# CWE Detail – CWE-301

## Description

Simple authentication protocols are subject to reflection attacks if a malicious user can use the target machine to impersonate a trusted user.

## Extended Description

A mutual authentication protocol requires each party to respond to a random challenge by the other party by encrypting it with a pre-shared key. Often, however, such protocols employ the same pre-shared key for communication with a number of different entities. A malicious user or an attacker can easily compromise this protocol without possessing the correct key by employing a reflection attack on the protocol. Reflection attacks capitalize on mutual authentication schemes in order to trick the target into revealing the secret shared between it and another valid user. In a basic mutual-authentication scheme, a secret is known to both the valid user and the server; this allows them to authenticate. In order that they may verify this shared secret without sending it plainly over the wire, they utilize a Diffie-Hellman-style scheme in which they each pick a value, then request the hash of that value as keyed by the shared secret. In a reflection attack, the attacker claims to be a valid user and requests the hash of a random value from the server. When the server returns this value and requests its own value to be hashed, the attacker opens another connection to the server. This time, the hash requested by the attacker is the value which the server requested in the first connection. When the server returns this hashed value, it is used in the first connection, authenticating the attacker successfully as the impersonated valid user.

## 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.

## Related Attack Patterns (CAPEC)

* CAPEC-90

## 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: The primary result of reflection attacks is successful authentication with a target machine -- as an impersonated user.

## Potential Mitigations

**•** Architecture and Design: Use different keys for the initiator and responder or of a different type of challenge for the initiator and responder. (Effectiveness: N/A)

**•** Architecture and Design: Let the initiator prove its identity before proceeding. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

## Notes

**•** Maintenance: The term "reflection" is used in multiple ways within CWE and the community, so its usage should be reviewed.