УДК 004.453.5

Н.Н. Самарин

АЛГОРИТМ ПОЛУЧЕНИЯ И ИНТЕРПРЕТАЦИИ ДАННЫХ ИЗ ЖУРНАЛА РАБОТЫ ВИРТУАЛЬНОЙ МАШИНЫ

Приведено исследование журнала работы виртуальной машины Bochs, которая предусматривает полную эмуляцию аппаратного обеспечения платформы x86. Цель работы заключается разработке алгоритма получения и интерпретации данных из журнала работы виртуальной машины с возможностью их дальнейшего использования при анализе областей памяти вычислительной системы.

Ключевые слова: виртуальная машина, программное обеспечение без исходного кода, область памяти, процессор, линейный адрес, физический адрес, недекларированные возможности.

Известно, что виртуальные машины часто применяются с целью предотвращения заражения работоспособной системы вредоносными программами, а также исключения аварийных ситуаций связанных с ошибками конфигурации гостевых систем, также системы виртуализации используются для анализа программного обеспечения без исходного кода на недекларированные возможности. Виртуальным машинам выделяются физические ресурсы хостовой системы, которые они используют для функционирования гостевых операционных систем, а также общего, прикладного и специального программного обеспечения работающего под управлением операционной системы.

Существуют несколько типов систем виртуализации: полная виртуализация, нативная виртуализация, виртуализация адресного пространства, паравиртуализация, виртуализация уровня операционной системы и виртуализация уровня приложений. Отличаются они степенью эмуляции аппаратного обеспечения. Остановимся подробно на полной виртуализации (эмуляции). Данный тип виртуализации основан на полной эмуляции аппаратного обеспечения платформы x86 и позволяет выполнять операционные системы, разработанные для процессоров IBM PowerPC.

Полная виртуализация применяется при разработке программного обеспечения под новые процессоры, которые еще не реализованы, а также низкоуровневой отладки операционных систем, так как предоставляет возможность отслеживать инструкции виртуального процессора. Учитывая полную эмуляцию системы и всех инструкций виртуального процессора, указанный вид виртуализации обладает очень низким быстродействием гостевой системы. Примерами таких эмуляторов являются Bochs, Hercules Emulator, QEMU (без ускорения). Для дальнейших исследований будем рассматривать виртуальную машину Bochs [2].

В ходе эмуляции работы виртуальной машины Bochs формирует файл журнала отладчика. Фрагмент файла журнала указан на рис.1.

```
(0).[386] [0x0000000f06ad] f000:06ad (unk. ctxt): and al, 0x02
(0).[387] [0x0000000f06af] f000:06af (unk. ctxt): test al, al
(0).[388] [0x0000000f06b1] f000:06b1 (unk. ctxt): jz .+27 (0x000f06ce)
(0).[389] [0x0000000f06ce] f000:06ce (unk. ctxt): pop bp
[CPU0 RD] LIN 0x0000ffc8 PHY 0x00000000ffc8 (len=2, pl=0): 0xFFD2
(0).[390] [0x0000000f06cf] f000:06cf (unk. ctxt): ret
[CPU0 RD] LIN 0x0000ffca PHY 0x00000000ffca (len=2, pl=0): 0x081D
(0).[391] [0x0000000f081d] f000:081d (unk. ctxt): add sp, 0x0004
(0).[392] [0x0000000f0820] f000:0820 (unk. ctxt): mov ax, word ptr ss:[bp+8]
[CPU0 RD] LIN 0x0000ffda PHY 0x00000000ffda (len=2, pl=0): 0x0166
(0).[393] [0x0000000f0823] f000:0823 (unk. ctxt): inc ax
(0).[394] [0x0000000f0824] f000:0824 (unk. ctxt): mov word ptr ss:[bp+8], ax
[CPU0 WR] LIN 0x0000ffda PHY 0x00000000ffda (len=2, pl=0): 0x0167
(0).[395] [0x0000000f0827] f000:0827 (unk. ctxt): push word ptr ss:[bp+6]
[CPU0 RD] LIN 0x0000ffd8 PHY 0x00000000ffd8 (len=2, pl=0): 0xF000
[CPU0 WR] LIN 0x0000ffce PHY 0x00000000ffce (len=2, pl=0): 0xF000
(0).[396] [0x0000000f082a] f000:082a (unk. ctxt): push word ptr ss:[bp+8]
```

Условные обозначения :

- Отчет о работе с памятью
- Номер такта процессора
- Операция записи в память
- Линейный адрес памяти
- Физический адрес памяти
- Операция чтения из памяти

Рис. 1. Фрагмент журнала работы виртуальной машины

На рис. 1. приведена информация о номерах тактов процессора, которые формируются в процессе работы виртуальной машины, сведения об операциях чтения из памяти и записи в неё, а так же указан линейный и физический адрес памяти. Из изложенного следует, что осуществляя выборку сведений из журнала работы виртуальной машины об операциях чтения и записи по конкретным адресам в области оперативной памяти, можно осуществлять контроль за всем программным обеспечением, которое функционирует под управлением гипервизора. Строки журнала содержат линейные адреса ячеек памяти, участвующих в операциях. Благодаря этому на основе данных журнала можно организовать отражение активности памяти на образ памяти в виде линии (первое измерение диаграммы состояния), а порядок в последова-

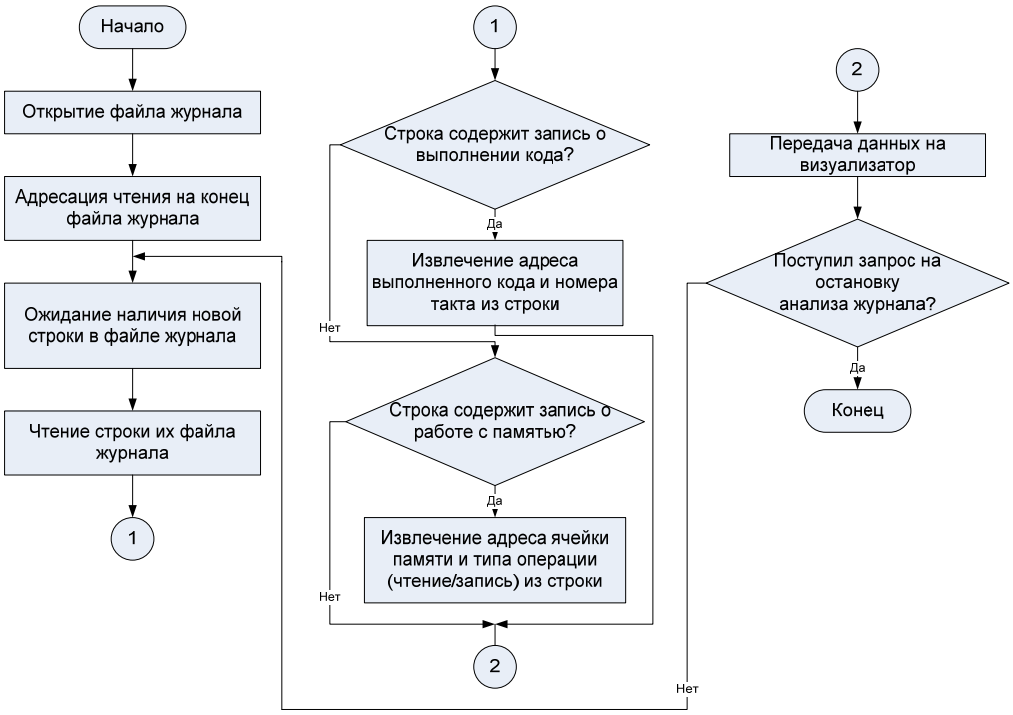

Рис. 2. Алгоритм получения и интерпретации данных из журнала работы виртуальной машины Bochs

тельности записей журнала может соответствовать строкам отображения активности (второе измерение диаграммы состояния).

Учитывая наши предположения, разработаем алгоритм получения и интерпретации данных из журнала работы виртуальной машины, который изображен на рис. 2.

Получаемые сведения пригодны для дальнейшего использования в процессе создания ленты событий об использовании областей памяти и ее визуализации. Указанный алгоритм в настоящее время апробируется в программном комплексе контроля и визуализации областей памяти электронной вычислительной системы [1].

Подводя итог выше сказанному, можно сделать следующие выводы:

Сведения, содержащиеся в журнале файла отладчика виртуальной машины, могут быть использованы для сбора данных о предоставлении операционной системе и программному обеспечению областей памяти, которая выделена виртуальной машине.

По адресам может быть выполнен контроль областей памяти использованных как операционной системой, так и программным обеспечением, в том числе возможно содержащим недекларированные возможности.

Требуется разработать программный комплекс контроля и визуализации областей памяти, которые используются программным обеспечением без исходного кода возможно содержащим недекларированные возможности.

СПИСОК ЛИТЕРАТУРЫ

1. *Самарин Н.Н.* Программный комплекс контроля и визуализации областей памяти электронной вычислительной системы / Баженов А.С., Борисов А.В. // Заявка на свидетельство о государственной регистрации программы для ЭВМ. №2013618878 от 03.10.2013.

2. *Исходные тексы* программ. [Электронный ресурс]. Режим доступа: http://bochs.sourceforge.net. ГИАБ

КОРОТКО ОБ АВТОРЕ

Самарин Николай Николаевич – начальник отдела, e-mail: samarin_nik@mail.ru, Федеральное государственное унитарное предприятие «Научно-исследовательский институт «Квант».

UDC 004.453.5

THE ALGORITHM OF THE RECEIVING AND INTERPRETING DATA FROM THE RUNTIME JOURNAL OF THE VIRTUAL MACHINE

Samarin N.N., Head of Division, Federal State Unitary Enterprise "Research Institute" Quantum", e-mail: samarin_nik@mail.ru

The article contains the research of the runtime journal of Bochs virtual machine that provides a complete hardware emulation of the x86 platform. The aim of the article is to develop the algorithm of the receiving and interpreting data from the runtime journal of the virtual machine with the possibility to use it in analysis of the memory areas of the computing system.

By implementing a sample log information about the virtual machine read and write operations on specific locations in the area of memory, it is possible to monitor all the software that runs under a hypervisor. On this basis, the algorithm of obtaining and interpreting the data from the job log of the virtual machine.

Key words: *virtual machine, sourceless software, memory area, processor, linear address, physical address, undocumented feature.*

REFERENCES

1. Samarin N.N. The program complex control and visualization of the memory areas of computer systems / Bazhenov, AS, AV Borisov / / The application for a certificate of state registration of the computer. Number 2013618878 from 10/03/2013.

2. Text source programs. [Electronic resource]. Access: http://bochs.sourceforge.net.