# CWE Detail – CWE-208

## Description

Two separate operations in a product require different amounts of time to complete, in a way that is observable to an actor and reveals security-relevant information about the state of the product, such as whether a particular operation was successful or not.

## Extended Description

In security-relevant contexts, even small variations in timing can be exploited by attackers to indirectly infer certain details about the product's internal operations. For example, in some cryptographic algorithms, attackers can use timing differences to infer certain properties about a private key, making the key easier to guess. Timing discrepancies effectively form a timing side channel.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2019-10071: Java-oriented framework compares HMAC signatures using String.equals() instead of a constant-time algorithm, causing timing discrepancies

**•** CVE-2019-10482: Smartphone OS uses comparison functions that are not in constant time, allowing side channels

**•** CVE-2014-0984: Password-checking function in router terminates validation of a password entry when it encounters the first incorrect character, which allows remote attackers to obtain passwords via a brute-force attack that relies on timing differences in responses to incorrect password guesses, aka a timing side-channel attack.

**•** CVE-2003-0078: SSL implementation does not perform a MAC computation if an incorrect block cipher padding is used, which causes an information leak (timing discrepancy) that may make it easier to launch cryptographic attacks that rely on distinguishing between padding and MAC verification errors, possibly leading to extraction of the original plaintext, aka the "Vaudenay timing attack."

**•** CVE-2000-1117: Virtual machine allows malicious web site operators to determine the existence of files on the client by measuring delays in the execution of the getSystemResource method.

**•** CVE-2003-0637: Product uses a shorter timeout for a non-existent user than a valid user, which makes it easier for remote attackers to guess usernames and conduct brute force password guessing.

**•** CVE-2003-0190: Product immediately sends an error message when a user does not exist, which allows remote attackers to determine valid usernames via a timing attack.

**•** CVE-2004-1602: FTP server responds in a different amount of time when a given username exists, which allows remote attackers to identify valid usernames by timing the server response.

**•** CVE-2005-0918: Browser allows remote attackers to determine the existence of arbitrary files by setting the src property to the target filename and using Javascript to determine if the web page immediately stops loading, which indicates whether the file exists or not.

## Related Attack Patterns (CAPEC)

* CAPEC-462
* CAPEC-541
* CAPEC-580

## Attack TTPs

**•** T1082: System Information Discovery (Tactics: discovery)

**•** T1592.002: Software (Tactics: reconnaissance)

## Modes of Introduction

**•** Architecture and Design: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data, Bypass Protection Mechanism — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** Since the code breaks on an incorrect entry of password, an attacker can guess the correct password for that byte-check iteration with few repeat attempts.

**•** When the attacker tries their own values, they can first try strings of various length. When they find a string of the right length, the computation will take a bit longer, because the for loop will run at least once. Additionally, with this code, the attacker can possibly learn one character of the password at a time, because when they guess the first character right, the computation will take longer than a wrong guesses. Such an attack can break even the most sophisticated password with a few hundred guesses.

## Notes

**•** Relationship: Often primary in cryptographic applications and algorithms.

**•** Maintenance: CWE 4.16 removed a demonstrative example for a hardware module because it was inaccurate and unable to be adapted. The CWE team is developing an alternative.