Threat Analysis

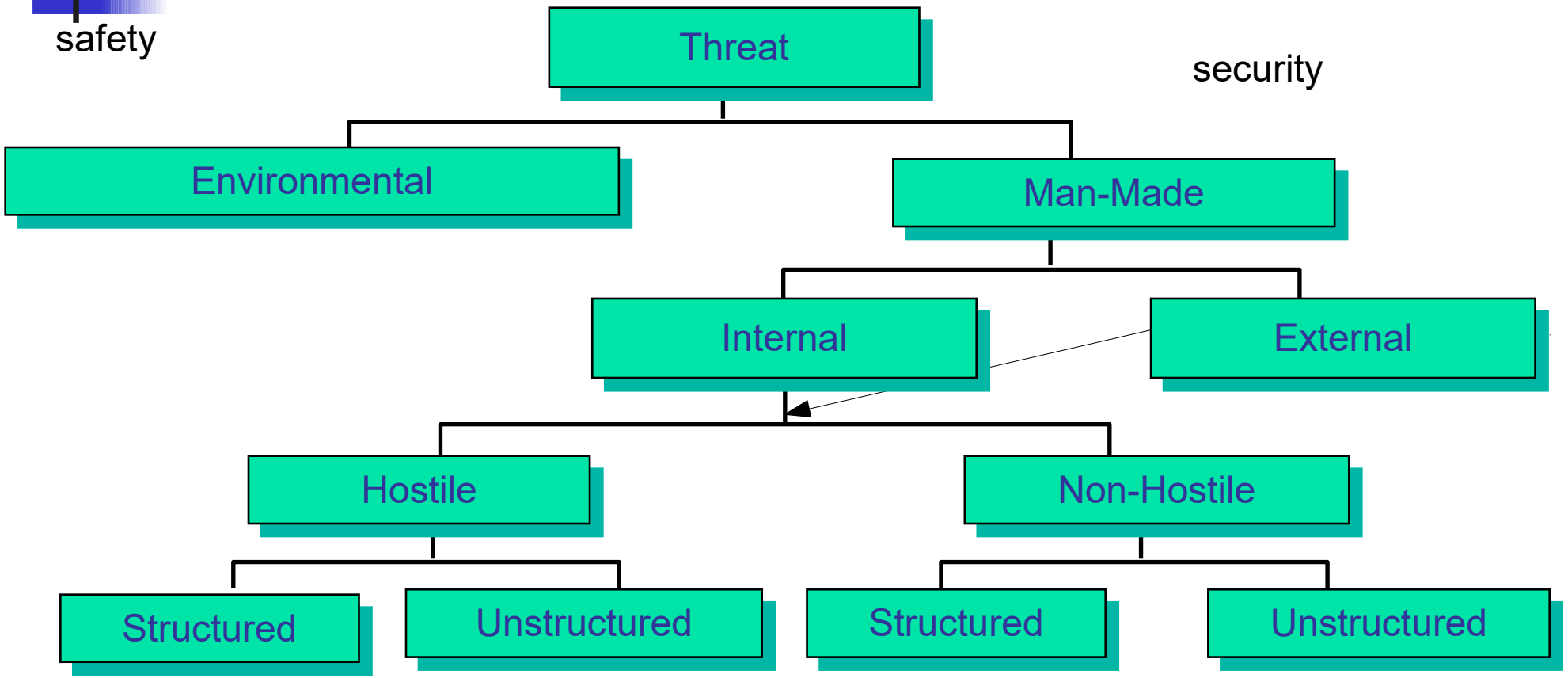
Threat analysis

- 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 catalogue

Table 1 – Threat Sources[5]

Threat Group	Threat Agent
Individuals	Employees/Contractors
	Customers/Clients
	Service Provider Employees/Contractors
	Hackers
	Hacktivists/Activists
	Criminals
	Terrorists
External Organisations	Service Providers
	Hacktivist or Activist Groups
	Foreign Governments
	State Sponsored Action Groups
	Organised Crime Syndicates
	Terrorist Groups
Technical Events	Malicious Code (e.g., viruses, worms etc.)
	Defective Code
	Equipment Failure
	Failure of air-conditioning
	Loss of power supply
Accidental Events	Fire
	Water damage
	Major Accident
	Destruction of equipment or media
Natural Events	Weather (e.g., electrical storm)
	Earthquake
	Volcanic Eruption
	Flood

Threat catalogue - Motivation

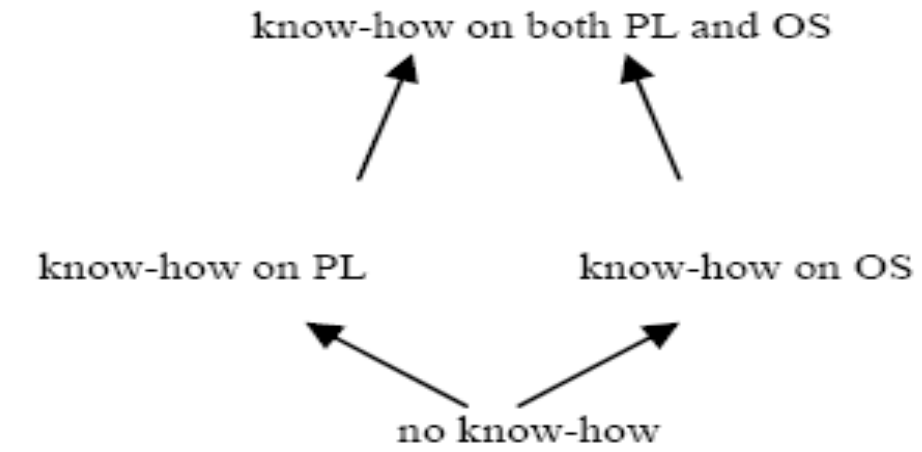
Table 2 – Threat Agent Motivation[6]

Threat Domain	Motivation
Individuals	Minimise their effort to complete a process or procedure
	Financial gain
	Revenge
	Gaining knowledge or information
	Exerting power
	Gaining peer recognition and respect
	Satisfying curiosity
	Furthering political or social aims
	Terrorising certain target groups or individuals
	Enhancing personal status with other individuals or a group
External Organisations	Gaining a competitive advantage
	Gaining an economic advantage
	Gaining a military advantage
	Gaining a political advantage
	Furthering political or social aims
	Financial gain
	Terrorising certain target groups

Threat analysis

- For each agent, the analysis determines
  - The goals= rights on components
  - The resources it has available
    - Tecnological
    - Information (security through obscurity)
    - Know how and abilities
  - The risk attitude
  - The legal access rights
- 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 potential impact
- Attacks can be ordered in the same way

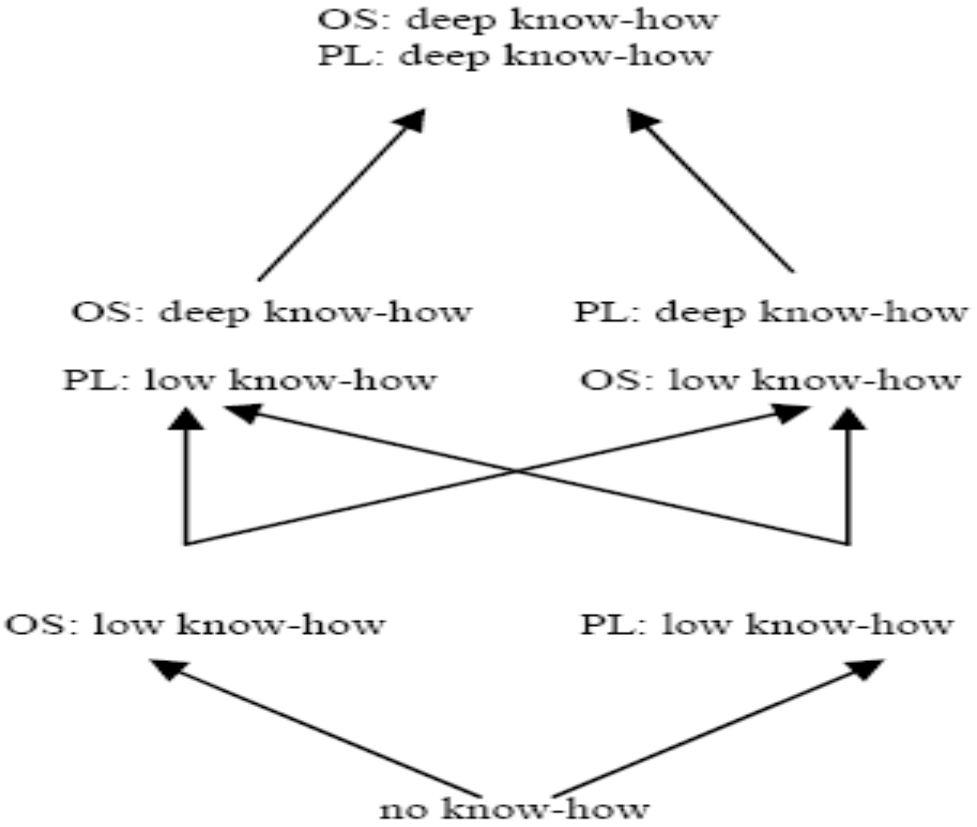
A lattice based description of agents



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

A finite model to describe threat agents

A lattice based description of agents



- A more refined model to describe threat agents

Describing agents and attacks

- 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 a basic checks

  a more powerful threat cannot implement a smaller set of attacks

- But do not support the discovery of threat, of attacks, or if a threat will attack us

What is new for ICT?

- Automated attacks
- Mass attack = automated + autonomous
- A threat agent does not attack a system but it programs an agent that can reproduce itself and propagate from one system to another one