портретов пользователей, что вполне достаточно для предотвращения замены пользователя злоумышленником. Это доказывает эффективность данной идеи.

Используя примененную в данной работе модель системы динамической аутентификации пользователя, можно создать гибридную модель, которая будет сочетать в себе статические и циклические методы аутентификации. Таким образом, усовершенствованная система управления доступом будет обеспечивать усиленную, по сравнению с классическими способами, процедуру защиты от несанкционированного доступа.

Э.И. Зигаев

ПРОБЛЕМЫ МАРШРУТИЗАЦИИ В КВАНТОВЫХ СЕТЯХ КАК ТЕХНОЛОГИИ БЕЗОПАСНОГО ОБМЕНА ДАННЫМИ

(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики)

В настоящее время существующие коммерческие решения в области квантовых коммуникаций обладают рядом значительных недостатков. Основные из них, препятствующие массовому распространению такие как: сложность внедрения, стоимость, относительно небольшой объем проведенных исследований в проблемной области. С технической точки зрения так же существуют некоторые затруднения. Одним из недостатков существующих систем квантовых коммуникаций является не способность переключаться на резервные каналы, при обнаружении не легитимного пользователя или при аварийных ситуациях в линии связи. Предложенные в настоящее время методы управления маршрутами в квантовой сети основаны либо на статическом задании пути, либо на протоколе OSPF [1].

Программно-конфигурируемые сети (ПКС) являются одним из приоритетных направлений развития компьютерных сетей. Основой подхода является логическая централизация управления потоками данных и информации о состоянии сети в сочетании с абстрагированием от сетевой инфраструктуры. Одним из важных элементов ПКС является контроллер, на который ложатся функции поддержания актуального состояния сети, конфигурирования оборудования и реализации политик маршрутизации. Все приложения, использующие сетевые возможности, должны взаимодействовать с контроллером, прямой доступ к сетевому оборудованию исключен. Такая архитектура позволяет избавиться от проблем, связанных с использованием сетевых устройств разных производителей, их неполной совместимостью и долгими циклами обновлений фирменного программного обеспечения. Перенос функций оборудования на программное обеспечение (ПО) должен облегчить процесс создания и развертывания новых сервисов, сделать его оперативным и автоматическим. Очевидно, что для решения стоящих перед ним задач контроллер должен иметь интерфейсы взаимодействия с сетевым оборудованием с одной стороны, и с пользо-

вателями и приложениями - с другой. Основным механизмом взаимодействия контроллера и коммутаторов в ПКС в настоящее время является протокол OpenFlow. Его продвижением и стандартизацией занимается международная организация Open Networking Foundation (ONF). OpenFlow предоставляет унифицированный доступ к оборудованию и обладает функциональностью, достаточной для решения стоящих перед ПКС задач. Фактически, он позволяет манипулировать механизмами продвижения пакетов в коммутаторе. ПКС позволяют осуществлять подобное управление наиболее эффективно и в случае необходимости сопряжения различных сегментов квантовых сетей и маршрутизации соответствующих потоков данных, поскольку перенаправление сетевых потоков может быть организовано прозрачным для пользователя образом без необходимости с его стороны внесения изменений в параметры соединения (IP-адресов, портов соединения, VLAN-тэгов и т.п.).

В последние годы основной тенденцией развития компьютерных сетей стал переход к программно-конфигурируемым решениям (Software-Defined Networks, SDN, Программно-Конфигурируемые Сети, ПКС). Формально развитие ПКС находится под контролем международной организации Open Networking Foundation (ONF) [2], однако фактически в сферу ее влияния входит лишь разработка и сопровождение протокола OpenFlow, который в настоящее время является лишь одним из возможных вариантов построения ПКС. Решить задачу маршрутизации в квантовой сети предлагается решить методами программно- конфигурируемых сетей (SDN, ПКС) [https://www.opennetworking.org/sdn-resources/sdn-definition]. Специализированный модуль контроллера после получения сигнала от системы передачи квантовых битовых последовательностей о компрометации соединения или его разрыва будет менять таблицы маршрутизации сетевых пакетов перенаправляя потоки данных через службы кодирования/декодирования использующих другие квантовые крипто-каналы или каналы использующие иные средства шифрования данных (напр. SSL/TLS или SSH). Данное решение сможет использоваться для любых комбинаций аппаратных и программных сетевых коммутаторов поддерживающих спецификацию OpenFlow. Будут использованы спецификации OpenFlow, предоставляющие набор средств для задания механизмов управления потоками данных, способных динамически перестраиваться в зависимости от текущего состояния сетевой инфраструктуры и требований к передаче потоков данных

Причины возникновения подхода ПКС и решаемые им проблемы описывает методический документ ONF [3]. Среди основных задач выделены: обеспечение совместимости, ликвидация зависимости от конкретного производителя сетевого оборудования, повышение масштабируемости существующих архитектур и их адаптация к современным требованиям сетевого взаимодействия, объемам и скоростям передачи данных.

Первая версия протокола OpenFlow появилась в 2008 году. С этого момента до настоящего времени было опубликовано 20 новых версий, вплоть до текущей 1.5.1 [4]. С одной стороны это говорит об интенсивном развитии и ин-

тересе к данному протоколу, но даже с учетом того, что не все отличия носили принципиальный характер, такое частое обновление затрудняло процесс внедрения, особенно на уровне аппаратной поддержки в сетевых коммутаторах. Необходимо отметить, что механизм выбора конкретной версии протокола для взаимодействия контроллера и коммутатора появился лишь в 2012 году в версии 1.3.1, что наряду с внедрением расширяемых структур данных в формате TLV (Type-Length-Value, Тип-Длина-Значение) позволило улучшить ситуацию с совместимостью оборудования.

Регулярное появление новых спецификаций было обусловлено тем, что первые редакции протокола были ориентированы на академические исследования и не отражали требований, предъявляемых к коммутаторам компьютерных сетей, которые должны обеспечить корректную обработку произвольного трафика. Показательным является тот факт, что протокол OpenFlow не предусматривает механизмов конфигурирования сетевого оборудования. Для исправления ситуации ONF пришлось разрабатывать параллельное семейство протоколов OF-CONFIG [5]. Протокол OpenFlow предполагает интенсивный опрос коммутатора со стороны контроллера, механизмы асинхронной нотификации об изменении состояния недостаточны. Очевидно, что в условиях реальной сети, когда один контроллер управляет как минимум десятками коммутаторов, такое решение не может обеспечить достаточной эффективности. Кроме этого, архитектура современных коммутаторов такова, что основные ресурсы сосредоточены в плоскости передачи данных. Коммуникационные интерфейсы не обеспечивают достаточной производительности. Переход к асинхронным нотификациям привел к необходимости разработки дополнительного механизма взаимодействия контроллера и коммутатора [6], внедрение которого только начинается. Расширения существующей спецификации необходимы и для организации эффективного взаимодействия с оптоволоконными сетями, широко использующими коммутацию каналов [7]. Без такого взаимодействия внедрение ПКС будет сильно ограничено. Нельзя не отметить, что аппаратная реализация OpenFlow сложна, и современное поколение коммутаторов не было предназначено для таких протоколов и в данный момент пока находится на стадии лабораторных испытаний. Так же, стоить отметить большие перспективы развития данной технологии.

Литература

1. Peev M. The SECOQC quantum key distribution network in Vienna [Текст] /M. Peev, C. Pacher, R. All´eaume, C. Barreiro et al // New J. Phys. – 2009. – V.11. – P.075001.

2. Open Networking Foundation [Электронный ресурс] - Режим доступа: https://www.opennetworking.org (дата обращения: 15.12.2015)

3. Open Networking Foundation White Paper Software-Defined Networking: The New Norm for Networks [Электронный ресурс] - Режим доступа: https://www.opennetworking.org/images/stories/downloads/sdn-resources/ white-papers/wp-sdn-newnorm.pdf (дата обращения: 22.11.2015))

4. ONF TS-025 OpenFlow Switch Specification Version 1.5.1 / Open Networking Foundation - 2015

5. ONF TS-016 OF-CONFIG 1.2 OpenFlow Management and Configuration Protocol / Open Networking Foundation - 2014

6. ONF TS-014 OpenFlow Notifications Framework OpenFlow Management Version 1.0 / Open Networking Foundation - 2013

7. ONF TS-022 Optical Transport Protocol Extensions Version 1.0 March 15,2015 / Open Networking Foundation - 2015

А.С. Кирьянцев, И.А. Стефанова

АЛГОРИТМ ДИНАМИЧЕСКОЙ ГЕНЕРАЦИИ КЛЮЧЕЙ И ПОДПИСЕЙ В ПРИЛОЖЕНИИ CRYP2CHAT

(Поволжский государственный университет телекоммуникаций и информатики)

Современное общество характеризуется интенсивным обменом, накоплением информации в электронном виде и её обработкой в компьютерных сетях, что требует оперативного решения постоянно возникающих проблем защиты информационного содержания и информационной безопасности.

Данная тема является весьма актуальной и подогрета заявлениями и публикациями технического специалиста, бывшего сотрудника ЦРУ Э. Сноудена, о том, что агентство национальной безопасности (АНБ) США ведёт нечестную игру в направлении прослушивания граждан по всему миру при помощи существующих информационных сетей и сетей связи.

Для обмена сообщений в реальном времени существуют программы – мессенджеры, которые могут применяться для передачи текстовых сообщений, звуковых сигналов, картинок, видео, игр, а так же для организации телеконференций путем шифрования сообщений пользователей сети. Обычно мессенджеры работают совместно с сервером и являются клиентскими программами со своими правилами работы и особенностями КУ ним можно отнести, например, программы ICQ, Skype. Основной недостаток этих программ заключается в том, что они оставляют метаданные на центральном сервере в незашифрованном виде, что позволяет, при необходимости, узнать информацию о самих абонентах, времени их общения, количестве сообщений в обычной сессии. Для устранения этого недостатка разработана программная реализация шифрования данных, на клиентской стороне с помощью приложения Cryp2Chat.

В интернет мессенджерах отсутствуют таки функции как:

– проверка наличия MITM (Men in the middle) – атаки,
– наличие «чистого» (без данных) сервера,
– самоуничтожение сообщения после закрытия сессии.

MITM-атака является самым распространенным способом атаки для кражи данных пользователя, когда атакующий способен читать и видоизменять по