

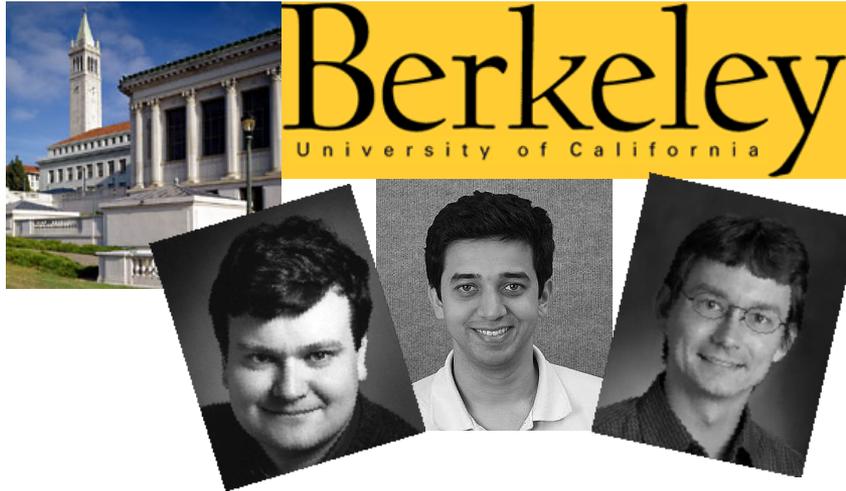
Predicate Analysis with BLAST 2.7.3

 Pavel Shved, Mikhail Mandrykin,
and Vadim Mutilin

ISPRAS

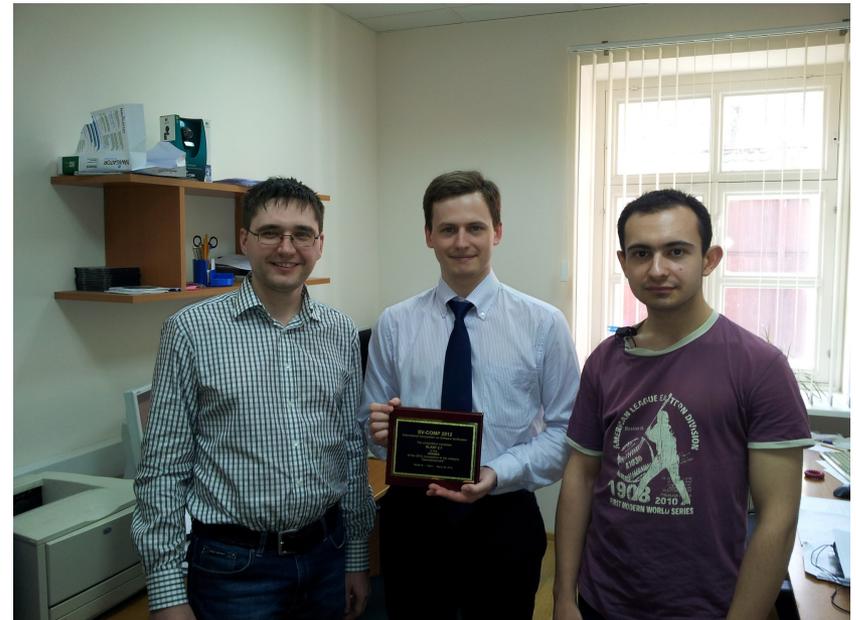
Institute for System Programming of the Russian Academy of Sciences

BLAST 2.5



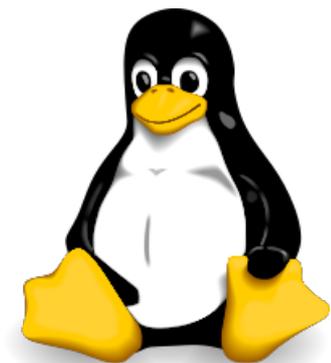
Berkeley
Lazy
Abstraction
Software
Verification
Tool

BLAST 2.7.3



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



New Benchmarks

Based on Linux kernels 3.12 and 3.16

- Pointers
- Arrays
- Bitvectors
- Bugs found in Linux kernel

Results Excerpt for Arrays (DeviceDrivers64)

BLAST	CPAchecker	Seahorn
witness confirmed	unknown	out of memory
witness ignored (recursion)	unknown	witness ignored (recursion)
true	true	true
true	true	timeout
witness timeout	witness timeout	out of memory
true	true	true
true	true	timeout
true	true	timeout
true	true	timeout
out of memory	out of memory	timeout
exception (gremlins)	timeout	timeout
timeout	timeout	timeout
out of memory	timeout	timeout
exception (gremlins)	timeout	timeout
timeout	timeout	witness timeout
exception (gremlins)	unknown	witness confirmed
timeout	unknown	timeout
witness timeout	unknown	timeout
witness timeout	witness timeout	witness timeout
witness timeout	out of memory	timeout
exception (gremlins)	unknown	timeout
witness timeout	witness timeout	witness timeout
witness timeout	witness timeout	witness timeout
true	true	timeout

Seahorn Error Witness in LDV Error Trace Visualizer

LDV Analytics Center 0.12 [Knowledge Base](#) [Help](#) [Support](#)

Error trace **Source code**

Function bodies Blocks Others...

```
804 *;  
814 *;  
848 *;  
458 _softing_card_shutdown  
458 {  
155     _ldv_mutex_lock_interruptible_12  
383     {  
388         _ldv_mutex_lock_interruptible_lock_of_NO  
404         {  
404             *;  
404             *;  
404             return ldv_mutex_lock_interruptible_lo  
161         }  
467         return ldv_mutex_lock_interruptible_12;  
472     }  
472     *;  
473     *;  
42     ±softing_set_reset_dpram  
475     *;  
166     _ldv_mutex_unlock_13  
524     {  
524         _ldv_mutex_unlock_lock_of_NOT_ARG_SIGN  
527     {  
10         *;  
         ±ldv_error  
     }  
     }  
 }  
 }
```

softing_main.c soft ldv rcv. devi iopc plat slab spir

```
454 }  
455 return 0;  
456 }  
457  
458 static void softing_card_shutdown(struct softing *card)  
459 {  
460     int fw_up = 0;  
461  
462     if (mutex_lock_interruptible(&card->fw.lock))  
463         /* return -ERESTARTSYS */;  
464     fw_up = card->fw.up;  
465     card->fw.up = 0;  
466  
467     if (card->irq.requested && card->irq.nr) {  
468         free_irq(card->irq.nr, card);  
469         card->irq.requested = 0;  
470     }  
471     if (fw_up) {  
472         if (card->pdat->enable_irq)  
473             card->pdat->enable_irq(card->pdev, 0);  
474         softing_set_reset_dpram(card);  
475         if (card->pdat->reset)  
476             card->pdat->reset(card->pdev, 1);  
477     }  
478     mutex_unlock(&card->fw.lock);  
479 }  
480  
481 static int softing_card_boot(struct softing *card)  
482 {  
483     int ret, j;  
484     static const uint8_t stream[] = {
```

Suggestions for Error Witnesses

- Better support for single path witnesses
- Cope with/extend timelimits for witness checking

Thank you!

 Vadim Mutilin
mutilin@ispras.ru
<http://linuxtesting.org/project/ldv>

ISPRAS

Institute for System Programming of the Russian Academy of Sciences