Трассировка многомодульного приложения в среде операционной системы z/OS

Ростислав Ефремов, 344 группа
Научный руководитель:
Вояковская Н.Н.
ЗАО «Ланит-Терком», главный конструктор

СПбГУ, Математико-Механический факультет, 2015

Цель

Анализ различных методов трассировки переходов между модулями:

- Сравнение производительности
- Исследование прозрачности
- Выбор метода и реализация прототипа трассировщика

Задачи

- Изучение архитектуры операционной системы z/OS и поиск методов перехвата переходов
- Разработка программы, реализующей основные методы трассировки для тестирования их производительности
- Разработка прототипа трассировщика, использующего один из методов

Существующие аналоги

- IDF (Interactive Debug Facility)
  - Стандартная утилита IBM из поставки HLASM toolkit
  - Сильные ограничения на окружение
- z/XDC (Extended Debugging Controller)
  - Недешевый продукт компании ColeSoft Marketing Inc.
  - Самое мощное средство динамического анализа для z/OS из существующих
- TDF (Trap Debug Facility)
  - Разрабатывается Arney Computer Systems
  - Есть слабые ограничения на окружение

Методы трассировки

- Неправильный код команды (ESTAE/ESPIE)
  - Записываем вместо целевой инструкции 0 и обрабатываем ошибки
- SVC hooking
  - Захватываем некоторое SVC и заменяем целевые инструкции на его вызов
- TRAP
  - Устанавливаем TRAP подпрограмму и заменяем целевые инструкции на ее вызов
- Неправильный адрес модуля
  - Перехватываем загрузку модуля, чтобы выдавать неправильный адрес, обрабатываем ошибки

Сравнение производительности

```
********************************** TOP OF DATA ***********************************
Start loop: 3
Step count: 100
=============================================
|ESTAI      |SVC        |TRAP       |ESPIE      |
|TIME       |TIME       |TIME       |TIME       |
|      12789|        928|          3|         88|
|      12927|        523|          2|        131|
|      12766|        370|          2|        137|
                  . . .
|      13795|        566|          5|        134|
|      14418|        506|          5|        126|
|      14794|        456|          3|        124|
|      13710|        846|          3|        146|
|      14356|        539|          4|        125|
|      12841|        438|          3|         85|
|      13299|        438|          3|         92|
=============================================
|   13872.62|     484.84|       3.79|     134.58|general average
=============================================
|1923044.00|   17886.49|       4.20|     979.24|general dispersion
******************************** BOTTOM OF DATA **********************************
```

Сравнение производительности

```
********************************** TOP OF DATA ************************************
Start loop: 15
Step count: 100
=============================================
|ESTAI      |SVC        |TRAP       |ESPIE      |
|TIME       |TIME       |TIME       |TIME       |
|      53374|        910|          4|        414|
|      54774|        356|          3|        490|
|      54845|        374|          3|        355|

|      55664|        499|          4|        356|
|      55815|        375|          3|        412|
|      56038|        392|          5|        348|
|      55783|        376|          4|        360|
|      55021|        392|          3|        376|
|      58700|        387|          4|        528|
|      54528|        379|          3|        407|
=============================================
|  56568.33|    401.08|      3.84|    435.55|general average
=============================================
|9667926.34|   4783.53|      3.57|   7538.69|general dispersion
******************************** BOTTOM OF DATA ***********************************
```

Методы трассировки

- Неправильный код команды (ESTAI/ESPIE)
  - Метод достаточно медленный (ESTAI)
  - Сильные ограничения на окружение
- SVC hooking
  - Метод быстрый
  - Средние ограничения на окружение
  - Привилегированный режим
- TRAP
  - Очень быстрый метод
  - Слабые ограничения на окружение
- Неправильный адрес модуля
  - Обнаружена серьезная проблема

SVC hooking

SVC hooking

- Реализовано в z/XDC и IDF
- Работает в любом окружении z/OS кроме SRB, cross memory mode
- Проще в реализации, чем TRAP
- Специфика реализации позволяет добавить TRAP трассировку для SRB и cross memory

Пример вывода

```
********************************** TOP OF DATA ***********************************
THREAD=START====================
 DEPARTURE                        DESTINATION
 MDL NAME  | CSECT NM  | OFFSET | MDL NAME  | csect NM  | OFFSET |

SMPL1M1    | SMPL1M1   |      8 | SMPL1M1   | SMPL1M1   |     14 |

SMPL1M1    | SMPL1M1   |     34 | SMPL1M1   | SMPL1M1   |     80 |

SMPL1M2    | SMPL1M2   |      8 | SMPL1M2   | SMPL1M2   |     14 |

SMPL1M3    | SMPL1M3   |      8 | SMPL1M3   | SMPL1M3   |     14 |

SMPL1M4    | SMPL1M4   |      8 | SMPL1M4   | SMPL1M4   |     14 |

SMPL1M4    | SMPL1M4   |     5E | SMPL1M3   | SMPL1M3   |     5C |

SMPL1M3    | SMPL1M3   |     76 | SMPL1M2   | SMPL1M2   |     5C |

SMPL1M2    | SMPL1M2   |     76 | SMPL1M1   | SMPL1M1   |     B0 |

SMPL1M1    | SMPL1M1   |     CA |           |           |      0 |
THREAD=END======================

THREAD=START====================
 DEPARTURE                        DESTINATION
 MDL NAME  | CSECT NM  | OFFSET | MDL NAME  | csect NM  | OFFSET |

SMPL1M6    | SMPL1M6   |      8 | SMPL1M6   | SMPL1M6   |     14 |

SMPL1M6    | SMPL1M6   |     50 | SMPL1M6   | SMPL1M6   |     58 |

SMPL1M6    | SMPL1M6   |     58 | SMPL1M6   | SMPL1M6   |     54 |

SMPL1M6    | SMPL1M6   |     54 | SMPL1M6   | SMPL1M6   |     5C |

SMPL1M6    | SMPL1M6   |     84 |           |           |      0 |
THREAD=END======================

******************************** BOTTOM OF DATA **********************************
```

Разработано

- Программа, реализующая все четыре метода перехвата прыжков
  - Тестирование скорости
  - Код для TRAP и ESTAE можно переносить в тестировщик
- Прототип трассировщика на SVC hooking
  - Разработан аналог соответствующим механизмам в IDF и z/XDC
  - Работает в любом окружении z/OS кроме SRB, cross memory mode
  - Нет проблем с авторизацией в отличие от TRAP
  - Позволяет добавить использование TRAP подпрограммы для трассировки

Дальнейшие действия

- Добавление поддержки SRB и разных режимов адресных пространств:
  - Добавление TRAP подпрограммы трассировки
  - Развитие анализатора кода
- Поиск способов трассировки SRB в secondary address space mode
- Реализация интерфейса для задания входных наборов данных