ISSN 2306-1561
Automation and Control in Technical Systems (ACTS)
2015, No 1, pp. 92-100.
DOI: 10.12731/2306-1561-2015-1-11

Evaluation and Ranking Functionality of Information Security Tools of Virtualization Software

Roman Michailovich Yudichev

Russian Federation, Leading Specialist.

Research Associate of NPO «Echelon», 107023, Russian Federation, Moscow, Electrozavodskaya Str., 24, Tel.: +7 (495) 223-23-92, http://www.npo-echelon.ru

mail@cnpo.ru

Maksim Nikolaevich Gorjunov

Russian Federation, Specialist.

The Academy of Federal Security Guard Service of the Russian Federation, 302034, Russian Federation, Orel, Priborostroitelnaya Str., 35, Tel.: +7 (4862) 54-97-63, http://academ.msk.rsnet.ru

max.gor@mail.ru

Abstract. The advantages of the international metastandard ISO 15408 in terms of developing relevant requirements for information security are shown. The typification of virtualization environments is proposed. The examples of virtualization environments are given. The main classes of threats to information security virtualization environments are substantiated. The new basic and special security features of virtualization environments are developed. The possibility of implementing safety requirements of the virtualization environment in notations of meta standard ISO 15408 is shown. The requirements for reliable isolation virtualization environments are formulated. The possibility of using a formal model of isolation virtualization platforms is shown. The feasibility of certification remedies virtualization environment for new requirements generated according to the methodology of ISO 15408 is concluded.

Keywords: technical protection of information, information security tools, virtualization environment, the threat of a virtualization environment, isolation virtualization environments.

ISSN 2306-1561
Автоматизация и управление в технических системах (АУТС)
2015. – № 1. – С. 92-100.
DOI: 10.12731/2306-1561-2015-1-11

УДК 004.056

Оценка и ранжирование функциональных возможностей средств защиты среды виртуализации

Юдичев Роман Михайлович

Российская Федерация, ведущий специалист.

ЗАО НПО "Эшелон", 107023, Российская Федерация, г. Москва, ул. Электрозаводская, д. 24, Тел.: +7 (495) 223-23-92, http://www.npo-echelon.ru

mail@cnpo.ru

Горюнов Максим Николаевич

Российская Федерация, сотрудник.

ГКОУ ВПО "Академия Федеральной службы охраны Российской Федерации", 302034, Российская Федерация, г. Орёл, ул. Приборостроительная, д. 35, Тел.: +7 (4862) 54-97-63, http://academ.msk.rsnet.ru

max.gor@mail.ru

Аннотация. Рассмотрены вопросы разработки нормативно-методической базы защиты среды виртуализации по требованиям безопасности информации. Показаны преимущества международного метастандарта ISO 15408 в плане разработки актуальных требований по безопасности информации. Предложена типизация сред виртуализации на основе гипервизоров 1-го и 2-го типов. Приведены примеры сред виртуализации. Обоснованы основные классы угроз информационной безопасности сред виртуализации. Разработаны новые базовые и специальные функции безопасности сред виртуализации. Показана возможность реализации требований по безопасности среды виртуализации в нотациях метастандарта ISO 15408. Сформулированы требования по надежности изоляции сред виртуализации. Показана возможность применения формальной модели изоляции платформ виртуализации. Сделан вывод о целесообразности сертификации средств защиты среды виртуализации по новым требованиям, формируемым согласно методологии ISO 15408.

Ключевые слова: техническая защита информации, средства защиты информации, среда виртуализации, угрозы среде виртуализации, изоляция сред виртуализации.

1. Введение

Системы виртуализации в последнее время получили широкое распространение практически во всех сферах и отраслях производства и обслуживания, что обусловлено такими достоинствами данных технологий, как более полная загрузка оборудования, упрощение процедур масштабирования и миграции информационных систем разной сложности. Вместе с тем, применение данных технологий связано с необходимостью глубокой проработки вопросов обеспечения безопасности информации в таких системах в контексте учета особенностей указанных технологий. По сути, среды виртуализации и построенные с их помощью виртуальные инфраструктуры, требуют концептуально нового подхода к обеспечению их информационной безопасности [1, 2]. Традиционная нормативная база, предполагающая сертификацию средств защиты информации в основном в качестве средств вычислительной техники, морально устарела и требует смены вектора развития в сторону учета особенностей продуктов информационных технологий и использования при формировании требований безопасности нормативно-методической базы «Общих критериев» [3, 4]. Такой курс, в частности, прослеживается в последних нормативных документах ФСТЭК России, касающихся систем обнаружения вторжений, средств антивирусной защиты и др. [5 – 7, 14, 15]. По аналогии с данными документами требования безопасности к средам виртуализации должны учитывать их типизацию и опираться на профили защиты 6 классов защищенности.

2. Типизация сред виртуализации

Общепринятой является следующая типизация сред виртуализации:

- среды виртуализации на основе гипервизора I типа – гипервизора, устанавливаемого непосредственно на аппаратное обеспечение в качестве системного программного обеспечения;
- среды виртуализации на основе гипервизора II типа – гипервизора, устанавливаемого в среде хостовой операционной системы в качестве прикладного программного обеспечения.

Однако в рамках формирования требований к средам виртуализации необходимо также рассмотреть вопрос о наложенных средствах защиты, которые целесообразно выделить в отдельный класс – наложенных средств защиты сред виртуализации. Примером такого средства является VGate – средство защиты информации для платформ VMware vSphere и Microsoft Hyper-V.

Методология «Общих критериев» предусматривает задание требований безопасности на основе целей безопасности. Цели безопасности формируются по результатам анализа среды безопасности объекта оценки. Данная среда описывается в терминах предположений, политик и угроз безопасности. Эти компоненты тесно взаимосвязаны, а их наполнение варьируется путем перевода элементов одной категории в другую. Например, часть угроз может быть учтена и определена в политиках (с помощью функциональных возможностей, которые уже противостоят

данной угрозе) или предположениях (в виде ограничений на применимость данной угрозы) [4, с.49].

3. Угрозы среде виртуализации

Проведенный анализ возможных угроз безопасности для сред виртуализации позволил систематизировать их в виде соответствующей классификационной схемы, представленной на рисунке 1. Однако данный перечень является широким и требует корректировки с точки зрения выделения ограниченного списка угроз, которые могут быть включены в соответствующий профиль защиты.

Рисунок 1 – Основные угрозы среде виртуализации

К таким угрозам могут быть отнесены следующие:

- Угроза-1 – истощение вычислительных ресурсов сервера виртуализации;
- Угроза-2 – несанкционированный доступ к функциям управления средой виртуализации, к обрабатываемой и хранимой информации среды виртуализации;
- Угроза-3 – несанкционированное изменение конфигурационных параметров среды виртуализации и/или средств защиты информации среды виртуализации;
- Угроза-4 – несанкционированное взаимодействие процессов различных экземпляров виртуальных машин;
- Угроза-5 – нарушение механизмов маршрутизации в виртуальной сети.

4. Функции безопасности сред виртуализации

4.1. Основные функции безопасности

В таблице 1 представлены основные функции безопасности (ФБ) сред виртуализации, сформированные на основе возможностей существующих сред виртуализации. Данные функции позволяют противостоять выделенным угрозам безопасности и учитывают потенциал развития сред виртуализации.

Таблица 1 – Основные функции безопасности сред виртуализации

Обозначение	Наименование	Краткое содержание
ФБ 1	Разграничение доступа к данным и функциям среды виртуализации	Разграничение доступа к данным и функциям среды виртуализации на основе процедур идентификации и аутентификации.
ФБ 2	Управление параметрами и работой среды виртуализации	Управление параметрами среды виртуализации, которые влияют на выполнение ФБ среды виртуализации. Управление режимами выполнения ФБ среды виртуализации.
ФБ 3	Аудит безопасности среды виртуализации	Регистрация и учет выполнения ФБ среды виртуализации.
ФБ 4	Защита данных аудита	Ограничение доступа к функциям просмотра данных аудита и защита записей аудита.
ФБ 5	Защита хранимых данных пользователей и среды виртуализации	Контроль целостности программных модулей и данных среды виртуализации, очистка ресурсов, освобождаемых виртуальными машинами, доверенная загрузка виртуальных машин
ФБ 6	Доступность среды виртуализации	Ограничение использования ресурсов сервера виртуализации. Анализ событий безопасности среды виртуализации и уведомление о возможных сбоях
ФБ 7	Изоляция виртуальных машин	Защита выполнения виртуальных машин от вмешательства и искажения со стороны других виртуальных машин
ФБ 8	Контроль виртуального коммутатора	Управление сетевыми потоками, проходящими через виртуальный коммутатор.
ФБ 9	Разграничение доступа к ресурсам среды виртуализации, имеющим разный уровень конфиденциальности	Разграничение доступа к ресурсам среды виртуализации на основе иерархических атрибутов безопасности.
ФБ 10	Безопасность передаваемых данных ФБ объекта (ФБО)	Обеспечение конфиденциальности и целостности данных ФБО, передаваемых между удаленными компонентами среды виртуализации или от среды виртуализации к другим доверенным продуктам ИТ
ФБ 11	Безопасность передаваемых данных пользователя	Обеспечение конфиденциальности и целостности данных пользователей и виртуальных машин в процессе их миграции между серверами виртуализации

4.2. Специальные функции безопасности

Анализ представленных функций безопасности показал, что в основном они все могут быть удовлетворены функциональными требованиями безопасности из метастандарта ГОСТ ИСО/МЭК 15408-2. Исключение составляют:

1. Функция безопасности – ФБ-7, касающаяся изоляции виртуальных машин, которая может быть удовлетворена следующим функциональным требованием безопасности, задаваемым в явном виде как разделение домена виртуальных машин (VDS_VMM_EXT):

- VDS_VMM_EXT.1 – разделение домена виртуальных машин;
- VDS_VMM_EXT.1.1 – ФБО должны поддерживать домен безопасности для выполнения каждой виртуальной машины, защищающий их от вмешательства и искажения недоверенными субъектами;
- VDS_VMM_EXT.1.2 – ФБО должны реализовать разделение между доменами безопасности виртуальных машин в области действия ФБО.

2. Функция безопасности – ФБ-6, в части автоматической реакции на события аудита, которая может быть удовлетворена следующим функциональным требованием безопасности, задаваемым в явном виде как автоматическая реакция на события безопасности (FAU_ARP_EXT):

- FAU_ARP_EXT.1 – автоматическая реакция на события безопасности;
- FAU_ARP_EXT.1.1 – ФБО должны уведомлять уполномоченных пользователей об обнаружении потенциального сбоя, связанных со средой виртуализации.

3. Функция безопасности – ФБ-5, в части доверенной загрузки виртуальных машин, которая может быть удовлетворена следующим функциональным требованием безопасности, задаваемым в явном виде как доверенная загрузка виртуальных машин (TRU_LVM_EXT):

- TRU_LVM_EXT.1 – доверенная загрузка виртуальных машин;
- TRU_LVM_EXT.1.1 – ФБО должны обеспечивать контроль целостности образов виртуальных машин (и файлов внутри этих образов) при получении команды на загрузку (включение) виртуальной машины;
- TRU_LVM_EXT.1.2 - при обнаружении ошибки целостности данных ФБО должны блокировать загрузку виртуальной машины (и другие предпринимаемые действия);
- TRU_LVM_EXT.1.3 – ФБО должны обеспечивать доверенную загрузку виртуальных машин до передачи управления загрузки виртуальному BIOS путем контроля неизменности параметров виртуального аппаратного обеспечения, контроля неизменности настроек виртуального BIOS и контроля целостности загрузочного сектора.

При этом необходимо констатировать, что базовой функцией безопасности для сред виртуализации, обусловленной технологией виртуализации, является изоляция

виртуальных машин, от реализации которой зависит безопасность всей виртуальной инфраструктуры.

В рамках данного вопроса необходимо отметить, что виртуализационное прозрачное разделение, принцип которого используется в средах виртуализации, не обеспечивает достаточно надёжного уровня изоляции между виртуальными машинами. Существующие исследования показали [8, 9], что совместное расположение виртуальных машин может привести к их несанкционированному взаимодействию посредством использования уязвимостей и скрытых каналов, пропускающих информацию о загрузке CPU, запросах на доступ к кэшу и прерываниях. Таким образом, свойства прозрачного разделения, реализуемого средами виртуализации, явно недостаточно для гарантии изоляции виртуальных машин.

Возможным способом подтверждения надежности реализации изоляции является доказательство ее соответствия формальной модели изоляции, в качестве которой может быть использована модель, представленная в работе [10]. Указанная работа отражает основные аспекты безопасности реализации механизма изоляции платформ виртуализации, в частности в ней:

- формализована модель изоляции «физически разделённых аппаратных средств» для сред виртуализации, охватывающая как явные, так и скрытые информационные потоки по времени. Выведены пять требований, позволяющих достичь на реальных системах с совместным использованием аппаратных средств эквивалентного для данной модели уровня изоляции. Кроме того, формально доказана достаточность данных требований для обеспечения надёжной изоляции;
- разработана формальная модель скрытых каналов по времени, ориентированная на первопричину проблемы, а именно на политики планирования аппаратных и программных ресурсов арбитрами. Проанализированы, как детерминированные политики планирования, для которых выведено доказательство изоляции, так и вероятностные политики планирования, для которых определено и измерено количество уровней утечки информации для определённого арбитра без памяти;
- проанализирована первопричина явных информационных потоков и показано, что контроль доступа и корректное выполнение операций сохранения и восстановления контекста являются достаточными для предотвращения явных информационных потоков в средах виртуализации. Полученные результаты справедливы для основных технологий виртуализации, включая технологии эмуляции программного обеспечения, такие как динамическая двоичная трансляция, паравиртуализация, поддержка виртуализации CPU и самовиртуализация периферийных устройств и IOMMU;
- проанализированы первопричины возникновения скрытых каналов по памяти и выявлены чёткие требования по их устранению.

В соответствии с [10] надежность изоляции достигается при удовлетворении следующих пяти требований:

- требование 1 (Loc Separation) – отсутствие явных информационных потоков;
- требование 2 (Implicit Parameter Separation) – независимость состояния виртуальных машин (ВМ) от состояния любых других ВМ;
- требование 3 (Error Signaling Separation) – независимость ошибок, проявляемых в одной ВМ, от состояния любых других ВМ;
- требование 4 (Conf Separation) – отсутствие скрытых информационных потоков по времени;
- требование 5 (Next Call Separation) – независимость выполнения ВМ от состояния любых других ВМ.

Требование 1 относится к явным информационным потокам; требования 2 и 3 охватывают скрытые каналы по памяти; требование 5 обеспечивает эквивалентность потоков управления выполнением ВМ в идеальной модели [11] и в реальной реализации [14]; требование 4 покрывает скрытые каналы по времени. При этом доказано, что скрытые каналы по времени, возникающие из-за задержек арбитра ресурсов могут быть устранены статичным временным разделением. При этом в формальном описании скрытых каналов по времени представлено доказательство изоляции для детерминированных арбитров ресурсов и показано, что только политики планирования с временным разделением (TDM) позволяют достичь надёжной изоляции. Однако, так как TDM-планировщики не пользуются особой популярностью из-за неэффективности, рассмотрено более общее определение изоляции, которое позволяет ограничить количество утечек, а также дискретизировать уровни утечек для подкласса вероятностных планировщиков без учёта предыстории.

Отметим, что также требует скорейшего решения практическая проблема максимально широкого внедрения средств доверенной загрузки виртуальных машин. Из присутствующих на рынке средств защиты информации (СЗИ) средств доверенной загрузки поддержка загрузки виртуальных машин декларирована только в МДЗ-Эшелон. Кроме того, функция контроля загрузочного сектора образов дисков виртуальных машин реализована в СЗИ vGate R2.

5. Заключение

Таким образом, вопрос сертификации сред виртуализации связан с решением вопроса разработки нормативно-правовых актов, регламентирующих требования безопасности к данным продуктам информационных технологий, а при проведении процесса оценки основной упор должен быть сделан на доказательство корректности и надежности реализации механизма изоляции виртуальных машин. Относительно небольшой размер кода, непосредственно реализующего функции гипервизора, внушает надежду на возможность применения для верификации рассмотренных требований формальных методов [12, 13].

Список информационных источников

[1] Зубарев И.В., Радин П.К. Основные угрозы безопасности информации в виртуальных средах и облачных платформах // Вопросы кибербезопасности. 2014. № 2 (3). С. 40-45.

[2] Зорин Е.Л., Чичварин Н.В. Информационная безопасность САПР/PLM, применяющих облачные технологии // Вопросы кибербезопасности. 2014. № 4 (7). С. 23-29.

[3] Барабанов А.В., Марков А.С., Рауткин Ю.В. Оценка соответствия средств защиты информации требованиям высших оценочных уровней доверия // Труды Научно-исследовательского института радио. 2012. № 3. С. 67-73.

[4] Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под ред. А.С. Маркова. М.: Радио и связь, 2012. 192 с.

[5] Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. С. 31-33.

[6] Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация средств антивирусной защиты по новым требованиям безопасности информации. // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2012. Спецвыпуск №5 "Информатика и системы управления". С.272-278.

[7] Барабанов А.В., Гришин М.И., Марков А.С., Цирлов В.Л. Формирование требований по безопасности информации к DLP-системам // Вопросы радиоэлектроники. 2013. №2. С. 67-76.

[8] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. // In Proc. ACM CCS, ACM, 2009, pp. 199–212.

[9] Yinqian Zhang, Ari Juels, Alina Oprea, and Michael K. Reiter. HomeAlone: Co-residency detection in the cloud via side-channel analysis. // In Proc. Oakland Security and Privacy, IEEE Computer Society, 2011, pp. 313–328.

[10] Montage: A Methodology for designing composable end-to-end secure distributed systems // Technical Report AFRL-RI-RS-TR-2012-196, IBMC, 2012, 191 p.

[11] Варламов О.О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия Южного федерального университета. Технические науки. 2006. № 7 (62). С. 216-223.

[12] Edmund M. Clarke, Orna Grumberg and Doron Peled. Model checking. In Carnegie Melon Univ., Pittsburg, PA, 1999, 330 pp.

[13] Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.

[14] Юрчик П.Ф., Пастухов Д.А. Сравнительный анализ гипервизоров // Автоматизация и управление в технических системах. – 2014. – № 4. – С. 129-140. DOI: 10.12731/2306-1561-2014-4-13.

[15] Ле К.Х., Суркова Н.Е., Остроух А.В. Генетические алгоритмы в задачах рациональной организации информационно-вычислительных процессов сетей // Автоматизация и управление в технических системах. – 2014. – №4 (12). – С. 82-99. DOI: 10.12731/2306-1561-2014-4-9.