# CWE Detail – CWE-300

## Description

The product does not adequately verify the identity of actors at both ends of a communication channel, or does not adequately ensure the integrity of the channel, in a way that allows the channel to be accessed or influenced by an actor that is not an endpoint.

## Extended Description

In order to establish secure communication between two parties, it is often important to adequately verify the identity of entities at each end of the communication channel. Inadequate or inconsistent verification may result in insufficient or incorrect identification of either communicating entity. This can have negative consequences such as misplaced trust in the entity at the other end of the channel. An attacker can leverage this by interposing between the communicating entities and masquerading as the original entity. In the absence of sufficient verification of identity, such an attacker can eavesdrop and potentially modify the communication between the original entities.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2014-1266: chain: incorrect "goto" in Apple SSL product bypasses certificate validation, allowing Adversry-in-the-Middle (AITM) attack (Apple "goto fail" bug). CWE-705 (Incorrect Control Flow Scoping) -> CWE-561 (Dead Code) -> CWE-295 (Improper Certificate Validation) -> CWE-393 (Return of Wrong Status Code) -> CWE-300 (Channel Accessible by Non-Endpoint).

## Related Attack Patterns (CAPEC)

* CAPEC-466
* CAPEC-57
* CAPEC-589
* CAPEC-590
* CAPEC-612
* CAPEC-613
* CAPEC-615
* CAPEC-662
* CAPEC-94

## Attack TTPs

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

**•** T1040: Network Sniffing (Tactics: credential-access, discovery)

**•** T1185: Browser Session Hijacking (Tactics: collection)

## Modes of Introduction

**•** Architecture and Design: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Read Application Data, Modify Application Data, Gain Privileges or Assume Identity — Notes: An attacker could pose as one of the entities and read or possibly modify the communication.

## Potential Mitigations

**•** Implementation: Always fully authenticate both ends of any communications channel. (Effectiveness: N/A)

**•** Architecture and Design: Adhere to the principle of complete mediation. (Effectiveness: N/A)

**•** Implementation: A certificate binds an identity to a cryptographic key to authenticate a communicating party. Often, the certificate takes the encrypted form of the hash of the identity of the subject, the public key, and information such as time of issue or expiration using the issuer's private key. The certificate can be validated by deciphering the certificate with the issuer's public key. See also X.509 certificate signature chains and the PGP certification structure. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** By eavesdropping on the communication channel or posing as the endpoint, an attacker would be able to read all of the transmitted data.

## Notes

**•** Maintenance: The summary identifies multiple distinct possibilities, suggesting that this is a category that must be broken into more specific weaknesses.