# CWE Detail – CWE-322

## Description

The product performs a key exchange with an actor without verifying the identity of that actor.

## Extended Description

Performing a key exchange will preserve the integrity of the information sent between two entities, but this will not guarantee that the entities are who they claim they are. This may enable an attacker to impersonate an actor by modifying traffic between the two entities. Typically, this involves a victim client that contacts a malicious server that is impersonating a trusted server. If the client skips authentication or ignores an authentication failure, the malicious server may request authentication information from the user. The malicious server can then use this authentication information to log in to the trusted server using the victim's credentials, sniff traffic between the victim and trusted server, etc.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Architecture and Design: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes: No authentication takes place in this process, bypassing an assumed protection of encryption.

**•** Impact: Read Application Data — Notes: The encrypted communication between a user and a trusted host may be subject to sniffing by any actor in the communication path.

## Potential Mitigations

**•** Architecture and Design: Ensure that proper authentication is included in the system design. (Effectiveness: N/A)

**•** Implementation: Understand and properly implement all checks necessary to ensure the identity of entities involved in encrypted communications. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A