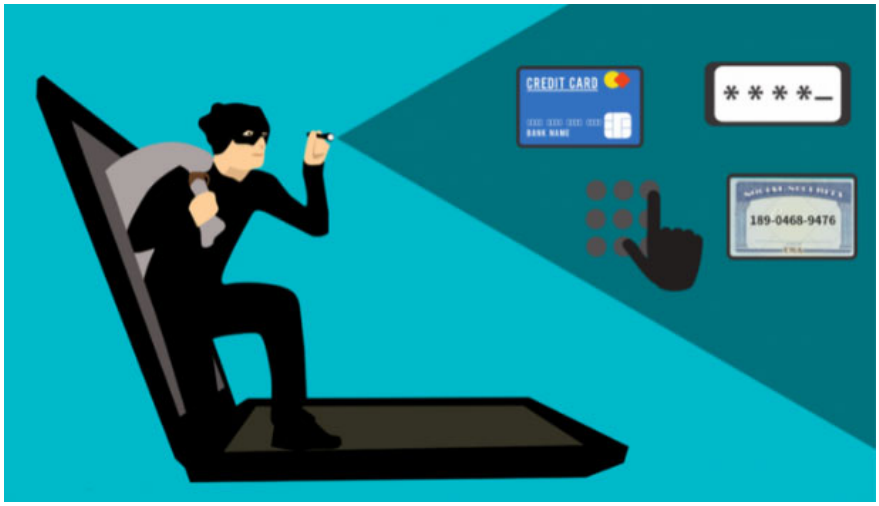
What is a Replay Attack?

A Replay Attack occurs when a cybercriminal eavesdroves a communication over a secure network, intercepts it, then delays or resends the content, to get the recipient to do what the hacker wants.

The danger level of Replay Attack is that the hacker does not even need advanced skills to decode a message, after obtaining it from the network. The attack can be successful by resending everything.

How does a Replay Attack work?



Replay Attack can cause serious financial loss
Let's look at a real world example of a Replay Attack. An employee at a company requests money transfer, by sending an encrypted message to the company's financial manager. The attacker eavesdropped on the message, intercepted the message, and is now able to resend it. Because it was a re-sent verification message, it is properly encrypted and looks legitimate to the financial manager.

In this case, the financial manager is capable of meeting this new requirement, unless there is good cause for doubt. And the consequence of this is a large amount of money deposited into the attacker's bank account.

How to prevent a Replay Attack

To prevent such an attack, you need the right encryption method. Encrypted messages carry keys within them and when they are decrypted at the end of transmission, the message opens. During a Replay Attack, the attacker intercepts the original message from being able to read or decrypt the key. All that attacker has to do is intercept and resend all messages and keys together.

To counter this possibility, both the sender and receiver must establish a completely random session key, which is valid for only one transaction and cannot be reused.

Another precaution against this type of attack is to use timestamp on all messages. This prevents hackers from resending previously sent messages, longer than a certain amount of time, thereby reducing the chance that an attacker could eavesdrop, alter the entire content of the message and send it. again.

Another method to avoid falling victim to Replay Attack is to have a password that can be used only once per transaction. That ensures that even if the message is logged and sent back by the attacker, the encryption code has expired and is no longer functional.