Group-Centric Secure Information Sharing: 
A Lattice Interpretation

Ravi Sandhu
Executive Director and Endowed Professor
September 14, 2012

ravi.sandhu@utsa.edu, www.profsandhu.com, www.ics.utsa.edu
Secure Information Sharing (SIS)

Goal: Share but protect

Containment challenge
- Client containment
  - Absolute assurance infeasible (e.g., analog hole)
  - Appropriate assurance achievable
- Server containment
  - Typically higher assurance than client

Policy challenge
- How to construct meaningful, usable, agile SIS policy
- How to develop an intertwined information and security model

Object Centric
- Dissemination oriented

Group Centric
- Collaboration oriented
Group-Centric Collaboration

Collaboration Group

Organization 1
Organization 2
Organization 3
Organization n
Individual Experts

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Operational aspects
- Group operation semantics
  - Add, Join, Leave, Remove, Export, Merge, etc
  - Multicast group is one example
- Object model
  - Read-only
  - Read-Write (no versioning vs versioning)
- User-subject model
  - Read-only vs read-write
- Policy specification

Administrative aspects
- Authorization to create group, user join/leave, object add/remove, object export/merge etc.

Group-Centric Collaboration

Collaboration Group

Organization 1

Organization 2

Organization 3

Organization n

Individual Experts

World-Leading Research with Real-World Impact!
Group-Centric Collaboration

Organization 1

Collaboration Group

True Insiders

Expedient Insiders

Individual Experts
Collaboration with Expedient Insiders in Traditional MAC (or LBAC)

Top Secret

Secret

Classified

Unclassified

Individual Experts

Sharing more information than necessary

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Collaboration by Adding a New Security Category in Traditional MAC (or LBAC)

Adding new security category $C$

Existing Lattice

Adding new security category $C$

Modified Lattice after adding new security category $C$

Sharing more information than necessary
Group Centric Collaboration with Expedient Insiders (GEI)
Theorem. GEI is formally equivalent to LCC

CONCLUSION
Traditional MAC (or LBAC) can support collaboration groups NOT with traditional categories BUT with collaboration categories

Sharing just right information sharing
Publications Include


