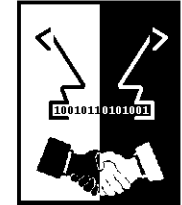


SECURE

Secure Environments for Collaboration
among Ubiquitous Roaming Entities

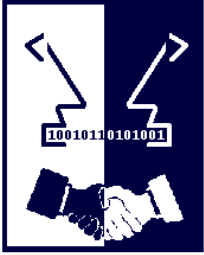


Implementing Trust

Trust-Based Admission Control in Collaborative Ad Hoc Applications

Elizabeth Gray



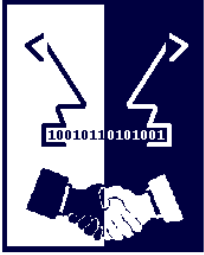


New Security Challenges

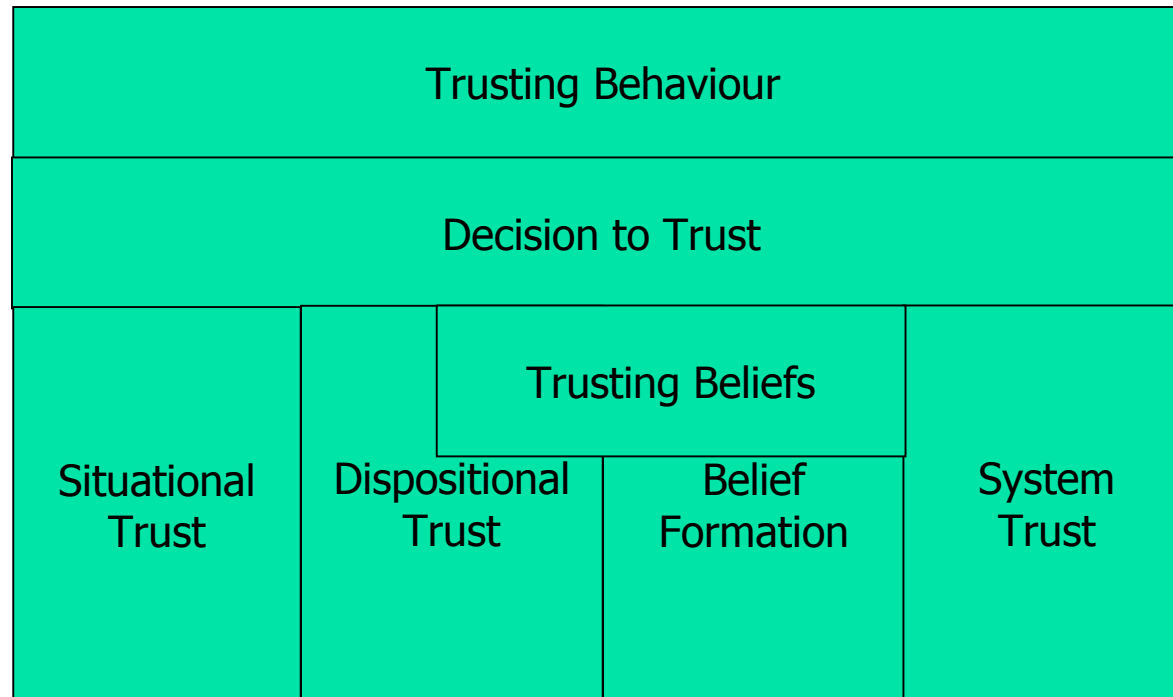
- Security properties of global computing environment
 - Large number of autonomous entities
 - Large number of administrative domains
 - No common trusted computing base
 - No global system trust
 - Virtual anonymity (identity \neq trust)
 - Identity conveys no a priori information about the likely behaviour of a prospective collaborator

- Properties exclude the use of current security mechanisms used in large distributed systems



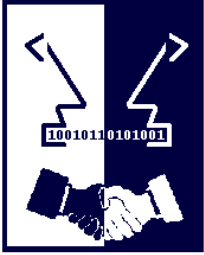


Human Notion of Trust

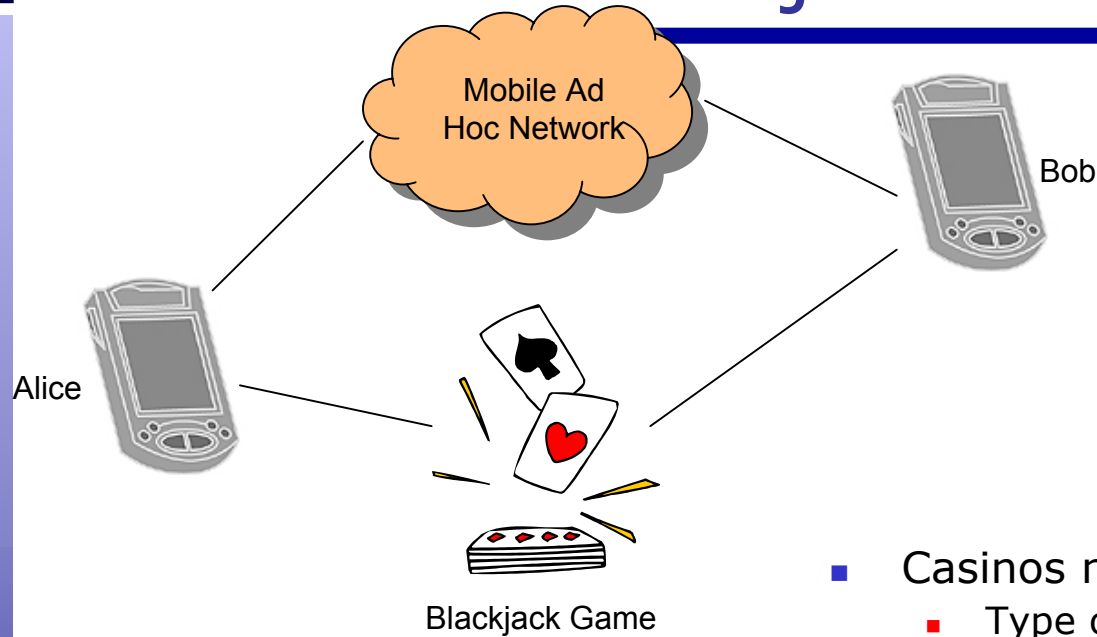


McKnight & Chervany's human trust framework



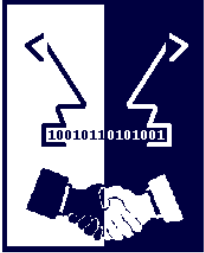


Blackjack Trust

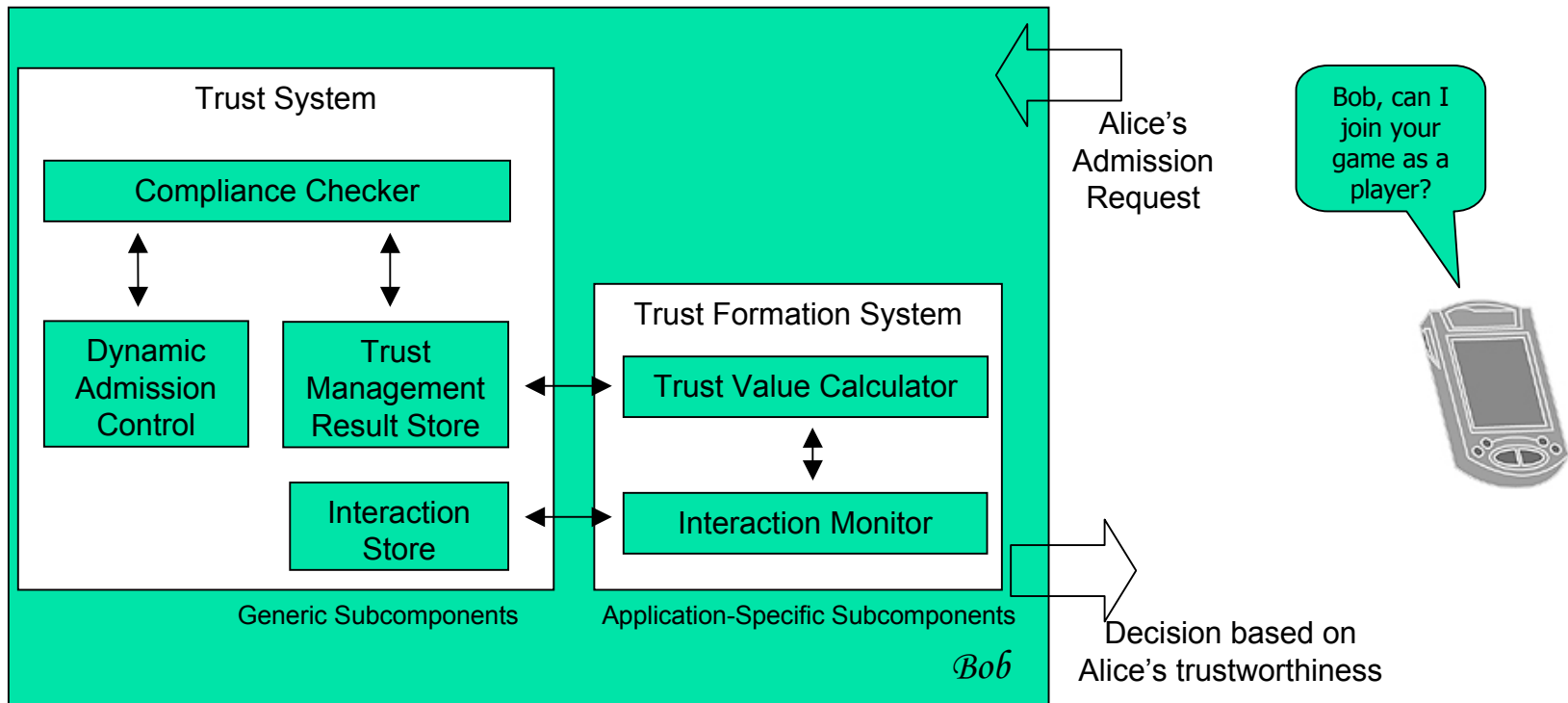


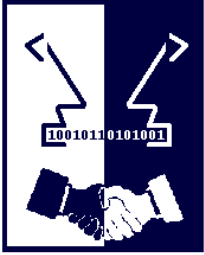
- Casinos monitor
 - Type of game played
 - Player's average bet
 - Player's skill level
 - Speed of the game
 - Date, time
 - Debt payment record
 - Usual co-players, table position





Local Trust-Based Admission Control





Initial Results

- Trust may be formed and evolved by principals in a collaborative ad hoc application in a manner very similar to human trust.
- LTBAC system behaves correctly in permitting or denying access to resources using a range of human-like restrictions, i.e. by adjusting trust value and implementing LTBAC policies. The system and policies match very closely with the human trust model, although we believe more complexity must be added.
- Have implemented the majority of McKnight and Chervany's human trust framework.

