**Motivation: Open System Security**

- **Open systems share resources across organizational boundaries**
  - Examples: supply chain management, web services, grid computing, peer-to-peer systems, semantic web, disaster response, joint military activities

- **Identity of users from outside an organization is insufficient to determine their access rights**
  - Dynamic nature of open systems makes preregistration impractical and unscalable

- **Solution**: authorization decision based on user attributes

**TrustBuilder2**

- **Flexible** environment for experimentation and development of scalable authorization solutions
- Support for extensible and user-defined policy languages, credential formats and negotiation protocols
- Enforcement of user-defined obligations
- Support for plug-ins
  - Arbitrary logging and visualization facilities
  - Inclusion of flexible policy and credential databases
  - Interaction with an extensible array of “helpful third-parties”

**Trust Negotiation Basics**

- **Authorization policy** for every open-system resource
  - Describes attributes of authorized users, in terms of digital credentials they must present
  - Resources: services, roles, capabilities, files, directories, credentials, authorization policies

- **Digital credentials**: verifiable, unforgeable attribute attestations
  - Examples: X.509 employee IDs, patient cards, drivers’ licenses, diplomas

- **Run-time negotiation** triggered by access attempt

**Example Trust Negotiation**

- ACME New York Employee Alice
- ACME Chicago Network

  - Access request
  - Policy: ACME employee or local partner? Anti-virus software v12 or higher?
  - ACME employee credential
  - ACME certified network credential
  - Patch level 4 credential
  - Access granted

**Automated, bilateral and iterative** exchange of credentials and policies allows previously unknown users to access previously untrusted resources

**Ongoing and Future Work**

- **Trust negotiation for critical infrastructure** and other high-assurance environments
  - Distributed audit, collusion detection, & accountability mechanisms via virtual fingerprints

- **Multiparty** trust negotiation
  - Theory
  - PeerAccess: formal framework for reasoning about correctness of authorization decisions in distributed systems
  - Systems
    - Heuristic credential search strategies for large networks
    - Appropriate notions of consistency for multiparty negotiations

- **Scalability, robustness** under heavy load and attack