LLBMC 0.9	Predator 20111011	QARMC -HSF	SATabs 3.0	Wolverine 0.5c
Affiliation	Moscow, Russia	Passau, Germany	Paderborn, Germany	Southampton, UK	Vienna, Austria	Karlsruhe, Germany	Brno, Czechia	Munich, Germany	Oxford, UK	Princeton, USA
ControlFlowInteger 93 files, max score: 144	71 9900 s	141 1000 s	140 3200 s	102 4500 s	28 580 s	100 2400 s	17 1100 s	140 4800 s	75 5400 s	39 580 s
DeviceDrivers 59 files, max score: 103	72 30 s	51 97 s	51 93 s	63 160 s	20 3.5 s	80 1.6 s	80 1.9 s	--	71 140 s	68 65 s
DeviceDrivers64 41 files, max score: 66	55 1400 s	26 1900 s	49 500 s	10 870 s	0 0 s	1 110 s	0 0 s	--	32 3200 s	16 1300 s
HeapManipulation 14 files, max score: 24	--	4 16 s	4 16 s	1 220 s	--	17 210 s	20 1.0 s	--	--	--
SystemC 62 files, max score: 87	33 4000 s	45 1100 s	36 450 s	67 760 s	--	8 2.4 s	21 630 s	8 820 s	57 5000 s	36 1900 s
Concurrency 8 files, max score: 11	--	0 0 s	0 0 s	6 270 s	0 0 s	--	0 0 s	--	1 1.4 s	--
Overall 277 files, max score: 435	231 15000 s	267 4100 s	280 4300 s	249 6800 s	48 580 s	206 2700 s	138 1700 s	148 5600 s	236 14000 s	159 3800 s


Отчет
LDV Core
Ядро
Kernel Manager
Драйвер
Build Cmd Extractor
Driver Environment Generator
Domain-Specific C Verifier
Модель правила
Rule Instrumentor
Reachability C Verifier
адаптер
адаптер
BLAST
CPAchecker
•••
Вердикт
Инструменты верификации

Интерфейсы

- ldv-manager
- ldv-git
- ldv-online

ldv-online

Online Linux Driver Verification Service (alpha)

Start Verification   Verification History   Rules

Start Verification

on x86_64 architecture

1. Ensure that drivers satisfy the following requirements:

- The driver is archived using gzip or bzip2 and has one of the following extensions: .tar.bz2, tar.gz, .tgz
- Archive should contain:
  - o Makefile (written to be compiled with the kernel)
    - + obj-m is mandatory
  - o Sources needed by Makefile
- Archive should not contain generated files left from builds

2. Upload driver.

3. Wait for results.

Browse...

Start Verification

ldv-online (2)

Verification Report

Driver: test-0032-wl12xx-unsafe.tar.bz2
Timestamp: 2011-01-19 20:51:12
Verification architecture: x86_64

You can see **verification verdict** for each rule and linux kernel. Verdict may be:

- ***Safe*** - there is no mistakes for the given linux kernel and rule.
- ***Unsafe*** - driver may contain an error. You can see the error trace by clicking on the "Unsafe" link for the corresponding linux kernel and rule.
- ***Build failed*** - your driver is not compatible with the given linux kernel. In this case you may see the compile error trace by clicking on the "more details" link.
- ***Unknown*** - tools can not determine whether your driver *Safe* or *Unsafe*.
- ***Queued*** - the driver waits for the turn to verification.

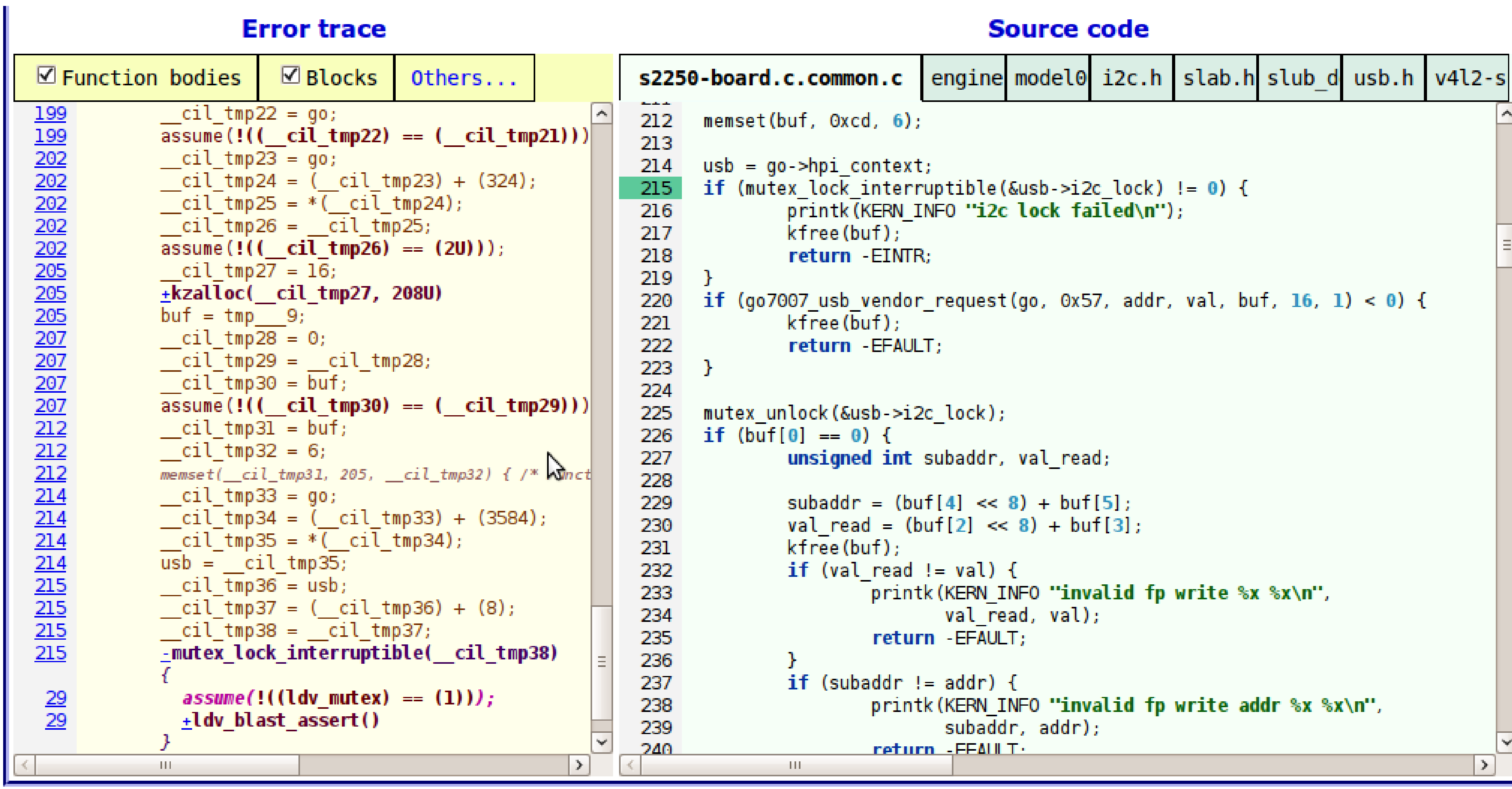
7%

linux-2.6.32.12	
Rule	**Verdict**
Mutex lock/unlock	Unsafe
NOIO allocation under usb_lock	Safe
Module get/put	
PCI pool create/destroy, alloc/free	Queued
Delay in probe_irq on/off	Queued
Memory allocation inside spinlocks	Queued
Linked list double add	Queued
Usb alloc/free urb	Queued
Spinlocks lock/unlock	Queued

База знаний

#	Task	Kernel	Rule	Total	Safe	Unsafe	Unknown	Verdicts: True	Verdicts: False	Verdicts: ?	Verdicts: ↯
1	Task description **May, 2011**	linux-2.6.38.2	Fail before RI	75	-	-	75	-	-	-	-
2			32_1a	2747	2077	66	604	-	-	-	-
3			32_7	2747	2227	20	500	3	13	-	-
4			39_7	2747	2244	15	488	2	11	-	-
5			68_1	2747	2129	68	550	2	26	-	-
6		linux-2.6.39	Fail before RI	81	-	-	81	-	-	-	-
7			32_7	2826	2278	21	527	2	19	-	-
8	Task description **June 2011**	linux-2.6.39	Fail before RI	81	-	-	81	-	-	-	-
9			08_1	2826	2124	50	652	-	-	-	-
10			32_7	2826	2292	29	505	5	24	-	-
11			39_7	2826	2319	19	488	4	15	-	-
12			43_1a	2826	1861	7	958	1	5	-	-
13			68_1	2826	2186	76	564	2	28	-	-
14	Task description **August 2011**	linux-3.0.1	Fail before RI	102	-	-	102	-	-	-	-
15			08_1	3203	2550	66	587	-	-	1	-
16			32_7	3203	2631	43	529	11	32	-	-
17			39_7	3203	2659	24	520	5	19	-	-
18			43_1a	3203	2623	8	572	1	7	-	-
19			68_1	3203	2524	90	589	3	58	1	-

Визуализатор трассы ошибки



Пример найденной ошибки

From	Alexey Khoroshilov <>
Subject	[PATCH] staging: go7007: fix mismatch in mutex lock-unlock in [read|write]_reg_fp
Date	Mon, 13 Feb 2012 16:01:32 +0100

```
If go7007_usb_vendor_request() fails in write_reg_fp()
or in read_reg_fp(), the usb->i2c_lock mutex left locked.

The patch moves mutex_unlock(&usb->i2c_lock) before check
for go7007_usb_vendor_request() returned value.

Found by Linux Driver Verification project (linuxtesting.org).

Signed-off-by: Alexey Khoroshilov <khoroshilov@ispras.ru>
---
 drivers/staging/media/go7007/s2250-board.c |   16 ++++++++++------
 1 files changed, 10 insertions(+), 6 deletions(-)
diff --git a/drivers/staging/media/go7007/s2250-board.c b/drivers/staging/media/go7007/s2250-board.c
index e7736a9..014d384 100644
--- a/drivers/staging/media/go7007/s2250-board.c
+++ b/drivers/staging/media/go7007/s2250-board.c
@@ -192,6 +192,7 @@ static int write_reg_fp(struct i2c_client *client, u16 addr, u16 val)
 {
        struct go7007 *go = i2c_get_adapdata(client->adapter);
        struct go7007_usb *usb;
+       int rc;
        u8 *buf;
        struct s2250 *dec = i2c_get_clientdata(client);

@@ -216,12 +217,13 @@ static int write_reg_fp(struct i2c_client *client, u16 addr, u16 val)
                kfree(buf);
                return -EINTR;
        }
-       if (go7007_usb_vendor_request(go, 0x57, addr, val, buf, 16, 1) < 0) {
+       rc = go7007_usb_vendor_request(go, 0x57, addr, val, buf, 16, 1);
+       mutex_unlock(&usb->i2c_lock);
+       if (rc < 0) {
                kfree(buf);
-               return -EFAULT;
+               return rc;
        }
```

Bugs Found

http://linuxtesting.org/results/ldv

- 44 патча уже применены

Problems in Linux Kernel

This section contains information about problems in Linux kernel found within Linux Driver Verification program.

No.	Type	Brief	Added on	Accepted	Status
L0050	Crash	carl9170: unlock of unheld mutex in carl9170_op_set_key	2011-08-30	https://lkml.org/lkml/2011/8/23/380 commit	Fixed in kernel 3.1-rc5
K0009	Leak	(ath5k) sc->ah is allocated in ath5k_init_softc() but is not freed	2011-08-08	Kernel Bug Tracker, bug #37592	Fixed in the kernel 3.1-rc1
L0049	Crash	hfsplus: Fix double iput of the same inode in hfsplus_fill_super()	2011-06-24	https://lkml.org/lkml/2011/6/23/675 commit	Fixed in kernel 3.0
L0048	Crash	hfsplus: add error checking for hfs_find_init()	2011-06-24	https://lkml.org/lkml/2011/7/5/500 commit	Fixed in kernel 3.1-rc1
L0047	Leak	drivers/video/hecubafb.c: absence of module_put on an error path in hecubafb_probe()	2011-06-20	https://lkml.org/lkml/2011/6/17/267 commit	Fixed in kernel 3.0-rc6
L0046	Leak	gigaset: absence of call module_put before restart of if_open()	2011-06-20	https://lkml.org/lkml/2011/6/17/321 commit 2f9381e	Fixed in kernel 3.0-rc4
L0045	Leak	drivers/net/wan/farsync.c: module_get() without module_put()	2011-06-20	https://lkml.org/lkml/2011/6/17/320 commit d0fd64c	Fixed in kernel

Направления развития

- Новые модели правил
- Генерация окружения
    - Связи между разными типами драйверов
    - Параллельные воздействия
- Инструментирование
    - Новые виды перехватываемых событий
    - Клонирование моделей правил
- Статические верификаторы
    - Более точный анализ операций с указателями
    - Верификация параллельных программ

LinuxTesting.org

Спасибо!

Вадим Мутилин
mutilin@ispras.ru
http://linuxtesting.org/project/ldv

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

LDV 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
- Provide a basis for education of young researches

Why Device Drivers?

- The main source of issues in Linux kernel
- Limited usage of complex data structures
- Almost no use of floating point arithmetics
- Small number of recursive functions
- Limited size of drivers

Identify Critical Bugs in CPAchecker

Added the problem pattern IASTBinaryExpression, which finds the error message:
java.lang.AssertionError: IASTBinaryExpression

Task	Total	CASTDesignatedInitializer	File not exists	IASTBinaryExpression	Main not found	MathsatInterpolatingProver	Unary	Aborted	Main/Label
Task description CPAchecker 06 Jun	2767	72	1	839	104	23	2	-	-

30%

Identify Critical Bugs in CPAchecker

Added the problem pattern IASTBinaryExpression, which finds the error message:
java.lang.AssertionError: IASTBinaryExpression

Task	Total	CASTDesignatedInitializer	File not exists	IASTBinaryExpression	Main not found	MathsatInterpolatingProver	Unary	Aborted	Main/Label
Task description **CPAchecker 06 Jun**	2767	72	1	839	104	23	2	-	-
Task description **CPAchecker 08 Jun**	2767	330	-	6	-	-	2	-	-

Comparing BLAST with CPAchecker

Total changes	Safe → Unsafe	Safe → Unknown	Unsafe → Unknown	Unknown → Safe	Unknown → Unsafe
0		-		-	
657	3	537	32	80	5

BLAST Safe → CPAchecker Unsafe

Safe → Unsafe							
							-
							3
#	Module	Entry point	Details		Module	Entry point	Details
1	drivers/block/nbd.ko	ldv_main0_sequence_infinite_withcheck_stateful	...		drivers/block/nbd.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
2	drivers/scsi/bnx2i/bnx2i.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	→	drivers/scsi/bnx2i/bnx2i.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
3	drivers/xen/xen-evtchn.ko	ldv_main0_sequence_infinite_withcheck_stateful	...		drivers/xen/xen-evtchn.ko	ldv_main0_sequence_infinite_withcheck_stateful	...

Empty linked list

~0UL evaluated as -1

BLAST Unsafe → CPAchecker Unknown

Unsafe → Unknown

32

#	Module	Entry point	Details	Module	Entry point	Details
1	drivers/block/cciss.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/block/cciss.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
2	drivers/char/ipmi/ipmi_watchdog.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/char/ipmi/ipmi_watchdog.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
3	drivers/char/moxa.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/char/moxa.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
4	drivers/hwmon/w83793.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/hwmon/w83793.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
5	drivers/infiniband/core/rdma_cm.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/infiniband/core/rdma_cm.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
6	drivers/input/keyboard/atkbd.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/input/keyboard/atkbd.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
7	drivers/media/dvb/dvb-usb/dvb-usb-anysee.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/media/dvb/dvb-usb/dvb-usb-anysee.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
8	drivers/media/dvb/ttpci/dvb-ttpci.ko	ldv_main4_sequence_infinite_withcheck_stateful	...	drivers/media/dvb/ttpci/dvb-ttpci.ko	ldv_main4_sequence_infinite_withcheck_stateful	...
9	drivers/media/dvb/ttusb-budget/dvb-ttusb-budget.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/media/dvb/ttusb-budget/dvb-ttusb-budget.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
10	drivers/media/IR/imon.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/media/IR/imon.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
11	drivers/media/video/au0828/au0828.ko	ldv_main4_sequence_infinite_withcheck_stateful	...	drivers/media/video/au0828/au0828.ko	ldv_main4_sequence_infinite_withcheck_stateful	...
12	drivers/media/video/cafe_ccic.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/media/video/cafe_ccic.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
13	drivers/media/video/em28xx/em28xx.ko	ldv_main2_sequence_infinite_withcheck_stateful	...	drivers/media/video/em28xx/em28xx.ko	ldv_main2_sequence_infinite_withcheck_stateful	...
14	drivers/media/video/hdpvr/hdpvr.ko	ldv_main2_sequence_infinite_withcheck_stateful	...	drivers/media/video/hdpvr/hdpvr.ko	ldv_main2_sequence_infinite_withcheck_stateful	...
15	drivers/media/video/tlg2300/poseidon.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/media/video/tlg2300/poseidon.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
16	drivers/mtd/ubi/ubi.ko	ldv_main3_sequence_infinite_withcheck_stateful	...	drivers/mtd/ubi/ubi.ko	ldv_main3_sequence_infinite_withcheck_stateful	...
17	drivers/net/ppp_generic.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/net/ppp_generic.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
18	drivers/net/wireless/ath/carl9170/carl9170.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/net/wireless/ath/carl9170/carl9170.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
19	drivers/net/wireless/mwl8k.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/net/wireless/mwl8k.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
20	drivers/scsi/dpt_i2o.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/scsi/dpt_i2o.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
21	drivers/scsi/megaraid.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/scsi/megaraid.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
22	drivers/scsi/mpt2sas/mpt2sas.ko	ldv_main2_sequence_infinite_withcheck_stateful	...	drivers/scsi/mpt2sas/mpt2sas.ko	ldv_main2_sequence_infinite_withcheck_stateful	...
23	drivers/scsi/osst.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/scsi/osst.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
24	drivers/scsi/st.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/scsi/st.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
25	drivers/serial/serial_core.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/serial/serial_core.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
26	drivers/usb/class/cdc-wdm.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/usb/class/cdc-wdm.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
27	drivers/usb/class/usblp.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/usb/class/usblp.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
28	drivers/usb/core/usbcore.ko	ldv_main15_sequence_infinite_withcheck_stateful	...	drivers/usb/core/usbcore.ko	ldv_main15_sequence_infinite_withcheck_stateful	...
29	drivers/usb/core/usbcore.ko	ldv_main17_sequence_infinite_withcheck_stateful	...	drivers/usb/core/usbcore.ko	ldv_main17_sequence_infinite_withcheck_stateful	...
30	drivers/usb/gadget/gadgetfs.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/usb/gadget/gadgetfs.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
31	drivers/usb/storage/usb-storage.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/usb/storage/usb-storage.ko	ldv_main0_sequence_infinite_withcheck_stateful	...
32	drivers/video/aty/atyfb.ko	ldv_main0_sequence_infinite_withcheck_stateful	...	drivers/video/aty/atyfb.ko	ldv_main0_sequence_infinite_withcheck_stateful	...

Out of memory

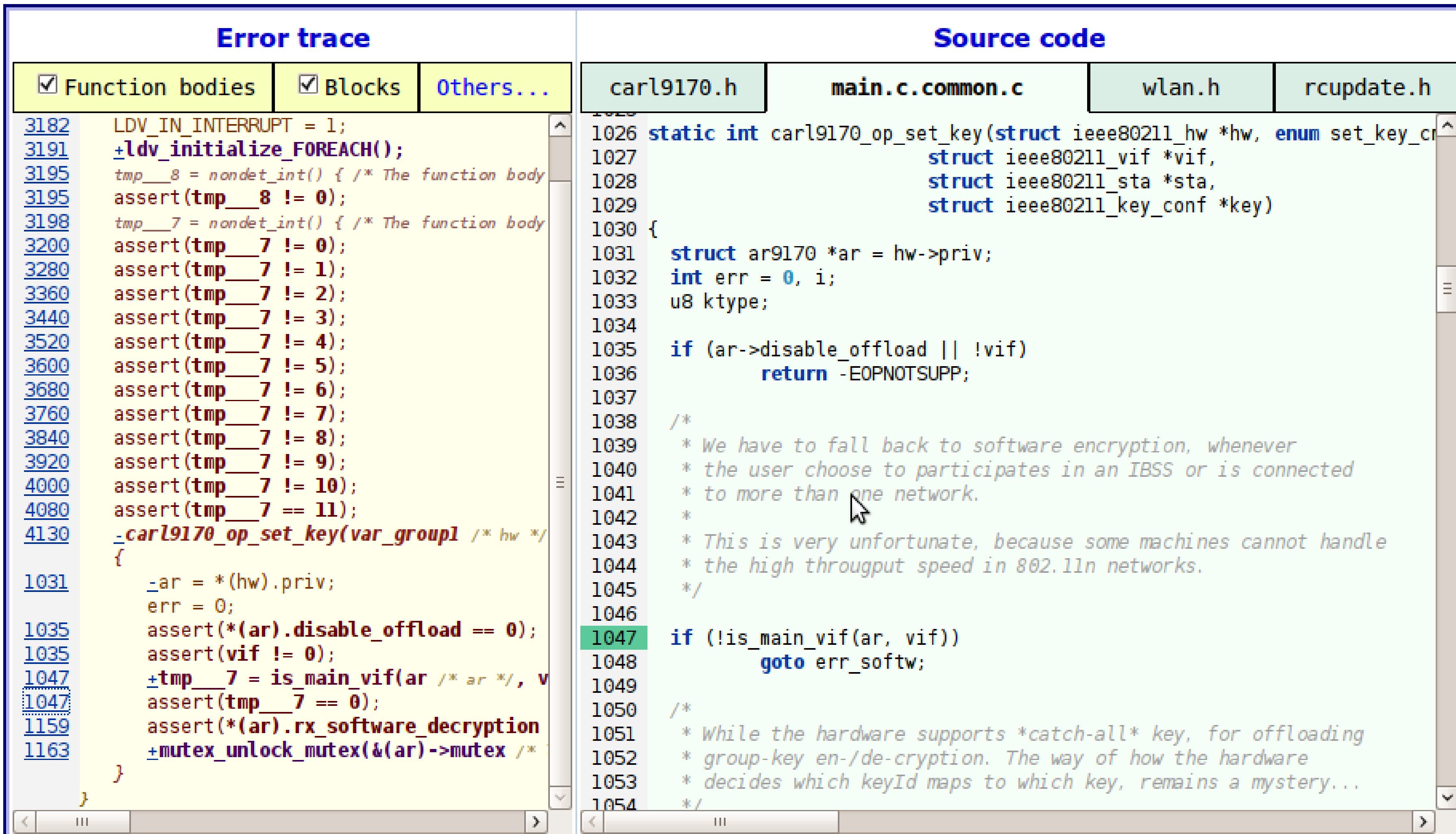
CIL Frontend errors

Knowledge Base

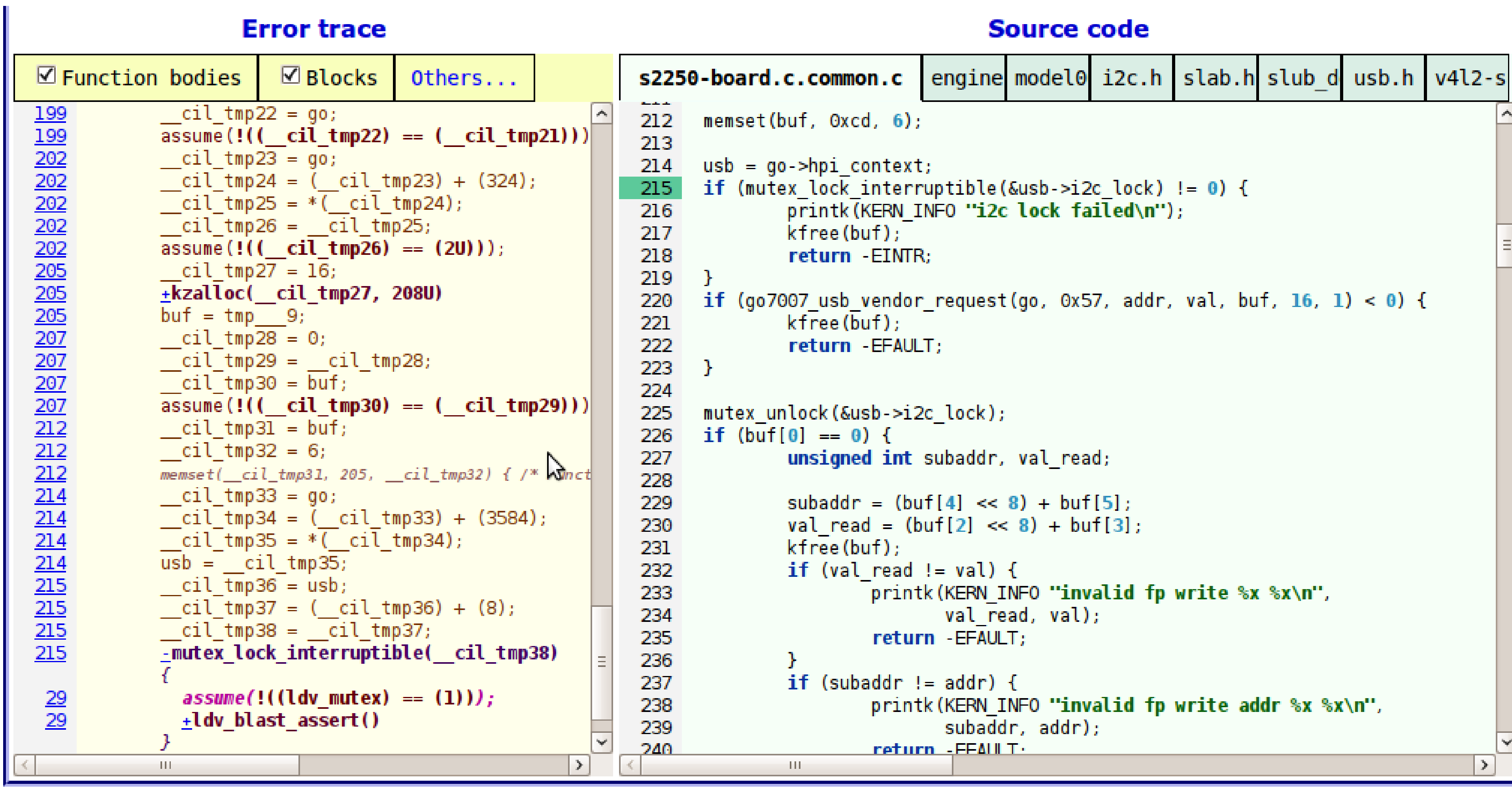
#		Task	Kernel	Rule	Total	Safe	Unsafe	Unknown	Verdicts			
									True	False	?	↯
1		Task description **May, 2011**	linux-2.6.38.2	Fail before RI	75	-	-	75	-	-	-	-
2				32_1a	2747	2077	66	604	-	-	-	-
3				32_7	2747	2227	20	500	3	13	-	-
4				39_7	2747	2244	15	488	2	11	-	-
5				68_1	2747	2129	68	550	2	26	-	-
6			linux-2.6.39	Fail before RI	81	-	-	81	-	-	-	-
7				32_7	2826	2278	21	527	2	19	-	-
8		Task description **June 2011**	linux-2.6.39	Fail before RI	81	-	-	81	-	-	-	-
9				08_1	2826	2124	50	652	-	-	-	-
10				32_7	2826	2292	29	505	5	24	-	-
11				39_7	2826	2319	19	488	4	15	-	-
12				43_1a	2826	1861	7	958	1	5	-	-
13				68_1	2826	2186	76	564	2	28	-	-
14		Task description **August 2011**	linux-3.0.1	Fail before RI	102	-	-	102	-	-	-	-
15				08_1	3203	2550	66	587	-	-	1	-
16				32_7	3203	2631	43	529	11	32	-	-
17				39_7	3203	2659	24	520	5	19	-	-
18				43_1a	3203	2623	8	572	1	7	-	-
19				68_1	3203	2524	90	589	3	58	1	-

Error Trace Visualizer

Rule: Mutex lock/unlock



Error Trace Visualizer



Bugs Found

http://linuxtesting.org/results/ldv

- 44 patches already applied

Problems in Linux Kernel

This section contains information about problems in Linux kernel found within Linux Driver Verification program.

No.	Type	Brief	Added on	Accepted	Status
L0050	Crash	carl9170: unlock of unheld mutex in carl9170_op_set_key	2011-08-30	https://lkml.org/lkml/2011/8/23/380 commit	Fixed in kernel 3.1-rc5
K0009	Leak	(ath5k) sc->ah is allocated in ath5k_init_softc() but is not freed	2011-08-08	Kernel Bug Tracker, bug #37592	Fixed in the kernel 3.1-rc1
L0049	Crash	hfsplus: Fix double iput of the same inode in hfsplus_fill_super()	2011-06-24	https://lkml.org/lkml/2011/6/23/675 commit	Fixed in kernel 3.0
L0048	Crash	hfsplus: add error checking for hfs_find_init()	2011-06-24	https://lkml.org/lkml/2011/7/5/500 commit	Fixed in kernel 3.1-rc1
L0047	Leak	drivers/video/hecubafb.c: absence of module_put on an error path in hecubafb_probe()	2011-06-20	https://lkml.org/lkml/2011/6/17/267 commit	Fixed in kernel 3.0-rc6
L0046	Leak	gigaset: absence of call module_put before restart of if_open()	2011-06-20	https://lkml.org/lkml/2011/6/17/321 commit 2f9381e	Fixed in kernel 3.0-rc4
L0045	Leak	drivers/net/wan/farsync.c: module_get() without module_put()	2011-06-20	https://lkml.org/lkml/2011/6/17/320 commit d0fd64c	Fixed in kernel

Example of a Report (L0014)

```
Date       Mon, 12 Oct 2009 11:25:13 +0200 (CEST)
From       Jiri Kosina <>
Subject    Re: [BUG] hidraw.c: double mutex_lock

On Mon, 12 Oct 2009, iceberg wrote:

>       KERNEL_VERSION: 2.6.31
>       DESCRIBE:
>       In driver ./drivers/hid/hidraw.c in function hidraw_read may be
> double mutex_lock:
>
> Path:
> 1. line 50: begin first iteration of "while(ret==0)"
> 2. line 52: first call to mutex_lock
> 3. inner loop "while (list->head == list->tail)" does not change state
> of mutex, because mutex_lock immediatelly follows mutex_unlock
> 4. if we go to the second iteration of "while(ret == 0)" in
> line 50 then there are second call to mutex_lock in line 52 (mutex
> aquired twice).
>
> Second iteration of loop "while(ret==0)" is possible if local variable
> ret is not changed at line 94: ret+=len - i.e. len==0;
> Variable len may be zero if hidraw_read is called with count==0 or
> list->buffer[list->tail].len == 0.

Good catch. I will fix that up by moving the mutex_lock() so that it's
locked before the loop is entered.

Thanks,

--
Jiri Kosina
SUSE Labs, Novell Inc.
```

Another Example of a Report

```
From      Alexey Khoroshilov <>
Subject   [PATCH] staging: go7007: fix mismatch in mutex lock-unlock in [read|write]_reg_fp
Date      Mon, 13 Feb 2012 16:01:32 +0100

If go7007_usb_vendor_request() fails in write_reg_fp()
or in read_reg_fp(), the usb->i2c_lock mutex left locked.

The patch moves mutex_unlock(&usb->i2c_lock) before check
for go7007_usb_vendor_request() returned value.

Found by Linux Driver Verification project (linuxtesting.org).

Signed-off-by: Alexey Khoroshilov <khoroshilov@ispras.ru>
---
 drivers/staging/media/go7007/s2250-board.c |   16 ++++++++++------
 1 files changed, 10 insertions(+), 6 deletions(-)
diff --git a/drivers/staging/media/go7007/s2250-board.c b/drivers/staging/media/go7007/s2250-board.c
index e7736a9..014d384 100644
--- a/drivers/staging/media/go7007/s2250-board.c
+++ b/drivers/staging/media/go7007/s2250-board.c
@@ -192,6 +192,7 @@ static int write_reg_fp(struct i2c_client *client, u16 addr, u16 val)
 {
        struct go7007 *go = i2c_get_adapdata(client->adapter);
        struct go7007_usb *usb;
+       int rc;
        u8 *buf;
        struct s2250 *dec = i2c_get_clientdata(client);

@@ -216,12 +217,13 @@ static int write_reg_fp(struct i2c_client *client, u16 addr, u16 val)
                kfree(buf);
                return -EINTR;
        }
-       if (go7007_usb_vendor_request(go, 0x57, addr, val, buf, 16, 1) < 0) {
+       rc = go7007_usb_vendor_request(go, 0x57, addr, val, buf, 16, 1);
+       mutex_unlock(&usb->i2c_lock);
+       if (rc < 0) {
                kfree(buf);
-               return -EFAULT;
+               return rc;
        }
```