ОПРЕДЕЛЕНИЕ ПРИНАДЛЕЖНОСТИ ФАЙЛОВЫХ ОБЪЕКТОВ К ПРОГРАММНО-АППАРАТНОЙ ПЛАТФОРМЕ НА ОСНОВЕ АНАЛИЗА ВРЕМЕННЫХ ОТМЕТОК

В. В. Бакланов[1], *Р. В. Гибилинда*[2]
([1] Екатеринбург, УрФУ, baklanov_v_v@mail.ru;
[2] Екатеринбург, gibilinda91@gmail.com)

Идея использования временных отметок (далее ВО) файлов для криминалистического анализа компьютерных систем принадлежит Брайану Кэрриэ [1]. Авторы настоящей статьи провели серию масштабных наблюдений за ВО файлов в NTFS Windows XP, Vista, 7. На основании проведенного анализа была спрогнозирована возможность ретроспективного анализа файловых операций по комбинации ВО. 12 внешних ВО, имеющиеся у каждого файла, позволяют достоверно определить прошлое файла на глубину до 5–6 операций [2].

К сожалению, точность анализа в сильной степени зависит от точности отсчета времени, которая определяется аппаратными и программными таймерами. Под программным таймером понимается реализованный в системе или слое аппаратной абстракции (например, HAL.dll) алгоритм, который задает численное значение отсчетов времени на основании счета тиков генератора синхронизирующих импульсов (далее ГСИ). В качестве аппаратного таймера используется кварцованный ГСИ материнской платы ЭВМ. Стабильность частоты сигналов ГСИ достигает $10^{-5}...10^{-7}$, что позволяет рассчитывать на высокую точность измерения времени без дополнительных схемных решений стабилизации частоты колебаний контура ГСИ. Однако подобная точность таймера не позволяет 100 наносекундную дискретность, выбранную фирмой Microsoft для 8-байтных ВО. Для оценки влияния таймерного интервала (далее ТИ) на точность формируемых ВО файлов авторами была проведена дополнительная серия наблюдений.

Исследовались аппаратные платформы:

- однопроцессорная система на базе Intel Pentium 4 (без HT);

• однопроцессорная система на базе двухъядерного Intel Core2duo;

• однопроцессорная система на базе двухъядерного Intel Atom;

Все перечисленные системы работают под управлением ОС: Windows XP Professional, Windows 7 Home premium, Windows 8.1 Professional.

Изменение значения таймера проводилось программным путем с помощью системного вызова NtSetTimerResolution [3]. Доступ к этому вызову можно получить с помощью функции timeBeginPeriod() [4]. Функция объявлена в Mmsystem.h и Windows.h. В описании сказано, что аргумент функции представляет собой числозначение таймера в миллисекундах, которое требуется установить. Была создана программа, которая присваивает системному таймеру различные значения. Для измерения текущего значения таймера использовалась утилита Марка Руссиновича ClockRes.exe [5].

В результате работы программы зафиксированы следующие наблюдения:

1. Установка системного таймера глобальна для всех приложений и системы в целом;

2. Установленное значение системного таймера обладает свойством модальности. Система всегда устанавливает значение ТИ по умолчанию, если иного не требует выполняющееся в данный момент времени приложение. В случае, если приложение вызывает timeBeginPeriod(), значение заданного ТИ действует до конца работы приложения или до вызова timeEndPeriod();

3. Нельзя задать произвольное значение ТИ. Аргумент функции timeBeginPeriod() представляет собой беззнаковое целое число, отличное от нуля. В то же время системный таймер по умолчанию имеет нецелое значение, и еще некоторые его значения можно получить в качестве дробного числа. Это зависит от того, каким образом обеспечивается вызов NtSetTimerResolution();

4. Значения ТИ для timeBeginPeriod() фиксированы (таблица).

Авторами были сделаны выводы о возможности использования этой информации в задачах обеспечения информационной безопасности. Анализ ВО дает возможность определить принадлежность файла конкретной программно-аппаратной платформе (далее ПАП)

Значения ТИ в различных версиях ОС Windows

Значение аргумента функции timeBeginPeriod()	Значение ТИ, полученного утилитой ClockRes, ms		
	Windows 7	Windows XP	Windows 8.1
1	1	0,997	1
2	1,25	1,953	2
3	2,5	1,953	3
4	2,5	3,906	4
5	5	3,906	5
6	5	3,906	6
7	5	3,906	7
8	5	15,625	8
9	5	15,625	9
10	10	15,625	10
11	10	15,625	11
12	10	15,625	12
13	10	15,625	13
14	10	15,625	14
15	10	15,625	15
16 и далее	15,6	15,625	15,625

по нескольким характерным следам. Во-первых, стандартное файловое копирование на другую ПАП позволяет провести анализ ВО файла на предмет его происхождения, так как NTFS создаст ВО уже на новой ПАП с учетом конкретного значения ТИ, но не полностью уничтожая информацию о прошлых значениях. Можно использовать побитовое копирование части раздела с файловым объектом с целью сохранения всех ВО конкретной ПАП. Во-вторых, существует возможность определения принадлежности объекта с помощью анализа внутренних отметок файлов на предмет определения значения ТИ и сравнения его с текущим на исследуемой ПАП. Важно

отметить, что внутренние ВО должны иметь высокую точность, т. е. иметь более 4 байт дискового пространства под каждую ВО. В-третьих, есть возможность переноса файлов в архиве. В Windows XP, 7, 8.1 при разархивировании у файлового объекта создаются текущие ВО о создании и последнем доступе, но сохраняется время последней модификации. Исходя из вышесказанного, в дальнейшем под переносом будет подразумеваться такая процедура копирования информации, при которой ВО файловых объектов сохраняются на новой ПАП:

1. Файлы, созданные в Windows XP и перенесенные в Windows 7, можно определить в случаях, если значение ТИ отличалось от значения по умолчанию. В случае значения по умолчанию системного таймера кратность интервалов изменения ВО можно обосновать девиацией значения таймера, что усложняет определение происхождения файлового объекта.

2. Если кратность интервалов изменения ВО файлов будет целой с учетом деления на 500 ± 15 мкс, то можно однозначно говорить о том, что файлы принесены с Windows XP, так как данное значение ТИ регулярно появляется при попытках зафиксировать ТИ.

3. Файлы, созданные в Windows 7 и перенесенные в Windows XP, можно определить в случаях, если значение ТИ составляло 1.25, 2.5, 5, 10 мс.

4. Файлы, созданные в Windows 7 или Windows XP и перенесенные в Windows 8.1, можно определить при любом значении ТИ, кроме значения по умолчанию. Объясняется это тем, что девиация таймера в Windows 8.1 достаточно мала. Тем не менее, если кратность интервала изменения ВО будет целым числом при делении на девиационное значение ТИ, превышающее максимальное значение в Windows 8.1, то можно однозначно говорить о том, что файлы перенесены из Windows XP или Windows 7.

5. Файлы, созданные в Windows 8.1 и перенесенные в Windows XP или в Windows 7, можно определить в любом случае, кроме значения по умолчанию. Объясняется это тем, что получаемые значения ТИ в допустимом интервале в Windows 8.1 не могут быть получены на других ОС.

6. «Гвоздем программы» является значение ТИ по умолчанию, которое сильнейшим образом усложняет задачу анализа ВО. Рекомендуется создавать резидентное приложение, выставляющее при загрузке системы отличное от стандартного значение системного таймера, что позволит при оперативном анализе определить файлы, занесенные из другой ОС.

7. Исследование внутренних ВО напрямую связано с наличием таковых ВО внутри формата файла. Задача актуальна для распространенных форматов электронных документов, исполняемых файлов, графических файлов. Узкоспециализированные форматы могут иметь ВО с точностью до секунд или не иметь их вообще, что делает такие файлы непригодными для анализа. Однако эта исследовательская задача выходит за рамки данной статьи.

8. При анализе ВО с учетом влияния системного таймера можно проследить дополнительные возможности по обеспечению безопасности, а именно:

• определение факта НСД к ПАП. При анализе файлов за определенный промежуток времени не должны присутствовать файловые объекты с другими значениями системного таймера;

• тест защитных систем ПАП: появление файлового объекта с ВО о последнем изменении отличной по значению ТИ от таковой на исследуемой ПАП говорит о том, что файл занесен в архиве и, вероятно, не работает система запрета подключения внешних носителей. Наличие файлового объекта с ВО, отличными по точности с исследуемой ПАП, говорит о том, что было произведено побитовое копирование, следовательно, возможна загрузка с внешнего носителя либо неправильно настроен аудит событий, если использовался HEX-редактор.

Библиографические ссылки

1. *Кэрриэ Б.* Криминалистический анализ файловых систем. СПб. : Питер, 2007. 480 с. : ил.

2. *Бакланов В. В.*, *Князева Н. С.*, *Хорьков Д. А.* Анализ временных отметок файловой системы NTFS в операционной системе Microsoft Windows XP / // Проблемы информационной безопасности. Компьютерные системы. 2012. № 4. С. 25–32.

3. NtSetTimerResolution : информ. портал. URL: http://undocumented.ntinternals.net/UserMode/Undocumented%20Functions/Time/NtSetTimerResolution.html (дата обращения: 05.11.2013).

4. timeBeginPeriod function : информ. портал. URL: http://msdn.microsoft.com/en-us/library/windows/desktop/dd757624(v=vs.85).aspx (дата обращения: 05.11.2013).

5. Windows Sysinternals : информ. портал. URL: http://technet.microsoft.com/ru-ru/sysinternals/bb897568.aspx (дата обращения: 07.11.2013).

МЕТОД ЗАЩИТЫ ОТ ПЕРЕХВАТА ПАКЕТОВ АВТОРИЗАЦИИ ПРИ БЕСПРОВОДНОЙ ПЕРЕДАЧЕ ДАННЫХ

Д. О. Деденев, М. П. Трухин
(Екатеринбург, УрФУ, danes1@mail.ru)

Постановка задачи

В данной работе рассматривается принцип взаимодействия между пользователем и беспроводной точкой доступа, т. е. то, каким образом осуществляется процесс подключения к точке доступа, как и при каких условиях передается ключ аутентификации, возможно ли влияние посторонним оборудованием на канал связи между авторизированным устройством и точкой доступа.

Процедура поиска уязвимости

Воспользуемся операционной средой Black Track 5 R1, с помощью которой мы сможем пронаблюдать за поведением устройств, отсылающих запросы подключения.

Переведем наше беспроводное оборудование в режим прослушивания эфира, в результате чего сможем наблюдать обнаруженные точки доступа.

В следующем окне увидим, например, что у нас получилось найти 3 беспроводных точки доступа со следующим наименованием и их MAC-адресами (рис.1):

– Tarasun MAC = 00:25:86:25:9B:2C
– sv-home MAC = 00:15:6D:EE:EA:F6
– Allysia MAC = 54:E6:FC:BA:35:1C