Многоаспектная верификация модулей ядра операционной системы Linux

Мордань Виталий Олегович

Аспирант

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: mordan@ispras.ru

Linux Driver Verification Tools (LDV Tools) [1] представляет собой конфигурируемую систему статической верификации, предоставляющую инфраструктуру для проверки модулей ядра ОС Linux с высокой степенью автоматизации и возможность для подключения различных инструментов статической верификации. Система LDV Tools позволила выявить более 140 критичных ошибок в модулях ядра ОС Linux, исправления которых были приняты разработчиками [2].

На данный момент большинство используемых в рамках LDV Tools инструментов статической верификации останавливаются после нахождения первой ошибки. На практике существуют ситуации, когда ошибок в модуле может быть несколько [2]. Последующая ошибка может быть найдена только после того, как будет внесено соответствующее изменение в исходный код, исправляющее первую ошибку, что существенно затрудняет исправление всех нарушений проверяемых правил.

Для решения данной проблемы предлагается использовать метод многоаспектной верификации. Суть метода заключается в том, что после нахождения новой ошибки инструмент статической верификации должен запомнить ее и продолжить анализ, по завершению которого выдается информация о всех найденных ошибках в удобном для анализа виде. Предложенный подход был экспериментально реализован на основе иснтрумента статической верификации CPAchecker [3], который интегрирован в LDV Tools. Эксперименты показали, что с помощью данного метода возможно нахождение нескольких реальных ошибок для заданного правила. Однако для этого требуется большее количество ресурсов, таких как процессорное время и память. Например, запуск на всех драйверах ядра linux-3.12-rc1 на правиле корректного использования мьютексов в одном потоке занял в 2.5 раза больше времени, чем при поиске только первой ошибки. Кроме того, остается ряд открытых вопросов, например, эквивалентность разных трасс ошибок (путей в исходном коде, на которых возможны нарушения проверяемых правил), которые требуют более подробного исследования для полноценного внедрения

многоаспектной верификации в LDV Tools.

Литература

1. Мутилин В. С., Новиков Е. М., Петренко А. К., Хорошилов А. В. Конфигурируемая система статической верификации модулей ядра операционных систем. Институт системного программирования РАН (ИСП РАН), Москва. 2013.

2. Список ошибок, выявленных в модулях ядра ОС Linux с помощью конфигурируемой системы статической верификации Linux Driver Verification Toolkit: `http://linuxtesting.org/results/ldv`.

3. D. Beyer, M. E. Keremoglu. CPAchecker: a tool for configurable software verification. Proceedings of the 23rd International Conference on Computer Aided Verification, pp. 184–190, 2011.