# CWE Detail – CWE-1302

## Description

The product implements a security identifier mechanism to differentiate what actions are allowed or disallowed when a transaction originates from an entity. A transaction is sent without a security identifier.

## Extended Description

In a System-On-Chip (SoC), various integrated circuits and hardware engines generate transactions such as to access (reads/writes) assets or perform certain actions (e.g., reset, fetch, compute). A typical transaction is comprised of source identity (to identify the originator of the transaction) and a destination identity (to route the transaction to the respective entity) in addition to much more information in the message. Sometimes the transactions are qualified with a Security Identifier. This Security Identifier helps the destination agent decide on the set of allowed or disallowed actions. A weakness that can exist in such transaction schemes is that the source agent does not consistently include the necessary Security Identifier with the transaction. If the Security Identifier is missing, the destination agent might drop the message (resulting in an inadvertent Denial-of-Service (DoS)) or take inappropriate action by default in its attempt to execute the transaction, resulting in privilege escalation or provision of unintended access.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Related Attack Patterns (CAPEC)

* CAPEC-121
* CAPEC-681

## Modes of Introduction

**•** Architecture and Design: Such issues could be introduced during hardware architecture and design and identified later during Testing or System Configuration phases.

**•** Implementation: Such issues could be introduced during implementation and identified later during Testing or System Configuration phases.

## Common Consequences

**•** Impact: Modify Memory, Read Memory, DoS: Crash, Exit, or Restart, Bypass Protection Mechanism, Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Architecture and Design: Transaction details must be reviewed for design inconsistency and common weaknesses. (Effectiveness: N/A)

**•** Implementation: Security identifier definition and programming flow must be tested in pre-silicon and post-silicon testing. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The originator sends a transaction with no security identifier, i.e., meaning the value is "0" or NULL. The AES-Key-access register does not allow the necessary action and drops the transaction because the originator failed to include the required security identifier.