## Виды шифрования

Есть два основных типа шифрования: симметричное и асимметричное. Главное отличие между ними заключается в применении ключей.

В симметричном шифровании используется один ключ для шифрования и дешифрования данных. Такой ключ должен быть установлен на устройствах обоих собеседников.


Асимметричное шифрование (шифрование с открытым ключом) применяет два ключа. Один из этих ключей является частным, второй открытым. Частный ключ располагается на вашем устройстве, а открытый ключ устройство отправляет на другое устройство, с которым вы будете связываться.


Принимающее устройство тоже требует собственного частного ключа для декодирования зашифрованных данных.

Часто используется сквозное шифрование, это способ передачи данных, в котором только пользователи, участвующие в общении, имеют доступ к сообщениям.

Рассмотрим самые популярные протоколы передачи данных:

HTTP

Протокол работает в формате запрос-ответ с двумя участниками общения:

клиент — формирует запросы и обрабатывает ответы;

сервер — обрабатывает запросы и формирует ответы.

HTTPS

HTTPS – это защищенный протокол передачи гипертекста (Hyper Text Transfer Protocol Secure). Для коммуникации данных используется 443-й порт.

HTTP и HTTPS предназначены для передачи данных и в итоге пользователи могут просматривать веб-страницы. HTTPS — это не отдельный протокол, а расширение HTTP, он безопаснее, так как использует SSL (Secure Sockets Layer) / TLS (Transport Layer Security) для шифрования обычных запросов и ответов.

HTTPS выполняет авторизацию вашего подключения, запрашивая сертификат цифрового или публичного ключа, который должен быть подписан доверенным третьим лицом.

Поясним некоторые термины выше:

SSL (Secure Sockets Layer — уровень защищённых сокетов) — это протокол шифрования, который позволяет кодировать данные для более безопасного обмена. Сертификат обеспечивает зашифрованное соединение между человеком и используемым сайтом.

TLS (Transport Layer Security - безопасность транспортного уровня) - криптографический протокол для более безопасной передачи информации на основе протокола SSL. TLS использует асимметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Также есть протокол SSH:

SSH (Secure SHell - защищенная оболочка) — сетевой протокол, предназначенный для безопасного удаленного доступа к UNIX-системам. Данный протокол эффективен тем, что шифрует всю передаваемую информацию по сети. По умолчанию, используется 22-й порт. В основном он нужен для удаленного управления данными пользователя на сервере, запуска служебных команд, работы в консольном режиме с базами данных.

Есть несколько вариантов, с помощью которых можно защитить данные:

1. Шифрованная файловая система (Encrypting file system)

Шифрованная файловая применяется для защиты файлов от злоумышленников, которые могут получить физический доступ к носителю информации.
Для обеспечения конфиденциальности данных в процессе шифрования применяется открытый ключ пользователя. Посторонние не смогут расшифровать информацию без соответствующего закрытого ключа. Для каждого зашифрованного файла создается специальный восстанавливающий ключ — его использует компетентный администратор в экстренных ситуациях, например в случае отсутствия сотрудника или при потере закрытого ключа.

2. Шифрование базы данных

Одним из примеров шифрования на уровне базы данных является шифрование на уровне столбцов (Column-Level Encryption), которое записывает в базу данных уже зашифрованные данные, а сама база данных без дальнейшего шифрования записывается в хранилище. Особенностью шифрования на уровне столбцов является использование единого ключа при обработке данных одного столбца. Ключи могут быть назначены пользователям и защищены паролем для предотвращения автоматической расшифровки.

3. Защита доступа к сети (например, приватный доступ к локальной сети)

Меры безопасности:

Защитные методы делятся на четыре группы:
- организационные;
- технические или аппаратные;
- программные;
- аппаратно-программные.

Основные барьеры для злоумышленников:
- физическое препятствие, исключающее возможность соприкосновения третьего лица с элементами сети;
- система контроля и управления доступом, регламентирующая уровни прав пользователей;
- использование криптографических средств защиты информации (шифрование данных);
- регламентация действий персонала;
- принятие мер дисциплинарного, гражданско-правового и даже уголовно-правового воздействия в целях защиты конфиденциальной информации.

4. Шифрующее программное обеспечение

Это программное обеспечение, основной задачей которого является шифрование и дешифрование данных, как правило, в виде файлов, жестких дисков и сменных

носителей, сообщений электронной почты или в виде пакетов, передаваемых через компьютерные сети. Шифрующее программное обеспечение выполняет алгоритм, который предназначен для шифрования данных компьютера таким образом, что они не могут быть восстановлены без ключа.

5. Аутентификация (идентификация конкретного пользователя, как «безопасного») с последующей авторизацией (получена информация, что пользователь «безопасный», теперь необходимо идентифицировать, кто это именно) пользователей.
Есть несколько способов авторизовать пользователя, например:

Базовая http авторизация (Basic access authentication)
В контексте протокола HTTP базовая аутентификация доступа – это метод, с помощью которого агент пользователя HTTP предоставляет имя пользователя и пароль при отправке запроса. При базовой аутентификации HTTP запрос содержит поле заголовка в форме, где учетные данные — это кодировка идентификатора и пароля Base64 (стандарт кодирования двоичных данных при помощи только 64 символов ASCII), соединенных одним двоеточием

JSON Web Token (Токен доступа)
Это открытый стандарт для создания токенов доступа, основанный на формате JSON. Как правило, используется для передачи данных для аутентификации в клиент-серверных приложениях. Токены создаются сервером, подписываются секретным ключом и передаются клиенту, который в дальнейшем использует данный токен для подтверждения подлинности аккаунта.

OAuth
Открытый протокол авторизации, обеспечивающий предоставление третьей стороне ограниченного доступа к защищённым ресурсам пользователя без передачи ей (третьей стороне) логина и пароля. Ключевая особенность применения OAuth заключается в том, что, если пользователь имеет хорошо защищённый аккаунт, то с его помощью и технологии OAuth он может пройти аутентификацию на других сервисах, при этом пользователю не требуется раскрывать свой основной пароль.

6. Разделение сессий и контроль доступа к сессиям

7. Шифрование в облачных хранилищах

Большинство популярных сервисов облачного хранения обеспечивают шифрование TSL/SSL при передаче данных и иногда при хранении данных.