THE UNIVERSITY OF BRITISH COLUMBIA

Secondary and Approximate Authorization Model (SAAM) and its Application to Bell-LaPadula Policies ($\mathrm{SAAM}_{\mathrm{BLP}}$)

Konstantin (Kosta) Beznosov

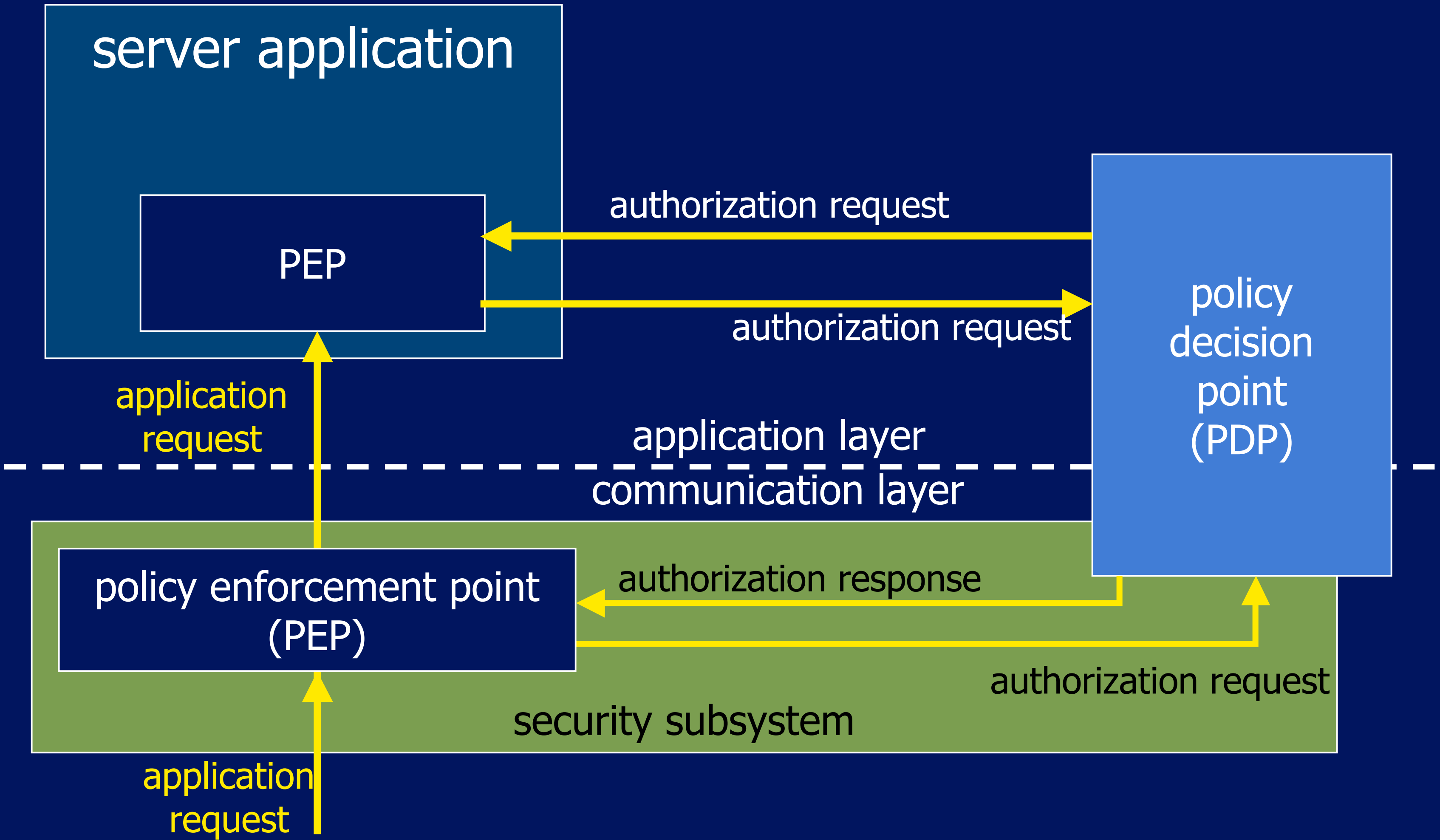
Laboratory for Education and Research in
Secure Systems Engineering

lersse.ece.ubc.ca

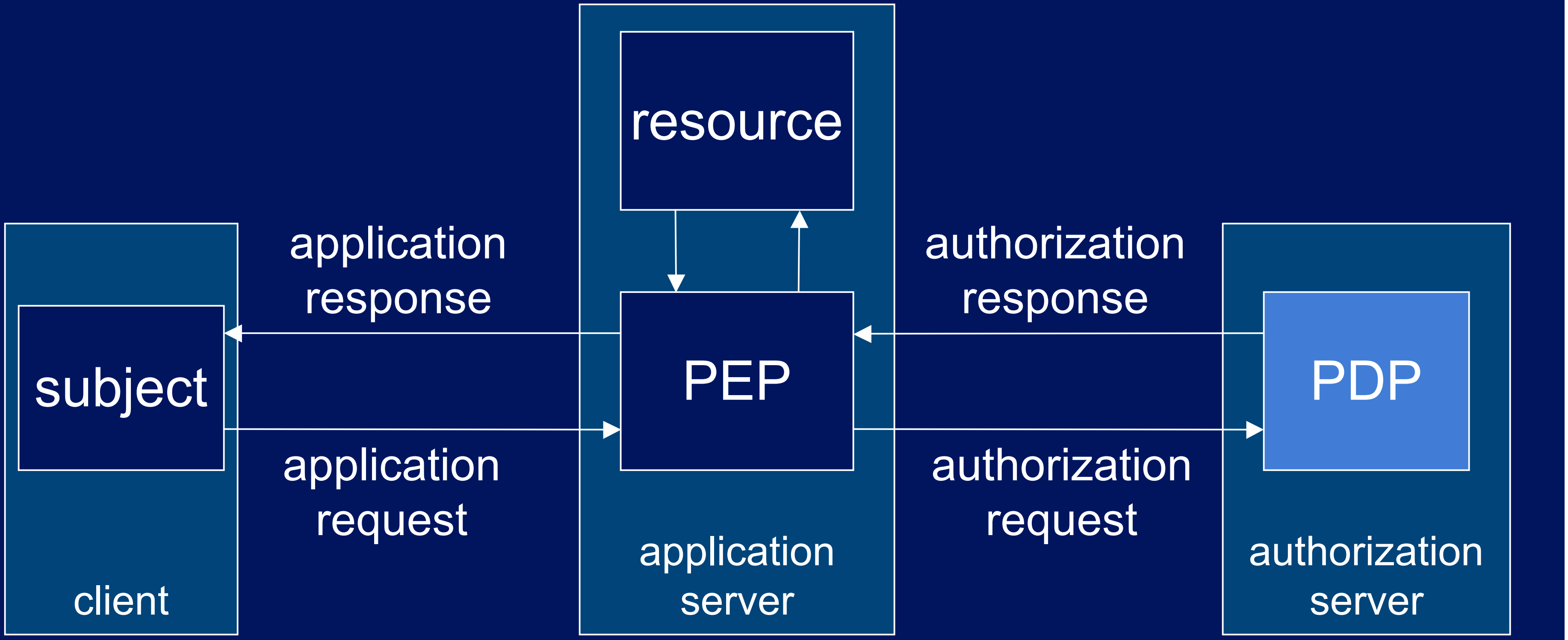
Electrical and Computer Engineering

how enterprise authorization systems work

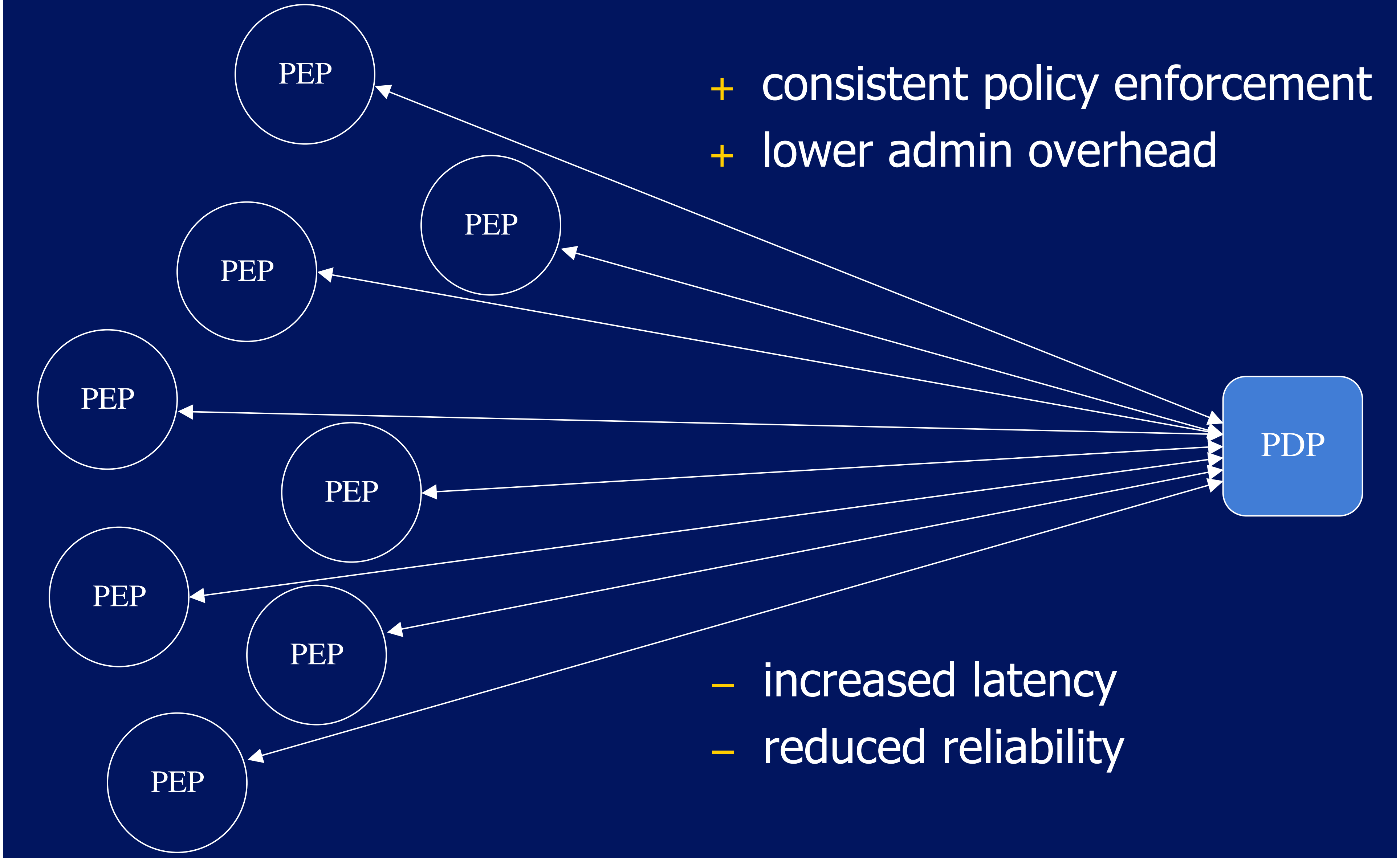
GetAccess, IBM Access Manager, CORBA, EJB, XACML



request-response paradigm



PEP-PDP decoupling: pros and cons



+ consistent policy enforcement
+ lower admin overhead

– increased latency
– reduced reliability

remedies

- caching -- “precise recycling”
  - improves performance & reliability
  - simple, inexpensive
  - serves only returning requests
- fault-tolerance solutions
  - improve reliability
  - require specialized software
  - poorly scale on large populations

our contribution

- concept and model for inferring new authorizations from previous "approximate authorization recycling"
- algorithms for BLP recycling

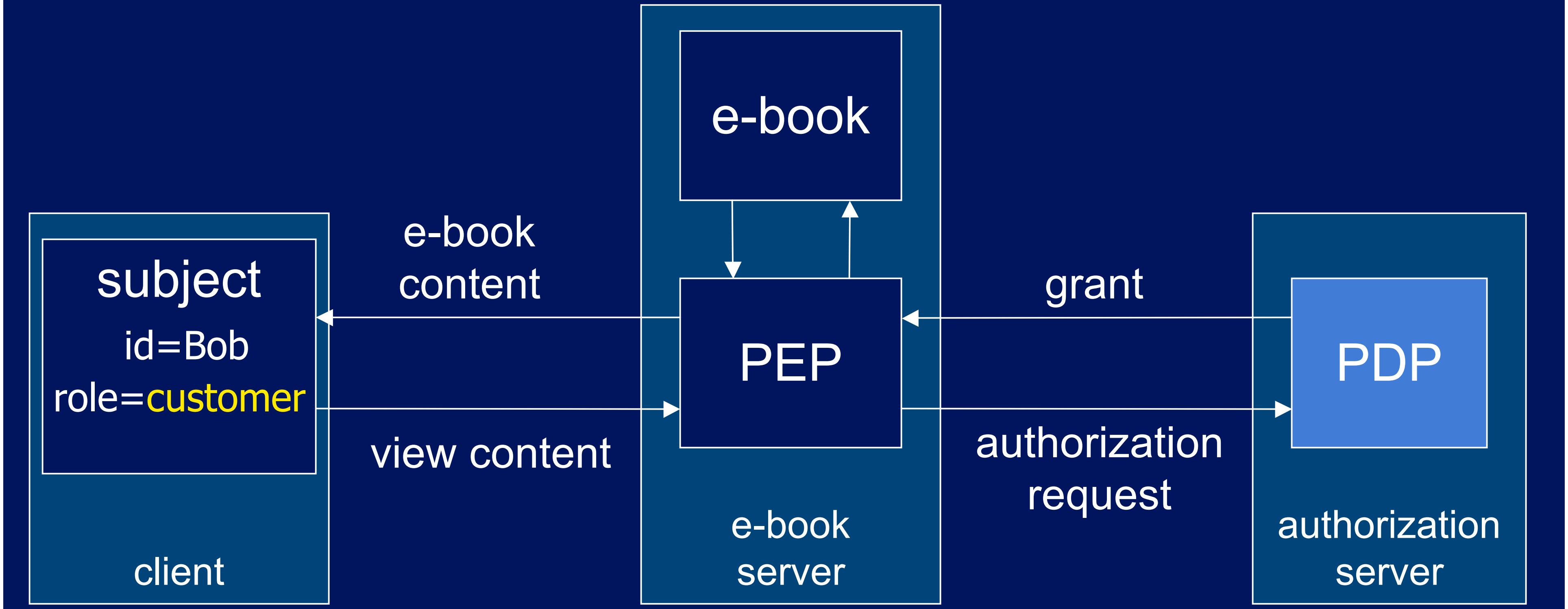
outline

- SAAM
- SAAM_{BLP}
  - evaluation study
- summary
- current status & future work

SAAM: Secondary and Approximate Authorization Model

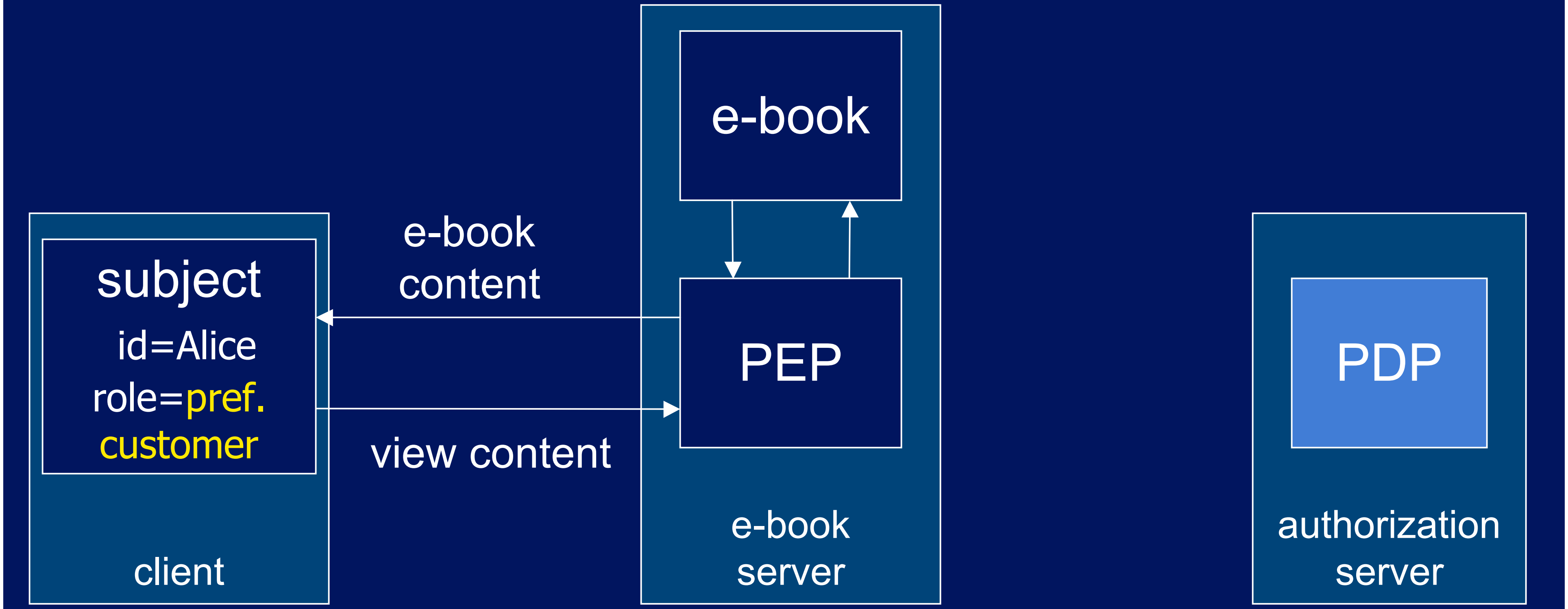
intuition

when Bob accesses the resource …



intuition

when Alice accesses the resource afterwards …



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=“05-08-15”}, 10>

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

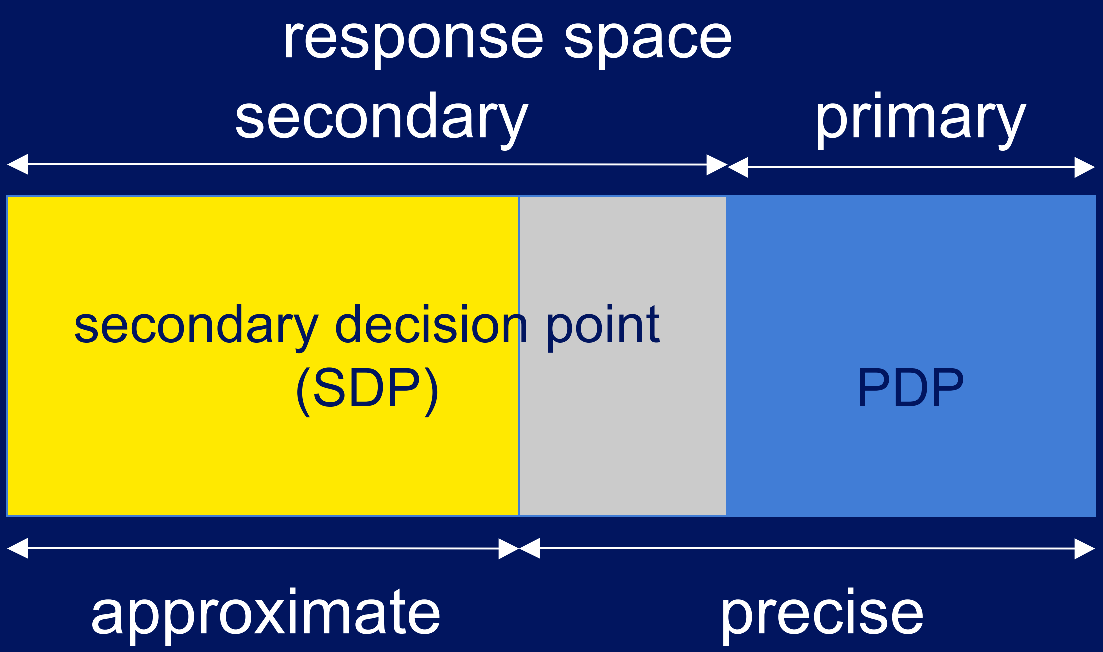
<{id=“Bob”, role=“customer”}, {id=“eB-23”}, view, {date=“05-08-15”}, 11>

equivalent

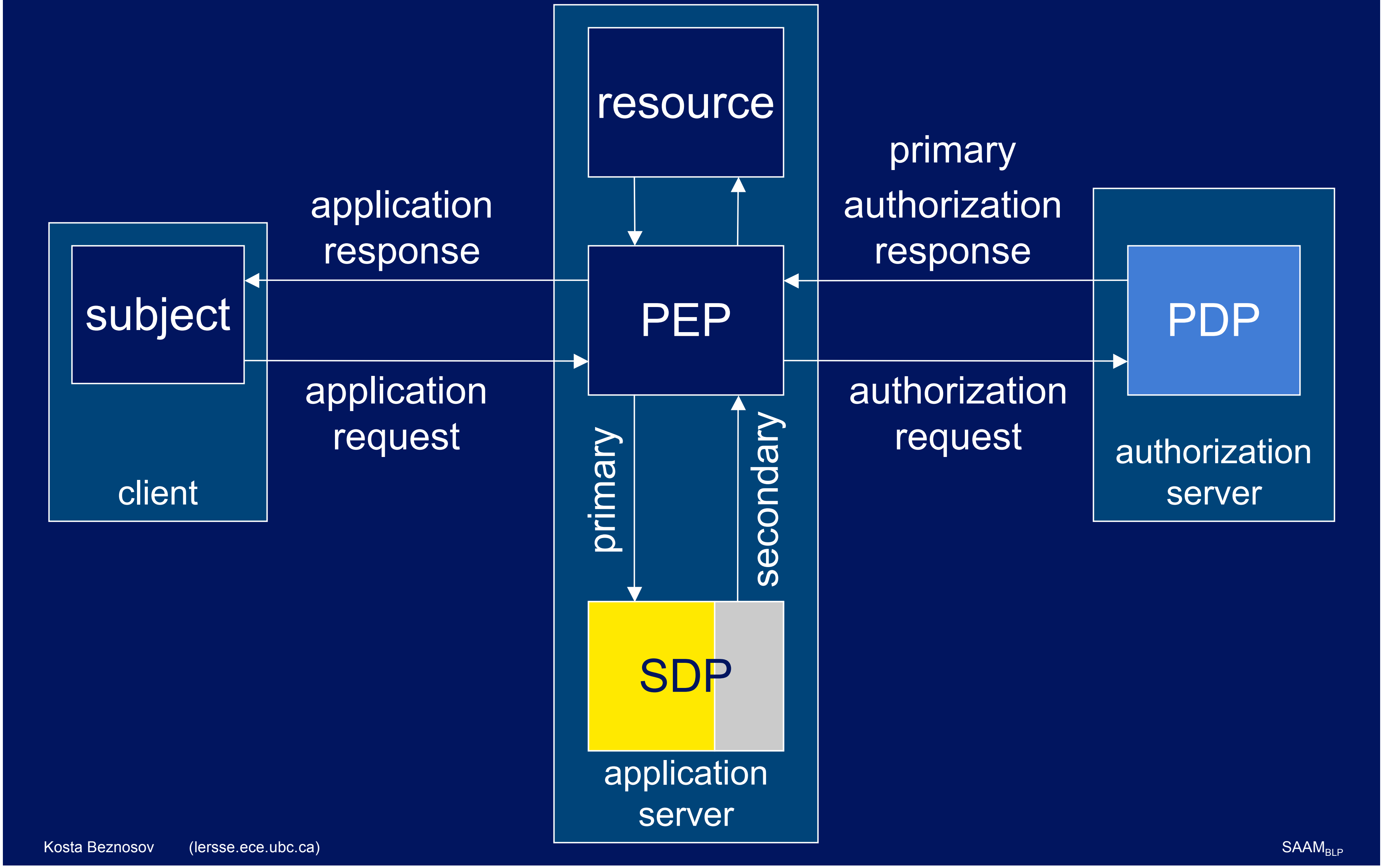
< 2, 11, [1], allow > -- precise response

<{id=“Alice”, role=“pr. cust.”}, {id=“eB-23”}, view, {date=“05-08-15”}, 12>

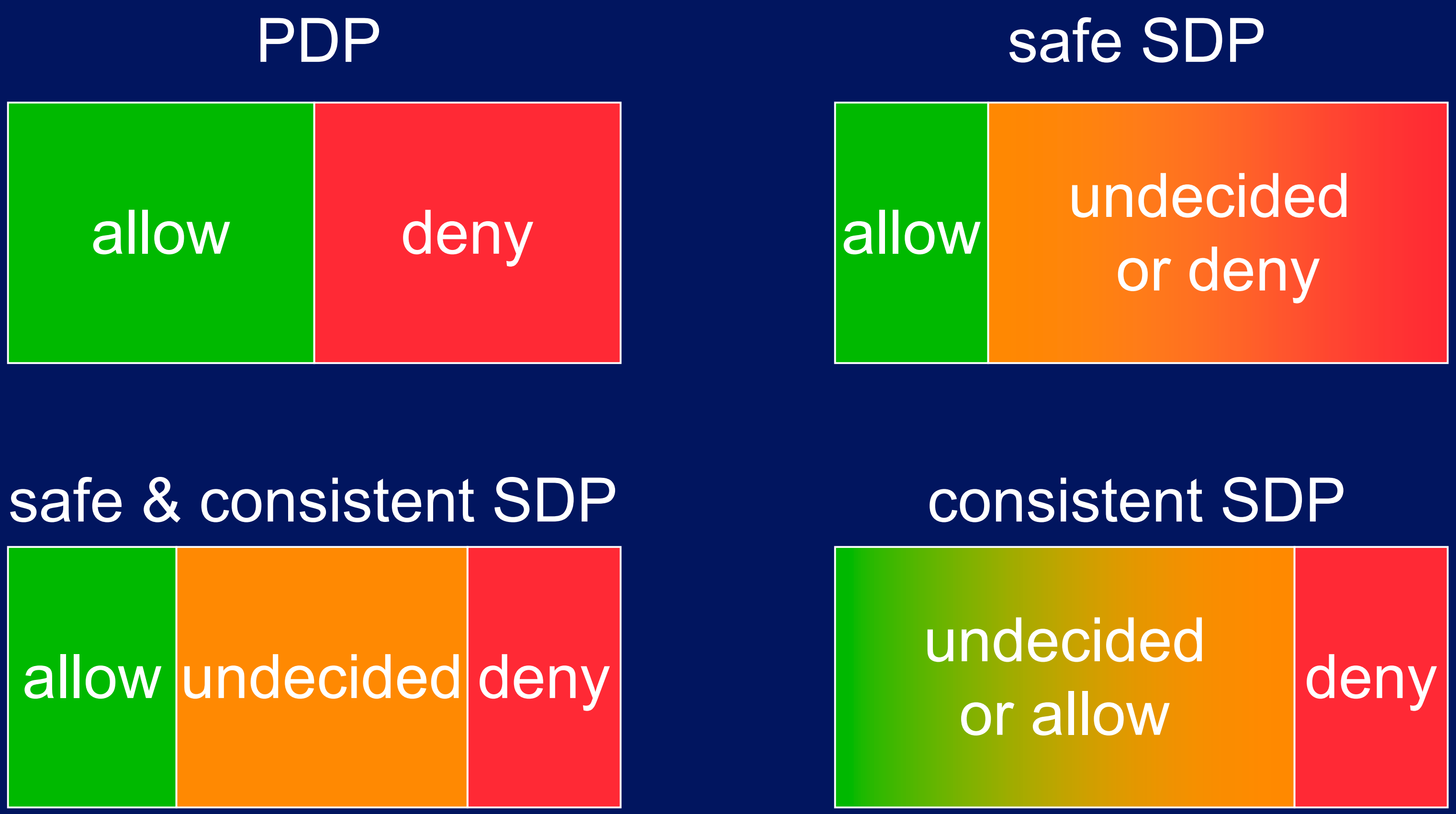
< 3, 12, [1], allow > -- secondary and approximate response



use of secondary decision point



SDP types



PDP

allow | deny

safe SDP

allow | undecided or deny

safe & consistent SDP

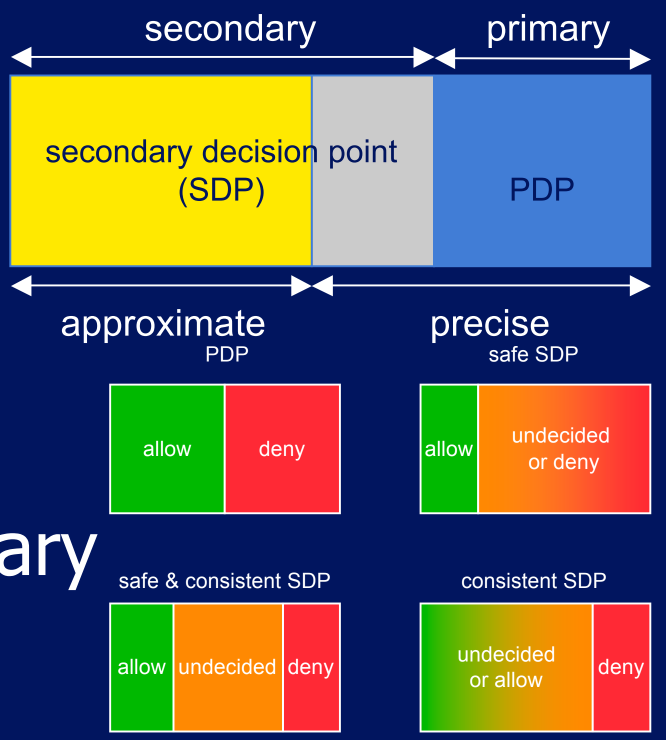
allow | undecided | deny

consistent SDP

undecided or allow | deny

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
  - can be safe and/or consistent



secondary

primary

secondary decision point (SDP)

PDP

approximate

precise

PDP

allow

deny

safe SDP

allow

undecided or deny

safe & consistent SDP

allow

undecided

deny

consistent SDP

undecided or allow

deny

SAAM_{BLP}: Application of SAAM to Bell-Lapadula Model

BLP Refresher

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

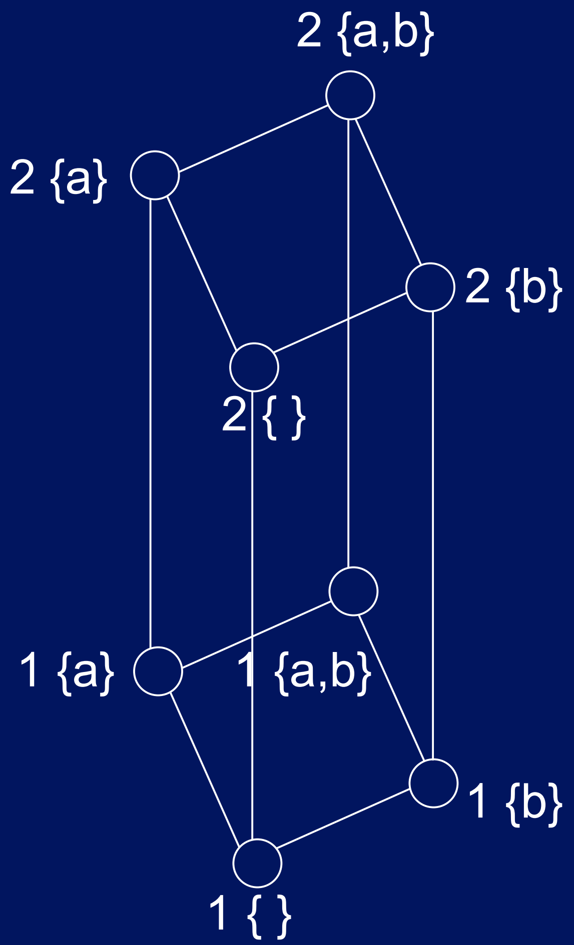
ss-property:

(s, o, read) $\Rightarrow \lambda(s) \geq \lambda(o)$

$*$-property:

(s, o, append) $\Rightarrow \lambda(o) \geq \lambda(s)$

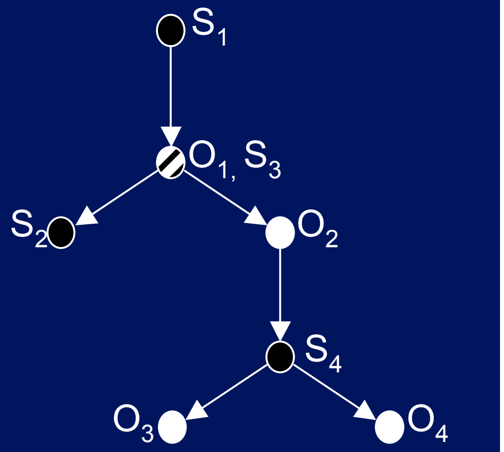
(s, o, write) $\Rightarrow \lambda(o) \equiv \lambda(s)$



three scenarios

1. $\lambda(s)$ and $\lambda(o)$ in request
   - PEP same as PDP
2. $\lambda(s)$ and $\lambda(o)$ in primary responses
   - SDP has L
   - SDP caches <x, $\lambda(x)$>
3. $\lambda(s)$ or $\lambda(o)$ not in request/response

What's SAAM_{BLP}?

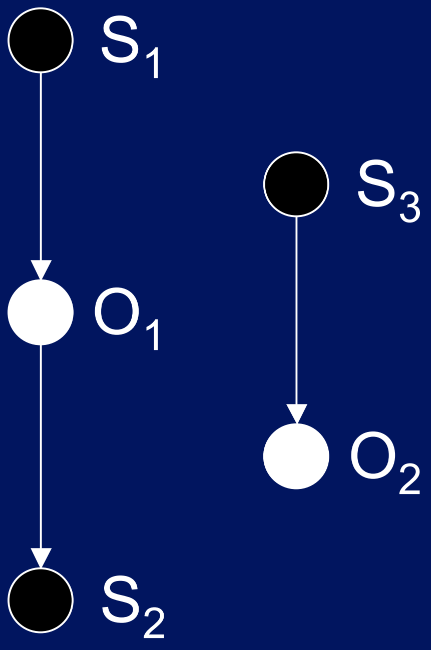


1. dominance graph (DG) -- ADG
2. algorithms for SDP to
   - modify DG based on (primary) authorizations
   - compute secondary authorizations using DG

Dominance Graph

allow

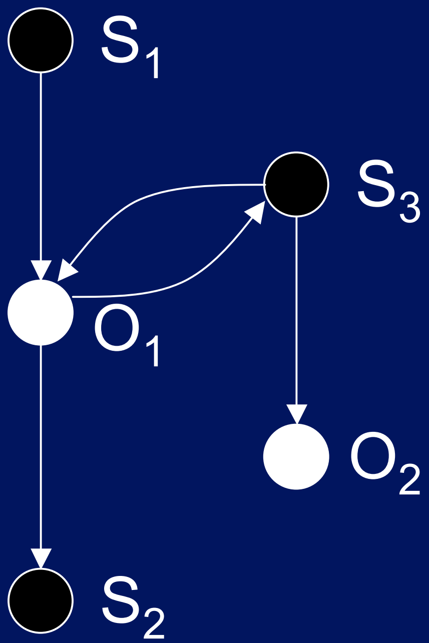
1. (s_1, o_1, read)
2. $(s_2, o_1, \text{append})$
3. (s_3, o_2, read)



Dominance Graph

allow

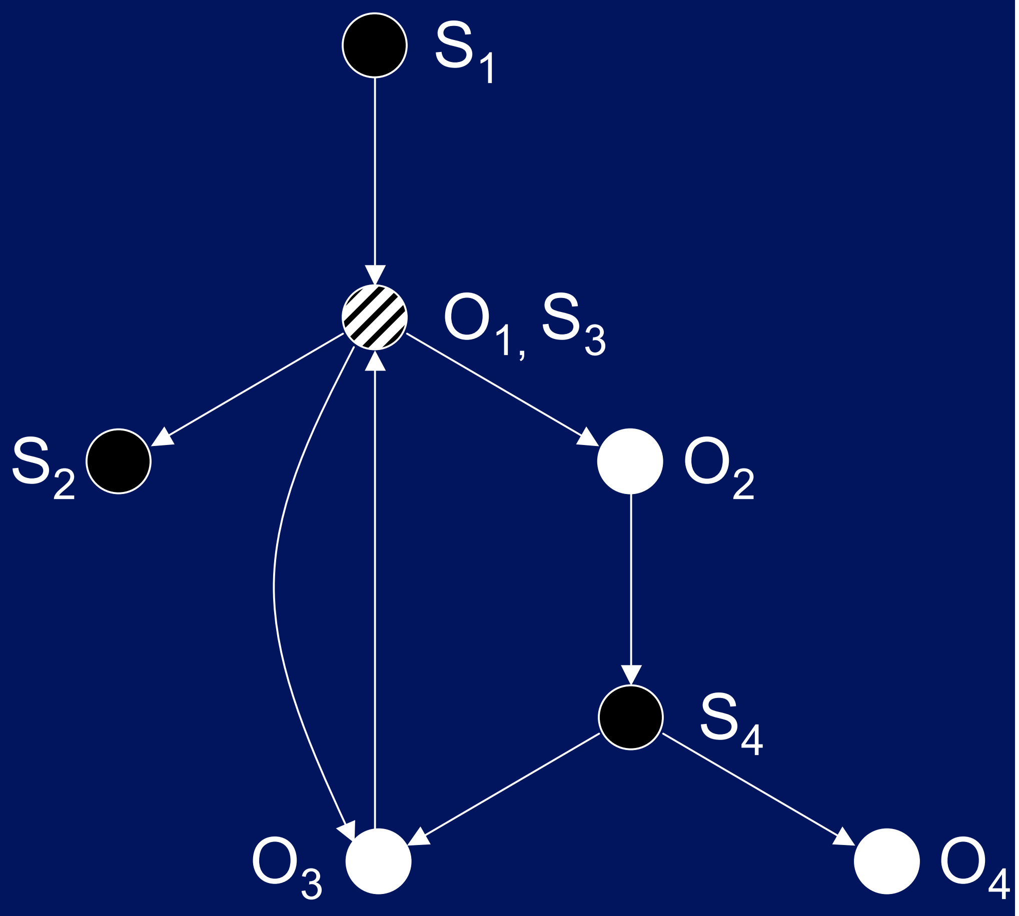
1. (s_1, o_1, read)
2. $(s_2, o_1, \text{append})$
3. (s_3, o_2, read)
4. (s_3, o_1, write)



Dominance Graph

allow

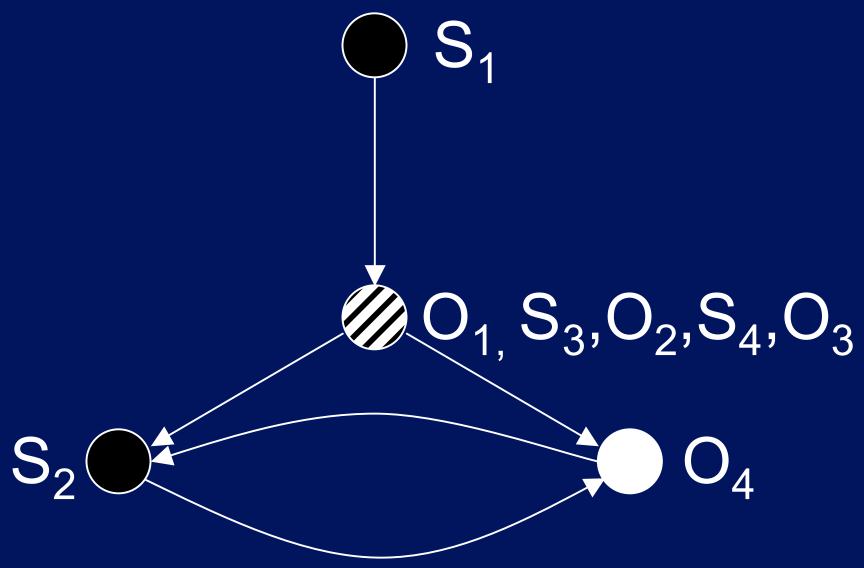
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)



Dominance Graph

allow

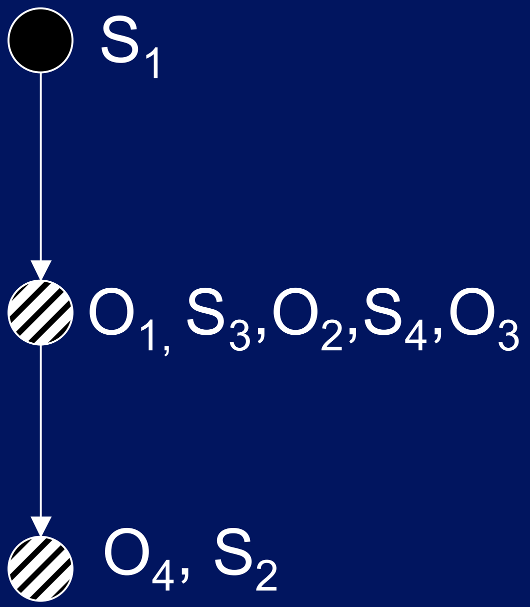
1. $(s_1, o_1, read)$
2. $(s_2, o_1, append)$
3. $(s_3, o_2, read)$
4. $(s_3, o_1, write)$
5. $(s_1, o_2, read)$
6. $(s_4, o_2, append)$
7. $(s_4, o_3, read)$
8. $(s_4, o_4, read)$
9. $(s_3, o_3, write)$
10. $(s_2, o_4, write)$



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)



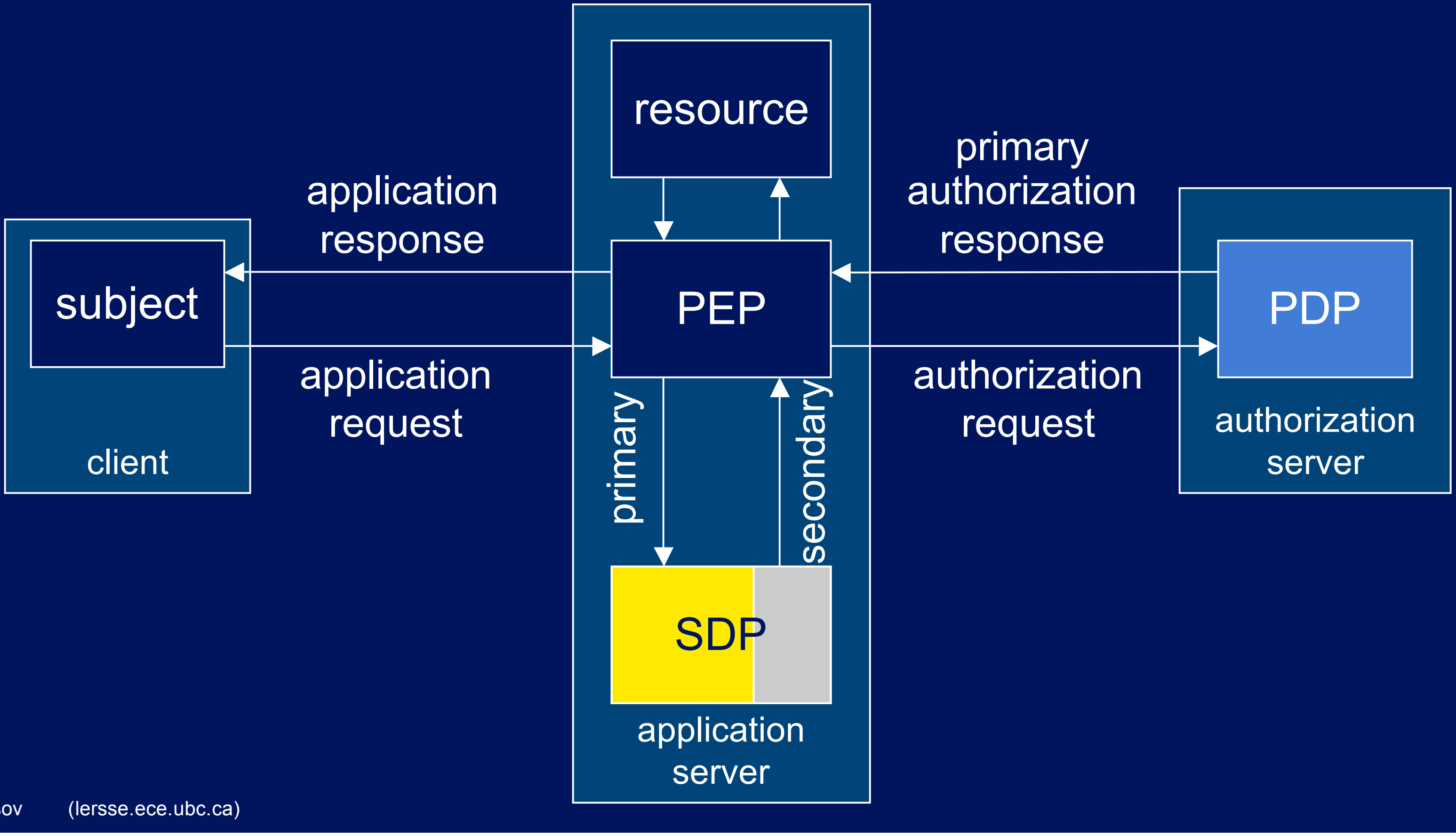
- (S_1, O_4, read)
- (S_4, O_1, write)
- (S_2, O_3, append)
- (S_3, O_4, read)

- (S_2, O_2, read)
- (S_1, O_3, write)
- (S_1, O_1, append)

Evaluation of SAAM$_{BLP}$

Availability

- How does the system availability depend on the SDP cache warmness?
- $A_A(A_{PDP}+A_{SDP}(w)-A_{PDP}*A_{SDP}(w))$

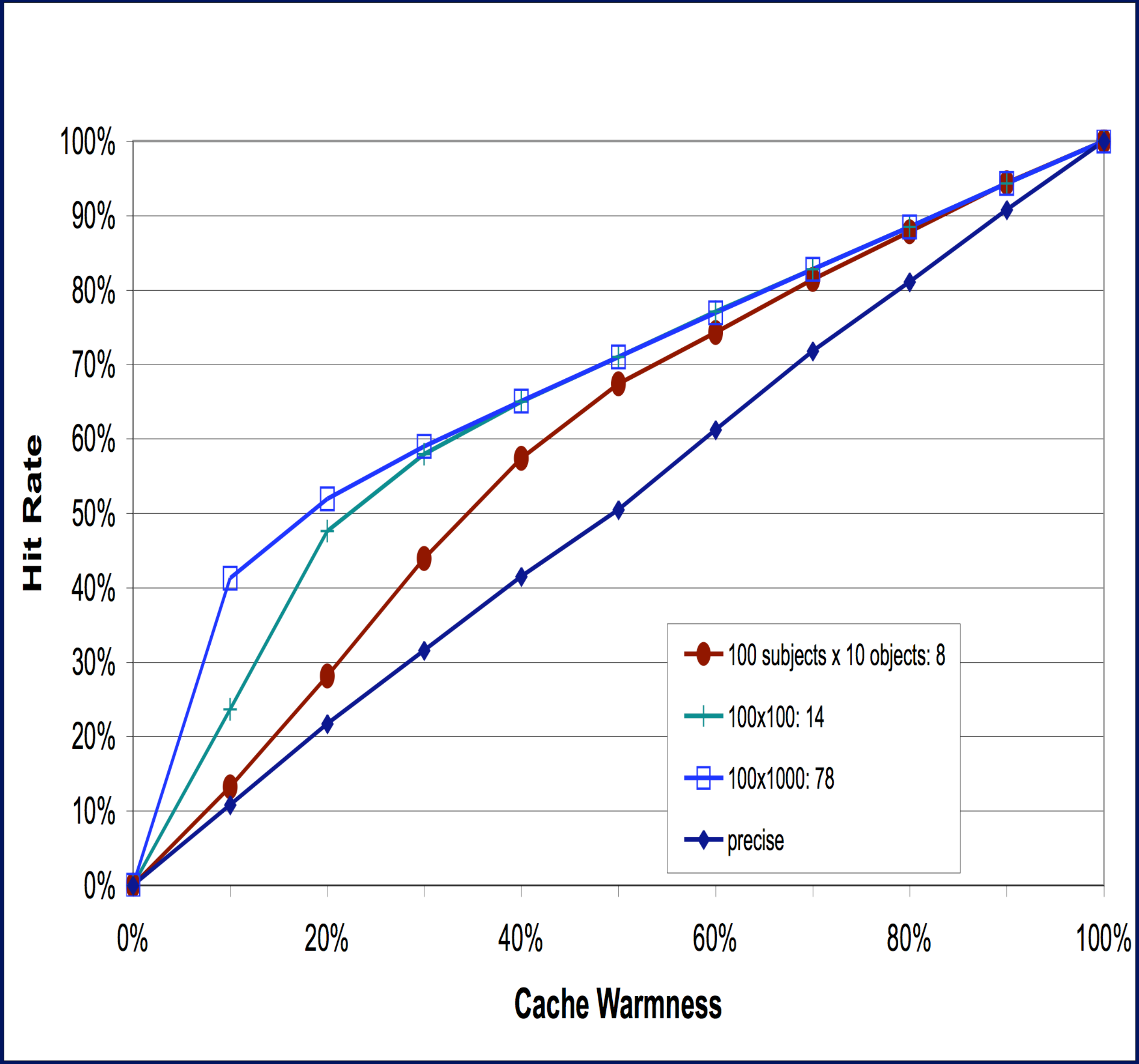


Methodology

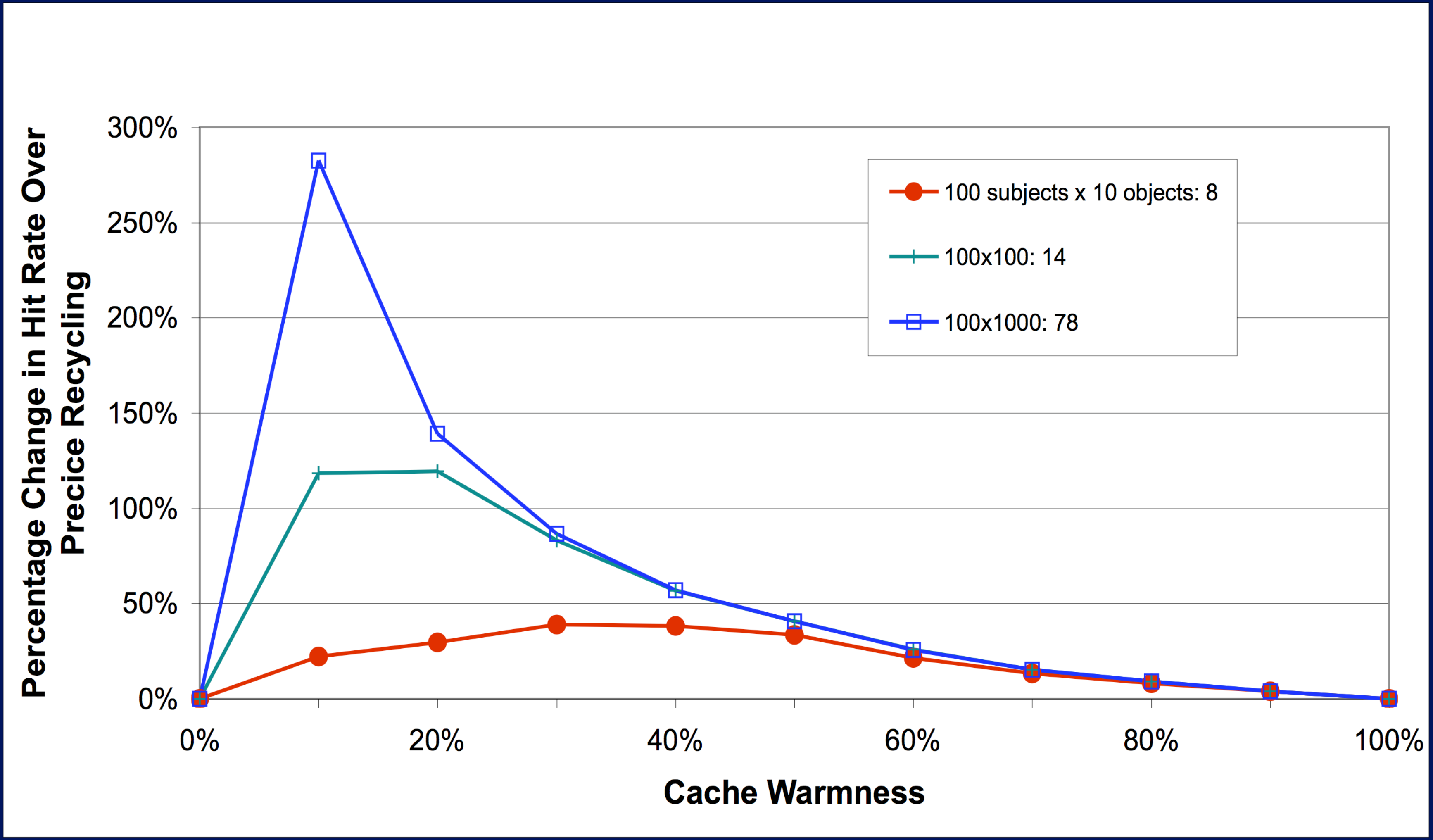
- Warming set $W \equiv S \times O \times A$
- Test set $|T| = 3\ |W|$
- Experiment
  1. warm SDP with W
  2. freeze DG
  3. measure hit rate with T

Preliminary Results

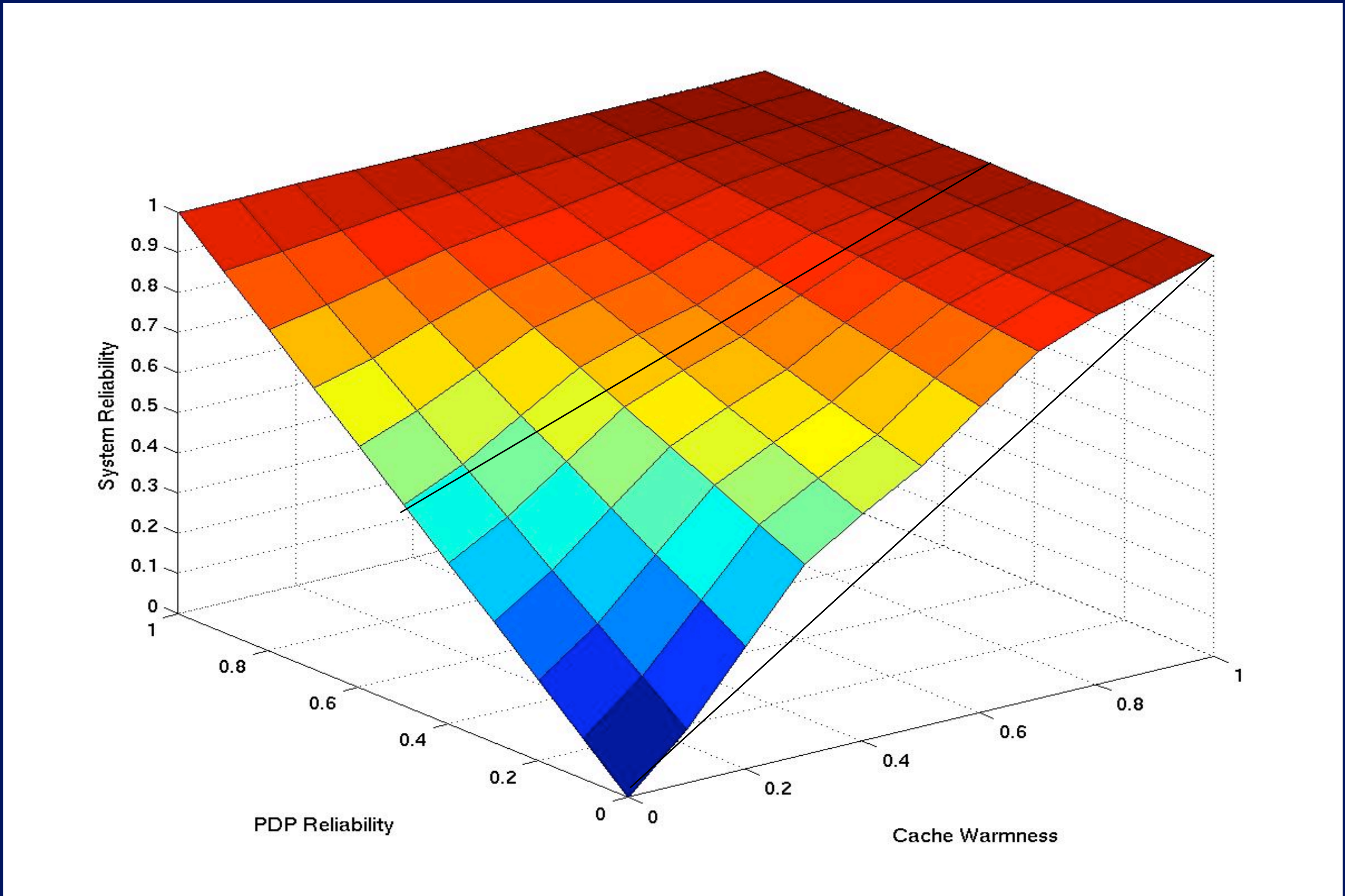
14-node lattice



percentage change over precise recycling

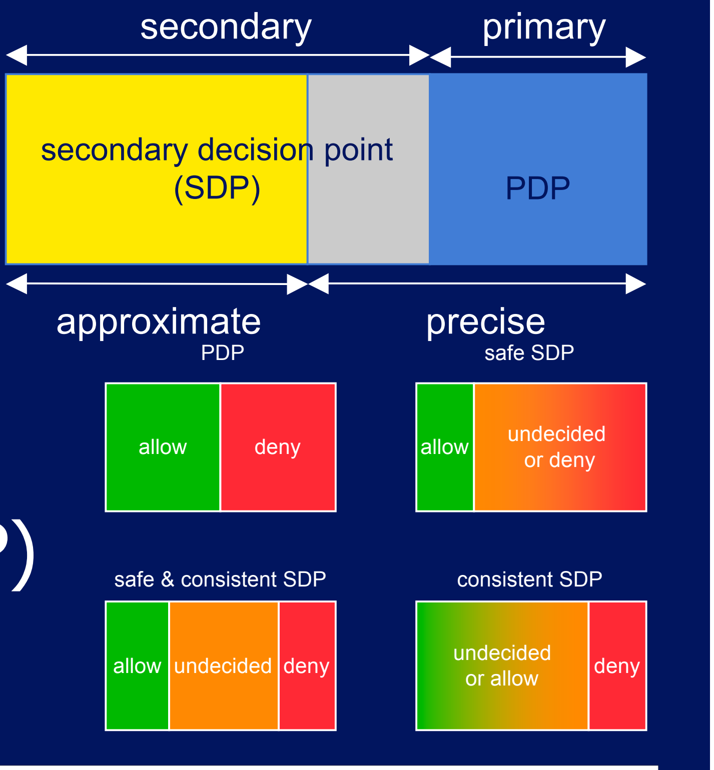


Availability: $A_A(A_{PDP}+A_{SDP}-A_{PDP}*A_{SDP})$



summary

- Secondary and approximate authorization model (SAAM)
  - authorization space
    - secondary vs. primary
    - approximate vs. precise
  - secondary decision point (SDP)
    - safe and/or consistent
- SAAM_{BLP}



secondary

primary

secondary decision point (SDP)

PDP

approximate

PDP

allow | deny

precise

safe SDP

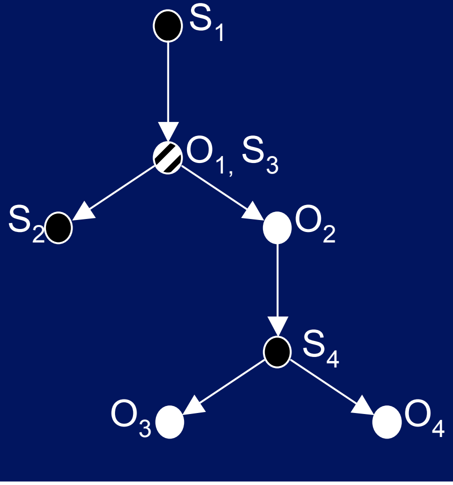
allow | undecided or deny

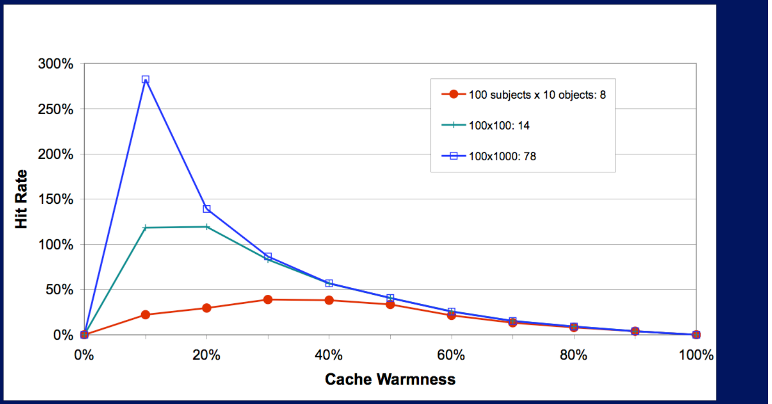
safe & consistent SDP

allow | undecided | deny

consistent SDP

undecided or allow | deny

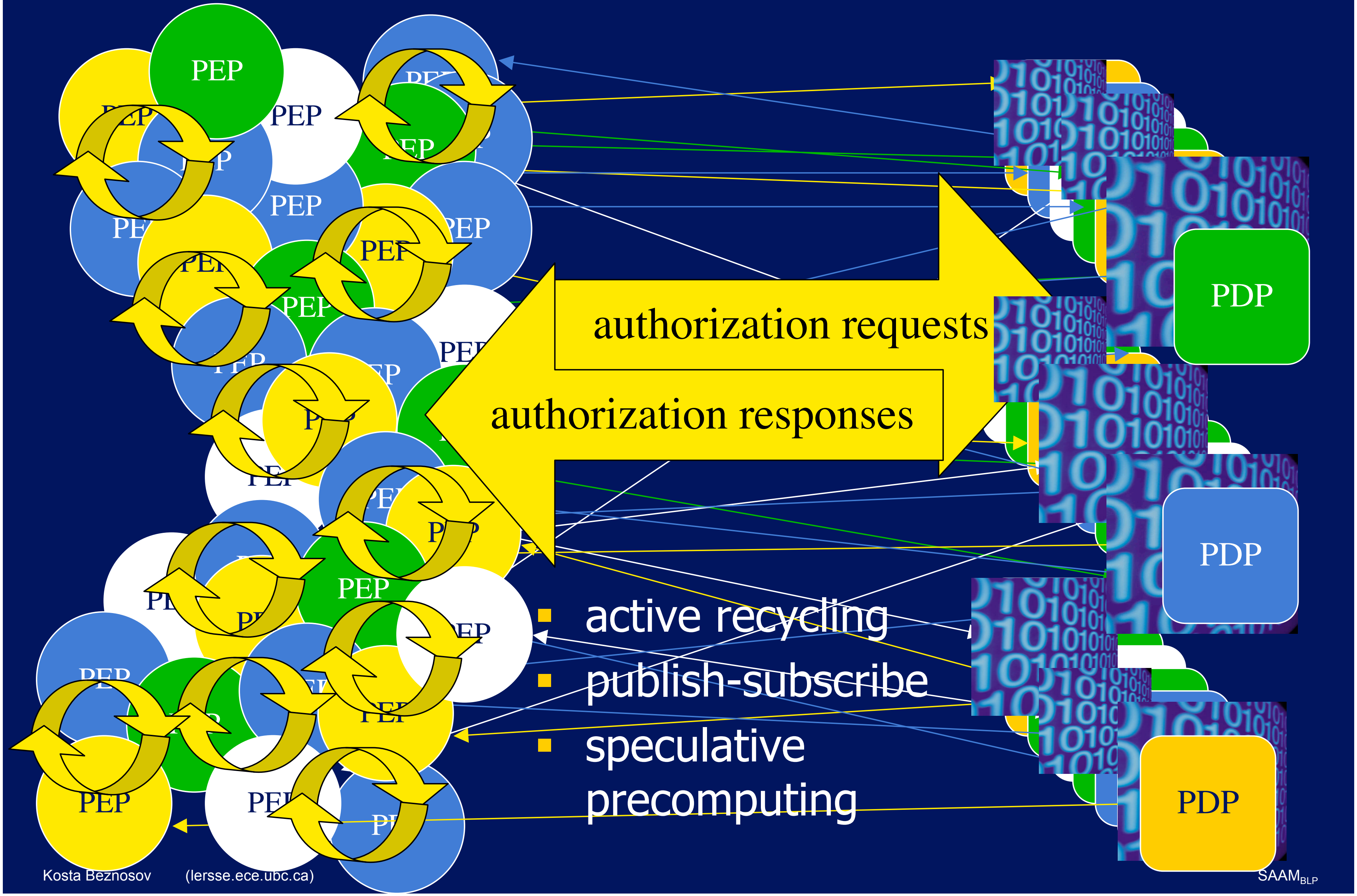




current status

- current work
  - SAAM
    - SAAM_{BLP}, $\text{SAAM}_{\text{RBAC}}$, …
  - authorization sharing across SDPs

future work



authorization requests

authorization responses

PEP

PDP

PDP

PDP

- active recycling
- publish-subscribe
- speculative precomputing

project team

- Information Security Group, Royal Holloway, University of London
  - Jason Crampton
- LERSSE, UBC
  - Kosta Beznosov
  - Wing Leung
  - Kyle Zeeuwen

Other Projects at LERSSE

- HOT Admin -- brining usability to security administration (NSERC, SAP, Entrust)
- CITI failures analysis
  - joint infrastructure interdependencies research program (JIIRP) (NSERC, PCEPCI)
- policy-based access management framework for IP-based multimedia services (TELUS)