Replay Attack | Bugcrowd

Archived: 2026-04-05 20:31:51 UTC

A replay attack is a form of network attack in which cyber attackers identify and detect a data transmission and then delay it or repeat it. The data transmission is delayed or repeated by the cyber attacker. Once the data is intercepted, it is retransmitted to the original destination, where the attacker now pretends to be the original sender. The party receives the authenticated message, but it is the message sent by the attacker. Of course, the message is received twice – this is why it is called a replay attack. The replay attack is particularly harmful in that the cyber attacker need not even decrypt the message they resend. However, they can still deceive the message recipient into believing that the received message is legitimate. Replay attacks enable cyber attackers to access targeted networks where they can access information that would not have been easily accessible.

How would a Replay Attack Work?

In this hypothetical example, Party A wants to request that Party B transfer $100 to Party A's account. Party A sends a legitimate message to Party B in support of this request. Since Party B believes that Party A's request is

legitimate, Party B sends the amount requested.

Instead, Party A's initial transfer message was intercepted by a cyber attacker that, in turn, resends the message to Party B. Once again, Party B thinks the message is from Party A, so Party B transfers the amount requested again. However, this time, Party B transmits the amount of money requested to the cyber attacker, not Party A. This is one example of how replay attacks can be used.

Networks and computers vulnerable to replay attacks will determine the attack process as legitimate messages. One example of a replay attack is to replay the message sent to a network by an attacker, which an authorized user earlier sent. Consider that the messages might be encrypted. A replay attack provides access to valuable resources by replaying an authentication message and confusing the recipient host.

How can Replay Attacks be Prevented?

One best practice in defense of the replay attack is to provide timestamps or sequence numbers for each message sent. Recipients can then identify a message with a repeated timestamp or sequence number and then discard it.

Another best practice is the use of digital signatures. Digital signatures allow the recipient to authenticate the sender.

Another best practice to mitigate replay attacks is to use random-session session keys. Random-session keys are generally time-specific. Therefore, these keys will change over time, making it difficult for the cyber attacker to deceive a recipient.

One-time passwords are another excellent best practice that can also be used to mitigate replay attacks. A one-time password is an automatically generated alphanumeric string of characters that authenticates a user for only one transaction or login session. One-time passwords are much more secure than typical passwords.

How Does the Internet Protocol Security (IPsec) Impact Replay Attacks?

IPsec is a suite of protocols and algorithms that secure data transmitted over the internet. The IETF developed IPsec protocols to secure the IP layer using authentication and encryption of IP network packets. IPsec's first definitions referred to two protocols to secure IP packets. These included the Authentication Header for data integrity and anti-replay services and the Encapsulating Security Payload, which encrypts and authenticates data.

The IPsec suite also includes an Internet Key Exchange used to generate shared security keys to establish a security association. Security associations are used by the encryption and decryption processes to create a security level between two entities. Typically, a firewall between two networks handles the security association process.

Want to learn more? Check out our FREE Bugcrowd University to sharpen your hacking skills.

Organizations the world over need your help! Join our researcher community to connect with hundreds of organization programs focused on finding their security vulnerabilities. Our vast directory includes programs for all skill levels across many industries and from around the world.

Source: https://www.bugcrowd.com/glossary/replay-attack/