# CWE Detail – CWE-1318

## Description

On-chip fabrics or buses either do not support or are not configured to support privilege separation or other security features, such as access control.

## Extended Description

Certain on-chip fabrics and buses, especially simple and low-power buses, do not support security features. Apart from data transfer and addressing ports, some fabrics and buses do not have any interfaces to transfer privilege, immutable identity, or any other security attribute coming from the bus master. Similarly, they do not have dedicated signals to transport security-sensitive data from slave to master, such as completions for certain types of transactions. Few other on-chip fabrics and buses support security features and define specific interfaces/signals for transporting security attributes from master to slave or vice-versa. However, including these signals is not mandatory and could be left unconfigured when generating the register-transfer-level (RTL) description for the fabric. Such fabrics or buses should not be used to transport any security attribute coming from the bus master. In general, peripherals with security assets should not be connected to such buses before the transaction from the bus master reaches the bus, unless some form of access control is performed at a fabric bridge or another intermediate module.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-1
* CAPEC-180

## Attack TTPs

**•** 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: DoS: Crash, Exit, or Restart, Read Memory, Modify Memory — Notes:

## Potential Mitigations

**•** Architecture and Design: If fabric does not support security features, implement security checks in a bridge or any component that is between the master and the fabric. Alternatively, connect all fabric slaves that do not have any security assets under one such fabric and connect peripherals with security assets to a different fabric that supports security features. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The APB bus is used to connect several bus masters, each with a unique and immutable hardware identity, to several slaves. For a CPU supporting 8 potential identities (each with varying privilege levels), 16 types of outgoing transactions can be made--8 read transactions with each supported privilege level and 8 write transactions with each supported privilege level.

**•** Since MReqInfo and SRespInfo are not mandatory, these signals are not configured when autogenerating RTL for the OCP fabric. Thus, the fabric cannot be used to transport security attributes from bus masters to slave.