# CWE Detail – CWE-1278

## Description

Information stored in hardware may be recovered by an attacker with the capability to capture and analyze images of the integrated circuit using techniques such as scanning electron microscopy.

## Extended Description

The physical structure of a device, viewed at high enough magnification, can reveal the information stored inside. Typical steps in IC reverse engineering involve removing the chip packaging (decapsulation) then using various imaging techniques ranging from high resolution x-ray microscopy to invasive techniques involving removing IC layers and imaging each layer using a scanning electron microscope. The goal of such activities is to recover secret keys, unique device identifiers, and proprietary code and circuit designs embedded in hardware that the attacker has been unsuccessful at accessing through other means. These secrets may be stored in non-volatile memory or in the circuit netlist. Memory technologies such as masked ROM allow easier to extraction of secrets than One-time Programmable (OTP) memory.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-188
* CAPEC-37
* CAPEC-545

## Attack TTPs

**•** T1555.001: Keychain (Tactics: credential-access)

**•** T1005: Data from Local System (Tactics: collection)

**•** T1552.004: Private Keys (Tactics: credential-access)

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Varies by Context — Notes: A common goal of malicious actors who reverse engineer ICs is to produce and sell counterfeit versions of the IC.

## Potential Mitigations

**•** Architecture and Design: The cost of secret extraction via IC reverse engineering should outweigh the potential value of the secrets being extracted. Threat model and value of secrets should be used to choose the technology used to safeguard those secrets. Examples include IC camouflaging and obfuscation, tamper-proof packaging, active shielding, and physical tampering detection information erasure. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

## Notes

**•** Maintenance: This entry is still under development and will continue to see updates and content improvements. It is more attack-oriented, so it might be more suited for CAPEC.