# CWE Detail – CWE-1292

## Description

The product implements a conversion mechanism to map certain bus-transaction signals to security identifiers. However, if the conversion is incorrectly implemented, untrusted agents can gain unauthorized access to the asset.

## 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, etc.). Among various types of message information, 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). Sometimes the transactions are qualified with a security identifier. This security identifier helps the destination agent decide on the set of allowed actions (e.g., access an asset for read and writes). A typical bus connects several leader and follower agents. Some follower agents implement bus protocols differently from leader agents. A protocol conversion happens at a bridge to seamlessly connect different protocols on the bus. One example is a system that implements a leader with the Advanced High-performance Bus (AHB) protocol and a follower with the Open-Core Protocol (OCP). A bridge AHB-to-OCP is needed to translate the transaction from one form to the other. A common weakness that can exist in this scenario is that this conversion between protocols is implemented incorrectly, whereupon an untrusted agent may gain unauthorized access to an asset.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Modes of Introduction

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

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

## Common Consequences

**•** Impact: Modify Memory, Read Memory, DoS: Resource Consumption (Other), Execute Unauthorized Code or Commands, Gain Privileges or Assume Identity, Quality Degradation — Notes:

## Potential Mitigations

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

**•** Implementation: Access and programming flows must be tested in pre-silicon and post-silicon testing. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Because of the incorrect conversion, the security identifier information is either lost or could be modified in such a way that an untrusted leader can access the AES-Key registers.