Федеральная целевая программа

«Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014—2020 годы»

Информационно-телекоммуникационные системы

Тема: *Разработка методов и инструментов для дедуктивной верификации модулей ядра ОС Linux*

Соглашение 14.604.21.0051
на период 2014 - 2016 гг.

Руководитель проекта: *А.В.Хорошилов, к.ф.-м.н., в.н.с.*

Получатель субсидии: *Институт системного программирования РАН*

Цели и задачи проекта

Целью проекта является разработка методов и инструментов дедуктивной верификации компонентов операционных систем.

Задачи проекта заключаются в развитии методов дедуктивной верификации с целью включения в область их применимости следующих особенностей исходного кода компонентов ядра операционных систем:

- наличие работы с разделяемыми данными, т. е. с данными, которые могут быть изменены параллельно выполняющимися функциями;

- наличие работы с состоянием потока управления, в котором выполняется функция;

- использование указателей на внутренние поля структур и адресная арифметика с такими указателями;

- наличие неявных преобразований типов посредством обращения к содержимому одной области памяти как к объектам разных типов;

- использование функциональных указателей.

Ожидаемые результаты проекта

Основные теоретические результаты:

- метод генерации модели памяти компонентов операционных систем с возможностью интерпретации участков памяти как объектов разных типов;

- метод генерации моделей памяти разделяемой между несколькими потоками управления;

- метод генерации условий верификации для программ, работающих с разделяемыми данными.

Основным практическим результатом является разработка экспериментального образца, реализующего предложенные методы дедуктивной верификации программ системного уровня на языке Си.

Перспективы практического использования

Разработанные методы дедуктивной верификации будут востребованы при разработке компонентов операционных систем, а также компонентов других уровней стека, применяемых в составе ответственных систем, то есть систем к которым предъявляются повышенные требования к надёжности. Примерами таких систем являются системы управления на транспорте, в медицине, на энергетических и промышленных объектах, от корректности поведения которых зависят жизни людей, а также информационные системы от защищенности которых зависит сохранность персональных, коммерческих и государственных данных.

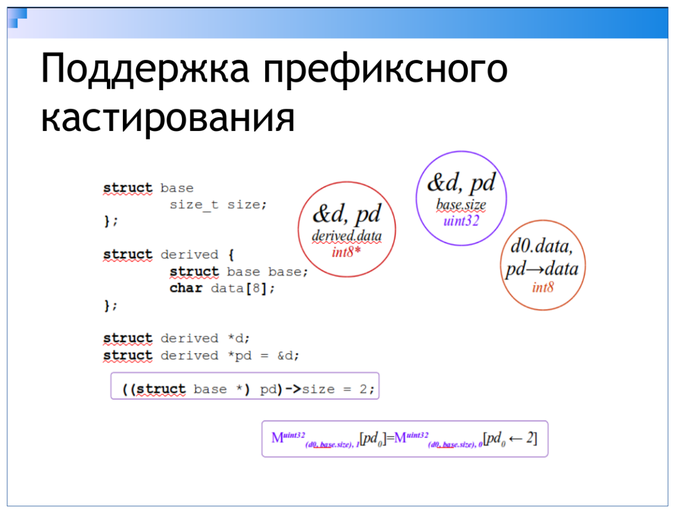
Результаты исследовательской работы, полученные в 2015 г.

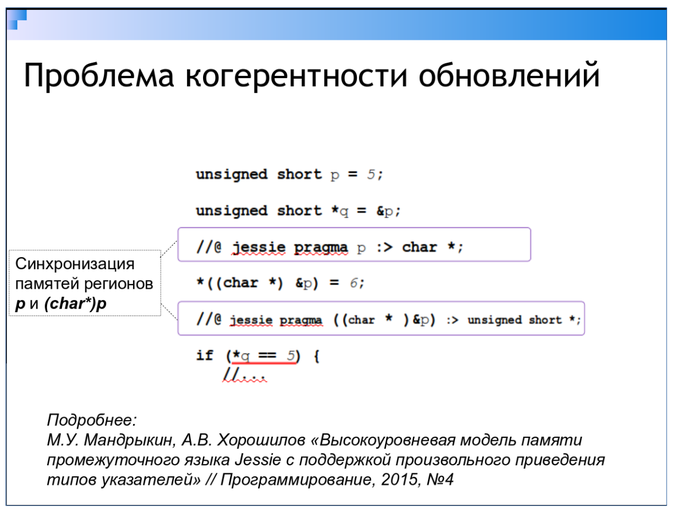
В 2015 году были разработаны следующие методы:

- метод генерации модели памяти компонентов операционных систем с возможностью интерпретации участков памяти как объектов разных типов;

- метод генерации моделей памяти разделяемой между несколькими потоками управления;

- метод генерации условий верификации для программ, работающих с разделяемыми данными.





Подробнее:
М.У. Мандрыкин, А.В. Хорошилов «Высокоуровневая модель памяти промежуточного языка Jessie с поддержкой произвольного приведения типов указателей» // Программирование, 2015, №4

Партнёры проекта

Индустриальный партнёр:

Открытое акционерное общество «Научно-производственное объединение «Русские базовые информационные технологии» (ОАО «НПО РусБИТех»)

Внебюджетное финансирование:

9,5 млн. рублей