

ОБОСНОВАНИЕ КРИТЕРИЕВ ПРИСУТСТВИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЮЩЕГО ТЕХНОЛОГИЮ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ, В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Современные технологии аппаратной виртуализации компьютерных систем позволяют снижать затраты на эксплуатацию информационной инфраструктуры предприятия, однако создают новые угрозы информационной безопасности, поскольку допускают бесконтрольное выполнение высоко привилегированного кода — программного обеспечения, использующего технологию аппаратной виртуализации (ПОАВ, гипервизора), прозрачно для пользователя и средств защиты информации.

Для предотвращения нелегального присутствия гипервизора в компьютерных системах выявлены статистики длительности выполнения трассы (ДВТ), позволяющие обнаруживать такие программные закладки в условиях противодействия [1].

Целью данной публикации является теоретическое обоснование предложенных критериев [2].

Согласно [1] ДВТ в случаях отсутствия и присутствия ПОАВ t_{OT} и t_{PP} выражается как

$$t_{OT} = (n_0 + m_{OT} * n_S) * k \quad (1)$$

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

где n_0 — количество инструкций в трассе; n_S и n_V — количество инструкций в обработчике процессорного режима системного управления (S-режим) и в обработчике режима ПОАВ соответственно; m_{OT} и m_{PP} — случайные величины, соответствующие числу переключений процессора в S-режим и подчиняющиеся закону биномиального распределения с параметрами $[n_0, p]$ и $[n_0 + n_0 * n_V, p]$ соответственно для случаев отсутствия и присутствия ПОАВ; k — длительность выполнения одной инструкции; δ — величина компрометации счётчика тактов со стороны нарушителя при выполнении каждой инструкции в трассе ($\delta < 0$).

Поскольку у нарушителя имеется возможность исказить показания счётчика тактов так, что выборочные средние ДВТ в случаях отсутствия и присутствия ПОАВ становятся неразличимыми, эти характеристики распределения ДВТ становятся непригодными для обнаружения ПОАВ. С другой стороны, как показывает опыт, такие статистики, как дисперсия $\hat{\sigma}^2$, момент 4-го порядка $\hat{v}_2$, длина вариационного ряда $\hat{l}$, при соблюдении определённых условий могут быть применены для обнаружения ПОАВ в случаях противодействия со стороны нарушителя [1], [3].

Теоретическими предпосылками для этого могут быть следующие.

Пусть в выражениях (1) и (2) параметры $n_0, n_S, n_V, \delta, k \in \mathbb{Z}; p \in \mathbb{R}$ — некоторые фиксированные значения; T_{OT} и T_{PP} — выборки объёма n , полученные при реализации случайных величин t_{OT} и t_{PP} ДВТ в случаях отсутствия и присутствия ПОАВ соответственно. Пусть $\vec{t}_n = (t_1, \dots, t_n)$ — выборка объёма n из генеральной совокупности $T: T = T_{OT} \cup T_{PP}$.

Критерий присутствия образца ПОАВ на основе дисперсии

Критическое множество (образец ПОАВ присутствует): $W = \{\vec{t}_n: \hat{\sigma}^2(\vec{t}_n) \geq [\hat{\sigma}^2]\}$, где $\hat{\sigma}^2$ — выборочная дисперсия, $[\hat{\sigma}^2] \in \mathbb{Z}$ — пороговое значение, определяемое экспериментом; $\vec{t}_n \notin W$.

Принимаемое решение: если $\vec{t}_n \in W$, то образец ПОАВ присутствует, если $\vec{t}_n \notin W$, то образец ПОАВ отсутствует.

Аналогично формулируются и другие критерии на основе выборочного момента 4-го порядка $\hat{v}_2$ и длины вариационного ряда $\hat{l}$. При этом пороговые значения $[\hat{v}_2]$ и $[\hat{l}]$, соответствующие вероятности ошибок первого и второго рода α и β , а также объём выборки n



определяются экспериментально. Предложенные критерии присутствия образца ПОАВ требуют экспериментальной проверки и уточнения.

Утверждение 1. Пусть $D_\varepsilon[\vec{t}_n]$ – выборочная дисперсия выборки $\vec{t}_n$, тогда справедливо следующее

$$D_\varepsilon[t_{\text{ПР}}] = D_\varepsilon[t_{\text{ОТ}}] * (n_V + 1) \quad (3)$$

Доказательство.

Из (1) и (2) с учётом [3-4] следует, что

$$\begin{aligned} D_\varepsilon[t_{\text{ОТ}}] &= n_0 * (1 - p) * p * k^2 * n_S^2, \\ D_\varepsilon[t_{\text{ПР}}] &= n_0 * (1 - p) * p * k^2 * n_S^2 * (n_V + 1). \end{aligned}$$

Тогда

$$\frac{D_\varepsilon[t_{\text{ПР}}]}{D_\varepsilon[t_{\text{ОТ}}]} = \frac{n_0 * (1 - p) * p * k^2 * n_S^2 * (n_V + 1)}{n_0 * (1 - p) * p * k^2 * n_S^2} = n_V + 1,$$

откуда следует, что утверждение (3) справедливо.

Это значит, что выборочная дисперсия ДВТ может служить базой для разработки критерия присутствия ПОАВ в компьютерных системах.

Утверждение 2. Пусть $\mu_\varepsilon[\vec{t}_n]$ – выборочный центральный момент 4-го порядка выборки $\vec{t}_n$, тогда при $n_0 > 2$ справедливо следующее

$$\mu_\varepsilon[t_{\text{ПР}}] > \mu_\varepsilon[t_{\text{ОТ}}]. \quad (4)$$

Доказательство.

Из (1) и (2) следует [4], что

$$\begin{aligned} \mu_\varepsilon[t_{\text{ОТ}}] &= n_0 * p * q * (3 * (n_0 - 2) * p * q + 1), \\ \mu_\varepsilon[t_{\text{ПР}}] &= (n_0 + n_0 * n_V) * p * q * (3 * (n_0 + n_0 * n_V - 2) * p * q + 1). \end{aligned}$$

Из полученных равенств следует, что

$$\frac{\mu_\varepsilon[t_{\text{ПР}}]}{\mu_\varepsilon[t_{\text{ОТ}}]} = 1 + 6 * \frac{n_0 * n_V}{3 * (n_0 - 2) + \frac{1}{p * q}} > 1,$$

откуда при $n_0 > 2$ следует справедливость утверждения (4).

Доказанное свидетельство о возможности создания критерия присутствия ПОАВ на базе момента 4-го порядка ДВТ.

Гипотеза. Пусть $\hat{l}[\vec{t}_n]$ – длина вариационного ряда выборки $\vec{t}_n$, тогда

$$\hat{l}[t_{\text{ПР}}] > \hat{l}[t_{\text{ОТ}}]. \quad (5)$$

Доказательство.

Из сравнения выражений (1) и (2) следует, что число переключений между режимами работы процессора в случае присутствия образца ПОАВ существенно больше, чем в случае его отсутствия.

Откуда следует, что в случае присутствия образца ПОАВ количество фиксированных значений $t_{\text{ПР}}$ должно быть больше, чем в случае его отсутствия, поэтому справедливо (5).

Это подтверждается как результатами вычислительных экспериментов, выполненных с использованием модельных формул (1) и (2) (см. рис. 1), так и многочисленными экспериментами.



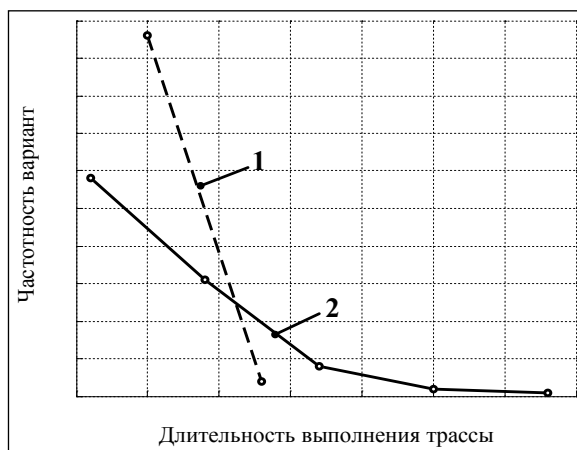


Рис. 1. Графики полигонов двух модельных распределений в случае отсутствия (1) и присутствия ПОАВ (2)

Из этого следует, что длину вариационного ряда ДВТ также можно использовать для обнаружения ПОАВ.

Вместе с тем, как показывает практика, непосредственное использование предложенных статистик ДВТ для обнаружения гипервизора возможно далеко не всегда. Необходимо учитывать, что из-за недостаточной воспроизводимости опытных данных [5] могут возникнуть проблемы с определением границ интервалов варьирования статистик, по которым вычисляются их пороговые значения.

Как показали исследования, эти проблемы преодолеваются, если повторные опыты выполнять до наступления стабилизации границ интервалов варьирования определяемых статистик при соответствующем уровне фильтрации получаемых опытных данных о ДВТ [1].

Экспериментальная проверка подтвердила достоверность предложенных критериев для обнаружения не только одиночных, но и нескольких вложенных гипервизоров в компьютерных системах.

СПИСОК ЛИТЕРАТУРЫ:

1. Korkin I. Strong approach to hardware-VM rootkits detection. Hakin9 Extra Magazine, English Edition. Issue 6/2011. P. 30–35. ISSN 1733-7186.
2. Жуков А. Е., Коркин И. Ю., Сухинин Б. М. Модели выполнения процессорных инструкций в условиях противодействия со стороны нарушителя для компьютерных систем с поддержкой технологии аппаратной виртуализации // Безопасность информационных технологий. 2012. № 2 (в печати).
3. Коркин И. Ю. Критерий обнаружения монитора виртуальных машин в компьютерных системах. // Материалы XIX Общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 5–10 июля 2010 года. Санкт-Петербург. Издательство Политехнического университета. 2010. С. 113–114.
4. Вентцель Е. С. Теория вероятностей: Учебник для студ. Вузов / Елена Сергеевна Вентцель. 10-е изд., стер. М.: Издательский центр «Академия». 2005. — 576 с.
5. ГОСТ Р ИСО 5725 2002 Точность (правильность и прецизионность) методов и результатов измерений, части 1-6, М.: ИПК Издательство стандартов, 2002.

