# CWE Detail – CWE-1311

## Description

The bridge incorrectly translates security attributes from either trusted to untrusted or from untrusted to trusted when converting from one fabric protocol to another.

## Extended Description

A bridge allows IP blocks supporting different fabric protocols to be integrated into the system. Fabric end-points or interfaces usually have dedicated signals to transport security attributes. For example, HPROT signals in AHB, AxPROT signals in AXI, and MReqInfo and SRespInfo signals in OCP. The values on these signals are used to indicate the security attributes of the transaction. These include the immutable hardware identity of the controller initiating the transaction, privilege level, and type of transaction (e.g., read/write, cacheable/non-cacheable, posted/non-posted). A weakness can arise if the bridge IP block, which translates the signals from the protocol used in the IP block endpoint to the protocol used by the central bus, does not properly translate the security attributes. As a result, the identity of the initiator could be translated from untrusted to trusted or vice-versa. This could result in access-control bypass, privilege escalation, or denial of service.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Related Attack Patterns (CAPEC)

* CAPEC-1
* CAPEC-180
* CAPEC-233

## Attack TTPs

**•** T1548: Abuse Elevation Control Mechanism (Tactics: privilege-escalation, defense-evasion)

**•** T1574.010: Services File Permissions Weakness (Tactics: persistence, privilege-escalation, defense-evasion)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Memory, Read Memory, Gain Privileges or Assume Identity, Bypass Protection Mechanism, Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Architecture and Design: The translation must map signals in such a way that untrusted agents cannot map to trusted agents or vice-versa. (Effectiveness: N/A)

**•** Implementation: Ensure that the translation maps signals in such a way that untrusted agents cannot map to trusted agents or vice-versa. (Effectiveness: N/A)

## Applicable Platforms

**•** Verilog (Class: None, Prevalence: Undetermined)

**•** VHDL (Class: None, Prevalence: Undetermined)

## Demonstrative Examples

**•** Logic in the case statement only checks for MReqInfo bits 4:2, i.e., hardware-identity bits 3:1. When ocp\_mreqinfo is 5'h1F or 5'h0E, p0\_mreqinfo\_o\_temp[2] will be 1. As a result, untrusted IDs from OCP 5'h1F and 5'h0E get translated to trusted ahb\_hprot values 2'b00.