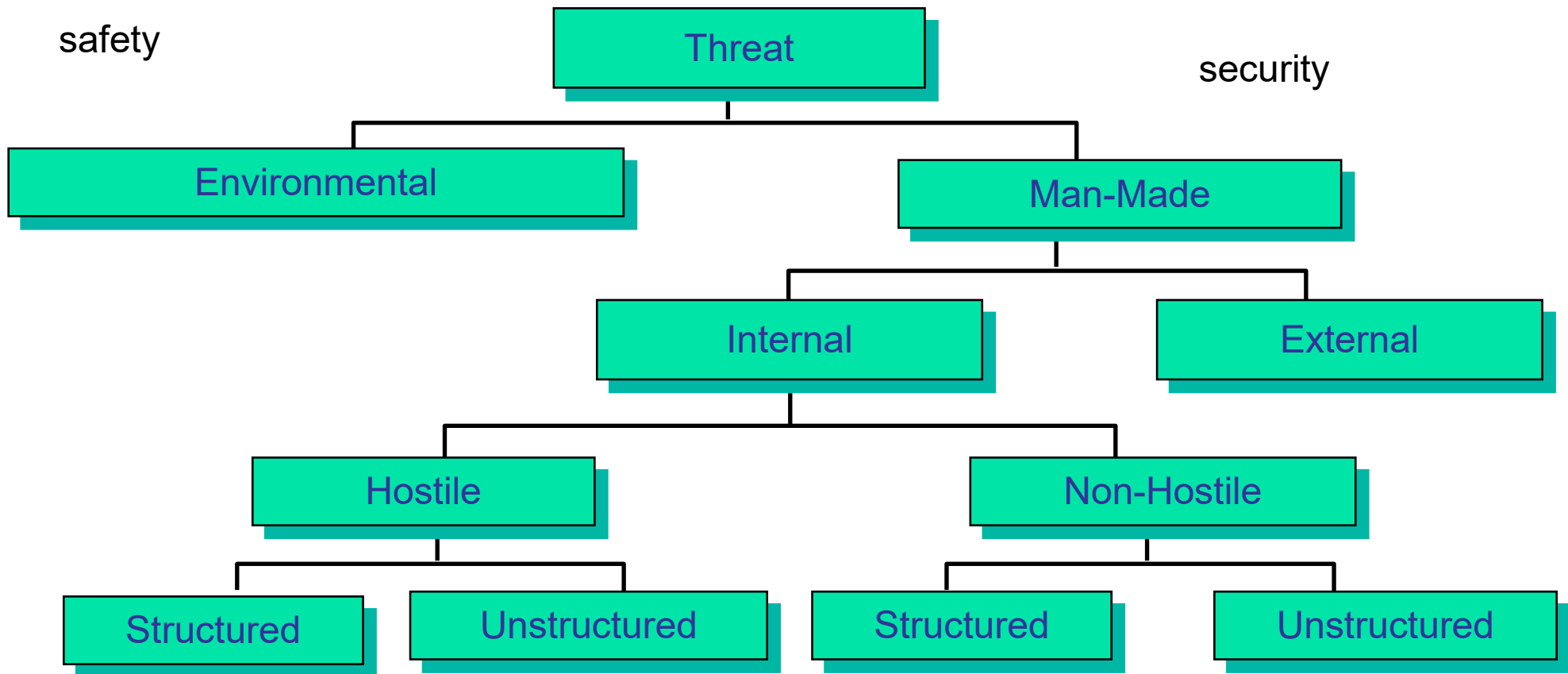# Threat Analysis

Threat analysis

- It has to determines the enemies of a system
  - Who is interested in attacking the system
  - Who can access the resources to attack a system
  - What are the events that may involve the system
- It determines the threats (classes) and the agents in each class
- If there is not a threat that can exploit a given vulnerability, then the assessment may neglect such a vulnerability
- It is strongly related (it may be interleaved with) the attack analysis (is there anyone that can implement this attack?)

A threat taxonomy

safety

security

```
                          Threat
                    ┌───────────┴───────────┐
              Environmental              Man-Made
                                    ┌────────┴────────┐
                                Internal          External
                          ┌─────────┴─────────┐
                       Hostile           Non-Hostile
                    ┌─────┴─────┐       ┌─────┴─────┐
              Structured  Unstructured  Structured  Unstructured
```

Threat analysis

- For each agent, the analysis determines
  - The agent goals= rights on components
  - The resources the agent can access
    - Tecnological
    - Information (security through obscurity)
    - Know how and abilities
  - The risk attitude of the agent
- Agents can be partially ordered according to
  - the resources they can access
  - the risk they are willing to take
- The higher the position, the larger the danger
- Attacks can be ordered in the same way
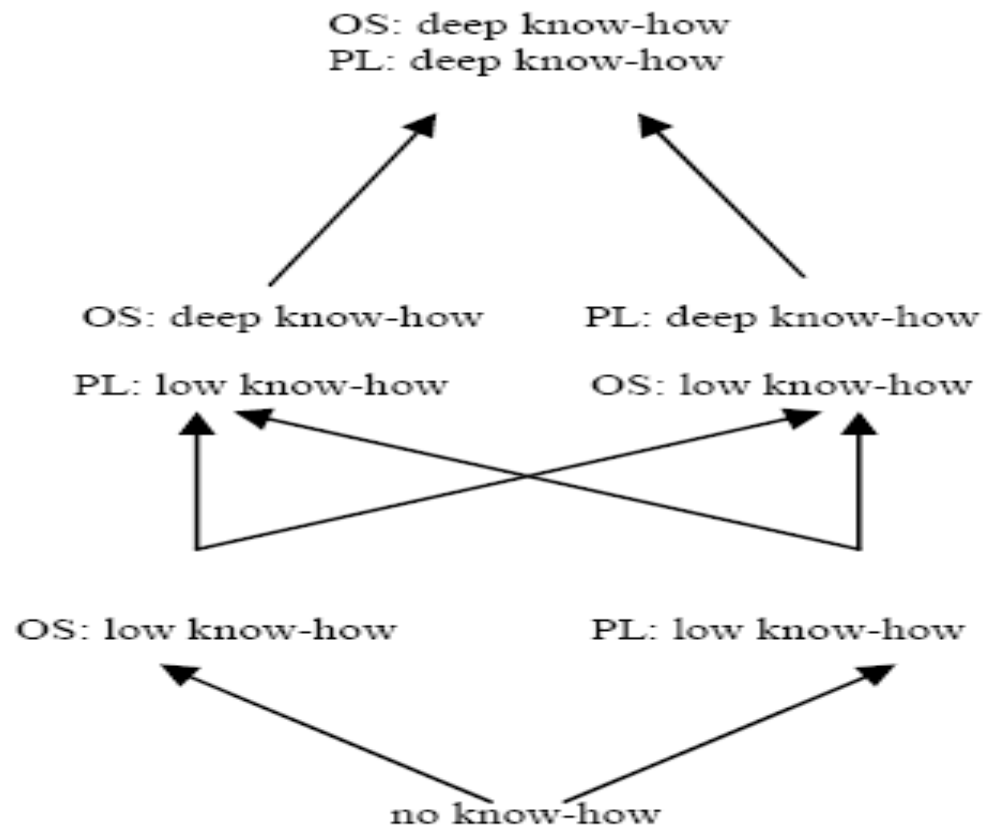
A lattice based description of agents

know-how on both PL and OS

know-how on PL   know-how on OS
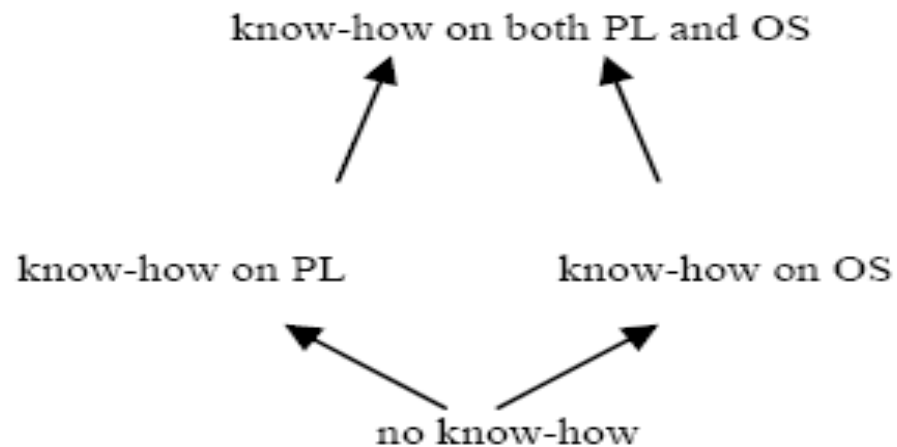
no know-how

a) A poset modelling the know-how of a threat

A finite model to describe threat agents

A lattice based description of agents

OS: deep know-how
PL: deep know-how

OS: deep know-how
PL: low know-how

PL: deep know-how
OS: low know-how

OS: low know-how

PL: low know-how

no know-how

A more refined model to describe threat agents

Describing an agent

- Each attack is described by a tuple of attributes and a noise

- Each agent is described by a tuple of attributes (same for attack) and an accepted noise

- We have one distinct partial order for each attribute

- This define a partial order for both agents and attacks

Feasible attacks

- Given

  - a tuple T_A that describes the attack A and where each element evaluates an attribute of A
  - a tuple T_M that describes a threat agent M and where each element evaluates the resources that M can access

- M can execute A provided

  - Each element of tuple T_M is larger than or equal to the corresponding elemen of T_A

  - The noise paired with A is smaller than or equal to the one that is accepted by M

Threat model

- Anytime a security problem is analysed there is the problem of formally determining the actions that any threat agent

  - can execute (owns the resources to execute)

  - cannot execute (lack of resources)

  - is not willing to execute

  should be considered

- It this problem is not solved, the analysis is not complete

- Not important when national security is involved

Threat model and partial orders

- The partial orders among threats and attacks are an important way to preserve the coherence of the analysis

- Implement the basic checks that a more powerful threat actually can implement a larger set of attacks (even if sometimes it may be not interested in implementing them)

- But do not support the discovery of threat or of attacks