Why Do We Trust Standards?

Pascal Meunier
CERIAS Symposium 2009
How do we reason about standards?

• Why do we trust one?
  – How much?
• How do we create one?
• How do we choose one?
  – Is a single flawed standard better than none?
    • Avoid standards paralysis at what cost?
      – e.g., NAC (no clear "winner")
Problems with standards

• Many to choose from
  – Many standards bodies
  – Each with many (ISO: over 17500)
• Controversial standards
• Flawed processes and standards
• Complex standards
• Dictated standards
• Failed standards
Trust Types

- **Direct**
  - You did the evaluation yourself with the appropriate criteria

- **Transitive**
  - Someone else evaluated with criteria appropriate for you

- **Assumptive**
  - Someone did an evaluation...

- **Not having a choice isn't trust**
Position Statement

• We should adopt standards based on transitive trust
  – Have sound justification why we trust them to be appropriate
  – But creation and adoption processes use mostly assumptive trust
    • e.g., countries with different criteria, needs, and political weaknesses vote...

• Retrofitting trust can be as problematic as retrofitting security
Possible Solutions

- Support transitive trust as part of standards themselves by carrying criteria and self-analysis
- Third parties hired to publish flexible evaluation using comprehensive list of criteria
- At adoption, combine appropriate criteria with weights to support decision