Несмотря на все вышеперечисленные методы аутентификации, существует комбинированная (мультимодальная) биометрическая система. Она позволяет соединить несколько типов биометрических технологий в системах аутентификации в одной. Комбинированные системы являются более надёжными с точки зрения возможности имитации биометрических данных человека.

Не существует идеального биометрического метода. Все биометрические методы имеют соответствующие преимущества и недостатки. Однако, некоторые биометрические методы более удобны, чем другие в определённых случаях.

Наиболее важными характеристиками метода идентификации являются:

- защищённость биометрического метода;
- доступность для пользователя;стоимость;
- простота использования.

Литература

1. Лакин Г.Ф. Биометрия: Учеб. пособие для биол. спец. вузов.2013г. – [Электронный ресурс]. – Дата доступа – 25.03.2019 г.

2. Тихонов В А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Уч. пособие. М.: Гелиос АРВ, 2006. – [Электронный ресурс]. – Дата доступа – 25.03.2019г.

Маскировка IP-адреса. Использование специализированных программ и серверов

Пронько М. В.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

IP-адреса – это глобальные адреса, используемые в системе протоколов TCP/IP для уникальной идентификации компьютеров в сети Интернет.

Каждое устройство, подключённое к сети Интернет имеет свой уникальный IP-адрес. Если устройство подключено через маршрутизатор или шлюз, то оно имеет адрес этого маршрутизатора или шлюза.

На данный момент, наиболее распространёнными версиями протокола IP являются:

1. IPv4 (далее просто IP) –первая широко используемая версия интернет-протокола, которая была описана в информационных документах Интернета в сентябре 1981 года. Использует 32-битные адреса. Традиционная форма записи – четыре десятичных числа (от 0 до 255), разделённых точками.

2. IPv6 – новая версия интернет-протокола, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4). Создан в 1996 году.

Адреса узлов в сети, согласно протоколу IPv4 имеют длину 32 бит, что даёт в совокупности 232 = 4 294 967 296 возможных адресов. Но не все адреса используются для глобального пространства (Интернет), часть адресов выделяется для специальных нужд, например, для организации локальных сетей, виртуальных сетевых интерфейсов, используются в тестовых целях, являются специальными адресами и так далее.

IPv4 адреса как правило записываются в виде четырёх десятичных чисел от 0 до 255 разделённых символом "**.**" (точка), например, минимальный возможный адрес – 0.0.0.0, максимальный – 255.255.255.255. Число от 0 до 255, как правило, в компьютерных системах требует для хранения 1 байт или 8 бит информации, таким образом 8 * 4 = 32 бита или 4 байта, что соответствует заявленной длине адреса.

IP-адрес называют *статическим* (постоянным, неизменяемым), если он назначается пользователем в настройках устройства.

IP-адрес называют *динамическим* (непостоянным, изменяемым), если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, указанного в сервисе назначавшего IP-адрес (DHCP).

Использование определения «маскировка IP-адреса» является не совсем корректным, т.к. любой компьютер, подключённый к сети, будет иметь свой идентификатор. Чаще всего, вместо данного определения, идёт речь об изменении IP-адреса для каких-либо целей.

Причины для смены IP-адреса:

1. Они часто привязаны к географическому положению. Многие люди не хотят, чтобы информация о их местоположении стала известна без их ведома. Также, некоторый контент в Интернете может быть недоступен в какой-либо стране, следовательно – можно изменить IP-адрес для его просмотра.

2. Защита личной информации. По IP-адресу, присваемому каждому устройству в сети Интернет, можно идентифицировать это устройство и его владельца. Поэтому, некоторые веб-сайты, сервисы или приложения, имея соответствующие технические возможности, могут связать те или иные действия в Интернете с конкретным человеком. Но не все люди

любят, когда информация о том, какие сайты он или она посещает, с кем разговаривает, что загружает, становится известной третьим лицам.

Веб-сайты, приложения и сервисы могут даже не знать, что IP-адрес пользовательского компьютера был скрыт или изменён. Для них человек, просматривающий веб-сайт, – просто анонимный пользователь Интернета.

Существует определённый спектр способов смены IP-адреса:VPN (VirtualPrivateNetwork), Proxy, SOCKS, Tor (TheOnionRouter), SSH-туннелинг (SecureShell), JAP и другие.

Рассмотрим каждый из них:

VPN. VPN-соединение похоже на обычную локальную сеть, приложения не заметят изменений в сети. Но, когда одно из них обратится к удалённому ресурсу, компьютер создаст специальный GRE-пакет (GenericRoutingEncapsulation – общая инкапсуляция маршрутов), который и будет отправлен VPN-серверу. Сервер расшифрует пакет, выяснит его суть (доступ к Web-странице, просто передача данных и т.д.) и выполнит это действие со своего IP. Затем, получив ответ, VPN-сервер поместит его в GRE-пакет, зашифрует и в этом виде отправит обратно клиенту. Чаще всего, VPN-клиент встроен в какой-либо сайт, либо существует в виде расширения для браузера. Наиболее распространённым является мультиплатформенное приложение HolaVPN.

HTTP-прокси. Это самый распространённый вид прокси. Принцип работы заключается в том, что программа или браузер посылает запрос прокси-серверу на открытие определённого URL ресурса. Прокси-сервер получает данные с запрашиваемого ресурса и отдаёт эти данные вашему браузеру.

Socks. Сетевой протокол, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер прозрачно (незаметно для них) и таким образом использовать сервисы за межсетевыми экранами (фаерволами). Более поздняя версия SOCKS5 предполагает аутентификацию, так что только авторизованные пользователи получают доступ к серверу. Использование Socks протокола активируется путём изменения настроек браузер.

Tor. Так называемая «луковая (многослойная) маршрутизация». Система (встречающаяся в виде интернет-браузера), позволяет пользователям соединяться анонимно, обеспечивая передачу пользовательских данных в зашифрованном виде. С помощью Tor пользователи могут сохранять анонимность при посещении web-сайтов, публикации материалов, отправке сообщений и работе с другими приложениями, использующими протокол TCP. Безопасность трафика обеспечивается за счёт использования распределённой сети серверов, называемых «многослойными маршрутизаторами» (onionrouters).

Принцип работы Tor похож на алгоритм передачи данных в VPN. Информация, связанная с запросом, помещается в зашифрованные пакеты. Затем, Tor убирает всю информацию, которая может использоваться для идентификации пользователя. После этого, Tor шифрует всю остальную информацию и все данные пересылаются через множество произвольных серверов. Каждый из серверов просматривает только ту информацию, которая необходима для определения отправителя и дальнейшего пути отправки этого пакета, таким образом обеспечивается анонимность.

SSH-туннелинг. Сетевой протокол, позволяющий производить удалённое управление компьютером и передачу файлов.Использует алгоритмы шифрования передаваемой информации. Данный тип маскировки IP-адреса представлен в виде сторонней программы.

SSH-туннелинг можно рассмотреть в качестве дешёвой замены VPN. При пересылке через SSH-туннель незашифрованный трафик любого протокола шифруется на одном конце SSH-соединения и расшифровывается на другом.

Литература

1. Информационная безопасность в таможенных органах : учебно-методическое пособие для студентов специальности 1-96 01 01 «Таможенное дело» / Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель. – Минск: БНТУ, 2019. – 118 с.
2. Способы сокрытия IP-адреса в сети Internet [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/72820/. – Дата доступа: 27.03.2019.
3. Wikipedia – свободная энциклопедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/. – Дата доступа: 24.03.2019.

Компьютерная стенография и её применение

Алданова Е.А.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

Задача надёжной защиты информации от несанкционированного доступа является одной из древнейших и не решённых до настоящего времени проблем. Способы и методы скрытия секретных сообщений известны с давних времён.

В дальнейшем для защиты информации стали использоваться более эффективные методы кодирования и криптографии. От криптографии стенография отличается тем, что с помощью криптографии можно скрыть