When Trust Does Not Compute

The Role of Trust in Ubiquitous Computing

Marc Langheinrich
ETH Zurich, Switzerland

RESEARCH GROUP FOR
Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Time for Trust!

- Pervasive Computing Systems Require a Security Architecture Based on Trust Rather Than Just User Authentication and Access Control
  - Kagal/Finin/Joshi, IEEE Computer 12/01
- Old Model Based on Verification of Credentials (Authentication) and Delegation Not Suitable
  - Ubicomp 2002 Security Workshop (Summary)
- [We Need] Security and Trust Technologies in Support of Privacy, Safety, and Dependability
  - Scenarios for Ambient Intelligence 2010, ISTAG

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Why (Computational) Trust?

- Simplify Authentication
  - No Passwords!
- Natural Form of Interaction
  - Ideally Suited for Ubiquitous Computing
- Improve Cooperation
  - More Flexibility
- Strengthen Security
  - 'Better' Evidence

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Step 1: What to Solve

- Starting Point: Scenarios
  - Allow Authors to Illustrate Problems and Solutions
- Examples
  - Gray et al: "Commuter-Train Black-Jack"
    (iTrust 2003)
  - Shand et al: "Trusted Phone Numbers"
    (PerCom 2003)
- Issues
  - Described Scenario Does Not Solve a Problem, or
  - Solves a Problem That Does Not Exist

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

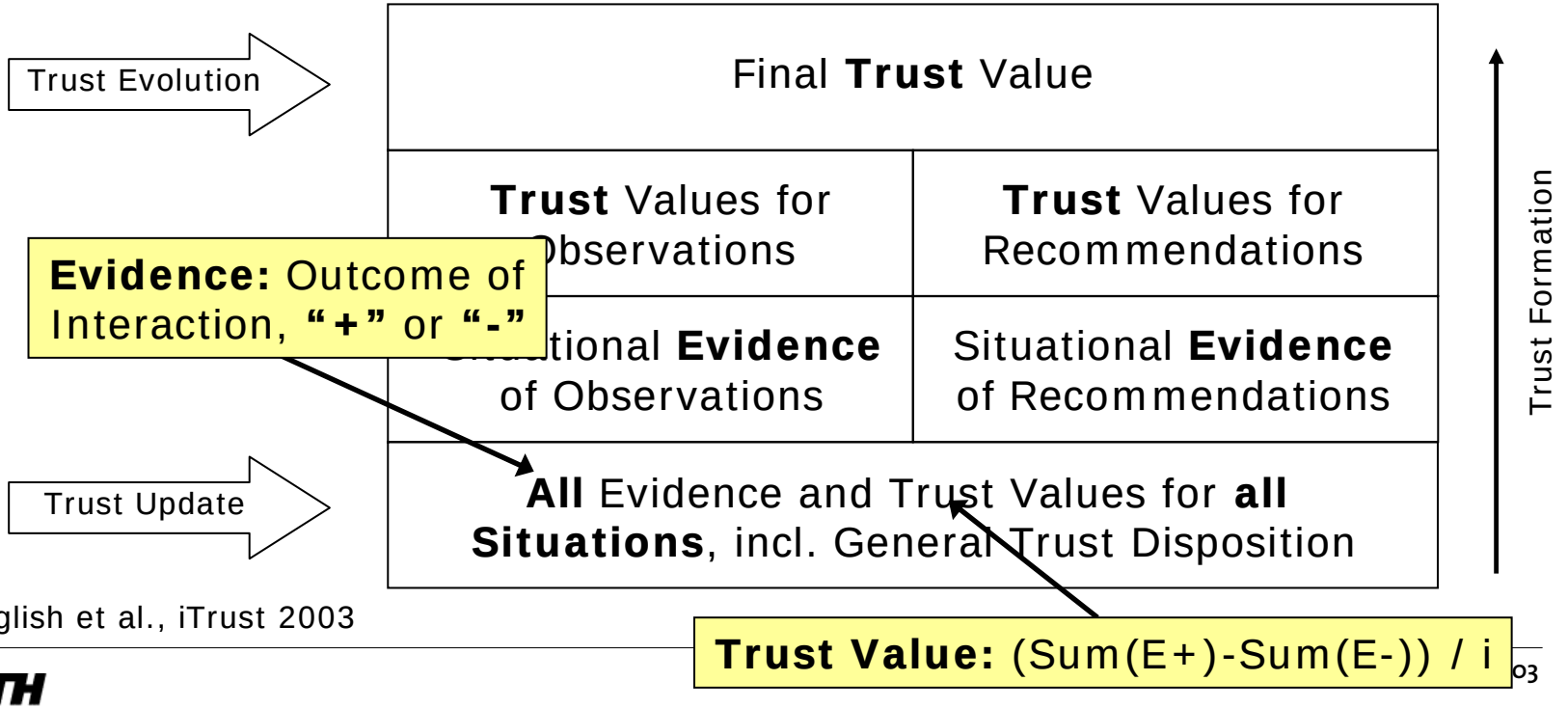
Step 2: How to Solve

- Compute Trust Value
  - Based on Prior Experience, Recommendations, Risk
  - Allow Exchange/Access if Above Threshold
  - Take Cues from Psychology, Sociology
- Examples
  - English et al.: "Trust Information Structure" (iTrust 2003)
  - Shand et al.: "Transparent Collaboration" (PerCom 2003)
  - Gray et al.: "Trust-Based Admission Control" (iTrust 2003)

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Trust Information Structure

- Models Human "Trust Lifecycle"
  - Trust Formation, Evolution, Exploitation
  - Uses Personal Observations and Recommendations



Transparent Collaboration

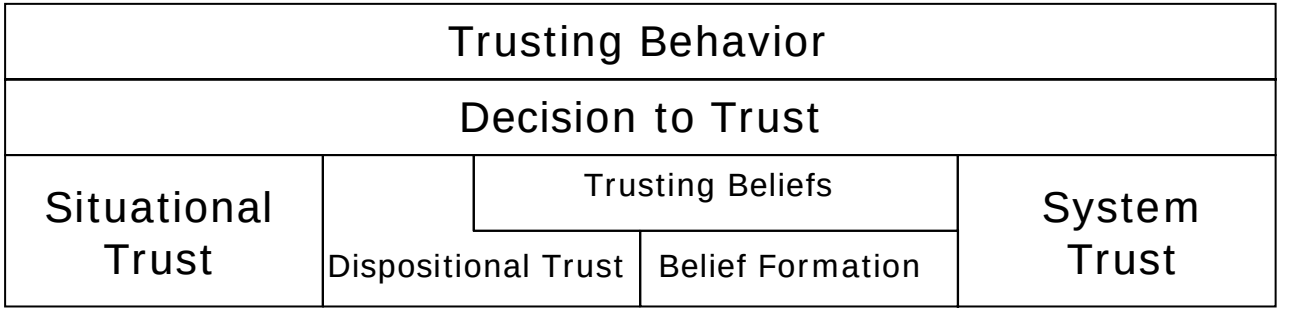
- Access Based on One's Own and External Recommendations (Trust Value)
  - Each Trust Value is (Belief, Disbelief)-Pair
  - Access Granted if Benefits > Risks
- Issues
  - User Must Specify Trust as "Weight of Evidence For and Against a Particular Trust Assignment" (Complexity?)
  - Risk-Assessment Required: "Maximum Benefit of Trusting *P* With *N*; Cost of *P* Ignoring Our Recommendations; Cost of Owner Being Asked for Guidance; ..." (Complexity?)

Shand et al., PerCom 2003

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Trust-Based Admission Control

- Uses Psychological Trust-Framework
  - Based On: Situational Trust, Dispositional Trust, System Trust, Beliefs, Intentions
  - Access Granted if Majority of Entities Agree



McKnight and Chervany's Trust Framework (1996)

Step 2: How to Solve

- Compute Trust Value
  - Based on Prior Experience, Recommendations, Risk
  - Allow Exchange/Access if Above Threshold
  - Take Cues from Psychology, Sociology
- Examples
  - English et al.: "Trust Information Structure"
  - Gray et al.: "Trust-Based Admission Control"
  - Shand et al.: "Transparent Collaboration"
- Issues
  - High Complexity, High Dynamics (Unpredictable?)
  - Unrealistic Scaling Assumptions (AI Revisited?)

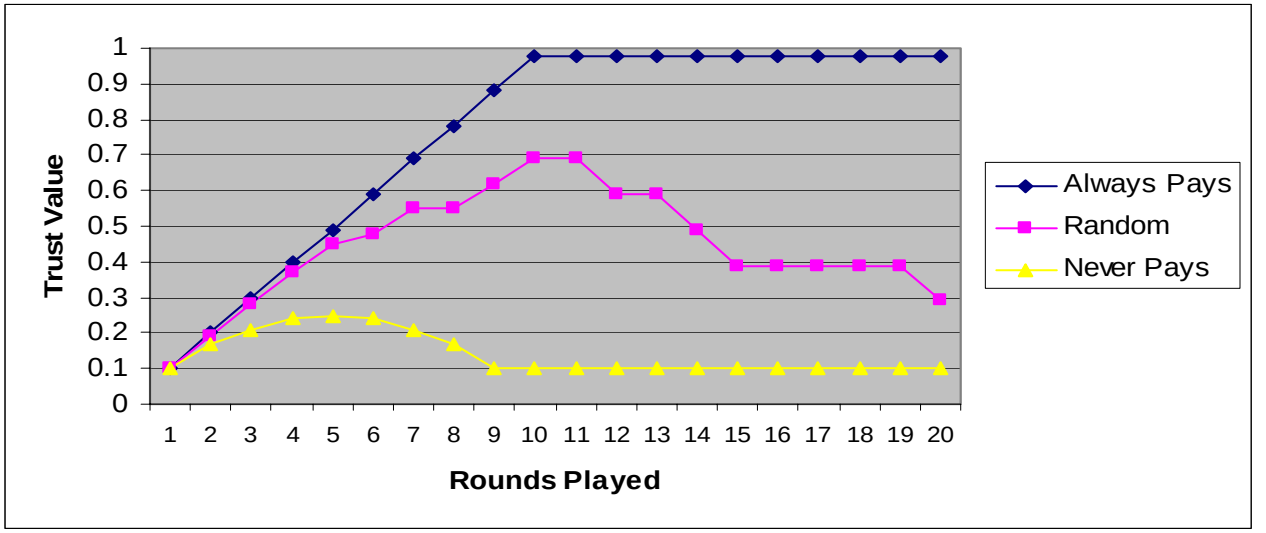
Scaling Assumptions

- Total/Partial Ordering of Trust Values
  - Can Trust-Comparisons be Chained?
- Humans can Rate/Rank Their Beliefs
  - How to Quantify "Gut Feeling"?
- Beliefs can be Inferred From Observation
  - Too Many Variables (Dispositions, Beliefs, ...)
- System or User can Identify Situations
  - How Consistent are Humans? (Exceptions!)

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Step 3: How to Validate

- When Does it Work?
  - Research Needs Evaluations Methods
  - Most Trust-Frameworks Lack Verification Step
- Example



  - Gray et al.: "Trust-Based Admission Control" (iTrust 2003)

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Goal 1: Do as I Think

- Emulate Human (Me!)
  - So I Can Delegate Decisions
  - Test: Compare Decisions on Range of Interactions
- Do I Always Know What I Want?
  - Split Decisions ("Near Miss" Tolerance)
  - Important vs. Unimportant Decisions
  - Wanting to Trust vs. Trusting

Goal 2: Do What is Best

- Maximize Expected Payoff
  - So I can Improve (Profits/Fun/Health/...)
  - Test: Compare With "Optimal" Decisions
- Needs Detailed Risk Assessment
  - Based on User- or 3rd-Party-Input?
  - Hindsight Argument: All Successful Decisions Seem to Have Been "Good"
  - How Much Disagreement is Tolerable?

Conclusions

- Problems with Ubicomp Trust
  - Don't Know What to Solve (Focus)
  - Don't Know How to Solve (Implementation)
  - Don't Know How to Verify (Validation)
- Automation Issues
  - Context Identification (Precise Enough?)
  - Quantification Possible? (Manual/Auto)
  - Computation Possible? (Expectations?)

Conclusions

- Support, Not Replace
  - Location-based Authentication
  - Reputation Display, Interaction History
  - Simplified Sharing, Temporary Overrides
- Trust as a Human Trait
  - Analyze When and Why Humans Trust
  - Create Systems that Humans can Trust!
  - Create Systems that can be Used to Trust!