УДК 004.056.5
DOI: 10.17586/0021-3454- 2021-64-5-364-369

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ ДЛЯ ОРГАНИЗАЦИИ РАЗГРАНИЧЕНИЯ ДОСТУПА

А. В. Переспелов, П. Ю. Богданов, Е. В. Краева

Российский государственный гидрометеорологический университет,
192007, Санкт-Петербург, Россия
E-mail: perespelov@mail.ru

Представлен обзор преимуществ операционных систем с открытым исходным кодом при проектировании системы защиты информации. Обсуждается технология виртуализации как эффективный способ защиты информационных систем. Приведен пример контейнерной виртуализации с построением адаптивной модели системы контроля доступа на ARM-процессоре. Оценка вероятности нестационарного проникновения в систему составила 2 %, что подтверждает эффективность предложенного решения и его применимость для построения адаптивной системы контроля доступа.

Ключевые слова: *информационная безопасность, разграничение доступа, виртуализация, идентификация, вероятность ошибки*

Введение. Практическая реализация моделей защиты информационных систем предполагает множество решений [1]. Рассмотрим совокупность перспективных информационных технологий, которые способны играть ключевую роль при разработке защищенных информационных систем.

Согласно анализу открытых источников [2—6], преобладают три класса устройств:

1) IoT — дешевые устройства с IP-адресами и доступом в Интернет;

2) персональные мобильные устройства, такие как современные телефоны и планшеты;

3) data-центры.

Для рассматриваемых классов устройств традиционно строится система разграничения доступа. В этой системе предусмотрен определенный перечень функций, в соответствии с которыми формируется защищенный вариант среды обработки информации при условии, что в системе не будет внутренних изъянов, позволяющих организовать хищение. Если такой изъян есть, то следует говорить о недекларируемых возможностях системы: закладках, логических бомбах и прочих особенностях, подрывающих четко определенный порядок изнутри. Система разграничения доступа представлена на рис. 1.

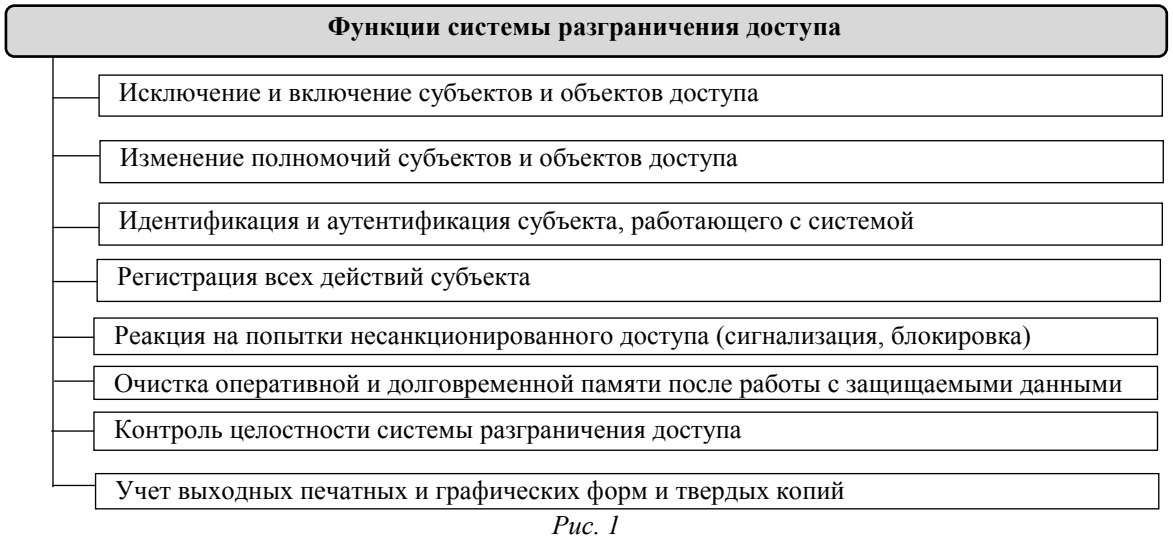

Рис. 1

Наличие системы разграничения доступа и правильное применение правил разграничения доступа исключают случайные или намеренные попытки несанкционированного доступа к устройствам и соответственно к хранящимся в них данным. Разграничение доступа решается специалистом операционной системы (ОС).

Существующая практика применения ОС показывает, что проприетарные ОС повсеместно заменяются на системы с открытым исходным кодом [7]. Преимущества свободного программного обеспечения заключаются в следующем:

— малые сроки внедрения;

— более низкая стоимость за счет повторного использования;

— невозможность добавления секретных кодов за счет прозрачности кода.

Такая практика сложилась в результате того, что обнаруженные секретные закладки в исходном коде программ делают возможным проникновение злоумышленника в обход системы защиты. Пользователи должны быть уверены в том, что в системе нет секретного кода, который сложно обнаружить. На основе полученного опыта эксплуатации систем с открытым исходным кодом развиваются методы безопасного использования или разработки программной части систем [8].

Одним из наиболее эффективных способов защиты информационных систем являются технологии виртуализации, позволяющие в одном физическом устройстве реализовать несколько изолированных друг от друга логических устройств с максимальным функционалом [9].

Технология виртуализации. Виртуализация осуществляется различными способами: эмуляция оборудования, аппаратная виртуализация, паравиртуализация, виртуализация на основе ОС (контейнерная виртуализация). В настоящей статье для защиты устройств предлагается использовать технологию контейнерной виртуализации как имеющую минимальные аппаратные требования к устройству.

Контейнерная виртуализация осуществляется на уровне ОС, при этом ядро ОС поддерживает несколько изолированных друг от друга пространств, называемых „пространством пользователя“. Эти пространства, с точки зрения пользователя, невозможно отличить от экземпляра операционной системы. Программы, находящиеся в разных контейнерах, не могут оказывать воздействие друг на друга, так как ядро обеспечивает полную изоляцию контейнеров. Каждый контейнер имеет свою собственную корневую файловую систему, процессы, память, устройства, сетевые интерфейсы и IP-адрес. Архитектура контейнера изображена на рис. 2.

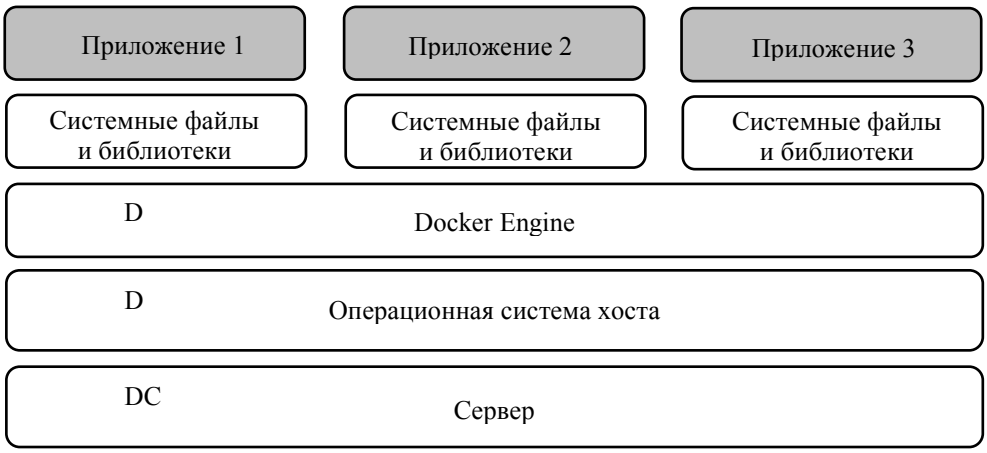

Рис. 2

Каждый контейнер имеет собственное изолированное пользовательское пространство, поэтому можно запускать несколько контейнеров на одном хосте. Контейнеры легковесны, так как архитектура уровня операционной системы разделяется между контейнерами.

Аппаратную часть устройства составляет процессор. Используя процессоры известных производителей, как правило, получаем проприетарный, т.е. закрытый продукт. Можно предположить, что в закрытом коде могут быть недокументированные функции устройства. Эти предположения неоднократно подтверждались [6]. Использовав „защищенную“ систему с проприетарным процессором, получим троянского коня. В настоящее время наиболее массовым для рассматриваемого класса устройств является ARM-процессор. На его основе строится адаптивная модель системы контроля доступа.

Цель настоящей работы — построение модели системы контроля доступа с основной операционной системой FreeBSD Jai. Было установлено программное обеспечение Docker, позволяющее автоматизировать процессы развертывания приложений в контейнерах. Данное программное обеспечение позволяет „упаковывать“ приложения с компонентами в Docker-контейнеры, управлять контейнерами для разработки и тестирования, доставлять эти контейнеры в data-центры и использовать облачные технологии [10—12].

В качестве защищаемого объекта рассматривался сервер базы данных MariaDB. Это серверная программа для хранения и получения данных с помощью SQL-запросов. Подобный класс программного обеспечения известен как система управления реляционными базами данных.

В качестве атакующего использовалось устройство, разработанное на основе ARM-процессора с установленной операционной системой Kali Linux. Дистрибутив отличается от других ему подобных большим количеством предустановленного специализированного программного обеспечения.

Оценка вероятности нарушения информационной безопасности. Для обеспечения информационной безопасности объекта важно следовать критериям и понятиям, описанным в стандарте ISO/IEC 27002:2005. Для оценки вероятности нарушения информационной безопасности используется формула о сложении вероятностей несовместных событий:

$$P(A+B+C) = P(A) + P(B) + P(C), \tag{1}$$

где A — событие, характеризующее нарушение конфиденциальности информации; B — событие, характеризующее нарушение доступности информации, C — событие, характеризующее нарушение целостности информации.

Вероятность суммы совместных событий

$$P(A+B) = P(A) + P(B) - P(AB). \tag{2}$$

Вероятность произведения независимых событий

$$P(AB) = P(A)P(B). \tag{3}$$

Для проверки конфиденциальности системы использована утилита SQLMAP. Это инструмент с открытым исходным кодом для пентестинга, который позволяет автоматизировать процесс обнаружения и использования SQL-инъекций и копирования серверных баз данных. Инструмент, предоставляемый с поисковым ядром, осуществляет проникновение с возможностью получения полезных сведений о базе данных и сведений от самой базы данных, получения доступа к основной файловой системе и выполнения команд над операционной системой посредством внеполосного подключения. Эта утилита может расшифровать хранимые в базе данные, в том числе и пароли.

Для защиты от атак типа DoS необходимо использовать правила и инструменты, описанные в [11]. Использование рассмотренной утилиты позволяет провести пентестинг готовой системы с целью обнаружения уязвимостей к каким-либо угрозам и атакам. Далее можно рассчитать вероятность проникновения в систему. Для этого готовая система, в которой не установлены настройки обеспечения безопасности, подвергается тестированию посредством ОС Kali Linux, с использованием утилиты 10 раз проводятся атаки и осуществляется наблюдение, сколько раз система будет взломана или будет нарушена ее работоспособность.

Далее, согласно выражению (1) рассчитывается вероятность проникновения в систему. По формуле (2) оценивается вероятность событий, если происходит проникновение посредством только одной утилиты. По формуле (3) оценивается вероятность событий, которые происходят одновременно.

Целостность системы нарушается во время каждой из атак, поэтому считаем, что вероятность $P(C)$ содержит первые два слагаемых. При тестировании системы получено $P(A)$= 0,7; $P(B)$=0,8. Если считать, что проникновение осуществлено посредством только одной утилиты, то $P(A+B) = P(A) + P(B) - P(AB) = 0,7 + 0,8 - (0,7 \cdot 0,8) = 0,94$. Следовательно, вероятность проникновения в систему равна 94 %. В случае если проникновение осуществляется с помощью двух утилит, то $P(AB) = P(A)P(B) = 0,7 \cdot 0,8 = 0,56$. Вероятность проникновения в систему составит 56 %.

После этого активируем средства безопасности Docker [12], проведя посредством каждой утилиты 10 атак, получаем $P(A)$=0,2; $P(B)$=0,1. Если считаем, что проникновение осуществлено с помощью только одной утилиты, то $P(A+B) = P(A) + P(B) - P(AB) = = 0,2 + 0,1 - (0,2 \cdot 0,1) = 0,28$. Следовательно, вероятность проникновения в систему составит 28 %. В случае проникновения с помощью двух утилит получим $P(AB) = P(A)P(B) = 0,2 \cdot 0,1 = 0,02$. Вероятность проникновения в систему составит 2 %.

Заключение. Показано, что технология контейнерной виртуализации является эффективным способом защиты информационных систем. Оценка вероятности несанкционированного проникновения в систему, построенной на ARM-процессоре, составила 2 % , что подтверждает эффективность предложенного решения и его применимость для построения адаптивной системы контроля доступа.

СПИСОК ЛИТЕРАТУРЫ

1. *Бурлов В. Г., Переспелов А. В., Переспелов Р. А.* О возможностях защиты аппаратной части информационной системы // Информационные технологии и системы: управление, экономика, транспорт, право. 2018. № 1(32). С. 63—71.
2. *Шваб К.* Глобализация 4.0. Новая архитектура для четвертой промышленной революции // Евразийская интеграция: экономика, право, политика. 2019. № 1(27). С. 79—84.
3. *Шнепс-Шнеппе М. А. Намиот Д. Е.* Цифровая экономика: телекоммуникации — решающее звено. М.: Горячая линия-Телеком, 2018. 150 с.
4. *Бакаров А. А., Девяткин Д. А., Ершова Т. В., Тихомиров И. А., Хохлов Ю. Е.* Научные заделы России по сквозным технологиям цифровой экономики // Информационное общество. 2018. № 4—5. С. 54—64.
5. *Тупчиенко В. А.* Цифровые платформы управления жизненным циклом комплексных систем. М.: Научный консультант, 2018. 439 с.
6. *Боков С. И.* О роли обеспечения системы управления цифровой экономикой России на основе организации единого информационного пространства // Наноиндустрия. 2019. Т. 12. С. 135—139.
7. *Переспелов А. В., Переспелов Р. А., Дубинина К. В., Матросова С. А.* Безопасность виртуализации в IT-технологиях // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 1 (33). С. 161—167.
8. *Верзун Н. А., Колбанёв М. О., Татарникова Т. М.* Аспекты безопасности информационно-экономической деятельности // Технологии информационно-экономической безопасности: Сб. СПб, 2016. С. 52—56.
9. *Зиновьев А. И., Шарыпова Д. В., Переспелов А. В.* Система для анонимного выхода сеть и тестирования на проникновение на базе микрокомпьютера Raspberry Pi 3 и дистрибутива Kali Linux // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 3 (35). С. 93—96.
10. *Бескид П. П., Татарникова Т. М.* О некоторых подходах к решению проблемы авторского права в сети Интернет // Ученые записки РГГМУ. 2010. № 15. С. 199—210.

11. *Переспелов А. В., Дубинина К. В., Матросова С. А.* Пентестинг передачи данных локальной сети // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 4 (36). С. 57—63.

12. *Переспелов А. В., Дубинина К. В., Матросова С. А.* Проверка безопасности СУБД MYSQL при помощи проведения пентестинга на Kali Linux // Устойчивое развитие науки и образования. 2019. № 10. С. 168—171.

Сведения об авторах

Анатолий Витальевич Переспелов — канд. техн. наук; РГГМУ, кафедра информационных технологий и систем безопасности; доцент; E-mail: perespelov@mail.ru

Павел Юрьевич Богданов — РГГМУ, кафедра информационных технологий и систем безопасности; ст. преподаватель; E-mail: 45bogdanov@gmail.com

Екатерина Витальевна Краева — РГГМУ, кафедра информационных технологий и систем безопасности; ассистент; E-mail: kate.smitt.by@mail.ru

Поступила в редакцию
23.01.2021 г.

Ссылка для цитирования: *Переспелов А. В., Богданов П. Ю., Краева Е. В.* Применение технологии виртуализации для организации разграничения доступа // Изв. вузов. Приборостроение. 2021. Т. 64, № 5. С. 364—369.

APPLICATION OF VIRTUALIZATION TECHNOLOGY TO ORGANIZE ACCESS CONTROL

A. V. Perespelov, P. Yu. Bogdanov, E. V. Kraeva

Russian State Hydrometeorological University,
192007, St. Petersburg, Russia
E-mail: perespelov@mail.ru

An overview of the advantages of open-source operating systems in information security system design is presented. Virtualization technology is discussed as an effective way to protect information systems. An example of container virtualization with the construction of an adaptive model of an access control system on an ARM processor is given. The assessment of the probability of non-stationary penetration into the system is 2%, which confirms the effectiveness of the proposed solution and its applicability for building an adaptive access control system.

Keywords: information security, access control, virtualization, identification, error probability

REFERENCES

1. Burlov V.G., Perespelov A.V., Perespelov R.A. *Informatsionnyye tekhnologii i sistemy: upravleniye, ekonomika, transport, pravo,* 2018, no. 1(32), pp. 63–71. (in Russ.)
2. Schwab K. *Eurasian Integration: Economics, Law, Politics,* 2019, no. 1(27), pp. 79–84. (in Russ.)
3. Shneps-Shneppe M.A. Namiot D.E. *Tsifrovaya ekonomika: telekommunikatsii – reshayushcheye zveno* (Digital Economy: Telecommunications is the Critical Link), Moscow, 2018, 150 p. (in Russ.)
4. Bakarov A.A., Devyatkin D.A., Ershova T.V., Tikhomirov I.A., Khokhlov Yu.E. *Information Society,* 2018, no. 4–5, pp. 54–64. (in Russ.)
5. Tupchiyenko V.A. *Tsifrovyye platformy upravleniya zhiznennym tsiklom kompleksnykh system* (Digital Platforms for Managing the Life Cycle of Complex Systems), Moscow, 2018, 439 p. (in Russ.)
6. Bokov S.I. *Nanoindustry*, 2019, vol. 12, pp. 135–139. (in Russ.)
7. Perespelov A.V., Perespelov R.A., Dubinina K.V., Matrosova S.A. *Informatsionnyye tekhnologii i sistemy: upravleniye, ekonomika, transport, pravo,* 2019, no. 1(33), pp. 161–167. (in Russ.)
8. Verzun N.A., Kolbanev M.O., Tatarnikova T.M. *Tekhnologii informatsionno-ekonomicheskoy bezopasnosti* (Information and Economic Security Technologies), St. Petersburg, 2016, pp. 52–56. (in Russ.)
9. Zinoviev A.I., Sharypova D.V., Perespelov A.V. *Informatsionnyye tekhnologii i sistemy: upravleniye, ekonomika, transport, pravo,* 2019, no. 3(35), pp. 93–96. (in Russ.)
10. Beskid P.P., Tatarnikova T.M. *Uchenyye zapiski Rossiyskogo gosudarstvennogo gidrometeorologicheskogo universiteta,* 2010, no. 15, pp. 199–210. (in Russ.)
11. Perespelov A.V., Dubinina K.V., Matrosova S.A. *Informatsionnyye tekhnologii i sistemy: upravleniye, ekonomika, transport, pravo,* 2019, no. 4(36), pp. 57–63. (in Russ.)
12. Perespelov A.V., Dubinina K.V., Matrosova S.A. *Ustoychivoye razvitiye nauki i obrazovaniya*, 2019, no. 10, pp. 168–171. (in Russ.)

Data on authors

Anatoly V. Perespelov — PhD; Russian State Hydrometeorological University, Department of Information Technology and Security Systems; Associate Professor; E-mail: perespelov@mail.ru

Pavel Yu. Bogdanov — Russian State Hydrometeorological University, Department of Information Technology and Security Systems; Senior Lecturer; E-mail: 45bogdanov@gmail.com

Ekaterina V. Kraeva — Russian State Hydrometeorological University, Department of Information Technology and Security Systems; Assistant; E-mail: kate.smitt.by@mail.ru

For citation: Perespelov A. V., Bogdanov P. Yu., Kraeva E. V. Application of virtualization technology to organize access control. *Journal of Instrument Engineering*. 2021. Vol. 64, N 5. P. 364—369 (in Russian).

DOI: 10.17586/0021-3454- 2021-64-5-364-369