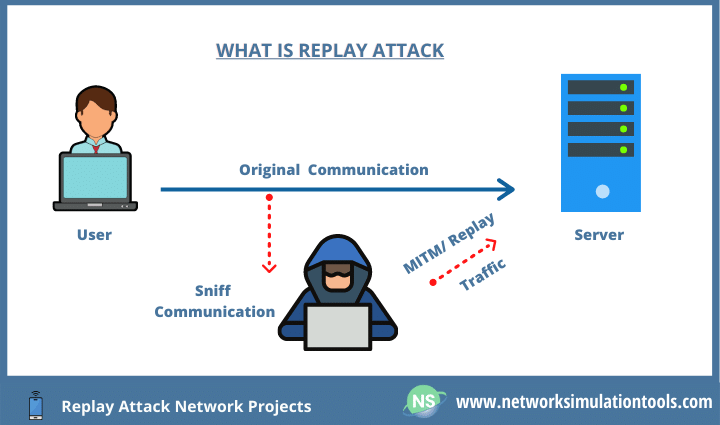
11.1. Авторизация. Возможность атаки типа Replay  
<https://stackoverflow.com/questions/3715920/is-it-worth-hashing-passwords-on-the-client-side>  
[https://ru.wikipedia.org/wiki/Атака\_повторного\_воспроизведения](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE%D0%B2%D1%82%D0%BE%D1%80%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B2%D0%BE%D1%81%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F)

Replay Attack – одна из разновидностей атаки Man-In-The-Middle, которая состоит в перехвате отправляемых на сервер данных авторизации и повторной их отправки с клиента злоумышленника без необходимости их расшифровки, таким образом атаке может быть подвержено даже защищенное https соединение.



В данном проекте такой тип атаки возможен в связи с передачей пароля на сервер в виде текста. Как было указано выше, защищенное соединение не играет роль в данном случае, так как у злоумышленника нет необходимости в расшифровке данных.

**Я не буду реализовывать защиту от данной атаки,** поскольку она реализована во всех протоколах, которые используются в реальной работе, а в данном проекте я пишу авторизацию собственноручно с целью проверить понимание самой концепции авторизации и токенизации, т.н. proof of concept. Написание такой защиты является затратной по времени.

В современных протоколах защита от данной атаки реализована путем формирования открытого ключа для каждой попытки входа на сайт. После первой попытки входа ключ становится невалидным. Однако это всё равно не защищает от атаки, если злоумышленник контролирует саму сеть, к которой вы подключены, а не является в ней таким же клиентом.