A Novel Security Vulnerability Detection Mechanism Using Information Flow Tracking on a given SOC

Surinder Sood

Agenda

Background: Different kinds of access mechanism

Motivation

Information flow Theory

Proposed Solution

Evidence

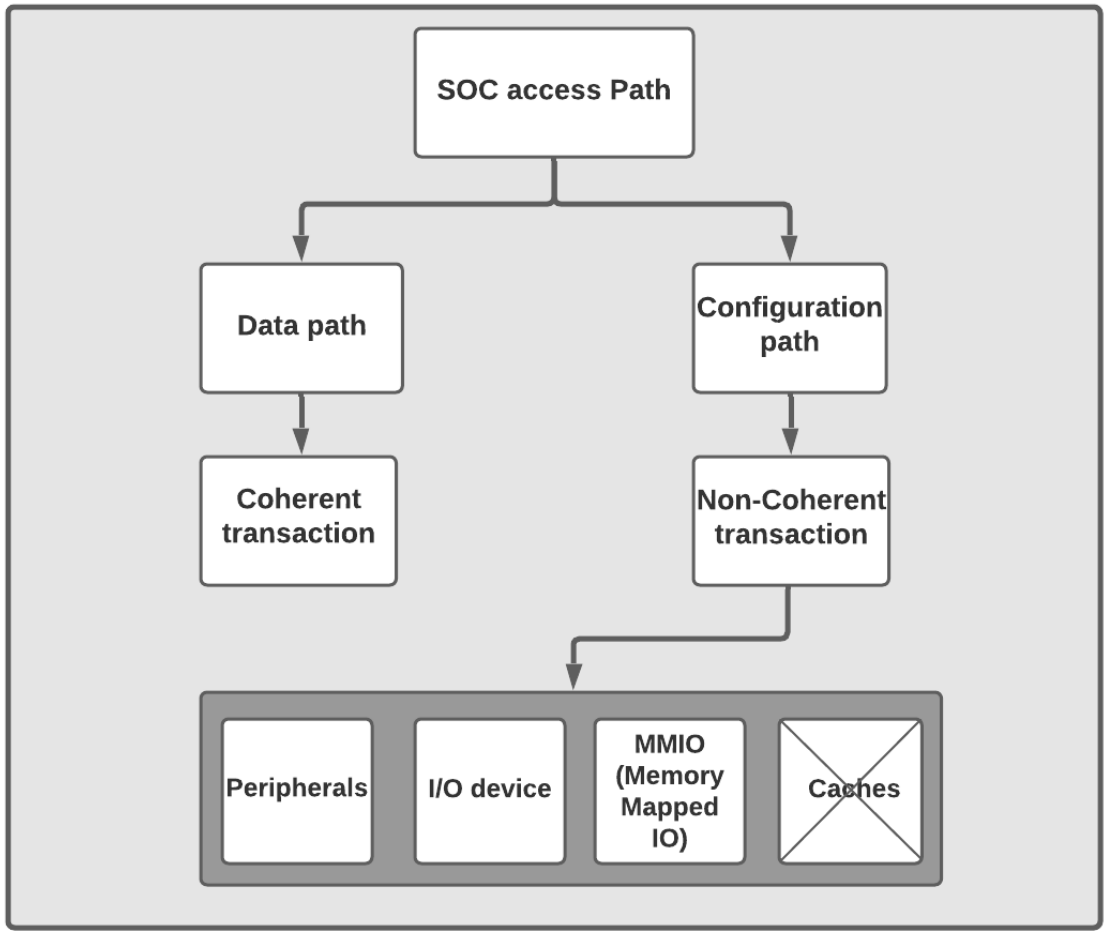
Conclusion

Terminology

- NCA = NCA- Non-Coherent Access
  - NCA is the mechanism used to exercise an NCT
- NCP = Non-Coherent Path
- Security Class = Set of access rights for a resource (e.g. register)
- Equivalent Security Class = Classes that have similar access rights
- Trust boundary = set of objects belonging to equivalent security classes
- Information Flow Model (FM)
  - Defined later

Background

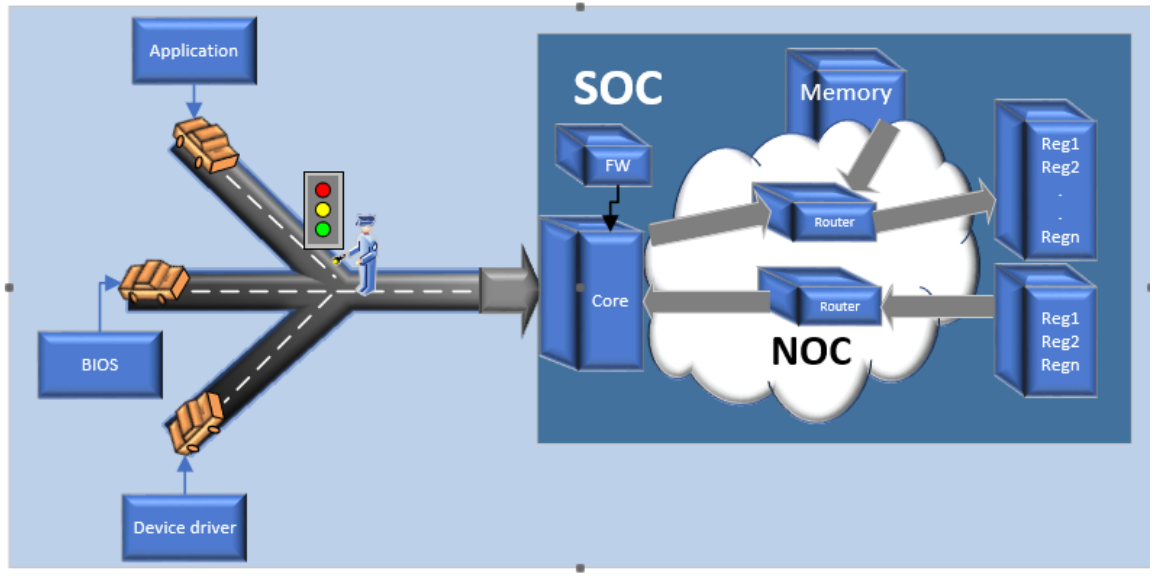
- SOC (System on Chip) access path – the communication channel from the initiator to the destination
- Data path – High bandwidth centric
- Configuration path – Initializing Components, peripherals etc
-



This work focusses on NCT (Non-Coherent Transactions)

Motivation[NC accesses]

- NC(Non-Coherent) transaction initiators
  - Software(SW) agents – BIOS, application, driver etc
  - Hardware (HW) agents - CPU, power unit etc
- Complex SOC
  - Numerous agents, access paths
  - 1000’s of registers



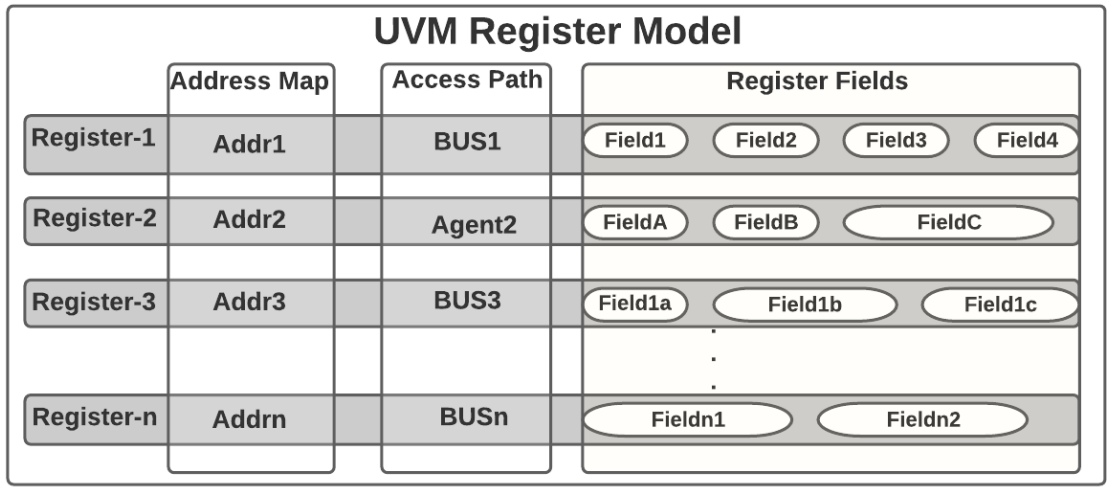
SOC advancement

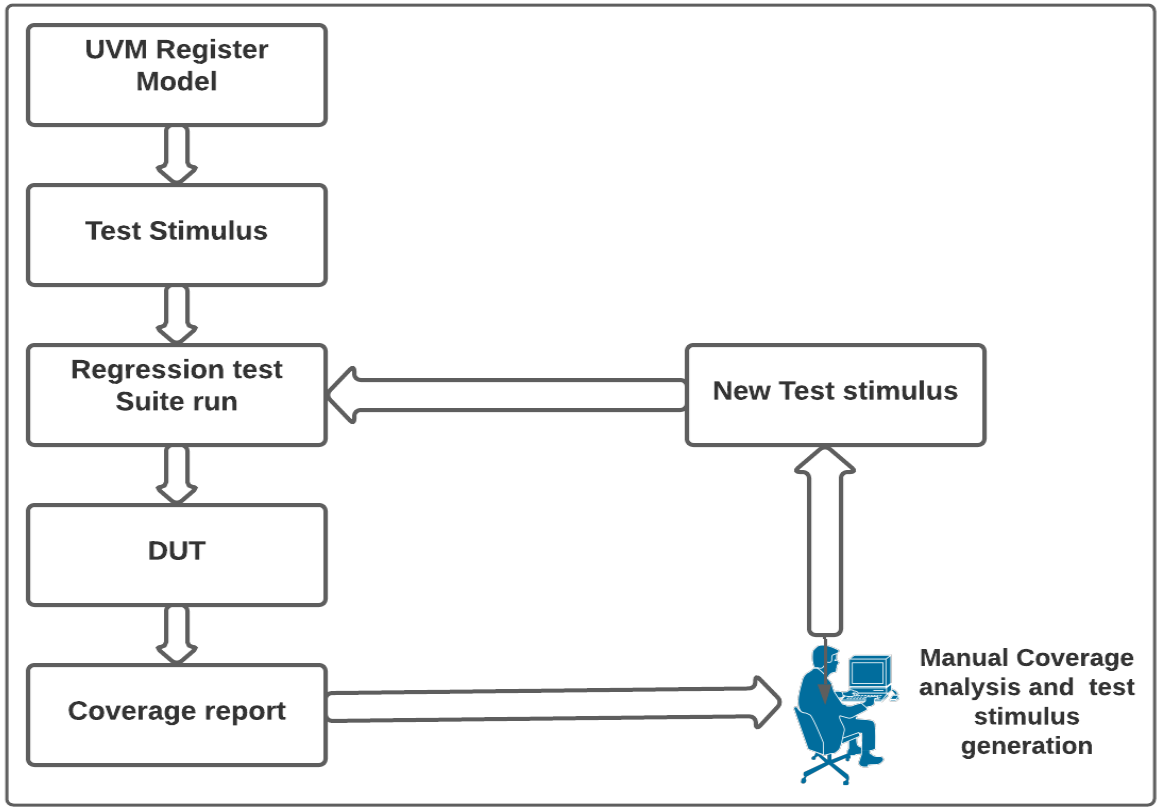
Increase in NOC complexity

Increase in NC access path complexity

Existing Solution

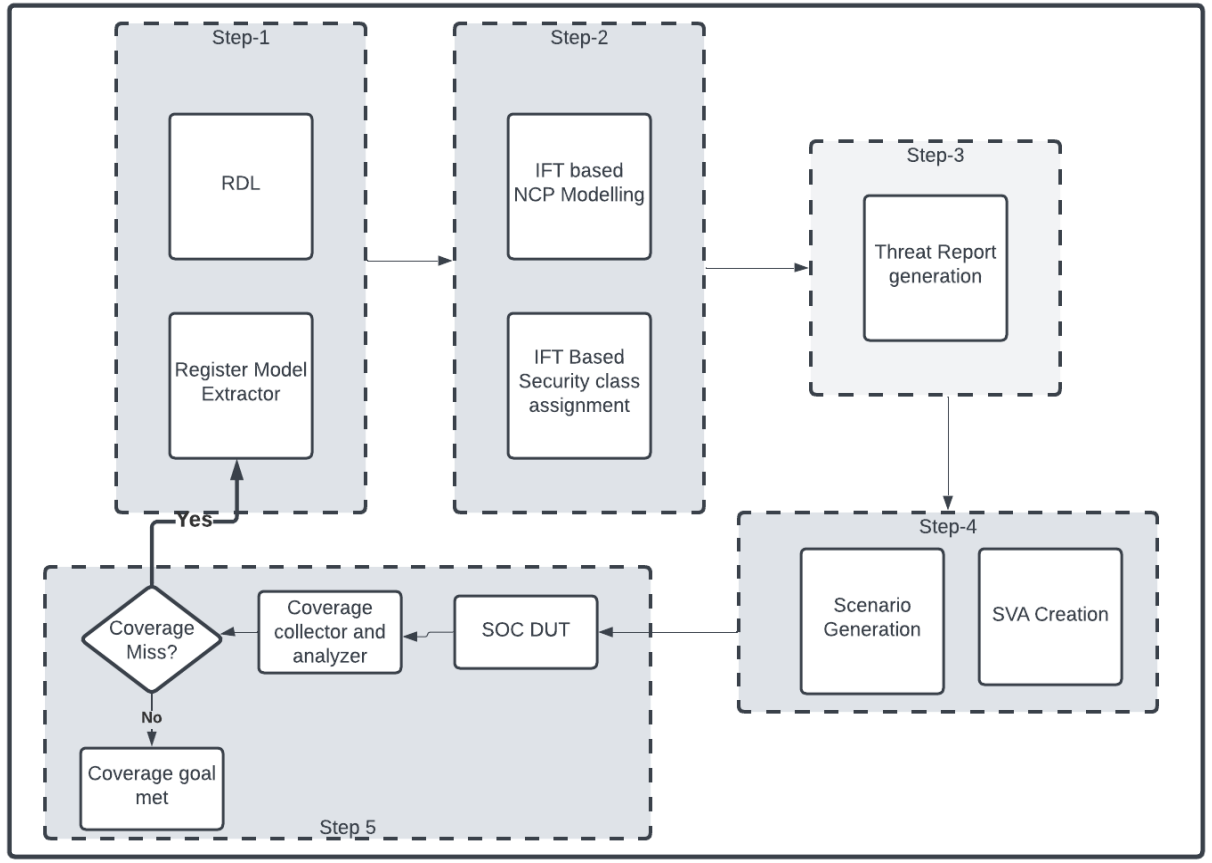
- RAL(Register Abstraction Layer) based approach
- Pros
  - Generic approach
- Cons
  - Complex modelling
  - Performance degradation – run time increases exponentially with the increase in the no of registers to validate





Proposed Solution

- Step 1: Register attributes generated for all SOC registers
- Step 2: Register is assigned to the security class and its NCPs
- Step 3: Generate a threat report for the NCPs that are not within the trust boundary.
- Step-4: Generate negative test scenarios from the threat report to verify it on the SOC design. SVAs are also created in this step.
- Step-5: Validate the threat scenarios on the DUT using the SVA (simulation, formal, etc)



Information Flow Tracking[1]

- Information Flow Tracking(IFT):
  - The core concept of the IFT technique is to represent the information/data flow propagation across the system by labeling the data objects with a security class and tracking the label during data calculation.
- It verifies or controls data movement by implementing security flow regulations,
  - where an information Flow Model (FM) is established,
  - Describing the permissible flow of information among N data objects using the security class SC and flow relation.
- An informative flow model FM, is specified for the DUT

1. M. K. Munigala, S. Sood, M. K.N and K. Baladaniya, "A Novel Security Vulnerability Detection Mechanism Using Information Flow Tracking on a Complex SOC," *2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Gold Coast, Australia, 2022, pp. 1-6, doi: 10.1109/CSDE56538.2022.10089277.

Example

- We have a system with 2 data objects A and B
- Goal: Check for security vulnerability when computing value *C* from *A* and *B*
  - Define the tags, describing the security classes of A, B, and C, respectively.
  - Using the IFT, check if the data from A and B is “allowed” to update security class C, i.e. do the security access rules permit this

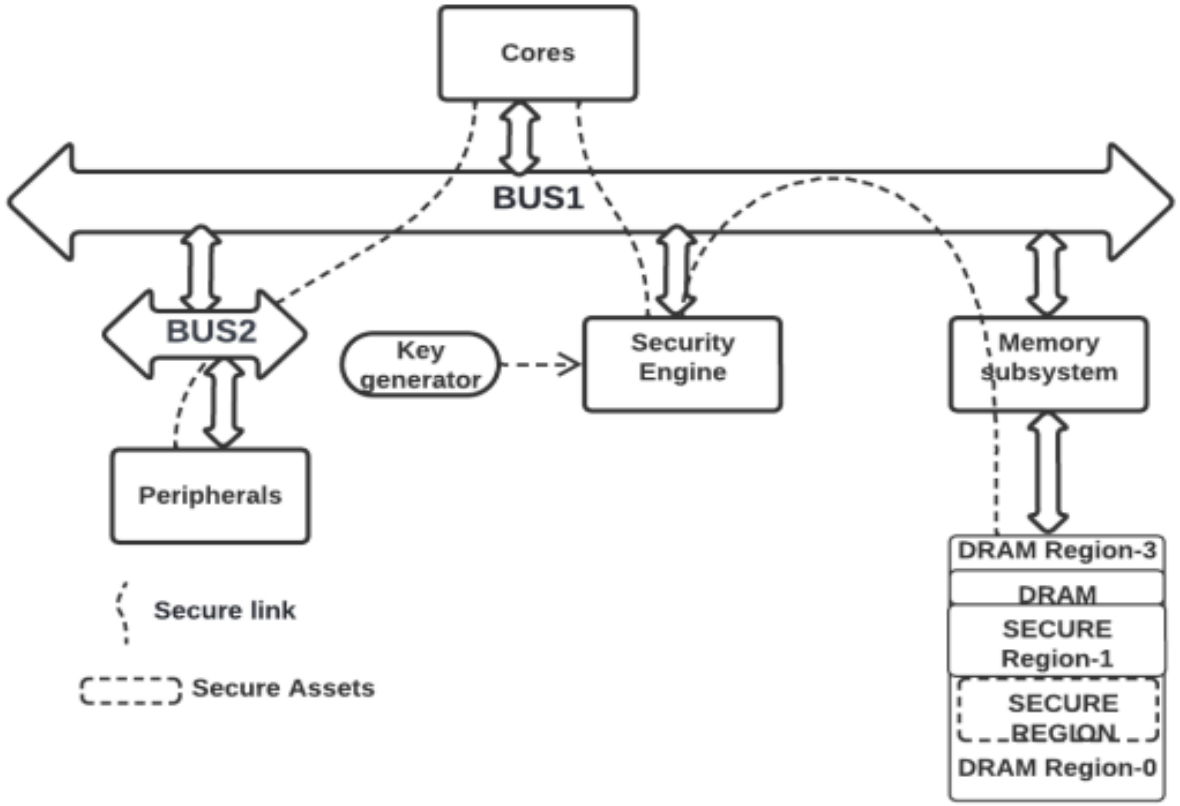
IFT Definition of SOC NCA

- For a given register in SOC, figure out all the NCPs.
- Generate NCA from NCP
- The security of any register is equal to access control security
- NCA is secure if and only if all its NCP’s are in trust boundary to access a specific register.

IFT for SOC

1. Storage objects = SOC registers

2. NCP is a path for data to reach those storage objects



Evidence

Approach is applied on one of the Intel's SOC

S.No	*Parameter*	*Proposed framework*
1.	No of NCAs Validated	10000
2.	No of NCPs Validated	20000+
3.	Test-generation time	150 Minutes per 10000 threat scenarios
4.	No of IPs/Components explored	4 HW agents and 3 SW agents
5.	Development effort	3 Weeks (Framework)
6.	Portability	Simulation, emulation and Post Si
7.	Corner case bugs	5