RT-Based Administrative Models for Community Cyber Security Information Sharing

Ravi Sandhu, Khalid Zaman Bijon, Xin Jin, Ram Krishnan
Institute for Cyber Security
University of Texas at San Antonio

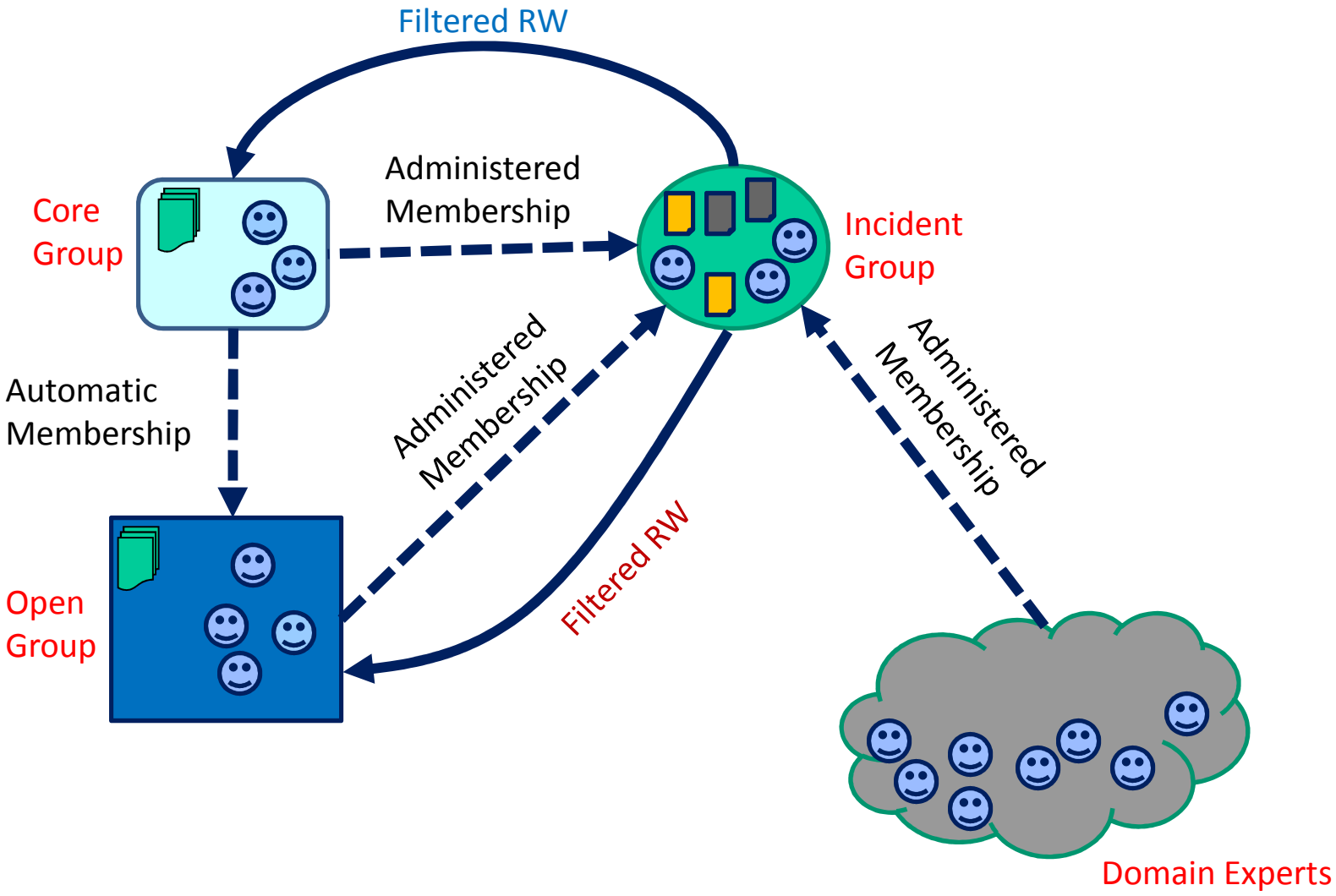
Oct. 15, 2011
International Workshop on Trusted Collaboration

Community Cyber Security

- Community is well demarcated geographical boundary
  - E.g. county or larger city
- Secure Information Sharing in Community
- Center for Infrastructure Assurance and Security (CIAS)
  - communication, incident response, disaster recovery, etc
- Sandhu et al[1] proposed an informal requirements for information sharing for cooperative cyber incident management in a community

[1]R. Sandhu, R. Krishnan, and G. White. Towards secure information sharing models for community cyber security. In Proc. 6th IEEE Int. Conf. on Collaborative Computing, 2010.

Community Cyber Security



Administrative Model

- [1]Role Based Trust Management (RT) framework
  - Strong mathematical foundation, explicit inclusions of roles, sizeable literature

- The basic constructs of RT_0
  - Entities (A, B_1, Alice, etc)
  - Role names (r, r_1, student, etc)
  - Role (A.r, $B_1.r_1$, U_1.student, etc)

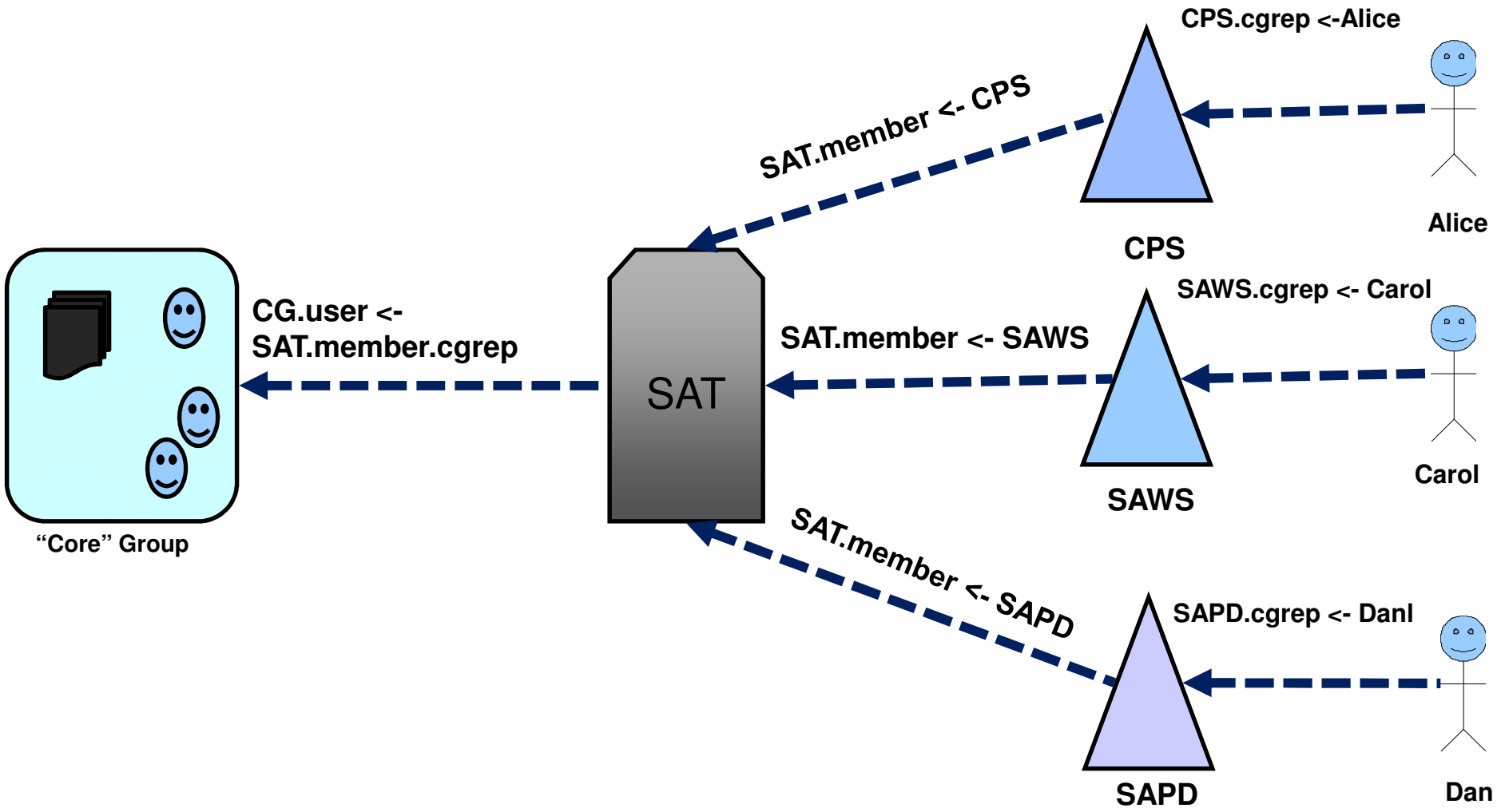
- Four types of credentials (An Entity can issue)
  - Simple Member: $A.r \leftarrow D$
  - Simple Inclusion: $A.r \leftarrow B.r$
  - Linking Inclusion: $A.r \leftarrow A.r_1.r_2$
  - Intersection Inclusion: $A.r \leftarrow B_1.r_1 \cap B_2.r_2$

[1]N. Li, J. C. Mitchell, and W. H. Winsborough. Design of a rolebased trust management framework. In Proc. of the IEEE Symposium on Security and Privacy, May 2002, 2010.

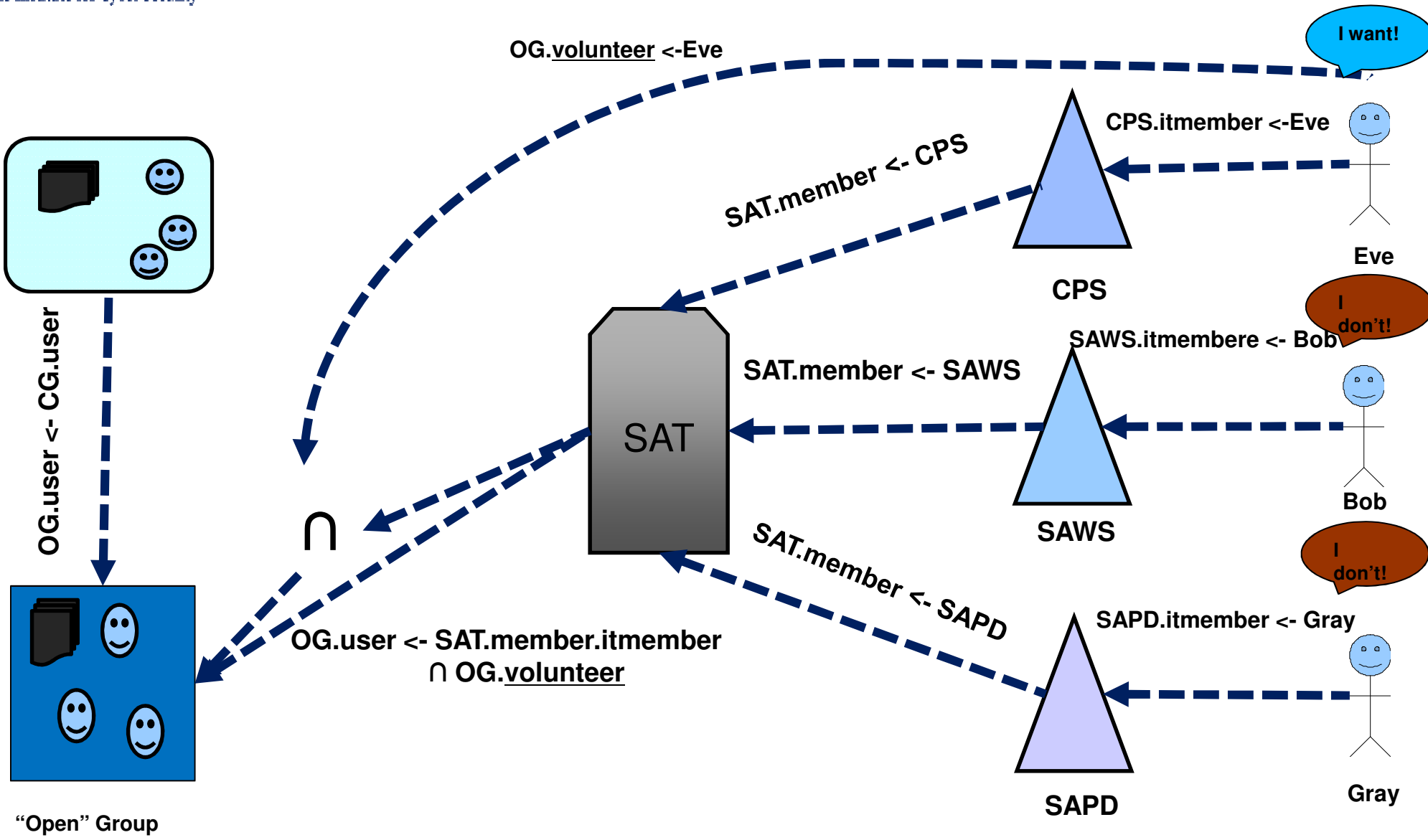
Community Elements

- Community Entities
  - CG (core group), OG (open group), IG (incident group)
  - CPS (San Antonio Energy Utility), SAWS (San Antonio Water System), SAPD (San Antonio Police Department)
  - SAT (Hypothetical Entity that represents the community), etc
- Roles
  - CG.user (All core group users)
  - SAT.member (Members of San Antonio Community)
  - CPS.itmember (IT members of CPS), etc

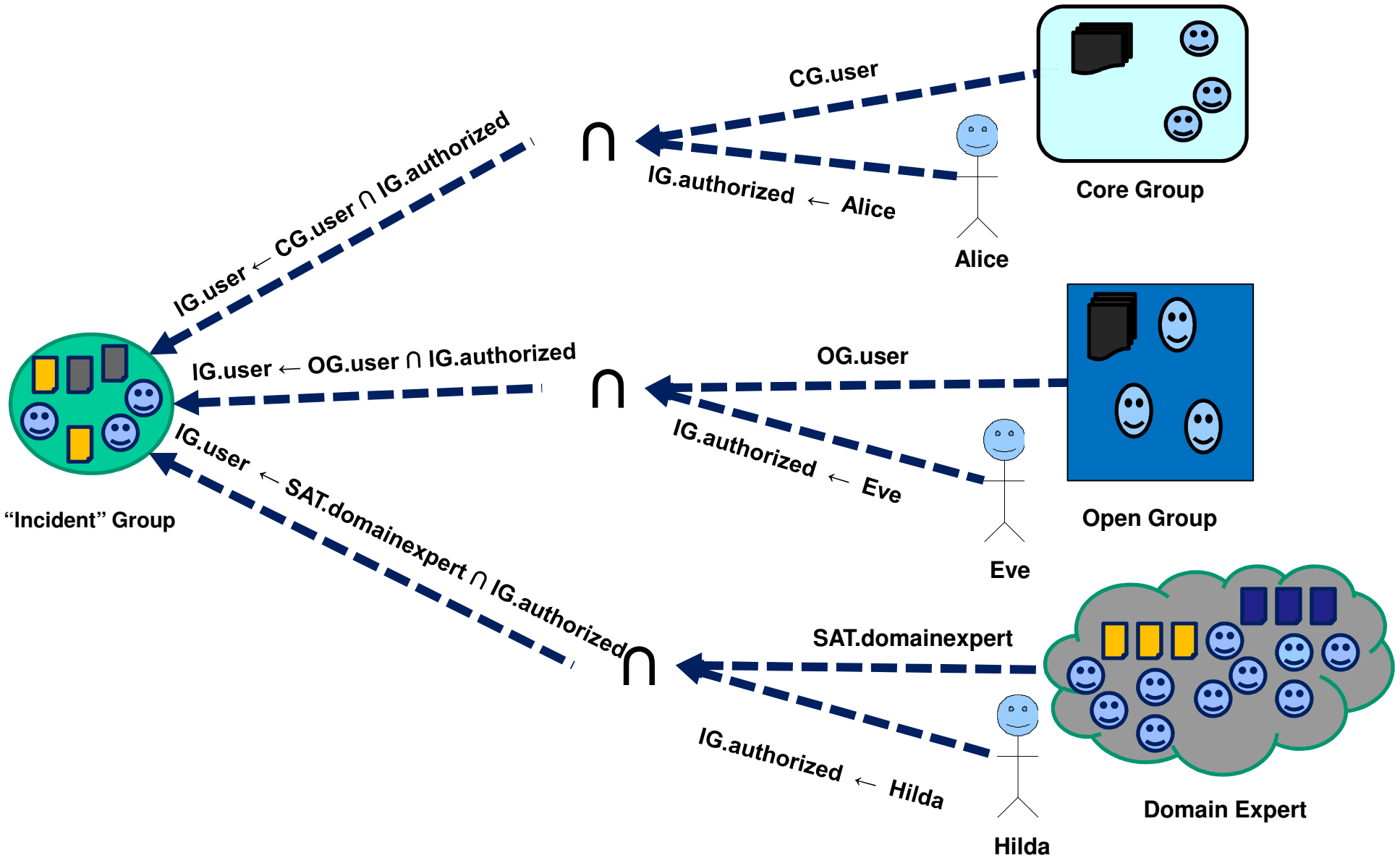
Membership Management (Core Group)



Membership Management (Open Group)



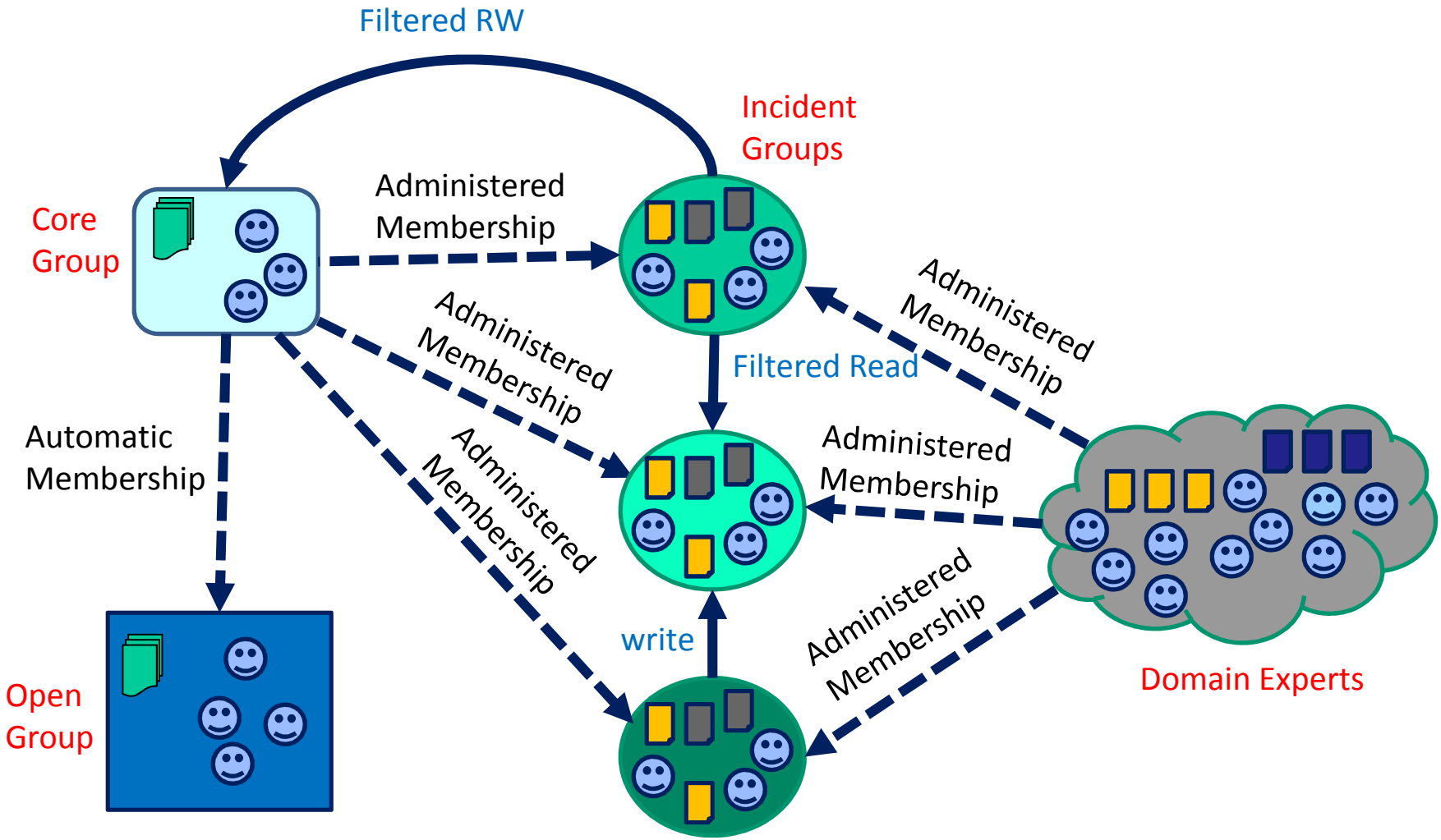
Membership Management (Incident Group)



Extended Features

- Single Document Releases to An Incident Group
  - Using RT_1 and RT_Θ
  - An incident group can request a particular document to core
  - Parameterized Role CG.read(?o) can read single object ?o upon approval from core
  - A CG.user can approve it if he is not an IG.user of that Incident group
- Delegation of Role Activation
  - Using RT^D

Community Cyber Security



Conclusion

- RT as an administrative model in this context

- Limitations of RT approach
  - Entity-Owned only membership
  - Reverse Credential Chains
  - Unable to Support Administration from an External Entity