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

Работа посвящена исследованию методов обнаружения скомпрометированных OpenFlow коммутаторов в программно-конфигурируемых сетях. Программно-конфигурируемые сети (ПКС) – это новый класс компьютерных сетей, главными особенностями которого являются разделение контуров передачи данных и управления сетью, и централизации управления сетью. Особенностью ПКС является наличие выделенного устройства, которое управляет сетью, состоящей из коммутаторов, и предоставляет возможность настраивать логику работы сети при помощи специальных сетевых приложений.

Одной из наиболее важных задач обеспечения информационной безопасности ПКС является задача обнаружения скомпрометированных коммутаторов, то есть коммутаторов, захваченных некоторым атакующим. Важность задачи обоснована тем, что скомпрометированный коммутатор позволяет злоумышленникам подготавливать и проводить большое количество типов атак как на клиентов сети, так и на контроллер.

К настоящему моменту разработано несколько средств для обнаружения скомпрометированных коммутаторов в ПКС. Однако, эти средства, как показано в диссертационной работе, обладают рядом недостатков, которые ограничивают их применимость в реальных сетях.

Структура диссертации

Диссертация состоит из введения, шести глав, заключения, одного приложения и списка литературы.

Первая глава посвящена описанию задачи обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях и основных проблем, связанных с этой задачей.

Вторая глава посвящена описанию различных типов атак, которые злоумышленник может проводить с использованием скомпрометированного коммутатора.

В третьей главе приводится сравнительный анализ существующих систем, решающих задачу обнаружения скомпрометированных коммутаторов в ПКС. Сравнительный анализ проводится на основе критериев, описывающих возможности систем по обнаружению различных типов атак и применимость в сетях с различными механизмами маршрутизации.

В четвертой главе описана и исследована разработанная автором математическая модель программно-конфигурируемой сети, которая описывает поведение счетчиков, установленных на правилах маршрутизации. На основе этой модели был разработан алгоритм, который предсказывает значения счетчиков правил маршрутизации, используя частичную информацию о сетевой статистике.

Пятая глава является описанием алгоритма обнаружения скомпрометированных коммутаторов в ПКС. Алгоритм использует разработанную математическую модель для обнаружения аномалий в значениях счетчиков правил маршрутизации.

Шестая глава представляет собой описание реализации системы обнаружения, основанной на разработанном алгоритме обнаружения скомпрометированных коммутаторов. Также приведены результаты проведенного экспериментального исследования. Эксперименты проводились для определения ошибок первого/второго рода, определения времени работы алгоритма и точности предсказания значений счетчиков на различных топологиях, описывающих реальные сети передачи данных, используемые операторами связи.

В заключении представлены результаты диссертационной работы.

В приложении А приведено подробное описание модулей реализованной системы обнаружения скомпрометированных коммутаторов.

Новизна научных положений и выводов диссертации определяется тем, что решена задача обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях. Автором получен ряд новых научных результатов, к числу которых можно отнести следующие.

1. Разработана математическая модель программно-конфигурируемой сети, описывающая динамику изменения счетчиков правил маршрутизации.
2. Разработан алгоритм предсказания значений счетчиков правил маршрутизации.
3. Разработан алгоритм обнаружения скомпрометированных коммутаторов, который не накладывает ограничения на топологию и приложения, работающие на контроллере.

Практическая значимость результатов работы заключается в том, что использование полученных результатов обеспечивает основу для разработки новых методов и средств обеспечения безопасности программно-конфигурируемых сетей.

Обоснованность и достоверность положений и выводов диссертации подтверждается соответствием теоретических и экспериментальных результатов, полученных на реальных программных коммутаторах и топологиях, отражающих сети существующих операторов связи.

Следует отметить четкость, ясность и лаконичность текста диссертации, элегантность доказательств теорем и самой конструкции модели. Хотелось бы также отметить обзор существующих систем обнаружения скомпрометированных коммутаторов и их сравнительный анализ на основе четких критериев, описывающих реальные требования к системам обнаружения вторжений. Разработанная система выгодно отличается от существующих систем обнаружения и не накладывает дополнительных ограничений на логику работы контроллера. Безусловным достоинством диссертации является экспериментальное исследование по оценке качества полученного решения и определения его применимости в реальных сетях. Здесь очень важно то, что автор четко описал и обосновал методику проведения экспериментов.

Недостатки диссертации

1. Разработанная автором модель сети могла бы иметь большую практическую ценностью, если бы она также моделировала задержки, связанные с обработкой трафика коммутаторами.
2. При описании путевой развертки в разделе 4.2.2 автору следовало бы привести пример построения путевой развертки по некоторому реальному графу зависимостей правил в целях ясности изложения.
3. В результатах экспериментального исследования описана зависимость времени работы алгоритма от размера сетевой топологии и количества правил маршрутизации в сети. При этом не описано, на каких сетевых топологиях достигалось наибольшее время работы алгоритма.
4. Замечания к структуре диссертации: главу 2 «Угрозы безопасности ПКС» стоило бы сделать разделом главы 1.

Отмеченные выше недостатки, в целом, не снижают высокого уровня работы.

Заключение

На основании вышеизложенного следует сделать вывод, что диссертация И.С. Петрова «Обнаружение скомпрометированных коммутаторов в программно-конфигурируемых сетях» представляет собой законченную работу в важном научном

направлении - разработке алгоритмов обеспечения информационной безопасности программно-конфигурируемых сетей. Положения и выводы, сформулированные в диссертации, обоснованы и достоверны. Теоретические результаты сопровождаются математическими доказательствами. Результаты диссертационной работы новы, представляют значительный научный интерес и подтверждаются экспериментами. Опубликованные работы и автореферат достаточно полно и правильно отражают основное содержание диссертации.

Представленная диссертационная работа соответствует требованиям, предъявляемым Положением о порядке присуждения ученых степеней к кандидатским диссертациям, соответствует профилю специальности 05.13.11 - «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей», а ее автор И.С. Петров заслуживает присуждения ему степени кандидата физико-математических наук по указанной специальности.

Официальный оппонент:
Кандидат технических наук,
начальник научно-технического центра
перспективных технологий информационных
процессов ФГАНУ ЦИТиС Селиванов С.А.

09 2019 г.