# CWE Detail – CWE-1192

## Description

The System-on-Chip (SoC) does not have unique, immutable identifiers for each of its components.

## Extended Description

A System-on-Chip (SoC) comprises several components (IP) with varied
 trust requirements. It is required that each IP is identified
 uniquely and should distinguish itself from other entities in
 the SoC without any ambiguity. The unique secured identity is
 required for various purposes. Most of the time the identity is used
 to route a transaction or perform certain actions, including
 resetting, retrieving a sensitive information, and acting upon or on
 behalf of something else. There are several variants of this weakness: A "missing" identifier is when the SoC does not define
 any mechanism to uniquely identify the IP. An "insufficient" identifier might provide
 some defenses - for example, against the most common
 attacks - but it does not protect against everything
 that is intended. A "misconfigured" mechanism occurs when a mechanism
 is available but not implemented correctly. An "ignored" identifier occurs when the SoC/IP has not applied
 any policies or does not act upon the identifier securely.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Related Attack Patterns (CAPEC)

* CAPEC-113

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Every identity generated in the SoC should be unique and
 immutable in hardware. The actions that an IP is trusted or
 not trusted should be clearly defined, implemented,
 configured, and tested. If the definition is implemented via a
 policy, then the policy should be immutable or protected with
 clear authentication and authorization. (Effectiveness: N/A)

## Applicable Platforms

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