Multi-level access control, directed graphs and partial orders in flow control for data secrecy and privacy

Luigi Logrippo

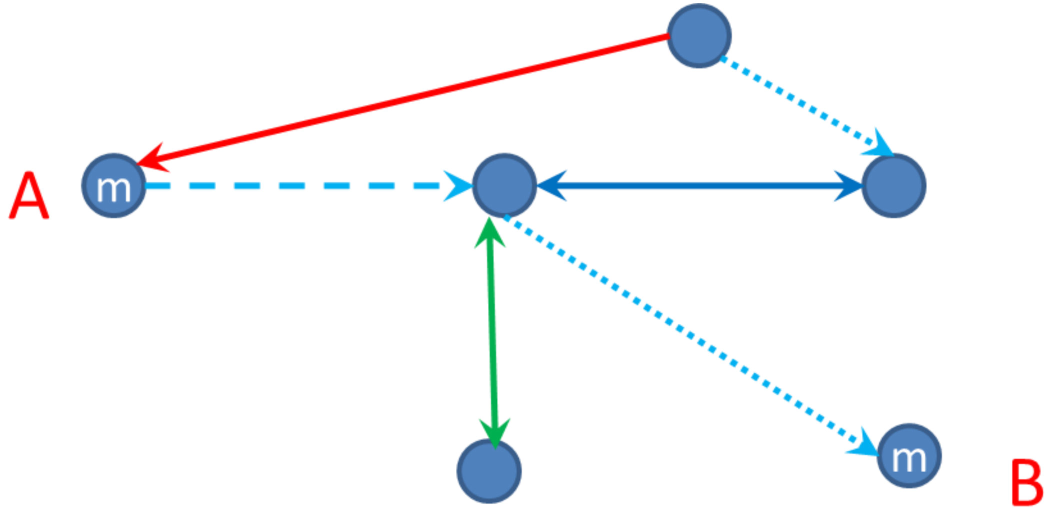
Université du Québec en Outaouais

University of Ottawa

Ottawa-Gatineau, Canada

What is this all about

- Controlling data flows in organizations, for data secrecy and data privacy
- If A knows m, can we conclude that B can also know it?
- If A knows m, how can we prevent B from knowing it?
    - (data privacy will be implied henceforth)



Multi-level systems

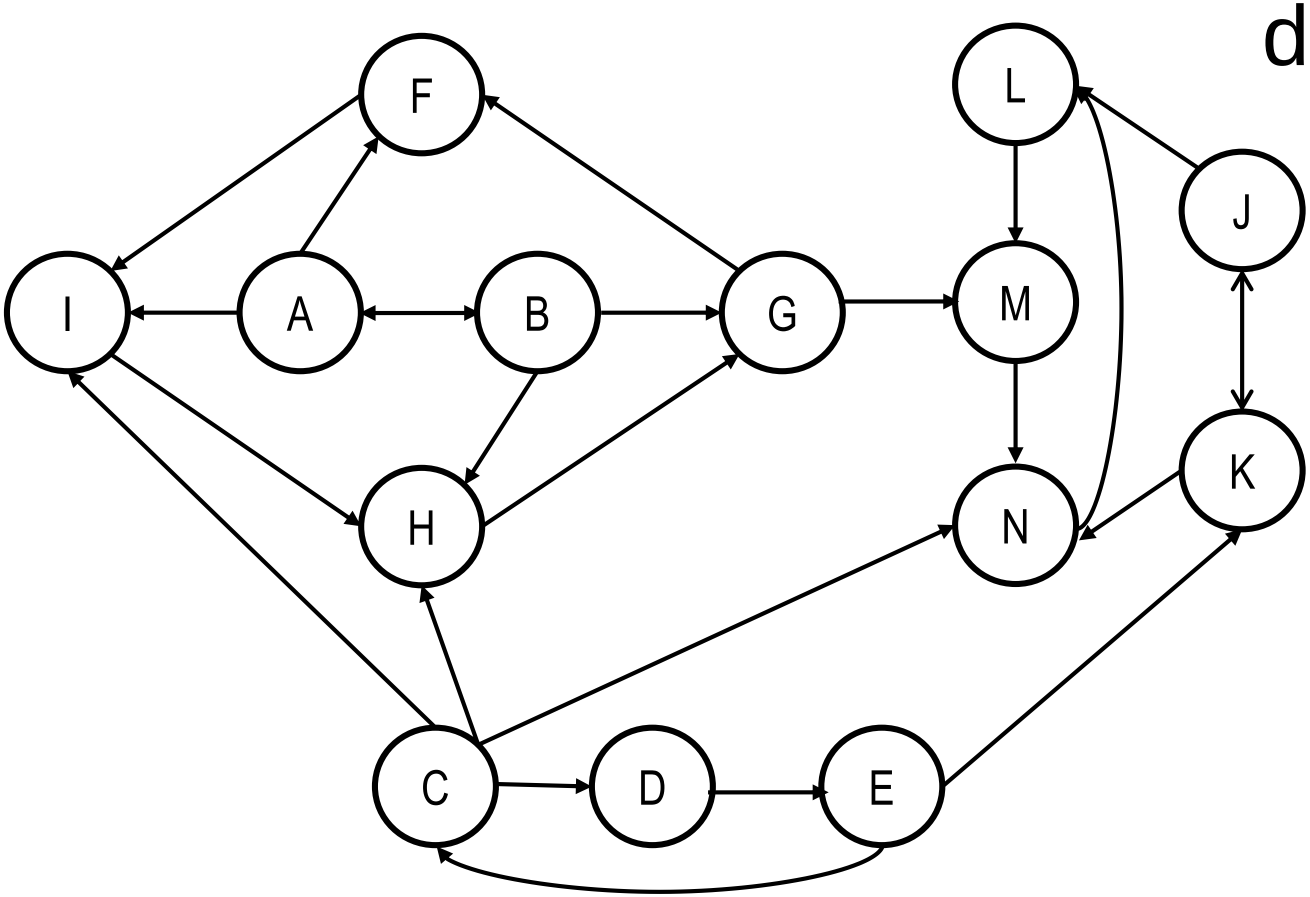
- Everyone knows the Bell-La Padula simple Multi-level system
- This concept has been generalized in many ways, and there is a well-known implementation in SE-Linux
  - *There are hierarchies of subjects and objects and data can move only upwards in the hierarchy*

Sufficient - necessary - available - constructible

- It is well-established that Multi-level systems can guarantee data secrecy
- We show that **Multi-level systems are *necessary* for data secrecy**
  - That is, any system that needs to guarantee data secrecy
  - Whether in the Cloud, in mobility, in RBAC, in ABAC. etc.
  - Needs to implement a Multi-level system
- We also show that all real-life systems are
  - Either one-level with no secrecy
  - Or multi-level with secrecy built-in
- Finally, multi-level systems can be constructed according to needs

Using digraphs to represent data flows

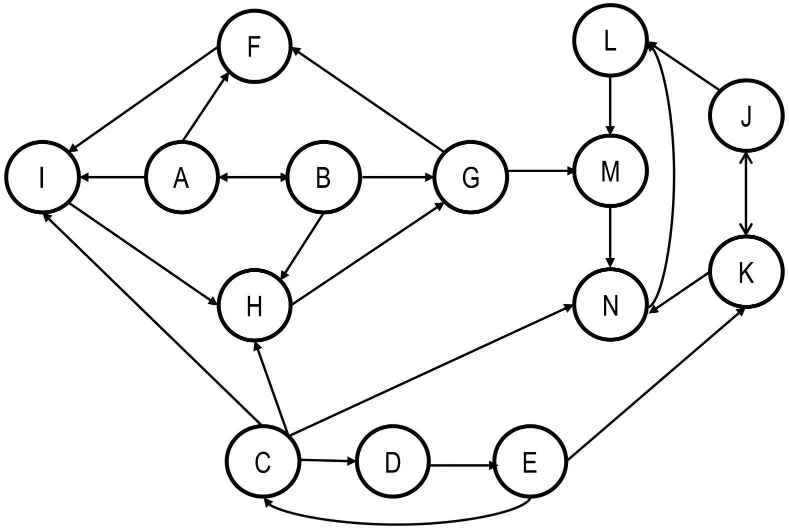
An arbitrary digraph



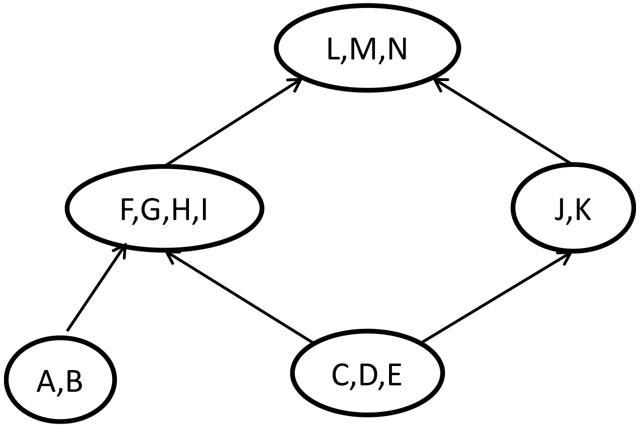
Data flow in a bank, among companies, in a social network, in the IoT …

A digraph for a reflexive, transitive relationship is a partial order of strongly connected components

- Original graph

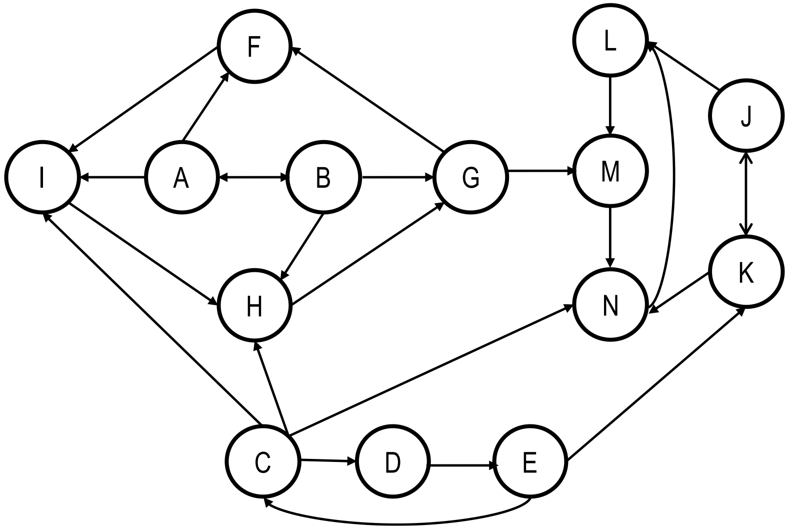


- Partial order

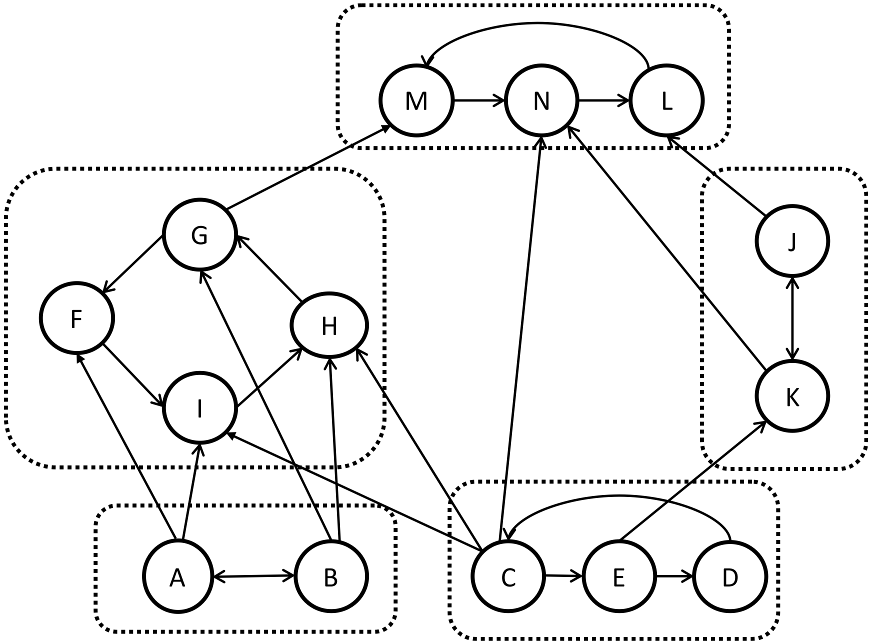


A digraph for a reflexive, transitive relationship is a partial order of strongly connected components

- Original graph

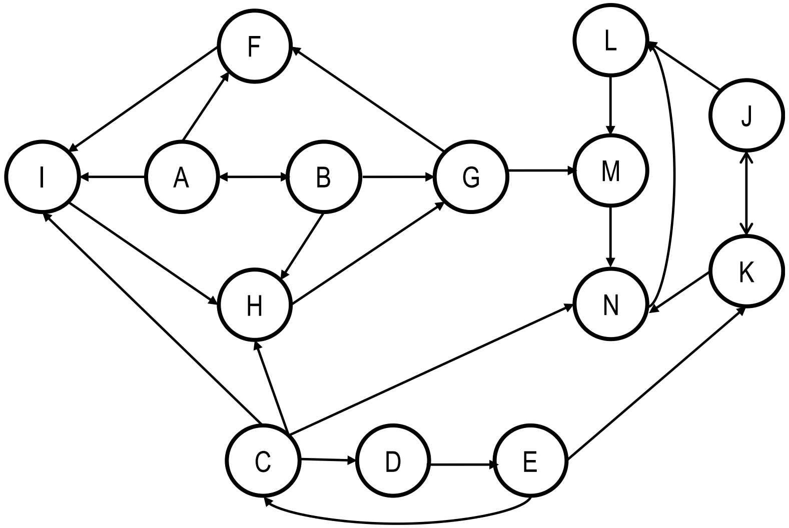


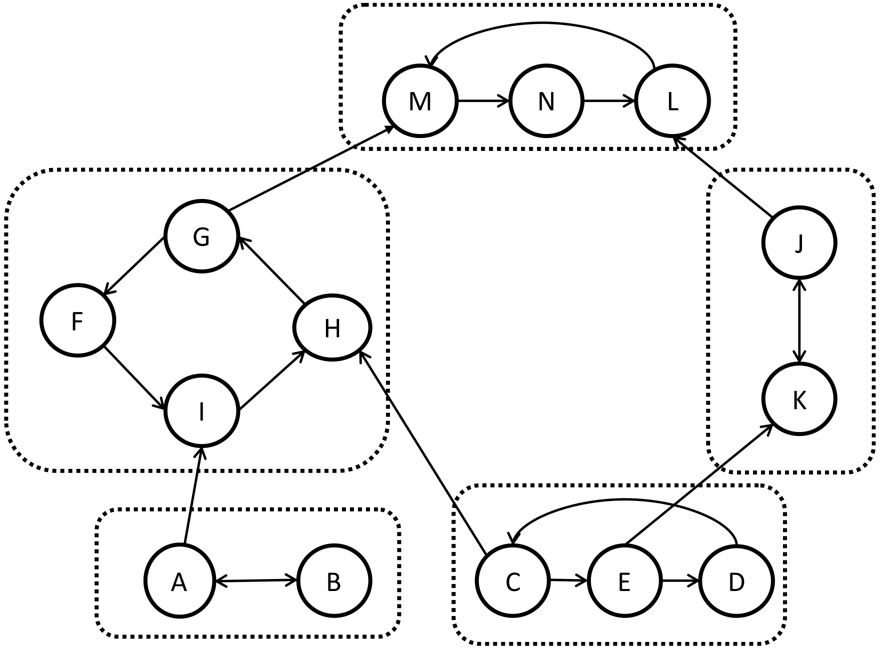
- Reorganized to show partial order of components



A digraph for a reflexive, transitive relationship is a partial order of strongly connected components

- Original graph
- Partial order, reduced paths

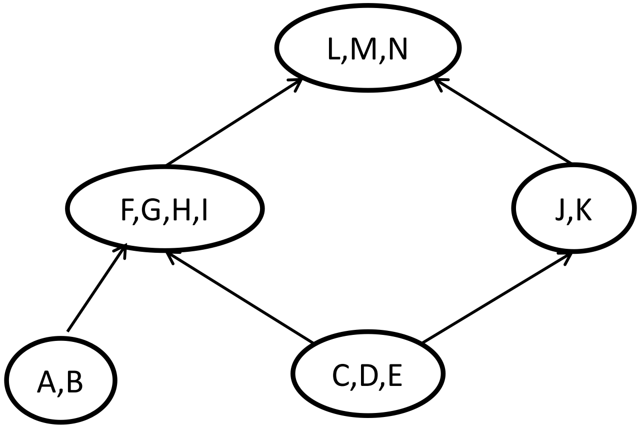


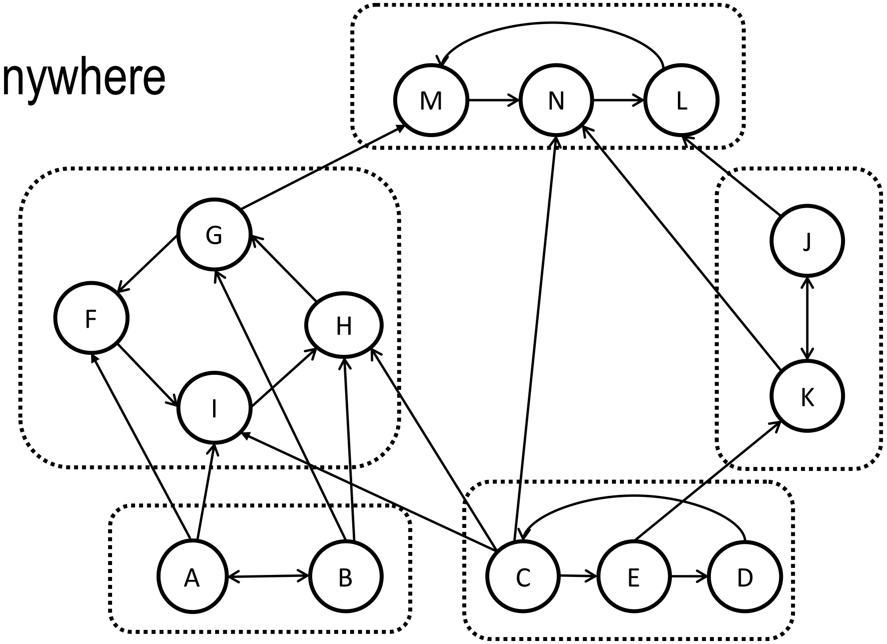


Transitive paths are implied…

For secrecy and privacy

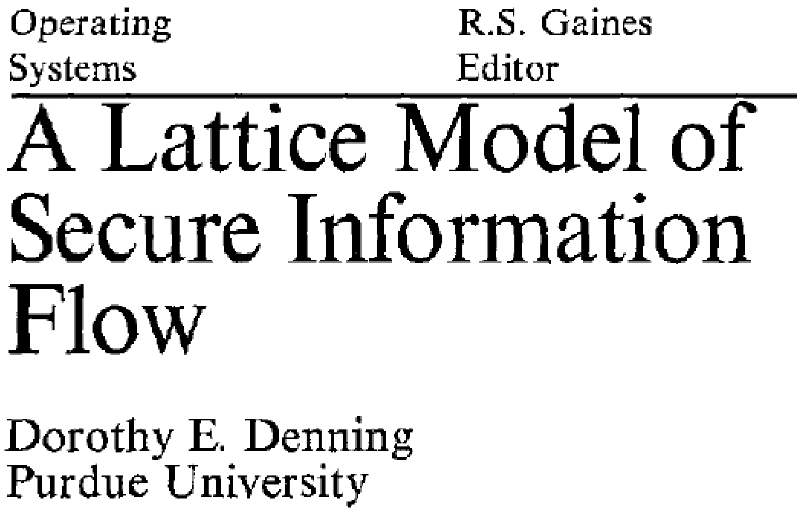
- No secrecy is possible within a single component
  - Anyone can transfer data to anyone else inside strongly connected components
  - If there are several components, then data can move only *upwards*
    - **Secrecy can be defined as the fact that data is constrained to certain components**
  - As ML models say, the most secret data must go where they can move the least, which is the top component(s)
  - The data in the bottom level can go anywhere





Concerning the Lattice Model

- We knew this, isn’t it the lattice model?!



Operating Systems

R.S. Gaines Editor

A Lattice Model of Secure Information Flow

Dorothy E. Denning
Purdue University

1976

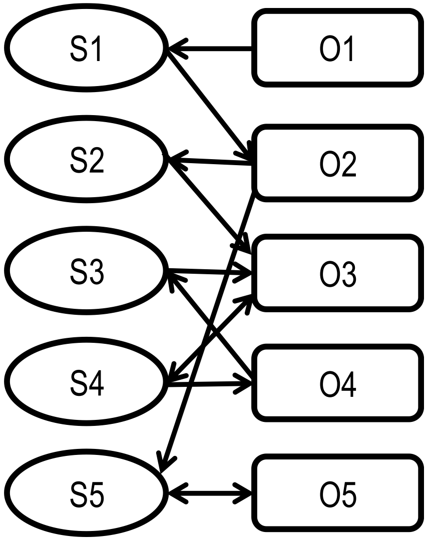
Are lattices a good secrecy model?

- Lattices require joins and meets
  - These don’t normally exist in organizations
  - May force the inclusion of unwanted entities and dataflows
- Lattices don’t tolerate symmetric relationships
  - In our model, these get encapsulated in components
- **« Partial order of components » is a better model than the « lattice model »**
  - **More general, more realistic, more applicable**
    - **Lattices : sufficient, require adaptations**
    - **Partial orders : necessary and sufficient, always exist**

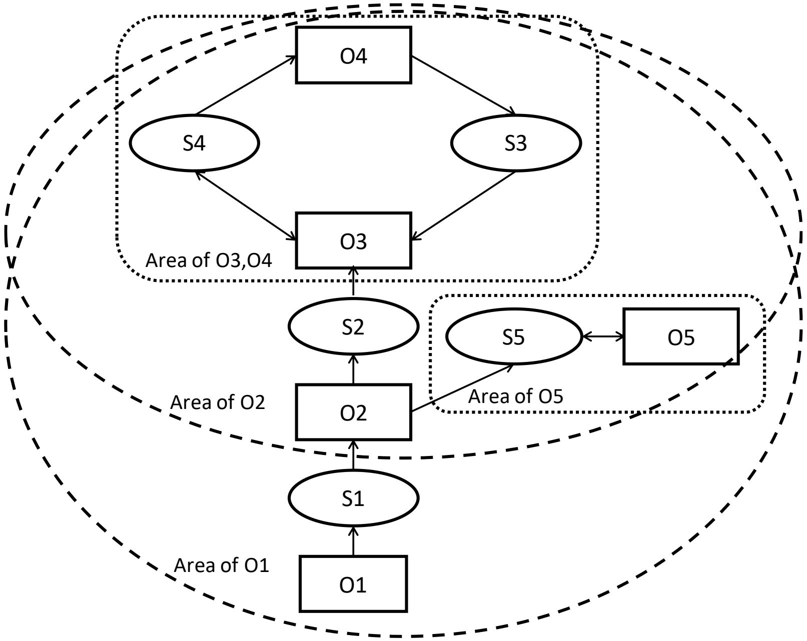
Two interesting problems

- Find the layered model which is inside any access control system
- Given a desired data flow, find an access control system that realizes it

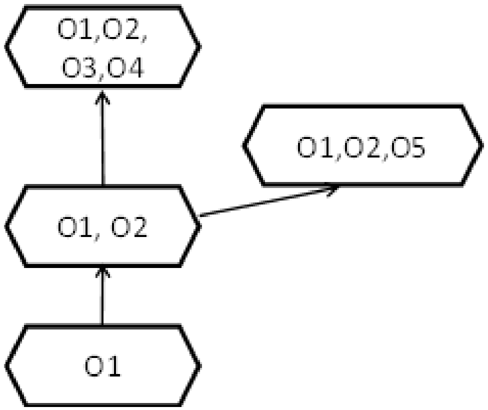
A) Finding the layered model which is inside *any* access control system



An *arbitrary* access control system (maybe RBAC?)



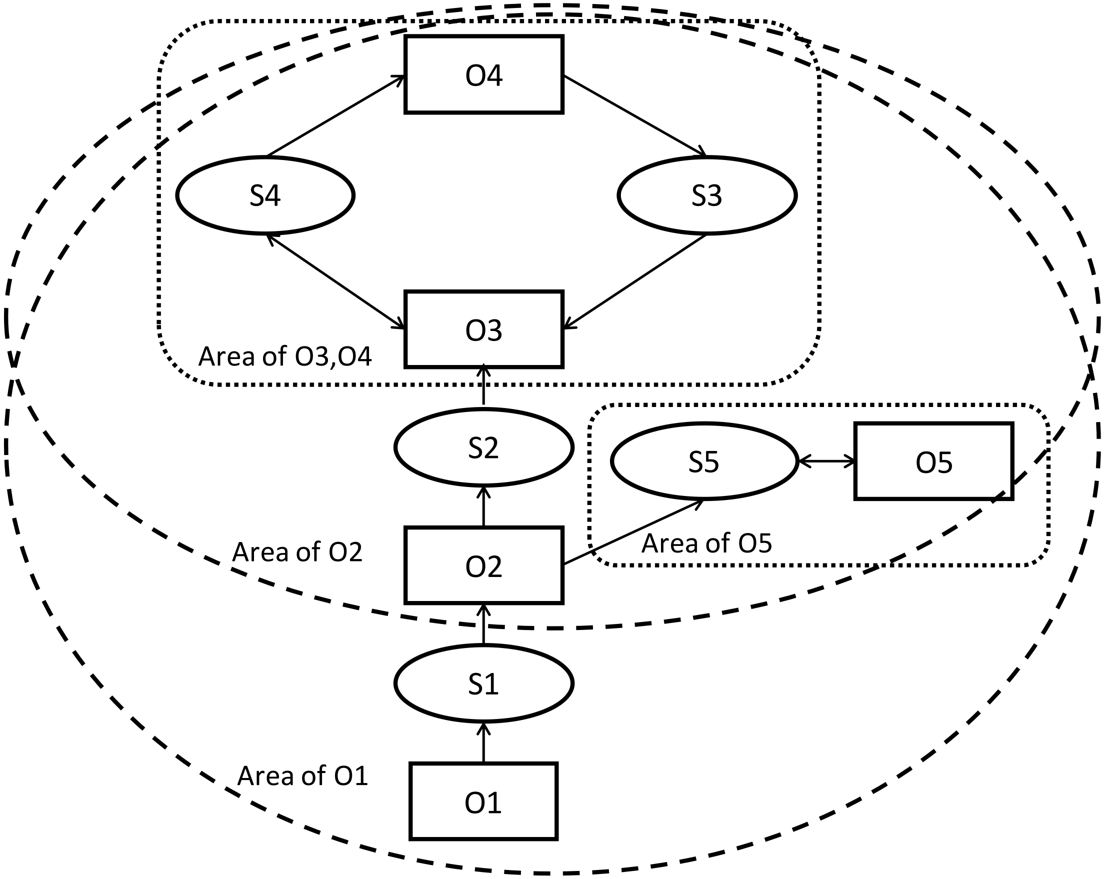
Its partial order (Hasse diagram)



Its schematized data flow (Hasse diagram)

Where would you put the most secret data?

Some interesting points …



The most secret data are those in O3, O4, O5, the less secret are those in O1
S3 and S4 can know the same data, O3 and O4 can store the same data
No subject who knows about O5 can also know about O3 or O4, and v.v.

So …

- Places for secret data always exist and can be found
- However they may not be structured as you want

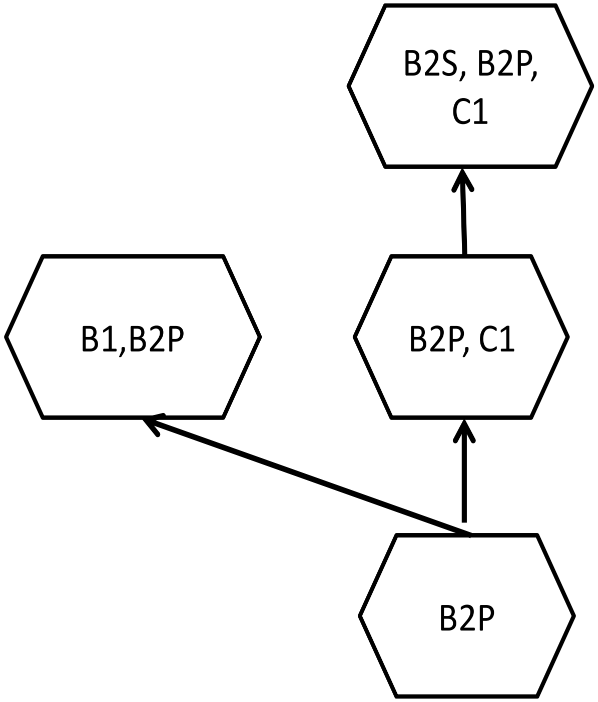
Practical!

- *Polynomial time algorithms* exist *to find data flows* in any access control system specified by:
  - Access control matrices
  - Or roles and permission lists etc.
    - Breadth-first search
    - Tarjan, Kosaraju algorithms
    - Hasse diagram construction algorithm …
- Simulation results show that this can be done in practice for up to tens of thousands of subjects and objects
  - Paper by Stambouli, Logrippo
    - **http://www.site.uottawa.ca/~luigi/papers/19_IPL.pdf**

B) Given a desired data flow, find an access control system that realizes it

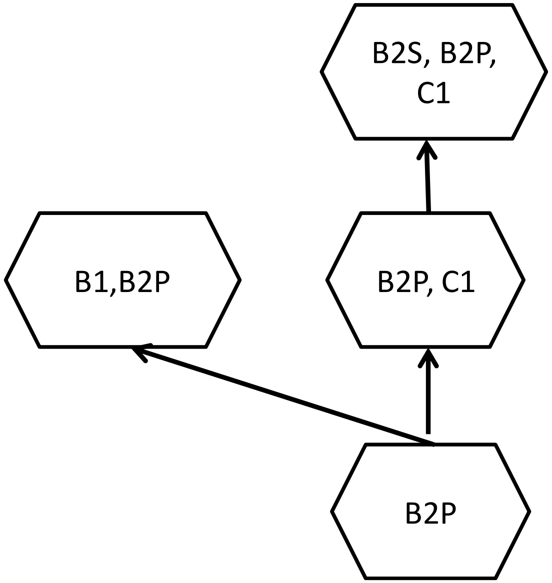
- We have two banks in conflict of interest, *Bank1* and *Bank 2*.
- *Bank1* has only one category of data, called *B1*.
- However *Bank 2* has public data labelled *B2P* that can be available to anyone, and secret data *B2S* that should be available only to its own employees.
- There is also a *Company 1* that collaborates with *Bank 1* and shares all its data *C1* with *Bank 2*.
- However *Bank 2* does not want its secret data *B2S* to be known to *Company 1*.

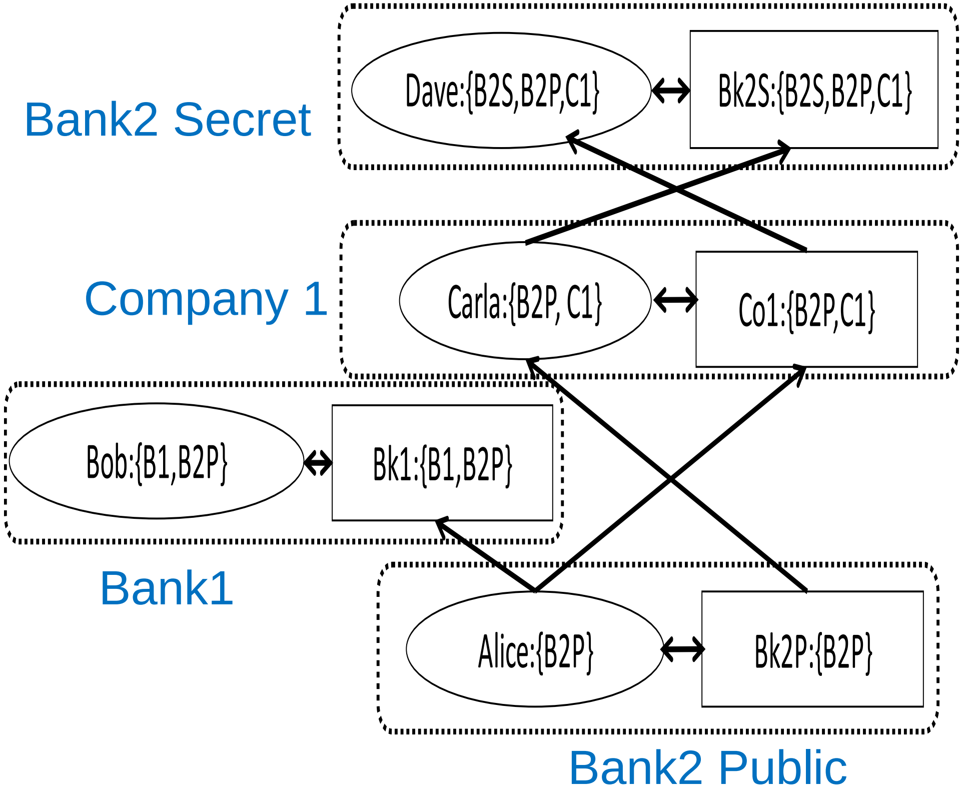
- Data flow diagram



Note partial order of inclusions

An organizational network for the data flow





Problem with Multi-level

- Data can move only up!
- Solution (known in the literature):
  - Certify certain subjects as capable of declassifying data and changing levels
  - A Director can collect all data
    - **Use them to generate directives**
    - **Move to a lower level where she can broadcast directives**

Problem with variability of data flows

- In practical systems, data flows can vary in time because of environmental conditions
- Research problem:
  - Find variation patterns that respect essential partial orders

Synthesis

- Any organizational data flow
- Any access control system
  - Is a partial order of strongly connected components
- Practical algorithms to find the data flows and the partial order exist
  - Given access control matrices or roles with permissions
- Given a desired partial order, it is possible to create an organizational structure for it

For secrecy and privacy

- Given an access control system,
  - We can determine where the most secret/private data should go
- Given a partial order showing privacy levels and conflicts
  - We can construct an access control system for it
- This is a better fitting
- More applicable model
  - Than the traditional lattice model