# CWE Detail – CWE-325

## Description

The product does not implement a required step in a cryptographic algorithm, resulting in weaker encryption than advertised by the algorithm.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2001-1585: Missing challenge-response step allows authentication bypass using public key.

## Related Attack Patterns (CAPEC)

* CAPEC-68

## Attack TTPs

**•** T1553.002: Code Signing (Tactics: defense-evasion)

## Modes of Introduction

**•** Implementation: Developers sometimes omit "expensive" (resource-intensive) steps in order to improve performance, especially in devices with limited memory or slower CPUs. This step may be taken under a mistaken impression that the step is unnecessary for the cryptographic algorithm.

**•** Requirements: This issue may happen when the requirements for the cryptographic algorithm are not clearly stated.

## Common Consequences

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

**•** Impact: Read Application Data, Modify Application Data — Notes:

**•** Impact: Hide Activities — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** However, this HMAC engine cannot handle messages that are longer than 512 bits. Moreover, a complete HMAC will contain an iterate hash function that breaks up a message into blocks of a fixed size and iterates over them with a compression function (e.g., SHA-256). Therefore, the implementation of the HMAC in OpenPiton SoC is incomplete. Such HMAC engines will not be used in real-world applications as the messages will usually be longer than 512 bits. For instance, OpenTitan offers a comprehensive HMAC implementation that utilizes a FIFO for temporarily storing the truncated message, as detailed in [REF-1359].

## Notes

**•** Relationship: Overlaps incomplete/missing security check.

**•** Relationship: Can be resultant.