# CWE Detail – CWE-1317

## Description

The product uses a fabric bridge for transactions between two Intellectual Property (IP) blocks, but the bridge does not properly perform the expected privilege, identity, or other access control checks between those IP blocks.

## Extended Description

In hardware designs, different IP blocks are connected through interconnect-bus fabrics (e.g. AHB and OCP). Within a System on Chip (SoC), the IP block subsystems could be using different bus protocols. In such a case, the IP blocks are then linked to the central bus (and to other IP blocks) through a fabric bridge. Bridges are used as bus-interconnect-routing modules that link different protocols or separate, different segments of the overall SoC interconnect. For overall system security, it is important that the access-control privileges associated with any fabric transaction are consistently maintained and applied, even when they are routed or translated by a fabric bridge. A bridge that is connected to a fabric without security features forwards transactions to the slave without checking the privilege level of the master and results in a weakness in SoC access-control security. The same weakness occurs if a bridge does not check the hardware identity of the transaction received from the slave interface of the bridge.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2019-6260: Baseboard Management Controller (BMC) device implements Advanced High-performance Bus (AHB) bridges that do not require authentication for arbitrary read and write access to the BMC's physical address space from the host, and possibly the network [REF-1138].

## Related Attack Patterns (CAPEC)

* CAPEC-122

## Attack TTPs

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

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Architecture and Design: Ensure that the design includes provisions for access-control checks in the bridge for both upstream and downstream transactions. (Effectiveness: N/A)

**•** Implementation: Implement access-control checks in the bridge for both upstream and downstream transactions. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The bridge does not implement the checks and allows reads and writes from all privilege levels.

**•** The previous code snippet [REF-1382] illustrates an instance of a vulnerable implementation of access control for the CLINT peripheral (see module clint). It also shows a correct implementation of access control for the AES peripheral (see module aes0\_wrapper) [REF-1381]. An enable signal (en\_o) from the fabric's AXI interface (present in both modules) is used to determine if an access request is made to the peripheral. In the case of the AES peripheral, this en\_o signal is first received in a temporary signal en\_acct. Then, the access request is enabled (by asserting the en signal) only if the request has sufficient access permissions (i.e., acct\_ctrl\_i signal should be enabled). However, in the case of the CLINT peripheral, the enable signal, en\_o, from the AXI interface, is directly used to enable accesses. As a result, users with insufficient access permissions also get full access to the CLINT peripheral.