Литература

1. Столлингс В. Криптография и защита сетей: принципы и практика. – М. , Изд. дом «Вильямс», 2001. – 672 стр.
2. Венбо Мао. Современная криптография. Теория и практика. – Москва–Санкт-Петербург–Киев: Лори Вильямс, 2005. –768 стр.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 1-2-е изд. –М.: Гелиос АРВ, 2002.-480 с

Н.А. Филатов

УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ

(Самарский университет)

Сегодня контроллеры OpenFlow [1], [2] работают, преимущественно, как некоторые точки координации, которые передают правила потока от приложений, отправляют запросы конфигурации и исследуют совокупность данных, чтобы получить информацию о состоянии. Так как контроллер взаимодействует со всеми коммутаторами в своей сети или сетевом срезе, он предоставляет средства для распределения скоординированного набора правил потока по сети для оптимизации маршрутов потока и переадресации, а также баланса трафика для повышения эффективности сети.

В области сетевой безопасности OpenFlow может предложить уникальный контроль над любым потоком (или участником потока), считающимся опасным. Приложение OpenFlow, направленное на безопасность может осуществить более сложную логику управления потоками, чем просто остановить или перенаправить поток. Подобные приложения могут включать логику составления правил потока с отслеживанием состояния для реализации сложных процедур помещения на карантин производителя потока, или они могут переносить вредоносное соединение в специальное приложение-ловушку для дальнейшего анализа вредоносной деятельности способом, незаметным для атакующего.

Тем не менее, существуют также и существенные проблемы безопасности, возникающие в OpenFlow и SDN. Например, то, какая политика сетевой безопасности осуществляется в коммутаторах OpenFlow, во всем зависит от того, как текущие приложения OpenFlow отвечают на поступающие запросы потока.

В данных тезисах рассматриваются проблемы определения уровня безопасности посредничества между прикладным уровнем OpenFlow (где должны существовать как приложения безопасности, так и приложения для управления трафиком) и плоскостью данных (где коммутаторы реализуют политики потоков, реализуемые правилами потоков, создаваемых приложениями OpenFlow). В качестве контроллера используется SE-Floodlight. SE-Floodlight расширяет

контроллер Floodlight с помощью ядра безопасности (SEK), функции которого также напрямую применимы к другим контроллерам OpenFlow. SEK добавляет уникальный набор функций безопасного управления приложениями, включая службу проверки подлинности, авторизацию на основе ролей, модель разрешения для оповещения всех запросов на изменение конфигурации на плоскости данных, разрешение конфликтов встроенного потока и службу аудита безопасности.

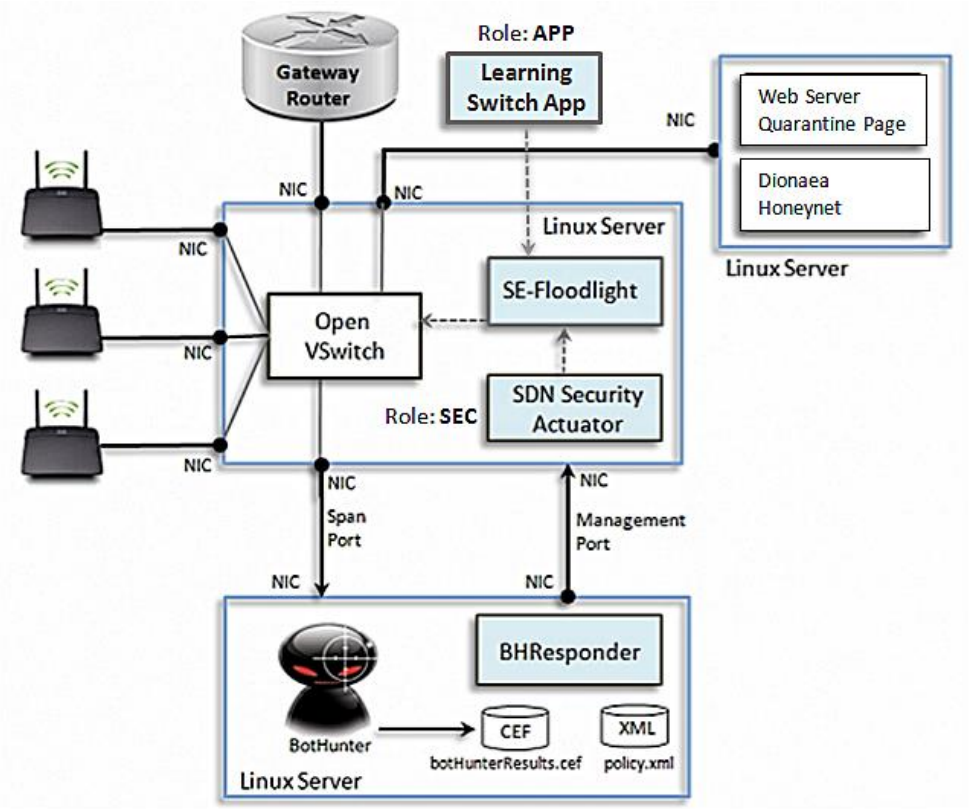

Рис. 1. Топология самозащищающейся беспроводной сети, которая использует SEFloodlight для управления службой защиты от вредоносных программ, названной BotHunter, параллельно с приложением обучения контроллера. Комбинированные приложения управляют беспроводным сетевым трафиком и автоматически помещают в карантин все потоки, поступающие к локальному беспроводному клиенту и от него, когда BotHunter обнаруживает, что беспроводной клиент заражен вредоносными программами

Для тестирования SDN технологий, SE-Floodlight был развернут в качестве общедоступной точки доступа беспроводной сети. Топология сети показана на рисунке 1. Плоскость данных беспроводной сети на основе OpenFlow воссоздана с помощью OpenVswitch, соединяющего набор точек доступа 802.11 b с интернетом. SE-Floodlight реализует уровень управления, запускающий несколько приложений OpenFlow. Первое является вариантом модуля Learning Switch, и применяется для передачи сетевых потоков от беспроводных клиентов на шлюз. Второе представляет из себя три независимых приложения. BotHunter осуществляет надзор за портом логического коммутатора, анализируя трафик от беспроводных клиентов. BotHunter использует свой алгоритм корреляции диалоговых окон для идентификации локальных беспроводных

клиентов, работающих в соответствии с координационно-ориентированной вредоносной программой [3]. Когда BotHunter создает профиль заражения, профиль передается в BHResponder, который реализует простой алгоритм сопоставления политики, чтобы решить, должен ли локальный ресурс быть помещен на карантин. Если это так, BHResponder передает директиву безопасности карантина, которая определяет IP-адрес локального беспроводного клиента в SDN Security Actuator. SDN Security Actuator – это приложение OpenFlow, работающее с ролью SEC, и использующее API SE-Floodlight Northbound для взаимодействия с SE-Floodlight. При активации он регистрирует обратный вызов для получения уведомлений обо всех потоковых запросах к зараженному клиенту и от него. Все подключения к клиенту и от него затем запрещаются.

Таким образом, была рассмотрена проблема безопасности, связанная с набором функций, которые позволят сети OpenFlow для нескольких приложений работать в чувствительной сетевой вычислительной среде, которая в свою очередь должна отвечать строгим требованиям безопасности [4]. А именно рассмотрено согласование динамического производства логики правил потока с необходимостью сохранения последовательных ограничений политики безопасности, которые в сетях OpenFlow, по существу, являются правилами потока, создаваемыми администратором или динамически вставляемыми приложениями безопасности в ответ на воспринимаемые угрозы. Следовательно, для уязвимых вычислительных сред существует достаточная мотивация, чтобы рассмотреть SDN как потенциальный источник инновационного устранения угроз.

Литература

1. FloodLight [Electronic resource] “Open SDN controller,” http://floodlight.openflowhub.org/.

2. N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, “NOX: Towards an Operating System for Networks,” in Proceedings of ACM Computer Communications Review, July 2008.

3. G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection Through IDS-driven Dialog Correlation,” in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, 2007.

4. Sukhov A. M., Sagatov E. S., Baskakov A. V. Rank distribution for determining the threshold values of network variables and the analysis of DDoS attacks //Procedia Engineering. – 2017. – Т. 201. – С. 417-427.

В.П. Цветов

О ВЛОЖЕНИИ ИЗМЕРИТЕЛЬНЫХ ШКАЛ

(Самарский университет)

В современной теории измерений выделяют пять основных видов шкал измеряемых величин [1].