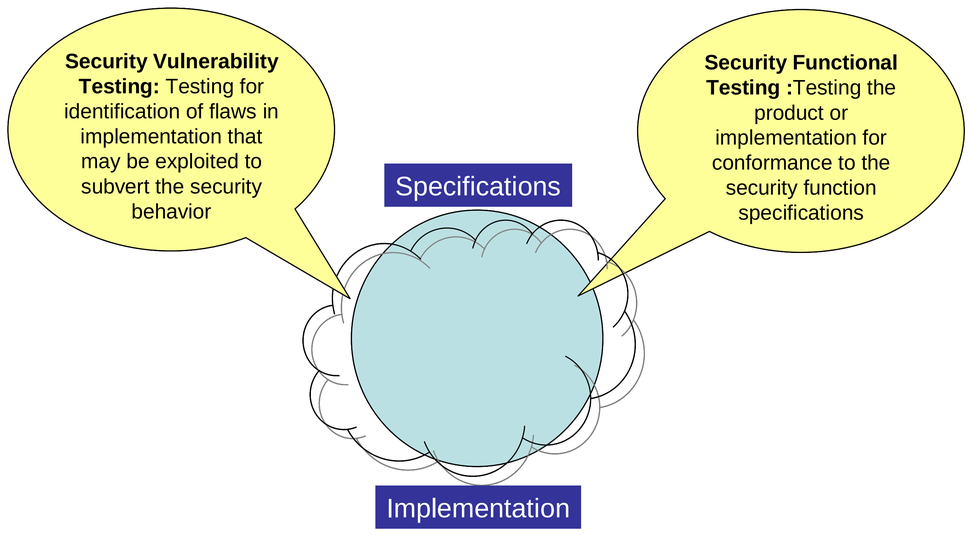
CERIAS

Security Based Testing of Access Control Systems

Ammar Masood,Rafae Bhatti, Aditya Mathur and Arif Ghafoor

Security Testing :-Testing whether the product meets its specified security objectives.

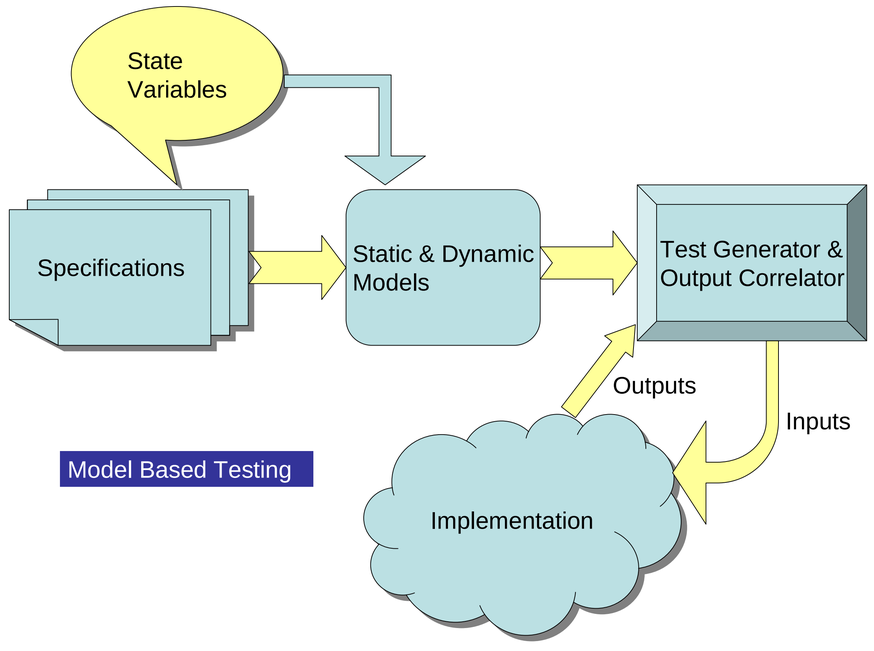


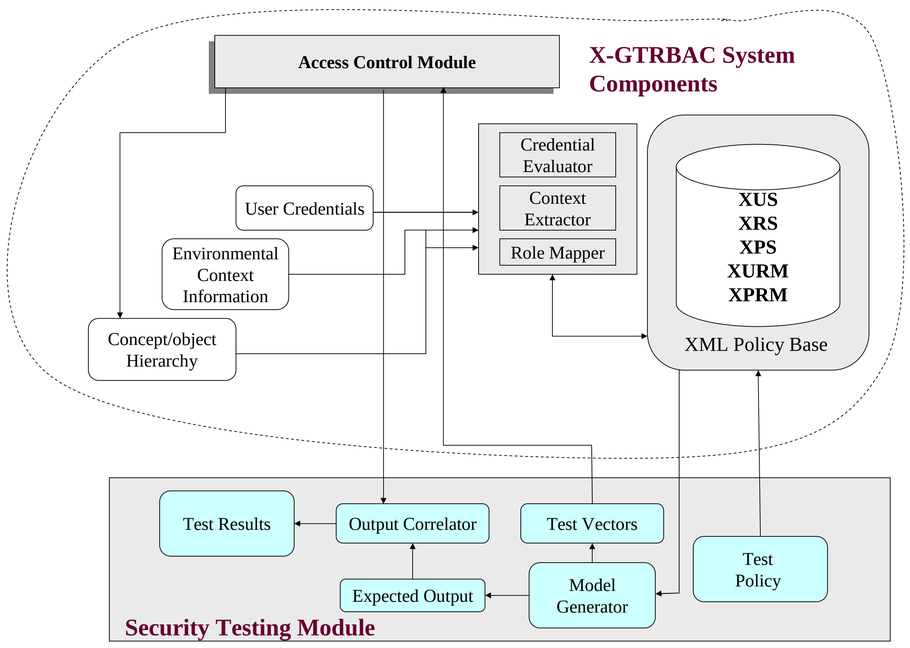
Model Based Security Testing

- Set of state variables used to represent system security state
- Specifications drives the distinction between Secure/legal states and insecure/illegal states.
- The objective of Security testing is two pronged
  - Validating that implementation stays in valid secure states as transitions are taken e.g. a single user role activation from initial state leads to state in which only that activation exists and no others
  - Confirming that systems does not enter into insecure states e.g. if an Separation of Duty constraint exists between two state variables then verifying its correctness by generating such transitions which can take the system to insecure states.

Models for Role Based Access Control

- Structural Model:- It is the static representation for the policy and relates to user-role assignments, role-permission assignments, static SOD constraints and Static cardinality constraints.
- Behavior Model:- It models the functional behavior and thus represents system state changes as a result of user-role activation while constrained by role hierarchy, dynamic Separation of Duty and cardinality constraints.
- **Types of required tests**
  - Tests to verify the static Structural Model
  - Tests to verify dynamic Behavior Model





Steps in Testing

1. Identification of State Variables
2. Generating and executing tests corresponding to structural model
3. Developing the system behavior model from the specifications (effectively a Finite State Machine Representation)
4. Generating Test Sequences i.e. A complete Test Suite from the dynamic model
5. Executing test sequences on the implementation