University of British Columbia

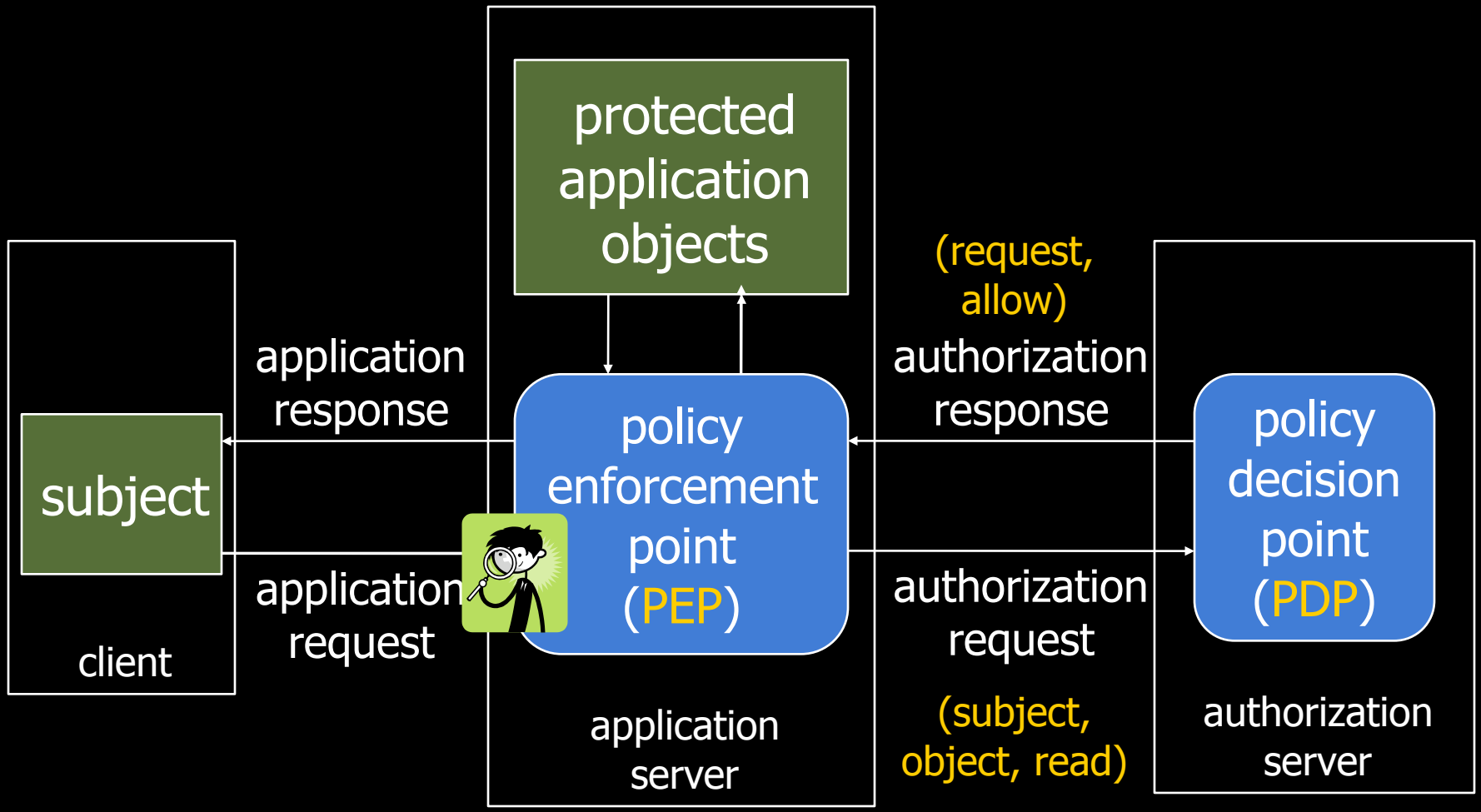
founded in 1908
ranked among the world top
- 35 institutes, by the *Shanghai Jiao Tong University (China)* in *2008*
- 34 universities, by the *Times Higher Education (UK)* in 2008

Toward Improving Availability and Performance of Enterprise Authorization Services

Konstantin (Kosta) Beznosov

Laboratory for Education and Research in Secure Systems Engineering
Department of Electrical and Computer Engineering
University of British Columbia, Canada

typical authorization architecture



IBM Access Manager, Entrust GetAccess, CA SiteMinder, etc.

request-response model

request-response model

+ re-use of authorization logic
+ consistent policy enforcement
+ lower admin overhead

- reduced availability
- increased latency
- reduced scalability

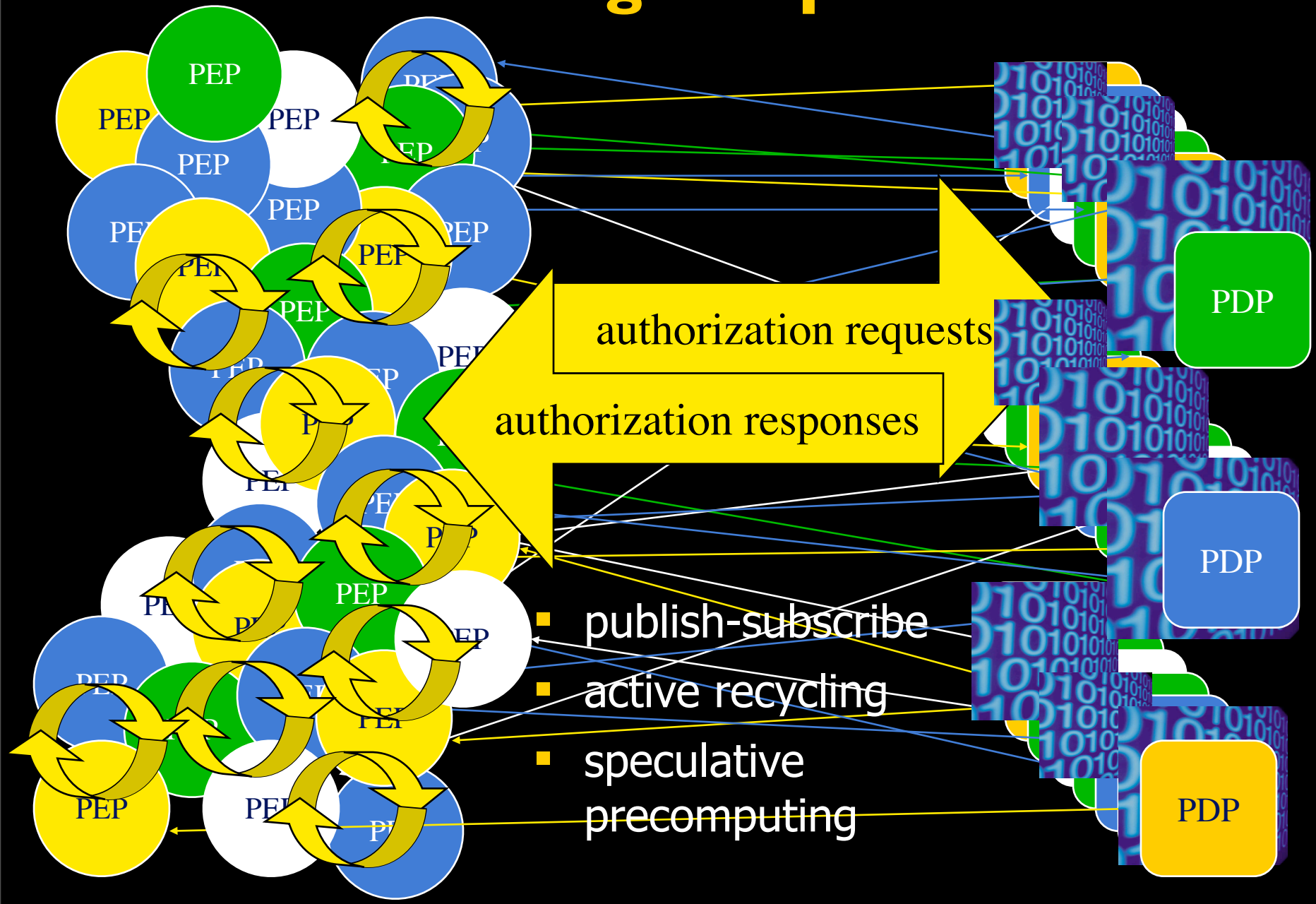
departing assumptions

1. processor resources virtually free
2. commodity computing most cost-effective
3. network bandwidth virtually unlimited
4. human time/attention expensive

existing approaches

- caching previous authorizations
  - + simple, inexpensive
  - + improves performance & availability
  - - serves only returning requests (precise recycling)
- generic fault-tolerance through replication/redundancy
  - + improve availability
  - - latency remains unchanged
  - - require specialized OS/middleware
  - - poorly scale on large populations

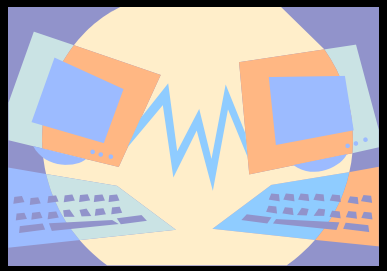
addressing the problem



K. Beznosov, "Flooding and Recycling Authorizations" in Proceedings of New Security Paradigms Workshop (NSPW), 2005, Lake Arrowhead, CA, USA, 20-23 September 2005, pp. 67-72.

outline

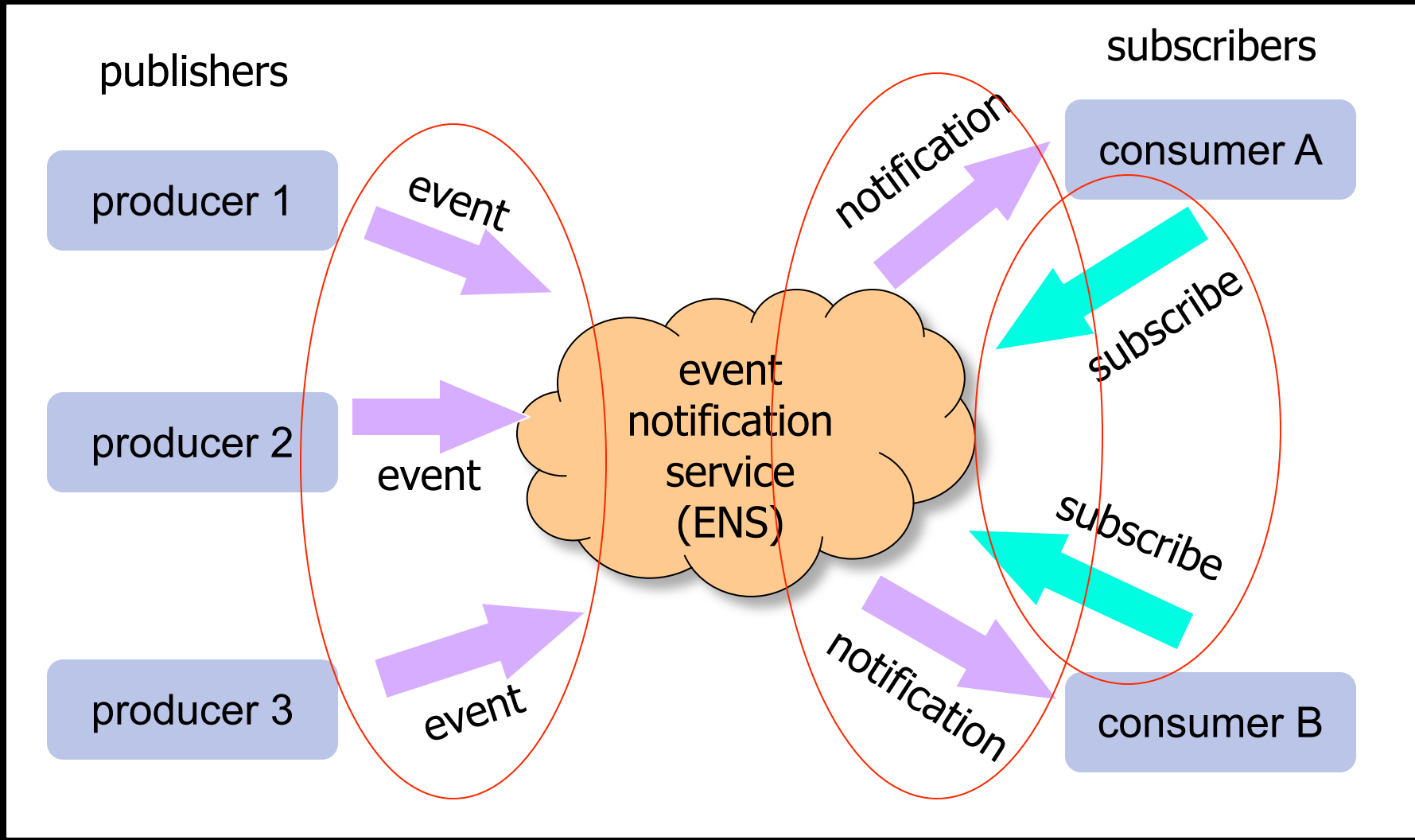
- authorization architecture based on pub-sub
- concept and model for inferring new authorizations from previous responses: secondary and approximate authorization model (SAAM)
- SAAM algorithms for BLP and RBAC
- distributed and cooperative SAAM



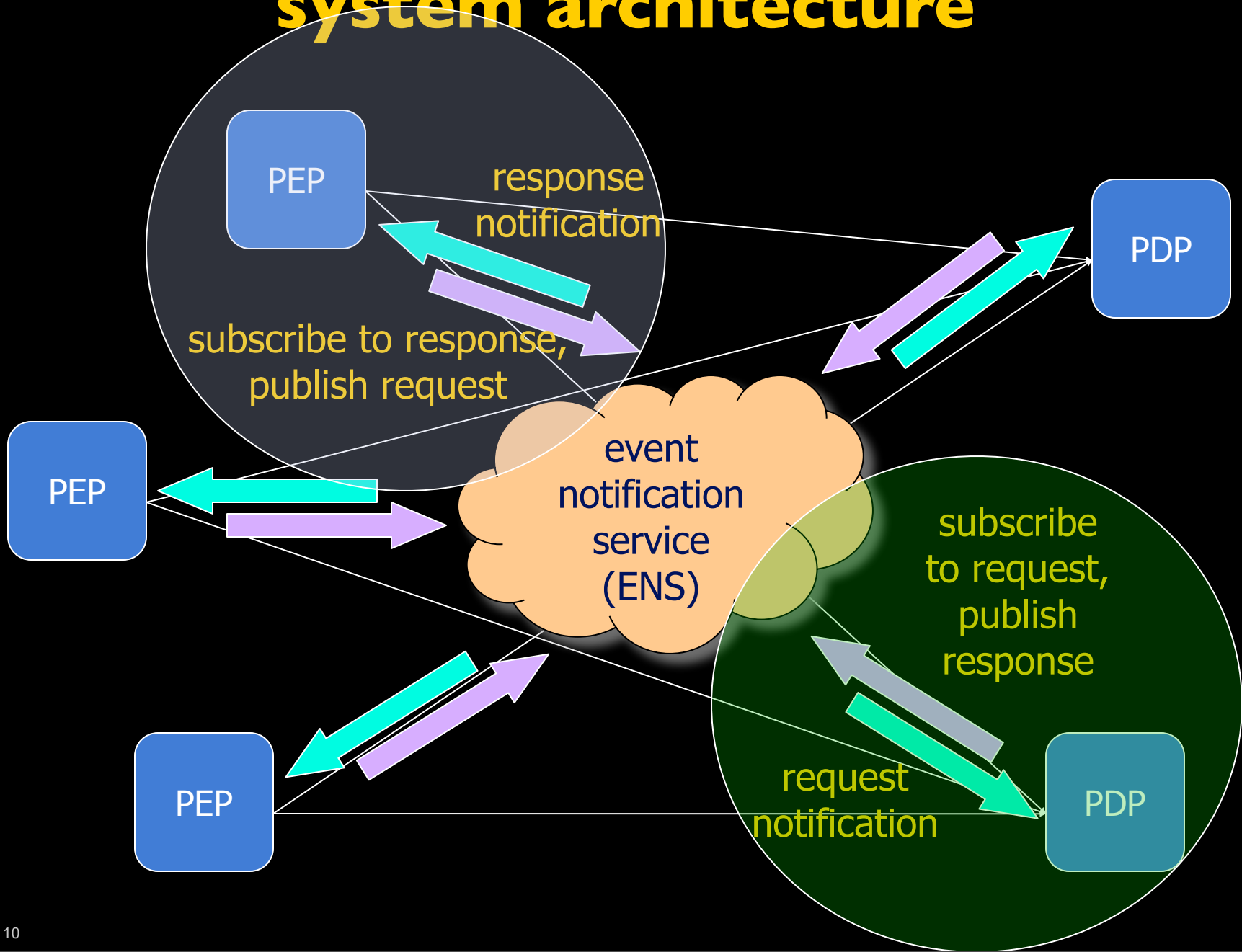
authorization architecture based on publish-subscribe model

Q. Wei, M. Ripeanu, K. Beznosov "Authorization using Publish-Subscribe Model," in *Proceedings of the IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA'08)*, December 10-12, 2008, Sydney, Australia, pp. 53-62

basic components in a publish/subscribe system

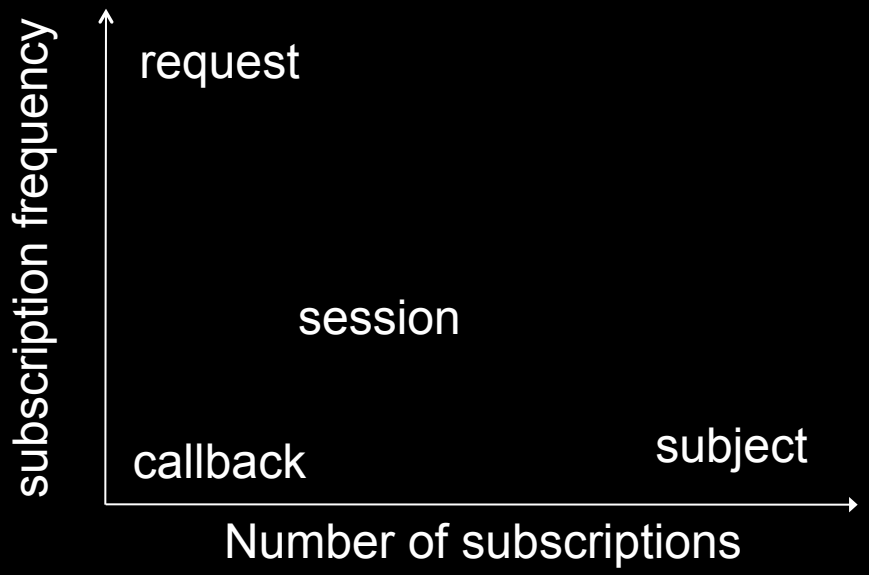


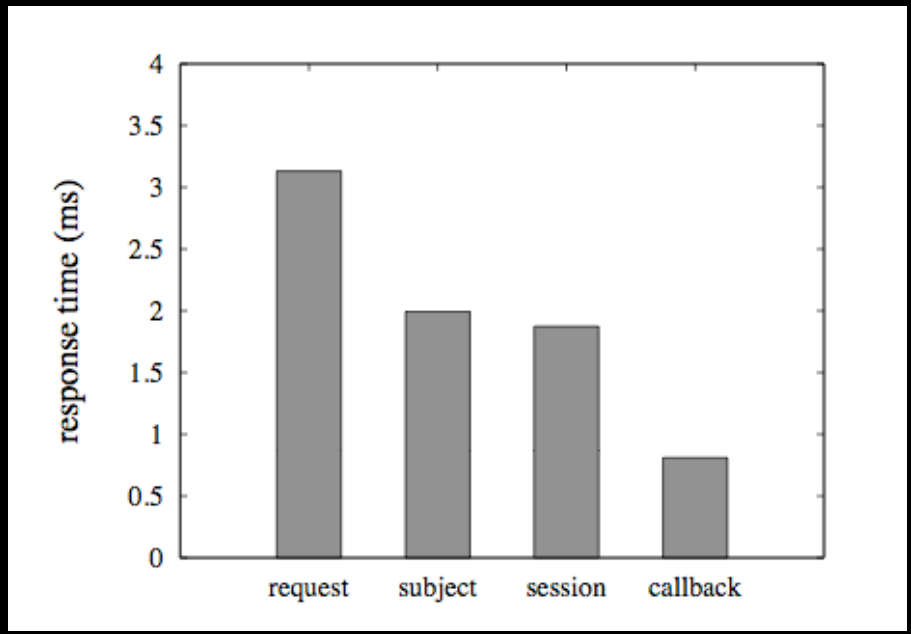
system architecture



PEP subscription schemes

- per request
- per subject
- per user session
- decisions delivered via callback, instead of pub-sub





PDP subscription schemes

- makes all the subscriptions at start-up
  - subscription frequency is zero
- can subscribe to
  - all requests
  - all resources
  - resource groups
  - application groups

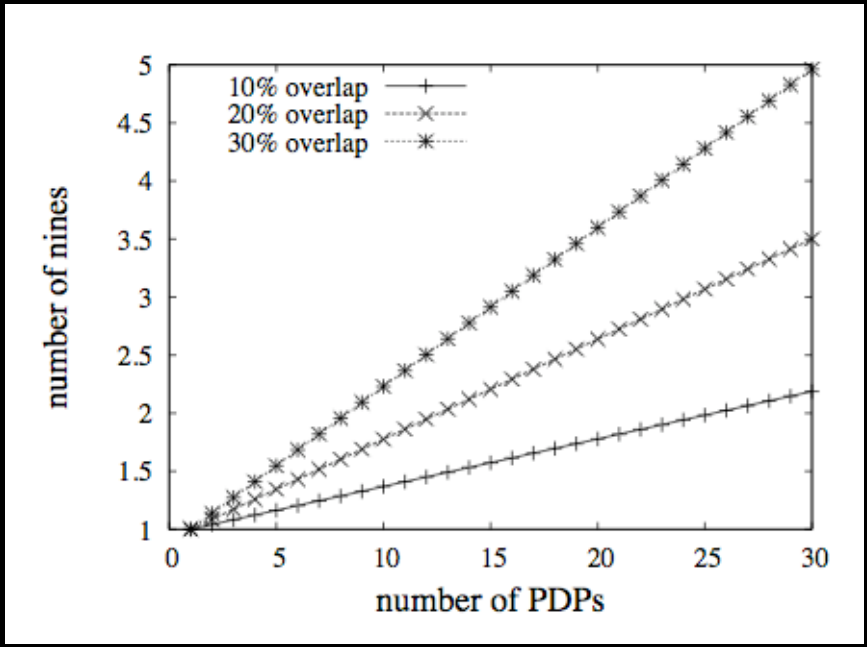
- other options
  - subject groups

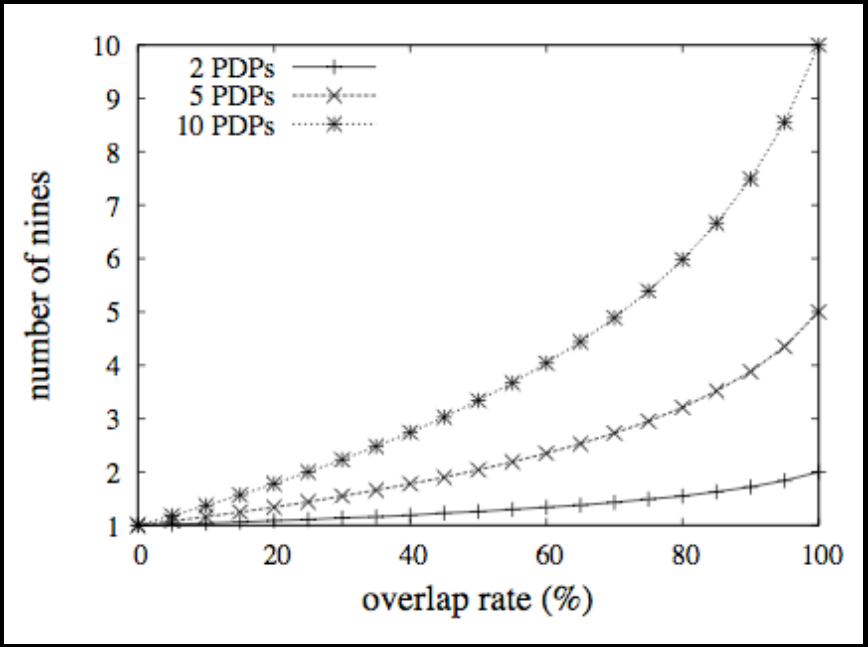
evaluation

availability analysis

$$p_t = 1 - (1 - p)\,(1 - p \cdot o)^{m-1}$$

- p - availability of each PDP
- m - number of PDPs
- o - overlap of served request spaces

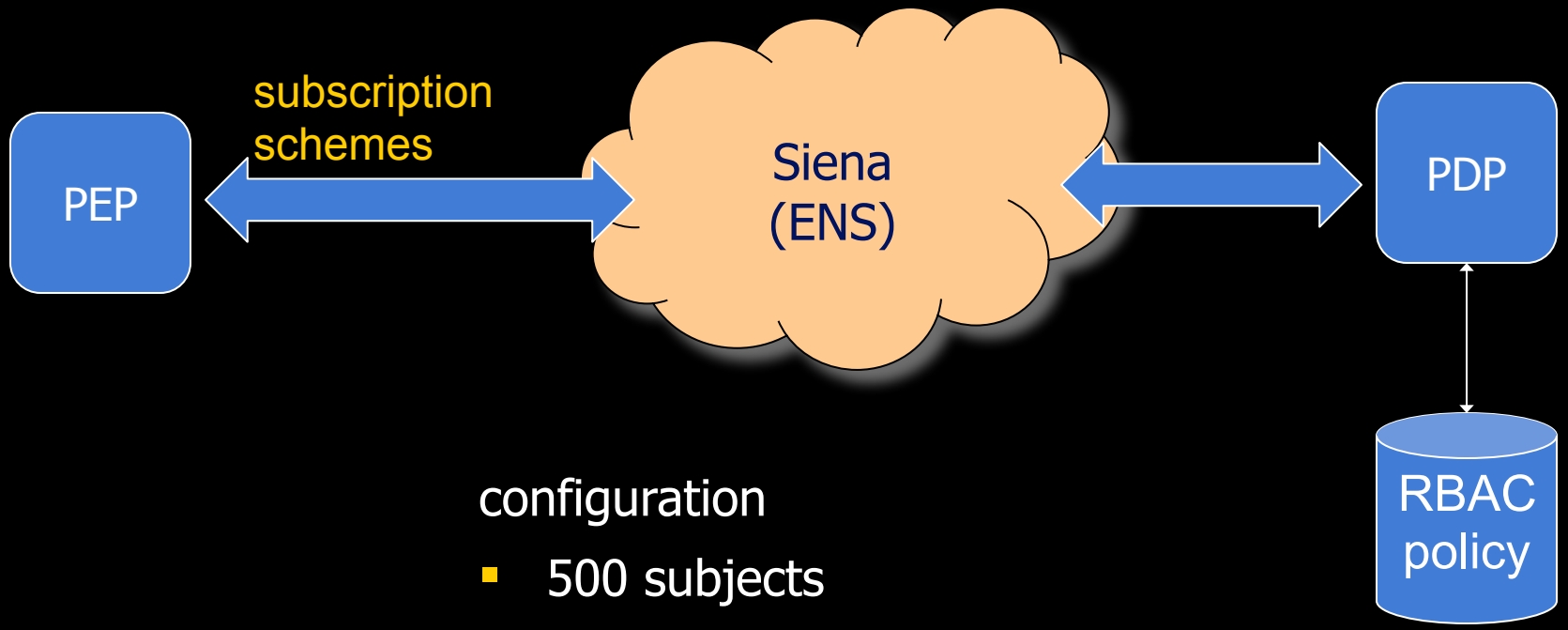




performance evaluation

- metrics
  - response time
  - maximum throughput
- influencing factors
  - number of subscriptions
  - subscription frequency

prototype

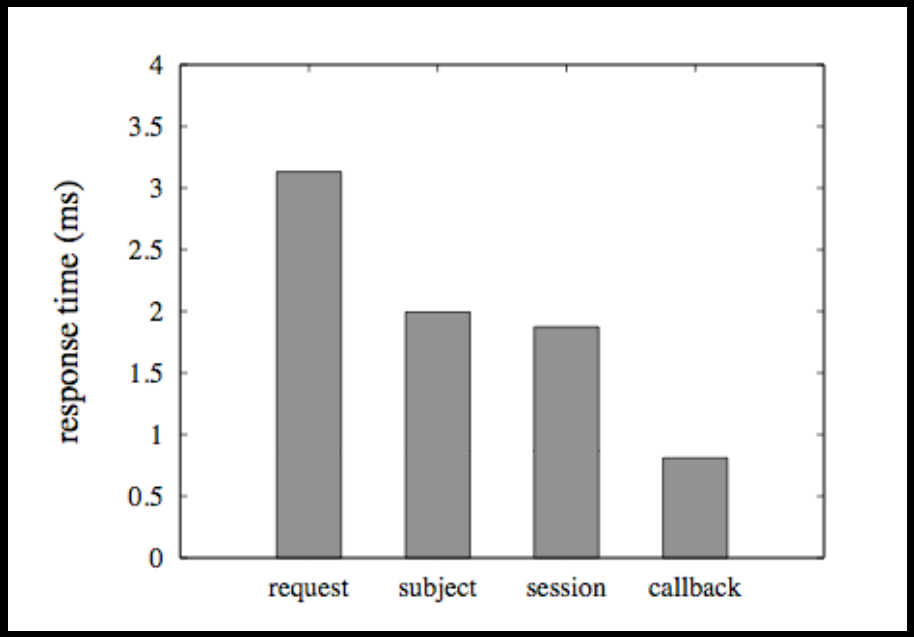


configuration

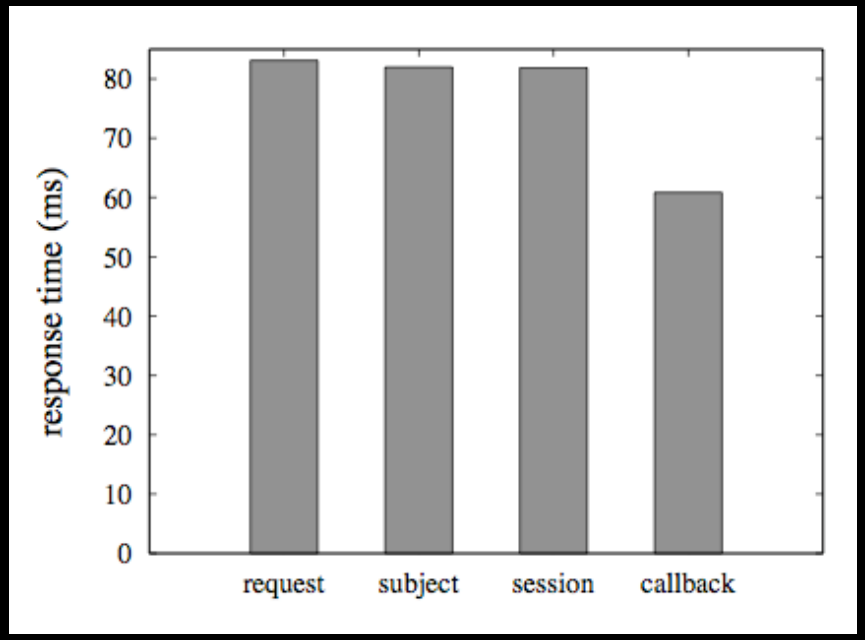
- 500 subjects
- 500 objects
- 3 access rights
- 100 requests/second
- 20 new subjects/second
- 100 active subjects (or sessions)

response time comparison

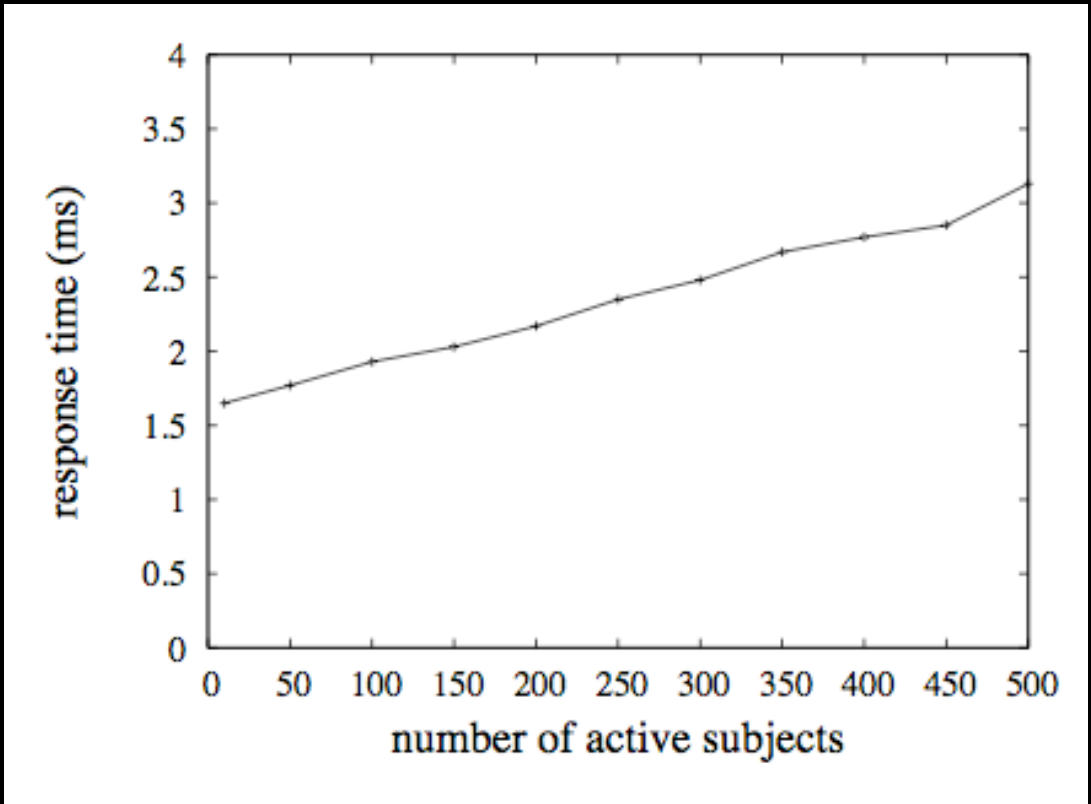
LAN (RTT < 0.1ms)



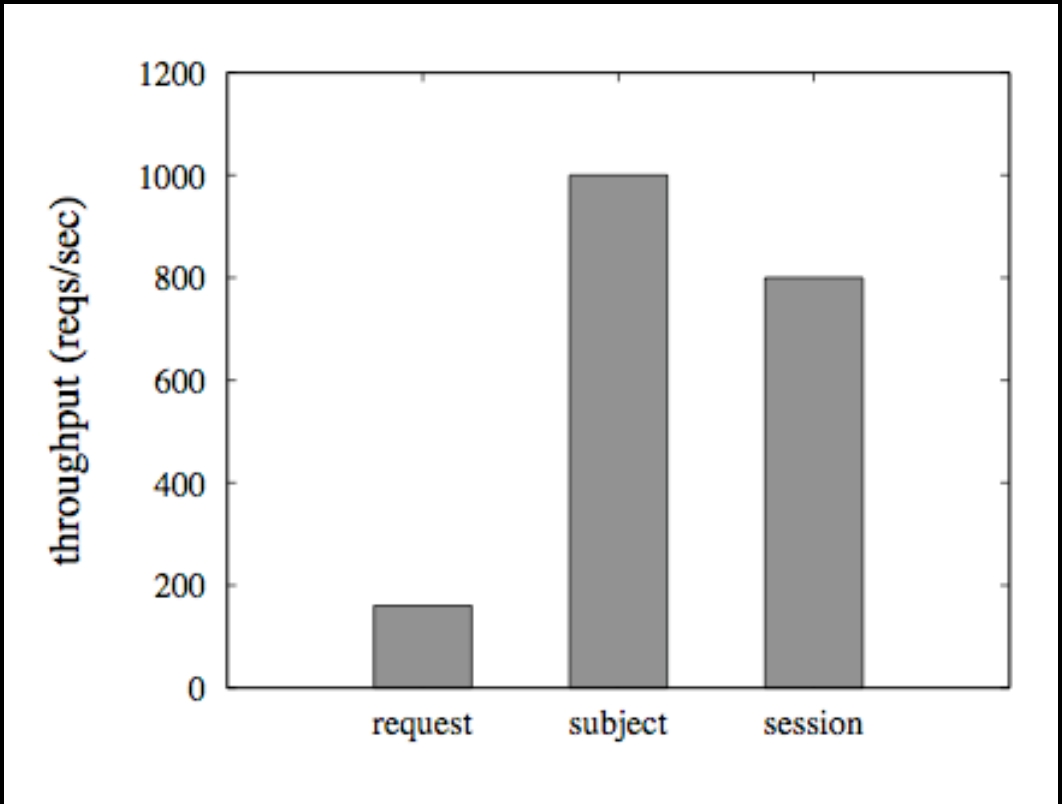
WAN (RTT 40ms)



outstanding subscriptions and latency



subscription frequency and throughput

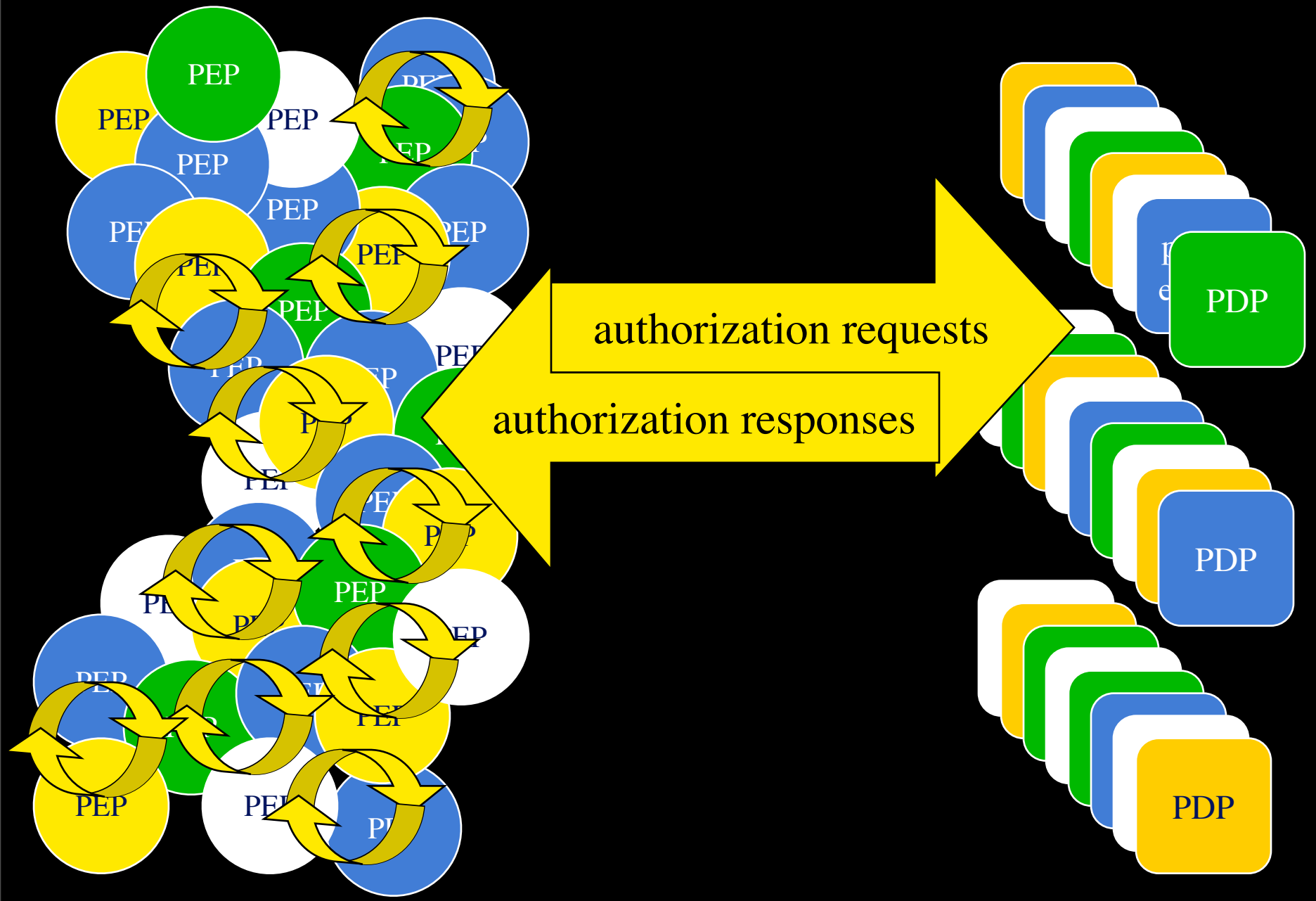


subscription additions/deletions result in ENS matching table updates

conclusions & work in progress

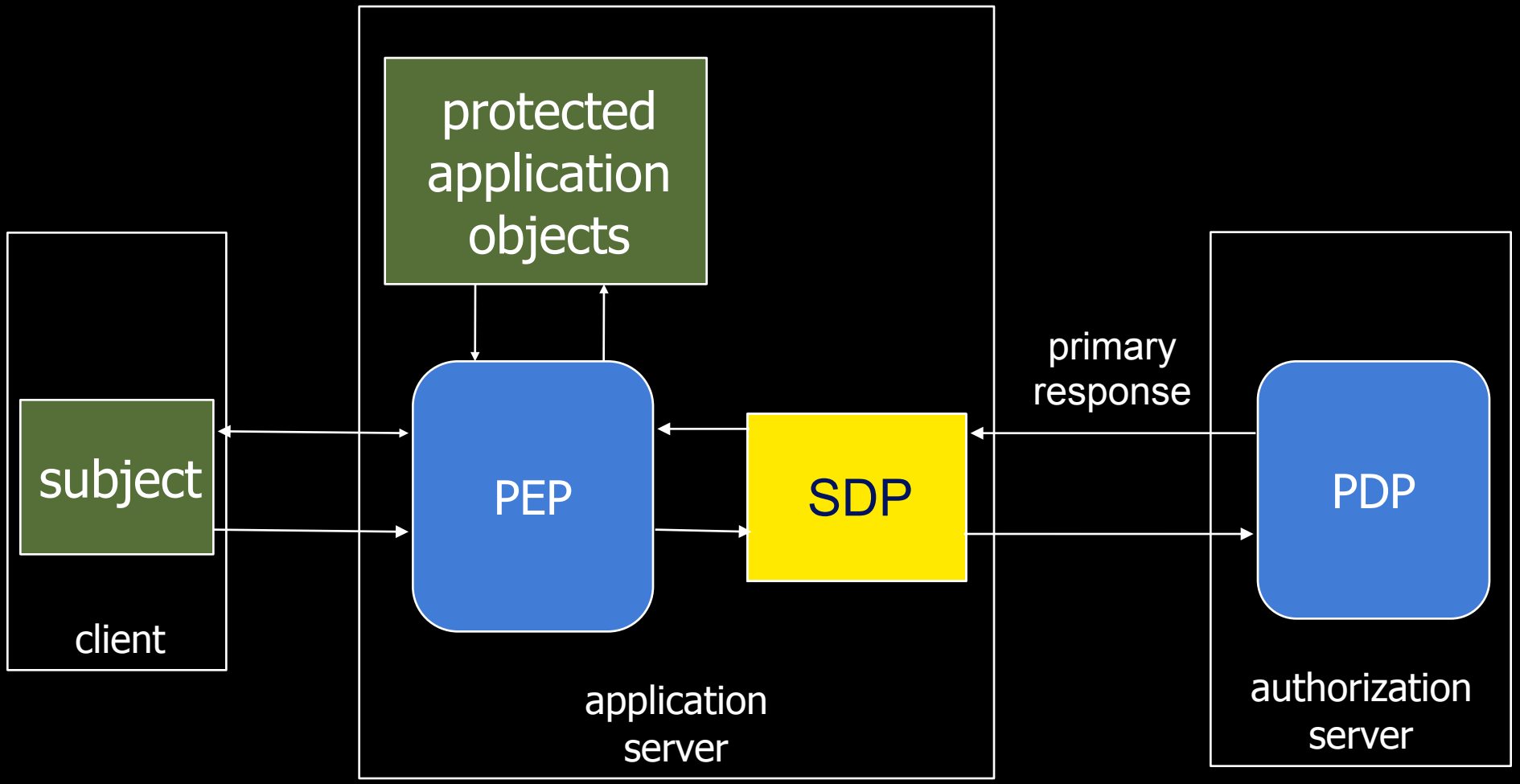
- pub-sub helps to improve system availability
- while employing pub-sub system, aim at
  - low subscription frequency
  - few outstanding subscriptions
- work in progress
  - security of the authorization infrastructure

recycling authorizations

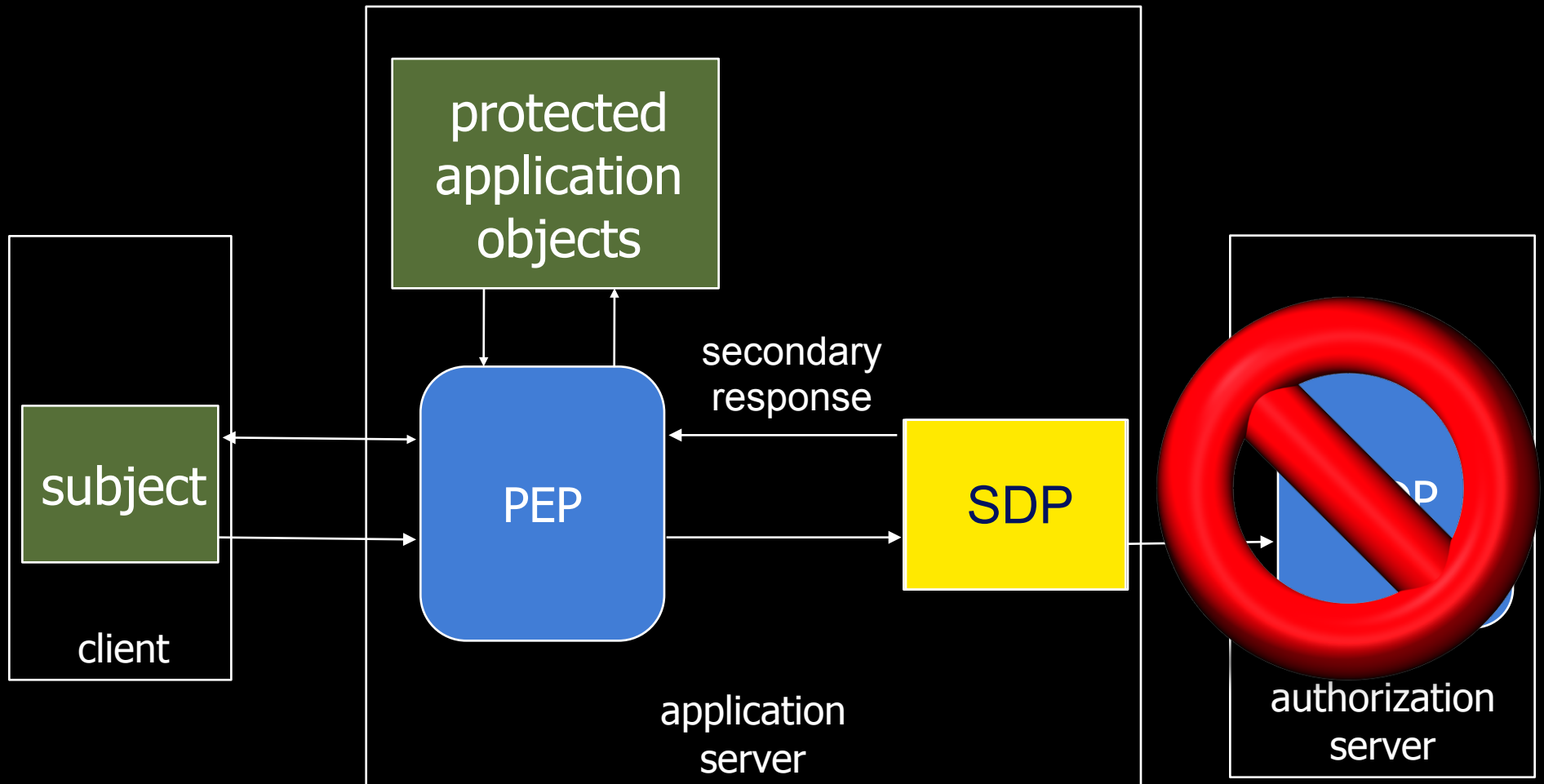


Secondary and Approximate Authorization Model (SAAM)

what SDP does



what SDP does



SAAM basic elements

- request
  <subject, object, access right, context, request id>

  < s , o , a , c , i >
  <{id="Bob", role="customer"}, {id="eB-23"}, view, {date="05-08-15"}, 10 >

- response
  <response id, request id, evidence, decision>

  < r, i, E , d >
  < 1, 10, [ ], allow >

authorization response types

<{id="Bob", role="customer"}, {id="eB-23"}, view, {date="05.06.08"}, 10>

< 1, 10, [ ], allow > -- primary (from PDP) response

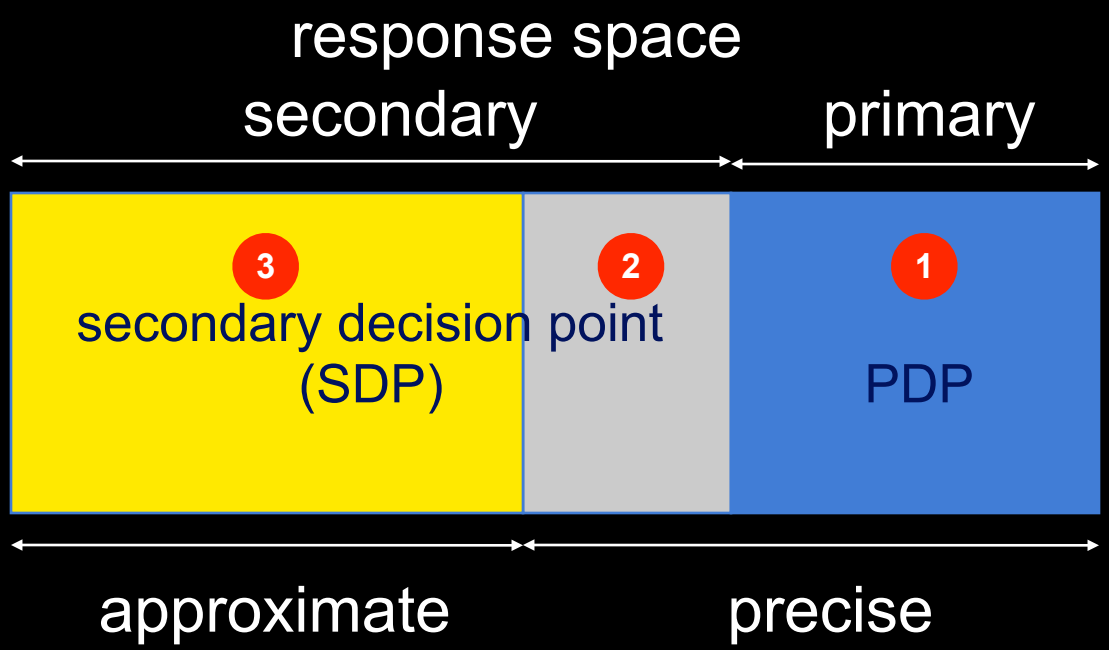
<{id="Bob", role="customer"}, {id="eB-23"}, view, {date="05.06.08"}, 11>

< 2, 11, [1], allow > -- secondary and precise response

<{id="Alice", role="customer"}, {id="eB-23"}, view, {date="05.06.08"}, 12>

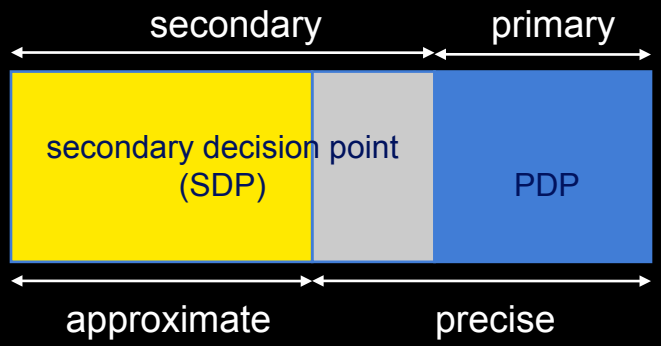
< 3, 12, [1], allow > -- secondary and approximate response

equivalent

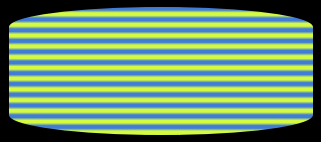


SAAM summary

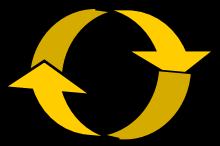
- basic elements
  - authorization requests <s, o, a, c, i>
  - authorization responses <r, i, E, d>
- responses can be
  - primary or secondary
  - precise or approximate
- secondary decision point
  - implemented at PEP
  - uses primary to compute secondary



recycling algorithms

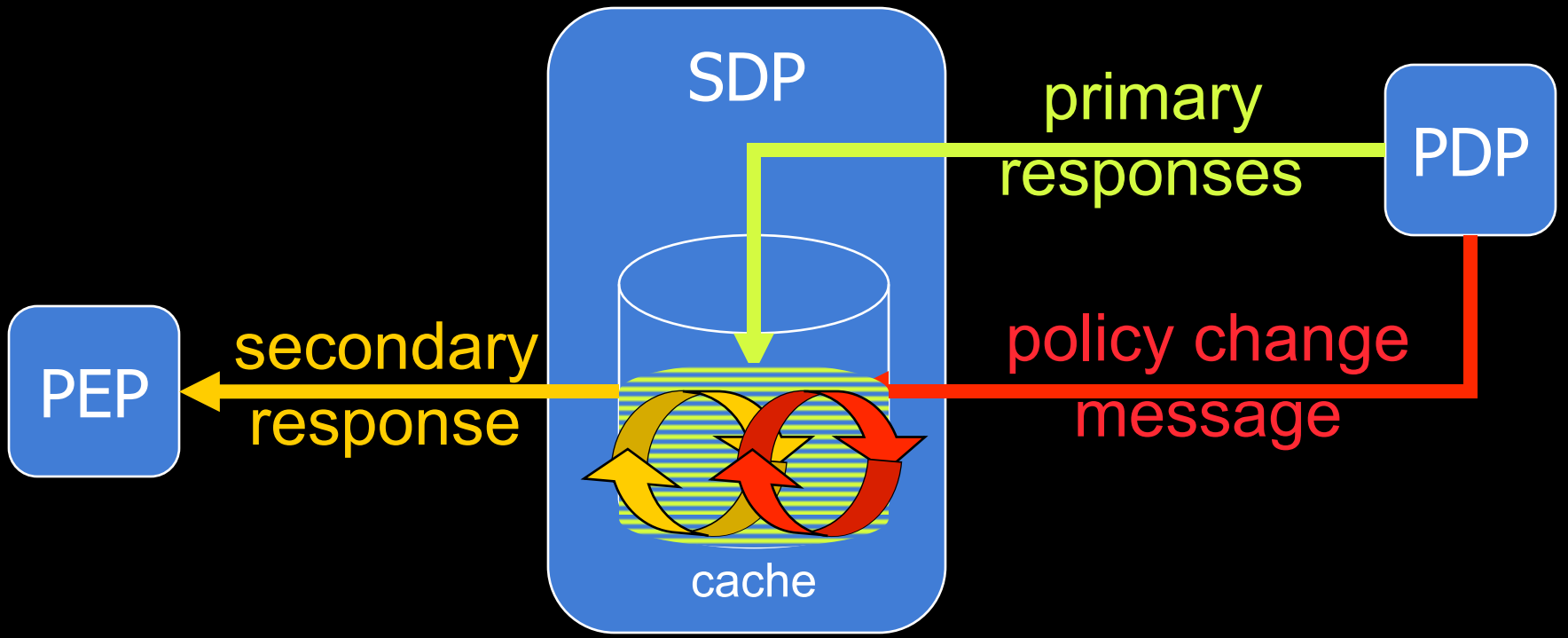


cache construction



decision

cache update



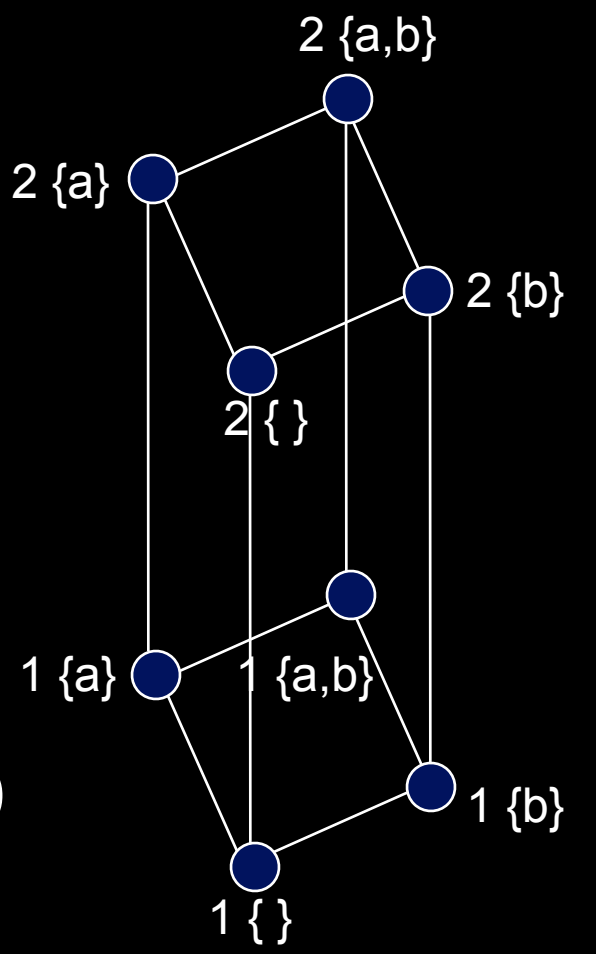
Application of SAAM to Bell LaPadula Policies

J. Crampton, W. Leung, K. Beznosov, "The Secondary and Approximate Authorization Model and its Application to Bell-LaPadula Policies," in *Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT)*, Lake Tahoe, California, USA, 7-9 June, 2006, pp. 111-120.

BLP refresher

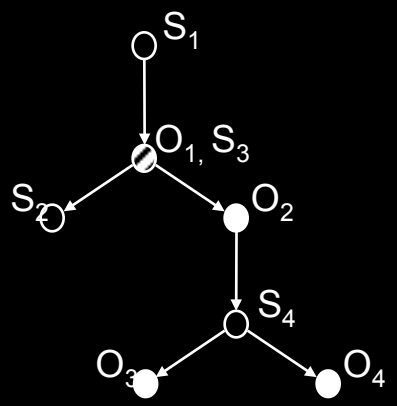
- S : subjects, O : objects
- DAC
- L: lattice of security labels
- λ: $S \cup O \rightarrow L$

- ss-property, $*$-property:
  - (s, o, read) is allowed $\Rightarrow \lambda(o) \leq \lambda(s)$
  - (s, o, append) is allowed $\Rightarrow \lambda(o) \geq \lambda(s)$
  - (s, o, write) is allowed $\Rightarrow \lambda(o) = \lambda(s)$



What's $SAAM_{BLP}$?

1. dominance graph (DG)

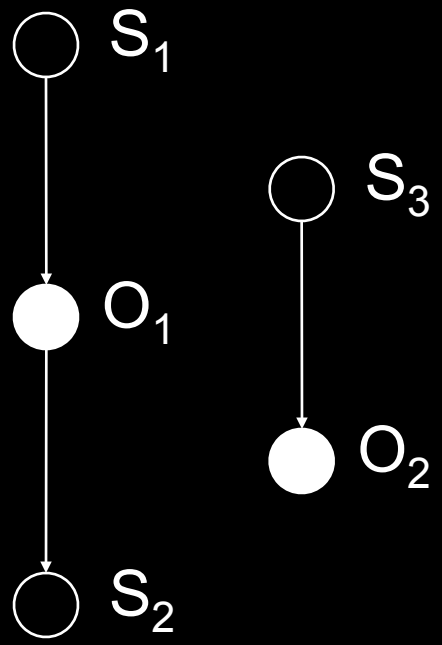


2. algorithms for SDP to
   - build DG from primary responses
   - compute secondary responses using DG

dominance graph

allow

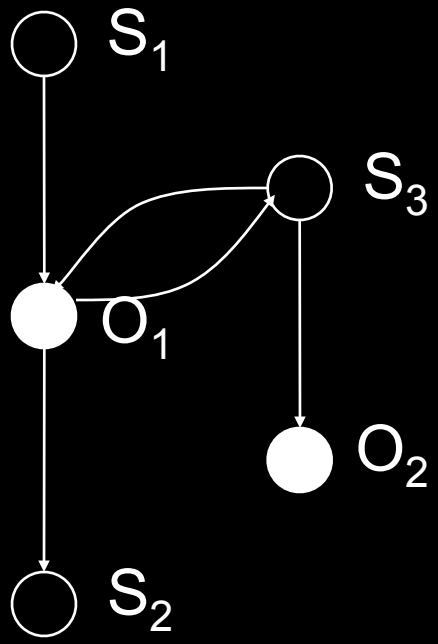
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)



dominance graph

allow

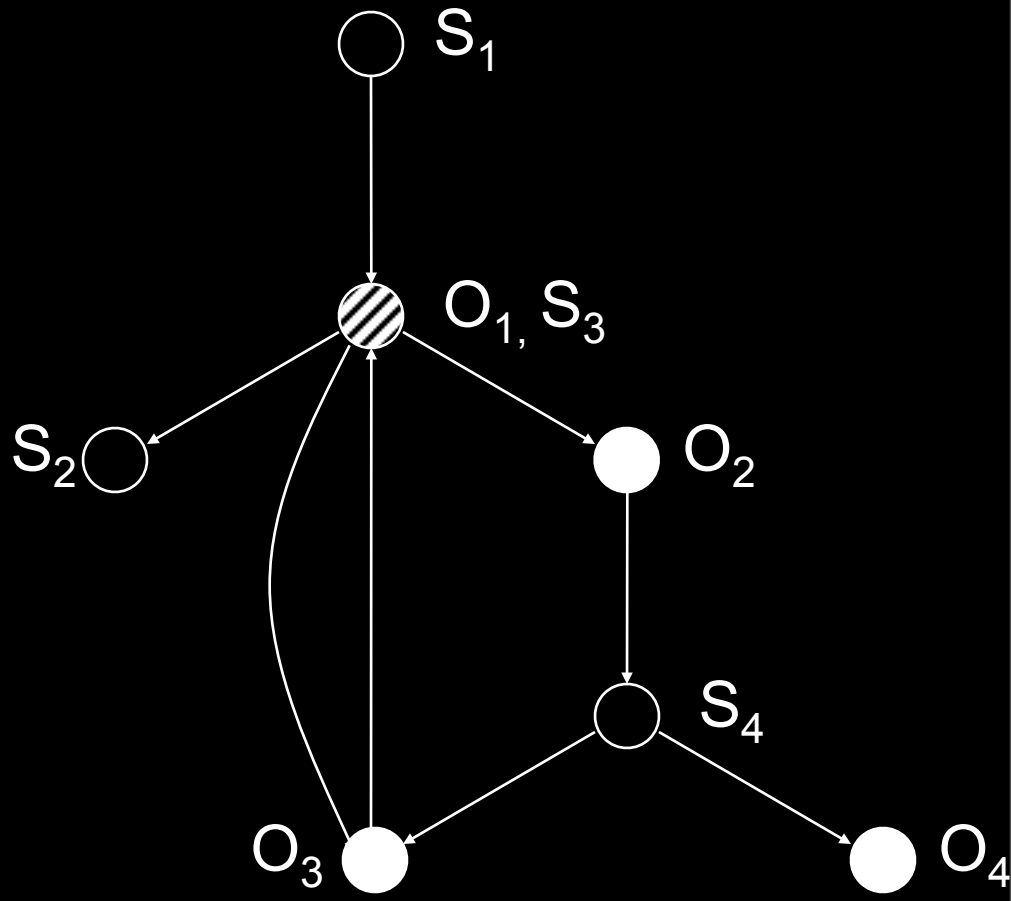
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)



dominance graph

allow

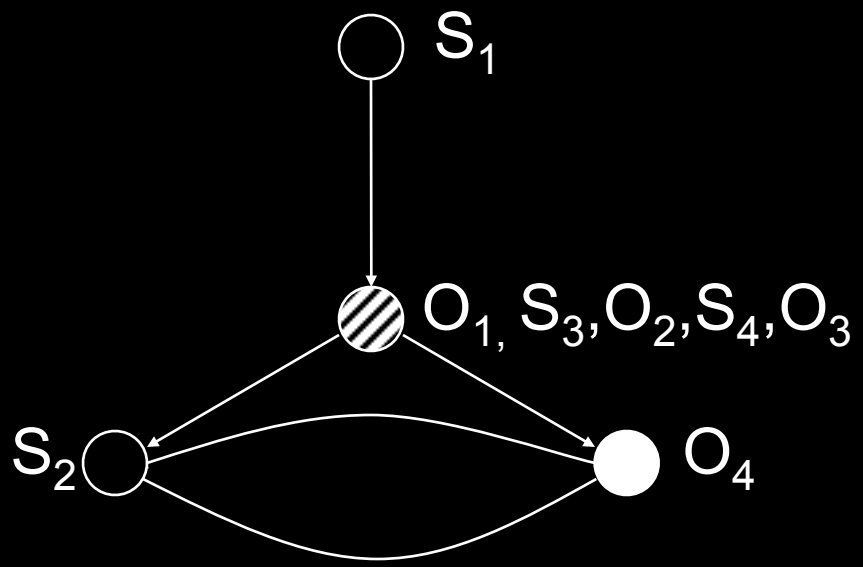
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)



dominance graph

allow

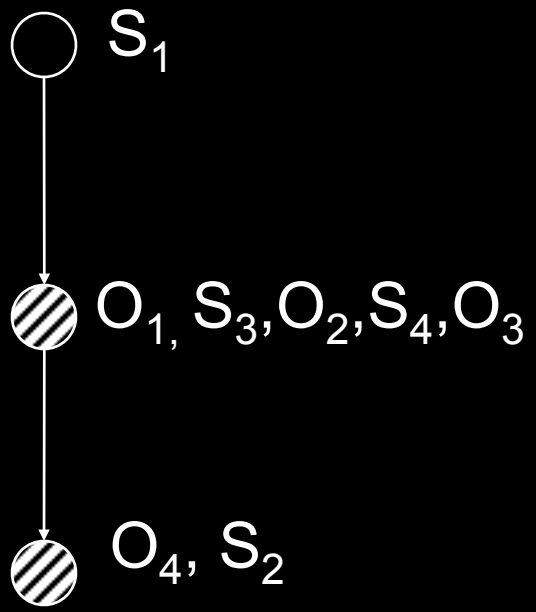
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)
10. (s_2, o_4, write)



dominance graph

allow

1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)
10. (s_2, o_4, write)



SDP may allow:

- (S_1, O_4, read)
- (S_4, O_1, write)
- (S_2, O_3, append)

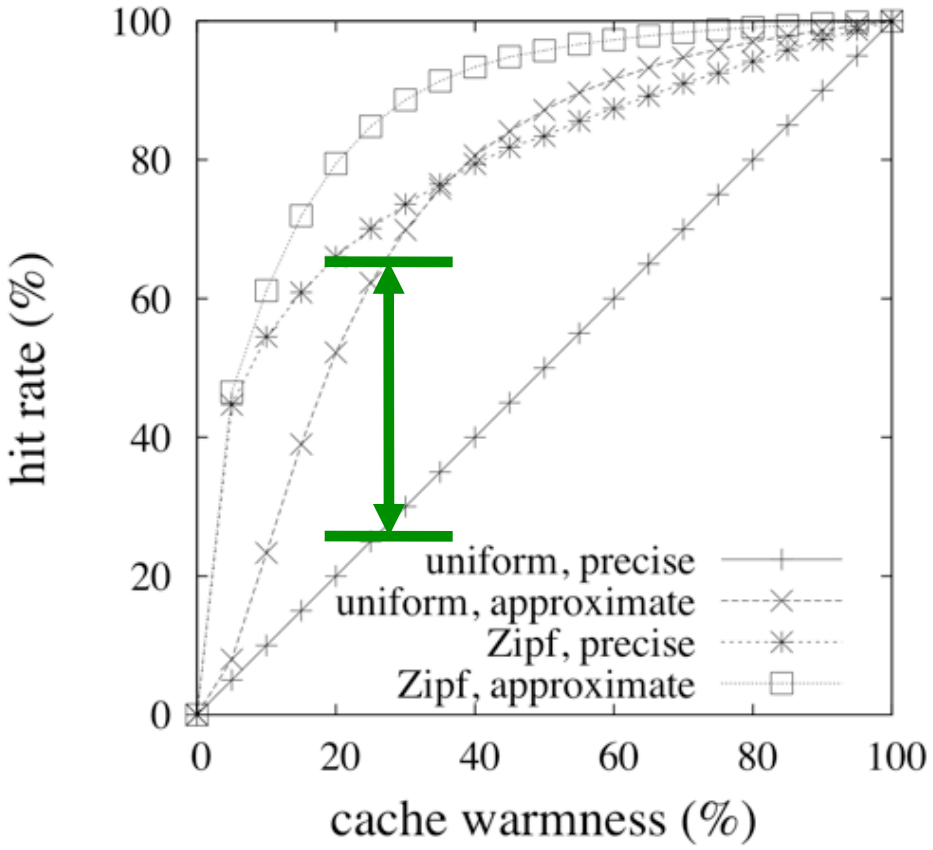
SDP cannot decide:

- (S_2, O_3, read)
- (S_1, O_4, write)
- (S_1, O_4, append)

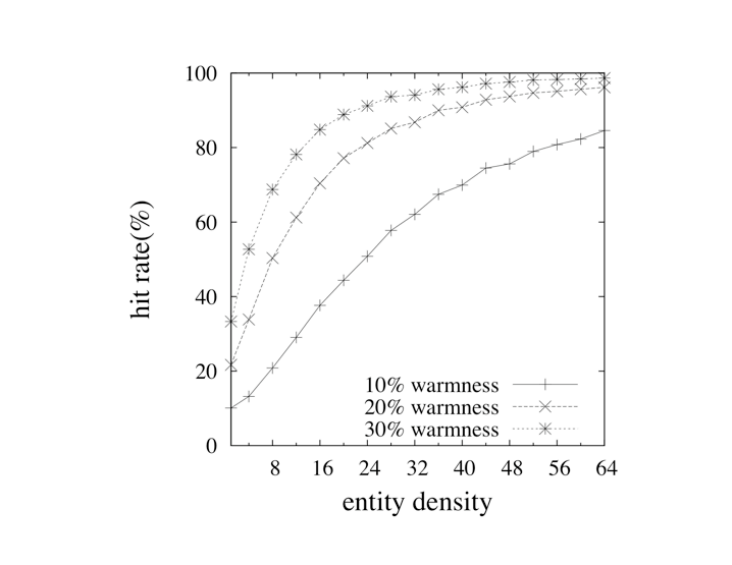
$SAAM_{BLP}$ evaluation

hit rate

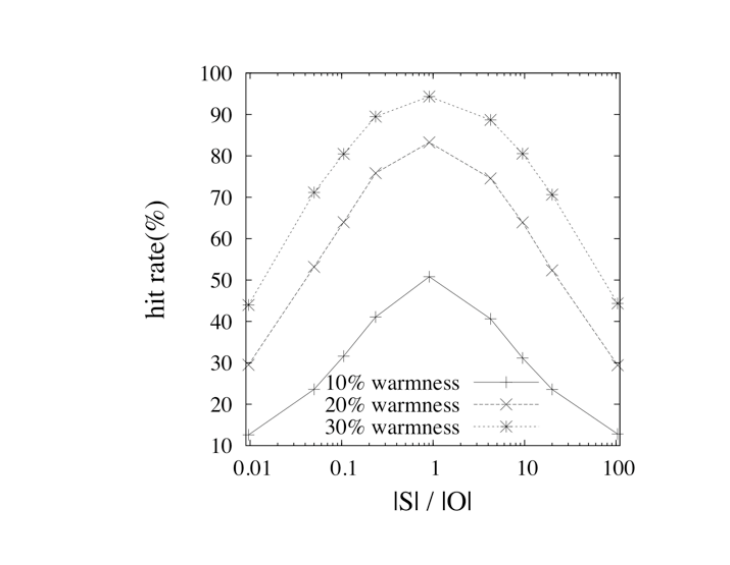
BLP policy: 5 levels, 5 categories, 50 subjects, 1,000 objects, 2 rights



impact of various system parameters



density of subjects and objects in the lattice



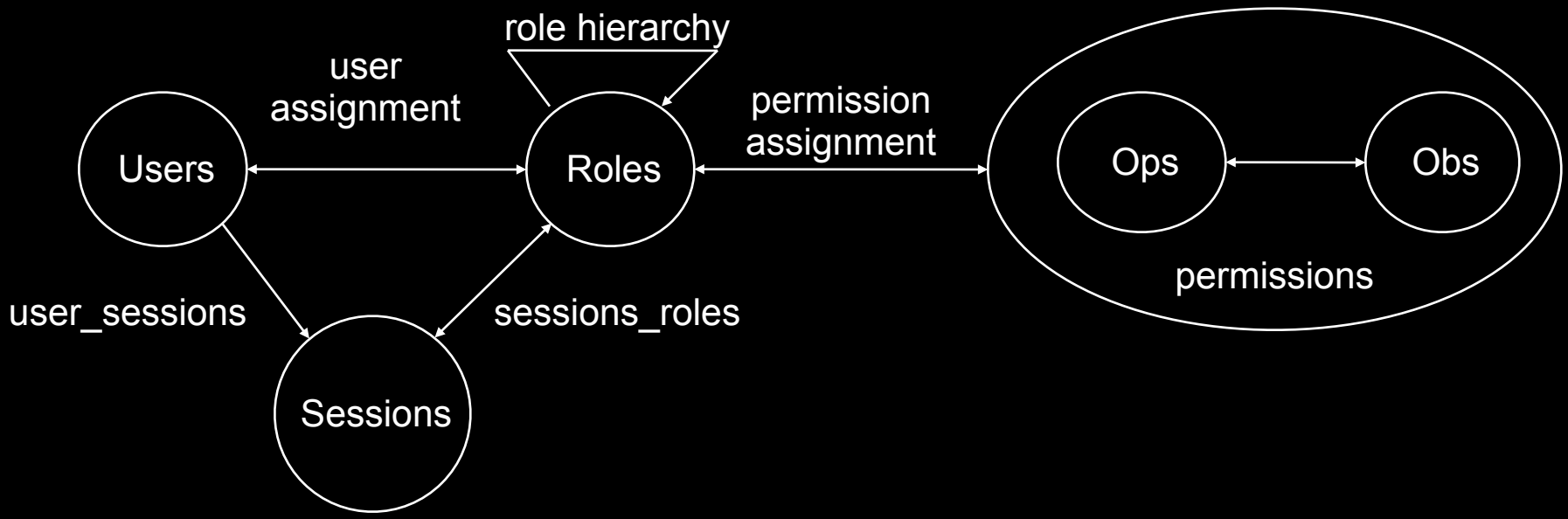
subject/object ratio

J. Crampton, W. Leung, K. Beznosov, "The Secondary and Approximate Authorization Model and its Application to Bell-LaPadula Policies," in *Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT)*, Lake Tahoe, California, USA, 7-9 June, 2006, pp. 111-120.

$SAAM_{RBAC}$: SAAM for RBAC

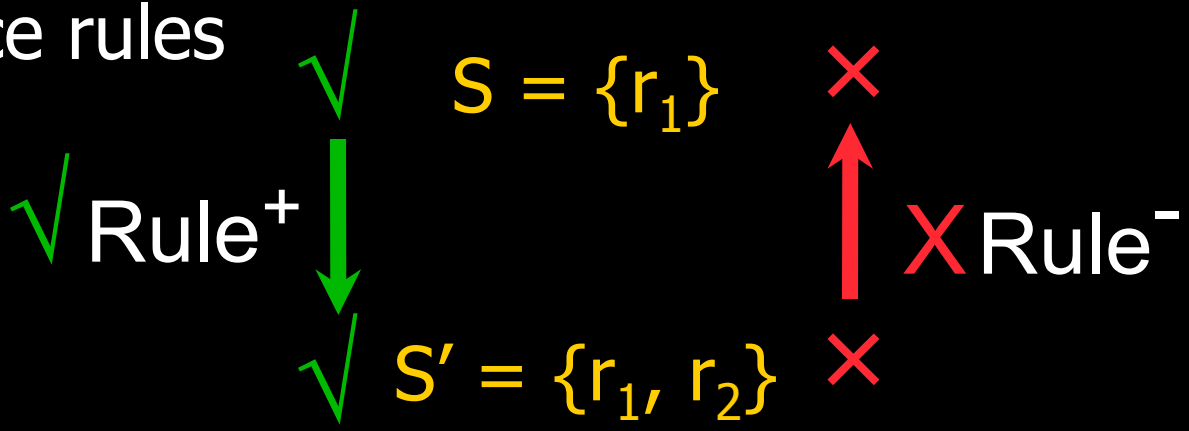
Q. Wei, J. Crampton, K. Beznosov, M. Ripeanu, "Authorization Recycling in RBAC Systems" to appear in Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Estes Park, Colorado, 11-13 June 2008.

RBAC review


role hierarchy
user
assignment
permission
assignment
Users
Roles
Ops
Obs
permissions
user_sessions
sessions_roles
Sessions

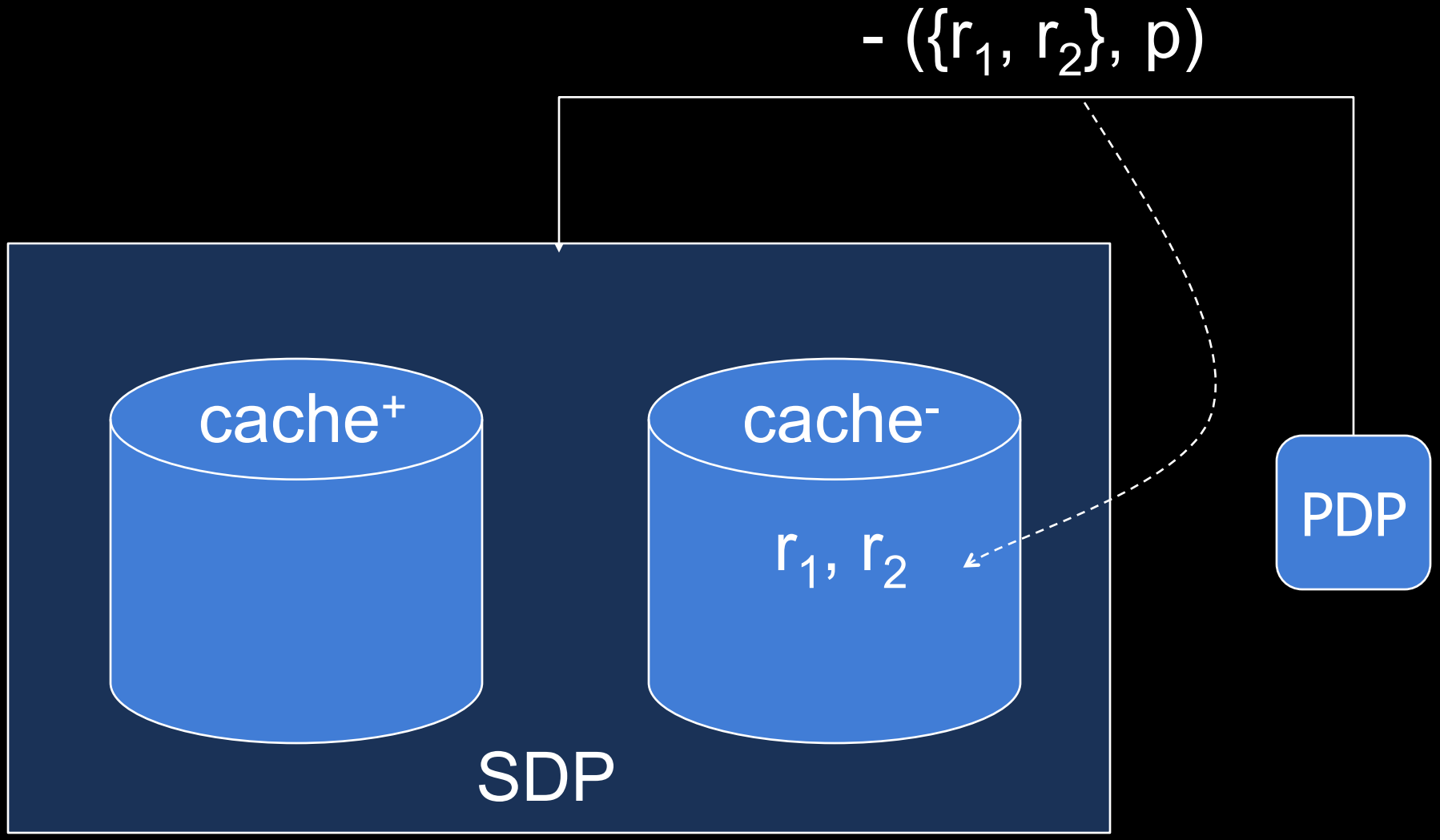
preliminaries

- request: issued by a subject for a permission.
  - request=(s,p)
- ±: denotes the decision to a request.
  - response=+(s,p) or –(s,p)
- subject: modeled as a set of roles.
  - s= $\{r_2, r_3, r_4\}$
- inference rules

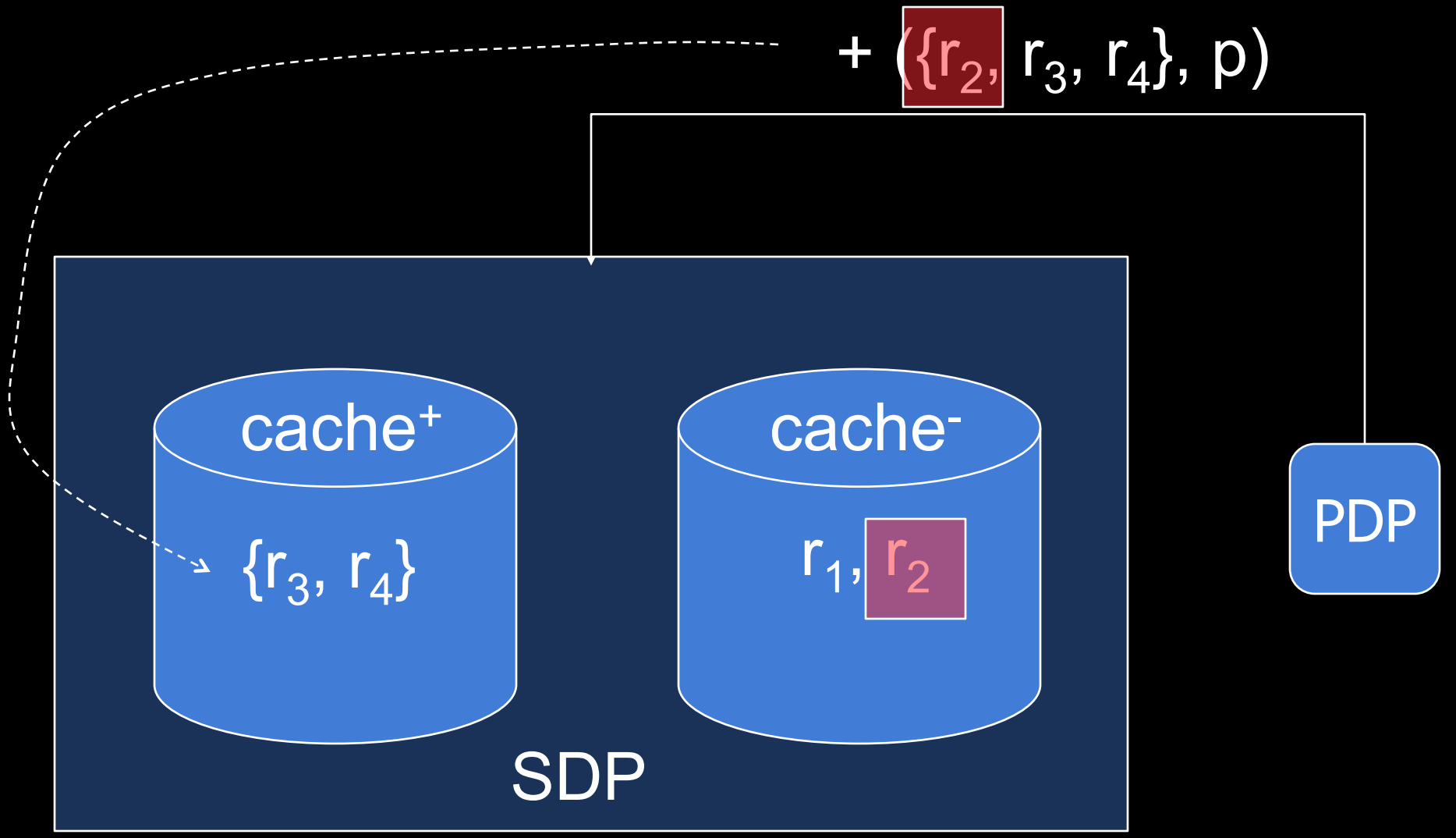


example

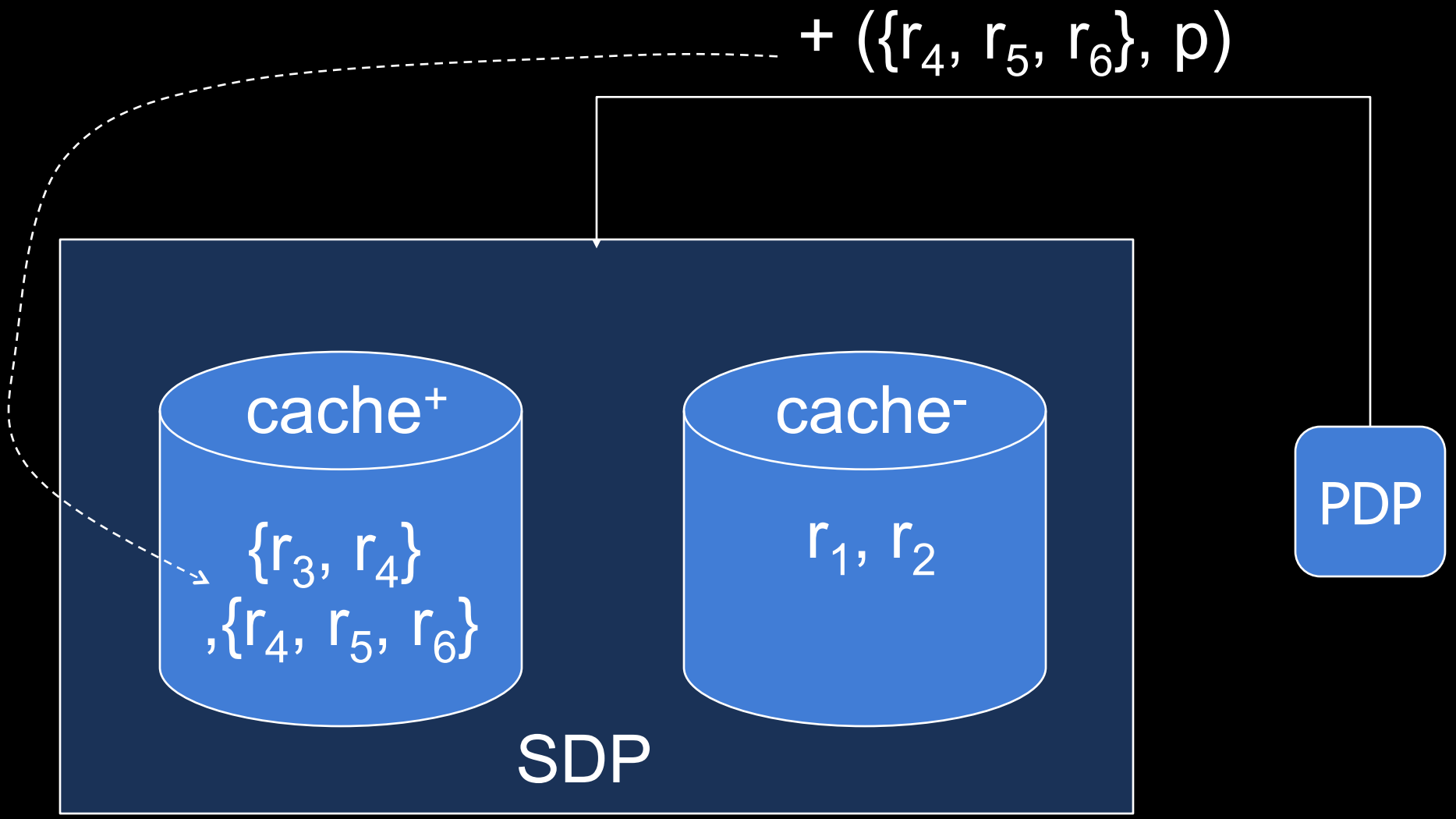
caching first negative decision



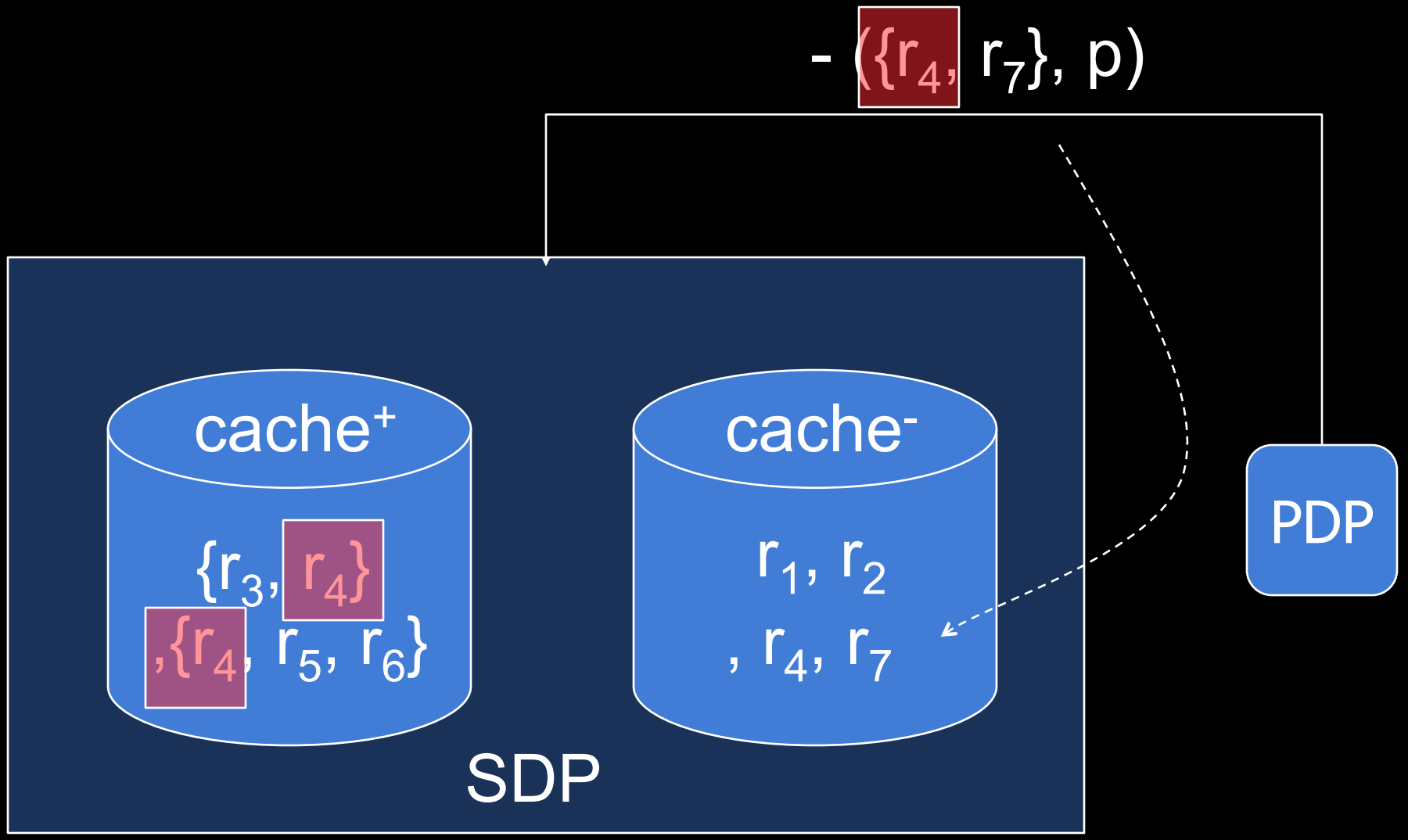
caching first positive decision



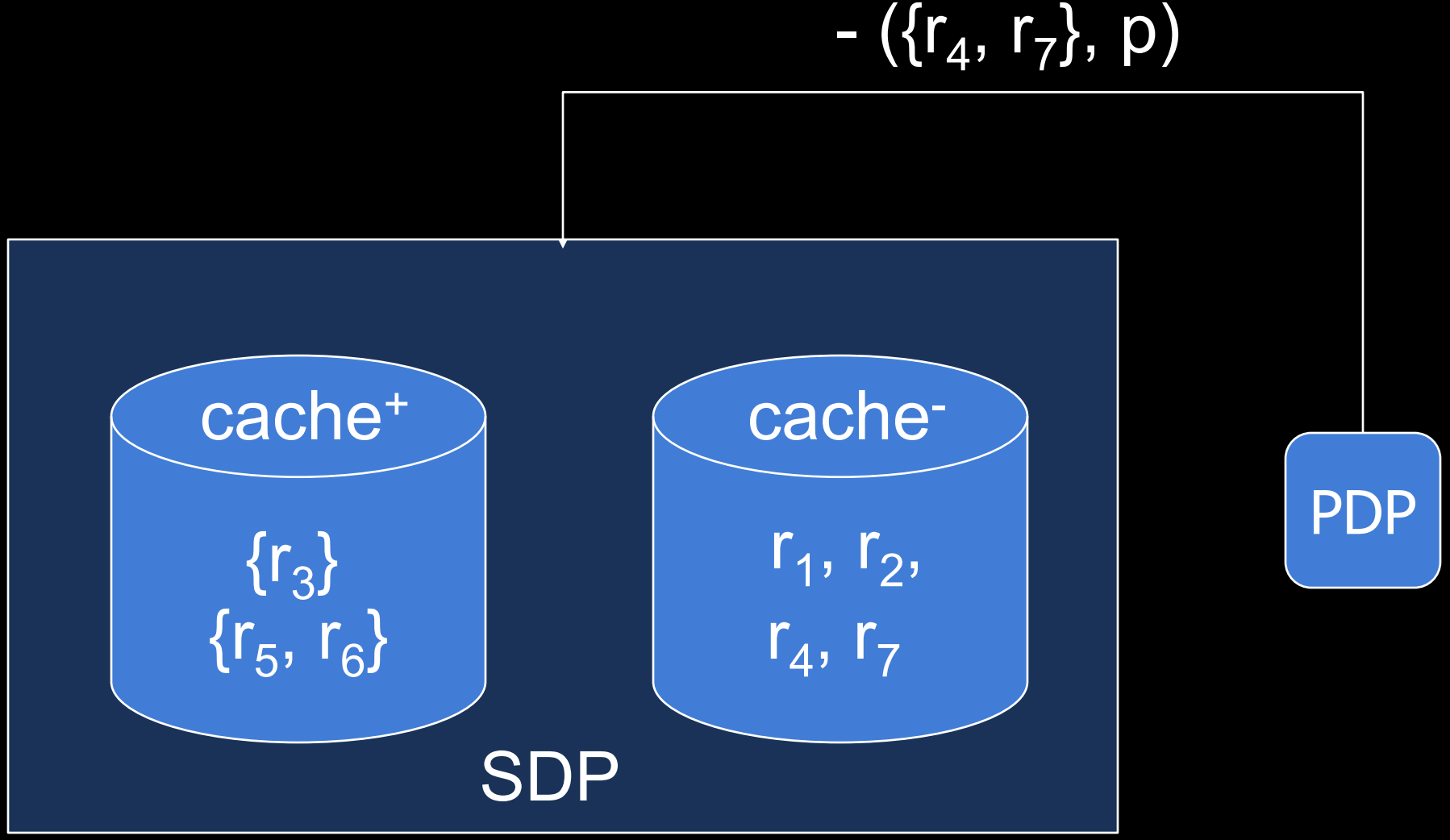
caching second positive decision



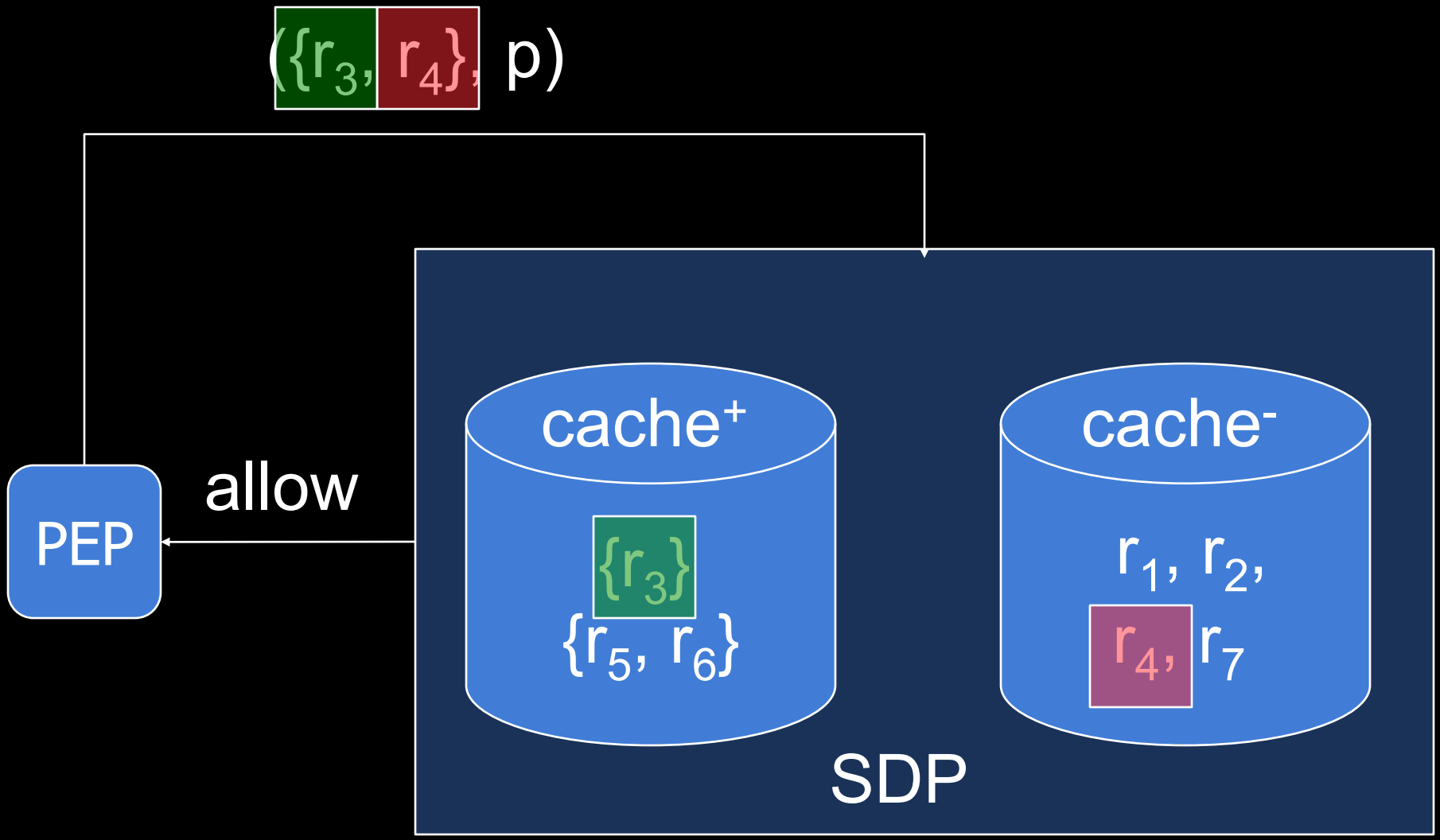
caching second negative decision



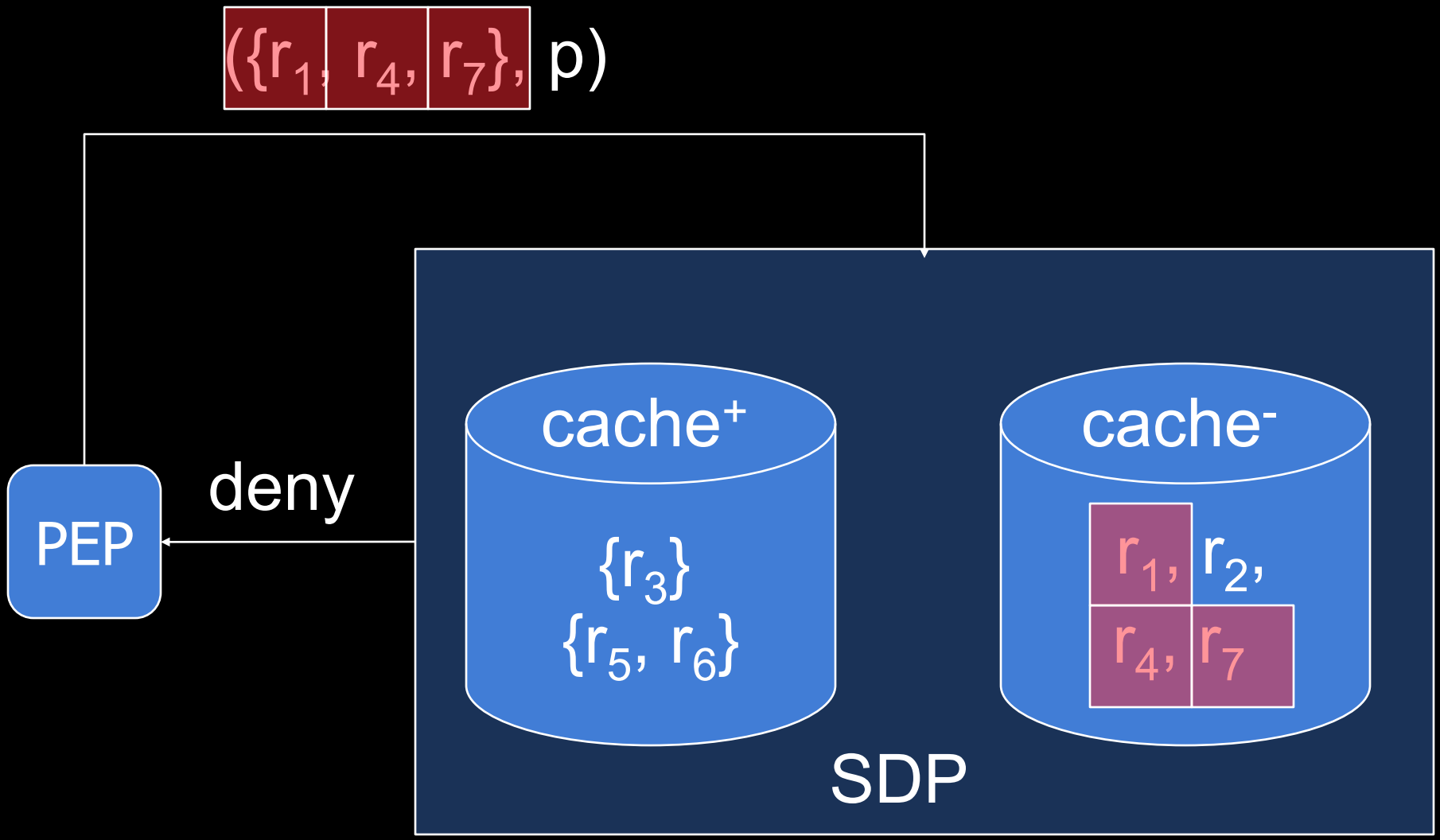
caching second negative decision



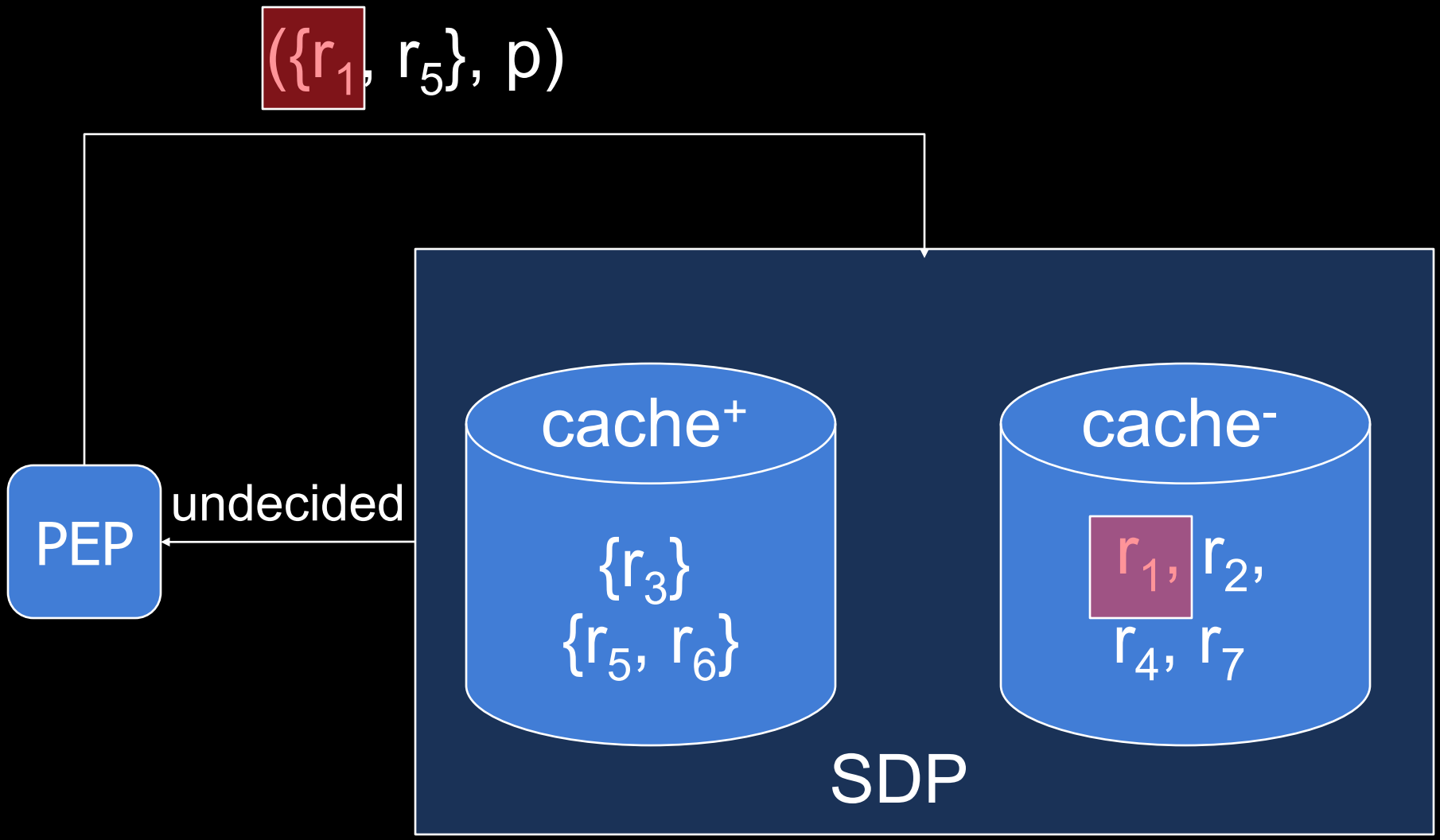
computing allowing authorization



computing denying authorization



computing undecided authorization

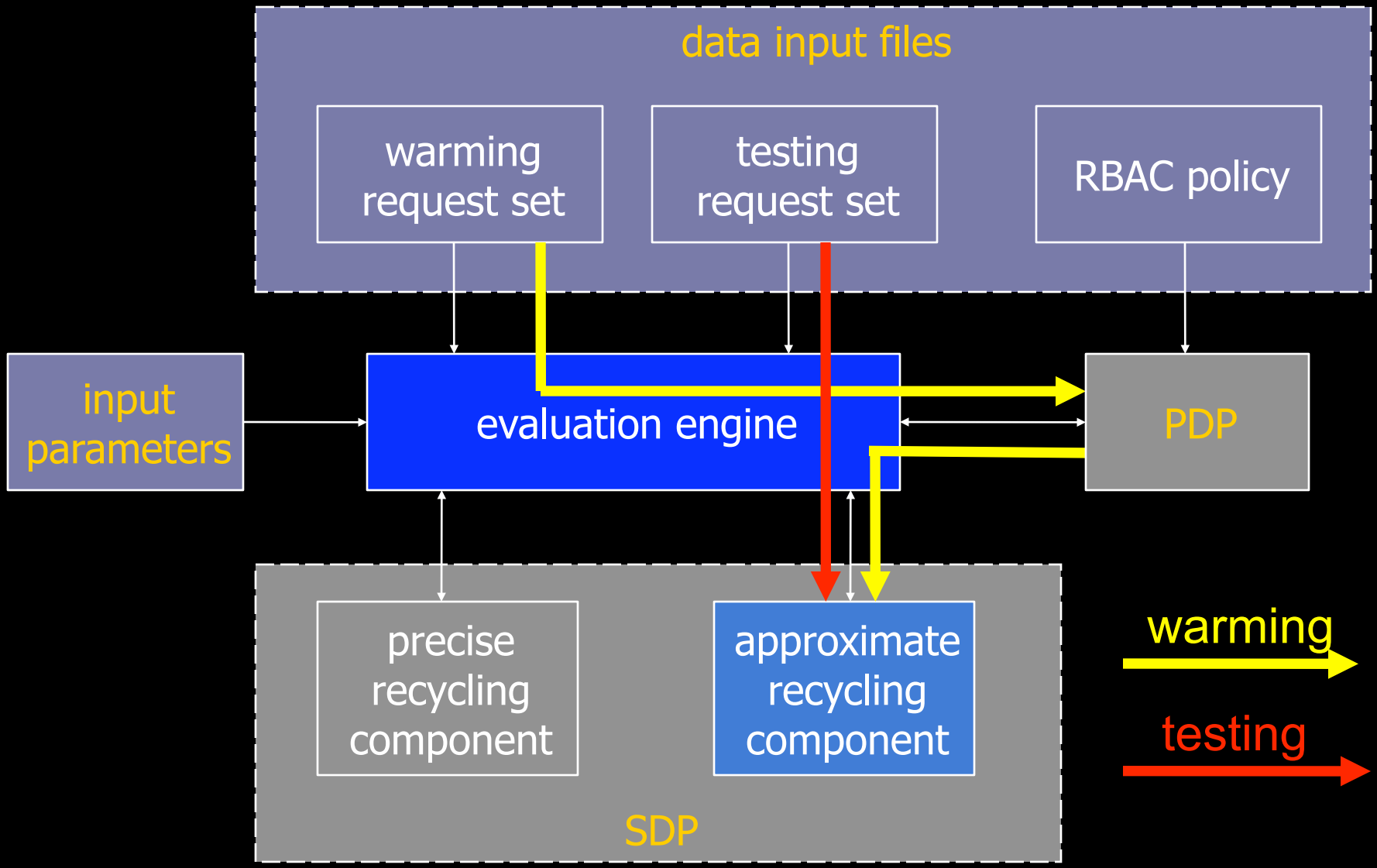


$SAAM_{RBAC}$ evaluation

evaluation metrics

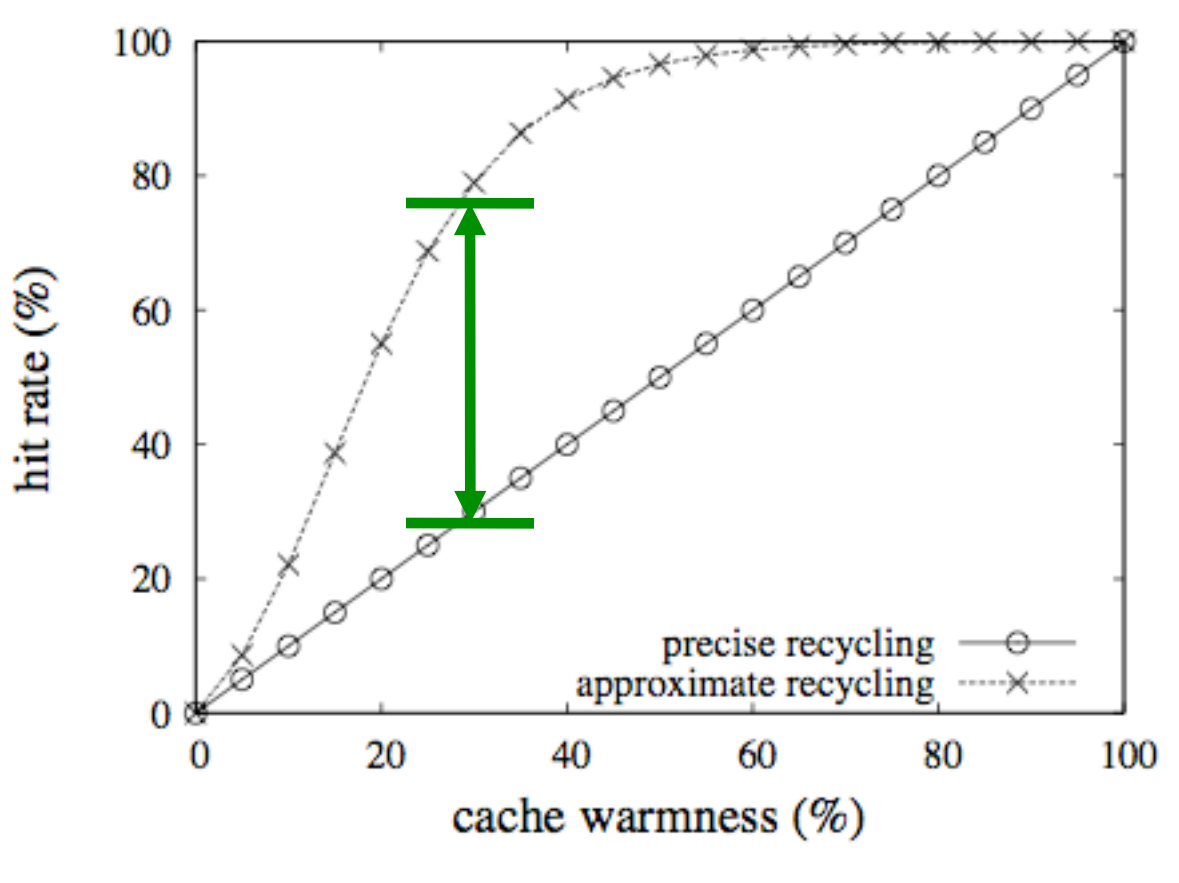
- SDP hit rate
- SDP inference time
  - the time used to infer approximate responses
  - less inference time, more efficient the system

evaluation methodology

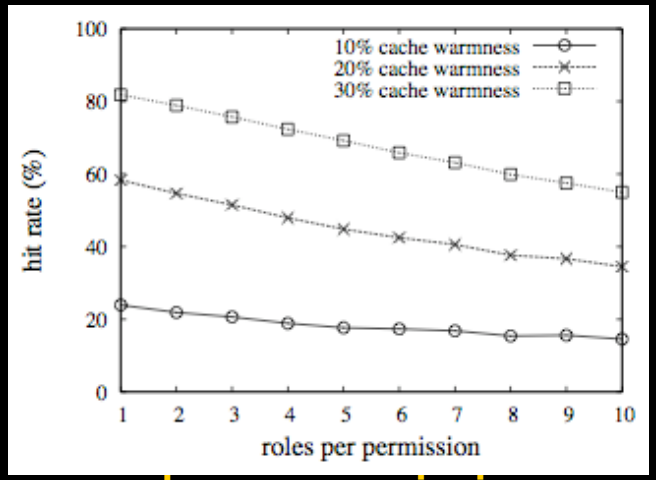


hit rate

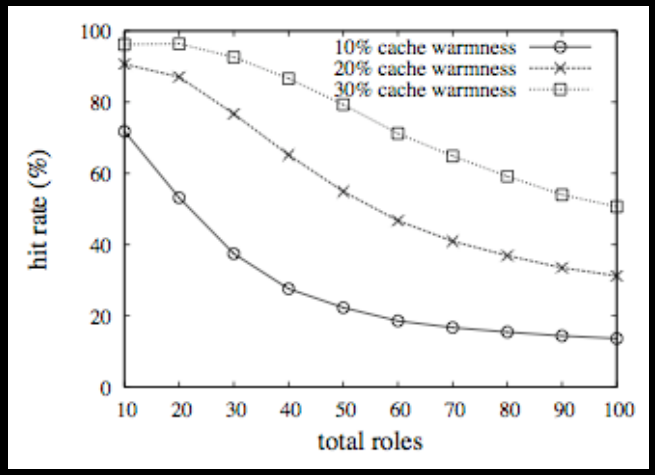
RBAC policy: 100 subjects, 1,000 objects, 50 roles
uniform distribution



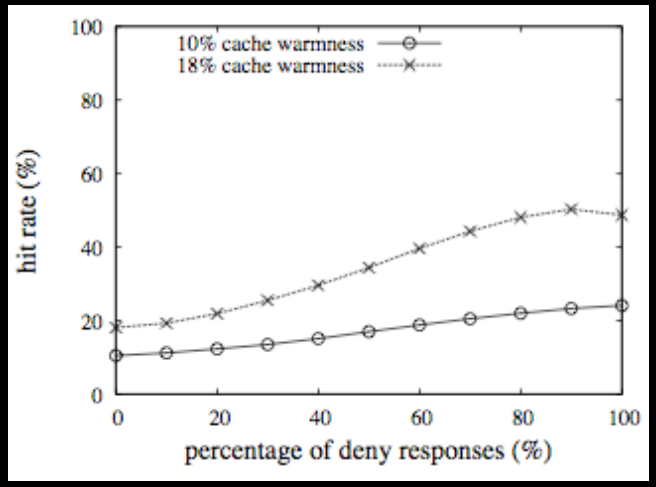
impact of various system parameters



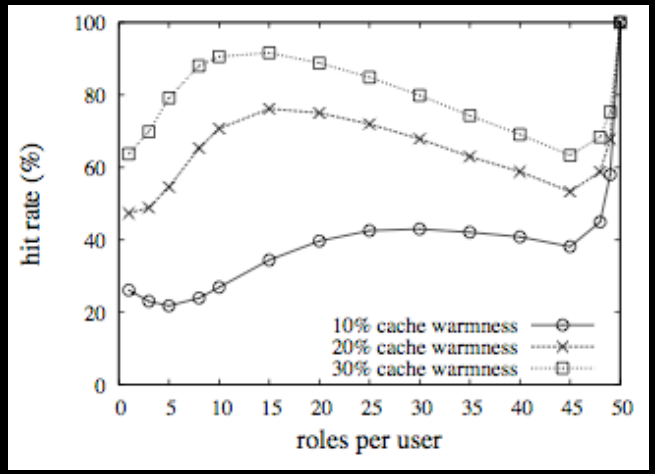
roles per permission



total roles

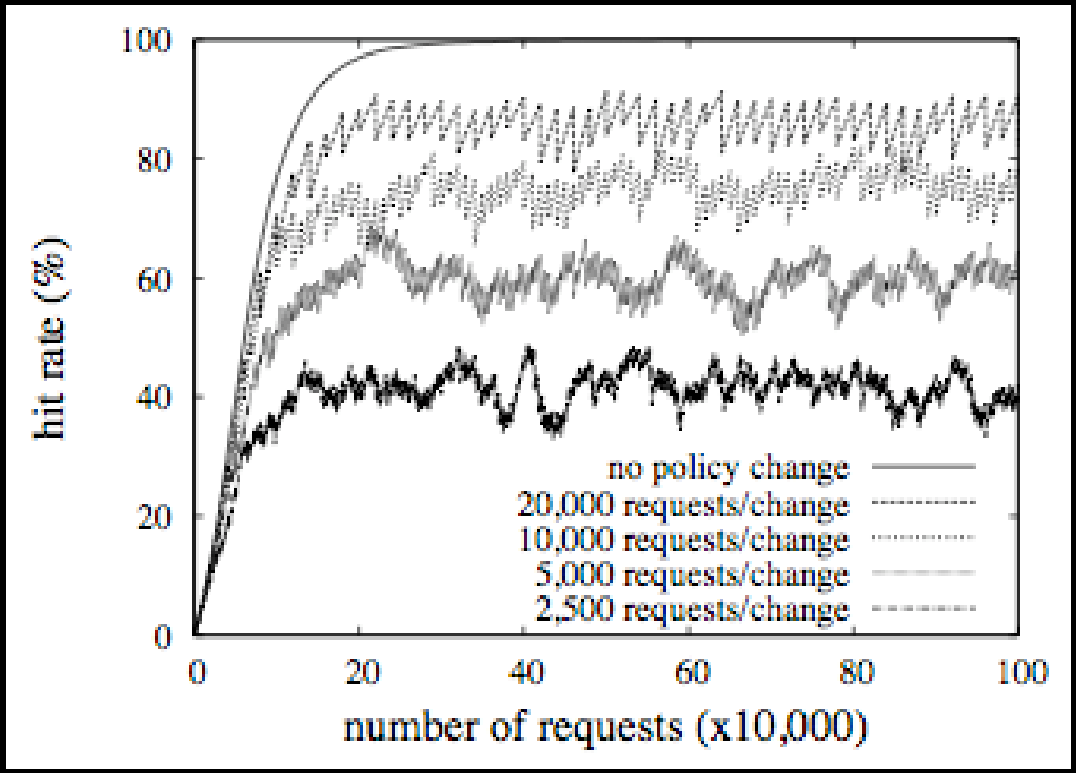


deny vs. allow responses

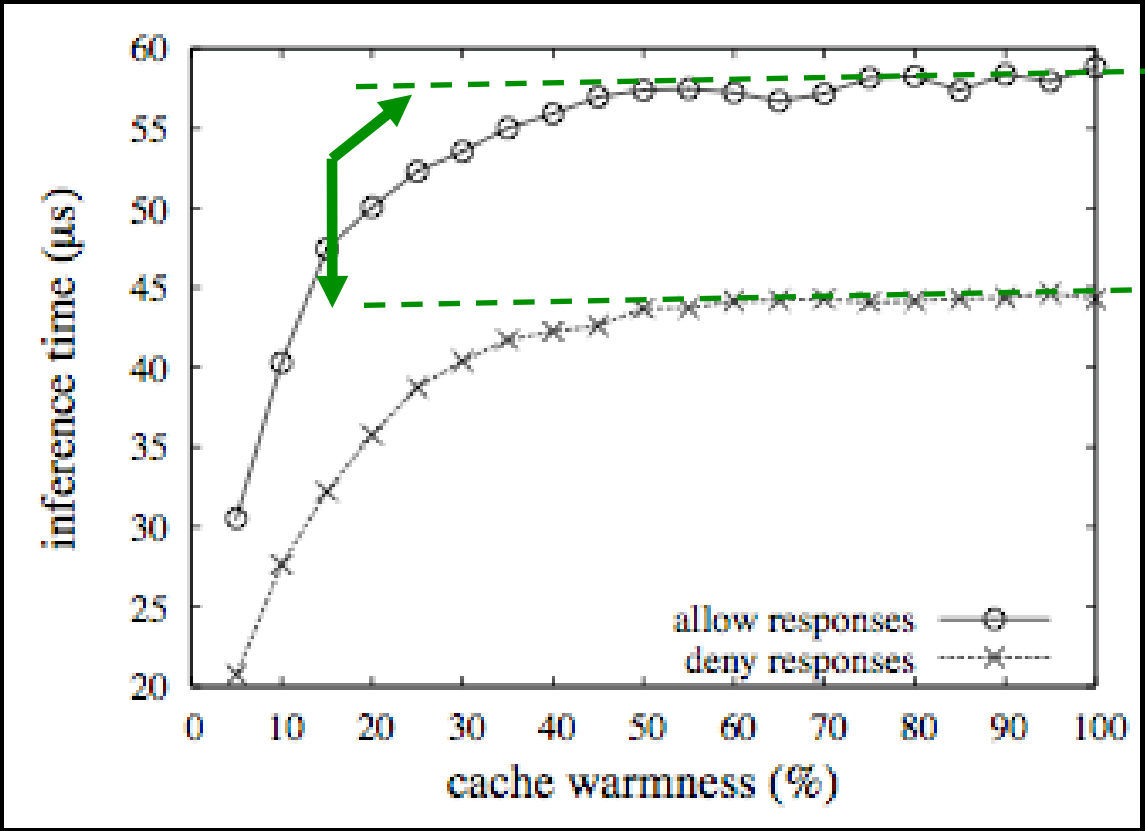


roles per user

impact of policy changes



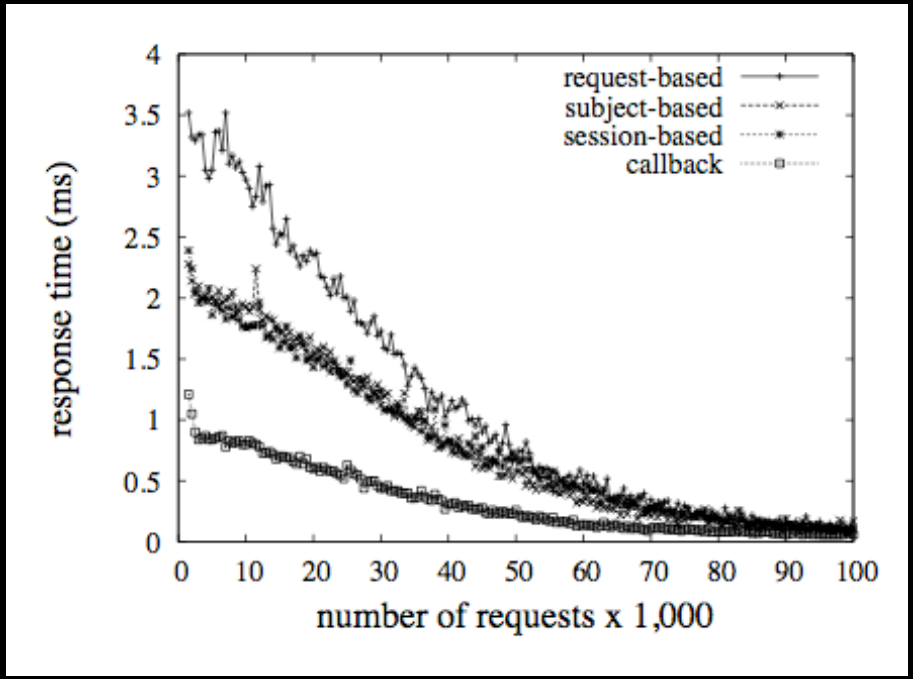
inference time



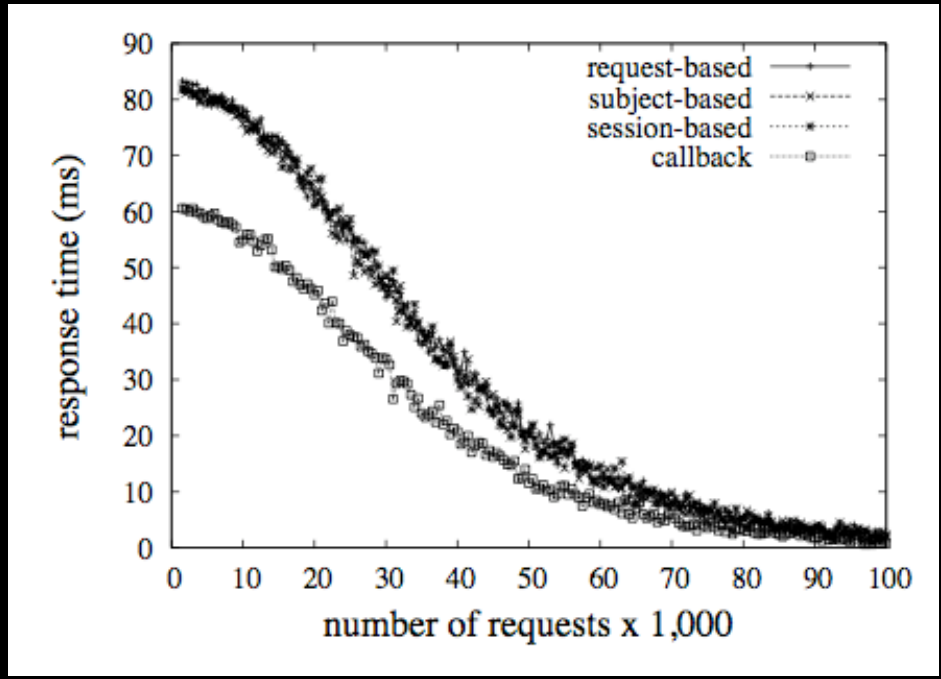
Q. Wei, J. Crampton, K. Beznosov, M. Ripeanu, "Authorization Recycling in RBAC Systems" to appear in Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Estes Park, Colorado, 11-13 June 2008.

combining pub-sub & recycling

LAN



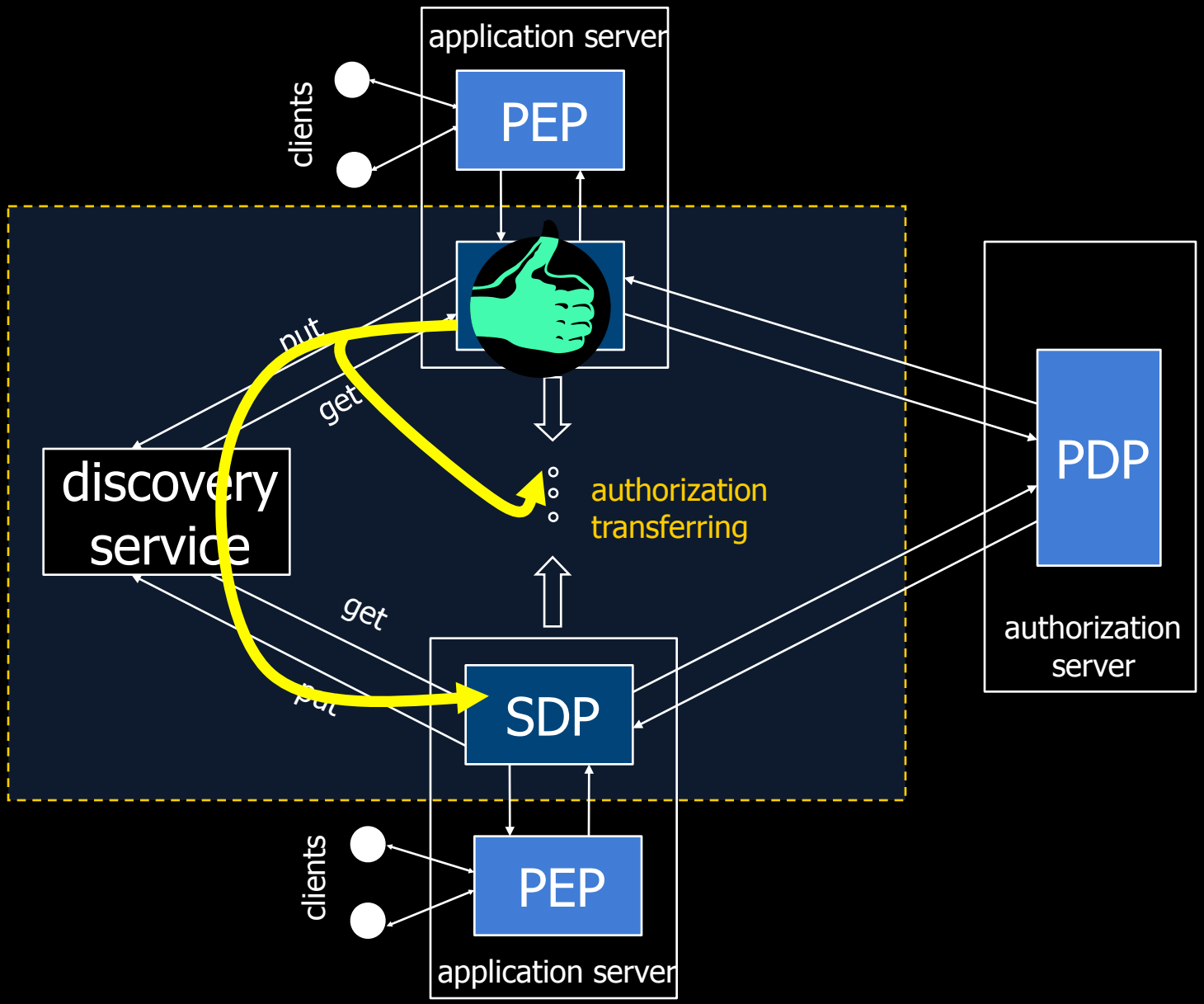
WAN



response time decreases with the number of requests

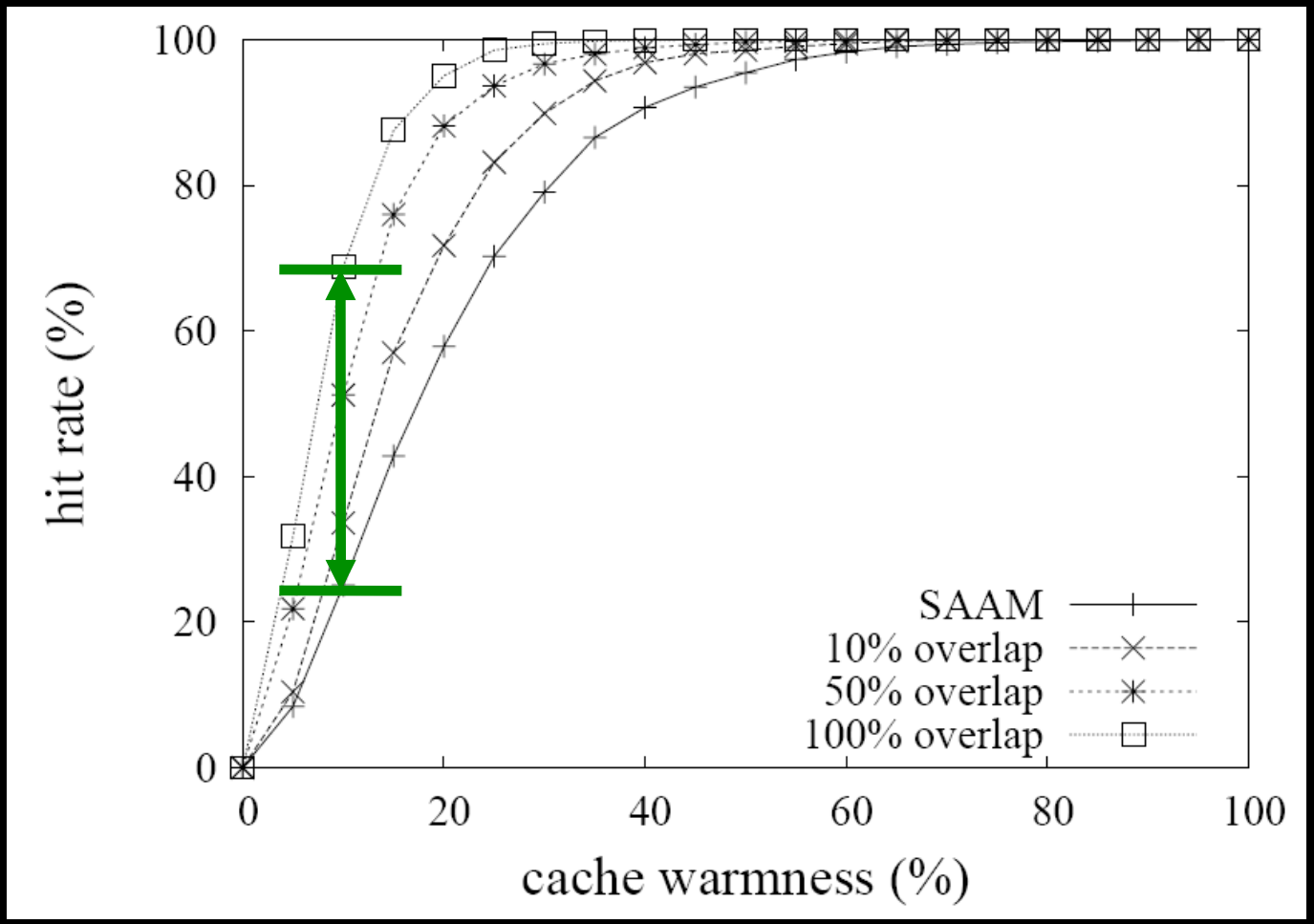
because more requests can be resolved by the local SDP

distributed and cooperative SAAM



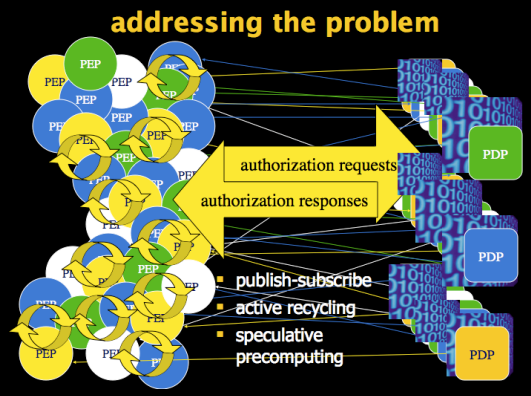
hit rate for distributed $SAAM_{BLP}$

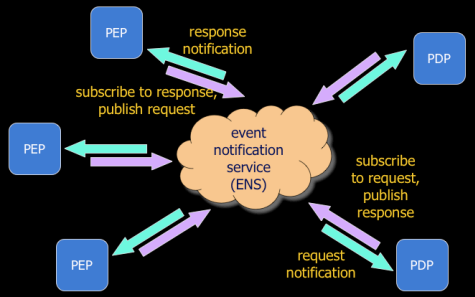
5 SDPs' cooperation, uniform requests

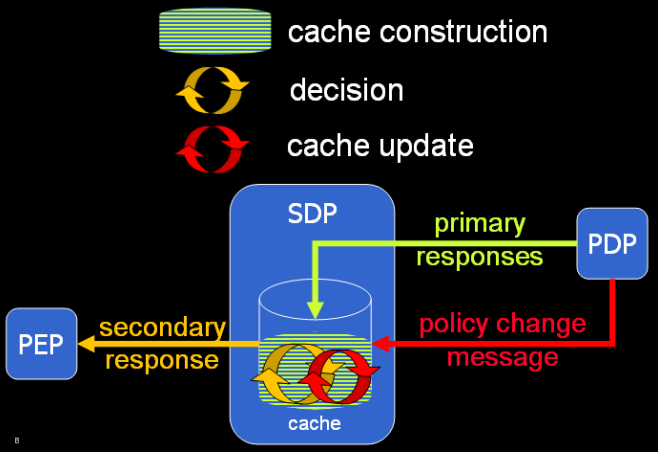


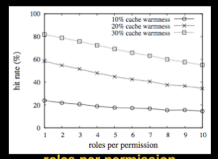
- Q. Wei, M. Repanu, K. Beznosov, "Cooperative Secondary and Approximate Authorization Recycling," in Proceedings of the IEEE International Symposium on High-Performance Distributed Computing (HPDC), Monterey Bay, CA, 27-29 June 2007, pp. 65-74.
- Q. Wei, M. Ripeanu, K. Beznosov, "Cooperative Secondary Authorization Recycling" in *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 2, February 2009, pp. 275-288.

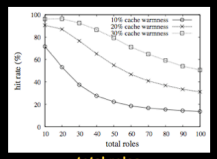
summary

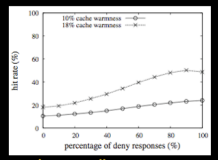

addressing the problem
PEP
PDP
authorization requests
authorization responses
publish-subscribe
active recycling
speculative precomputing

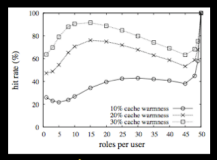

PEP
PDP
response notification
subscribe to response, publish request
event notification service (ENS)
subscribe to request, publish response
request notification

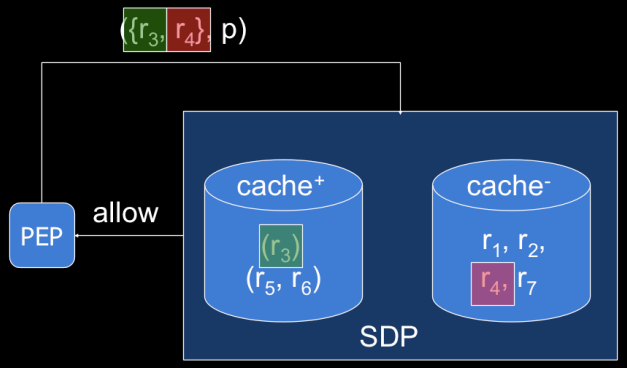

cache construction
decision
cache update
SDP
primary responses
PDP
PEP
secondary response
policy change message
cache

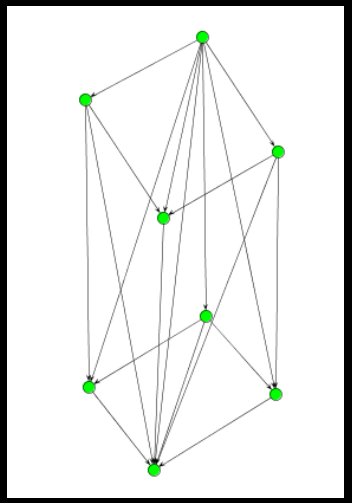

roles per permission


total roles


deny vs. allow responses


roles per user


p)
PEP
allow
cache+
cache-
SDP



project team

Qiang Wei

Wing Leung

Matei Ripeanu

Jason Crampton
Information Security
Group at Royal Holloway
University of London

Kosta Beznosov

selected project publications

- K. Beznosov, "Flooding and Recycling Authorizations" in Proceedings of New Security Paradigms Workshop (NSPW), 2005, Lake Arrowhead, CA, USA, 20-23 September 2005, pp. 67-72.
- pub-sub for authorization
  - Q. Wei, M. Ripeanu, K. Beznosov "Authorization using Publish-Subscribe Model," in *Proceedings of the IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA'08)*, December 10-12, 2008, Sydney, Australia, pp. 53-62
- SAAM for RBAC
  - Q. Wei, J. Crampton, K. Beznosov, M. Ripeanu, "Authorization Recycling in RBAC Systems" in *Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT)*, Estes Park, Colorado, 11-13 June 2008, pp. 63-72.
- SAAM for Bell-Lapadula
  - J. Crampton, W. Leung, K. Beznosov, "The Secondary and Approximate Authorization Model and its Application to Bell-LaPadula Policies," in Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Lake Tahoe, California, USA, 7-9 June, 2006, pp. 111-120.
- Distributed and cooperative SAAM
  - Q. Wei, M. Repanu, K. Beznosov, "Cooperative Secondary and Approximate Authorization Recycling," in Proceedings of the IEEE International Symposium on High-Performance Distributed Computing (HPDC), Monterey Bay, CA, 27-29 June 2007, pp. 65-74.
  - Q. Wei, M. Ripeanu, K. Beznosov, "Cooperative Secondary Authorization Recycling" in IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 2, February 2009, pp. 275-288.

Konstantin (Kosta) Beznosov

konstantin.beznosov.net