Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Смирнова
Злата Дмитриевна

Обеспечение целостности данных при использовании технологии контейнеризации в информационных системах

АВТОРЕФЕРАТ

магистерской диссертации на соискание степени магистра технических наук

по специальности 98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
Богуш В.А.
д.ф-м.н., профессор

Минск 2019

ВВЕДЕНИЕ

Один из основных способов для возможности управления большим количеством хостов, является способ деления существующих физических машин на более мелкие части. Традиционная виртуализация принесла значительную выгоду в уменьшении расходов при управлении большим числом хостов. Но она имеет существенный минус. Разделение физического сервера несёт за собой определённые расходы. Одна из проблем при использовании виртуальных машин заключается в необходимости выделения ресурсов для ее функционирования. Чем больше виртуальных машин управляется гипервизором, тем больше ресурсов требуется. Другая проблема виртуализации кроется в конфликте среды. При развёртывании двух сервисов, которым нужны разные версии поддерживающей среды, может возникнуть конфликт версий и некорректность работы как самих сервисов, так и среды. И даже если бы оба сервиса требовали поддержку одной и той же среды, в случае внесения необходимых первому сервису изменений в среду, это затронет все сервисы, развернутые на этой машине.

Недостатки традиционных виртуальных машин стали катализатором роста популярности контейнеров. Данная технология предоставляет изолированное окружение в операционной системе. В данном подходе, ядро операционной системы предоставляет изолированное виртуальное пространство. Каждое из виртуальных пространств называется контейнером. Контейнеры позволяют процессам создавать изолированное окружение на операционной системе содержащей эти контейнеры.

Как и у любой другой технологии, у контейнеризации существует ряд недостатков. Поскольку в большинстве случаев загрузка образов контейнера производится по открытым каналам связи, а сам сервис общедоступен из внешней сети, то встаёт проблема обеспечения безопасной доставки образа Docker от разработчика до клиента, а также контроля целостности файлов самого приложения.

Имеющаяся в Docker технология контроля целостности обеспечивает защиту от подмены образа, получаемого извне, при создании контейнера, но никак не контролирует целостность приложений внутри работающего контейнера.

Целью данной работы является разработка методики обеспечения целостности данных при использовании технологии контейнеризации в информационных системах и программного комплекса для реализации данной методики.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке методики обеспечения целостности данных при использовании технологии контейнеризации в информационных системах и программного комплекса для реализации данной методики.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Сравнить технологии виртуализации и контейнеризации.
2. Подробно разобрать особенности реализации технологии контейнеризации
3. Разработать методику обеспечения целостности данных и автоматизировать её с помощью программного комплекса.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XXIII Белорусско-российской научно-практической конференции «Комплексная защита информации» (Суздаль, 2018).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 тезисы доклада в сборнике материалов конференции.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения и библиографического списка. Общий объем диссертации 52 страницы, 23 наименования в библиографическом списке.

Во введение приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней приводится общее описание технологий виртуализации и контейнеризации. Описана архитектура виртуальных машин, их преимущества и недостатки. Также описана архитектура виртуальных машин, их преимущества и недостатки. Приводится сравнение технологий виртуализации и контейнеризации.

Вторая глава посвящена технологии контейнеризации Docker. Подробно рассмотрена основа, на которой базируется Docker, его преимущества. Описана архитектура технологии Docker. Подробно рассмотрены все базовые составляющие контейнеров, загрузка образов из репозиториев Docker Hub.

В третьей главе описывается проблема контроля целостности образов при доставке образа Docker от разработчика до клиента. Выявлены проблемы в обеспечении безопасности при использовании среды контейнеризации Docker. Описывается разработка методики обеспечения целостности данных при использовании технологии контейнеризации в информационных системах. Создан программный комплекс для автоматизации данной методики.

Для реализации разработанной методики было использовано «Программное обеспечение контроля целостности AIDE», имеющее сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь. Выполнена предварительная настройка программного средства контроля целостности для использования в поставленных целях. Для автоматизации дальнейшего использования был создан скрипт на языке сценариев командной оболочки (Shell Script), управляющий средством контроля целостности. Наконец, был настроен плановый периодический запуск скрипта проверки целостности данных внутри контейнера для оповещения администратора об угрозе безопасности и возможном нарушении целостности данных в контейнере.

В заключении сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

Технология контейнеризации приложений используется для легковесного развертывания и запуска изолированных приложений на одной системе вместо запуска виртуальной машины для каждого приложения. В целом, контейнеризация – это метод виртуализации на уровне операционной системы. Несколько изолированных приложений или служб работают на одном хосте и имеют доступ к одному и тому же ядру ОС. Контейнеры могут работать как на «голом железе», так и в облачных инфраструктурах, на виртуальных и физических машинах.

В ходе анализа представленной технологии было выделено несколько проблем в обеспечении безопасности при использовании среды контейнеризации Docker:

1) Хоть контейнеризация и имеет значительные преимущества перед виртуализацией, в том числе из-за легковесности и возможности развёртывания большого числа сервисов на одном хосте, по этой же причине несёт в себе больший риск проникновения в систему ввиду меньшей изоляции сервисов друг от друга и от хостовой ОС;

2) Имеющаяся в Docker технология контроля целостности обеспечивает защиту от подмены образа, получаемого извне, при создании контейнера, но никак не контролирует целостность приложений внутри работающего контейнера;

3) Если говорить о практическом применении технологии контейнеризации не в общем, а конкретно для организаций и продуктов, находящихся на белорусском рынке, то по требованию законодательства для всех криптографических операций (в том числе выработки ЭЦП и вычисления хэш-сумм) должны быть использованы алгоритмы шифрования, соответствующие нормативно-правовым требованиям РБ.

В рамках работы была разработана методика обеспечения целостности данных при использовании технологии контейнеризации в информационных системах и создан программный комплекс для реализации данной методики.

Таким образом, решена проблема обеспечения защиты сервисов, развёртываемых в среде контейнеризации, от несанкционированного изменения или удаления, а также внесения модификаций в критически важные для функционирования данные. То есть решена проблема контроля целостности данных при использовании технологии контейнеризации.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1А. Смирнова З.Д. уязвимости Spectre и Meltdown / З.Д. Смирнова, Т.В. Борботько// Комплексная защита информации: Мат. XXIII науч.-практ. конф. / Москва: Медиа Группа «Авангард», 2018. С. 181-182. (22-24 мая 2018 г.).