# CWE Detail – CWE-358

## Description

The product does not implement or incorrectly implements one or more security-relevant checks as specified by the design of a standardized algorithm, protocol, or technique.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-0862: Browser does not verify Basic Constraints of a certificate, even though it is required, allowing spoofing of trusted certificates.

**•** CVE-2002-0970: Browser does not verify Basic Constraints of a certificate, even though it is required, allowing spoofing of trusted certificates.

**•** CVE-2002-1407: Browser does not verify Basic Constraints of a certificate, even though it is required, allowing spoofing of trusted certificates.

**•** CVE-2005-0198: Logic error prevents some required conditions from being enforced during Challenge-Response Authentication Mechanism with MD5 (CRAM-MD5).

**•** CVE-2004-2163: Shared secret not verified in a RADIUS response packet, allowing authentication bypass by spoofing server replies.

**•** CVE-2005-2181: Insufficient verification in VoIP implementation, in violation of standard, allows spoofed messages.

**•** CVE-2005-2182: Insufficient verification in VoIP implementation, in violation of standard, allows spoofed messages.

**•** CVE-2005-2298: Security check not applied to all components, allowing bypass.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: This is an implementation error, in which the algorithm/technique requires certain security-related behaviors or conditions that are not implemented or checked properly, thus causing a vulnerability.

## Common Consequences

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

## Applicable Platforms

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

## Notes

**•** Relationship: This is a "missing step" error on the product side, which can overlap weaknesses such as insufficient verification and spoofing. It is frequently found in cryptographic and authentication errors. It is sometimes resultant.