# CWE Detail – CWE-1268

## Description

The product's hardware-enforced access control for a particular resource improperly accounts for privilege discrepancies between control and write policies.

## Extended Description

Integrated circuits and hardware engines may provide access to resources (device-configuration, encryption keys, etc.) belonging to trusted firmware or software modules (commonly set by a BIOS or a bootloader). These accesses are typically controlled and limited by the hardware. Hardware design access control is sometimes implemented using a policy. A policy defines which entity or agent may or may not be allowed to perform an action. When a system implements multiple levels of policies, a control policy may allow direct access to a resource as well as changes to the policies themselves. Resources that include agents in their control policy but not in their write policy could unintentionally allow an untrusted agent to insert itself in the write policy register. Inclusion in the write policy register could allow a malicious or misbehaving agent write access to resources. This action could result in security compromises including leaked information, leaked encryption keys, or modification of device configuration.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-180

## Attack TTPs

**•** T1574.010: Services File Permissions Weakness (Tactics: persistence, privilege-escalation, defense-evasion)

## Modes of Introduction

**•** Architecture and Design: This weakness may be introduced during the design of a device when the architect does not comprehensively specify all of the policies required by an agent.

**•** Implementation: This weakness may be introduced during implementation if device policy restrictions do not sufficiently constrain less-privileged clients.

## Common Consequences

**•** Impact: Modify Memory, Read Memory, DoS: Crash, Exit, or Restart, Execute Unauthorized Code or Commands, Gain Privileges or Assume Identity, Bypass Protection Mechanism, Read Files or Directories, Reduce Reliability — Notes:

## Potential Mitigations

**•** Architecture and Design: Access-control-policy definition and programming flow must be sufficiently tested in pre-silicon and post-silicon testing. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** IThe AES\_KEY\_CONTROL\_POLICY register value is 0x00000018. In binary, the lower 8 bits will be 0001 1000, meaning that: Bits 3 and 4 are set, thus Agents 3 and 4 will have write access to AES\_KEY\_READ\_POLICY or AES\_KEY\_WRITE\_POLICY. All other bits are clear, hence agents other than 3 and 4 will not have access to write to AES\_KEY\_READ\_POLICY or AES\_KEY\_WRITE\_POLICY. The AES\_KEY\_READ\_POLICY register value is 0x00000002. In binary, the lower 8 bits will be 0000 0010, meaning that: Bit 1 is set, thus Agent 1 will be able to read the AES key registers. The AES\_KEY\_WRITE\_POLICY register value is 0x00000004. In binary, the lower 8 bits will be 0000 0100, meaning that: Bit 2 is set, thus Agent 2 will be able to write the AES Key registers. The configured access control policy for Agents 1,2,3,4 is summarized in table below. Agent Read Write Control Agent 1 Allowed Not Allowed Not Allowed Agent 2 Not Allowed Allowed Not Allowed Agent 3 Not Allowed Not Allowed Allowed Agent 4 Not Allowed Not Allowed Allowed At this point Agents 3 and 4 can only configure which agents can read AES keys and which agents can write AES keys. Agents 3 and 4 cannot read or write AES keys - just configure access control. Now, recall Agent 3 is untrusted. As explained above, the value of the AES\_KEY\_CONTROL\_POLICY register gives agent 3 access to write to the AES\_KEY\_WRITE\_POLICY register. Agent 3 can use this write access to add themselves to the AES\_KEY\_WRITE\_POLICY register. This is accomplished by Agent 3 writing the value 0x00000006. In binary, the lower 8 bits are 0000 0110, meaning that bit 3 will be set. Thus, giving Agent 3 having the ability to write to the AES Key registers. If the AES\_KEY\_CONTROL\_POLICY register value is 0x00000010, the lower 8 bits will be 0001 0000. This will give Agent 4, a trusted agent, write access to AES\_KEY\_WRITE\_POLICY, but Agent 3, who is untrusted, will not have write access. The Policy register values should therefore be as follows:

## Notes

**•** Maintenance: This entry is still under development and will continue to see updates and content improvements.