

УДК: 004.7

DOI: 10.30987/article_5d8d113d968333.98732766

М.Ю. Рытов, Р.Ю.Калашников

ПРИМЕНЕНИЕ МЕТОДОЛОГИИ STRIDE ДЛЯ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЕЙ

В статье рассматривается применение модели угроз STRIDE к общим концепциям SDN. Выявлены основные недостатки безопасности в современных концепциях программно-определяемых сетей. По результатам анализа предложена основа для разработки безопасной архитектуры SDN.

Ключевые слова: оценка рисков, программно-определяемая сеть, информационная безопасность.

M.Yu. Rytov, R.Yu. Kalashnikov

APPLICATION OF STRIDE METHODOLOGY FOR DETERMINING CURRENT SECURITY THREATS FOR PROGRAM-DEFINED NETWORKS

In this paper, STRIDE threat model is applied to the generic SDN concepts. The current security flaws in modern concepts of software-defined networks are discussed. As a result of the analysis the basis for developing a secure SDN architecture is presented.

Keywords: risk assessment, software-defined networks, information security.

Введение

Основная идея программно-определяемых сетей (SDN) состоит в том, чтобы отделить данные и плоскость управления от сетевых компонентов и перенести функциональность плоскости управления на отдельные контроллеры SDN. Эта концепция связана с фундаментальными изменениями, касающимися управления сетью.

Одним из основных направлений развития концепции является применение SDN в сетях магистральной инфраструктуры интернета. Эта потенциальная область применения придает безопасности в SDN первостепенное значение.

Протокол Open Flow, несмотря на наличие альтернатив, является де-факто стандартным интерфейсом между платформой управления на основе SDN и плоскостью данных. Поддержкой, развитием, а также поиском потенциальных уязвимостей в реализациях протокола занимается организация Open Networking Foundation (ONF). Тем не менее, производители сетевого оборудования зачастую пренебрегают вопросами безопасности SDN в пользу функциональности и функциональной совместимости, которые являются важными преимуществами и, таким образом, обычно имеют приоритет над улучшениями безопасности в отношении разработки микропрограмм и программного обеспечения.

При рассмотрении вопроса о развертывании технологии SDN организациям рекомендуется проводить анализ рисков и выгод, состоящий из величины потенциальных потерь и вероятности возникновения таких потерь. Для оценки рисков необходимо определить угрозы. Microsoft STRIDE - методика определения актуальных угроз информационных систем, и поэтому она пригодна для оценки безопасности SDN. Данная методика включает в себя оценку рисков информационной безопасности по следующим категориям: спуфинг, модификация, отказ от авторства, разглашение, отказ в обслуживании и повышение привилегий. Данная статья посвящена декомпозиции концепции SDN на основные элементы (плоскость данных, плоскость управления и протокол Open Flow) и применению анализа STRIDE к этим компонентам.

1. Определение актуальных угроз в сетях SDN

SDN переносит управление всей сетью в единую автономную программную систему. Результатом этого является возможность гибкой настройки и управления сетью, но в то же время повышается зависимость от единого узла управления. Следовательно, архитектура может таить в себе непредвиденные риски. Повышенное внимание к программному обеспечению, программируемости и открытым интерфейсам может открыть для злоумышленника несколько новых векторов атаки. Кроме того, центральный контроллер является основной целью для DoS-атак, так как работа всей сети зависит от одного устройства. Поскольку влияние скомпрометированных устройств значительно возрастает, разработка устройств SDN должна подвергаться постоянному анализу угроз.

Модель угроз STRIDE (табл. 1) используется для анализа недостатков и возможных уязвимостей концепции. Для построения структуры исследуемой SDN, в статье использованы стандартные описания [1], [2] и конфигурации сети по умолчанию.

Таблица 1 – Перечень угроз в методологии STRIDE

Угроза	Описание
Спуфинг	Позволяет злоумышленникам скрыть или подделать их личность. Данный тип атак становится возможным ввиду отсутствия надлежащей аутентификации.
Модификация	Позволяет злоумышленникам поставить под угрозу целостность передаваемых или хранимых данных.
Отказ от авторства	Позволяет пользователям в системе отречься от своих действий или обвинить в них других. Системы мониторинга и журналы действий при этом не способны корректно идентифицировать злоумышленника.
Разглашение информации	Эксплуатация этой уязвимости может привести к раскрытию значимой информации или паролей. Она также часто коррелирует с атаками подмены и модификации.
Отказ в обслуживании	Устройства могут подвергаться атаке, которая делает службу или систему временно непригодными для клиентов или пользователей. Этот метод оказывает значительное финансовое влияние и поэтому является одной из наиболее распространенных угроз.
Повышение привилегий	Эта уязвимость часто возникает из-за отсутствия контроля доступа. Простой пользователь или клиент может повысить свои полномочия в системе, что дает им возможность свободного доступа к ограниченным или классифицированным активам.

А. Спуфинг

Несмотря на то, что злоумышленнику приходится использовать для реализации атаки спуфинга в SDN те же методы, что и в обычных сетях, реализация атаки может иметь более негативные последствия. SDN представляет два новых компонента сети - контроллер и приложения. Они имеют корневое значение для безопасности сети и поэтому становятся главной целью атаки. Программируемость и программные интерфейсы потенциально скрывают множество уязвимостей. Кроме того, виртуализация физических сетевых устройств, таких как коммутаторы и контроллер, снижает барьер для атаки.

Традиционные протоколы аутентификации могут служить контрмерой. Однако исследования механизмов безопасности демонстрируют, что их может быть недостаточно для защиты контроллеров и коммутаторов [3]. Важность контроллера в SDN делает спуфинг значительной угрозой, в большей степени, чем в обычных сетях. Даже если предположить, что поток данных в сети защищен, попытки спуфинга все же возможны. Таким образом, в данном анализе спуфинг считается базовой уязвимостью, которая делает возможным эксплуатацию прочих уязвимостей модели STRIDE.

В. Модификация

Атака модификации имеет схожий со спуфингом принцип реализации. Риск несанкционированного доступа при этом не усугубляется, если меры аутентификации осуществляются должным образом и сеть физически защищена. Тем не менее, плоскость управления открывает несколько новых векторов атаки. Логика маршрутизации в SDN не распределена, и коммутаторы зависят от единственного объекта, поддерживающего представление сети. Если база данных маршрутизации скомпрометирована, вся сеть подвергается риску. Контроллер должен правильно идентифицировать модифицированную и конфликтующую информацию так же, как и обнаруживать попытки спуфинга.

С. Отказ от авторства

Угроза отказа от авторства для SDN не имеет существенных отличий, ввиду поддержки основных криптографических протоколов. [1]. Кроме того, контроллер предоставляет возможность централизованного обзора сети, что дает больше возможностей для отслеживания несанкционированных попыток подключения и скрытых устройств [2]. В данном анализе STRIDE проблемы отказа от авторства в Open Flow в основном являются результатом модификации информации или халатной реализации, при которой не реализованы механизмы аутентификации.

D. Раскрытие информации

Сетевые компоненты в SDN предоставляют возможности для сбора данных. Гибкая и программируемая природа сети Open Flow увеличивает риск раскрытия информации, поскольку отдельные устройства могут быть быстро перенастроены для перенаправления трафика по обходным путям. Разница во времени отклика помогает злоумышленникам воссоздавать схему сети без необходимости доступа к какому-либо устройству. В SDN несколько элементов хранят информацию обо всей сети в таблицах потоков и базах данных виртуализации. Эта информация может быть раскрыта с помощью удаленных запросов или получения доступа к серверу. Хотя пользовательские данные могут быть защищены с помощью TLS, базовая SDN не предоставляет достаточных методов для сокрытия информации об общей структуре сети.

E. Отказ в обслуживании

SDN в значительной степени увеличивает риск отказа в обслуживании в сети. Узлы сети лишаются независимости работы в пользу гибкости и простоты настройки. Однако, если контроллер выходит из строя, то вся сеть теряет работоспособность. Программируемый и программно-ориентированный подход вводит новые векторы атак и увеличивает риск ошибок, которые могут привести к сбоям в работе сети. Кроме того, низкая отказоустойчивость системы расширяет спектр возможных атак.

Тем не менее, SDN может предоставить несколько возможностей для динамического смягчения последствий атак отказа в обслуживании. Приложения могут изолировать скомпрометированные хосты, если они будут своевременно выявлены. Трафик можно быстро перенаправить во избежание перегрузок. Датчик пропускной способности Open Flow способен автоматически ограничивать поток входящих данных, что приводит к динамической и быстрой защите уязвимых участков сети. [1] Постоянный и централизованный мониторинг сети контроллера может быстро выявить аномальное поведение. Эти возможности, однако, основаны на предположении, что контроллер использует необходимые защитные инструменты. Open Flow не включает эти возможности по умолчанию. Для обеспечения надежной защиты от атак и масштабируемости необходимо наличие нескольких контроллеров, либо одного распределенного контроллера.

F. Повышение привилегий

На текущем этапе развития SDN существует проблема определения потенциальных рисков в сетях разделяемых сервисов. На сегодняшний день не существует достаточно крупных коммерческих разработок, по которым можно было бы судить об эффективности конкретных проектных решений. Кроме того, пока нет доступных механизмов для совместного использования ресурсов контроллера несколькими пользователями сети. Исходя из этого, можно сделать вывод, что авторизация и политики разграничения доступа являются краеугольным камнем при развертывании крупномасштабной программно-определяемой сети.

2. Предлагаемые меры противодействия основным угрозам в SDN

Анализ угроз по методологии STRIDE демонстрируют, что SDN в сочетании с механизмами защиты обычных сетей нельзя считать безопасной. Традиционные меры безопасности, такие как шифрование, межсетевые экраны или системы обнаружения вторжений (IDS), должны быть адаптированы к дизайну программно-определяемой сети. Таким образом, в данной статье модель STRIDE используется, чтобы наметить реальную архитектуру безопасности, которая объединяет традиционные и специфичные решения защиты. Проект может быть использован для оценки потенциала безопасности будущих SDN, а также для формулирования минимально необходимых требований безопасности для более крупных программно-определяемых сетей.

Для выбора средств и методов, позволяющих снизить риски реализации угроз

безопасности в SDN, была проведена консультация с соответствующей литературой, проанализированы передовые решения в области безопасности, и определены требования и варианты дизайна, которые предусматривают комплексные механизмы защиты сети. Кроме того, приняты во внимание рекомендации ONF, определяющие необходимые средства безопасности для протокола Open Flow [2]. Они включают обязательное использование протоколов безопасности, введение уникальной идентификации и четкое определение границ доверия и безопасности. Таблица 2 суммирует проблемы и решения, определенные в данной статье. В результате в данной работе предлагается модель защищенной сети, использующий принципы, содержащиеся в технической спецификации ONF [1], а также текущие предложения по безопасности.

Первым и абсолютным условием в защищенной системе является использование механизмов аутентификации и проверки целостности для любого узла сети, поскольку этот функционал игнорируется в текущих стандартных разработках. Любой обмен данными между приложениями, контроллерами и коммутаторами должен проходить взаимную аутентификацию, а конфиденциальные сообщения, такие как отчеты о топологии и сообщения о модификации, должны проверяться на целостность. База данных самого контроллера должна быть подписана, чтобы гарантировать использование целостность данных. Канал управления может быть развернут вне сети либо физически, либо виртуально в конфигурациях VLAN.

Для того, чтобы избежать зависимости от одного устройства, в сети должны быть развернуты как минимум два независимых контроллера. Они могут координировать или принимать на себя управление соседними сетями, в случае если один из контроллеров выходит из строя. Подключение коммутаторов к нескольким логически децентрализованным контроллерам может предотвратить негативные последствия в случае компрометации одного из контроллеров. Контроллеры при этом могут обмениваются данными напрямую или косвенно через распределенную сетевую базу данных.

Плоскость управления должна находиться в защищенной зоне, аналогично важным базам данных в обычной сети. Только аутентифицированные хосты, являющиеся частью физически и логически защищенного домена, должны иметь доступ к настройке серверов. Любой трафик, не являющийся сообщением Open Flow, должен фильтруется с помощью встроенных межсетевых экранов.

Удаленные приложения и хосты, пытающиеся получить доступ к серверной зоне, следует проверять на основе местоположения и идентификации с использованием AAA-серверов и алгоритмов управления. Они также должны быть ограничены в правах, наборе действий и доступе к карте сети. Компоненты безопасности и чувствительные к задержке приложения могут быть запущены непосредственно на управляющем сервере, но должны выполняются в отдельном процессе и пространстве памяти. Приложения с более высокими привилегиями должны иметь возможность отменять действия более низкого уровня, а приложения администратора должны обладать полными правами конфигурации.

Управляющие приложения должны отслеживать и протоколировать действия узлов сети и приложений. Поскольку контроллеры являются незаменимыми, они могут быть защищены с помощью систем обнаружения вторжений или межсетевого экрана с хранением состояния. Так, например, для быстрого выявления атак во всей сети коммутаторы могут зеркалировать трафик на серверы обнаружения вторжений. Они сообщают результаты анализа контроллеру, который быстро перенастраивает сеть, чтобы изолировать скомпрометированные участки. Кроме того, контроллер может идентифицировать подозрительное поведение сети на основе шаблонов пакетов. О любых событиях и аномалиях в сети следует сообщать управляющему приложению или системе управления информацией и событиями безопасности (SIEM).

Как правило, рекомендуется блокировать доступ к сети из сетей с более низким уровнем безопасности и разделять сеть на сегменты с различным уровнем защищенности при помощи межсетевых экранов.

Обеспечение бесперебойной работы при установке обновлений безопасности может быть достигнуто при помощи использования технологии Hot Swap [5] или обновления путем замены единичных модулей.

Таблица 2. Угрозы и уязвимости SDN в соответствии с моделью STRIDE

УгрозаSDN	Уязвимость	Возможноерешение
Спуфинг	Возможность аутентифицироваться в качестве контроллера, коммутатора или приложения ввиду отсутствия средств защиты или ошибок в ПО.	Внедрение обязательных процедур аутентификации в рабочих операциях.
Модификация	Злоумышленник может перезаписать политики контроллера. Перехват и модификация управляющих сообщений Open Flow может иметь значительные негативные последствия для конфигурации сети.	Внедрение механизмов контроля доступа и проверки целостности на северном и южном интерфейсах SDN. Важные действия выполняются после верификации несколькими независимыми элементами управления.
Отказ от авторства	Отсутствие мониторинга состояния коммутаторов и управляющего программного обеспечения может открыть возможности для выполнения скрытых операций.	Уникальная идентификация элементов SDN. Механизмы журналирования и отслеживания должны выполняться автоматически и должны быть защищены.
Раскрытие информации	Централизованное хранение информации упрощает сбор данных о структуре сети. Кроме того, компрометация серверного ПО может привести к раскрытию учетных данных и сетевой базы данных.	Перемещение коммуникаций SDN на отдельные защищенные каналы. Контроллер и хранилище данных о состоянии сети при этом должны быть удалены из сети передачи данных.
Отказ в обслуживании	Функциональность коммутаторов зависит от единого контроллера и канала управления, который подвержен множеству возможных атак, таких как флуд, эксплойты, а также ошибки в ПО. Таблицы коммутации при этом ограничены и быстро переполняются.	Развертывание контроллера в сочетании с механизмами обнаружения вторжений; использование механизмов восстановления и избыточности сетевых узлов.
Повышение привилегий	Контроллеры SDN, к которым имеет доступ множество пользователей, в случае компрометации могут раскрыть информацию о соседних сетях. Кроме того, поскольку не существует различий в приоритетах команд приложений, вредоносные клиентские приложения могут взять на себя все полномочия контроллера.	К общим ресурсам должны применяться строгие механизмы контроля доступа на основе ролей, в то время как доверие к операциям клиентов должно быть минимальным. Программное обеспечение должно подвергаться регулярным проверкам во время разработки.

Заключение

Программно-определяемые сети являются развивающейся концепцией для сетей дата-центров и сетей доступа к магистральной инфраструктуре интернета. Поэтому безопасность становится важным аспектом, который в настоящее время рассматривается как научным сообществом, так и производителями оборудования.

Тем не менее, более тщательный анализ безопасности на текущем этапе развития SDN, показывает широкий спектр специфичных для SDN угроз, адекватных мер противодействия которым ещё не выработано. Некоторые из них по своей природе связаны с принципами проектирования SDN, например, контроллеры являются потенциально главными объектами атаки; другие наследуются от базовой инфраструктуры, как, например, подверженность спуфингу. Основываясь на результатах этого анализа, в данной статье определены основные угрозы и предложены решения, позволяющие разработать защищенную архитектуру SDN. Также подчеркнута роль контроля подлинности и целостности для узлов сети и сообщений управляющего протокола, которыми они обмениваются. Ключевым элементом предложенной модели является обеспечение того, чтобы меры безопасности не только предотвращали, но и обнаруживали попытки и успешные атаки на компоненты SDN. Стоит также отметить, что для обеспечения безопасности управляющей связи все еще необходимо полагаться на устоявшиеся традиционные концепции, такие как внеполосное управление

или, по крайней мере, отдельные VLAN управления. Кроме того, решения для противодействия атакам на переполнение таблицы потоков, например, в результате DoS-атак, на сегодняшний день не разработаны.

Список литературы:

1. Техническая спецификация Open Flow Switch Specification 1.5.1, Open Networking Foundation, 2015.
2. Техническая спецификация Threat Analysis for the SDN Architecture 1.0, Open Networking Foundation, 2016.
3. S. Scott-Hayward, S. Natarajan, S. Sezer, A survey of security in software defined networks// IEEE Communications Surveys and Tutorials, 2015, с. 1.
4. J. Francois and O. Festor. Anomaly Traceback using Software Defined Networking // International Workshop on Information Forensics and Security, 2014.
5. L. Vanbever, J. Reich, T. Benson, N. Foster, J. Rexford, HotSwap: Correct and Efficient Controller Upgrades for Software-defined Networks // Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, 2013, с. 133-138.

References:

1. Technical specification:OpenFlow Switch Specification 1.5.1, Open Networking Foundation, 2015.
2. Technical specification: Threat Analysis for the SDN Architecture 1.0, Open Networking Foundation, 2016.
3. S. Scott-Hayward, S. Natarajan, S. Sezer, A survey of security in software defined networks// IEEE Communications Surveys and Tutorials, 2015, с. 1.;
4. J. Francois and O. Festor. Anomaly Traceback using Software Defined Networking // International Workshop on Information Forensics and Security, 2014.
- 5 L. Vanbever, J. Reich, T. Benson, N. Foster, J. Rexford, HotSwap: Correct and Efficient Controller Upgrades for Software-defined Networks // Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, 2013, с. 133-138.

Статья поступила в редколлегию 06.05.19.

Рецензент:

д.т.н., доцент,

*Брянский государственный
технический университет*

Спасенников В.В.

Статья принята к публикации 20.05.19.

Сведения об авторах:

Рытов Михаил Юрьевич

кандидат технических наук, доцент,
заведующий кафедрой «Системы информационной безопасности» Брянского государственного технического университета.
Тел.: +79103300237
E-mail: rmy@tu-bryansk.ru

Калашников Руслан Юрьевич

аспирант кафедры «Системы информационной безопасности» Брянского государственного технического университета.
Тел.: +79206025080
E-mail: human033@gmail.com

Information about authors:

Rytov Mikhail Yurevich

Candidate of Technical Sciences, Associate Professor,
Head of the department
«Information security systems»,
Bryansk state technical university
Phone: +79103300237
E-mail: rmy@tu-bryansk.ru

Kalashnikov Ruslan Yurevich

post-graduate student of the department «Information security systems»,
Bryansk state technical university
Phone: +79206025080
E-mail: human033@gmail.com