9. Duc N.M. Your face is not your password , 2009. – 16c.

10. Liveness detection method Liveness detection method and apparatus of video image : пат. 8355530 США / detection method Liveness – 2013.

11. Maatta J. Face spoofing detection from single images using micro-texture analysis , 2011.

12. Methods for performing Methods for performing biometric recognition of a human eye and corroboration of same : пат. 8260008 США // – 2012.

13. REKHA P.S. Spoofing Face Recognition Using Neural Network with 3D Mask / P. S. REKHA // Int. J. Emerg. Technol. Comput. Sci. Electron. – 2015. – Т. 14 – № 1 – 123–127c.

14. Secure biometric authentication Secure biometric authentication from an insecure device: заяв. пат. 12/960,511 США / biometric authentication Secure – 2010.

15. Yang J. Face liveness detection with component dependent descriptor , 2013. – 1–6c.

В.А. Заступов, М.В. Кузнецов

ЦИКЛИЧЕСКАЯ АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ТРАДИЦИОННЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

(Поволжский государственный университет
телекоммуникаций и информатики)

Мы живем в информационном веке. Ежедневно взаимодействуем с электронными устройствами, храним свои данные на информационных носителях и в памяти компьютера, используем интернет ресурсы для работы и проведения досуга. В наше время, вопрос о защите информации является одним из основных практически в любой сфере деятельности.

На данный момент существует множество методов защиты системы от несанкционированного доступа. Из них можно выделить стандартные (ввод логина/пароля, ответ на секретный вопрос, ввод пин-кода) и более сложные системы защиты, построенные на использовании уникального предмета (электронный ключ, магнитная карта и т.д.).

Данные методы имеют недостатки, главным из которых является то, что в случае, когда злоумышленнику удается заполучить необходимую информацию для проникновения в систему (будь то пароль или материальный атрибут) происходит имитация санкционированного доступа и все ресурсы автоматически становятся доступны для использования. Именно решение этой проблемы и стоит в основе данной работы.

Все мы слышали фразу о том, что каждый человек уникален. На этом факте были созданы биометрические системы защиты такие как: сканирование сетчатки глаза, отпечатков пальцев, формы лица и т.д. Все эти системы представляют собой дорогостоящие устройства и в большинстве своем имеют одношаговый этап аутентификации. Циклическая аутентификация на основе традиционных действий пользователя – это метод, не прекращающий действие на протяжении всего взаимодействия пользователя с персональным компьютером, прост и дёшев в реализации, имеет возможность работать в скрытном режиме (незаметно для пользователя). Также важной особенностью является то, что данная идея позволяет аутентифицировать пользователя при работе с интернет ресурсами.

Принцип работы циклической аутентификации состоит из трёх этапов:

1) Этап обучения. При работе с персональным компьютером мы часто сталкиваемся с действиями, которые можно выполнить различными способами (переключение языка, работа с буфером обмена, сохранение документа и т.д.). Каждый пользователь выполняет все эти действия, исходя из своих привычек, выработанных за время работы с ПК. Задачей этапа обучения является фиксация таких действий и способов их выполнения. Данный этап выполняется при помощи программного обеспечения «Кейлогер», позволяющее осуществлять контроль над деятельностью пользователя персонального компьютера, фиксировать действия мышью, набор горячих клавиш. По истечению времени обучения, формируется лог-файл.

2) Этап формирования портрета пользователя. Имеющийся лог-файл зашифровывается и отправляется на удаленный сервер безопасности. По прибытии файл расшифровывается, производится анализ данных, нахождение закономерностей, выявление особенностей и, в итоге, формирование индивидуального портрета пользователя - эталон. Необходимо отметить, что после продолжительного времени работы с такой системой необходимо вносить изменения в эталонные характеристики, поскольку «привычки» со временем имеют свойство меняться.

3) Этап аутентификации. На данном этапе происходит непосредственно сравнение действий пользователя с эталоном в реальном времени при работе за ПК. В случае, когда процент несоответствий превышает заданный порог доверия, система автоматически отключается и на сервер безопасности отправляется сигнал о несанкционированном доступе.

Для доказательства эффективности данного метода было произведено анкетирование среди постоянных пользователей ПК. Опрашиваемому предлагался список действий и методы его выполнения, из которых он должен был выбрать тот, каким наиболее часто пользуется.

Всего было предоставлено 44 действия и на каждое действие минимум 4 варианта ответа. Также был отдельно произведен опрос касательно сочетания правого и левого Shift-ов с той или иной клавишей на клавиатуре. Участие приняло свыше 80-ти человек.

Проанализировав полученные результаты, было установлено, что самое ближайшее совпадение между традиционными действиями двух пользователей составило 80%, среднее число совпадений составило 46%, минимальное совпадение между двумя пользователями составило 16%. С учетом максимального совпадения в 80% мы имеем 20-ти процентное несоответствие индивидуальных

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-