ОТЗЫВ

официального оппонента на диссертационную работу
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 диссертации

Диссертационная работа И.С. Петрова посвящена исследованию одной из **важных и актуальных** задач обеспечения информационной безопасности программно-конфигурируемых сетей (ПКС): обнаружению скомпрометированных коммутаторов в ПКС сетях на основе OpenFlow протокола. ПКС – это новая парадигма создания компьютерных сетей, которая с момента своего появления вызывает большой интерес, как академических исследователей, так и практиков. Основу парадигмы ПКС составляет отделение контура управления от контура передачи данных и централизация управления сетью в контуре управления за счет введения нового сетевого устройства – контроллера ПКС. Контроллер ПКС управляет сетью, состоящей из коммутаторов, при помощи различных протоколов. Протокол OpenFlow является одним из наиболее популярных протоколов управления коммутаторами.

Важность и актуальность представленного исследования связана с угрозой наличия в сети скомпрометированных коммутаторов и необходимостью обнаруживать такие коммутаторы для предотвращения их негативного влияния на сеть. Под скомпрометированным коммутатором понимается коммутатор, который был захвачен атакующим при помощи эксплуатации некоторой уязвимости. Такие коммутаторы являются угрозой информационной безопасности программно-конфигурируемой сети из-за широких возможностей их использованию в качестве платформ для проведения сетевых атак.

Структура диссертации

Диссертация состоит из введения, шести глав, заключения, одного приложения и списка литературы, содержащего 83 наименования. Полный объем диссертации составляет 156 страниц.

Во **введении** описываются принципы организации программно-конфигурируемых сетей; задачи, связанные с обеспечением безопасности таких сетей; обосновываются актуальность и цели представленной работы по обнаружению скомпрометированных коммутаторов.

В **первой главе** соискателем описана постановка задачи обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях, и основные проблемы, возникающие при решении поставленной задачи.

Во **второй главе** соискатель описывает возможные атаки, проводимые на сеть с использованием скомпрометированных коммутаторов. Атаки подразделяются на атаки на контур передачи данных и атаки на контур управления. В главе описаны как традиционные атаки, применимые к любым типам сетей, так и атаки, характерные только для ПКС.

Третья глава содержит обзор существующих систем обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях. Существующие системы сравниваются на основе критериев, основанных на возможности обнаружения различных типов атак и ограничений, накладываемых на приложения контроллера. Результат обзора показывает, что существующие системы имеют ряд недостатков и серьезных ограничений.

В **четвертой главе** приведены разработанная соискателем математическая модель динамики изменения счетчиков правил маршрутизации и исследование ее основных свойств. Модель сети представлена в виде графа, в котором вершины описывают правила маршрутизации, а ребра описывают возможные переходы пакетов между правилами. На графе зависимостей правил также вводится специальная потоковая функция, которая отражает значения счетчиков правил маршрутизации. На основе описанной модели в диссертационной работе разработан алгоритм предсказания значений счетчиков правил маршрутизации и доказана его корректность.

В **пятой главе** описан разработанный автором алгоритм обнаружения скомпрометированных коммутаторов. Алгоритм использует разработанную математическую модель для предсказания значений счетчиков правил маршрутизации и обнаружения отклонений в сетевой статистике.

В **шестой главе** приводится подробное описание архитектуры реализации алгоритма обнаружения скомпрометированных коммутаторов. Также в главе описано исследование времени работы алгоритма и величин ошибок первого/второго рода при обнаружении скомпрометированных коммутаторов. Результаты экспериментального исследования показывают, что разработанная система может быть полезна для обеспечения безопасности программно-конфигурируемых сетей, используемых реальными операторами связи и центрами обработки данных.

В **заключении** приведены основные результаты диссертационной работы.

Достоверность, научная новизна и практическая значимость

Отметим основные научные результаты, приведенные в работе:

1. Разработана математическая модель, описывающая динамику счетчиков OpenFlow правил в ПКС, которая инвариантна относительно типа алгоритмов маршрутизации, используемых в сети.
2. В рамках разработанной модели построен алгоритм предсказания значений счетчиков правил маршрутизации. Доказана корректность этого алгоритма.
3. Разработан алгоритм обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях. Для разработанного алгоритма экспериментально показано, что он может использоваться в реальных сетях операторов связи и в центрах обработки данных.

К достоинствам работы следует отнести оригинальность математической модели, которая позволила сформулировать и доказать ряд интересных и важных для решаемой задачи свойств поведения счетчиков правил в OpenFlow коммутаторах, методическую грамотность при разработке математической модели программно-конфигурируемой сети, подробное исследование основных свойств разработанной модели и обоснованность полученных теоретических результатов.

Замечания

В качестве замечаний к работе отметим следующее:

1. В работе автор не всегда придерживается единой терминологии. Так, например, в тексте автор говорит о правилах маршрутизации, а на с. 116 употребляется термин OpenFlow правило.
2. В диссертационной работе не приведены результаты исследований масштабируемости, то есть роста времени работы алгоритма в зависимости от количества работающих на контроллере приложений.
3. Предложенный автором алгоритм построения путевой развертки выполняет множество однотипных задач над элементами пространства заголовков, и, по всей вероятности, его реализация могла бы быть значительно ускорена за счет распараллеливания и использования графических ускорителей.
4. Модель, описывающая динамику изменения счетчиков правил маршрутизации, не учитывает особенностей сетей передачи данных, а именно затрат времени на передачу сообщения.

Указанные недостатки, однако, не являются принципиальными и не умаляют достоинств диссертации.

Заключение

В диссертационной работе Петрова Ивана Сергеевича представлено решение задачи обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях. Задача является актуальной, приведенные в работе результаты экспериментальных исследований показывают, что разработанный алгоритм может быть использован для обеспечения информационной безопасности сетей операторов связи и центров обработки данных.

Основные результаты диссертации полно отражены в публикациях автора, в том числе в журналах, входящих в перечень рецензируемых журналов ВАК и индексируемых системами Scopus и Web of Science.

Диссертация Петрова И.С. является законченной научно-квалификационной работой и отвечает требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 - математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Официальный оппонент:
Доктор физико-математических наук, профессор,
заведующая научно-учебной лабораторией
процессно-ориентированных информационных систем
факультета компьютерных наук
Национального исследовательского университета
«Высшая школа экономики» Ломазова И.А.

«23» апреля 2019 г.