А. Е. Жуков, И. Ю. Коркин, Б. М. Сухинин

МОДЕЛИ ВЫПОЛНЕНИЯ ПРОЦЕССОРНЫХ ИНСТРУКЦИЙ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ СО СТОРОНЫ НАРУШИТЕЛЯ ДЛЯ КОМПЬЮТЕРНЫХ СИСТЕМ С ПОДДЕРЖКОЙ ТЕХНОЛОГИИ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ

Современные процессоры с поддержкой технологии аппаратной виртуализации не только расширили эксплуатационные возможности ЭВМ, но и создали новые угрозы информационной безопасности. Программное обеспечение, использующее технологию аппаратной виртуализации (ПОАВ, гипервизор), функционирует на архитектурном уровне, более привилегированном, чем уровень операционной системы (ОС). Поскольку обнаружить такое ПО средствами ОС невозможно, решалась задача разработки теоретических основ для создания методов обнаружения ПОАВ в условиях противодействия со стороны нарушителя.

При этом в качестве подхода к решению поставленной задачи использовалось вероятностно-временное моделирование функционирования процессора при выполнении набора процессорных инструкций (трассы), безусловно перехватываемых ПОАВ.

Согласно работе [1], в случае отсутствия ПОАВ процессор может находиться в одном из двух режимов: в защищенном (R-режиме), в котором выполняются пользовательские инструкции и трасса, и в режиме системного управления (S-режиме).

Если в качестве основного принять первый режим, то смену указанных режимов в случае отсутствия ПОАВ можно представить схемой, приведенной на рис. 1.

При получении прерывания системного управления SMI (System Management Interrupt) процессор переходит из R- в S-режим, а возврат происходит при выполнении инструкции RSM (Resume from System Management mode). При отсутствии прерывания SMI переход из R- в S-режим не происходит.

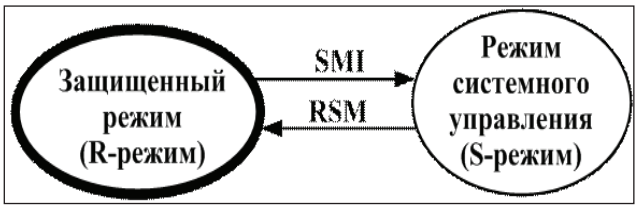

Рис. 1. Схема переключения между режимами работы процессора при выполнении трассы в случае отсутствия ПОАВ в ЭВМ

В случае присутствия ПОАВ процессор может находиться не в двух, а в трех режимах: R- и S-режимы сохраняются и добавляется режим монитора виртуальных машин (VMX root mode, V-режим). В этом случае R-режим называется режимом гостевой машины (VMX non root mode).

На рис. 2 показана смена этих режимов, из которых R-режим принят в качестве основного, а режим S для удобства разнесен на S и S_1. При выполнении каждой инструкции трассы в R-режиме управление всегда передается в V-режим, из которого управление возвращается обратно (на рисунке это условно обозначено стрелками «VM Exit» и «VM Entry»).

При получении процессором прерывания SMI происходит переключение в S-режим, после чего управление возвращается в режим, в котором произошло прерывание. Такое переключение может произойти из R- либо из V-режима.

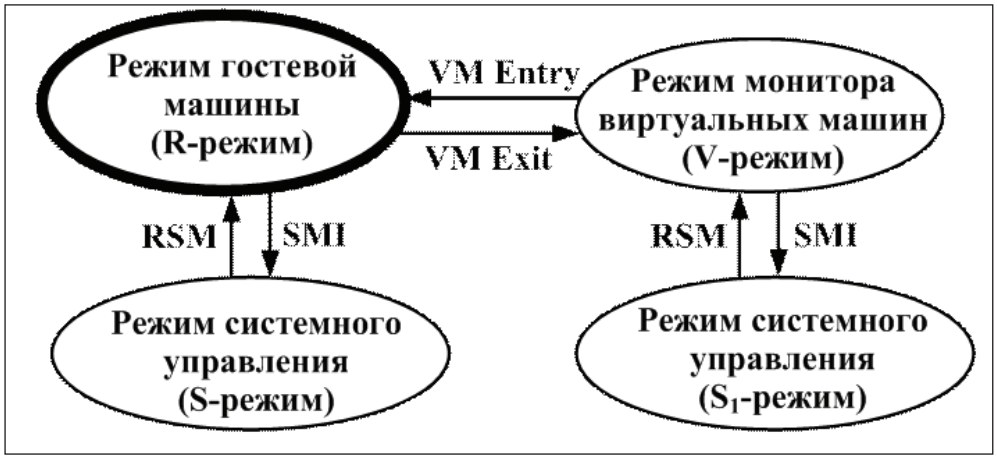

Рис. 2. Схема переключения между режимами процессора при выполнении трассы в случае присутствия одного образца ПОАВ

Поскольку в случаях отсутствия и присутствия ПОАВ появление прерывания SMI имеет случайный характер, процессор можно рассматривать как вероятностную систему, причем появление V-режима усиливает хаотичность смены режимов, вследствие чего вариабельность статистик длительности выполнения трассы возрастает.

Из рассмотренного также следует, что в случае присутствия ПОАВ трасса выполняется дольше, следовательно, частота переключений в S-режим будет больше. В результате длительность выполнения трассы и ее показатели вариабельности существенно возрастут.

Схему рис. 2 можно распространить и на случай, когда в ЭВМ не один, а несколько вложенных образцов ПОАВ. В этом случае процессор также может находиться в указанных выше трех режимах, но ситуация будет отличаться наличием нескольких обработчиков ПОАВ (Рис. 3). Каждый из них может быть прерван переключением в S-режим, который на схеме разнесли на S, S_1,..., S_e.

Рис. 3. Схема переключения между режимами работы процессора при выполнении трассы в случае присутствия нескольких вложенных образцов ПОАВ

Указанные обработчики ПОАВ работают в привилегированном V-режиме, который на схеме обозначен заштрихованным прямоугольником. При выполнении каждой инструкции трассы в R-режиме происходит переключение в V-режим и управление, как по цепочке, передается последовательно от первого к последнему обработчику ПОАВ, после чего управление возвращается в R-режим [2].

Прерывание SMI может приостановить работу любого из обработчиков ПОАВ (на схеме это обозначено стрелками «RSM» и «SMI»).

Как и в предыдущих случаях, функционирование процессора имеет вероятностный характер с тем отличием, что в случае нескольких вложенных образцов ПОАВ длительность выполнения трассы и хаотичность смены режимов еще более возрастают.

На основе представленных схем были построены модели длительности выполнения трассы процессором. При этом были приняты следующие допущения:

- все инструкции процессора выполняются последовательно на одном вычислительном устройстве;
- длительность выполнения каждой инструкции трассы одинакова и составляет k единиц (тактов);
- при получении управления образец ПОАВ в целях собственного сокрытия компрометирует счетчик тактов на некоторую постоянную величину δ;
- случайное число переключений процессора в S-режим при выполнении инструкции подчиняется биномиальному распределению.

На основании изложенного в случае отсутствия ПОАВ выполнение трассы можно представить в виде ориентированного помеченного мультиграфа (рис. 4) [3]. Его вершинами U_1, U_2, ..., U_{n_0} являются инструкции трассы, n_0 — число инструкций в трассе, n_s — число инструкций в обработчике S-режима, дуги соответствуют возможным переключениям между режимами процессора. При выполнении каждой инструкции трассы процессор может перейти с вероятностью ρ из R- в S-режим, на схеме это показано нижней дугой. Как альтернативный вариант инструкция выполняется в R-режиме без перехода в S-режим, на схеме это отмечено верхней дугой. Вероятность такого события $q = 1-\rho$.

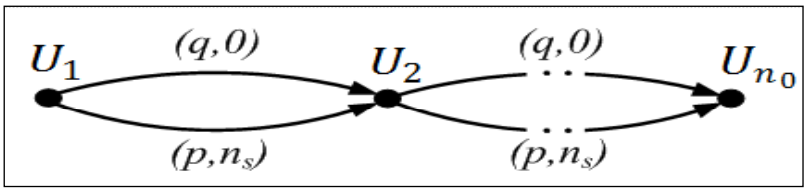

Рис. 4. Модель выполнения трассы в случае отсутствия ПОАВ

Длительность выполнения трассы t_{OT} из n_0 инструкций в случае отсутствия ПОАВ можно выразить следующим образом

$$t_{OT} = (n_0 + m_{OT} * n_S) * k, \quad (4)$$

где случайная величина m_{OT} , соответствующая числу переключений в S-режим, подчиняется закону биномиального распределения с параметрами n_0 и ρ [4].

В случае присутствия одного образца ПОАВ модель выполнения трассы представляется также ориентированным мультиграфом с помеченными дугами, который приведен на рис. 5, с тем отличием, что при выполнении каждой инструкции трассы U_i управление передается в ПОАВ, инструкции которого на рисунке помечены символами V_i, $i=1, ..., n_v$, где n_v — число инструкций в этом образце.

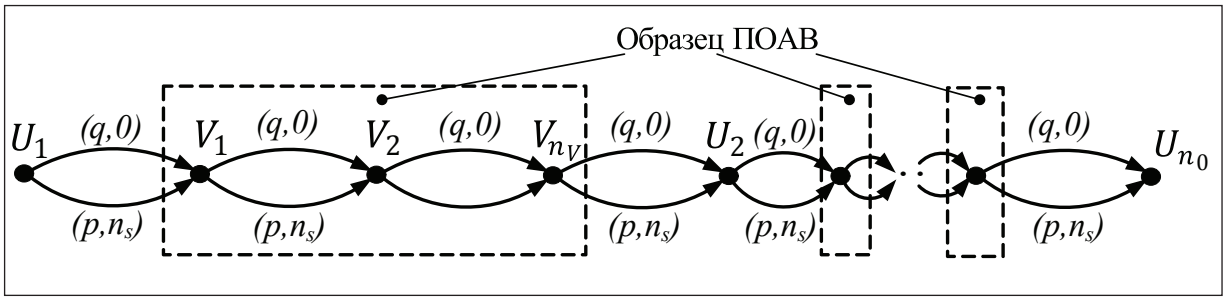

Рис. 5. Модель выполнения трассы в случае присутствия одного образца ПОАВ

При выполнении любых инструкций, как трассы, так и ПОАВ, возможен переход в S-режим (на рисунке это обозначено нижними дугами). Ситуации, когда таких переходов нет, обозначены верхними дугами.

Длительность выполнения трассы $t_{ПР}$ из n_0 инструкций в случае присутствия одного ПОАВ можно представить как

$$t_{ПР} = (n_0 + n_0 * n_V + m_{ПР} * n_S + n_0 * \delta) * k, \quad (2)$$

где $m_{ПР}$ — случайная величина, соответствующая числу переключений в S-режим, подчиняющаяся также закону биномиального распределения с параметрами $(n_0+n_0*n_v)$ и ρ; слагаемое n_0*n_v соответствует тому, что при выполнении каждой из n_0 инструкций трассы происходит переключение в V-режим (передача управления образцу ПОАВ). Нарушитель может противодействовать обнаружению ПОАВ с помощью компрометации значений счётчика тактов при выполнении каждой инструкции трассы. Компрометация заключается в прибавлении к значению счётчика тактов величины δ, $\delta < 0$, таким образом, слагаемое $n_0*\delta$ отражает описанное противодействие.

В случае присутствия нескольких вложенных образцов ПОАВ модель выполнения трассы представляется ориентированным мультиграфом с помеченными дугами (Рис. 6).

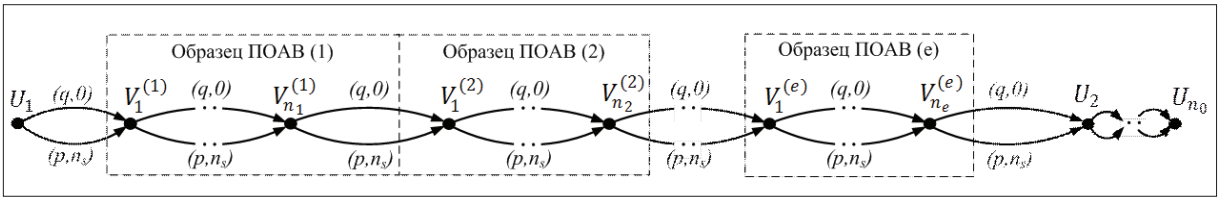

Рис. 6. Модель выполнения трассы в случае присутствия e-вложенных образцов ПОАВ

Данный граф аналогичен предыдущему графу за исключением того, что управление передается последовательно каждому образцу ПОАВ. Вершина $V_i^{(j)}$, где $i=1, \ldots, n_j$, $j=1, \ldots, e$, интерпретируется как i-я инструкция j-го образца ПОАВ; n_j— число инструкций в обработчике j-го ПОАВ; e — число вложенных образцов ПОАВ.

Тогда длительность выполнения трассы определяется как

$$t_{ВЛ} = (\, n_0 + n_0 * \sum_{j=1}^{e} n_j + m_{ВЛ} * n_S + n_0 * \sum_{j=1}^{e} \delta_j) \; * k, \quad (3)$$

где $m_{ВЛ}$ — случайная величина, соответствующая числу переключений в S-режим и подчиняющаяся закону биномиального распределения с параметрами $(n_0+n_0*\Sigma^e_{j=1}n_j)$ и ρ. При этом вероятность ρ переключения в S-режим осталась неизменной, а число инструкций, при выполнении которых возможен переход в S-режим (количество независимых испытаний в терминах схемы Бернулли), увеличилось по сравнению со случаем отсутствия ПОАВ на величину $n_0*\Sigma^e_{j=1}n_j$, свидетельствующую о возрастании числа переключений в S-режим. Сумма $\Sigma^e_{j=1}n_j$ обусловлена тем, что выполнение очередной инструкции трассы прерывается и обрабатывается поочередно каждым вложенным образцом ПОАВ. Слагаемое $n_0*\Sigma^e_{j=1}\delta_j$ означает суммарную величину компрометации счетчика при обработке трассы каждым образцом ПОАВ. При передаче управления j-му образцу ПОАВ он прибавляет к значению счетчика тактов величину δ_j, $\delta_j < 0$, $j = 1, \ldots, e$.

Из анализа модельных формул (1)—(3) следуют важные для обеспечения информационной безопасности выводы.

1. Так, при $\delta = -(\rho*n_s+1)*n_v$ у нарушителя появляется возможность такого искажения показаний счетчика, при котором по средним арифметическим длительности выполнения трассы

обнаружить ПОАВ невозможно. Для подобных ситуаций нужны такие статистики длительности выполнения трассы, исказить которые у нарушителя нет возможности.

Анализ показывает, а опыт подтверждает, что такими статистиками являются моменты кратных порядков длительности выполнения трассы.

Поскольку в выражениях (1) – (3) случайные величины $m_{ОТ}$, $m_{ПР}$ и $m_{ВЛ}$ принимают значения из фиксированного множества, то длительность выполнения трассы представляет собой также случайную величину, распределенную по фиксированным уровням, причем в случае присутствия ПОАВ число уровней длительностей выполнения трассы будет больше. При увеличении количества образцов ПОАВ в системе число уровней будет еще больше. Следовательно, по таким статистикам, как длина вариационного ряда и центр тяжести полигона частот, также можно обнаруживать ПОАВ.

Выводы

Предложенные модели выполнения трассы процессором позволили выявить ряд статистик длительности выполнения трассы, пригодных для обнаружения ПОАВ в компьютерных системах в условиях противодействия со стороны нарушителя.

СПИСОК ЛИТЕРАТУРЫ:

1. *Duflot L., Etiemble D. and Grumelard O.* Using CPU System Management Mode to Circumvent Operating System Security Functions // Proceedings of the 7th CanSecWest conference. Citeseer, 2006. P. 38–49.
2. *Коркин И. Ю.* Обнаружение вложенных мо-иторов виртуальных машин методами математической статистики // Материалы XX Общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 27 июня – 1 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета, 2011. С. 146–147.
3. *Харари Ф.* Теория графов. М.: Мир, 1973. – 300 с.
4. *Вентцель Е. С.* Теория вероятностей: Учебник для студ. вузов. 10-е изд., стер. М.: Издательский центр «Академия», 2005. – 576 с.