LinuxTesting.org

10 лет Центра верификации ОС Linux

Верификация реального ПО – мечта или реальность?

Александр К.Петренко,
Алексей В. Хорошилов

ИСП РАН

Институт системного программирования РАН

Предыстория

- 1994 – тестирование на основе формальных спецификаций SBT/MBT: NORTEL (API ОС – переносимость – интероперабельность)
- 2000 – 2002 – IPv6/CTesk Microsoft Research
- 2001 – LSB – борьба за интероперабельность и против фрагментации рынка приложений ОС Linux
- 2004 – LSB: Intel - фальстарт

Первый период. Развитие вширь.

- 2005 – OLVER+LVC: Минобрнауки при поддержке Президиума РАН (LSB Core, 1500 функций)
- 2006 – FSG – FSG+OSDL=Linux Foundation-LF (2007)
- 2007-2011 – LF+Nokia+Motorola – развитие вширь (более 25-ти тысяч функций)
- 2007 – POSIX+ARINC-653: НИИСИ РАН Багет ОС2000/3000/4000 РПКБ/КРЭТ/Электроавтоматика

- Аналог: Microsoft Interoperability Initiative (2008-2010)

Первый период. Развитие вширь.

Технология	Выделено требований	Протестировано функций	Найдено ошибок (реал./требов.)
CTESK / UniTESK	**24 000**	**1532**	**100 / 100**
T2C	**4 476**	**1553**	**40 / 40**
API Sanity AutoTest	**0**	**24 000**	**10 / 0**

Первый период. Развитие вширь.

Промежуточные итоги:

- Информационная инфраструктура стандарта LSB (> 40 тысяч функций)
- Три слоя технологий тестирования

Технология	Производительность (функций в неделю)	Качество тестирования
CTESK / UniTESK	1-2	высокое
T2C	>5	среднее
API Sanity AutoTest	>100	Проверка работоспособности (sanity testing)

- False positive – 0% (?)
- Требования к квалификации – пользователь библиотек ОС

Второй период. Развитие вглубь.

(Минобрнауки/Google/ГосНИИАС/РусБИТех)

- 2007 – software model checking – BLAST, CPAChecker
- 2011 – тестирование ядра ОС в условиях отказов оборудования
- 2012 – гипервизор для защиты приложений от скомпромитированной ОС
- 2013 – дедуктивная верификация, развитие Frama-C/Why-3/Jessie
- 2005 – система управления требованиями

- Аналоги
  - Microsoft Research SLAM/SDK/WDK (2002 по н.в.)
  - seL4 verification project (2006-2014

Software Model Checking

- Результаты
  - Найдено и исправлено >200 ошибок в ядре Linux
  - Первое место в международных соревнованиях SV-COMP'2012 и SV-COMP'2014 по software verification в категории DeviceDrivers64

Номер	Тип	Краткое описание	Добавлено	Принято	Статус
L0205	Утечка	mcb: утечки в mcb_pci_probe()	2015-10-05	https://lkml.org/lkml/2015/7/8/1041 commit	Исправлено в ядре 4.3-rc5
L0204	Утечка	usb: gadget: amd5536udc: утечки при обработке ошибок в udc_pci_probe()	2015-09-14	https://lkml.org/lkml/2015/9/5/225 commit	Исправлено в ядре 4.3-rc3
L0203	Утечка	mtd: nettel: утечка в nettel_init() в случае ошибки в mtd_device_register()	2015-08-18	https://lkml.org/lkml/2015/8/13/753 commit	Исправлено в ядре 4.3-rc1
L0202	Блокировка	gpio/grgpio: взаимная блокировка в grgpio_irq_unmap()	2015-08-17	https://lkml.org/lkml/2015/8/17/117	Исправлено в ядре
L0201	Утечка	bfa: утечка bfad_im_port_index			

See details: http://linuxtesting.org/ldv

Institute for System Programming of the Russian Academy of Sciences

VERIFICATION CENTER OF THE OPERATING SYSTEM Linux

About Us

- About Center
- Our Team
- News
- Partners
- Contacts

Projects

- Linux Kernel Space Verification
- LSB Infrastructure
- Testing Technologies
- Tests and Frameworks
- Portability Tools

Results

- Contribution
- Publications
- Events

khoroshilov

- My account
- User list
- Create content
- Feed aggregator
- Administer
- Log out

18-Feb-2015: The first public release of Astraver Toolset

View | Edit | Track | Translate

Submitted by Mikhail Mandrykin on Wed, 18/02/2015 - 18:30

We are happy to announce the first public release of **Astraver Toolset 1.0** that is built on top of the '**Frama-C** + **Jessie** + **Why3 IDE**' deductive verification toolchain. The toolchain was adapted, so it can be used to specify and prove properties of Linux kernel code. The most of our modifications go to the Jessie plugin, while the Frama-C front-end and the Why3 platform have got just minor fixes or improvements. Some of our modifications were already applied upstream, while the rest is available in **our public repositories**.

The most important modifications are described below.

C Language Support

- Low-level reinterpret type casts between pointers to integral types. This feature required modification of the Jessie memory model as described in our paper "Extended High-Level C-Compatible Memory Model with Limited Low-Level Pointer Cast Support for Jessie Intermediate Language". The overall idea can be summarized as an ability to do certain ghost re-allocations of memory blocks in explicitly specified points in order to transform arrays of allocated objects (structures) from one type to another. **WARNING.** Discriminated unions support is not yet fully adapted to the modified memory model.
- Prefix type casts between outer structures and their corresponding first substructures (through field inlining and structure inheritance relation in Jessie).
- Kernel memory (de)allocating functions kmalloc()/kzalloc(), kfree().
- Builtin C99 __Bool type.
- Standard library functions memcpy(), memmove(), memcmp() and memset(). The support for these functions is implemented through type-based specialization of several pre-defined pattern specifications. **(*)**
- Function pointers (through exhaustive may-aliases checking). **(*)**
- Variadic functions (through additional array argument). **(*)**
- Inline assembly (through undefined function calls). **(*)**

> ***(*)***_The main purpose of implementing support for these features was the ability to use the tools on our target code without the need for its significant preliminary modification. As a result the support is not complete enough to be usable for verification of code that significantly relies on these features. For instance:_

Второй период. Развитие вглубь.

Промежуточные итоги:

- Software model checking
  - трудоемкость - 2 правила в месяц,
  - скорость верификации – 4000 драйверов * 1 правило = 1 день
  - false positive – 10-90%
  - требования к квалификации – разработчик драйвера ОС
- Дедуктивная верификация
  - трудоемкость 1 функция в месяц
  - время "переверификации" – 1 неделя
  - false positive – 0%
  - требования к квалификации
    - разработчик драйвера ОС + дедуктивная верификация

Планы

- 2017 – масштабируемая верификация модулей ОС Linux
- 2017 – дедуктивная верификация многопоточности в ядре ОС Linux
- 2016-2018 – сертифицируемая ОС реального времени – макет и пакет сертификационных документов

Дискуссия

Верификация реального ПО – мечта или реальность?

- Каковы причины такого положения дел?
- Что мешает применению новых технологий?
- Как выбирать эффективный набор технологий в контексте конкретной практической задачи?
- Вопрос надо ставить в другой плоскости?

LinuxTesting.org

Все на фуршет!

ИСП РАН

Институт системного программирования РАН