# CWE Detail – CWE-1300

## Description

The device does not contain sufficient protection
 mechanisms to prevent physical side channels from exposing
 sensitive information due to patterns in physically observable
 phenomena such as variations in power consumption,
 electromagnetic emissions (EME), or acoustic emissions.

## Extended Description

An adversary could monitor and measure physical
 phenomena to detect patterns and make inferences, even if it
 is not possible to extract the information in the digital
 domain. Physical side channels have been well-studied for
 decades in the context of breaking implementations of
 cryptographic algorithms or other attacks against security
 features. These side channels may be easily observed by an
 adversary with physical access to the device, or using a
 tool that is in close proximity. If the adversary can
 monitor hardware operation and correlate its data processing
 with power, EME, and acoustic measurements, the adversary
 might be able to recover of secret keys and data.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2022-35888: Power side-channels leak secret information from processor

**•** CVE-2021-3011: electromagnetic-wave side-channel in security-related microcontrollers allows extraction of private key

**•** CVE-2019-14353: Crypto hardware wallet's power consumption relates to total number of pixels illuminated, creating a side channel in the USB connection that allows attackers to determine secrets displayed such as PIN numbers and passwords

**•** CVE-2020-27211: Chain: microcontroller system-on-chip contains uses a register value stored in flash to set product protection state on the memory bus but does not contain protection against fault injection (CWE-1319), which leads to an incorrect initialization of the memory bus (CWE-1419) leading the product to be in an unprotected state.

**•** CVE-2013-4576: message encryption software uses certain instruction sequences that allows RSA key extraction using a chosen-ciphertext attack and acoustic cryptanalysis

**•** CVE-2020-28368: virtualization product allows recovery of AES keys from the guest OS using a side channel attack against a power/energy monitoring interface.

**•** CVE-2019-18673: power consumption varies based on number of pixels being illuminated in a display, allowing reading of secrets such as the PIN by using the USB interface to measure power consumption

## Related Attack Patterns (CAPEC)

* CAPEC-189
* CAPEC-699

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Architecture and Design: Apply blinding or masking techniques to implementations of cryptographic algorithms. (Effectiveness: N/A)

**•** Implementation: Add shielding or tamper-resistant protections to the device to increase the difficulty of obtaining measurements of the side-channel. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** PIN numbers used to unlock a cell phone
 should not exhibit any characteristics about
 themselves. This creates a side channel. An
 attacker could monitor the pulses using an
 oscilloscope or other method. Once the first
 character is correctly guessed (based on the
 oscilloscope readings), they can then move to the
 next character, which is much more efficient than
 the brute force method of guessing every possible
 sequence of characters.

**•** N/A

**•** The vulnerable code shows a buggy implementation of binary exponentiation where it updates the result register (result\_reg) only when the corresponding exponent bit (exponent\_reg[0]) is set to 1. However, when this exponent bit is 0, the output register is not updated. It's important to note that this implementation introduces a physical power side-channel vulnerability within the RSA core. This vulnerability could expose the private exponent to a determined physical attacker. Such exposure of the private exponent could lead to a complete compromise of the private key.