More Access – Less Control
Access Control in the Web 2.0

Michael Hart, Rob Johnson, Amanda Stent
Stony Brook University

The New Social Context

- Social networks and content-based sites have come of age

- These sites are incredibly popular
  - MySpace one of most requested domains
  - 85% of college students use Facebook
  - YouTube serves more than 45 terabytes of video

Consequences

- Job loss
- Stalking and harassment
- Sexual predators
- Currently in the news: Stacy Snyder
  - Student denied degree on the eve of her graduation because of MySpace photo

"You have to be an idiot to put pictures out on the internet like that, and then think that nobody is looking at them...

We've turned away a lot of candidates based on some of the stuff we see there."

- Posted Anonymously

Current Access Control Models

- Most sites employ inflexible access control
  - Documents are either public or private
- Most successful: Friends model
  - Users befriend others using invitation system
- Advantages
  - Fits user expectations
  - Leverages pre-existing site features
- Disadvantages
  - "Friend" takes on many levels of intimacy
  - Trade off between popularity and privacy
- Friends-based access control is too coarse

Improving Access Control

- ## Users need:
  - Access control that mirrors their mental model
  - Usable policy authoring
  - Expressive policy language
- ## Constraints
  - Administrator-less environment
  - Dynamic content

Content-Based Access Control (CBAC)

- Access to an object is partially or entirely based on the content of the objects in the system
- Example policies

    - "Allow College Friends to see posts on Stony Brook"

    - "Allow Friends from Boston to see entries on Red Sox"

    - "Don't let my parents see pictures from parties"

CBAC Advantages

- Reduces user work
  - Don't have to specify access per document
  - Take advantage of pre-existing categorical information
- Small policies
  - Easy to understand
  - Easy to change
- Expressive
  - Able to capture many levels of granularity
- Intuitive
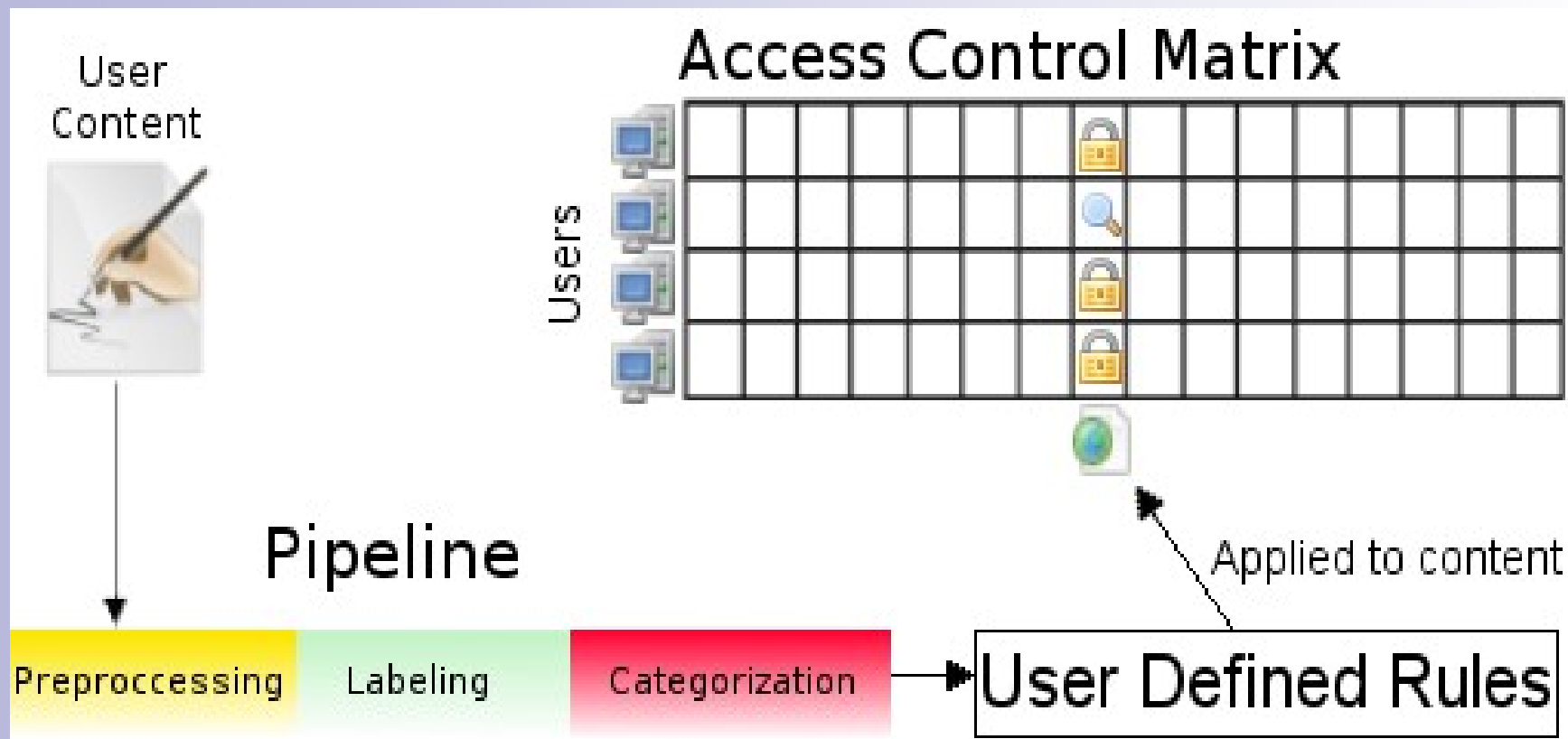 - Works on a domain of author's expertise

Is this feasible?

- Automatic policy application
  - Use pre-existing classification information (i.e. tags)
  - Wealth of lightweight techniques for classification
- Policy authoring
  - Brodie et. al demonstrated several interfaces for policy acquisition with favorable results
    - Natural language
    - Templates
    - Guides

Architecture

PLOG: **P**rivacy/**P**olicy-aware b**log**ging

- CBAC-enabled blogging
- Policies expressed in terms of tags and social groups
  - Template-based policy editor
- Tags automatically assigned to entries
  - Bayesian classifier in current version

CBAC applications

- We can implement system wide policies using the same CBAC principles
- Affinity-Based Access Control
- Need to Know-Access Control
- Inference Control
- Integrity Control

Affinity-Based Access Control

- Social networks facilitate social interaction
  - We would like to share our thoughts with like-minded people
- The problem is when these channels are used for ulterior motives
- Create a new CBAC system-wide policy
  - My posts on some topic T are visible to other users that have demonstrated a "sincere interest" in T
- The benefits are immediate:
  - Connects like-minded people
  - Prevents others from trawling these networks

Need to Know-Access Control

- May be desirable to restrict content to those mentioned directly or indirectly in entry
  - Many social networks contain membership information about users (i.e. clubs, teams)
- This would allow users to:
  - Automatically maintain separate groups
  - Requires minimal policy specification

Inference Control

- Stalkers analyze their victims' posts
- Some users are careful to omit identifying information
- Use natural language processing and text summarization to:
  - Identify personal/sensitive information
  - Warn user of disclosing personal information
  - Give options in order to protect information

Integrity Control

- Wikipedia is a popular Web 2.0 application
  - Takes advantage of a distributed expert knowledge base
  - Vandalized by malicious users
- Current solutions to vandalism negate egalitarian approach
- Ideally, grant write access only to edits that maintain integrity of article
- Solution: bring interdisciplinary techniques to bear on this problem
  - For example, ignore edits that are opinionated or framed in a subjective manner

Conclusion

- Current web access controls allow frequent privacy violations
- Users need automatic, intuitive access controls
- Content-Based Access Control is
  - Simple
  - Intuitive
  - Automatable