производительность устройство и на время его работы. В качестве альтернативы, можно предложить использовать магнитный чип, подобный тому, что установлен в пластиковых картах и проездных, выступающий в качестве посредника. NFC-модуль пациента записывает на чип номер пациента, по которому можно получить информацию. Затем модуль NFC на устройстве пациента можно отключить, т.к. теперь необходимые данные есть на чипе. После этого, при необходимости фельдшер сможет получить данные с чипа вне зависимости от состояния телефона.

УДК 004.056.55

Студ. П.П. Позняк
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

СКВОЗНОЕ ШИФРОВАНИЕ ИЛИ END-TO-END ENCRYPTION (E2EE) В МЕССЕНДЖЕРАХ

Современные технологии связи позволяют людям общаться мгновенно, независимо от расстояния и времени. Однако, при этом, возникает вопрос безопасности передачи информации [1, 2]. Одним из методов защиты данных является сквозное шифрование (СШ), которое позволяет защитить сообщения, передаваемые через мессенджер, от доступа третьих сторон. В данном исследовании мы рассмотрим, почему мессенджеры, использующие СШ, являются более защищенными, чем те, что не используют его.

Для понимания того, как работает данный метод, необходимо прояснить, что он из себя представляет. СШ, или end-to-endencryption – это технология шифрования, которая позволяет зашифровать сообщения перед отправкой, таким образом, что только отправитель и получатель могут их прочитать [3].

Как работает СШ на примере двух пользователей А и Б? Пользователь Б хочет поздороваться с А конфиденциальным сообщением. Расшифровать его может только закрытый ключ А. Открытый ключ может быть передан кому угодно, но закрытый ключ предназначен только для А.

Сначала Б использует открытый ключ А для шифрования сообщения и преобразует сообщение «Привет А от Б!» в закодированный текст, буквы которого кажутся бессмысленными и случайными. Б отправляет это зашифрованное сообщение через общедоступный Интернет. Это сообщение может проходить через несколько серверов, включая серверы почтовых провайдеров и серверы интернет-провайдеров.

Эти компании могут захотеть прочитать это сообщение и даже поделиться им с третьими лицами. Но преобразовать зашифрованный текст в простой текст невозможно. Это может сделать только пользователь А, когда сообщение достигает его папки «Входящие», потому что только А имеет доступ к своему закрытому ключу. Когда Ахочет ответить Б, он просто повторяет процесс, и его сообщение зашифровывается с использованием открытого ключа Б.Данный метод позволяет избежать таких угроз, как прослушивание и перехват сообщений, небезопасное хранение сообщений на серверах мессенджера, возможность перехвата метаданных, внедрение вредоносного кода.

Таким образом, видно, что ключевым отличием СШ от простой пересылки сообщений является высокий уровень безопасности, так как при простой пересылке сообщение передается через сервер провайдера мессенджера и хранится на этом сервере. При этом провайдер мессенджера может иметь доступ к содержанию сообщения и может использовать его для различных целей.

Есть ряд приложений, которые имеют СШ в качестве опции, либо включены по умолчанию. После опроса ряда пользователей, было выявлено, что большинство считают свои данные защищенными и доверяют таким мессенджерам, как WhatsApp, Telegram, iMassage, которые как раз и являются примерами приложений, использующих СШ. К не менее известным мессенджерам, использующим данную технологию, также относятся Signal, Threema, Wire, GoogleMessage.

После выявления достоинствСШ, может возникнуть предположение, что оно непобедимо. Тем не менее, помимо криптографии, следует помнить и о других вещах. Его может легко обойти, например, тот, кто имеет доступ к вашему телефону и знает ваш пароль. Люди, ставшие жертвами фишинговых атак, также уязвимы, независимо от того, сколько их приложений используют сквозное шифрование.

СШ также не защитит вас от недобросовестных разработчиков. Компания может заявить, что обеспечивает сквозное шифрование, но, возможно, внедрила его неправильно или добавила лазейку, позволяющую посторонним читать ваши сообщения. В конечном счете, вы должны быть в состоянии доверять разработчику приложения, чтобы сквозное шифрование было вообще полезным.

Таким образом, в ходе исследования было установлено, что сквозное шифрование хоть и является одним из важных инструментов обеспечения безопасности современных коммуникационных систем, но не гарантирует абсолютной конфиденциальности в обмене информацией.

ЛИТЕРАТУРА

1. Урбанович, П. П. Компьютерные сети и сетевые технологии: учебное пособие / П. П. Урбанович, Д. М. Романенко. – Минск: БГТУ, 2022. – 606 с.
2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ. – Минск: БГТУ, 2016. – 220 с.
3. Moyer F. What is end-to-end encryption?[Электронный ресурс]. – 2022. – Режим доступа: http://bp21.org.by/ru/art/a041031.html. – Дата доступа: 02.04.2023.

УДК 004.491.22

Студ. А.Д. Мозолевский, М.Л. Дащинский
Науч. рук. проф. П. П. Урбанович
(каф. информационных систем и технологий, БГТУ)

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ И МОДЕЛИ ОБНАРУЖЕНИЯ ТРОЯНСКИХ ПРОГРАММ REMOTE ACCESS TROJAN

Троянские программы Remote Access Trojan (RAT) – это вид вредоносного ПО, который может получить удаленный доступ к зараженному устройству без согласия его владельца [1]. RAT-программы могут быть использованы для кражи личной информации, включая пароли, банковские данные и другие конфиденциальные данные [2]. Заражение троянской программой RAT может происходить по разным каналам. Одним из распространенных способов заражения RAT является установка программного обеспечения, содержащего в себе RAT.

Для обнаружения RAT существует несколько подходов. Один из наиболее распространенных – это сигнатурная модель [3]. Этот метод использует базу данных сигнатур, которые определяют уникальные характеристики RAT-программ. Поведенческая модель использует набор поведенческих характеристик, которые определяют вредоносное поведение RAT на зараженном устройстве: изменения файловой системы или сетевой активности могут указывать на наличие RAT-программы. Модель машинного обучения использует алгоритмы, которые могут обучаться на большом количестве данных, чтобы распознавать и обнаруживать RAT-программы на зараженных устройствах [4]. Аномальный метод обнаружения использует анализ необычных паттернов в данных. Например, если RAT-программа пытается изменить системные файлы, это может быть необычным событием, и метод аномального обнаружения может сработать.