Обфускация

Обфускация — это процесс, в ходе которого вы берёте что-то, что обычно легко понять, и делаете это что-то гораздо более сложным для понимания. Один из интересных аспектов обфускации заключается в том, что, если вы знаете, как выполняется обфускация, вы можете обратить процесс вспять и получить доступ к исходным данным. С помощью обфускации вы эффективно скрываете информацию, но она находится у вас на виду. И только если вы знаете, как она была скрыта, вы поймёте, что внутри этого объекта действительно содержатся данные.

Одним из очень популярных видов обфускации является стеганография, с помощью которой мы можем скрыть информацию внутри изображения. Где-то в этом изображении есть данные, которые мы могли бы восстановить, если бы знали, как они изначально хранились. Слово «стеганография» имеет греческие корни. Оно означает «скрытое письмо». Это способ скрыть данные в изображении, подобном этому.

Мы часто называем стеганографию своего рода «безопасностью через неизвестность». Это значит, что если вы знаете процесс, который использовался для сокрытия данных, то можете легко их восстановить. Именно поэтому мы часто говорим, что «безопасность через неизвестность» на самом деле не является безопасностью.

Конечно, сокрытие информации в изображении — это лишь один из видов стеганографии. Стеганографию можно использовать в самых разных средах и формах.

Например, вы можете скрыть информацию в сетевом трафике и встроить сообщения в TCP-пакеты, которые вы отправляете по сети. Очевидно, что эти данные отправляются по несколько бит или байтов за раз. И если вы знаете, как отправляются данные, вы можете восстановить их на другой стороне.

Что ж. Если вы можете хранить информацию внутри изображения, то, конечно, можете хранить её и в других типах медиа. Например, можно использовать аудиостеганографию, когда вы скрываете информацию внутри аудиофайла или аудиодорожки. Мы также можем использовать видеостеганографию. Таким образом, видео, подобное этому, можно использовать для сокрытия большого объёма информации внутри конкретного файла.

Очень популярная форма обфускации, которую мы используем каждый день, — это токенизация. Она заключается в том, что мы берём конфиденциальные данные и заменяем их токеном этих конфиденциальных данных. Например, мы можем взять номер социального страхования, который является относительно конфиденциальной информацией, и заменить его на совершенно другой номер. Но на самом деле мы сопоставляем эти два номера.

Это значит, что мы можем передать изменённое число по сети. А на другой стороне оно преобразуется в фактическое число. Если кому-то удастся получить информацию, содержащую этот токен, он не сможет использовать её в практических целях, потому что это не настоящий номер социального страхования.

Возможно, вы этого не осознаёте, но это тот же процесс, который происходит, когда вы оплачиваете покупки в магазине с помощью мобильного телефона или смарт-часов. На основе номера вашей кредитной карты создаётся временный токен. Именно этот токен отправляется по сети. Это одноразовый токен, то есть, если кто-то перехватит этот токен во время перевода, а затем попытается использовать его снова, в использовании токена будет отказано, поскольку его можно использовать только один раз.

Это значит, что мы можем передавать эти данные по сети без необходимости их шифрования. Поскольку мы заменили конфиденциальную информацию о кредитной карте одноразовым токеном, мы можем отправлять эти данные по сети без необходимости их шифрования или хеширования. Если эти данные попадут в чужие руки, злоумышленники ничего не смогут с ними сделать. А поскольку они не связаны математически с номером вашей кредитной карты, их можно совершенно безопасно отправлять по сети.

Вот как происходит токенизация кредитной карты. Первый шаг — регистрация номера кредитной карты на вашем мобильном телефоне. Когда вы выполняете эту процедуру, ваш телефон обращается к удалённому серверу токенизации для регистрации кредитной карты. В этот момент сервер предоставляет вам ряд токенов, которые будут храниться на вашем телефоне.

Обратите внимание, что токен сильно отличается от фактического номера кредитной карты, который мы зарегистрировали на нашем телефоне. В большинстве случаев мы вообще не видим этот токен. Однако если вы посмотрите на чек, то можете заметить, что в нём указан номер кредитной карты, который не совпадает с фактическим номером кредитной карты. Теперь, когда мы получили эти токены, наш телефон готов к использованию при оформлении заказа.

Итак, мы пойдём в магазин. И во время оформления заказа мы воспользуемся технологией беспроводной связи для передачи этого токена в платёжную систему. Таким образом, вместо того чтобы вводить номер нашей реальной кредитной карты, мы оплачиваем покупку одним из токенов, которые изначально получили от сервера службы токенов.

Затем продавец отправляет этот токен на сервер службы токенов. Сервер выполняет обратный поиск, чтобы определить фактический номер кредитной карты. Теперь, когда система знает фактический номер кредитной карты, она может проверить, достаточно ли у вас средств или кредита для совершения этой транзакции. Сервер проверяет токен и одобряет транзакцию для продавца.

Теперь, когда этот токен был использован, ваш телефон удалит его. Его больше нельзя будет использовать для будущих транзакций. Затем ваш телефон подготовит следующий токен из вашего списка или запросит новый токен у сервера службы токенов. Именно этот токен будет использоваться для следующей транзакции.

Когда вы получите квитанцию об оплате, вы можете заметить, что в ней используется дополнительная маскировка. Если вы посмотрите на номер кредитной карты в квитанции, то обычно увидите ряд звёздочек и последние четыре цифры номера кредитной карты. Это называется маскировкой данных: мы скрываем часть исходного номера и показываем в квитанции только его часть. Таким образом вы предотвращаете возможность получения кем-либо доступа к вашим чекам и использования номеров ваших кредитных карт для совершения собственных платежей.

Поэтому, если вы позвоните в компанию, выпустившую вашу кредитную карту, вам могут сказать, что они проверяют кредитную карту с последними четырьмя цифрами 2512. Чтобы обеспечить безопасность всего номера, компании нередко ограничивают доступ к этой информации. И человек, которому вы звоните, может видеть только часть номера вашей кредитной карты.