# CWE Detail – CWE-294

## Description

A capture-replay flaw exists when the design of the product makes it possible for a malicious user to sniff network traffic and bypass authentication by replaying it to the server in question to the same effect as the original message (or with minor changes).

## Extended Description

Capture-replay attacks are common and can be difficult to defeat without cryptography. They are a subset of network injection attacks that rely on observing previously-sent valid commands, then changing them slightly if necessary and resending the same commands to the server.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2005-3435: product authentication succeeds if user-provided MD5 hash matches the hash in its database; this can be subjected to replay attacks.

**•** CVE-2007-4961: Chain: cleartext transmission of the MD5 hash of password (CWE-319) enables attacks against a server that is susceptible to replay (CWE-294).

## Related Attack Patterns (CAPEC)

* CAPEC-102
* CAPEC-509
* CAPEC-555
* CAPEC-561
* CAPEC-60
* CAPEC-644
* CAPEC-645
* CAPEC-652
* CAPEC-701
* CAPEC-94

## Attack TTPs

**•** T1557: Adversary-in-the-Middle (Tactics: credential-access, collection)

**•** T1133: External Remote Services (Tactics: persistence, initial-access)

**•** T1558: Steal or Forge Kerberos Tickets (Tactics: credential-access)

**•** T1021.002: SMB/Windows Admin Shares (Tactics: lateral-movement)

**•** T1021: Remote Services (Tactics: lateral-movement)

**•** T1550.003: Pass the Ticket (Tactics: defense-evasion, lateral-movement)

**•** T1134.001: Token Impersonation/Theft (Tactics: defense-evasion, privilege-escalation)

**•** T1114.002: Remote Email Collection (Tactics: collection)

**•** T1550.004: Web Session Cookie (Tactics: defense-evasion, lateral-movement)

**•** T1550.002: Pass the Hash (Tactics: defense-evasion, lateral-movement)

**•** T1558.003: Kerberoasting (Tactics: credential-access)

## Modes of Introduction

**•** Architecture and Design: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes: Messages sent with a capture-relay attack allow access to resources which are not otherwise accessible without proper authentication.

## Potential Mitigations

**•** Architecture and Design: Utilize some sequence or time stamping functionality along with a checksum which takes this into account in order to ensure that messages can be parsed only once. (Effectiveness: N/A)

**•** Architecture and Design: Since any attacker who can listen to traffic can see sequence numbers, it is necessary to sign messages with some kind of cryptography to ensure that sequence numbers are not simply doctored along with content. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)