



Addressing Trustworthiness in Design

Michael C. Loui

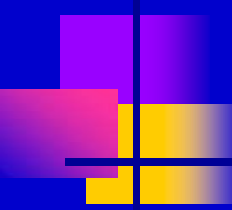
University of Illinois at Urbana-Champaign

December 3, 2004



Bertino: New Challenges in Database Security

- New environment:
 - Voluminous, valuable data
 - Disintermediation of access
- Traditional concerns: availability, confidentiality, integrity
- New concerns: correctness, completeness, provenance, compliance with complex fine-grained access policies



Elnozahy: Simulator reveals unanticipated interactions

- Current situation
 - System components interact in complex ways; situations not envisioned in specifications
 - Economics: smaller teams, shorter cycles
- Current response: conservative, incremental
- Full system simulation
 - Reveals unexpected interactions
 - Expensive to build, slow to run
- *(cf. scale models for aircraft, skyscrapers)*



Gligor: Examine implied trust relations

- Trust establishment requires judgment on body of evidence
- Difficulties:
 - Ad hoc networks: no a priori trusted nodes
 - Uncertain, negative, false evidence
- Need MRI to discover hidden trust relations, dependencies
- (*MRI inventor Lauterbur is at Illinois*)



Waidner: State trust explicitly in risk terms

- Translate “Does A trust B for x?” into “How does A’s overall risk change if A uses service B(x)?”
- (*cf. definition of safety in ethics literature*)
- Examples:
 - Hardware-based attestations
 - Redundancy in distributed systems, threshold cryptography



Design Challenges Have Common Themes

- Need for metrics on evidence/attestations
 - Data quality and completeness
 - Judgment evaluation for level of trust
- Economic and social factors
 - Expense of integrating design features, running full system simulation, to improve trust; “pay now or pay later”
 - Designing mechanisms for usability