Secure Interoperation in a Multi-Domain Environment

Mutli-domain System
A collection of (autonomous and heterogeneous) systems collaborating to accomplish common goals

Security Issues
Semantic heterogeneity
• Different systems may use different security policies or variations of the same
• Naming(Structural) conflict on security attributes(rules)

Principle of autonomy
If an access is permitted within an individual system, it must also be permitted under secure interoperation in a multi-domain environment

Principle of security
If an access is not permitted within an individual system, it must not be permitted under secure interoperation

† Preserving both security and autonomy may not be feasible. Which one can be compromised?
  – Security principle should not be violated
  – Autonomy may be compromised for the greater benefit of information and resource sharing

† An interoperation policy must:
  – Maximize inter-domain information and resource accesses
  – Preserve the security of each collaborating domain
  – Be scalable
  – Allow evolution of domain policies
  – Minimize autonomy violations

General Framework for policy Integration