A Socio-Cognitive Approach to Modeling Policies in Open Environments

Tatyana Ryutov
USC Information Sciences Institute

Motivation

- Most Internet interactions involve risk and uncertainty
  - lack of prior interactions
  - insufficient information about participants
- Today’s online interactions are effectively a form of social exchange where both communicating parties are exposed to risk
- Shift from attempts to mitigate all potential risks, to accepting threats as intrinsic part of any open system and minimizing the risks by building trust
  - Trust becomes “soft” security mechanism
- Handling risky mutual exchanges and establishing trust in open ad hoc environments are the new challenges of access control and authentication

Trust and Social Exchange

- Trust is individual’s opinion (believe) of another entity that evolves based on available evidence [Josang]

- Trust is a decision to accept risk (participate in exchange) faced with positive or negative outcomes of interaction which depend on the actions of the opponent

- A *social exchange* is interaction in which one party is obligated to satisfy particular requirements, usually at some cost, in order to receive benefits from the other party

Approach: Balance Risk and Trust

- Socio-cognitive approach: reason about uncertainty and risk involved in a transaction, and automatically calculate the minimum *trust threshold*

- The threshold is based on balancing objective (based on mechanisms) and subjective (based on beliefs) components, which together predict that a transaction will result in an acceptable outcome

- Subjective and objective trust types are complementary

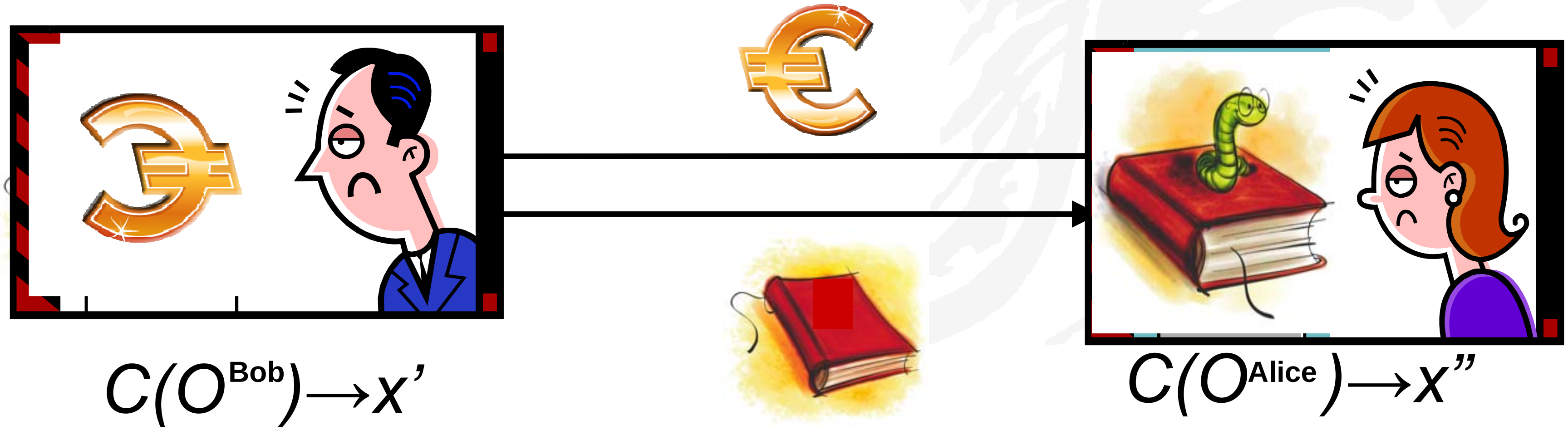
Phases of Exchange

Exchange phases:

- Initial
  - Determine what items are to be contributed by each party
  - Determine a set of issues (e.g., quality, timeliness, etc.) for each item to be contributed or received
  - Calculate possible outcomes of the exchange in terms of gains and losses
  - Apply access control policy to find a set of acceptable outcomes
  - Determine a set of subjective/objective trust metrics (trust threshold) which predicts the acceptable outcomes
- Negotiation
  - Participants negotiate trust thresholds using private negotiation strategies
  - This process can be iterative
- Final
  - participants evaluate the actual outcomes of the exchange and update interaction history

Outcome Evaluation

- *outcome evaluation function* represents consequences of the exchange in terms of gains and losses: $C(O) \rightarrow x$
  - scoring functions map the observed value that a particular issue takes to a *satisfaction rating*
  - *outcome* for participant *a* is a set of satisfaction ratings with the *b*'s performance on each issue
- The result depends on:
  - Desirability of resource
  - Importance of particular issue

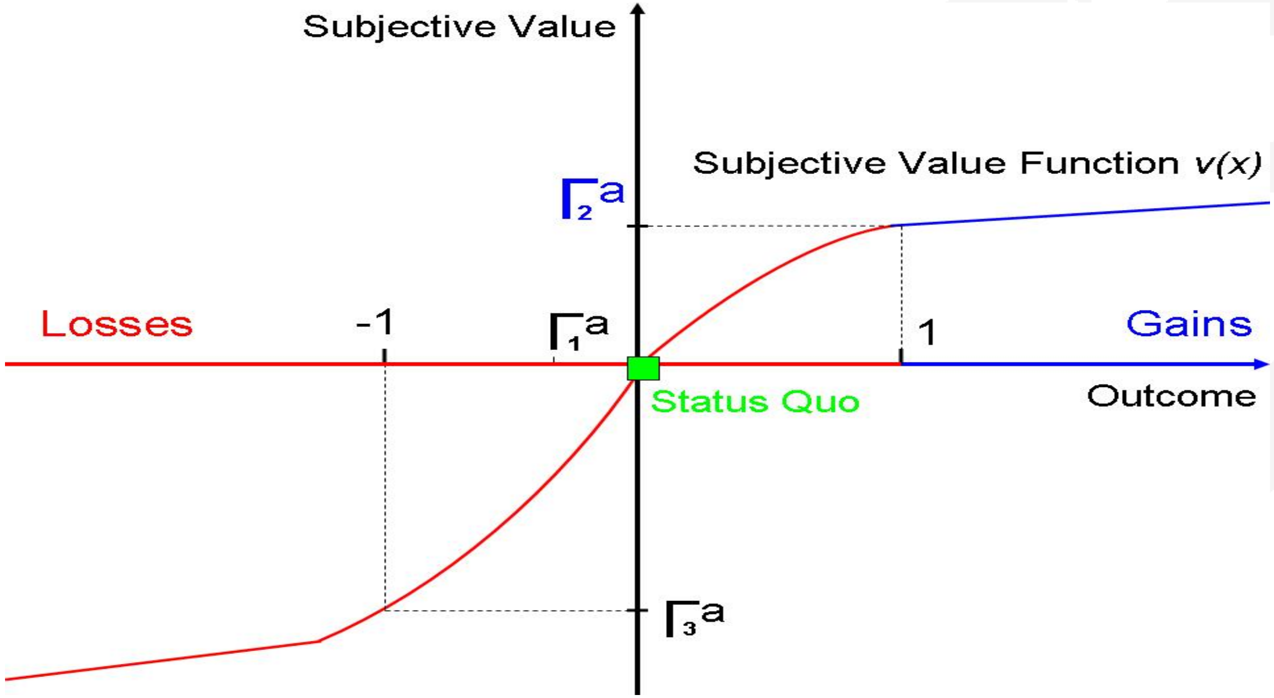


$C(O^{Bob}) \rightarrow x'$

$C(O^{Alice}) \rightarrow x''$

Exchange Policy

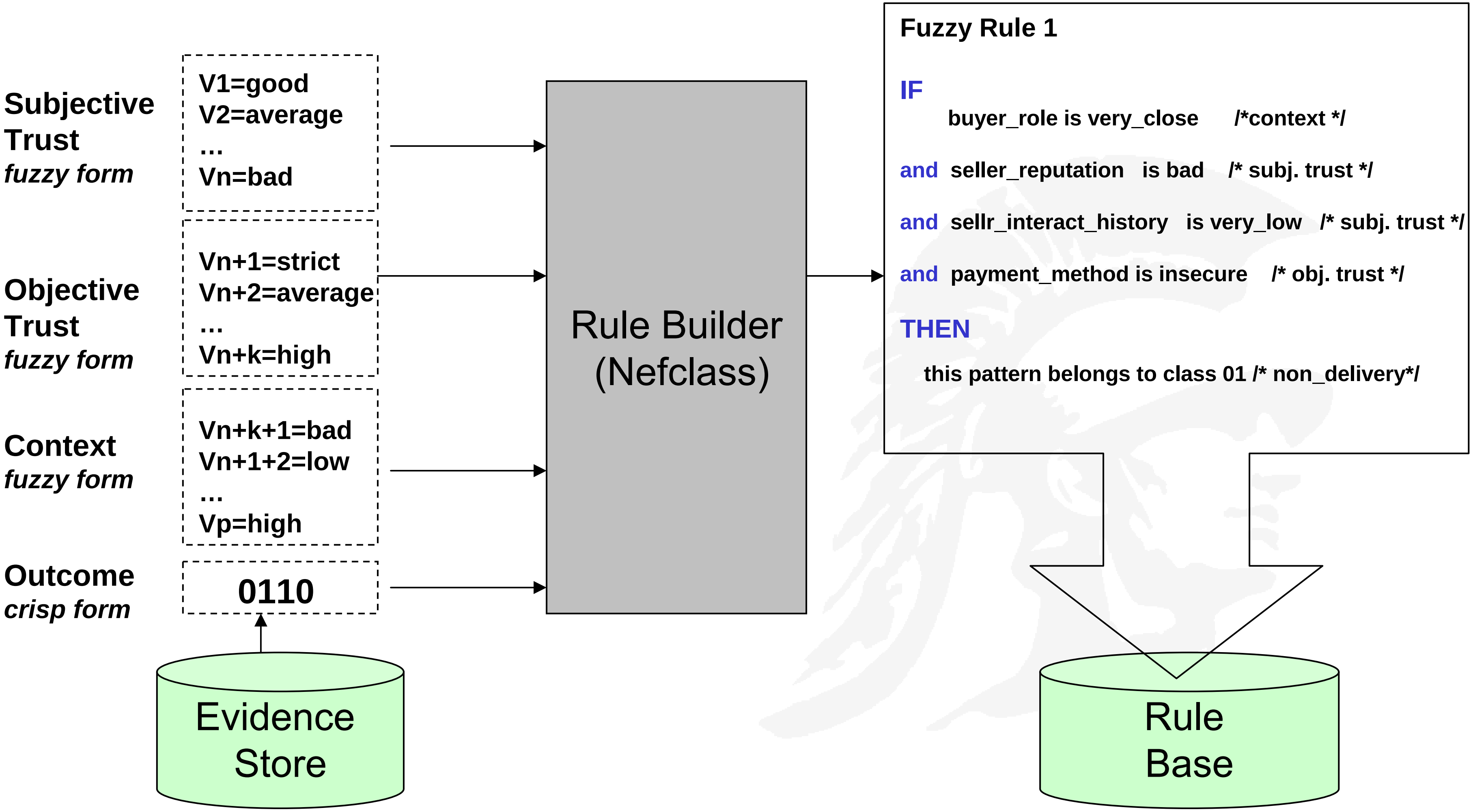
- subjective value of an outcome: *v(x)* from the Prospect Theory
- access control policy determines the set of outcomes with utility value Γ^a acceptable for a
- Exchange policy: $\boxed{v(C(O^a)) \geq \Gamma^a}$



Calculating Trust Threshold (TT)

- A trust threshold predicts an exchange to result in an outcome with the value greater or equal to the minimum acceptable value
- How to calculate TT?
  - Imitate how people deal with trust issues
  - Neuro-fuzzy approach
    - constructed **IF-THAN** fuzzy rules represent the relationships between a context of an exchange, negotiated objective and subjective trust, and the observed outcome

Generating Fuzzy Rules



Subjective Trust *fuzzy form*

V1=good
V2=average
…
Vn=bad

Objective Trust *fuzzy form*

Vn+1=strict
Vn+2=average
…
Vn+k=high

Context *fuzzy form*

Vn+k+1=bad
Vn+1+2=low
…
Vp=high

Outcome *crisp form*

0110

Evidence Store

Rule Builder (Nefclass)

Fuzzy Rule 1

IF
buyer_role is very_close /*context */
and seller_reputation is bad /* subj. trust */
and sellr_interact_history is very_low /* subj. trust */
and payment_method is insecure /* obj. trust */
THEN
this pattern belongs to class 01 /* non_delivery*/

Rule Base

Extracting TT from the Fuzzy Rule Base

- Uses the rule base to determine TTs as follows:
  - select a set of fuzzy rules *F* where rule *antecedent* contains variables of the type “context” which match the context of the experiment
  - from the set *F* construct a subset *F’* by selecting rules where the rule *consequent* represents an acceptable outcome
  - for each fuzzy rule *fi* from the set *F’* construct a trust threshold *Ti* by extracting a set of values of the type “subj. trust” and of the type “obj. trust”.
  - constructs set of all acceptable thresholds by taking a conjunction of the sets constructed during the previous step
- Negotiate TT
  - NOTE: TT predicts the worst acceptable outcome, may want to start negotiation for a better deal

Modeling Trust in Cyber Security Testbed Environment

- A testbed is risky and uncertain environment
  - Risks: malicious code may hurt the testbed, interfere with other experiments or escape into the Internet
  - The sources of uncertainty:
    - testing virulent code with unknown characteristics
    - incomplete knowledge about the "maliciousness" of the code
    - the ability and reliability of the investigators to provide accurate threat assessment
    - subjectivity of judgment

- Admission to security testbed: whether a particular experiment should be admitted and what the protection level should be

- To admit an experiment a Trust Threshold must be reached
  - Subjective trust :
    - trusting investigator's ability to correctly predict code behavior due to perceived qualities (e.g., reputation, skills) or based on the history of prior interactions
    - trusting the code: belief that the code will behave as expected because, for example, one has run this code before
  - Objective trust - one has formed an intention to trust (run an experiment) due to the mechanisms that mitigate expected vulnerabilities introduced by code as well as unexpected threats caused by misbehaving code.

Conclusions

- a new risk/trust balancing approach to model policies in open competitive environments
- a neuro-fuzzy approach to calculate TT
- Supports flexible trust threshold negotiation
- Other application areas
  - Socio-cognitive grids
  - Scientific and commercial collaborations
  - Ad hoc on line trading
  - Semantic web