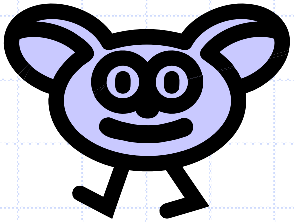
Flexible, fine-grained distributed access control

John Mitchell
Stanford

with Adam Barth, Anupam Datta, Ninghui Li (Purdue), Helen Nissenbaum (NYU), Will Winsborough, ….

April 2006

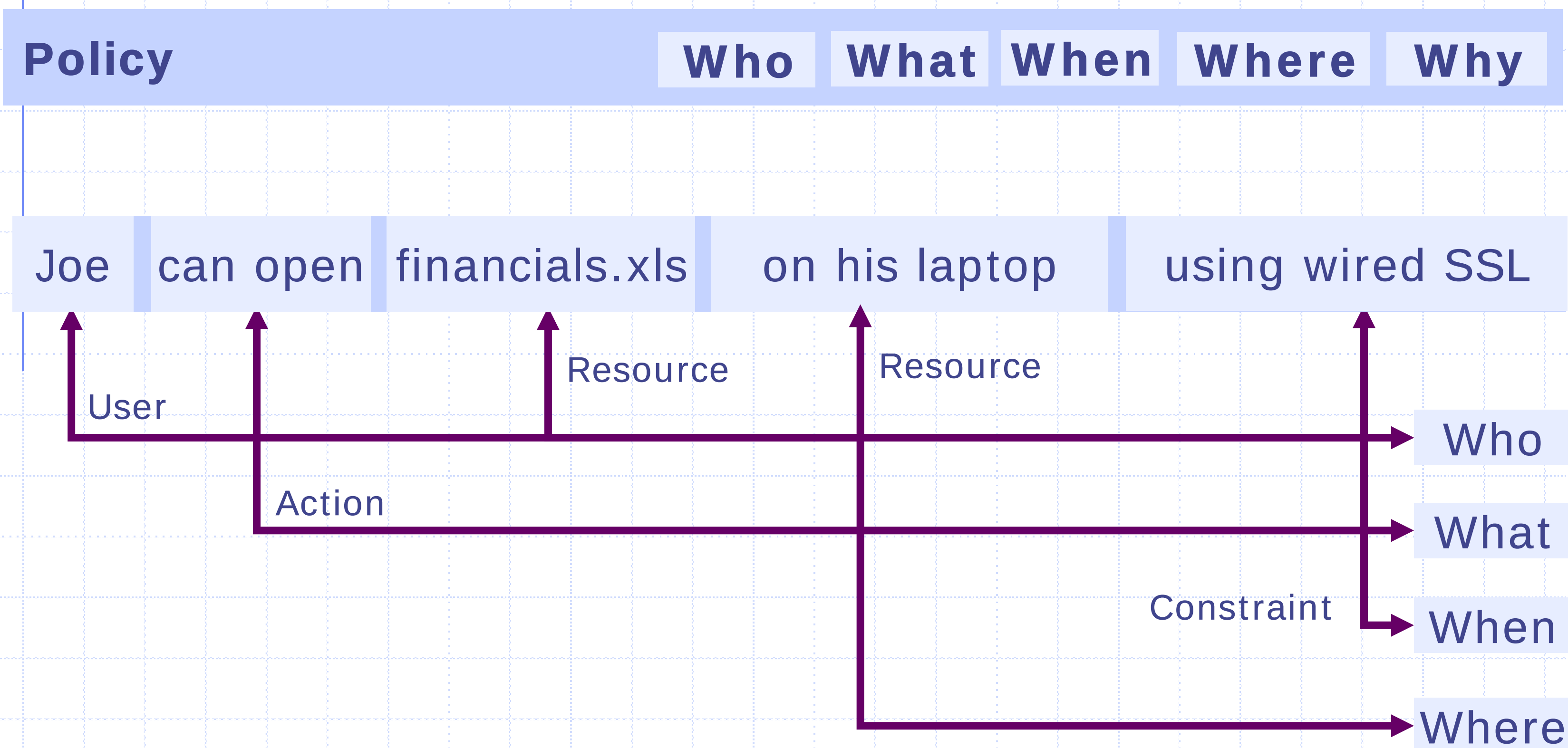
We’re all ears



- What policy concepts are important in healthcare?
- What kind of systems should understand or enforce these policies?
- How can tech geeks be useful?
- What’s all this talk about Brazilian skiing?

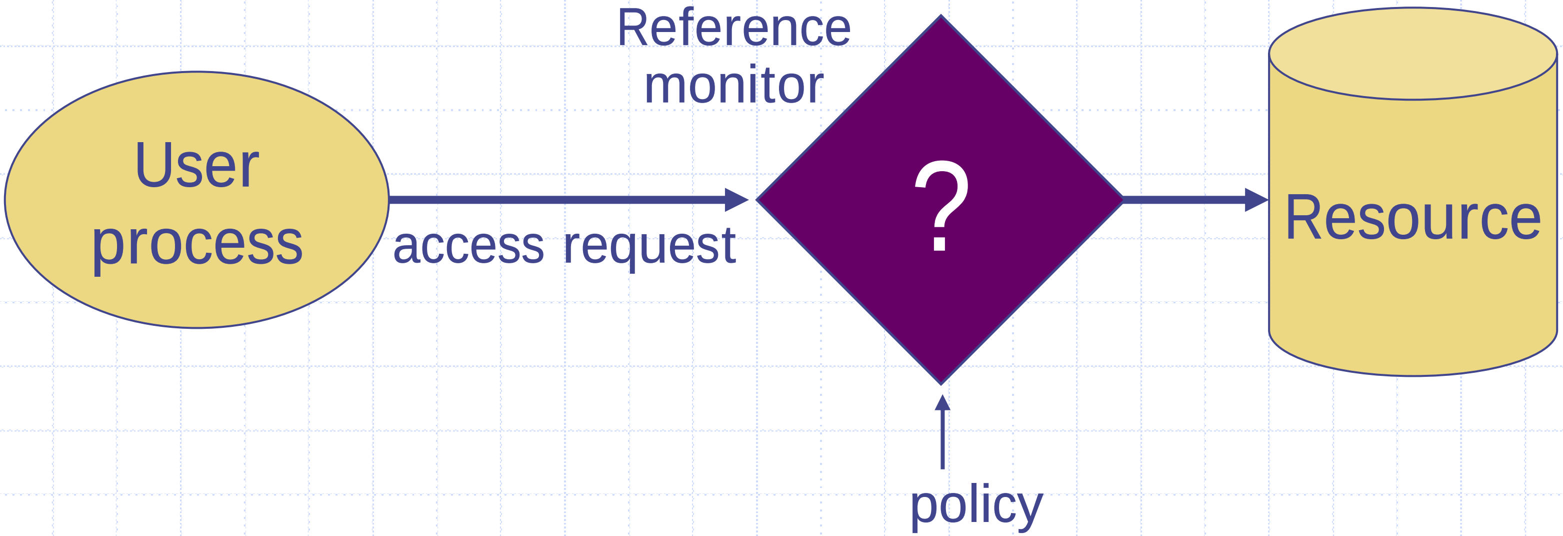
mitchell@cs.stanford.edu abarth@cs.stanford.edu

Enterprise Access Control



Traditional mechanisms

- Assumptions
  - System knows who the user is
    - User has entered a name and password, or other info
  - Access requests pass through gatekeeper
    - System must not allow monitor to be bypassed



Access control matrix [Lampson]

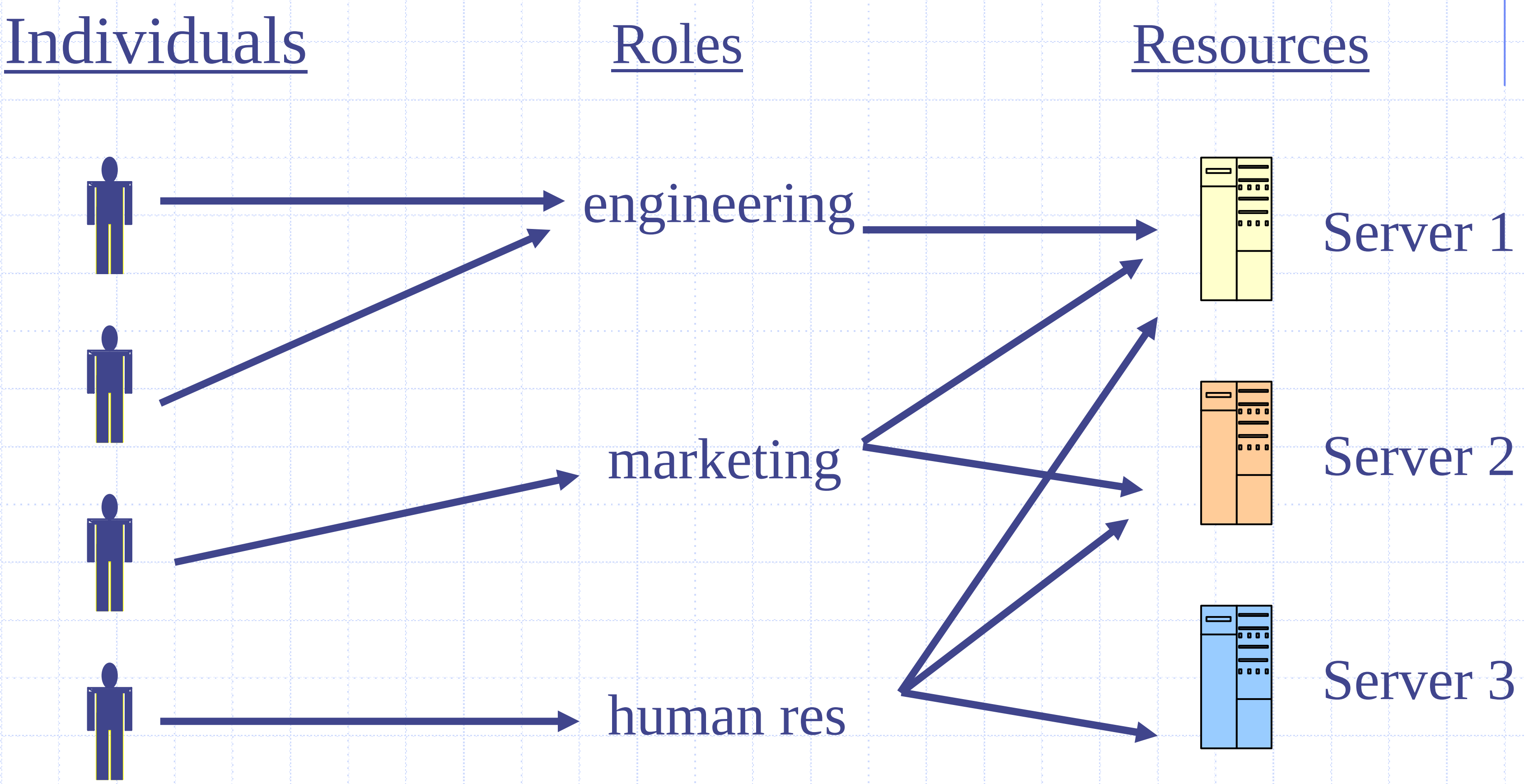
Objects

Subjects

	File 1	File 2	File 3	…	File n
User 1	read	write	-	-	read
User 2	write	write	write	-	-
User 3	-	-	-	read	read
…					
User m	read	write	read	write	read

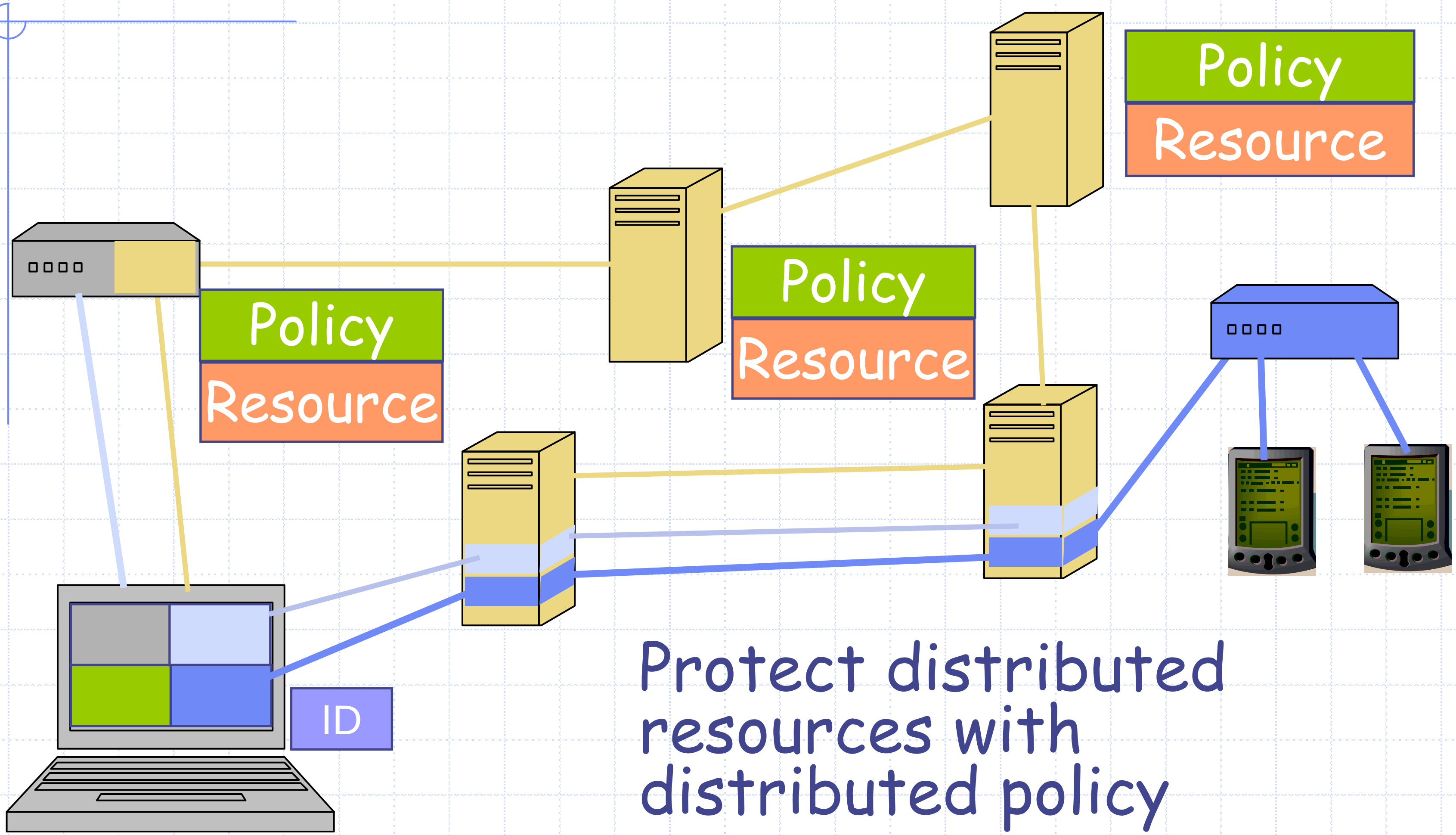
Access control list (ACL): column of matrix, often stored at resource

Role-Based Access Control



Leverage: user's change more frequently than roles

Distributed Access Control

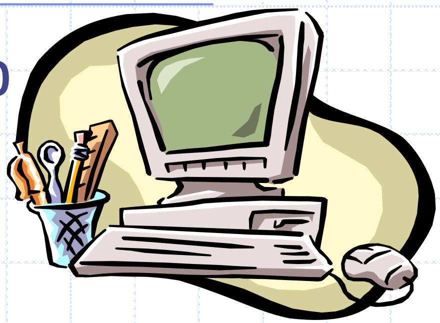


Protect distributed resources with distributed policy

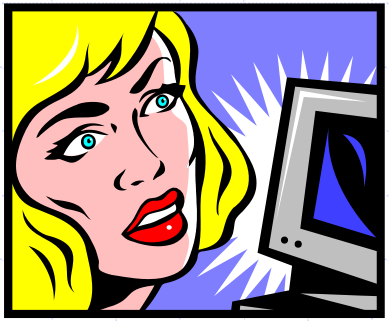
Policy at site A may govern resources at site B

Decentralized Policy Example

EPub



Alice



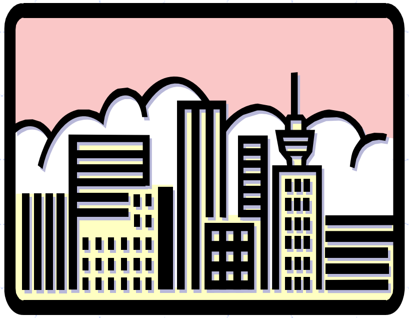
Grants access to university students

Trusts universities to certify students

Trusts ABU to certify universities

Alice is a student

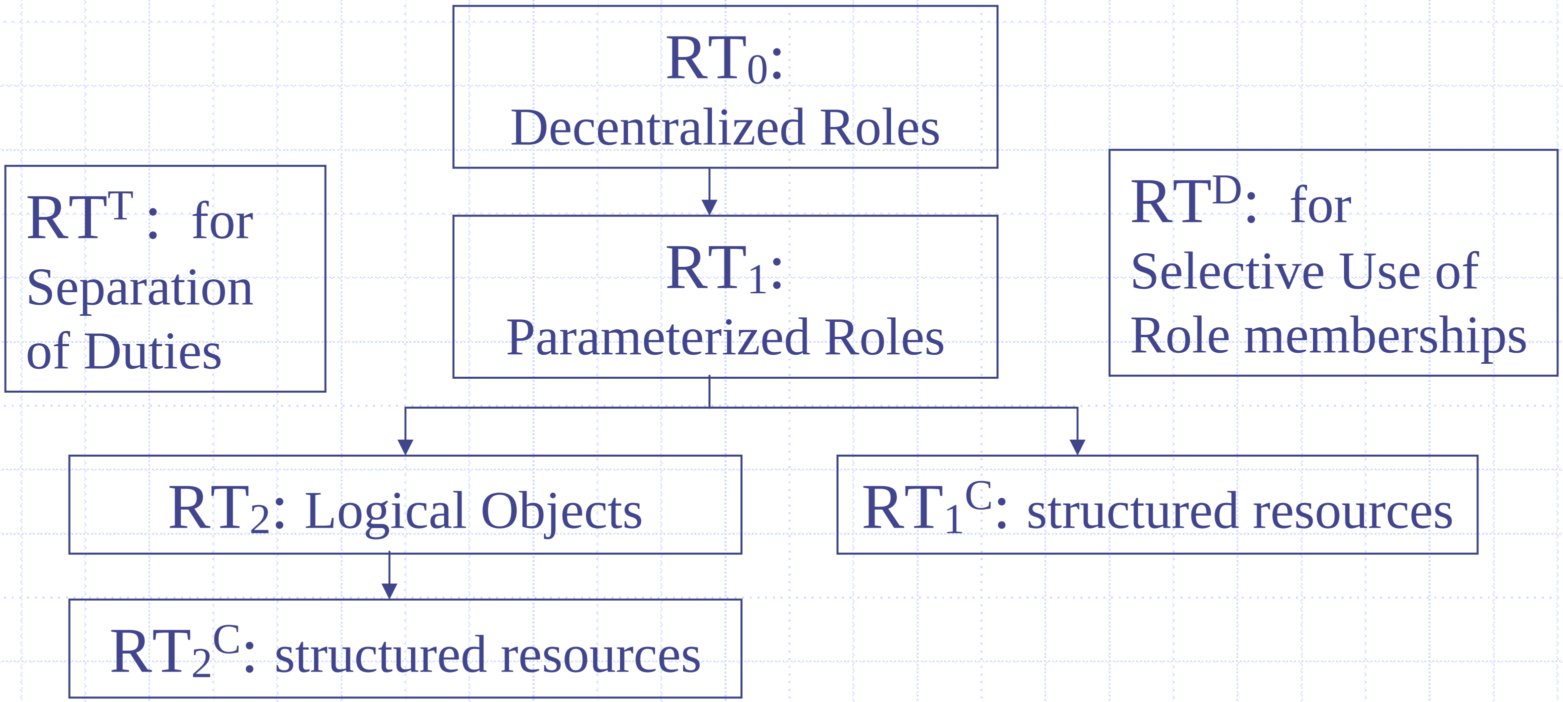
ABU



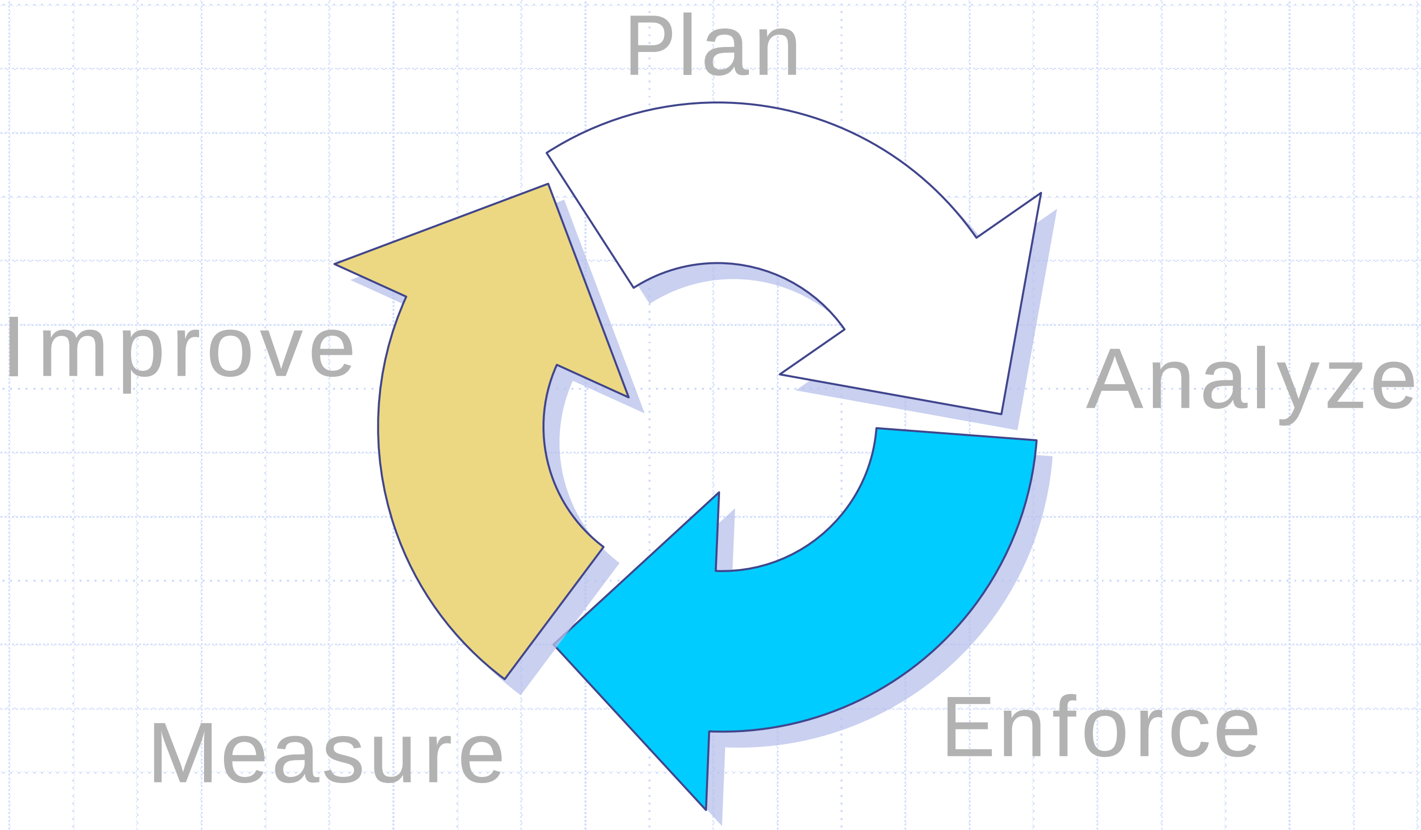
StateU

StateU is a university

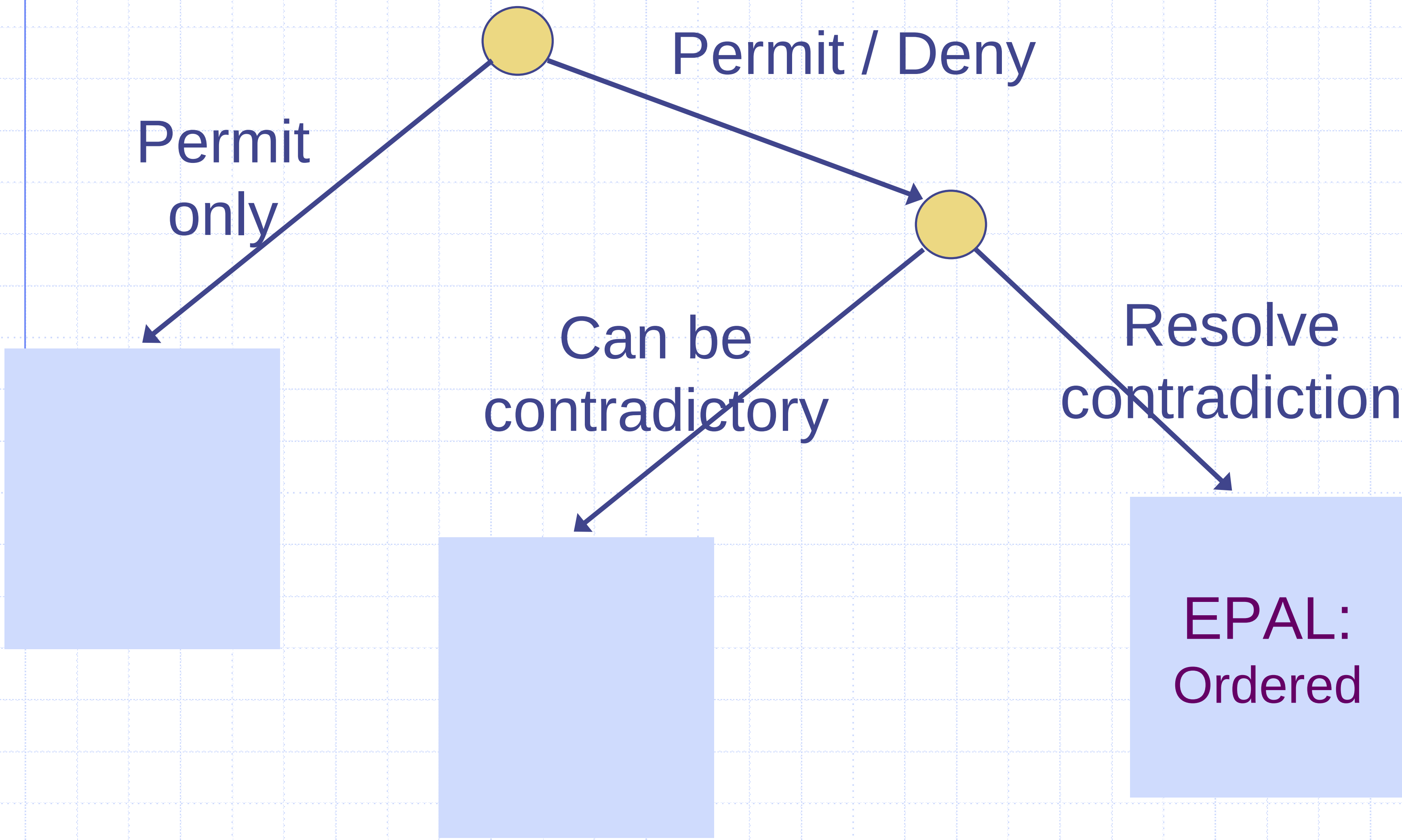
Role-based Trust-management (RT)



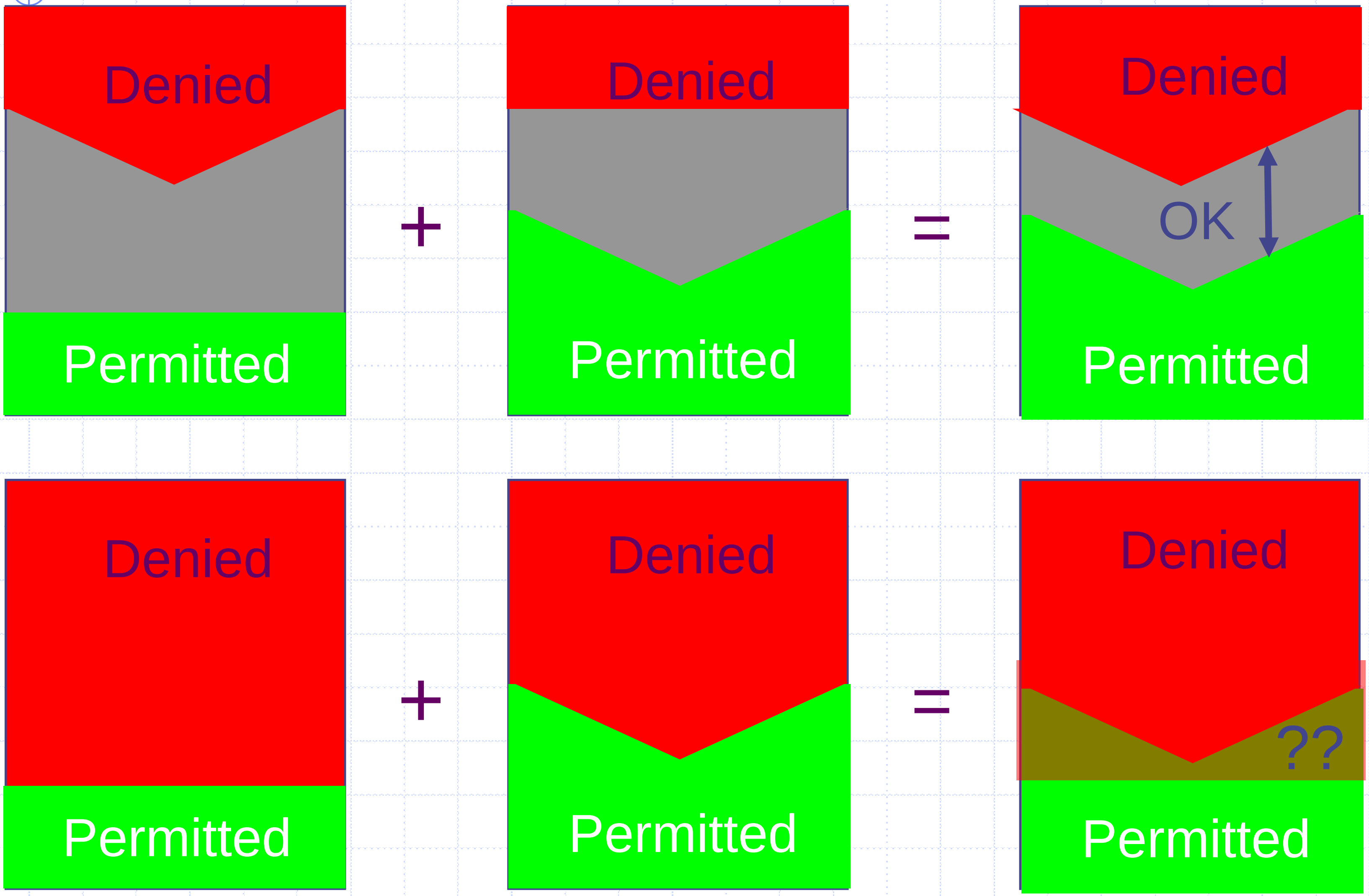
Policy Management Lifecycle



Policy language design space



Policy Combination



Contextual Integrity

- Framework for privacy:
  - Concept of contextual integrity
  - Formalization in Linear Temporal Logic
- Application to privacy laws:
  - HIPAA, GLBA, COPPA
- Related Work
  - RBAC, XACML, P3P, EPAL

Overview of Contextual Integrity

- Transfer of information between agents
  - "Alice give Bob information about Charlie"
- Categorization
  - Agents grouped into roles
  - Information categorized by types
- Basic policy statements
  - Manager may read employee's performance data
  - If m is a manager, e is an employee,
    d is performance data about e, and
    m is e's manager
    then m may read d

Formalization in Temporal Logic

- Syntax of logic

$$\varphi ::= \text{send}(p_1, p_2, m) \mid \text{contains}(m, q, t) \mid \text{inrole}(p, r) \mid \text{incontext}(p, c) \mid t \in t' \mid \varphi \wedge \varphi \mid \neg\varphi \mid \varphi \mathcal{U} \varphi \mid \varphi \mathcal{S} \varphi \mid \bigcirc \varphi \mid \exists x : \tau . \varphi$$

- Formula representing contextual norms

$$\sigma \models \Box \forall p_1, p_2, q : P. \forall m : M. \forall t : T. \text{incontext}(p_1, c) \wedge \text{send}(p_1, p_2, m) \wedge \text{contains}(m, q, t) \rightarrow \bigvee_{\varphi^+ \in \text{norms}^+(c)} \varphi^+ \wedge \bigwedge_{\varphi^- \in \text{norms}^-(c)} \varphi^-$$

where norms have specific forms

positive norm: $\text{inrole}(p_1, \hat{r}_1) \wedge \text{inrole}(p_2, \hat{r}_2) \wedge \text{inrole}(q, \hat{r}) \wedge (t \in \hat{t}) \wedge \theta \wedge \psi$

negative norm: $\text{inrole}(p_1, \hat{r}_1) \wedge \text{inrole}(p_2, \hat{r}_2) \wedge \text{inrole}(q, \hat{r}) \wedge (t \in \hat{t}) \wedge \theta \rightarrow \psi$

Policy Operations and Relations

- Standard automated LTL tools are applicable
  - Policy consistency: LTL satisfiability
  - Refinement: logical implication
  - Combination: conjunction and disjunction
  - Strong compliance: satisfiability
  - Weak compliance: computable efficiently using concepts from LTL runtime verification

Application: HIPAA

- Privacy Rule
  - Covered entities (e.g. hospitals) can give protected health information about patients to health care providers
    - Sender role: Covered entity
    - Recipient role: Health care provider
    - Subject role: Patient
    - Information type: Protected health information

$$\mathrm{inrole}(p_1, \textit{covered-entity}) \land \mathrm{inrole}(p_2, \textit{provider}) \land \mathrm{inrole}(q, \textit{patient}) \land (t \in \textit{phi})$$

Application: GLBA

- Privacy Rule
  - Financial institutions must notify consumers if they share their non-public personal information with non-affiliated companies, but the notification may occur either before or after the information sharing occurs.
    - Sender role: Financial institution
    - Recipient role: Non-affiliated company
    - Subject role: Consumer
    - Information type: Non-public personal information
    - Temporal condition: Notify data subject

$$\text{inrole}(p_1, \textit{institution}) \land \text{inrole}(p_2, \textit{non-affiliate}) \land \text{inrole}(q, \textit{consumer}) \land (t \in \textit{npi}) \rightarrow \Diamond \text{send}(p_1, q, \textit{privacy-notice}) \lor \diamondminus \text{send}(p_1, q, \textit{privacy-notice})$$

Comparison

- Role-based access control
  - No subject of data, attributes, temporal conditions
- XACML
  - Attributes handled incorrectly (inheritance)
  - Combination occurs functionally, not logically
- EPAL
  - Obligations treated as uninterpreted symbols
  - Can only enforce week compliance
- P3P
  - Contains only simple opt-in / opt-out conditions