На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції

Одеса
25–26 квітня 2016 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 25–26 квітня 2016 р. - Одеса, Видавництво ОНАХТ, 2016 р. - 176 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

БЕЗОПАСНОСТЬ ВИРТУАЛЬНЫХ КОНТЕЙНЕРОВ

Волков В.А.

Технология контейнерной виртуализации является новой разработкой решения актуальных проблем обеспечения безопасности. Данную технологию используют и развивают такие компании Google, IBM, Microsoft, VMware и другие. Поэтому разработки, касающиеся применения средств безопасности в этом сегменте, рассматриваются, сегодня, как важный составной элемент для выстраивания новой платформы [1].

Целью данной работы является анализ существующих направлений развития безопасности технологии контейнерной виртуализации.

Виртуальные контейнеры служат для размещения системных служб, сервисов или приложений в изолированном окружении. Они появились как альтернатива для популярных ныне виртуальных машин (ВМ), представляющих собой изолированные программные объекты с полным набором операционных средств и прикладным контентом [2]. Хотя контейнеры появились значительно позже, и их разработка велась с учётом прежних проблем, уровень защищённости ВМ значительно выше. Это можно объяснить следующими причинами: приложения, исполняемые на разных ВМ, имеют более высокую степень изоляции, чем при запуске внутри контейнеров; уровень изоляции контейнеров от хоста также оказался ниже, чем у гипервизора; системы управления контейнерами ещё не достаточно зрелые; ИТ-специалисты не имеют опыта работы с контейнерами.

Помимо экономии ресурсов сервера, контейнеры обладают плюсами и с точки зрения безопасности [3]:

- контейнеры обеспечивают более высокий уровень изоляции между приложениями, запускаемыми на одном хосте;
- внедрение контейнеров облегчает набор системных приложений, поэтому возможности для проведения атак сужаются;
- применение контейнеров облегчает задачу первичного развёртывания и повторной установки приложений.

Проведем анализ основных направлений в сегменте систем безопасности для технологии контейнерной виртуализации. Флагман в области виртуализации VMware предлагает обезопасить контейнеры путём запуска их внутри ВМ. Такой подход предполагает, что в целях безопасности каждое приложение, работающее в контейнере, должно помещаться внутрь собственной ВМ. В этом случае степень изоляции приложений будет максимальной, как от хоста, так и от других контейнеров, а, соответственно, и уровень защиты тоже. Однако размещение контейнеров внутри ВМ ведёт к тому, что многие преимущества этой технологии становятся нереализуемыми. Одно из таких преимуществ это очень быстрый старт, значительно опережающий по времени запуск через ВМ, или, например, запуск на одном хосте большого числа контейнеров, значительно превышающего то, что допустимо для ВМ.

Плюсом этого направления является то, что оно предусматривает возможность индивидуального управления каждым контейнером, а для устранения ограничений, VMware предлагает использовать Photon OS, совместно с лёгковесным «микровизором» Photon Machine, созданным на основе гипервизора ESXi.

Следующий подход предусматривает создание безопасной среды для работы контейнеров. Он связан с использованием операционной системы CoreOS, которая на рынке контейнерной виртуализации выступает главным конкурентом Docker. Этот подход предполагает использование системы Distributed Trusted Computing (DTC). Это механизм криптографической проверки целостности всего комплекса программных средств, которые формируют контейнерную среду. Недостатком системы DCT является то, что заказчику придётся приобрести все элементы контейнерной экосистемы CoreOS(в отличии от Docker).

Конкурентом предыдущему варианту выступает открытая контейнерная платформа Docker, которая занимается созданием средств защиты. Особенность этой технологии в том, что она позволяет отделить приложение от инфраструктуры и работать с ней, как с управляемым приложением. Наращивание безопасности для контейнеров на этой платформе ведётся в нескольких направлениях: это развитие проекта Notary и создание набора инструментов Docker Content Trust, которые позволяют применять авторизированные образы программ и создают специальный механизм защиты пользователей от атак типа man-in-the-midle при установке обновлений. Кроме этого, компания Docker имеет ещё несколько новых инициатив. Среди них можно выделить Project Nautilus, который призван выявлять уязвимости в приложениях, размещаемых в оболочке контейнера. Ещё одним новым направлением стало создание пользовательских пространств имён, что позволит повысить эффективность уже имеющихся средств. В будущем в Docker также планируется появление средств системных вызовов seccomp, что поможет управлять процессами в контейнере. Кроме того, компания Docker разрабатывает процедуры аутентификации и авторизации и совершенствует их путём использования стандартных механизмов: Kerberos, LDAP, Microsoft Active Directory, SASL.

В данной работе проведен анализ существующих направлений развития безопасности технологии контейнерной виртуализации, указаны преимущества и недостатки каждого направления. В ходе анализа найдены новые методы применения указанных решений.

Литература:

1. Why (and how) VMware created a new type of virtualization just for containers. [Электронный ресурс] Режим Доступа:
http://www.networkworld.com/article/2983023/data-center/
2. Немного о контейнерах. [Электронный ресурс] Режим доступа:
https://habrahabr.ru/company/it-grad/blog/279229/