# Trust Management

A Simple, Scaleable Solution to Internet Client Security...

Or is it???

# Panelists

- Li Gong, Javasoft
- Blair Dillaway, Microsoft
- Bob Blakley, IBM
- **Format:**
  - Individual speakers + Questions
  - Group Q & A

# Trust Management

- PolicyMaker [BFL96, 98] (AT&T)
- REFEREE [CFLRS97] (AT&T & W3C)
- Extends the ACL model
  - ACL = yes/no
  - Trust = multi-dimensional
    - *X trusts Y under conditions Z*
    - Model applies **policy** to trust decisions

# Public Key Trust

- Models
  - PGP (web of trust) = key-centric
  - PKIX (X.509) = certificate-centric
  - Chains (Fuzzy) = rooted vs. cross-certificates
- Real world applications
  - PGP, SSL, S/MIME, Code signing

# Issues for this panel

- Authentication vs. Authorization
  - Publisher vs. Permissions the code needs
- Granularity means complexity
- PKI is not fully-baked
  - Certificate POLICY
  - Package-level revocation?
  - Immature legal framework
  - Incomplete standards