ВЕРЖДАЮ

1-й .Г. Демидова

.А. Кащенко.

2019 г.

ОТЗЫВ

ведущей организации - федерального государственного бюджетного

образовательного учреждения высшего образования

«Ярославский государственный университет им. П.Г. Демидова»

на диссертацию **Петрова Ивана Сергеевича**

по теме «Обнаружение скомпрометированных коммутаторов в программно-конфигурируемых сетях»,

представленную на соискание ученой степени

кандидата физико-математических наук по специальности

05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Актуальность темы

Программно-конфигурируемые сети (ПКС) – одна из наиболее перспективных и исследуемых тем в области сетей передачи данных. ПКС представляют собой класс сетей с централизованным управлением и унифицированными интерфейсами сетевых устройств. В отличие от традиционных сетей с полностью децентрализованным управлением, где практически невозможно математически строгое введение понятия состояния сети, в этом классе сетей – такое возможно, что создает хорошую перспективу для построения математических моделей функционирования сетей этого класса. С математической точки зрения, это важное достоинство ПКС сетей. Кроме этого, открытые интерфейсы контура управления (протокол OpenFlow) и контура передачи данных делают ПКС вендоронезависимыми и позволяют разрабатывать программное обеспечение для управления сетью независимо от производителя оборудования в виде приложений на выделенном устройстве – контроллере.

Однако, новая концепция построения сети также открывает новые возможности для злоумышленников, которые могут использовать свойства таких сетей для проведения неизвестных ранее атак. Таким образом, необходимы исследования,

нацеленные на определения новых векторов атак и на создание алгоритмов и систем защиты информационной безопасности программно-конфигурируемых сетей.

Одна из наиболее серьезных угроз для ПКС – угроза наличия в сети скомпрометированных коммутаторов, то есть коммутаторов, захваченных некоторым злоумышленником. Серьезность угрозы обусловлена тем, что такие коммутаторы могут использоваться для широкого спектра атак как на контур управления, так и на контур передачи данных. Сложность задачи обнаружения скомпрометированных коммутаторов обусловлена невозможностью использования криптографических методов аутентификации и возможностью использования злоумышленником различных техник сокрытия атак. Серьезность и сложность описанной задачи обосновывает необходимость разработки алгоритмов и средств для обнаружения скомпрометированных коммутаторов и минимизации их воздействия на сеть.

Степень обоснованности научных положений, выводов и рекомендаций

В диссертации Петрова И.С. рассматривается задача обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях.

В первой главе проводится введение в предметную область, вводятся основные понятия, приводится содержательное описание задачи обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях и описываются проблемы, связанные с этой задачей.

Во второй главе рассмотрены угрозы, связанные с наличием в сети скомпрометированного коммутатора, и основные атаки, которые злоумышленники могут проводить с использованием таких коммутаторов.

В третьей главе приведен сравнительный анализ существующих средств для обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях. На основе сравнительного анализа было показано, что существующие системы обладают рядом ограничений, таких как: неспособность разграничения вредоносного и легитимного сброса пакетов и зависимость от используемых в сети алгоритмов маршрутизации. Также в главе сформулированы требования к системе обнаружения скомпрометированных коммутаторов в ПКС.

В четвертой главе приводится описание разработанной математической модели, описывающей динамику изменения значений счетчиков OpenFlow правил, которая позволяет описывать произвольную логику маршрутизации в сети. Разработанная модель описывает счетчики в виде значений потоковой функции на графе специального вида. Также в главе описан разработанный алгоритм предсказания значений таких счетчиков на основе информации о сетевой статистике на границе сети.

В пятой главе приводится описание разработанного алгоритма обнаружения скомпрометированных коммутаторов. Алгоритм устанавливает в сеть специальный набор дополнительных правил маршрутизации, которые используются для предсказания значений счетчиков произвольных правил маршрутизации. Далее, предсказанные значения сравниваются с реальными значениями, полученными от коммутаторов, и на основе анализа отклонений таких значений, производится обнаружение скомпрометированных коммутаторов.

В шестой главе приведено описание архитектуры разработанной автором системы обнаружения скомпрометированных коммутаторов и результаты проведенного экспериментального исследования. В главе был сделан вывод о том, что разработанная системы может быть использована в реальных сетях операторов связи и центрах обработки данных.

Достоверность результатов диссертации обеспечивается использованием методов теории графов, формулировкой и доказательством основных свойств разработанной модели и доказательством корректности разработанного алгоритма, а также достаточным объемом проведенных экспериментальных исследований.

Практическая ценность и новизна работы

Практическая ценность диссертации обеспечивается популярностью программно-конфигурируемых сетей и растущими требованиями к информационной безопасности таких сетей. Результаты работы могут быть использованы для обеспечения безопасности в сетях телеком-операторов и центрах обработки данных.

Работа содержит интересные новые научные результаты. Так, например, следует отметить оригинальность и эффективность новой математической модели, которая позволяет описывать динамику изменения счетчиков правил маршрутизации в программно-конфигурируемых сетях, работающих по протоколу OpenFlow. В работе подробно исследованы свойства этой модели. Показано, что введенная в модели потоковая функция является потоком с мультипликаторами, также доказано, что эта функция допускает разложение по доменным путям графа зависимостей правил.

Результаты, полученные при исследовании модели, позволили разработать алгоритмы предсказания счетчиков правил маршрутизации и обнаружения скомпрометированных коммутаторов, не накладывающие ограничения на набор приложений, используемых контроллером.

К достоинствам работы следует в первую очередь отнести то, что разработанный алгоритм применим в реальных сетях операторов связи и центров обработки данных. Убедительно показано, что алгоритм свободен от недостатков существующих алгоритмов обнаружения скомпрометированных коммутаторов. Также необходимо

отметить тщательное экспериментальное исследование свойств разработанного алгоритма.

Замечания по диссертационной работе

В целом работа оставляет положительное впечатление. Следует отметить четкость, строгость и ясность изложения. Однако в целях улучшения работы, можно было бы сформулировать следующие замечания:

1. В главе 4, описывающей разработанную автором модель, не совсем удачно выбраны некоторые обозначения, например, для описания подмножеств множества N выбран символ D.
2. В исследовании рассматриваются коммутаторы, захваченные некоторым злоумышленником и использующиеся для проведения сетевых атак. Однако, не рассмотрена возможность наличия в сети некорректно работающих коммутаторов, которые, в принципе, могут быть неотличимы от скомпрометированных.

Указанные замечания не влияют на положительную оценку работы и не ставят под сомнения основные выводы диссертационной работы.

Заключение

Автореферат правильно отражает содержание диссертации.

Диссертация в целом представляет собой законченный научный труд, в котором содержится решение задач, имеющих существенное значение для теории и практики обеспечения безопасности компьютерных сетей.

Работа удовлетворяет требованиям ВАК, предъявляемым к кандидатским диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей», а Петров И.С. достоин присуждения ему искомой степени.

Отзыв рассмотрен на заседании кафедры теоретической информатики Ярославского государственного университета им. П.Г. Демидова

3 апреля 2019 г., протокол № 10.

Зав. кафедрой теоретической информатики
д.ф.-м.н., профессор Соколов Валерий Анатольевич