НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2017 Том 17 № 3 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2017 Vol. 17 No 3 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.6

МЕТОДИКА ПРОВЕДЕНИЯ ПОСТИНЦИДЕНТНОГО ВНУТРЕННЕГО АУДИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

И.С. Пантюхин[a], И.А. Зикратов[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: zevall@cit.ifmo.ru

Информация о статье
Поступила в редакцию 02.03.17, принята к печати 12.04.17
doi: 10.17586/2226-1494-2017-17-3-467-474
Язык статьи – русский

Ссылка для цитирования: Пантюхин И.С., Зикратов И.А. Методика проведения постинцидентного внутреннего аудита средств вычислительной техники // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 3. С. 467–474. doi: 10.17586/2226-1494-2017-17-3-467-474

Аннотация

Представлена методика проведения постинцидентного внутреннего аудита средств вычислительной техники, позволяющая исследовать компьютерные инциденты в различных средствах вычислительной техники (в том числе в нескольких одновременно) в условиях постоянного роста числа компьютерных инцидентов, объема хранимой и обрабатываемой информации. Сведения о компьютерных инцидентах получаются путем анализа данных в энергозависимой памяти, энергонезависимой памяти и сетевом трафике. Задача решена путем анализа атрибутов и их значений, полученных с постинцидентного средства вычислительной техники. Разработана методика комплексного внутреннего аудита данных. Показан способ снижения временных затрат за счет использования анализа атрибутов и их значений. Методика включает в себя обработку данных, описание взаимосвязей между ними, применение интеллектуальных методов и алгоритмов. Даны описания этих элементов, их нотации и функциональное назначение. Выполнен расчет вычислительной сложности предлагаемой методики. Предлагаемая методика может найти применение при исследовании компьютерных инцидентов, для снижения временных затрат исследования компьютерных инцидентов, повышения точности и информативности проведения постинцидентного внутреннего аудита средств вычислительной техники. Предложенные решения могут быть применены при разработке проактивных систем защиты от компьютерных инцидентов.

Ключевые слова

методика, постинцидентный внутренний аудит, компьютерный инцидент, компьютерная криминалистика, информационная безопасность, средство вычислительной техники

POST-INCIDENT INTERNAL AUDIT PROCEDURE OF COMPUTER DEVICES

I.S. Pantiukhin[a], I.A. Zikratov[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: zevall@cit.ifmo.ru

Article info
Received 02.03.17, accepted 12.04.17
doi: 10.17586/2226-1494-2017-17-3-467-474
Article in Russian

For citation: Pantiukhin I.S., Zikratov I.A. Post-incident internal audit procedure of computer devices. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 3, pp. 467–474 (in Russian). doi: 10.17586/2226-1494-2017-17-3-467-474

Abstract

The paper presents post-incident internal audit procedure of computer equipment. It enables to study computer incidents in various computer equipment (including several ones simultaneously) in the conditions of a constant increasing number of computer incidents, the volume of stored and processed information. Information about computer incidents is obtained by analyzing data in volatile and non-volatile memory, and network traffic. The problem is solved by analyzing the attributes and their values obtained from the post-incident computer equipment and resources. The technique of complex internal data audit is presented. This approach (analysis of attributes and their values) reduces the time costs. This technique includes data processing, description of the interrelationships, the usage of intelligent methods and algorithms. The descriptions of these elements, their notations and functional purposes are presented. Calculation of the proposed technique computational complexity is given. The technique can be used to examine computer incidents. It reduces time costs for study, improves accuracy and increases information content of the post-incident internal audit of computer equipment. The proposed solutions can be used to develop proactive protection systems against computer incidents.

Keywords

technique, post-incident internal audit, computer incident, computer forensics, information security, computer devices

Введение

В настоящее время наблюдается постоянный рост числа компьютерных инцидентов, которые произошли в средствах вычислительной техники. Важной задачей является исследование таких компьютерных инцидентов, в частности, проведение постинцидентного внутреннего аудита. Под постинцидентным внутренним аудитом подразумевается восстановление событий инцидентов информационной безопасности, произошедших в средствах вычислительной техники. Постинцидентный внутренний аудит преследует цель получения данных со средства вычислительной техники и поиска в них информации об компьютерных инцидентах, которые могут находиться в дампах энергонезависимой памяти, энергозависимой памяти, сетевого трафика [1].

Существующие методики проведения постинцидентного внутреннего аудита средств вычислительной техники направлены на исследование отдельных типов памяти [2–4]. Как известно, сведения о современных компьютерных инцидентах можно получить путем анализа данных в энергозависимой памяти, в энергонезависимой памяти, в сетевом трафике, а также одновременно в них всех [5–7]. В этой связи исследование типов (дампов) памяти комплексно является актуальной задачей. Помимо этого, существующие решения основаны на анализе контента (содержимого данных типов компьютерной памяти и сетевого трафика), что в случае обработки большого объема данных и работы с большим количеством возможных компьютерных инцидентов значительно увеличивает время поиска и снижает точность обнаружения компьютерного инцидента [8]. В связи с этим встает задача разработки новых методик проведения постинцидентного внутреннего аудита средств вычислительной техники, отвечающих современному состоянию развития науки и техники, комплексному внутреннему аудиту типов компьютерной памяти средств вычислительной техники, росту числа компьютерных инцидентов, росту объемов хранимой и обрабатываемой информации.

Предлагаемая в работе методика позволяет проводить комплексный внутренний аудит данных с постинцидентных средств вычислительной техники (средства вычислительной техники, на которых произошли компьютерные инциденты). Анализ атрибутов и их значений с энергозависимой памяти, энергонезависимой памяти, сетевого трафика позволяет достичь снижения временных затрат и предоставляет возможность исследовать компьютерные инциденты в условиях постоянного роста хранимых и обрабатываемых данных. Применение интеллектуальных алгоритмов и методов позволяет достичь повышения точности и информативности получаемых сведений о компьютерном инциденте.

Описание методики

Для исследования компьютерных инцидентов со средств вычислительной техники была разработана методика. Она состоит из совокупности элементов (рис. 1), направленных на проведение комплексного внутреннего аудита данных с постинцидентного средства вычислительной техники, повышение точности и информативности сведений о компьютерном инциденте, снижение временных затрат получения сведений о компьютерных инцидентах. В работе под комплексным аудитом данных постинцидентного средства вычислительной техники понимается анализ энергонезависимой памяти, энергозависимой памяти, сетевого трафика. Важность комплексного аудита данных обусловлена тем, что сведения о современных компьютерных инцидентах могут находиться не только в одном типе компьютерной памяти, но и в нескольких одновременно. Примеры атрибутов и их значений представлены в табл. 1–3.

Path	/Windows/System32/DriverStore/FileRepository/prnep00a.inf_amd64_ neutral_92a4c727cdf4c2f7/Amd64/EP0NH43R.DLL
filename	EP0NH43R.DLL
MIME type	application/x-dosexec
Endianness	Littleendian
Creationdate	2009-07-14 01:28:27
permitions	777
Formatversion	PortableExecutable
extension	DLL
Comment	CPU
...	...

Таблица 1. Пример атрибутов и их значений, полученных с данных энергонезависимой памяти

Путем комбинирования атрибутов и их значений из энергозависимой памяти, энергонезависимой памяти, сетевого трафика можно добиться повышения информативности сведений о компьютерных инцидентах. Это достигается за счет представления данных (с дампов энергозависимой памяти, энергонезависимой памяти, сетевого трафика) в виде атрибутов и их значений со средств вычислительной техники, описания взаимосвязей между ними [1], применения интеллектуальных методов и алгоритмов. Данный подход позволяет исследовать компьютерные инциденты, которые произошли даже на нескольких ском-

прометированных устройствах. Рассмотрим функциональные элементы методики и протекающие в ней линейные процессы.

Под средствами вычислительной техники могут подразумеваться различные устройства, такие как персональные компьютеры, мобильные телефоны и планшеты, сервера. На всех средствах вычислительной техники есть энергозависимая память, энергонезависимая память, а также присутствует возможность получения сетевого трафика [9].

Offset (V)	"0xfffffa8000caf040"
Prevelegies	[2, SeCreateTokenPrivilege, "Create"]
PDB	"0x000000001d6a0000"
Process_path	"C:\Windows\system32\services.exe"
Exit-data-time	"2016-11-10 13:08:59 UTC+0000"
Dll_list	["0x00000000772c0000","0x1a9000","0xffff","C:\Windows\SYSTEM32\ntdll.dll"]
Handles	["0xfffff8a0012fd550", "0x4","0x9","Key","MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS"]
Connection	["0x3e32c2d0","TCPv6", ":::49156",":::0","LISTENING","-","-","-"]
Security	["S-1-5-18", "LocalSystem"]
...	...

Таблица 2. Пример атрибутов и их значений, полученных с данных энергозависимой памяти

Time	03:00:38
Date	2016-10-02
Source	192.168.1.253
TTL	1
Destination	66.102.9.99
SourcePort	1985
Protocol	HTTP
DestinationPort	1985
...	...

Таблица 3. Пример атрибутов и их значений, полученных с дампа сетевого трафика

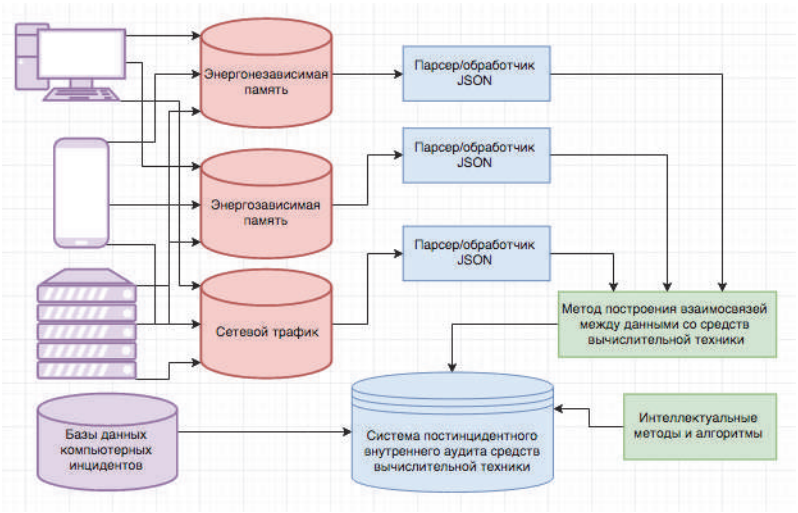

Рис. 1. Функциональная схема проведения постинцидентного внутреннего аудита средств вычислительной техники

Входными параметрами методики могут быть данные с энергозависимой памяти, энергонезависимой памяти, сетевого трафика. Это обусловлено тем, что сведения о современных компьютерных инцидентах могут быть во всех типах компьютерной памяти, как на одном, так и на нескольких средствах вычислительной техники. В связи с этим комплексный анализ типов компьютерной памяти является важной задачей. Для его осуществления необходимо получение максимального количества данных со средства вычислительной техники. Декомпозиция получения данных представлена на рис. 2, далее по тексту приводится ее описание.

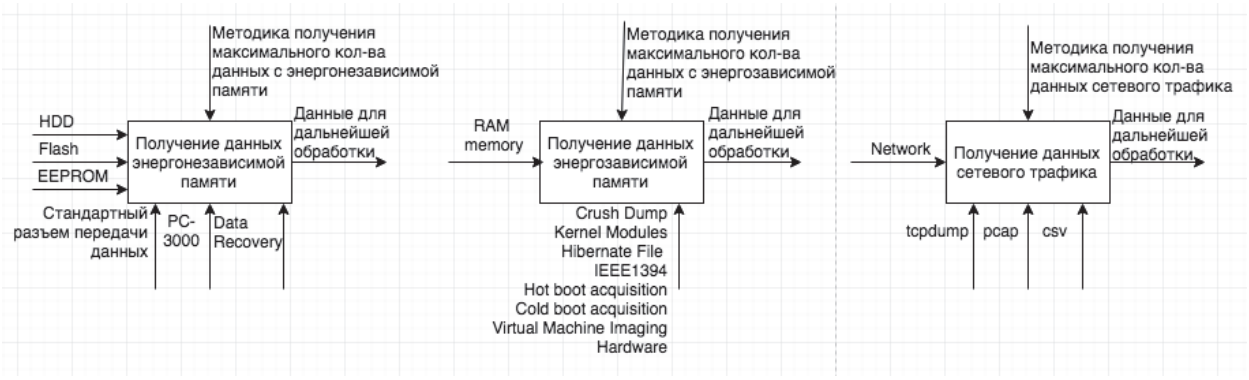

Рис. 2. Декомпозиция получения данных с постинцидентного средства вычислительной техники

Получение данных энергонезависимой памяти. Под энергонезависимой памятью понимается носитель, который после обесточивания электропитания сохраняет в себе набор хранящейся в ней информации. Примерами такой памяти могут служить классические жесткие диски (НЖМД), диски SSD, Flash-накопители, EEPROM. Ввиду их особенностей, физической структуры, программной реализации существуют подходы к получению максимального объема информации с носителя энергонезависимой памяти. Эти подходы описаны в методиках в работах [10–12]. Для считывания данных с энергонезависимой памяти существуют два основных подхода.

1. Аппаратный. Под аппаратным способом понимается получение доступа к данным, когда считывание с помощью стандартных программных средств невозможно. Обычно в таком случае применяют средства и методы аппаратного восстановления данных (PC-3000, DFL-DDP Data Recovery Equipment) [13].
2. Программный. Данный способ получения данных является стандартным и наиболее распространенным. Обычно носитель информации подключается к последовательному порту, и осуществляется считывание информации через различные программные средства [14, 15].

Получение данных энергозависимой памяти. Под энергозависимой памятью подразумевается носитель информации, который после обесточивания электропитания теряет данные, хранящиеся в ней. Средства вычислительной техники могут работать на различном аппаратном и программном обеспечении, следовательно, на каждом из них могут быть различные трудности в доступе к энергозависимой памяти. Ввиду таких особенностей получение данных из энергозависимой памяти может быть затруднено. Существуют следующие способы получения данных из энергозависимой памяти: Crush Dump, Kernel Modules, Hibernate File, IEEE1394, Hot boot acquisition, Cold boot acquisition, Virtual Machine Imaging, Hardware [16]. Для получения максимального количества данных энергозависимой памяти с помощью этих способов существуют методики, описанные в работах [17, 18].

Получение данных сетевого трафика. Сетевой трафик может быть получен с мест его агрегации, в форматах полного дампа или в формате заголовков пакетов. Обработка данных может состоять в представлении его в виде текстового файла формата csv, pcap, tcpdump, после чего можно будет обрабатывать его на предмет постинцидентного внутреннего аудита. Процесс получения и анализа сетевого трафика описан в работах [19, 20].

После получения дампов памяти с постинцидентного средства вычислительной техники их необходимо обработать для извлечения информации. Для достижения этих целей были разработаны скрипты на языке Python, которые выполняют функции извлечения атрибутов и их значения с дампов памяти в формат JSON. После обработки данных и формирования JSON осуществляется процесс описания взаимосвязей между атрибутами и их значениями. Взаимосвязи можно описывать как в рамках одного средства вычислительной техники, так и нескольких. Это может быть частным случаем, когда компьютерный инцидент произошел с участием нескольких средств вычислительной техники. Описание взаимосвязи происходит в системе проведения постинцидентного внутреннего аудита средств вычислительной техники с помощью метода [1]. Ниже представлено краткое его описание.

Сущность метода заключается в описании взаимосвязей между слабоструктурированными данными с использованием теории графов. Метод предназначен для описания свойств инцидента информационной безопасности при проведении внутреннего постинцидентного аудита средств вычислительной техники. В данном методе происходит описание взаимосвязей между атрибутами и их значениями в нереляционной системе управления базой данных (NoSQL СУБД). Примерами атрибутов могут быть: хэш файла (Hash), имя файла (Name), полный путь к файлу (Directory), тип файла (Type), права файла (Permission), дата создания файла (Date) – энергонезависимой памяти, название процесса (NamePid), pid процесса (Pid), смещение в адресе (Offset) – в энергозависимой памяти, тип протокола (Protocol), адрес назначения (Destination) в сетевом трафике.

Важным элементом методики является база данных существующих компьютерных инцидентов. Она необходима для более точного определения компьютерных инцидентов в данных, полученных с постинцидентного средства вычислительной техники. База данных существующих компьютерных инцидентов формировалась путем получения информации с сайта http://malwr.com[1]. Размер выборки в базе данных составил примерно 200 тысяч экземпляров.

Для проведения постинцидентного внутреннего аудита средств вычислительной техники рост объемов хранимых и обрабатываемых данных является проблемой. Одним из возможных решений является классификация данных, которые относятся непосредственно к операционной системе и к деятельности пользователя. Это позволит достичь снижения объемов обрабатываемой информации, исследуя только те данные, которые относятся к деятельности пользователя и к компьютерным инцидентам. Один из методов решения задачи классификации данных с постинцидентного средства вычислительной техники на пользовательские и системные описан в работе [21]. Ниже представлено краткое его описание.

Под пользовательскими данными подразумевается информация, с которой работал (сохранял и изменял) пользователь в операционной системе на средстве вычислительной техники. К системным относятся данные операционной системы и прикладного программного обеспечения. Использование описанного в настоящей работе метода позволяет определить информативность признаков и на их основе рассчитать точность классификации данных на пользовательские и системные. В работе был проведен эксперимент, в ходе которого была рассчитана информативность и выделены наиболее значимые атрибуты. Результатом решения задачи классификации с применением данного метода является снижение объемов обрабатываемых данных с постинцидентного средства вычислительной техники, что в тенденции к росту общего числа данных или увеличения количества средств вычислительной техники может повысить точность обнаружения сведений о компьютерном инциденте.

Помимо решения задачи классификации, можно применять и иные методы, такие как идентификация исполняемых файлов [22, 23], лингвистический анализ текста [24–26], анализ аудио- и видеоданных [27]. В совокупности они позволят достичь повышения информативности цифровых улик (сведений о компьютерном инциденте) при проведении постинцидентного внутреннего аудита средств вычислительной техники.

Оценка вычислительной сложности проведения постинцидентного внутреннего аудита средств вычислительной техники

Рост объемов хранимой и обрабатываемой информации в последнее время способствует увеличению времени поиска сведений о компьютерных инцидентах в случае их наступления. Стоит учитывать и тот факт, что количество типов и классов компьютерных инцидентов тоже растет. Путем исключения содержимого данных, анализируя только атрибуты и их значения с применением описания взаимосвязей между ними, а также за счет применения интеллектуальных методов и алгоритмов появляется возможность исследования компьютерных инцидентов в условиях роста объемов хранимой и обрабатываемой информации, числа типов и классов компьютерных инцидентов.

Предлагаемая методика позволяет проводить исследования компьютерных инцидентов с постинцидентного средства вычислительной техники на основе анализа атрибутов и их значений. Был проведен эксперимент, заключающийся в оценке вычислительной сложности на основе применения предлагаемой методики. Эксперимент состоял в анализе дампов памяти (энергонезависимой памяти, энергозависимой памяти и сетевого трафика), полученных со средств вычислительной техники, на которых произошел компьютерный инцидент. Процесс обработки дампов памяти позволил получить атрибуты и их значения в формате JSON. Ниже представлены табл. 4–6, в которых отражены: размер исходного дампа памяти; количество объектов (файлов, процессов, пакетов, и др.) в нем; общий размер атрибутов и их значений (какое количество информации в килобайтах занимают атрибуты и их значения на основе предлагаемой методики); средний размер сущности (объем информации, описывающий объект с дампа памяти); затраченное время на обработку дампов памяти.

Общий размер объектов, ГБ	Количество объектов	Размер атрибутов и их значений, КБ	Средний размер сущности, КБ	Время на обработку, мин
100,55	68053	31600	0,47	160
46,35	1196	604	0,5	80
8,21	129	60	0,47	12,6
2,93	2095	912	0,44	5,1
3,04	992	497	0,5	5,7

Таблица 4. Таблица результатов обработки дампов памяти с энергонезависимой памяти

[1]malwr.com – сервис бесплатного анализа вредоносного программного обеспечения

Общий размер объектов, ГБ	Количество объектов	Размер атрибутов и их значений, МБ	Средний размер сущности, КБ	Время на обработку, мин
8,3	318	9,7	31,24	13,2
6,1	196	5,61	29,31	11,4
2	81	2,23	28,19	3,1
3,8	126	3,71	30,15	6,7
1,42	67	1,91	29,19	2,1

Таблица 5. Таблица результатов обработки дампов памяти с энергозависимой памяти

Общий размер объектов, МБ	Количество объектов	Размер атрибутов и их значений, МБ	Средний размер сущности, КБ	Время на обработку, мин
943	904072	98,06	0,11	13,4
952	1126150	122,08	0,11	13,5
963	1141694	124,04	0,11	14,1
896	860222	92,88	0,11	11,4
1,300	1497884	162,87	0,11	18,7

Таблица 6. Таблица результатов обработки дампов сетевого трафика

Из таблиц видно, что средний размер сущности в энергонезависимой памяти не превышает 0,5 кБ, в энергозависимой – 31,24 КБ, в сетевом трафике – 0,11 КБ. На основе этих данных можно спрогнозировать временные затраты при проведении постинцидентного внутреннего аудита в больших объемах данных. По данным из табл. 4–6 были построены графики зависимости времени обработки от общего размера объектов (дампов памяти).

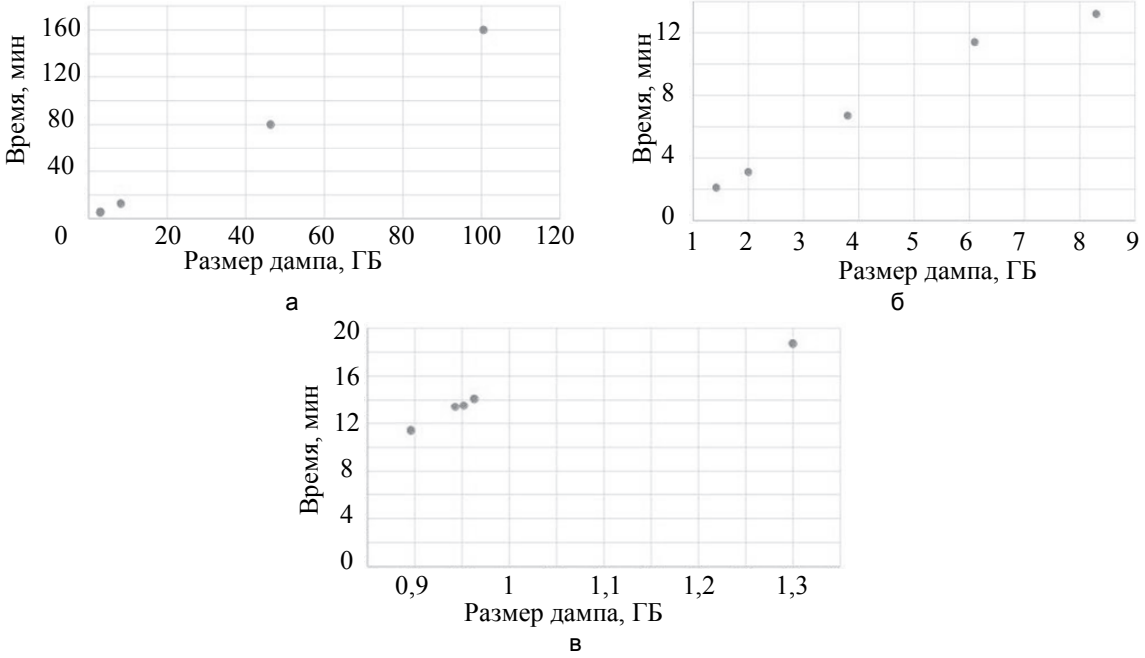

Рис. 3. Зависимости времени обработки от размера дампов памяти: энергонезависимой памяти (а); энергозависимой памяти (б); сетевого трафика (в)

Как видно на рис. 3, имеется практически линейная зависимость времени обработки от размеров дампов памяти. Это связано с тем, что в алгоритмах получения атрибутов и их значений при формировании файлов в формате JSON применяются итеративные процессы, которые проводятся отдельно для каждого объекта данных (файла, процесса, сетевого пакета и др.), вне зависимости от его размера. Теоретически линейность может быть нарушена в случае, когда обрабатывается небольшое количество данных большого объема. С практической точки зрения с ростом сущностей растет и общий объем данных, а следовательно, итеративные алгоритмы, применяемые в методике, имеют линейную зависимость времени обработки от общего размера обрабатываемых сущностей. Это позволяет экстраполировать полученные временные значения и тем самым оценить временные затраты применения методики. При помощи метода наименьших квадратов с использованием полученных значений временных затрат в зависимости от размера исследуемых данных можно найти аппроксимирующую функцию, которая будет давать воз-

можность оценить временные затраты на вычисления. Примерные соотношения для расчета временных затрат (линейная аппроксимация) при заданных размерах дампов памяти имеют следующий вид:

$$T(hdd) = 1{,}139 + 1{,}599 \cdot V$$
$$T(ram) = -0{,}01 + 1{,}69 \cdot V$$
$$T(net) = -2{,}03 + 16{,}08 \cdot V,$$

где $T(hdd)$ – время обработки энергонезависимой памяти; $T(ram)$ – время обработки энергозависимой памяти; $T(net)$ – время обработки сетевого трафика; V – размер дампа памяти в гигабайтах.

Представленные соотношения позволяют оценить время работы методики в задачах исследования компьютерных инцидентов. Временные затраты на обработку дампов памяти зависят непосредственно от объема самих данных, физической структуры носителя информации и алгоритма доступа к атрибутам и их значениям.

Полученные сведения в формате JSON в результате применения предлагаемой методики позволяют описывать сведения о компьютерном инциденте, добиться снижения объемов обрабатываемой информации, что, в свою очередь, снизит временные затраты на сам процесс постинцидентного внутреннего аудита средств вычислительной техники. По сравнению с существующими методиками, эффективность предлагаемого решения определяется возможностью исследования компьютерных инцидентов одновременно с нескольких средств вычислительной техники за счет анализа атрибутов и их значений, предоставляет возможность исследования компьютерных инцидентов в условиях роста объемов хранимой и обрабатываемой информации. За счет применения интеллектуальных методов и алгоритмов методика способствует повышению получаемых сведений о компьютерных инцидентах, которые произошли на различных средствах вычислительной техники.

Заключение

Предлагаемая методика позволяет исследовать компьютерные инциденты с постинцидентного средства вычислительной техники. За счет комплексного анализа атрибутов и их значений с энергозависимой памяти, энергонезависимой памяти, сетевого трафика возможно улучшение сведений о компьютерном инциденте. Путем исключения содержимого данных, анализируя только атрибуты и их значения, можно снизить вычислительную сложность, таким образом, появляется возможность исследования компьютерных инцидентов в условиях постоянного роста объема хранимых и обрабатываемых данных, числа типов и классов компьютерных инцидентов. Предлагаемая в работе методика является универсальной и может применяться для исследования компьютерных инцидентов в различных средствах вычислительной техники, таких как персональные компьютеры, сервера, мобильные устройства и планшеты, даже на нескольких скомпрометированных устройствах одновременно. Методика имеет практическую применимость для исследования компьютерных инцидентов, повышения точности и информативности сведений о компьютерных инцидентах при проведении постинцидентного внутреннего аудита средств вычислительной техники, может применяться при разработке проактивных систем защиты от компьютерных инцидентов путем интеграции.

Литература

1. Пантюхин И.С., Зикратов И.А., Левина А.Б. Метод проведения постинцидентного внутреннего аудита средств вычислительной техники на основе графов // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 3. С. 506–512. doi: 10.17586/2226-1494-2016-16-3-506-512
2. Nelson B., Phillips A., Steuart C. Guide to Computer Forensics and Investigations: Processing Digital Evidence. 5th ed. Cengage Learning, 2016. 752 p.
3. Altheide C., Carvey H. Digital Forensics with Open Source Tools. Elsevier, 2011. 288 p.
4. Polstra P. Linux Forensics. Pentester Academy, 2015. 370 p.
5. Physical Memory Attacks [Электронный ресурс]. Режим доступа: https://privatecore.com/resources-overview/physical-memory-attacks/, свободный (дата обращения 08.02.2017).
6. Bishop M. An overview of computer viruses in a research environment. Technical Report PCS-TR91-156. Dartmouth College, Hanover, 1990.
7. Choi H., Lee H., Kim H. Fast detection and visualization of network attacks on parallel coordinates // Computers and Security. 2009. V. 28. N 5. P. 276–288. doi: 10.1016/j.cose.2008.12.003
8. Hickok G. Digital Forensics Global Trends [Электронный ресурс]. 2014. Режим доступа: http://www.security-daily.com/dsp_getFeaturesDetails.cfm?CID=3875, свободный (дата обращения 08.02.2017).
9. Таненбаум Э., Остин Т. Архитектура компьютера. 6-е изд.

References

1. Pantiukhin I.S., Zikratov I.A., Levina A.B. Graph-based post incident internal audit method of computer equipment. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2016, vol. 16, no. 3, pp. 506–512. (In Russian) doi: 10.17586/2226-1494-2016-16-3-506-512
2. Nelson B., Phillips A., Steuart C. *Guide to Computer Forensics and Investigations: Processing Digital Evidence*. 5th ed. Cengage Learning, 2016, 752 p.
3. Altheide C., Carvey H. *Digital Forensics with Open Source Tools*. Elsevier, 2011, 288 p.
4. Polstra P. *Linux Forensics*. Pentester Academy, 2015, 370 p.
5. *Physical Memory Attacks*. Available at: https://privatecore.com/resources-overview/physical-memory-attacks/ (accessed 08.02.2017).
6. Bishop M. An overview of computer viruses in a research environment. *Technical Report PCS-TR91-156*. Dartmouth College, Hanover, 1990.
7. Choi H., Lee H., Kim H. Fast detection and visualization of network attacks on parallel coordinates // *Computers and Security*, 2009, vol. 28, no. 5, pp. 276–288. doi: 10.1016/j.cose.2008.12.003
8. Hickok G. *Digital Forensics Global Trends*. 2014. Available at: http://www.security-daily.com/dsp_getFeaturesDetails.cfm?CID=3875 (accessed 08.02.2017).
9. Tanenbaum A.S., Austin T. *Structured Computer Organization*.

СПб.: Питер, 2013. 816 с.
10. Volonino L., Anzaldua R. Computer Forensics for Dummies. John Wiley & Sons, 2008. 388 p.
11. Solomon M.G., Rudolph K., Tittel E. et al. Computer Forensics JumpStart. John Wiley & Sons, 2011. 336 p.
12. Nelson B., Phillips A., Steuart C. Guide to Computer Forensics and Investigations. Cengage Learning, 2014. 720 p.
13. Касперски К. Восстановление данных. Практическое руководство. СПб.: БХВ-Петербург, 2006. 352 с.
14. Сенкевич Г.Е. Искусство восстановления данных. СПб.: БХВ-Петербург, 2011. 304 с.
15. Ташков П.А. Восстановление данных на 100%. СПб.: Питер, 2008. 206 с.
16. Burdach M. Physical Memory Forensics. Black Hat, USA, 2006. 53 p.
17. Ligh M.H., Case A., Levy J., Walters A. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Wiley, 2014. 912 p.
18. Case A., Richard G.G. Memory forensics: the path forward // Digital Investigation. 2017. V. 20. P. 22–33. doi: 10.1016/j.diin.2016.12.004
19. Davidoff S., Ham J. Network Forensics: Tracking Hackers through Cyberspace. Prentice Hall, 2012. 576 p.
20. Meghanathan N., Allam S.R., Moore L.A. Tools and techniques for network forensics // arXiv preprint arXiv:1004.0570. 2010.
21. Zikratov I., Pantiukhin I., Sizykh A. The method of classification of user and system data based on the attributes // Proc. 18th Conference of Open Innovations Association. St. Petersburg, Russia, 2016. P. 404–409. doi: 10.1109/FRUCT-ISPIT.2016.7561557
22. Zikratov I.A., Pantiukhin I.S., Krivtsova I.E., Druzhinin N.K. The method of elf-files identification based on the metric classification // Proc. 18th Conference of Open Innovations Association. St. Petersburg, Russia, 2016. P. 397–403. doi: 10.1109/FRUCT-ISPIT.2016.7561556
23. Кривцова И.Е., Салахутдинова К.И., Юрин И.В. Метод идентификации исполняемых файлов по их сигнатурам // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2016. № 1(35). С. 215–224.
24. Воробьева А.А. Отбор информативных признаков для идентификации Интернет-пользователей по коротким электронным сообщениям // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 1. С. 117–128. doi: 10.17586/2226-1494-2017-17-1-117-128
25. Vorobeva A.A. Examining the performance of classification algorithms for imbalanced data sets in web author identification // Proc. 18th Conference of Open Innovations Association. St. Petersburg, Russia, 2016. P. 385–390. doi: 10.1109/fruct-ispit.2016.7561554
26. Воробьева А.А. Компьютерная криминалистика: идентификация автора Интернет-текстов // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 2. С. 295–302. doi: 10.17586/2226-1494-2016-16-2-295-302
27. Юрин И.В., Пантюхин И.С. Проверка гипотезы создания цифрового полиграфа на основе видео и аудио данных // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2015. № 3 (31).С. 202–209.

6th ed. Pearson, 2012, 800 p.
10. Volonino L., Anzaldua R. *Computer Forensics for Dummies*. John Wiley & Sons, 2008, 388 p.
11. Solomon M.G., Rudolph K., Tittel E. et al. *Computer Forensics JumpStart*. John Wiley & Sons, 2011, 336 p.
12. Nelson B., Phillips A., Steuart C. *Guide to Computer Forensics and Investigations*. Cengage Learning, 2014, 720 p.
13. Kaspersky K. *Data Recovery. Manual*. St. Petersburg, BKhV-Peterburg Publ., 2006, 352 p. (In Russian)
14. Senkevich G.E. *Art of Data Recovery*. St. Petersburg, BKhV-Peterburg Publ., 2011, 304 p. (In Russian)
15. Tashkov P.A. *100% Data Recovery*. St. Petersburg, Piter Publ., 2008, 206 p. (In Russian)
16. Burdach M. *Physical Memory Forensics*. Black Hat, USA, 2006, 53 p.
17. Ligh M.H., Case A., Levy J., Walters A. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Wiley, 2014, 912 p.
18. Case A., Richard G.G. Memory forensics: the path forward. *Digital Investigation*, 2017, vol. 20, pp. 22–33. doi: 10.1016/j.diin.2016.12.004
19. Davidoff S., Ham J. *Network Forensics: Tracking Hackers through Cyberspace*. Prentice Hall, 2012, 576 p.
20. Meghanathan N., Allam S.R., Moore L.A. Tools and techniques for network forensics. arXiv preprint arXiv:1004.0570, 2010.
21. Zikratov I., Pantiukhin I., Sizykh A. The method of classification of user and system data based on the attributes. *Proc. 18th Conference of Open Innovations Association*. St. Petersburg, Russia, 2016, pp. 404–409. doi: 10.1109/FRUCT-ISPIT.2016.7561557
22. Zikratov I.A., Pantiukhin I.S., Krivtsova I.E., Druzhinin N.K. The method of elf-files identification based on the metric classification. *Proc. 18th Conference of Open Innovations Association*. St. Petersburg, Russia, 2016, pp. 397–403. doi: 10.1109/FRUCT-ISPIT.2016.7561556
23. Krivtsova I.E., Salakhutdinova K.I., Yurin I.V. Method of executable filts identification by their signatures. *Vestnik Gosudarstvennogo Universiteta Morskogo i Rechnogo Flota imeni Admirala S.O. Makarova*, 2016, no. 1, pp. 215–224. (In Russian)
24. Vorobeva A.A. Dynamic feature selection for web user identification on linguistic and stylistic features of online texts. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 1, pp. 117–128. (In Russian). doi: 10.17586/2226-1494-2017-17-1-117-128
25. Vorobeva A.A. Examining the performance of classification algorithms for imbalanced data sets in web author identification. *Proc. 18th Conference of Open Innovations Association*. St. Petersburg, Russia, 2016, pp. 385–390. doi: 10.1109/fruct-ispit.2016.7561554
26. Vorobeva A.A. Forensic linguistics: automatic web author identification. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2016, vol. 16, no. 2, pp. 295–302. (In Russian). doi:10.17586/2226-1494-2016-16-2-295-302
27. Yurin I.V., Pantyukhin I.S. Testing the hypothesis of creating a digital polygraph based on video and audio data. *Vestnik Gosudarstvennogo Universiteta Morskogo i Rechnogo Flota imeni Admirala S.O. Makarova*, 2015, no. 3, pp. 202–209. (In Russian)

Авторы

Пантюхин Игорь Сергеевич – тьютор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, zevall@cit.ifmo.ru

Зикратов Игорь Алексеевич – доктор технических наук, профессор, заведующий кафедрой, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, zikratov@cit.ifmo.ru

Authors

Igor S. Pantiukhin – tutor, ITMO University, Saint Petersburg, 197101, Russian Federation, zevall@cit.ifmo.ru

Igor A. Zikratov – D.Sc., Professor, Head of Chair, ITMO University, Saint Petersburg, 197101, Russian Federation, zikratov@cit.ifmo.ru