Group-Centric Models for Secure and Agile Information Sharing

Ravi Sandhu
Executive Director and Endowed Professor
October 2010

ravi.sandhu@utsa.edu, www.profsandhu.com, www.ics.utsa.edu

Goal: 4th Element

- 3 succesful access control models in 40+ years
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
  - Role-base Access Control (RBAC)
- Crucial ingredients for success
  - Strong mathematical foundations
  - Strong intuitive foundations
  - Significant real-world deployment

What is the 4th Element?

- DAC – owner control
- MAC – information flow
- RBAC – organizational/social alignment
- Dynamics/agility
  - Unconstrained DAC: too loose, too fine-grained
  - Group-centric conceived to fill this gap

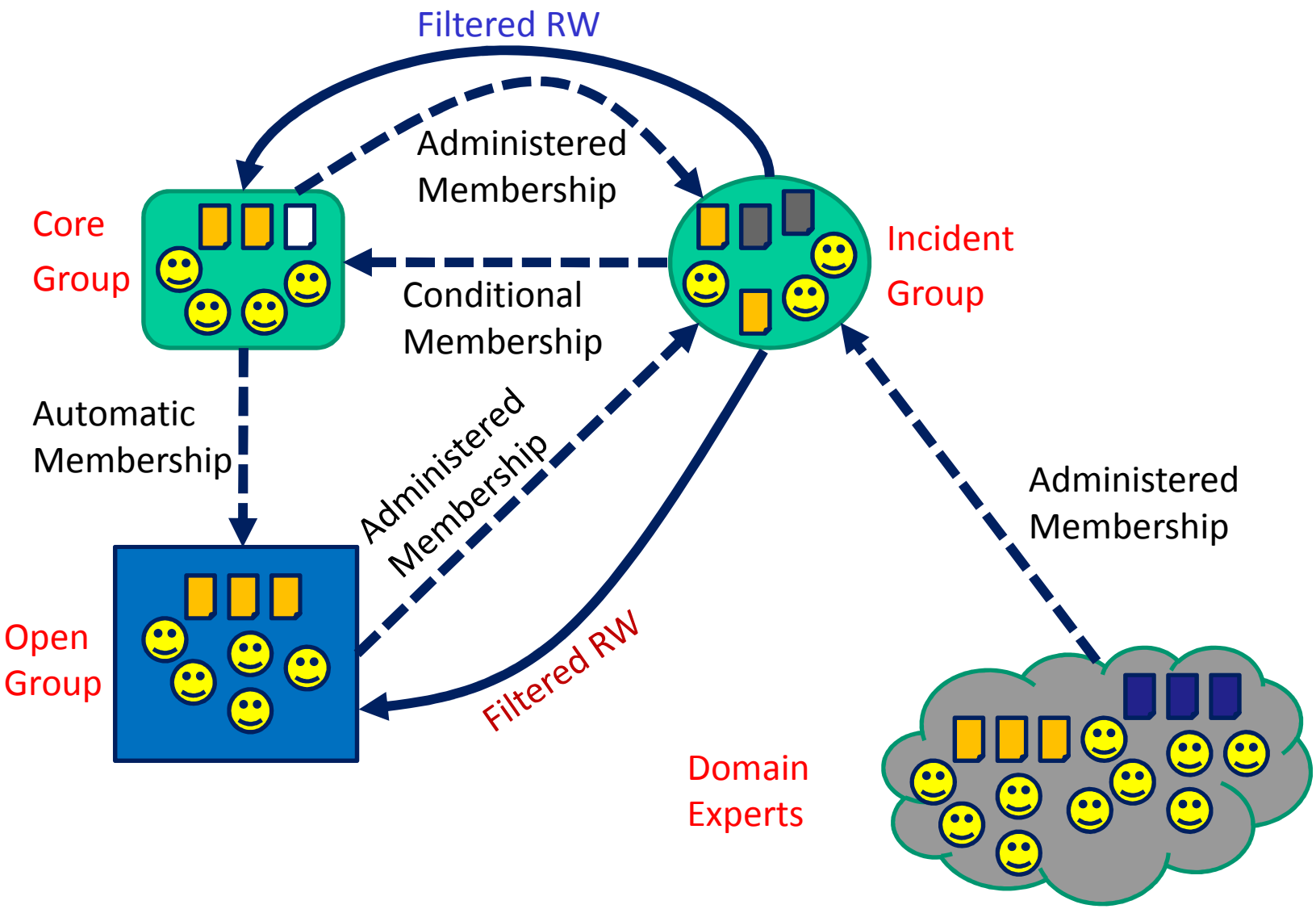
Historical Aside on Dynamics/Agility

- Harrison, Russo and Ullman 1976: HRU
  - dynamics leads to undecidable safety
- Jones, Lipton, Snyder 1978: Take-Grant
  - simple models can be efficiently decidable
- Sandhu, 1988, 1992: SPM, TAM
  - sophisticated models can be efficiently decidable

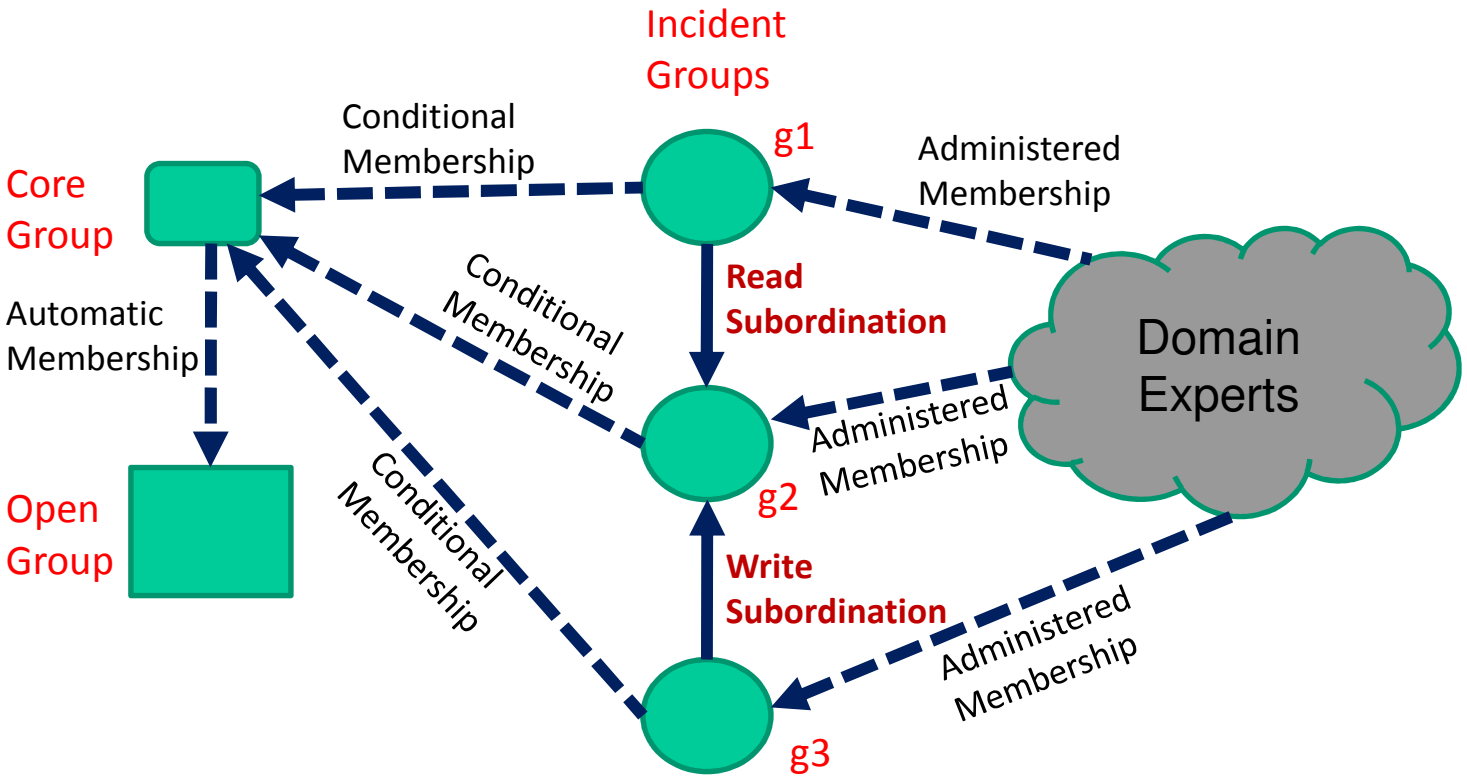
Goal: Share but protect

- Containment challenge
  - Client containment
    - Ultimate assurance infeasible (e.g., the analog hole)
    - Appropriate assurance achievable
  - Server containment
    - Will typically have higher assurance than client containment
- Policy challenge
  - How to construct meaningful, usable, agile SIS policy
  - How to develop an intertwined information and security model

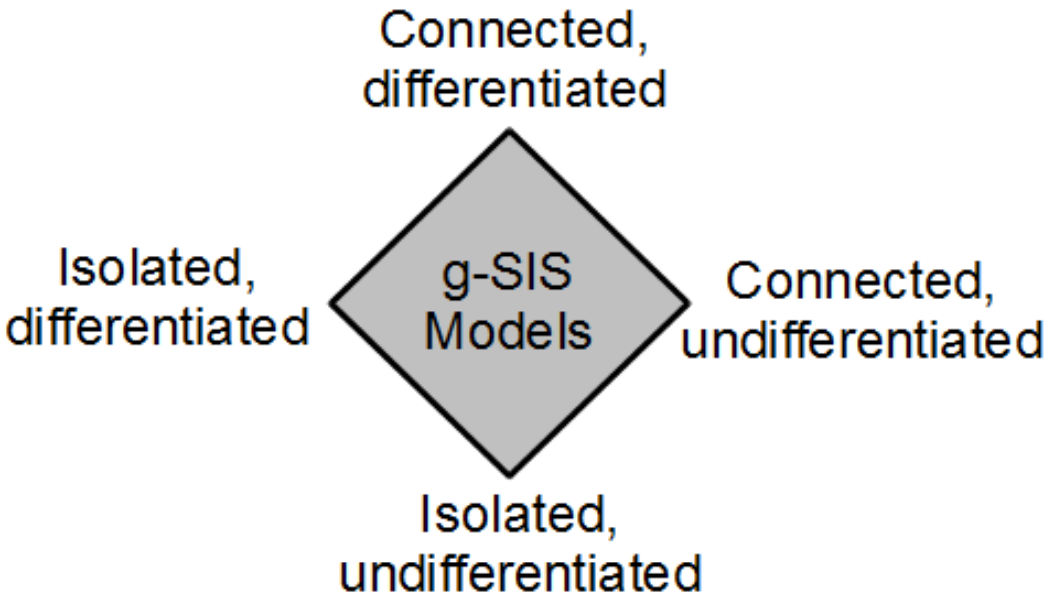
Community Cyber Security



Community Cyber Security

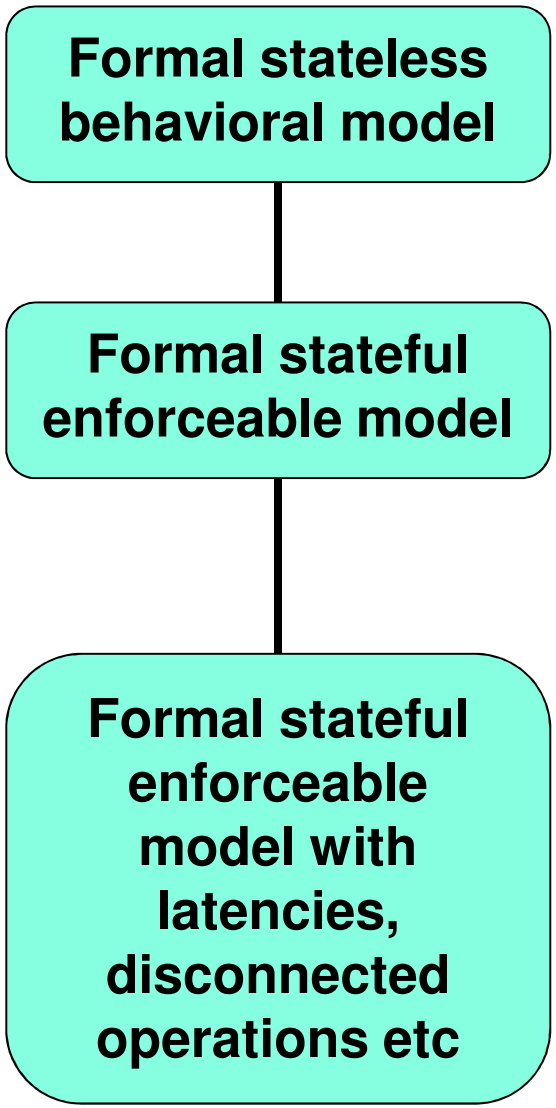


A Family of g-SIS Models



- We have achieved a deep, formal understanding of isolated, undifferentiated groups
- Next challenge: extend the theory to connected, differentiated groups

Formal Models Development



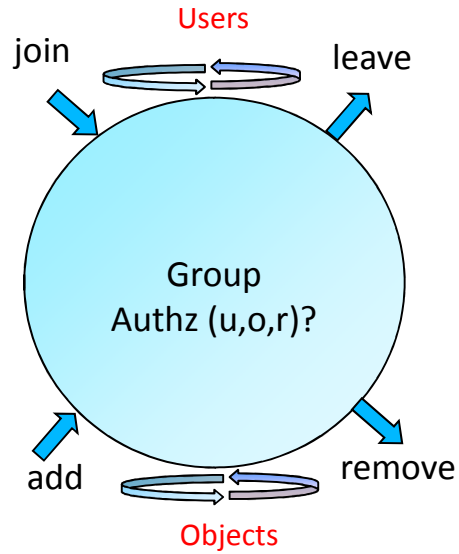
Provable security properties

Proof of equivalence

Proof of safe equivalence

g-SIS Model Components

- Operational aspects
  - Group operation semantics
    - Add, Join, Leave, Remove, 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, etc.



Core Properties

- Authorization Persistence
  - *Authorization cannot change unless some group event occurs*

$$\kappa_0 = \forall u : \mathrm{U}.\forall o : \mathrm{O}.\forall v : \mathrm{V}.\forall g : \mathrm{G}.$$
$$\sqsubset(\mathrm{Authz}(u,o,v,g,\mathbf{r}) \rightarrow (\mathrm{Authz}(u,o,v,g,\mathbf{r})\,\mathcal{W}\,(\mathrm{Join}(u,g) \vee \mathrm{Leave}(u,g) \vee$$
$$\mathrm{Add}(o,v,g) \vee \mathrm{Remove}(o,v,g))))$$

$$\kappa_1 = \forall u : \mathrm{U}.\forall o : \mathrm{O}.\forall v : \mathrm{V}.\forall g : \mathrm{G}.$$
$$\Box(\mathrm{Authz}(u,o,v,g,\mathbf{w}) \rightarrow (\mathrm{Authz}(u,o,v,g,\mathbf{w})\,\mathcal{W}\,\mathrm{Leave}(u,g)))$$

$$\kappa_2 = \forall u : \mathrm{U}.\forall o : \mathrm{O}.\forall v_1 : \mathrm{V}.\forall g : \mathrm{G}.\exists s : \mathrm{S}.\exists v_2 : \mathrm{V}.$$
$$\Box(\neg\mathrm{Authz}(u,o,v_1,g,\mathbf{r}) \rightarrow (\neg\mathrm{Authz}(u,o,v_1,g,\mathbf{r})\,\mathcal{W}\,(\mathrm{Join}(u,g) \vee$$
$$\mathrm{Leave}(u,g) \vee \mathrm{Add}(o,v_1,g) \vee \mathrm{Remove}(o,v_1,g) \vee$$
$$\mathrm{CreateO}(o,v_1,g) \vee \mathrm{update}(s,o,v_2,v_1,g))))$$

$$\kappa_3 = \forall u : \mathrm{U}.\forall o : \mathrm{O}.\forall v_1 : \mathrm{V}.\forall g : \mathrm{G}.\exists s : \mathrm{S}.\exists v_2 : \mathrm{V}.$$
$$\Box(\neg\mathrm{Authz}(u,o,v_1,g,\mathbf{w}) \rightarrow (\neg\mathrm{Authz}(u,o,v_1,g,\mathbf{w})\,\mathcal{W}\,(\mathrm{Join}(u,g) \vee$$
$$\mathrm{CreateO}(o,v_1,g) \vee \mathrm{update}(s,o,v_2,v_1,g))))$$

The π-system Specification

Table 1: The π-system.

$$\chi_0 = \forall u : \mathrm{U}.\forall o : \mathrm{O}.\forall v : \mathrm{V}.\forall g : \mathrm{G}.$$
$$\Box(\mathbf{Authz}(u, o, v, g, \mathbf{r}) \leftrightarrow \exists v_1 : \mathrm{V}.\exists s : \mathrm{S}.(\lambda_0(u, o, v, g) \vee \ldots \vee \lambda_3(u, s, o, v_1, v, g) \vee$$
$$\lambda'_0(u, o, v, g) \vee \ldots \vee \lambda'_4(u, s, o, v_1, v, g)))$$

$$\chi_1 = \forall u : \mathrm{U}.\forall o : \mathrm{O}.\forall v : \mathrm{V}.\forall g : \mathrm{G}.$$
$$\Box(\mathbf{Authz}(u, o, v, g, \mathbf{w}) \leftrightarrow \mathrm{Authz}(u, o, v, g, \mathbf{r}) \wedge (\neg \mathrm{Leave}(u, g)\, \mathcal{S}\, \mathrm{Join}(u, g)) \wedge$$
$$(\exists v_1 : \mathrm{V}.\exists s : \mathrm{S}.\blacklozenge \mathbf{update}(s, o, v_1, v, g) \vee \blacklozenge(\mathrm{LC}(o, v, g) \vee \mathrm{SC}(o, v, g))))$$

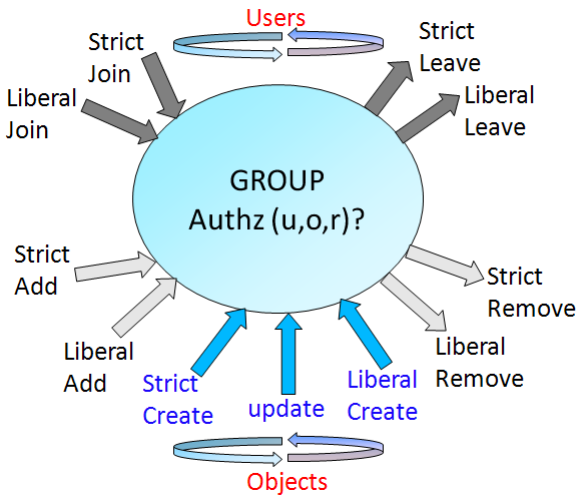
$$\chi_2 = \forall u : \mathrm{U}.\forall s : \mathrm{S}.\forall g : \mathrm{G}.$$
$$\Box(\mathbf{createS}(u, s, g) \rightarrow \blacklozenge \mathbf{Join}(u, g))$$

$$\chi_3 = \forall s : \mathrm{S}.\forall o : \mathrm{O}.\forall v : \mathrm{V}.\forall g : \mathrm{G}.$$
$$\Box(\mathbf{AuthzS}(s, o, v, g, \mathbf{r}) \leftrightarrow \exists u : \mathrm{U}.(\mathbf{Authz}(u, o, v, g, \mathbf{r}) \wedge$$
$$(\neg \mathbf{kill}(u, s, g)\, \mathcal{S}\, \mathbf{createS}(u, s, g))))$$

$$\chi_4 = \forall s : \mathrm{S}.\forall o : \mathrm{O}.\forall v : \mathrm{V}.\forall g : \mathrm{G}.$$
$$\Box(\mathbf{AuthzS}(s, o, v, g, \mathbf{w}) \leftrightarrow \exists u : \mathrm{U}.(\mathrm{Authz}(u, o, v, g, \mathbf{w}) \wedge$$
$$(\neg \mathbf{kill}(u, s, g)\, \mathcal{S}\, \mathbf{createS}(u, s, g))))$$

$$\chi_5 = \forall s : \mathrm{S}.\forall o : \mathrm{O}.\forall v_1, v_2 : \mathrm{V}.\forall g : \mathrm{G}.$$
$$\Box(\mathbf{read}(s, o, v_1, g) \rightarrow \mathbf{AuthzS}(s, o, v_1, g, \mathbf{r})) \wedge$$
$$\Box(\mathbf{update}(s, o, v_1, v_2, g) \rightarrow \mathbf{AuthzS}(s, o, v_1, g, \mathbf{w}))$$

$$\chi_6 = \forall u_1, u_2 : \mathrm{U}.\forall s_1, s_2 : \mathrm{S}.\forall o : \mathrm{O}.\forall v_1, v_2, v_3 : \mathrm{V}.\forall g_1, g_2 : \mathrm{G}.$$
$$\tau_0(u_1, s_1, s_2, o, v_1, v_2, v_3, g_1) \wedge \ldots \wedge \tau_3(u_1, s_1, o, v_1, g_1)$$



$$\pi = \chi_0 \wedge \chi_1 \wedge \chi_2 \wedge \chi_3 \wedge \chi_4 \wedge \chi_5 \wedge \chi_6$$

Sample Stateful Specification

Authz (s,o,r) ->

Add-TS(o) > Join-TS(s) &

Leave-TS(s) = NULL &

Remove-TS(o) = NULL

Summary

- The 4th element, crucial for dynamic/agile secure information sharing
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
  - Role-base Access Control (RBAC)
  - Group-centric Secure Information Sharing (g-SIS)
- Crucial ingredients for success
  - Strong mathematical foundations
  - Strong intuitive foundations
  - Significant real-world deployment

Publications

- Ram Krishnan, Jianwei Niu, Ravi Sandhu and William Winsborough, "Group-Centric Secure Information Sharing Models for Isolated Groups." *ACM Transactions on Information and System Security*, accepted with minor revision.
- Ravi Sandhu, Ram Krishnan and Gregory White, "Towards Secure Information Sharing Models for Community Cyber Security." In *Proceedings 5th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, Chicago, Illinois, October 9-12, 2010.
- Ravi Sandhu, Ram Krishnan, Jianwei Niu and William Winsborough, "Group-Centric Models for Secure and Agile Information Sharing." In *Proceedings 5th International Conference, on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010, St. Petersburg, Russia, September 8-10, 2010*, pages 55-69. Published as Springer Lecture Notes in Computer Science Vol. 6258, *Computer Network Security* (Igor Kotenko and Victor Skormin, editors), 2010.
- Ram Krishnan, Ravi Sandhu, Jianwei Niu and William Winsborough, "Towards a Framework for Group-Centric Secure Collaboration." In *Proc. 5th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, Crystal City, Virginia, November 11-14, 2009, pages 1-10.
- Ram Krishnan and Ravi Sandhu, "A Hybrid Enforcement Model for Group-Centric Secure Information Sharing." *Proc. IEEE International Conference on Computational Science and Engineering (CSE-09)*, Vancouver, Canada, August 29-31, 2009, pages 189-194.
- Ram Krishnan, Ravi Sandhu, Jianwei Niu and William Winsborough, "Formal Models for Group-Centric Secure Information Sharing." *Proc. 14th ACM Symposium on Access Control Models and Technologies (SACMAT)*, Stresa, Italy, June 3-5, 2009, pages 115-124.
- Ram Krishnan, Ravi Sandhu, Jianwei Niu and William Winsborough, "A Conceptual Framework for Group-Centric Secure Information Sharing." *Proc. 4th ACM Symposium on Information, Computer and Communications Security (AsiaCCS),* Sydney, Australia, March 10-12, 2009, pages 384-387.
- Ram Krishnan, Jianwei Niu, Ravi Sandhu and William Winsborough, "Stale-Safe Security Properties for Group-Based Secure Information Sharing." *Proc. 6th ACM-CCS Workshop on Formal Methods in Security Engineering (FMSE),* Alexandria, Virginia, October 27, 2008, pages 53-62.