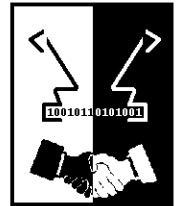


**SECURE**

Secure Environments for Collaboration  
among Ubiquitous Roaming Entities



---

# Implementing Trust-Based Decision Support Systems

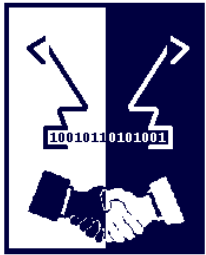
---

Christian Damsgaard Jensen  
Informatics & Mathematical Modelling  
Technical University of Denmark

Email: [Christian.Jensen@imm.dtu.dk](mailto:Christian.Jensen@imm.dtu.dk)

URL: <http://www.imm.dtu.dk/~cdj>





# Definition of Trust

every presenter needs one :-)

- “Trust is a particular level of subjective probability with which an agent will perform a particular action, both before we can monitor such action and in a context in which it affects our own action”

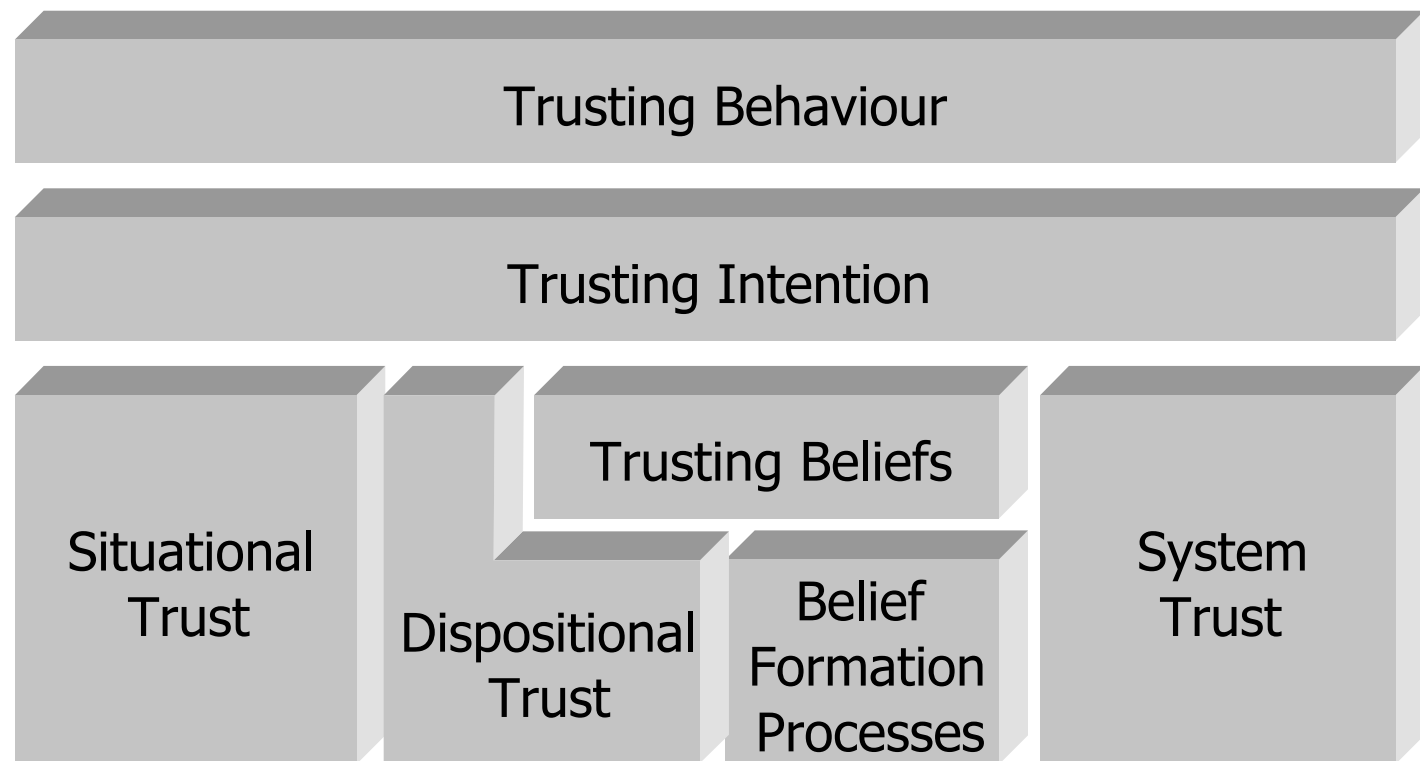
Diego Gambetta, Can we Trust Trust?.

- Two important implementation properties:
  - Trust and Risk must both be considered together
    - Trust is irrelevant unless there is a risk
  - Trust assumes a choice of action
    - Trust is irrelevant if there is no choice
    - It's the only show in town, he holds a gun to my head, ...
      - Coercion and threats are “good” trust substitutes



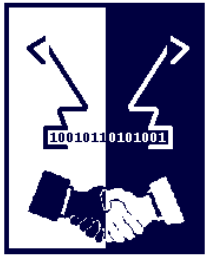


# A Human Model of Trust



(McKnight & Chervany, 1997)

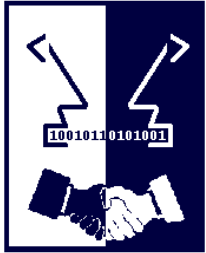




# A Computational Model of Trust

- Computational trust has two components:
  - $\mathcal{T}$  is set of (possibly complex) trust values
  - $\mathcal{P}$  is a partial ordering on  $\mathcal{T}$ , which compares two trust values
- Structure of  $\mathcal{T}$ :
  - Integer values
  - Belief, disbelief, and uncertainty
  - Sets of histories (records of previous interactions)
  - External factors (risk, context, recommendations and reputation)
- Purpose of  $\mathcal{P}$ :
  - Compare two (or more) trust values to determine who among multiple potential partners is the most trustworthy
  - Compare trust value of a given principal with a defined threshold to determine if a request should be granted





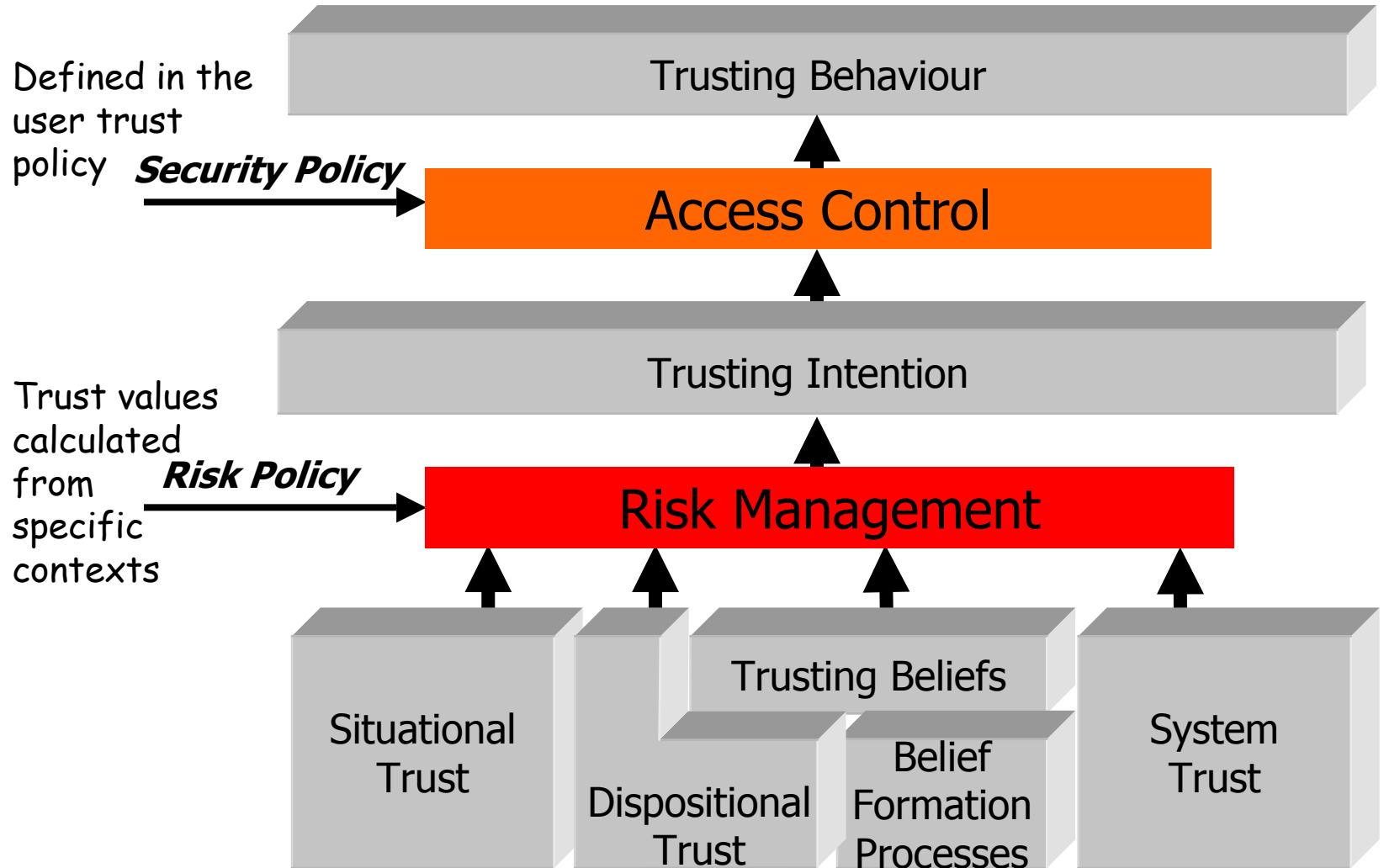
# External Factors

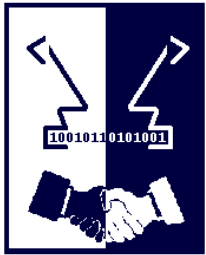
- Risk
  - Risk assessment is normally based on statistics
  - Real-time risk assessment is “difficult”
- Context
  - Trust means different things in different contexts
    - Action under consideration
    - Logical Environment - application, neighbouring nodes, ...
    - Physical Environment - physical location (e.g. inside or outside firewall), specific hazards (theft of mobile devices), ...
- Observations, recommendations and reputation
  - Observations and recommendations must be based on personal experiences
    - Recommendations based on reputation may be self-magnifying





# Applying Trust in Security





# Principals in Trust-Based Systems

## entity recognition

- Identity is in itself irrelevant in a security system based exclusively on personal experience
- Entity recognition identifies recognisable features and assigns a pseudonym (a local identifier) to the other entity, thereby facilitating subsequent recognition
  - ER must be reliable
    - Low rate of false positives
    - Low rate of false negatives, except when other party changes identifying characteristics (change of “virtual identity”)
- ER-authentication must allow parties to establish equivalences between autonomous recognitions
  - Pseudonyms may be used to transfer statements about experiences (recommendations) between parties
- Entity recognition is a superset of authentication
  - ER does not bind recognition to “real world” identities
  - Multiple pseudonyms allow better protection of privacy





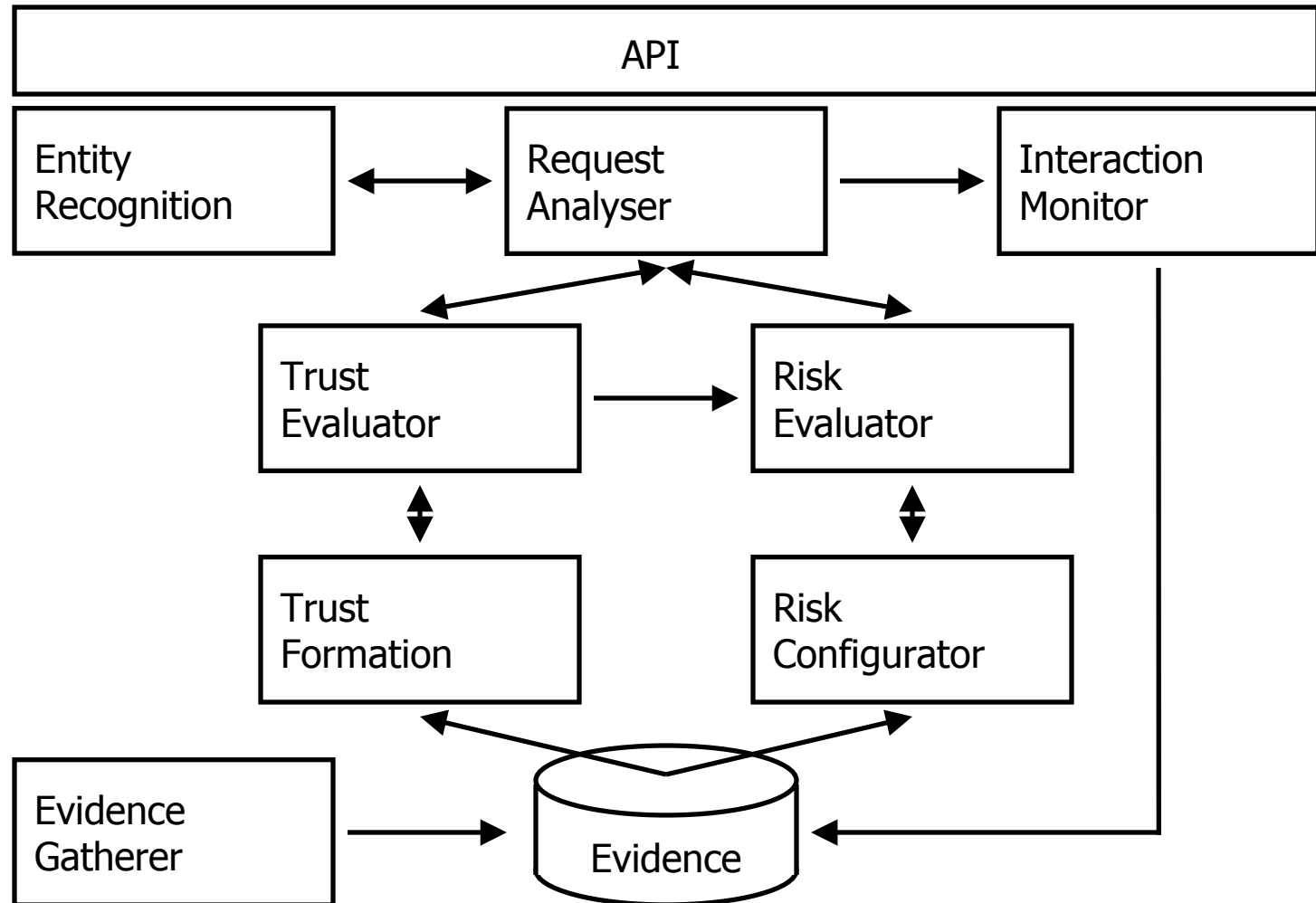
# Authentication vs. Entity Recognition

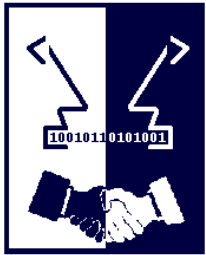
Authentication	Entity Recognition
A.1. <b>Enrollment</b> : generally involves an administrator or human intervention	
A.2. <b>Triggering</b> : e.g. someone clicks on a Web link to a resource that requires authentication to be downloaded	E.1. <b>Triggering</b> (passive and active sense): mainly triggering (as in A.2), with the idea that the recognizing entity can trigger itself
A.3. <b>Detective work</b> : the main task is to verify that the principal's claimed identity is the peer's	E.2. <b>Detective work</b> : to recognize the entity to-be recognized using the negotiated and available recognition scheme(s)
	E.3. <b>Retention</b> (optional): "preservation of the after effects of experience and learning that makes recall or recognition possible"
A.4. <b>Action</b> : the identification is subsequently used in some ways. Actually, the claim of the identity may be done in steps 2 or 3 depending on the the authentication solution (loop to A.2)	E.4. <b>Action</b> (optional): the outcome of the recognition is subsequently used in some ways (loop to E.1)





# SECURE Framework overview

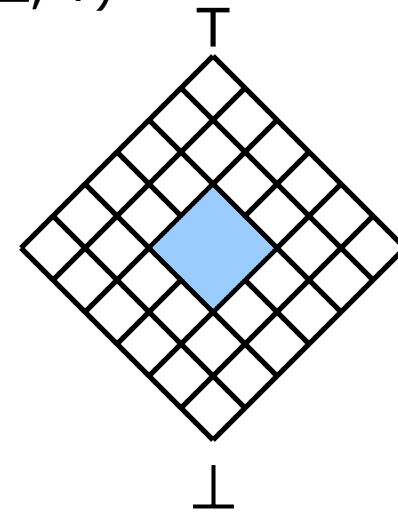


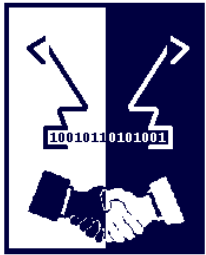


# SECURE Trust Calculations

## trust model

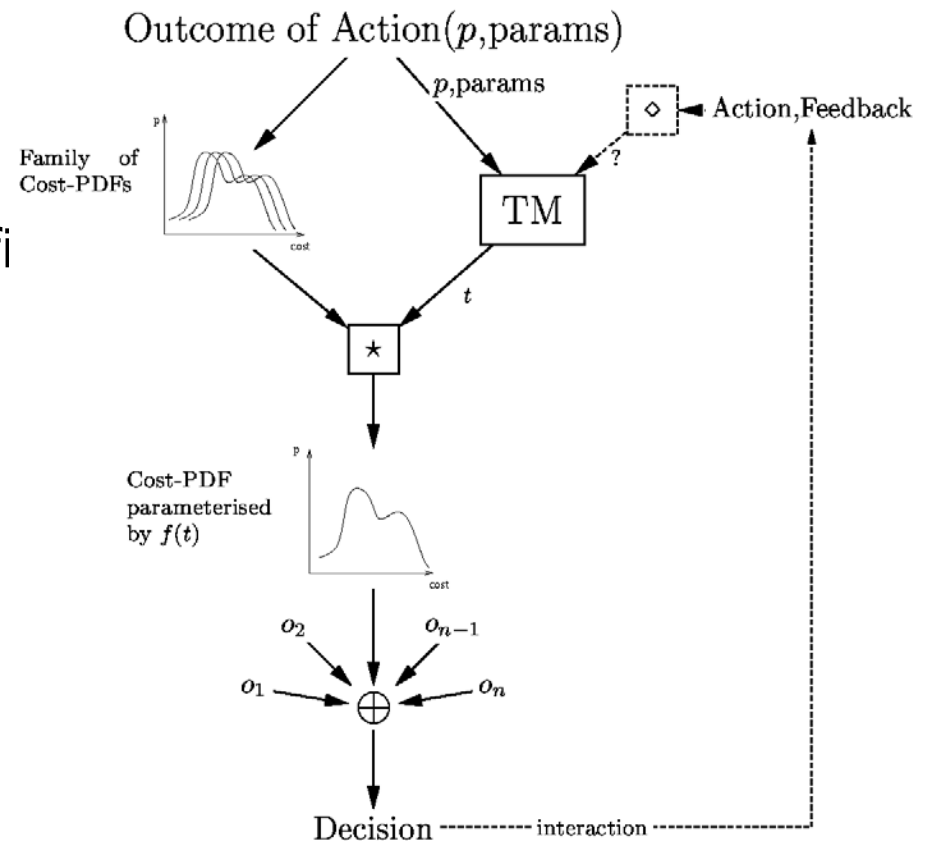
- Model defines a set of trust values and two partial orders that both define a lattice
  - Trust order compares trust values
  - Information order compares amount of information
- Intervals (glb, lub) express partial information
  - The trust value could be anywhere in the interval
  - Strangers are assigned trust value  $(\perp, T)$
  - More trust moves the interval upwards in the lattice
  - More information shrinks the size of the interval
  - Intervals can be used to express trust-based security policies

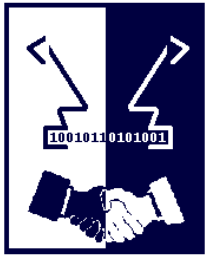




# SECURE Risk Calculations risk model

- Actions are mapped to possible outcomes
- Each outcome has an associated cost / benefit to the principal
- A projection function extracts information,  $t$ , from the Trust Model's state, using  $p, \text{params}$

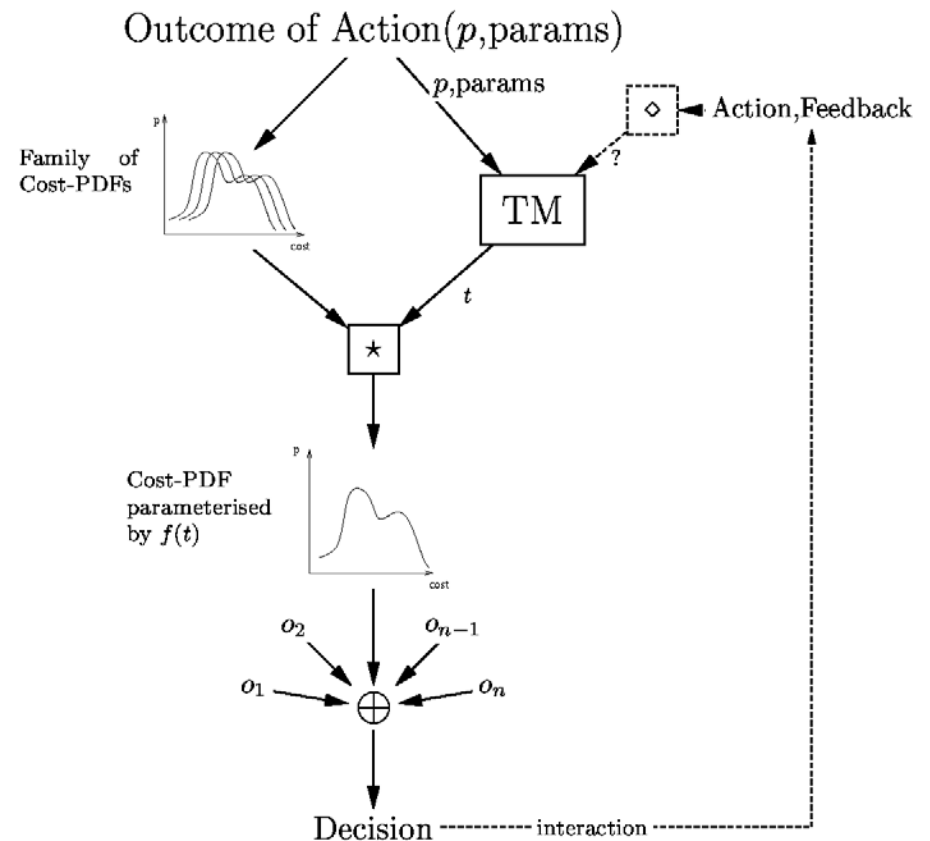


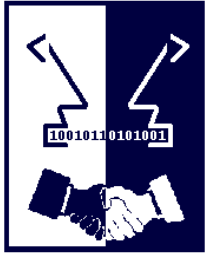


# SECURE Risk Calculations (contd.)

## risk model

- The output  $t$  helps determine the likelihood of each outcome
  - ★ chooses the cost-PDF for an outcome.
- All outcomes' costs are combined (by  $\oplus$ ) to make the decision
- The decision is not necessarily binary
  - e.g. {Yes, No, Ask}





# Lessons Learned

- Trust is subjective, so recommendations and reputation must also be subjective (not directly transferable)
- Trust is context specific, so a general trust engine must be parameterised by the context
  - It is important to consider why trust is needed
  - Trust build in one context cannot automatically be transferred to another context
- Trust is a means to an ends, not the ends in itself
  - Model of trust needs only be sufficiently accurate to be useful, it need not capture all the many facets of trust
  - Metaphor that provide end-users with an intuition that helps them understand and configure the system
- Beware of complexity explosion (feature creep)
  - There is so much interesting stuff that you can do

