Speculative Authorizations

Student: Pranab Kini Supervisor: Konstantin Beznosov

Problem

Lack of mechanisms that can understand subject behaviour of accessing resources in distributed systems and eventually prefetch authorization responses for resources that would probably be requested in future

Requirements

- Model should not interfere with regular operations
- Accurately understand subject behaviour and obtain high hit rate
- Computation of policies expensive, thus unused responses should be minimal in cache
- Model should attain high sensitivity
- Area under ROC curve should be as high as possible
- Incorporate prediction for resources added at runtime
- Model should not generate infeasible requests

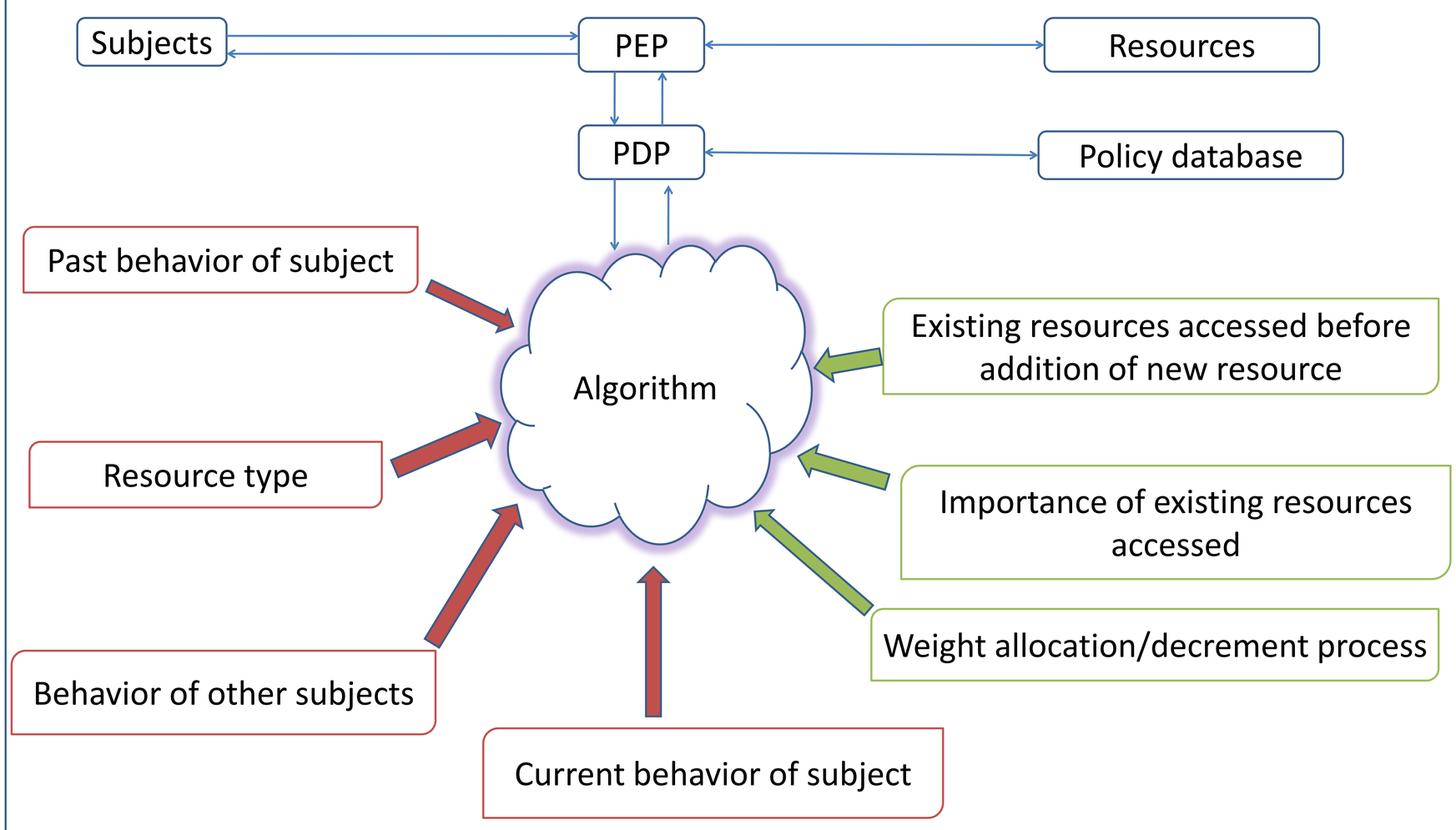
Comparison to Related Work

Resources in distributed system differ from web pages

- Not all resources can be accessed by every other subject
- Different subjects have different access level on different resources
- Range of resources to be considered is higher
- Storage size of access responses very small
- Dynamic changes in system need to be considered, e.g. new resources being added
- Optimum feature selection required to find tradeoff between complexity and sensitivity

Approach

- **Existing resources**: Check for relationship between resources and associated permissions using mixture of first order Markov Model
- **New resources**: Allocate weight to resources added at runtime based on position where they get added



Model Design

Design

- **Existing resources**: When subject requests for permission on any existing resource, check for
  - Past behavior of subject after this request
  - Behavior of other subjects (same group/role) after this request
  - Overall current behavior of subject
  - Resource type (Public/Private)
- **New resources**: When subject adds new resources at runtime
  - Position indicates weight of resource
  - Decrement weight as time progresses
  - Further prediction would rely on ‘existing resources’ mechanism

Experiments, Ongoing Work and Initial Results

- We obtained log traces from online distance education course having 12 instructors, 3 teaching assistants and 80 students
- Instructors and teaching assistants have accesses to more resources than students with greater set of permissions on all resources
- Trace contains 200,000 requests made during entire duration of course
- Instructors and teaching assistants can add course material, discussion topics and students can post replies to these topics
- Overall, the trace is a representation of enterprise system where policy enforcement is crucial
- Initial results for existing resources suggest hit rate of 47% as compared to 38% using regular first order Markov Model
- The decrement of weight for new resources added at runtime follows Poisson distribution

Laboratory for Education and Research in Secure Systems Engineering, University of British Columbia
Contact: Pranab Kini <pranabk@ece.ubc.ca>