Designing trust-centric open decentralized systems

In the absence of a centralized authority to protect them against malicious attacks, independent peers in open decentralized systems can use reputation-based trust relationships to establish confidence in each other. A number of reputation models exist but two issues have remained unexplored –

- How to select a suitable reputation model for a given application
- How to design the architecture of a decentralized peer and properly integrate the reputation model within it, so that the resultant architecture is secure in the face of malicious attacks

**New approach**
- Use threats of decentralization to
  - compare reputation models and choose an appropriate model for a given application setting
  - identify design guidelines

**Research Impact**
- Principles to guide design of secure peers
- Reusable components that enable the realization of guaranteed benefits
- Simulator to assess and compare reputation models

---

**TREF**
- Threat-centric REputation Framework
- theoretically compare abilities of reputation models against threats to select a starting set of abilities

**SIFT**
- Simulation Framework for Trust models
- characterize reputation models and applications using a set of parameters
- subject parameters to threat scenarios
- analyze results to determine which model best suits the application

**4C Framework**
- help describe reputation models
- Content, Communication, Computation, Counteraction sub-models

---

**PACE Components**
- HTTP Sender
- Custom Protocols
- Multicast Manager
- Communication Manager
- Signature Manager
- Key Manager
- Credential Manager
- Trust Manager
- Application Trust Rules

---

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT