Grand Challenges in Data Usage Control

Prof. Ravi Sandhu
Executive Director and
Endowed Chair

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

Fundamental Premise

- Cyber Security is about tradeoffs
  - confidentiality, integrity, availability, usage, privacy, cost, usability, productivity, etc
- Tradeoffs require application context

Productivity **Security**

Let's build it
Cash out the benefits
Next generation can secure it

Let's not build it
Let's bake in super-security to make it unusable/unaffordable

The cyber security grand challenge

Sweet spots exist
How to predictably find them?

Sweet Spots Exist

- Proof point: Automatic Teller Machines
  - secure enough
  - global and growing
  - not pitched as a success story
- Proof points: others in consumer space
  - on-line banking
  - e-retail
  - electronic payments (suggested by David Chadwick)
- Proof points: beyond consumer space
  - US President's nuclear football
  - secret formula for Coca Cola

Limits of Data Usage Control

- Once data has escaped into the wild it cannot be recaptured
  - Closing the barn door after the horse has fled and been cloned multiple times
- Data can leak from legitimate recipients through analog and digital holes
  - Mal-users can leak
  - Mal-ware can leak (w/o requiring mal-users)

Preventive Technologies have Absolute Limits
Detection and Recourse Technologies have Scaling Limits

What is Data Usage Control

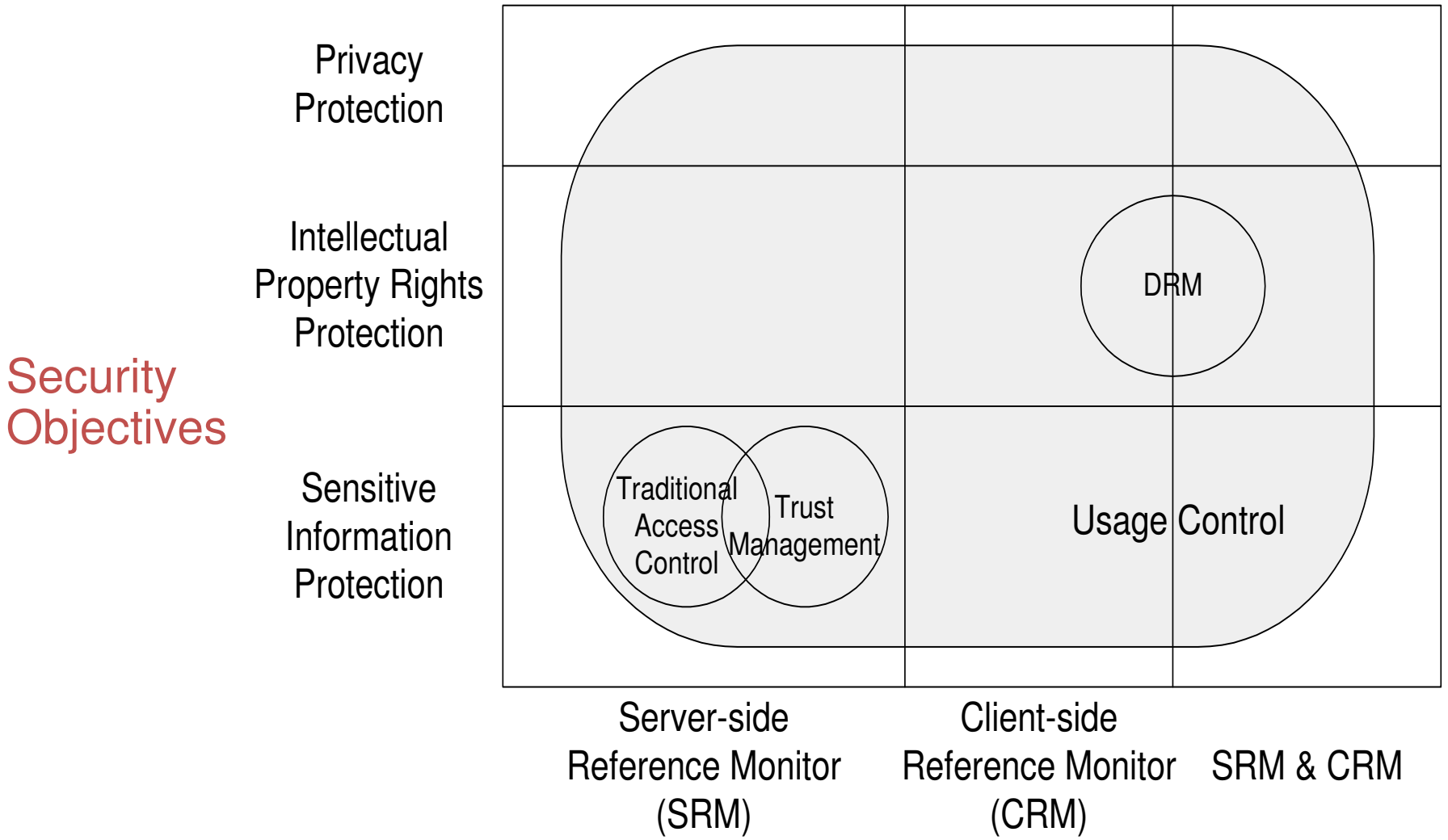
- Jaehong Park and Ravi Sandhu. 2004. The $UCON_{ABC}$ usage control model. *ACM Trans. Inf. Syst. Secur.* 7, 1 (February 2004), 128-174.

  • **Emphasis on authorizations and obligations before and during usage**

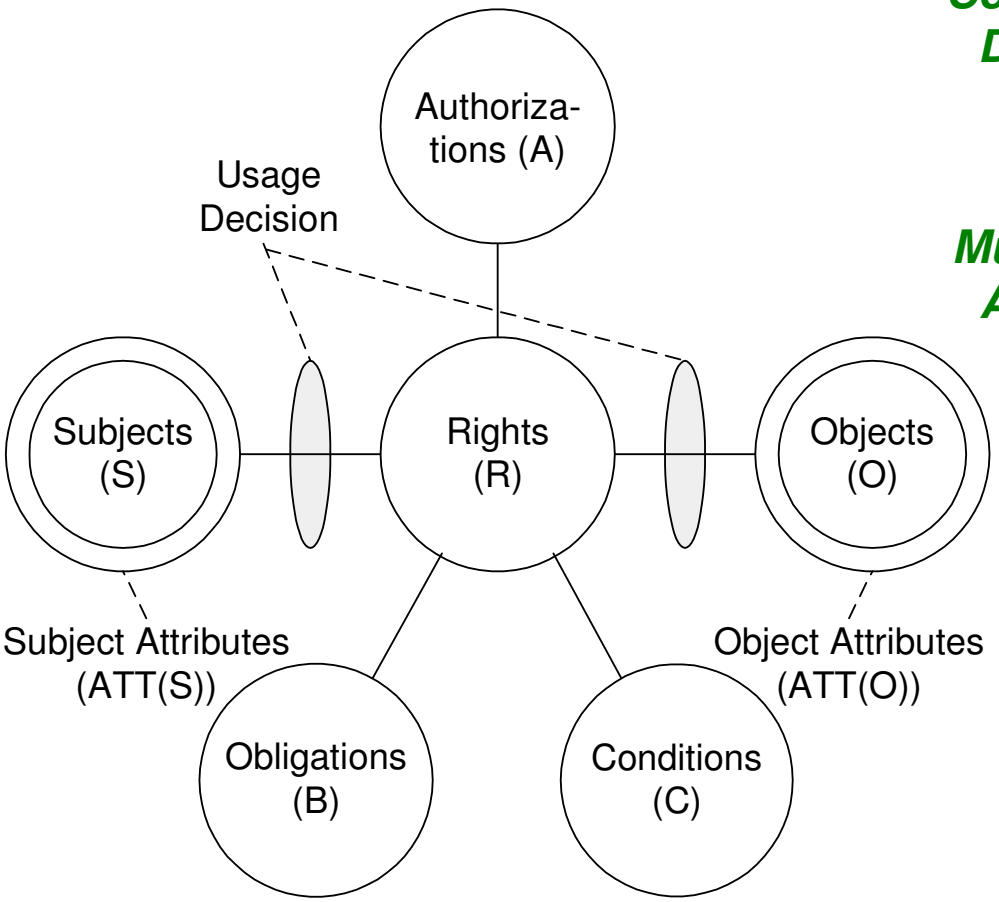
- Alexander Pretschner, Manuel Hilty, and David Basin. 2006. Distributed usage control. *Commun. ACM* 49, 9 (September 2006), 39-44.

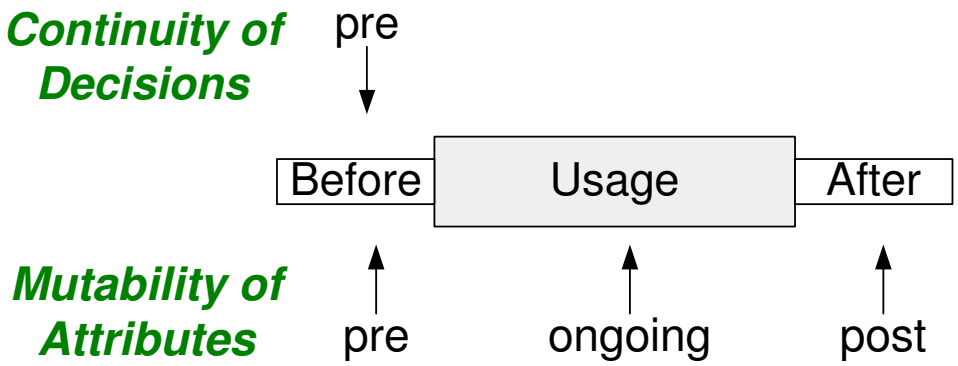
  • **Emphasis on post-usage obligations**

Usage Control Motivators



$UCON_{ABC}$ Models





Continuity

Decision can be made during usage for continuous enforcement

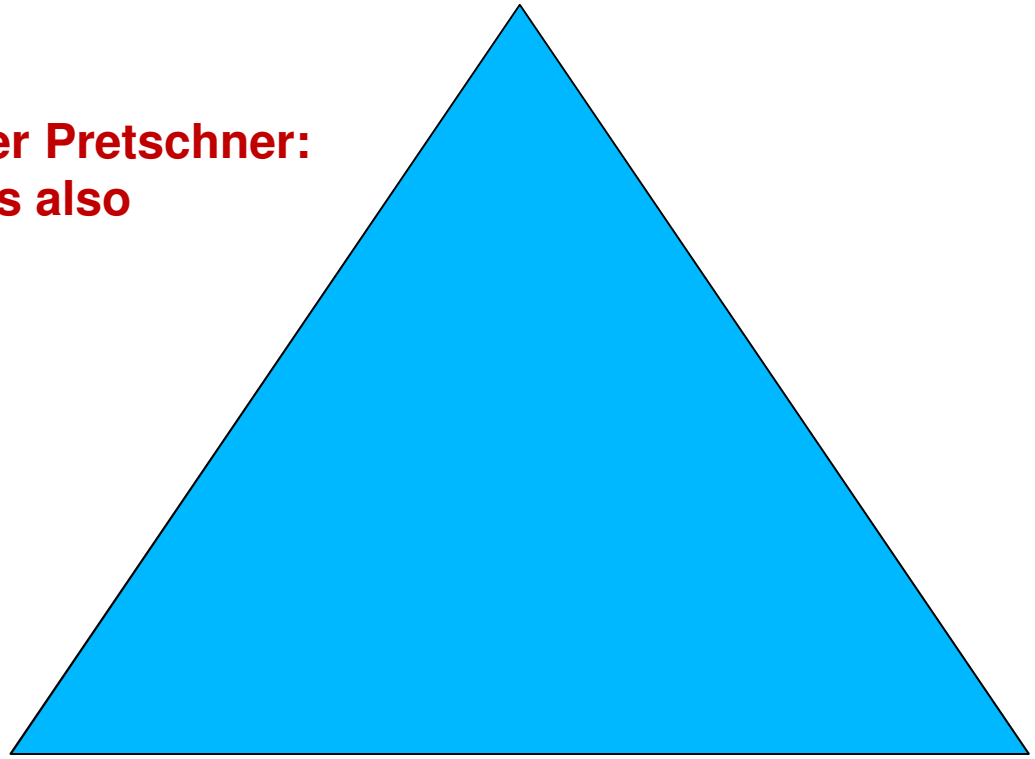
Mutability

Attributes can be updated as side-effects of subjects' actions

Contexts for Data Usage

C
Individual Consumer

Comment by Alexander Pretschner:
Need attacker contexts also



P
Individual Professional

B
Business Enterprises

Contexts for Data Usage

	C	P	B
C	Social NW (consumer)	B2C lite	B2C
P	--	Social NW (professional)	B2B lite
B	--	--	B2B

Contexts crossover and bleed into one another

Data Usage Control Laws (USA)

- Fair Credit Reporting Act (FCRA)
  - 1970 onwards
- Internal Revenue Service
- Federal Bureau of Investigation (FBI) vis a vis Central Intelligence Agency (CIA) and National Security Agency (NSA)
  - pre and post 9/11
- Family Educational Rights and Privacy Act (FERPA)
  - 1974 onwards

Digital Rights Management

- Digital Audio Tape (DAT)
- iTunes

Grand Challenges

- Laws, norms, business contracts are all necessary
- What can be done technically
  - The Containment Challenge
  - The Policy Challenge
  - The Reality Challenge

- Not included in delivered talk:
  - How should microsec and macrosec play into this?