اقدامات انجام شده برای جلوگیری از replay attacks:

همانطور که در داک گفته شده است فرد مهاجم پیام های رد و بدل شده بین سرور و کلاینت را ذخیره میکند و دوباره آنها رو به سمت مقصد میفرستد. یکی از راه های جلوگیری از این تهاجم استفاده از زمان است به این صورت که هر پیامی که بین سرور و کلاینت منتقل میشود زمان ایجاد شدن خود را نیز نگه می دارد. پس از دریافت پیام در مقصد چک میشود فاصله زمانی ایجاد شدن پیام و دریافت پیام از حدی بیشتر نباشد در غیر اینصورت پیام پذیرفته نخواهد شد.

- هر پیام زمان ایجاد شدن خود را نگه میدارد:

```
public class Message implements Serializable {
    private String sender;
    private Object[] inputs;
    private Object output;
    protected MessageType messageType;
    private final Date date = new Date();
```

- پس از دریافت هر پیام چک میشود که فاصله زمانی ایجاد و دریافت پیام از ۳۰ ثانیه بیشتر نباشد:

```
private void processMessage(Message message) throws Exception {
    if(new Date().getTime()-message.getDate().getTime()>30*1000){
        objectOutputStream.writeObject(new Message(new Exception("we got you sucker!")));
        return;
    }
```