УДК 004.056.5

АНАЛИЗ СПОСОБОВ ЗАЩИТЫ МЕЖСЕТЕВЫХ ЭКРАНОВ С МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИЕЙ

П.В. Чарикова, И.В. Лофицкий
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Решение задачи обеспечения информационной безопасности на всех предприятиях является важной задачей. Современный подход к созданию защищенной от внешних угроз информационной системы предполагает совокупность отдельных мер и решений. Важнейшим элементом данной системы является технические решения с использованием специальных систем и средств защиты.

Одним из вариантов реализации данного решения является использование аппаратного межсетевого экрана, обладающим рядом таких преимуществ, как обеспечение необходимой производительности, простоты в установке и использовании, обеспечением дополнительной защиты от несанкционированного доступа.

Дополнительная защита межсетевого экрана заключается в том, что только пользователь, который прошёл процедуру аутентификации, имеет право воспользоваться сервисом устройства. Самой простой и распространенной схемой является однофакторная аутентификация. Обычно это использование логина и пароля. Данный способ аутентификации является не очень надежным, так как весьма просто подобрать используемый пароль.

Более надежными схемами являются двухфакторные или многофакторные аутентификации. В двухфакторной аутентификации (2FA) от пользователя необходимо представление факторов двух разных категорий: фактор владения и фактор знания. Многофакторная аутентификация (MFA) шире, чем двухфакторная аутентификация. Она требует использование двух или более факторов в процессе аутентификации.

Несмотря на распространенное внедрение многофакторной аутентификации, возникает проблема практик парольной политики, которые препятствуют эффективному управлению для достижения современных стандартов информационной безопасности и технической защиты информации. Примером может быть инцидент, связанный с утечкой конфиденциальной информации через возможности подготовки внутреннего нарушителя. Анализ данного инцидента представлен в интервью от 29 июня 2020 года ТАСС «Первые лица бизнеса». Там одной из кардинальных мер было представлено резкое сокращение числа администраторов, которые имеют доступ к конфиденциальной клиентской информации [1].

Для исключения подобных ситуаций используется введение строгой многофакторной аутентификации, которая подразумевает использование двух факторов аутентификации различных типов. Первым фактором может быть наличие аппаратного токена, например USB-токена или смарт-карты, вторым – PIN-код, который необходим для совершения криптографических операций.

Также существуют другие типы технологий многофакторной аутентификации. Например, биометрическая, мобильная или внеполосная аутентификации.

Биометрическая аутентификация обычно из себя представляет сканирование сетчатки глаза, считывание отпечатков пальцев, сканирование геометрии рук. Данные способы обеспечивают высокий уровень аутентификации, и их гораздо труднее скомпрометировать. Так как они являются инвазивными, а также их сложнее собрать. Это может считаться самой надежной формой аутентификации, в настоящее время она используется реже всего [2].

Не всегда наборы биометрических характеристик пользователей совпадают на 100% с данными, которые внесены в считывающее устройство. Поэтому идентичности невозможно добиться даже для двух показателей биометрии. Это происходит по причине механических повреждений на коже. Также воздействие на изменение биометрических данных влияет возраст. Кроме этого, присутствует вероятность ложного опознавания, если в базу внесено большое количество пользователей.

Более распространенным способом повышения безопасности является использование мобильной и внеполосной аутентификации. Для первой используют одноразовые SMS-пароли [3]. Использование таких паролей имеют более низкий, по сравнению с аппаратными токенами, уровень защиты, так как сети сотовых операторов слабо защищены. Это повышает риск перехвата сообщения. Более защищенным методом получения одноразового пароля является внеполосная аутентификация. Основная идея которой заключается в использовании беспроводной сети. Данный тип аутентификации может быть эффективным, если мошенники не получили доступ к самой системы мобильного телефона пользователя. Но опять, это только временная защита, если субъект смог перехватывать связь пользователя по мобильному телефону, то сможет и преодолеть протоколы безопасности внеполосной аутентификации.

Использование аппаратных токенов устраняет возможность перехвата пароля, но требует установки драйверов, специальных плагинов, что создает сложности для обычных пользователей. Но использование стандартного компьютерного интерфейса облегчает его использование. Также к минусам можно отнести высокую стоимость криптографических токенов [4].

Плюсом является простота использования аппаратного токена. Это небольшое устройство, которое владелец использует для процесса аутентификации. Зачастую реализуется в виде USB-ключа. Данный метод

защиты является наиболее надежным, так как может поддерживать строгую аутентификацию с использованием одноразовых паролей.

Все средства безопасности имеют свои недостатки, так и многофакторная аутентификация не является идеальной. Однако является более безопасной, чем традиционные механизмы защиты.

Список использованных источников

1. Герман Греф: я – игрок в долгую. 29 июня 2020 г. [Электронный ресурс]. – Режим доступа: https://tass.ru/business-officials/8827375 (дата обращения: 22.02.2023)

2. Чужиков, Н. О. Многофакторная аутентификация / Н. О. Чужиков. — Текст: непосредственный // Молодой ученый. — 2022. — № 21 (416). — С. 226-228. — URL: https://moluch.ru/archive/416/92149/ (дата обращения: 07.03.2023).

3. Статистика основных угроз безопасности в сетях ss7 мобильной связи. [Электронный ресурс] – URL: https://www.ptsecurity.com/upload/ptru/analytics/SS7-Vulnerability-2016-rus.pdf (дата обращения: 24.02.2023).

4. Галимов, Р.Р. Программно-аппаратные средства защиты информации в вычислительных системах: учебное пособие/ Р.Р. Галимов, А.А. Рычкова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2017. – 132 с.

Чарикова Полина Вячеславовна, студент гр. 6271-110401D, charikova99@gmail.com.
Лофицкий Игорь Вадимович, к.т.н., доцент каф. радиотехники, ivl60@mail.ru.

УДК 004.056.5

РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ АППАРАТНОГО ТОКЕНА НА БАЗЕ СЕМЕЙСТВА МИКРОКОНТРОЛЛЕРОВ STM32

П.В. Чарикова, И.В. Лофицкий
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Устройства, которые используются в системах безопасности, например, аппаратные токены, являются достаточно сложными системами, у которых развита внутренняя архитектура, и они имеют широкий спектр функций. Такие устройства должны отвечать жестким требованиям безопасности, так как от их корректной работы зависит правильность выполнения производственных процессов и т.д.

Главной составляющей таких устройств являются микроконтроллеры. Следовательно, микроконтроллеры становятся основной целью атаки злоумышленников. Основной проблематикой криптографической защиты на микроконтроллерах заключается в том, что, например, при использовании для защиты передачи данных секретный ключ, который хранится в памяти