A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

Dimitrios Sisiaridis
University of Northumbria
Newcastle, UK, NE1 ST
d.sisiaridis@unn.ac.uk

Nick Rossiter
University of Northumbria
Newcastle, UK, NE1 ST
nick.rossiter@unn.ac.uk
http://computing.unn.ac.uk/staff/CGNR1/

Michael Heather
Ambrose Solicitors St
Bede's Chambers
Jarrow NE32 5JB
United Kingdom
michael.heather@cantab.net

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- In modern heterogeneous interoperable systems such as **Distributed Information Systems** (DIS)
  - **higher-order** operations are needed as same conditions applied in different systems may lead to unpredictable results
- **Security** for Distributed Information Systems
  - Can be achieved by securing the processes and the channels used for their interactions and by protecting the resources against unauthorized access

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

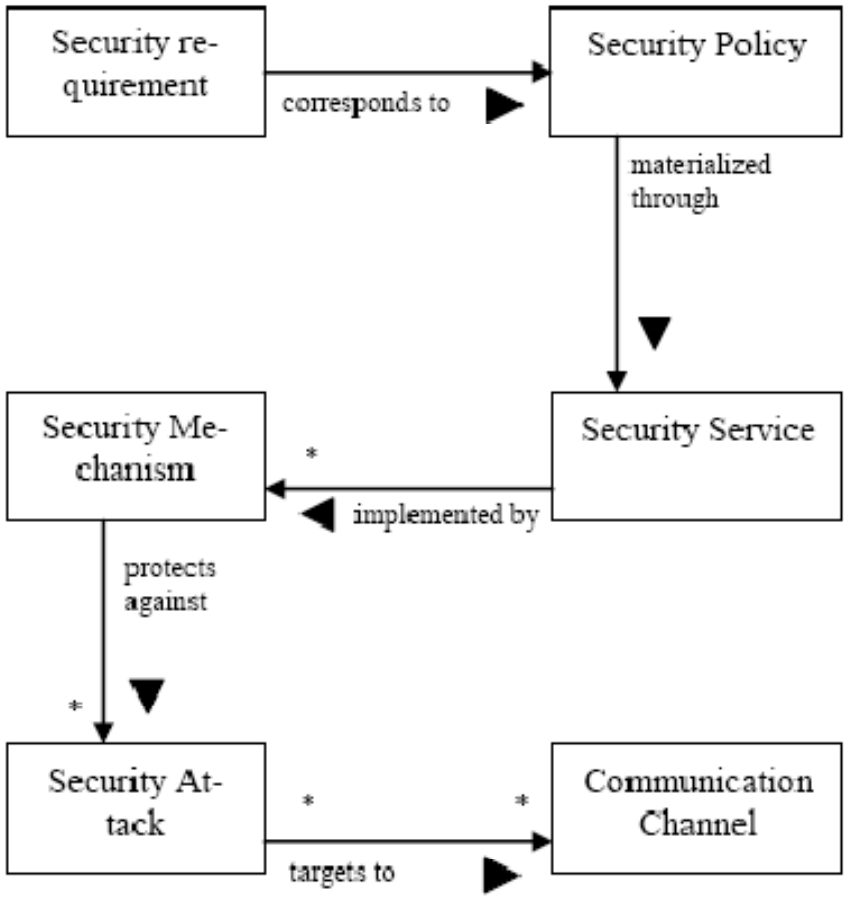

Fig 1: Security in distributed information system

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- Security is a higher order activity, related to issues as:
  - **data integrity**
    - enforcement of database integrity constraints
    - concurrency control
    - backup and recovery procedures, within
    - an overall security and access control framework
  - **interoperability**
    - among complex heterogeneous systems
    - a global requirement of higher order
    - cannot be handled in a complete and decidable manner by axiomatic methods such as first order predicate calculus

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- Current security approaches are characterized by their **locality**
  - They can be seen as **first-order** activities
- Organizations usually respond to security threats on a **piecemeal basis** following hardware and software solutions
  - inevitably leave gaps and generate inconsistencies, which can be exploited by intruders

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- **Bottom-up** approaches, such as *risk analysis* and *risk management*, are subjective
- **Top-down** approaches (e.g. *baseline* approaches), such as *ISO/IEC 27001:2005* specification and the *ISO/IEC 17799:2005 Code of Practice*, leave the choice of control to the user
- A complete security strategy needs to be layered
- A promising solution is to include security considerations as *core processes* of the system itself.

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

– A **holistic approach** with *natural closure* seems necessary to describe a complete and global view.

- Based on the **CIA security principles**, namely *confidentiality*, *integrity* and *availability*
- Focused on securing the infrastructure itself by forcing users to adopt best security practices while ensuring that the system is "*secure by design*" rather than by post-rational customization

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- In the context of Distributed Information Systems
  - A **distributed computation** *M,* e.g. a *distributed transaction*, is composed of a dynamic group of **processes** *P* running on different resources and sites expressed in the form of a group of **communication channels** *W*
  - The processes *P* :
    - Have a disjoint address space
    - Communicate with each other by **message passing** via *W* using a variety of mechanisms, including unicast and multicast

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- **Category theory** provides a formal approach to process simply by the use of the **arrow**
  - It is inherently holistic
  - and with intrinsic natural closure
- A **category**：
  - A *class*, consisting of arrows between objects
  - It provides a much greater power than functions between sets
  - It is also of the nature of a *type*

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- Fundamental category theory shows that for physical existence the real world operates as a **Cartesian Closed Category** (that is a category of *real world objects*)
- It has been shown in previous work that, any realizable system can be conceptually expressed using *four interchangeable levels* in categorical terms (Figures 2 & 3)

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

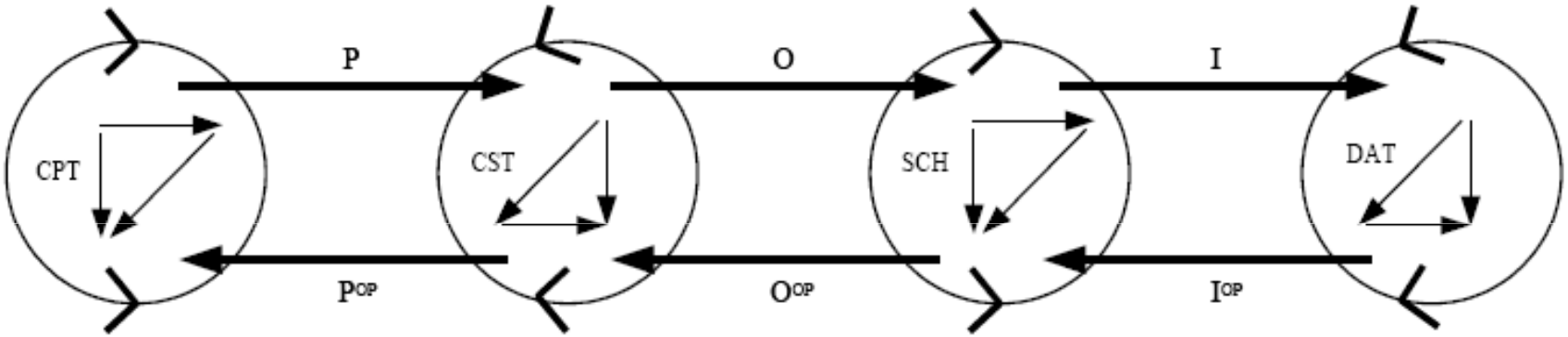

Fig 2: Natural composition of adjoint functors

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

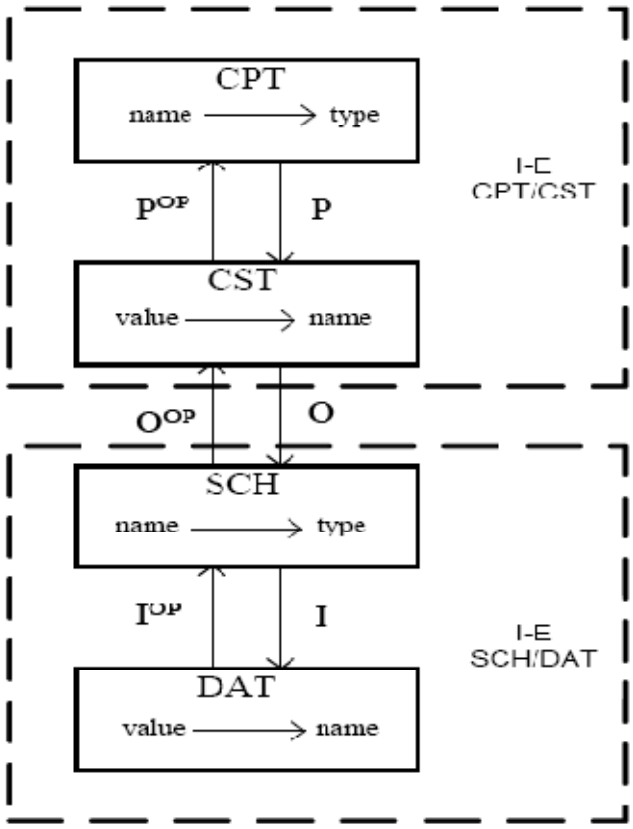

Fig 3: Four levels defined with contravariant functors and intension-extension pairs

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- **Adjointness** characterizes the unique relationship between these *Cartesian Closed Categories*
  - *Interoperability* is expressed in terms of the adjunction of the adjoint functors in Figure 4.
  - *Naturality* is based on the ordering and interoperability of the two free and open represented category systems
- From an **application** viewpoint, a useful view of an adjunction is that of *insertion in a constrained environment*
  - The unit η can be thought of as quantitative creation, the counit ε as qualitative validation (Figure 5)

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

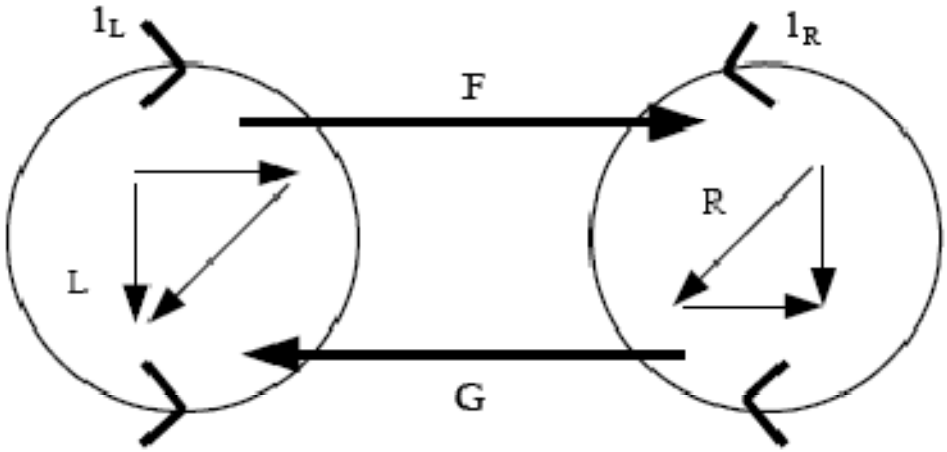

Fig 4: Adjointness between two systems

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

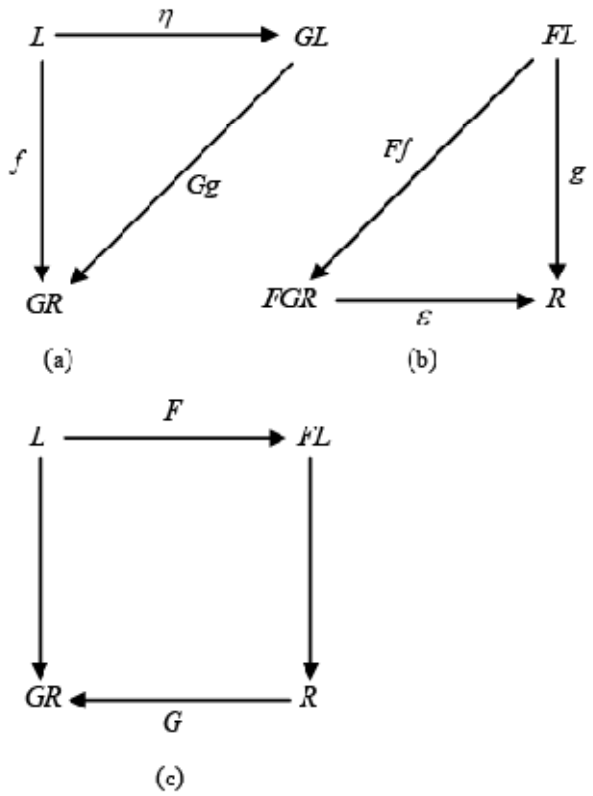

Fig 5: Adjointness between two systems L & R
(a): the unit of the adjunction,
(b) the co-unit of the adjunction,
(c) adjoint functors *F* & *G*

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- The proposed **Holistic Security Framework** is developed in two parallel stages
  - In **stage 1**, security entities such as objects and object hierarchies are *categorified* into Cartesian Closed Categories.
  - In **stage 2**, distributed computations, e.g distributed transactions, between processes or groups of processes (each one consisted of a series of events), can be broken up into a *series of composed adjoints*

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

- The holistic security architecture, in categorical terms, can be visualized as **mappings between pairs of adjoint functors**
- For **example**:
  - *Local extensionalities*, e.g. local security policies in the form of **comma categories**, are interconnected one with another through *global intentionality* e.g. global security policy or meta-policy framework

A Holistic Security Architecture for Distributed Information Systems – A Categorical Approach

– Summary

- Current security approaches are characterized by their **locality** and are based on **axiomatic set theory**, which offend Gödel.
- **But**, security for heterogeneous distributed information systems is based on **higher order** activities.
- The object-oriented approach, in the context of distributed information systems security, needs to be founded in **applied category theory** to be **complete** and **decidable**
- A **holistic**, modular security approach provides *natural closure* and follows the '*process*' approach of the DIS itself