УДК 004.4:004.7

ПРОГРАММНО-КОНФИГУРИРУЕМАЯ СЕТЬ: НОВЫЕ ПОДХОД К СЕТЯМ ПЯТОГО ПОКОЛЕНИЯ - ПРОБЛЕМЫ БЕЗОПАСНОСТИ И ВЫЗОВЫ НА БУДУЩЕЕ

Бехруз Данешманд (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель - д.т.н. , доцент Грудинин Владимир Алексеевич (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. Программно-конфигурируемая сетевая парадигма коренным образом меняет телекоммуникационные сети и широко используется в качестве мощной технологии в таких инициативах, как 5G или Интернет вещей (IoE). В ней перечислен ряд доказанных причин для этого, включая объем данных, экспоненциальный рост числа подключенных устройств и необходимость быстрой обработки данных. Хотя, с момента создания прошло более двух десятилетий, SDN постоянно развиваются, и в мире технологий растет число потребностей, которые требуют динамических, более гибких и более безопасных SDN. В отличие от перечисленных преимуществ, архитектура SDN предполагает некоторые уязвимости. В приложениях следующего поколения будут использоваться более точные агенты SDN для улучшения применения политик, а также для обнаружения и устранения аномалий трафика. Эти программы могут блокировать проникновение злоумышленников в критические области сети. Если безопасность SDN не может быть гарантирована, их разработка встретит сильное сопротивление и даже не будет иметь никакого отношения к процессу замены традиционной сетевой архитектуры. Поскольку существует достаточно проверенных исследований аспектов безопасности традиционной сетевой архитектуры, эта статья ограничивается акцентом на аспектах безопасности архитектуры SDN. Основная цель этой статьи - обсудить архитектуру SDN, уязвимости безопасности и меры противодействия угрозам SDN.

Цель работы . Целью исследования является углубленное изучение распространенных проблем безопасности SDN, от базовой технологии до проблем безопасности на каждом уровне в SDN.

Базовые положения исследования . Основное содержание исследования сосредоточено на нескольких областях, которые описаны ниже:

1- Подход к моделированию угроз на основе уровня управления

2- SDN с точки зрения безопасности, поведения и ошибок

3- Девять типов атак на SDN и методы защиты.

4- Анализ SDN-атаку с акцентом на каждом уровне

Основной результат . В этой статье основное внимание уделяется развивающейся сетевой архитектуре, программно-конфигурируемым сетям и существующим проблемам безопасности. Это факт, что в сетях нового поколения мы стремимся к программно-конфигурируемым сетям

(SDN), но существует проблема - сетевая безопасность. С точки зрения безопасности элементы, составляющие архитектуру SDN, имеют ряд уязвимостей, которые могут быть использованы злоумышленниками для выполнения злонамеренных действий и таким образом, воздействия на сеть и ее службы. Программно-конфигурируемые сетевые атаки, к сожалению, в наши дни стали реальностью. В докладе также анализируются различные архитектурные недостатки и разрабатываются векторы атак на каждом уровне, что позволяет сделать выводы о дальнейшем прогрессе в выявлении последствий атак и предложении стратегий защиты от угроз.

Доклад завершается анализом различных типов атак на разных уровнях сети SDN и предлагает более широкую перспективу для понимания и продвижения вперед в сокращении атак, тем самым создавая уникальное представление. Отдельная архитектура SDN имеет дополнительное преимущество в том, что она программируема и совместима. Если эта развивающаяся сетевая архитектура не сможет принять соответствующие методы повышения уровня безопасности и защиты от угроз, упомянутых и обсужденных выше, возникнут недостатки. Дальнейшая работа может быть сосредоточена на тестировании и сравнении различных решений, которые могут защитить разные уровни архитектуры.