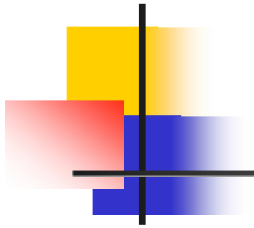
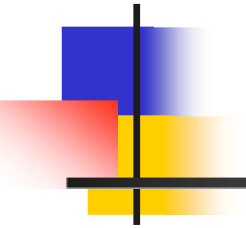


CSE 543

Information Assurance and Security



IA Applications of Formal Methods

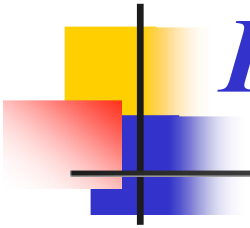
Professor Stephen S. Yau

Fall 2022

IA Applications of Formal Methods

- ***Objective:***

More precisely determine the requirements, and analyze the information system so that ***security incidents can be prevented or at least identified.***



IA Applications of Formal Methods

Step 1*: System Specification: *Abstraction and modeling with a well-defined syntactic and semantic structure for system to operate.

IA Applications of Formal Methods

Step 2: Requirement Specification: Security modeling (e.g., BLP model) to represent the security requirements ***unambiguously.***

IA Applications of Formal Methods

Step 3*: *Validation: Formally validate the system with respect to its requirements.

- ***Model checkin***g (by searching the satisfiability of the given characteristics of the system in the possible models)
- ***Theorem proving*** (by inference of given system characteristics using syntactical inference rules in theory proving)

Formal Methods – Modeling

- Abstract representations of a system using mathematical entities and concepts
- **Modeling: C*apture essential system characteristics and ignore irrelevant details***
- Model can be used for mathematical reasoning to prove system properties or predict new behavior
- Two types of models: continuous and discrete

Formal Methods – Modeling

- ***Advantages of using formal specification***:
  - Clarify ***requirements and design***
  - Articulate ***implicit assumptions***
  - Identify ***undocumented or unexpected assumptions***
  - Expose ***defects***
  - Identify ***exceptions***
  - Evaluate ***test coverage***

Formal Methods – Generating Formal Specifications

- Need ***to translate non-mathematical description*** (diagrams, table, natural language) ***to a formal specification language***
- The specification is a ***concise and precise description of high-level behavior and properties of a system***
- Well-defined language ***semantics*** are needed to support formal deduction of specification

Formal Methods – Generating Formal Specifications (cont.)

- Types of formal specifications,
  - ***Model oriented:*** Based on a model of the system behavior in terms of mathematical objects, like sets, sequences, etc.
    - Statecharts, SCR (Software Cost Reduction), VDM (Vienna Development Method)
    - Petri nets, automata theoretic models

Formal Methods – Generating Formal Specifications (cont.)

- Types of formal specifications (cont.)
  - ***Property oriented***: Based on a set of properties sufficient to describe system behavior in terms of axioms, rules, etc.
    - Algebraic semantics
    - Temporal logic

Formal Method – Role in System Design and Engineering

- Motivated by the expectation that performing appropriate mathematical analysis can contribute to the reliability and robustness of an information system design

* *https://en.wikipedia.org/wiki/Formal_methods*

Formal Method – Role in System Design and Engineering (cont.)

- Formal specification of an information system may be used as a guide while the system is being developed.
  - If the formal specification is in ***operational semantics*** (executable), the observed behavior of the system can be compared with the behavior of the specification.
  - If the formal specification is in ***axiomatic semantics***, the pre-conditions and post-conditions of the specification may become assertions in the executable code.*

* ***https://en.wikipedia.org/wiki/Formal_methods***

Formal Methods – Bell-LaPadula (BLP) Model

- For ***enforcing access control*** in information systems and built on the concept of a ***state machine with allowable states in a computer system***.

http://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model

Formal Methods – Bell-LaPadula (BLP) Model (cont.)

- The model defines ***two MAC rules and one DAC rule with three security properties:***
  - Simple Security Property - a subject at a given security level ***may not read*** an object at a higher security level (**no read-up**)

Formal Methods – Bell-LaPadula (BLP) Model (cont.)

- ★-property ("star"-property) - a subject at a given security level ***must not write*** to any object at a lower security level (**no write-down**)
- Discretionary Security Property - use of an access matrix to specify the discretionary access control. ***http://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model***

Limitations of Formal Methods

- Requires sound mathematical knowledge of the developer
- Different aspects of a design may be represented by different formal specification methods
- Useful for ***consistency checks***, but cannot guarantee the ***completeness*** of a specifications