УДК 004

Методы создания копии состояния оперативной памяти

Д. В. Угаров
ЗАО «ОКБ САПР», Москва, Россия

Рассмотрена задача проверки механизмов очистки освобождаемых областей памяти. Предложено решение с использованием технологии виртуализации, позволяющее упростить данную процедуру.

Ключевые слова: тестирование средств защиты информации (СЗИ), очистка освобождаемых областей памяти, копия состояния оперативной памяти, виртуализация, виртуальная машина.

Оперативная память является одним из основных источников информации, достаточной для компрометации системы. Примером такой информации могут служить криптографические ключи, пароли, а также части некорректно завершенных исполняемых процессов. По этой причине СЗИ, осуществляющие очистку освобождаемых областей памяти, становятся все более востребованными.

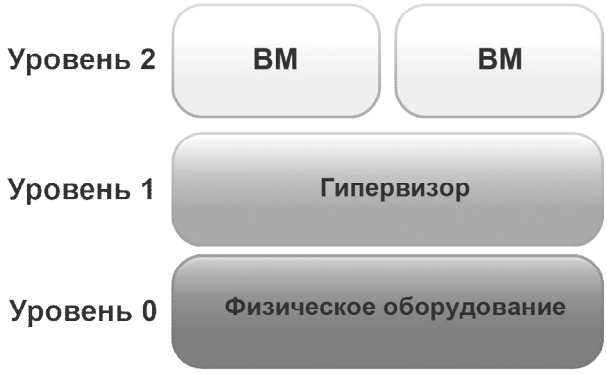
Реализация данного функционала является технически сложной задачей. Необходимо быть уверенным в том, что учтены все области, связанные с процессом, и не упущены специфические (в том числе недокументированные) механизмы исполняющей среды. Например, системный вызов, изменяющий размер области отображения (при этом перемещающий ее при необходимости), или кэширование данных операционной системой. Именно поэтому недостаточно проверять выборочные области оперативной памяти, необходимо анализировать полную копию оперативной памяти используемой среды.

Рассмотрим используемые в настоящее время способы получения копии оперативной памяти:

- программные средства (например, дополнительный модуль ядра в испытуемой среде или live cd дистрибутив с утилитами создания копии памяти);
- физическое изъятие оперативной памяти (требует замораживания);
- непосредственный доступ к памяти. PCI или FireWire устройства, использующие технологию DMA (Direct Memory Access).

Процесс, работающий внутри системы, изменяет и состояние оперативной памяти в ней. По этой причине, несмотря на существующие пути получения прямого доступа к оперативной памяти из исполняемой среды, вариант использования программных средств не является приемлемым. Для получения корректных результатов необходимо внешнее воздействие на систему. Остальные два подхода, хотя и позволяют достичь требуемых результатов, все же требуют значительных затрат на приобретение/разработку дорогостоящих устройств. А это отталкивает львиную долю исследователей в данной области.

В результате, в настоящее время не было предложено простых методик, позволяющих получить полную копию оперативной памяти для анализа, что в свою очередь сильно тормозит прогресс в данной области. По этой причине необходим новый подход, упрощающий данную процедуру. Основой для такого подхода может выступить технология виртуализации. Внешнее воздействие по отношению к виртуальной машине (ВМ) может обеспечить гипервизор (рисунок), так как он осуществляет управление ее ресурсами.



Иерархия в виртуальной инфраструктуре

При таком подходе необходимо понимать, что оперативную память для ВМ выделяет гипервизор. Поэтому возможны ситуации, в которых ВМ уже в момент старта содержит в памяти мусор, что приведет к некорректным результатам. Чтобы избе-

Угаров Дмитрий Владимирович, руководитель группы разработки СЗИ для систем виртуализации.
E-mail: dugarov@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

жать этого, требуется проверка выбранного гипервизора на предмет предварительной очистки предоставляемой для ВМ области оперативной памяти. Такая проверка возможна благодаря функции nested virtualization, позволяющей создать конфигурацию, в которой гипервизор, работающий на физическом оборудовании, имеет в качестве ВМ такой же гипервизор. Если же требуемые очистки не выполняются, после каждого опыта необходимо будет перезагружать физическое оборудование.

Одним из гипервизоров, удовлетворяющих указанному критерию, является ESXi. При старте ВМ он предоставляет ей обезличенную область памяти, а также перед выделением каждой дополнительной страницы памяти производит ее обнуление [1]. Для получения полной копии оперативной памяти с использованием данного гипервизора достаточно приостановить выполнение ВМ (перевести в состояние suspend). В таком случае ESXi сохранит состояние памяти в виде файла с расширением «vmss». Для поиска паттернов, оставленных утилитами анализа, достаточно воспользоваться встроенной утилитой гипервизора, вызвав команду:

cat /<путь к папке вм>/<имя_вм>.vmss | grep <паттерн для поиска>.

Учитывая простоту решения, а также факт существования ESXi в бесплатной редакции, можно заключить, что данный подход найдет широкое применение среди разработчиков СЗИ. Также необходимо отметить, что указанный механизм может быть расширен для анализа других элементов, например, для анализа внешней памяти.

Литература

1. *Foley M.* Security of VMware vSphere Hypervisor.— VMware, 2014.

Methods of creating memory snapshots

D. V. Ugarov
OKB SAPR JSC, Moscow, Russia

The article is devoted to the problem of examination of memory sanitizing process. The approach based on virtualization technology which simplifying this procedure.

Keywords: DST testing, memory sanitizing, memory snapshots, virtualization, virtual machine

Bibliography — 1 reference. *Received June 14, 2014*