Секция «Вычислительная математика и кибернетика»

Моделирование окружения драйверов операционной системы Linux для поддержки процесса статической верификации

Захаров Илья Сергеевич
Студент
Московский физико-технический институт, Факультет управления и прикладной математики, Москва, Россия
E-mail: ilja.zakharov@ispras.ru

В настоящее время ядро операционной системы Linux динамично развивается. Новые версии ядра появляются каждые 2-3 месяца и могут включать в себя более 10 тысяч патчей, а в их подготовке обычно участвует порядка тысячи разработчиков [6]. Большую часть ядра составляют драйверы. В большинстве случаев падение системы происходят именно из-за них [3]. Поэтому именно драйверы нуждаются в верификации в первую очередь, так как при текущих темпах развития осуществлять их поддержку вручную слишком трудоемкая задача. Одним из способов решения этой проблемы является применение инструментов статической верификации.

Работа драйвера тесно связана с работой основной части ядра. Но на сегодняшний день уровень развития инструментов статической верификации не позволяет анализировать модули драйвера вместе с основной частью ядра из-за ее большого объема и высокой сложности кода. Поэтому для модуля драйвера необходимо готовить модель окружения, которая предоставляет все те сценарии работы драйвера, которые происходят при реальном взаимодействии ядра и драйвера. Инструмент статической верификации анализирует драйвер вместе с моделью окружения, поэтому при некорректной модели ошибки могут быть пропущены или могут возникнуть ложные сообщения об ошибках в драйвере.

Системы статической верификации драйверов, такие как Microsoft SDV [1] (входит в набор Windows Development Kit для разработчиков драйверов Windows), Avinux [2] (разработана в университете города Тюбинген в Германии), DDVerify [5] (разработка Оксфордского университета), а также LDV [4] (разработана в институте системного программирования РАН), имеют ряд существенных недостатков в построения модели окружения. Данная работа посвящена новому подходу к генерации модели окружения для драйверов Linux, который был реализован в системе LDV.

Литература

1. Ball T., Bounimova E., Levin V., Kumar R., Lichtenberg J. The Static Driver Verifier Research Platform // CAV 2010. 2010.

2. Hendrik P., Wolfgang K. Integrated Static Analysis for Linux Device Driver Verification. // IFM'07 Proceedings of the 6th international conference on Integrated formal methods. 2007, p. 518-537.

3. Swift M., Bershad B., Levy H. Improving the reliability of commodity operating systems. // SOSP '03. 2003.

4. Khoroshilov A., Mutilin V., Shcherbina V. et al. How to cook an automated system for Linux verification // 2nd Spring Young Researchers' Colloquium on Software Engineering. 2008, Vol. 2. p. 11–14.

5. Witkowski T., Blanc N., Kroening D., Weissenbacher G. Model Checking Concurrent Linux Device Drivers ASE '07: Proceedings of the twenty-second IEEE/ACM international conference on Automated software engineering // ACM. 2007. p. 501–504.

6. Corbet J., Kroah-Hartman G., McPherson A. Linux kernel development. How Fast it is Going, Who is Doing It, What They are Doing, and Who is Sponsoring It: http://go.linuxfoundation.org/who-writes-linux-2012