Система для выявления состояний гонки в ядре Linux

Комаров Н.Ю., аспирант ИСП РАН I г.о.
Научный руководитель: д.ф-м.н., проф. Петренко А.К.

Состояние гонки

Одновременное обращение двух или более потоков в паралелльной программе к одной области памяти при отсутствии между этими обращениями принудительного упорядочивания по времени, когда хотя бы одно из обращений — на запись

Состояние гонки: пример

```
Thread1 {
    while (true) {
        x = x + 1;
    }
}

Thread2 {
    while (true) {
        x = x - 1;
    }
}
```

Состояние гонки: пример

```
Thread1 {
   while (true) {
      mov ax, x
      inc ax
      mov x, ax
   }
}
```

```
Thread2 {
   while (true) {
      mov bx, x
      dec bx
      mov x, bx
   }
}
```

Состояние гонки: пример

		x=1,ax=0,bx=0
mov ax, x		x=1,ax=1,bx=0
	mov bx, x	x=1,ax=1,bx=1
inc ax		x=1,ax=2,bx=1
	dec bx	x=1,ax=2,bx=0
mov x, ax		x=2,ax=2,bx=0
	mov x, bx	x=0,ax=2,bx=0

Linux

- Ядро — многопоточная система
- Исследование комментариев к изменениям в ядре: состояния гонки — первое место, ~17% типовых ошибок[1]
- На II и III месте — утечки специфичных объектов и разыменование нулевого указателя (по ~9%)

[1] В.С. Мутилин, Е.М. Новиков, А.В. Хорошилов. Анализ типовых ошибок в драйверах операционной системы Linux

Therac-25

- Аппарат лучевой терапии
- Состояние гонки между управляющей программой и обработчиком клавиатуры
- Переоблучение пациентов
- От 2 до 4 погибших

Выявление состояний гонки

- Lockset
- Happens-before

Lockset

- Предположение: состояния гонки происходят, когда используемые разными потоками переменные не защищены механизмами синхронизации
- Проверка наличия синхронизации при обращении к общим переменным

Lockset

- Позволяет выявлять большую часть потенциальных состояний гонки
- Большое количество ложных срабатываний

- Самый известный инструмент — Eraser

Happens-before

Определение:

- Из двух последовательных событий в одном потоке следующее первым имеет отношение happens-before к следующему вторым
- Операция блокировки в одном потоке имеет отношение happens-before к операции разблокировки в другом потоке для одного синхронизационного объекта
- Отношение happens-before транзитивно

Happens-before

Таким образом, для двух обращений к одной переменной может существовать состояние гонки, если между ними нельзя установить отношение happens-before

Happens-before

- Позволяет выявлять небольшое подмножество ошибок
- Меньше ложных срабатываний, чем у Lockset

Helgrind

- На базе Valgrind, для пользовательских приложений
- Помимо выявления состояний гонки, проверяет правильность использования механизмов синхронизации
- Алгоритм Happens-before

ThreadSanitizer

- Для модулей ядра Linux
- Happens-before
- Инструментирование кода модуля: добавление вызовов специальных функций при каждом обращении к памяти и при каждом использовании механизмов синхронизации

Data Collider

- Microsoft Research
- Для драйверов Windows
- Простой алгоритм, исследующий исключительно реальное выполнение программы

Data Collider: алгоритм

- Периодическая случайная расстановка точек прерывания на выполнение отдельных инструкций программы
- При срабатывании точки прерывания:
  - Декодирование инструкции, получение адреса, по которому она обращается
  - Получение значения по этому адресу
  - Установка точки прерывания на обращение по этому адресу
  - Задержка
  - Повторное получение значения, сравнение с исходным

Data Collider: алгоритм

Состояние гонки точно присутствует при срабатывании точки прерывания на обращение к адресу либо при изменении значения по адресу за прошедшее время

Data Collider

Достоинства:

- Простой алгоритм, прост в использовании
- Почти не требует вмешательства пользователя при работе
- Не дает ложных срабатываний
- Низкие накладные расходы при выполнении: ~5%

Недостатки:

- Находит небольшую часть ошибок
- Сильно зависит от оборудования

Data Collider

Найдено 25 подтвержденных ошибок
в ядре Windows

Racehound

Постановка задачи:

- Разработать систему для выявления состояний гонки в ядре Linux, использующую алгоритм работы, аналогичный Data Collider

Racehound

- Основная часть системы — модуль ядра
- Интерфейс на базе debugfs

Racehound: алгоритм

- Периодическая случайная расстановка программных точек прерывания на выполнение отдельных инструкций программы (Software Breakpoints/Kprobes)
- При срабатывании точки прерывания:
  - Декодирование инструкции, получение адреса, по которому она обращается
  - Получение значения по этому адресу
  - Установка аппаратной точки прерывания на обращение по этому адресу (Hardware Breakpoint)
  - Задержка
  - Повторное получение значения, сравнение с исходным

Racehound: особенности реализации

Декодирование инструкций:

- Декодер из ядра Linux (insn.h, inat.h)
- Доработан в рамках проекта KEDR
- При старте декодируются все инструкции модуля, выделяются те, которые обращаются к памяти
- При работе на основании инструкции и значений регистров определяется адрес, по которому обращается инструкция, и размер данных по этому адресу

Racehound: проблемы

- Проблема: обработчик программной точки прерывания выполняется в атомарном контексте, установка аппаратной точки невозможна
- Решение: установка аппаратной точки прерывания из очереди заданий
- Минус: временной зазор между началом задержки и установкой аппаратной точки прерывания; снижение точности

Racehound: проблемы

- Проблема: выполнение исходной инструкции при срабатывании программной точки прерывания
- Решение: вместо выполнения исходной инструкции отдельно — восстановление этой инструкции. Повторная установка программной точки прерывания по таймеру
- Минус: появляется промежуток времени, когда программная точка не установлена

Racehound: ограничения

- Невозможность работы на однопроцессорных системах
- Версия ядра Linux >=2.6.33

Racehound: состояние

- Разработан прототип
- Окончательный вариант системы в разработке

Racehound: планы

- Апробация на реальных драйверах
- Настройка параметров (количество точек прерывания, временные интервалы и т.д.)
- Оценка эффективности работы

- Интеграция с другими методами выявления состояний гонки, в т.ч. статическими
- Включение в состав ядра Linux

Спасибо!