Purpose-Centric Secure Information Sharing

Ravi Sandhu
Executive Director and Endowed Professor
Institute for Cyber Security (ICS)
University of Texas at San Antonio

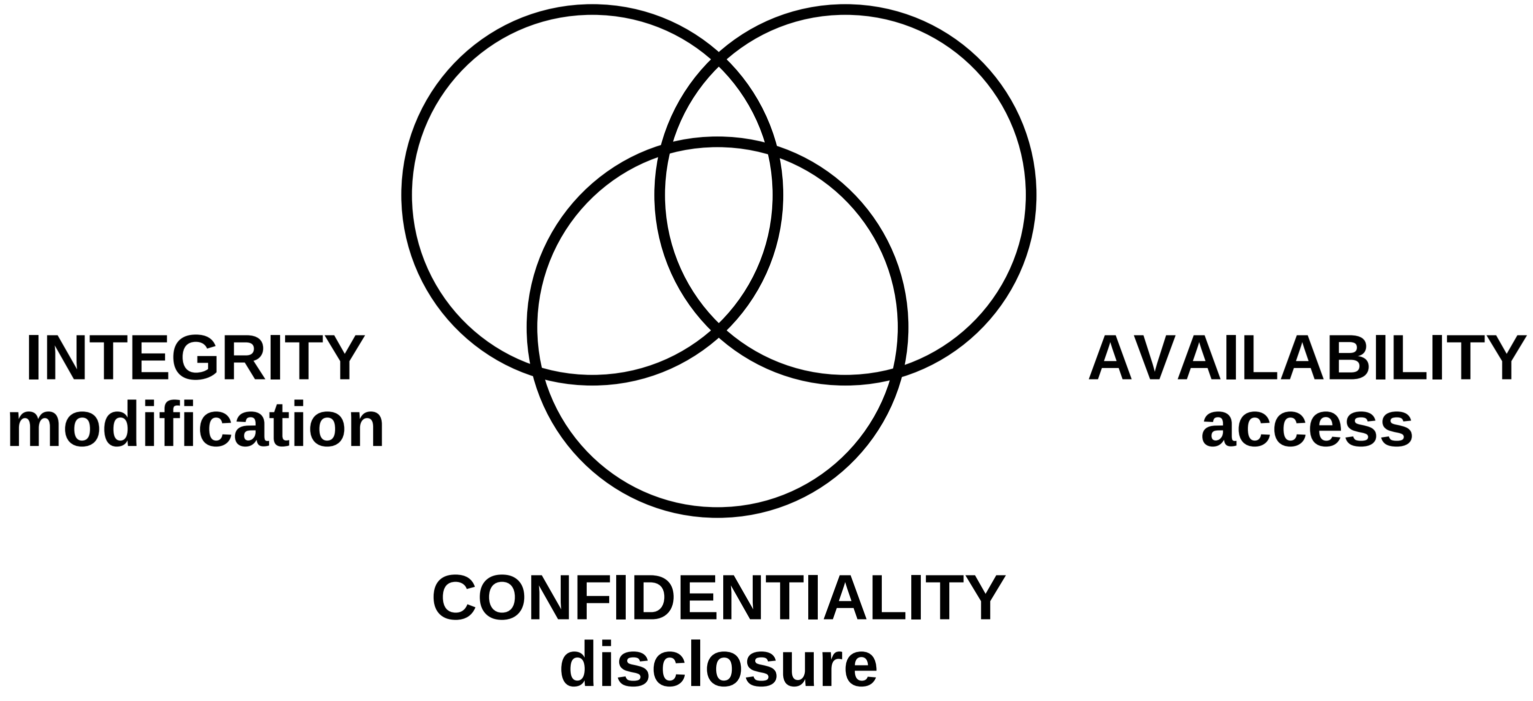
September 2009

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

Butler Lampson Paraphrased (I think)

- Computer scientists could never have designed the web because they would have tried to make it work.
  But the Web does “work.”
  What does it mean for the Web to “work”?
- Security geeks could never have designed the ATM network because they would have tried to make it secure.
  But the ATM network is “secure.
  What does it mean for the ATM network to be “secure”?

Security Objectives

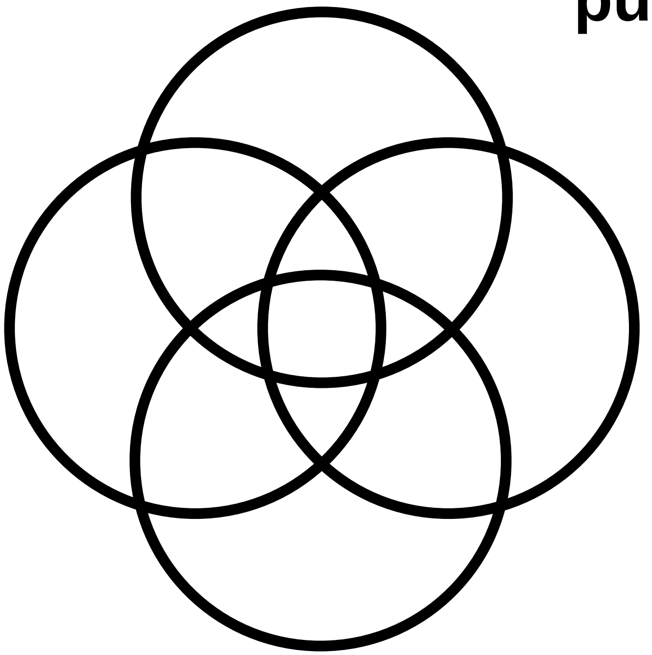


INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives



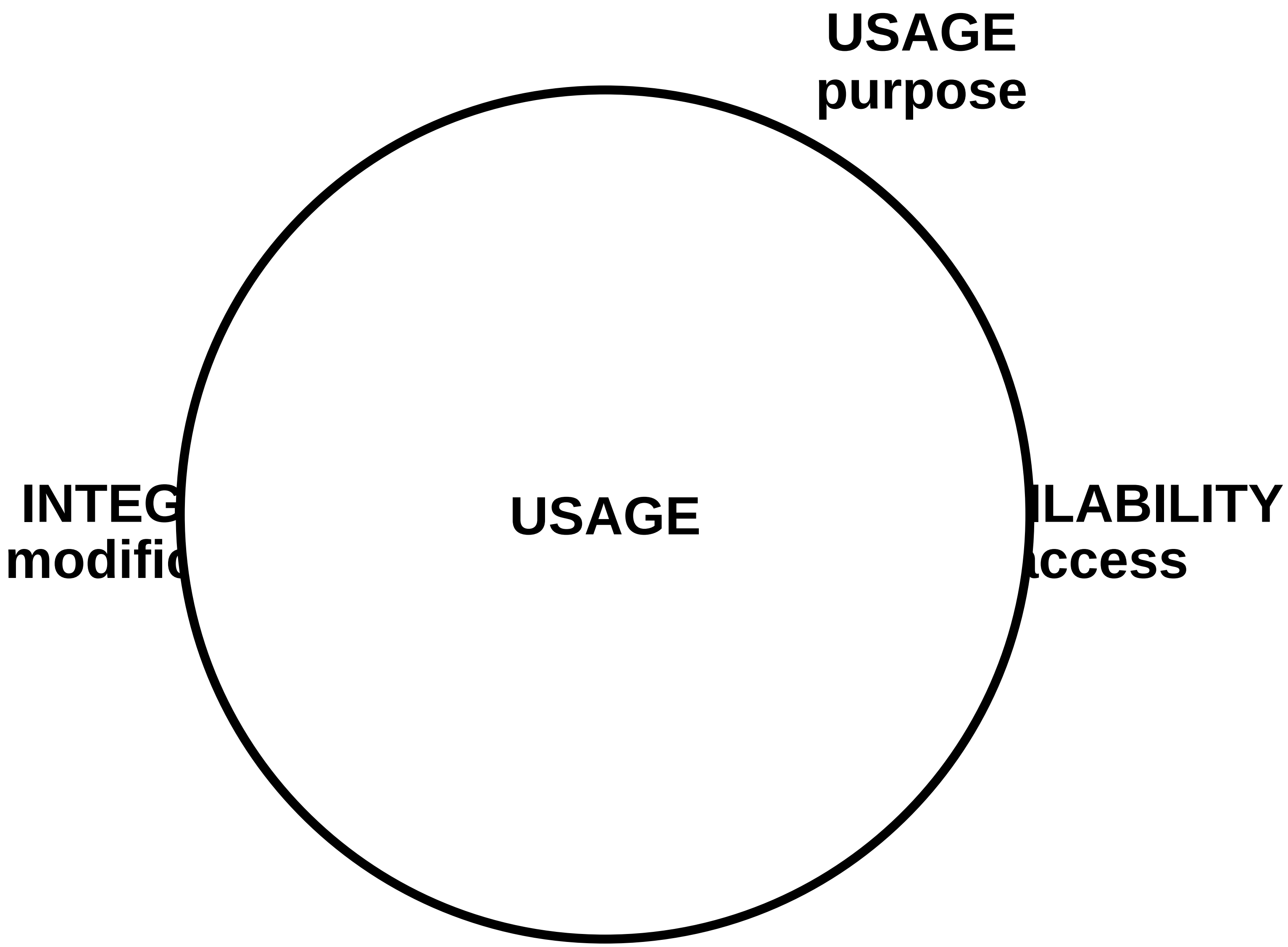
USAGE
purpose

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives



USAGE
purpose

INTEG
modific

USAGE

ILABILITY
ccess

Information Sharing Modes

Fundamental Goal: Share BUT Protect

I. Dissemination-Centric Sharing

- Digital Rights Management
- Enterprise Rights Management
- XrML

II. Query-Centric Sharing

- Queries wrt a protected dataset
- Several talks yesterday focused on privacy protection
- More generally de-aggregation/inference protection

III. Purpose-Centric Sharing

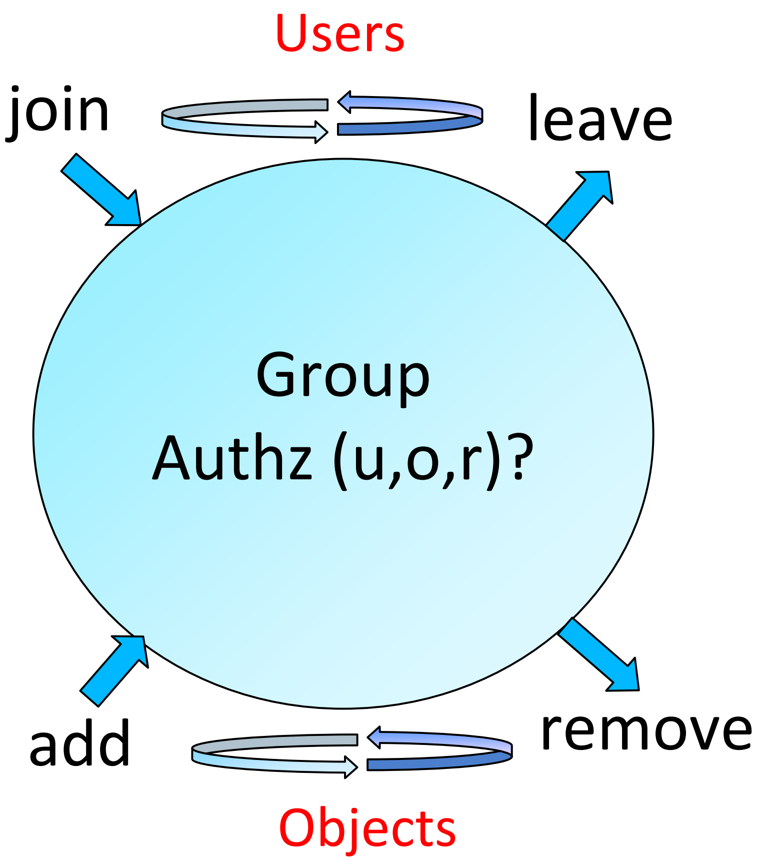
- Sharing for a purpose
- Mission-centric sharing
- Group-centric sharing

Information Protection Models

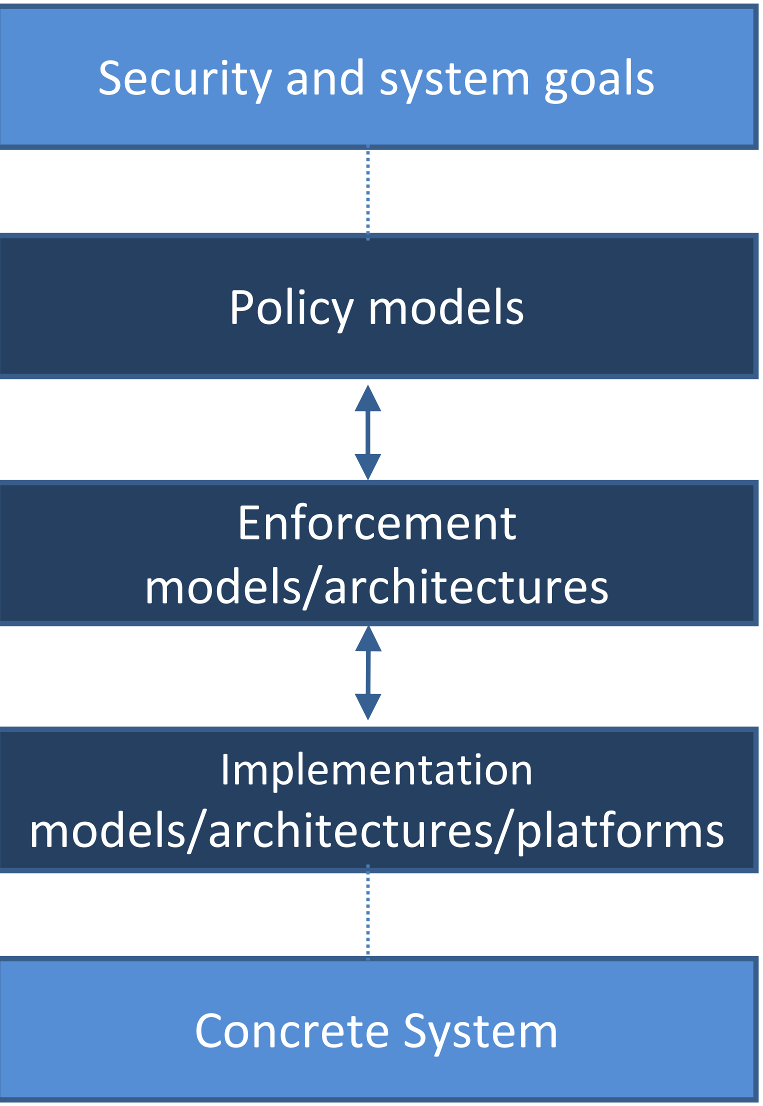
- Discretionary Access Control (DAC)
  - Owner-based discretion
  - Classic formulation fails to distinguish copy from read
- Lattice-Based Access Control (LBAC)
  - One directional information flow in a lattice of security labels
  - Rigid and coarse-grained due to strict one-directional information flow within predefined security labels
- Role-Based Access Control (RBAC)
  - Role is central, administration is simplified
  - Flexible: can be configured to do DAC or LBAC
  - Role engineering/discovery is challenging
- Attribute-Based Access Control (ABAC)
  - Subsumes security labels, roles and more
  - Attribute engineering even more challenging
- Usage Control (UCON)
  - ABAC on steroids
  - Consumable rights, usage limits, obligations, conditions

Group-Centric Sharing (g-SIS)

- Brings users & objects together in a group for some purpose
- Metaphor: secure meeting room
- Research goal: combine elements of DAC, LBAC, RBAC, ABAC, UCON, g-SIS into a coherent framework for purpose-centric information sharing while leveraging dissemination-centric and data-centric information sharing
- Initial focus: understand and formalize g-SIS



PEI Layers World-View


Security and system goals
Policy models
Enforcement models/architectures
Implementation models/architectures/platforms
Concrete System

- Necessarily informal

- Specified in terms of users, subjects, objects, administrators, labels, roles, groups, etc. in an idealized setting.
- Security analysis (e.g. security objectives, security properties, etc.)

- Approximated policy realized using system architecture with trusted servers, secure protocols, etc. in a real-world setting
- Enforcement level security analysis (e.g. safe approximations with respect to network latency, protocol proofs, security properties, etc.)

- Technologies and standards such as SOA, Cloud, SaaS, TCG/TPM, MILS, X.509, SAML, XACML, Oath, Oauth, etc.
- Implementation level security analysis (e.g. vulnerability analysis, penetration testing, protocol proofs, security properties, etc.)

- Layered software stacks executing on hardware

Published Results to Date

- Ram Krishnan, Ravi Sandhu, Jianwei Niu and William Winsborough, Foundations for Group-Centric Secure Information Sharing Models. *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.
- Ram Krishnan and Ravi Sandhu, A Hybrid Enforcement Model for Group-Centric Secure Information Sharing. *Proc. IEEE International Symposium on Secure Computing (SecureCom-09)*, Vancouver, Canada, August 29-31, 2009.
- Ram Krishnan and Ravi Sandhu, Enforcement Architecture and Implementation Model for Group-Centric Information Sharing. *Proc. 1st International Workshop on Security and Communication Networks (IWSCN)*, Trondheim, Norway, May 20-22, 2009.