PARTIAL ORDERS vs LATTICES FOR DATA SECURITY MODELS

By Luigi Logrippo (luigi@uqo.ca)

Université du Québec en Outaouais
University of Ottawa

June 2019

Lattice theory for data security:
Historical basis

- In 1976, Dorothy Denning published a famous article:
  - *A Lattice Model for Secure Information Flow*
  - Communications of the ACM, May 1976, Vol. 19, No. 5, 236-243

Abstract of Denning's paper

This paper investigates mechanisms that guarantee secure information flow in a computer system. These mechanisms are examined within a mathematical framework suitable for formulating the requirements of secure information flow among security classes. The central component of the model is a lattice structure derived from the security classes and justified by the semantics of information flow. The lattice properties permit concise formulations of the security requirements of different existing systems and facilitate the construction of mechanisms that enforce security. The model provides a unifying view of all systems that restrict information flow, enables a classification of them according to security objectives, and suggests some new approaches. It also leads to the construction of automatic program certification mechanisms for verifying the secure flow of information through a program.

To be precise, it addresses a different context than us.
Most examples are about programs.

+ and -

- The paper used a ‘relational’ rather than state-oriented model
- It correctly pointed out that equivalent entities can be identified
  - “practical assumption of irredundant classes, for A → B and B → A would imply that anything in one class can be moved into the other, whereupon one of them is unnecessary”
- However did not take notice of the fact that what is left after this is a partial order and not necessarily a lattice

Since then

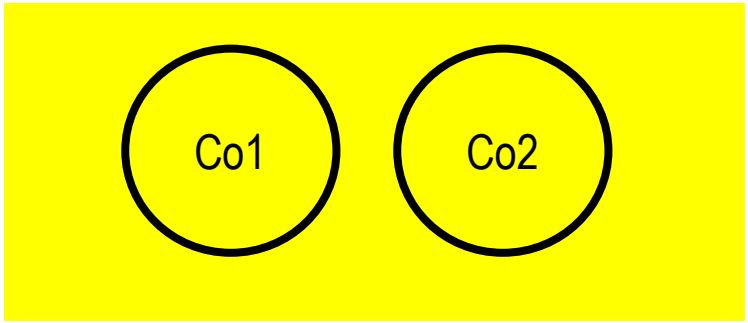
- The lattice model has become **the** universally recognized basic model for access control to data and data flow control for security, search 'Lattice-Based Access Control'
- Numerous scientific papers have developed the 'lattice' idea in many directions
- But we can do better and our solution applies
  - For protecting data security in
    - Organizational networks
    - The Internet of Things (!)

Partial order-based data security

- In several papers, we have shown that simple partial orders, rather than lattices, should be used as basic models for secure information flow
- Start from the following presentation:
  - http://www.site.uottawa.ca/~luigi/presentations/public_presentations/18_FPS.pdf
- A heavier paper:
  - https://www.site.uottawa.ca/~luigi/papers/20_Multilevel.pdf

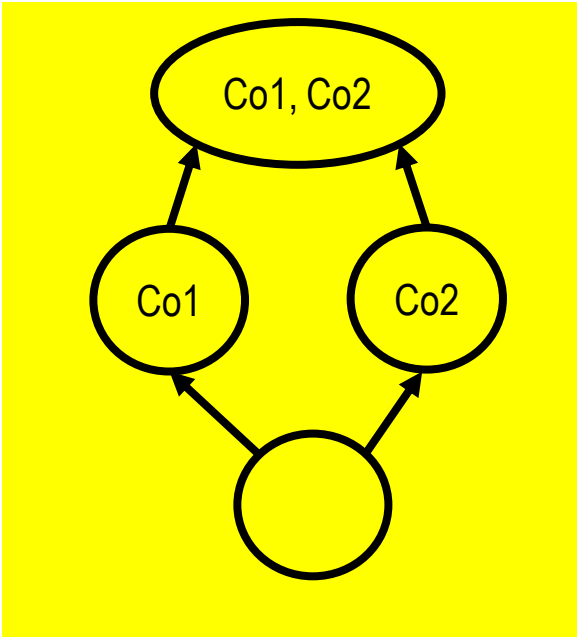
Example 1, with partial orders

- Requirement:
  - Design a very simple system, consisting only of two companies in conflict of interest
- Neither company should receive data from the other
- The partial order model:
  - Two isolated nodes, as desired
- It represents exactly the required network



Example 1, with lattices

- It is necessary to introduce upper and lower bounds for the two entities
  - An entity that can receive data from both companies
    - Contrary to the conflict of interests specification!
  - And an entity which cannot know anything
    - Useless and not mentioned in the requirements
  - The network is now extended to four entities!
    - This cannot be used for implementation
  - The lattice model complicates the system unnecessarily



Objections and replies

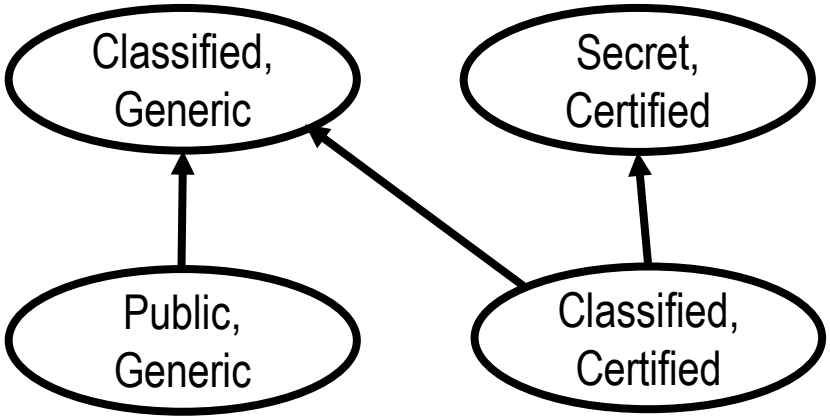
- Objection: But any partial order is embedded in a lattice
- Replies:
  - We don't need lattices, which can be more complicated
    - Can you easily check whether a given structure is a lattice?
    - Lattice properties are not req'd to reason about data security
      - The concept of set union is sufficient
  - The algorithm to complete a partial order into a lattice is non-trivial
    - See « Dedekind-MacNeille completion »
  - Partial orders exist in any directed graph and there are efficient algorithms to find them
    - Tarjan, Kosaraju algorithms

Combining partial orders

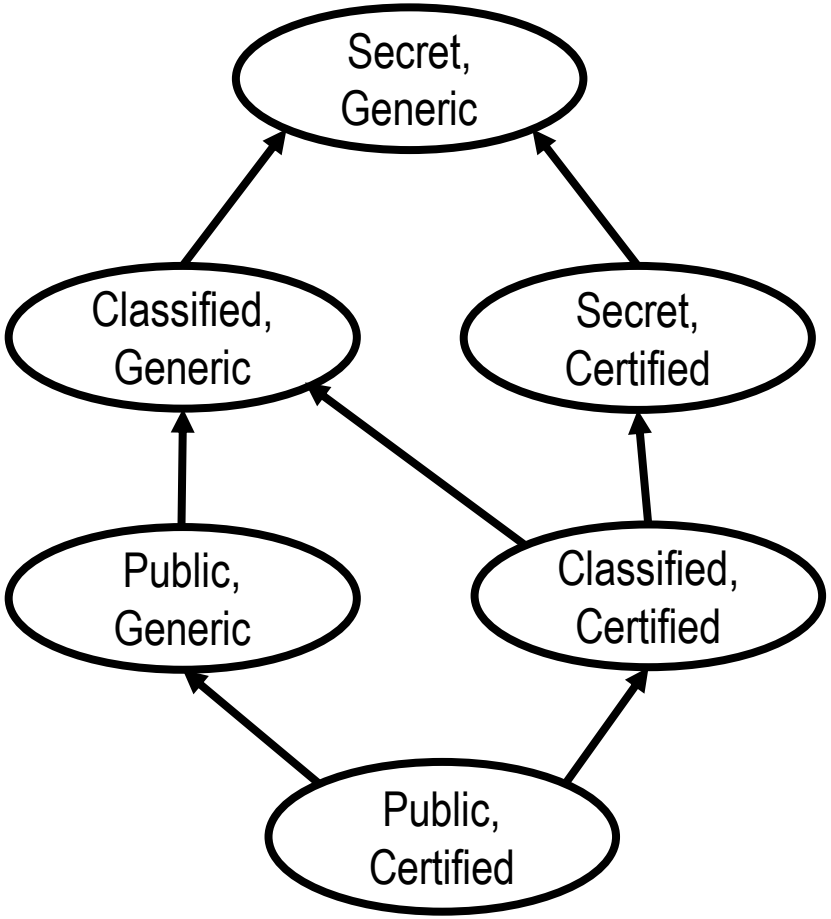
- The product of two partial orders is a partial order
- Secrecy and integrity constraints often coexist in the same system and can be combined
  - Unfortunately, Bell-La Padula and Biba models are usually presented in contrasting ways and so may appear to be incompatible

Example 2: Combining secrecy and integrity

- Requirements:
  - Secrecy : there are three secrecy levels, with the following allowed flow:
    - Public → Classified → Secret
  - Integrity : there are two integrity levels, with the following allowed flow:
    - Certified→Generic
- At right is an example where only four of the six possible combinations are used



All possibilities (doesn't need to be a lattice)



Both *secrecy* and *integrity* constraints are satisfied in networks that implement any part of this partial order

Updates

- Another important asset of the partial order model is its tolerance to updates
- Moving entities in a lattice does not necessarily yield a lattice
- But moving entities in a partial order necessarily yields a partial order

Related issue: Data flow vs information flow

- Although much research in this area mentions 'information flow control', often it only addresses 'data flow control'
- Information flow can involve inferences:
  - From data, it is possible to infer information, which can then become data, etc.
- The problem of information flow control is more complex
  - It involves checking all inference possibilities, which can be many and unknown

Summing up on this and related research

- In any non-trivial network of communicating entities, each containing data
  - There exists a partial order of ‘more’ and ‘less’ secret entities.
  - This order can be efficiently found.
  - An order can also be efficiently constructed if it is required that some entities must be more secret than others.
  - The same holds for integrity.
  - Orders can be constructed to satisfy both secrecy and integrity constraints.
  - However, the entities that have the greatest secrecy will have the lowest integrity and vice-versa.
  - Also certain combinations of secrecy and integrity constraints may be unfeasible (e.g. if it is desired that the most secret data have also the greatest integrity).

Concluding lesson:

- Revisiting established theory can lead to discoveries