THE UNIVERSITY OF BRITISH COLUMBIA

Employing Secondary and Approximate Authorizations to Improve Access Control Systems

Konstantin (Kosta) Beznosov

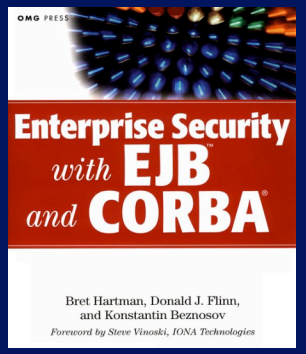
Laboratory for Education and Research in Secure Systems Engineering

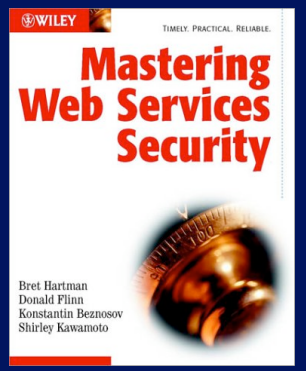
lersse.ece.ubc.ca

Department of Electrical and Computer Engineering

Who's Konstantin Beznosov

- Education
  - M.S. (1997) & Ph.D. (2000) in CS, Florida International University
  - B.S. in Physics (1993), Novosibirsk State University
- Experience
  - Assistant Prof., Electr. and Comp. Egn., UBC (2003-present)
  - founded and directs
    Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
  - US industry (1997-2003): end-user, consulting,
    and software vendor organizations
- Contributed to
  - OMG
    - CORBA Security revisions
    - Resource Access Decision
    - Security Domain Membership Management
  - OASIS
    - eXtensible Access Control Markup Language (XACML) v1.0





secondary and approximate authorizations

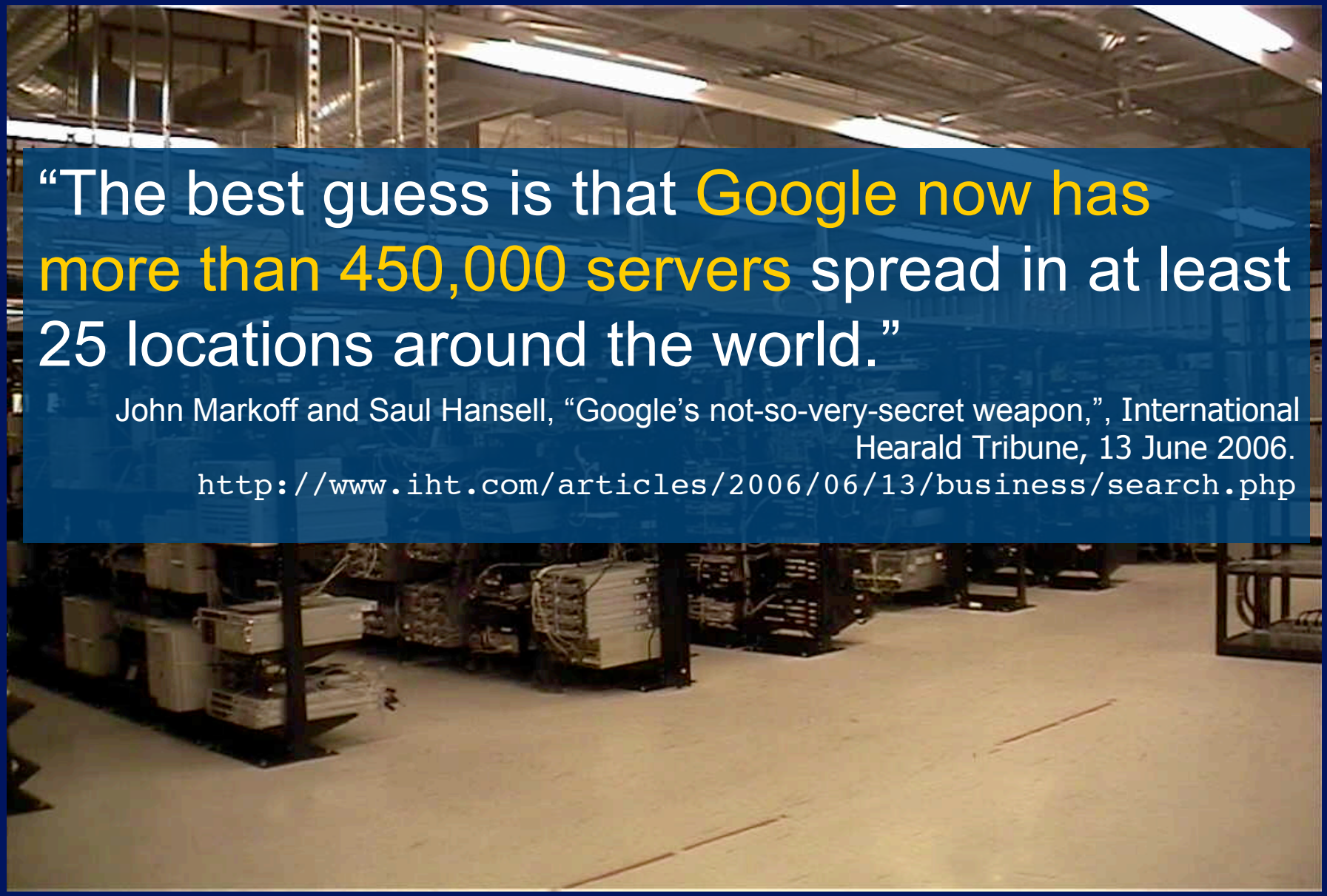
THE UNIVERSITY OF BRITISH COLUMBIA

the problem

departing assumptions

- processor resources virtually free
- commodity computing most cost-effective
- network bandwidth virtually unlimited
- human time/attention expensive

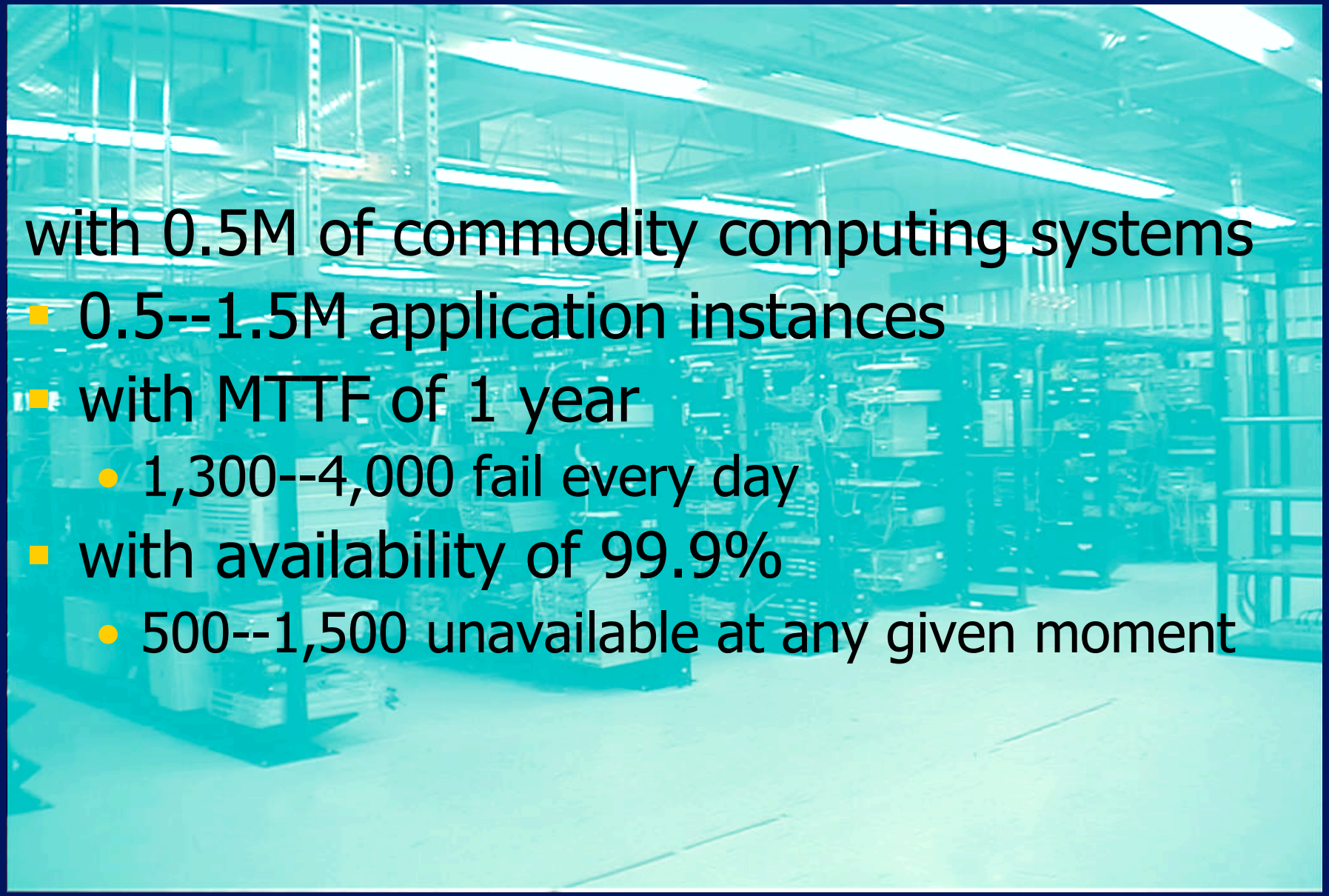
target environments



"The best guess is that Google now has more than 450,000 servers spread in at least 25 locations around the world."

John Markoff and Saul Hansell, "Google's not-so-very-secret weapon,", International Hearald Tribune, 13 June 2006.
http://www.iht.com/articles/2006/06/13/business/search.php

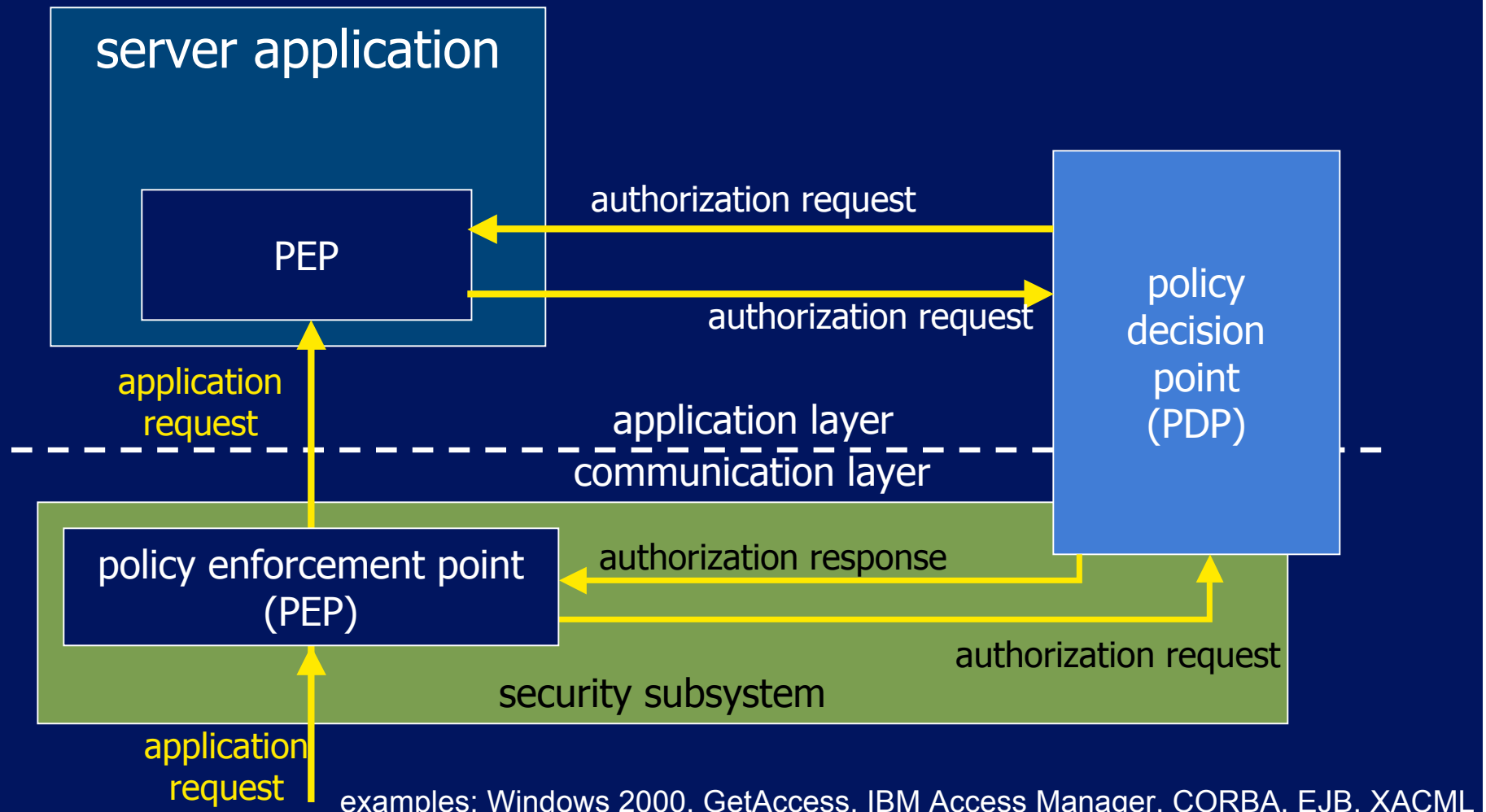
target environments



with 0.5M of commodity computing systems

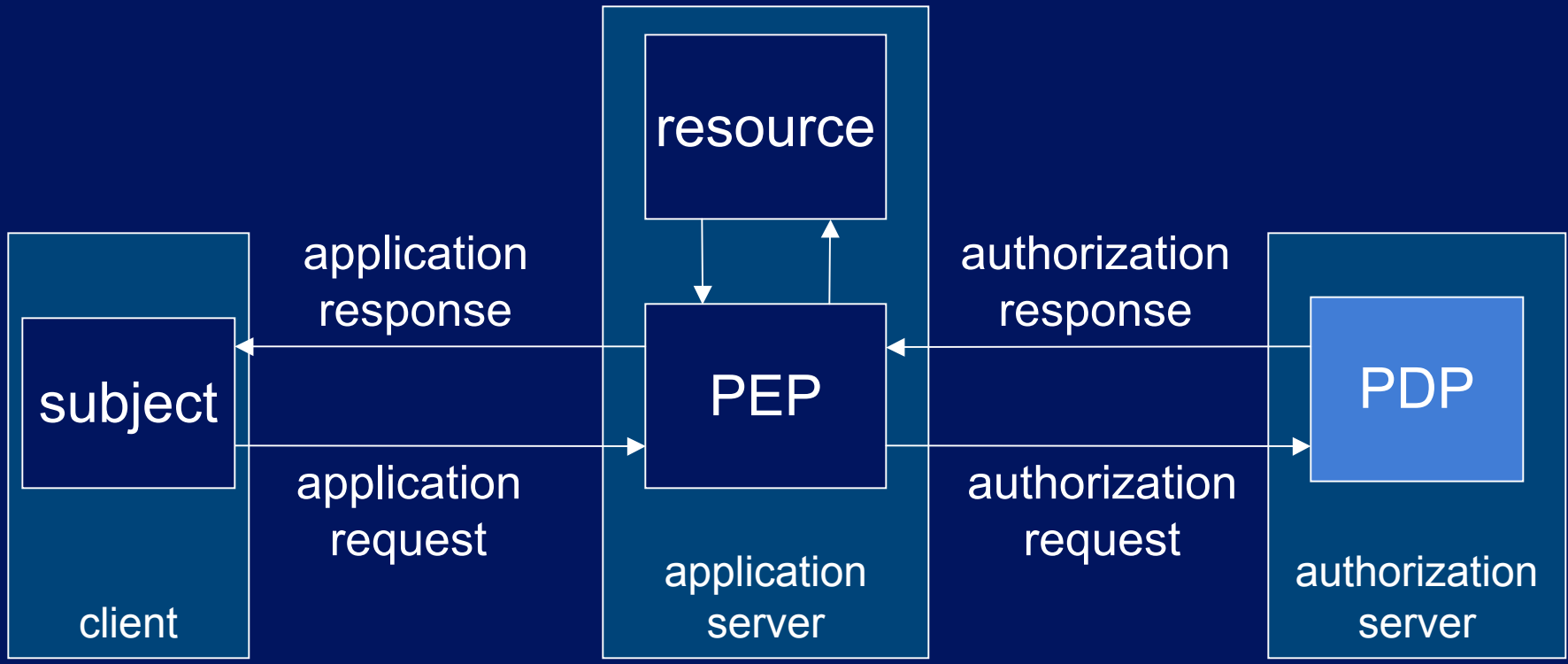
- 0.5--1.5M application instances
- with MTTF of 1 year
  - 1,300--4,000 fail every day
- with availability of 99.9%
  - 500--1,500 unavailable at any given moment

how enterprise authorization systems work

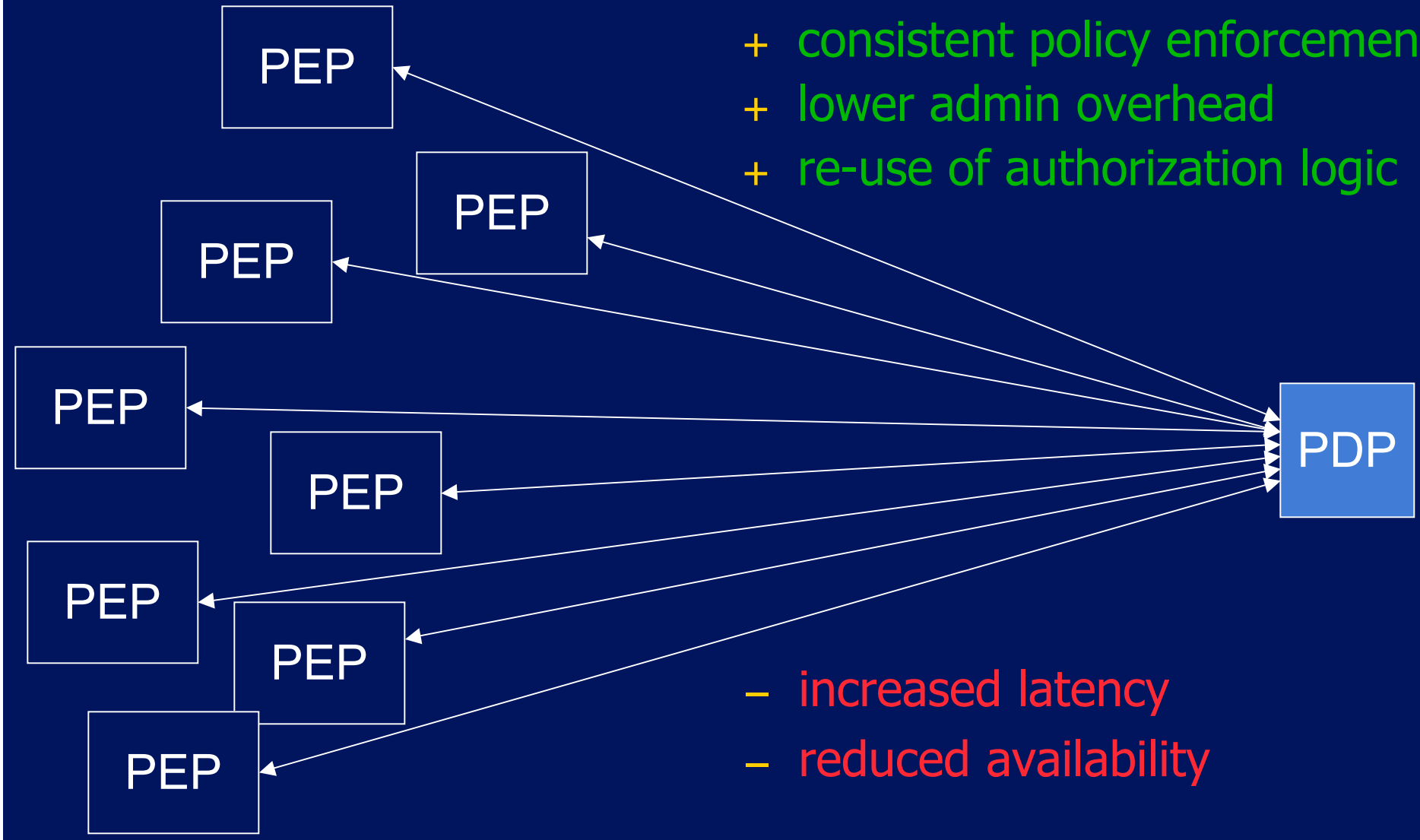


examples: Windows 2000, GetAccess, IBM Access Manager, CORBA, EJB, XACML

request-response paradigm



PEP-PDP decoupling: pros and cons



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

– increased latency
– reduced availability

problem summary

point-to-point authorization architectures at massive scale

- become too fragile
  - require costly human attention
  - jeopardize organizational goals
- fail to reduce latency
  - security-related performance overhead is high

existing remedies

- caching -- “precise recycling”
  - + improves performance & availability
  - + simple, inexpensive
  - – serves only returning requests
- fault-tolerance solutions
  - + improve availability
  - – require specialized specialized OS/middleware
  - – poorly scale on large populations

outline

- junk authorizations for massive-scale enterprise services (JAMES)
- active recycling of authorizations
  - SAAM
    - $SAAM_{BLP}$
  - CSAR
- overview of other projects

THE UNIVERSITY OF BRITISH COLUMBIA

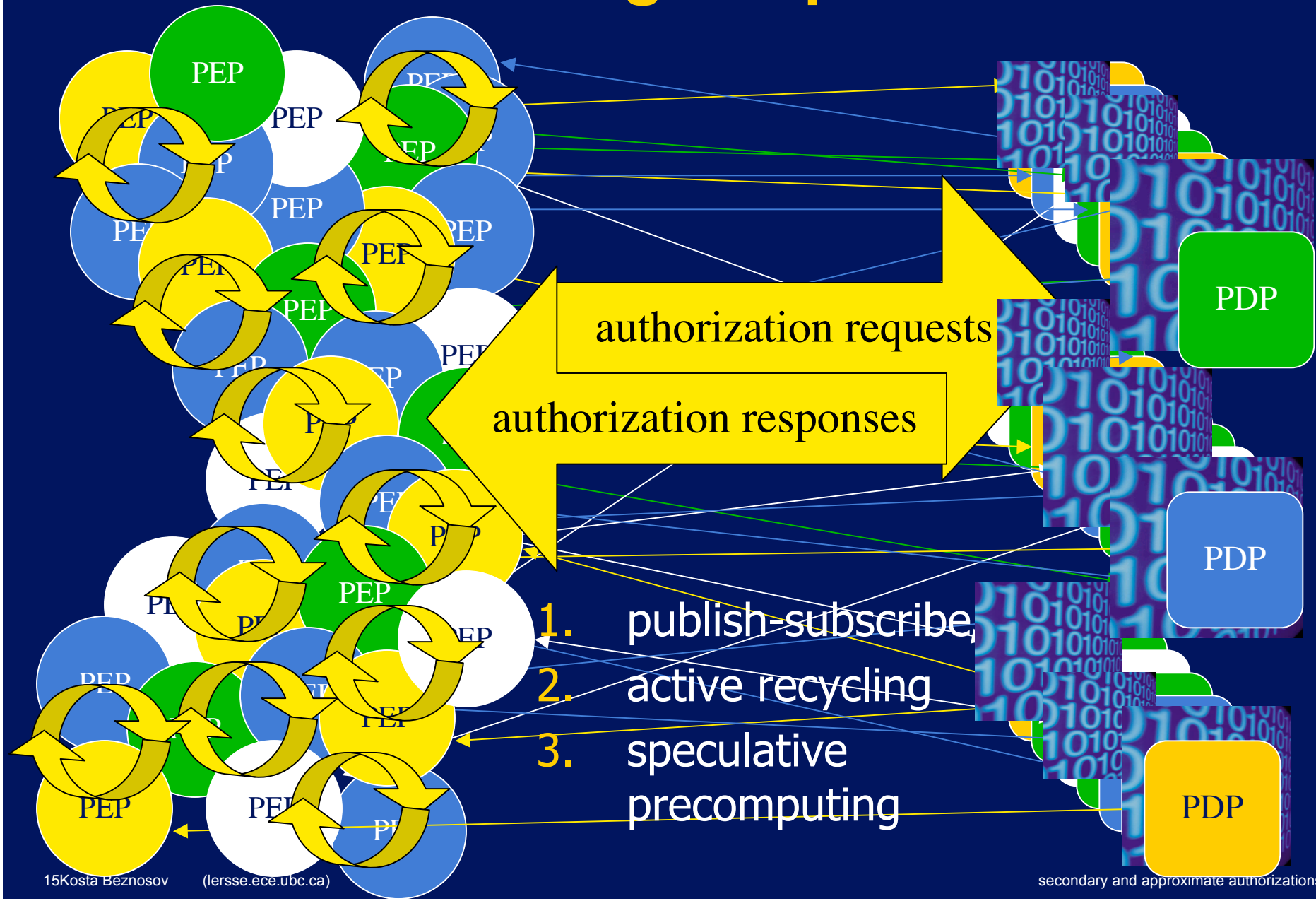
a solution

THE UNIVERSITY OF BRITISH COLUMBIA

approach:
junk authorizations for
massive-scale enterprise services

(JAMES)

addressing the problem



THE UNIVERSITY OF BRITISH COLUMBIA

active recycling of authorizations

technical contributions on recycling

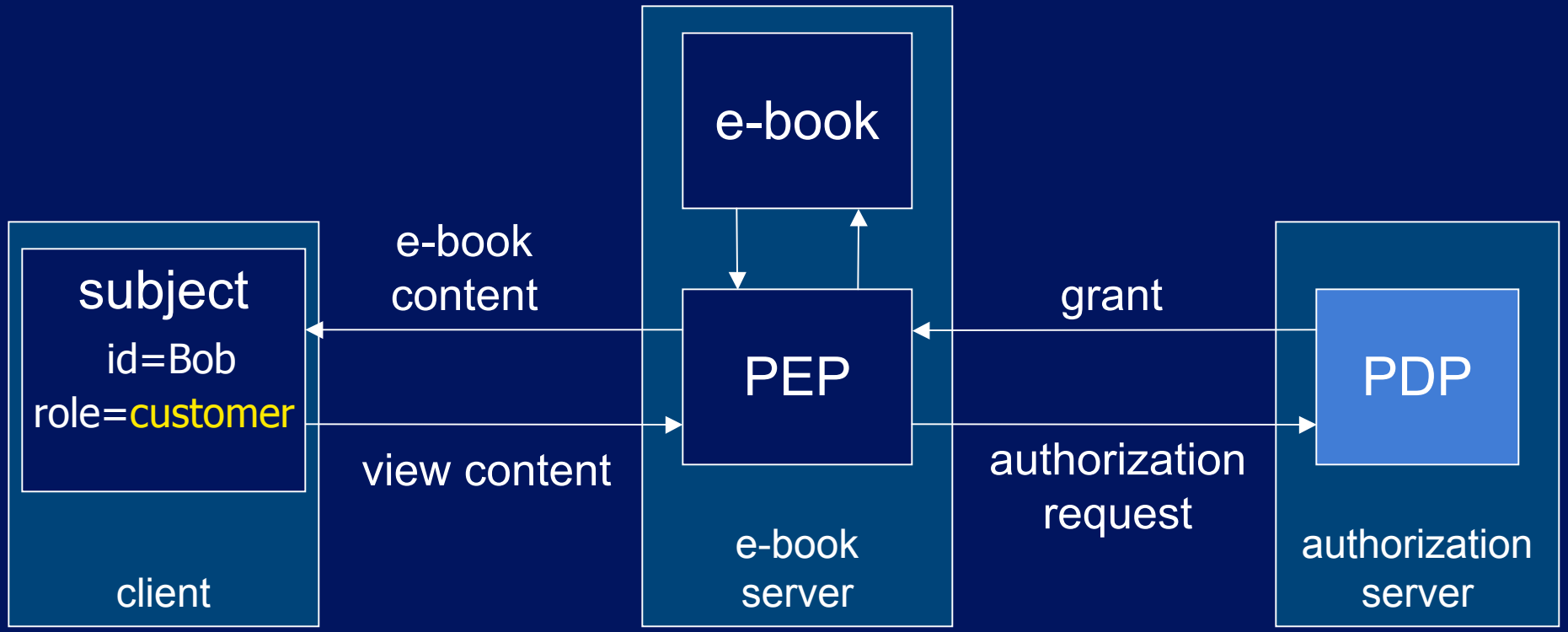
1. secondary and approximate authorizations model (SAAM)
   - concept and model for inferring new authorizations from previous
2. BLP-specific SAAM algorithms ($SAAM_{BLP}$)
3. architecture for cooperative secondary authorizations recycling (CSAR)

THE UNIVERSITY OF BRITISH COLUMBIA

secondary and approximate authorization model

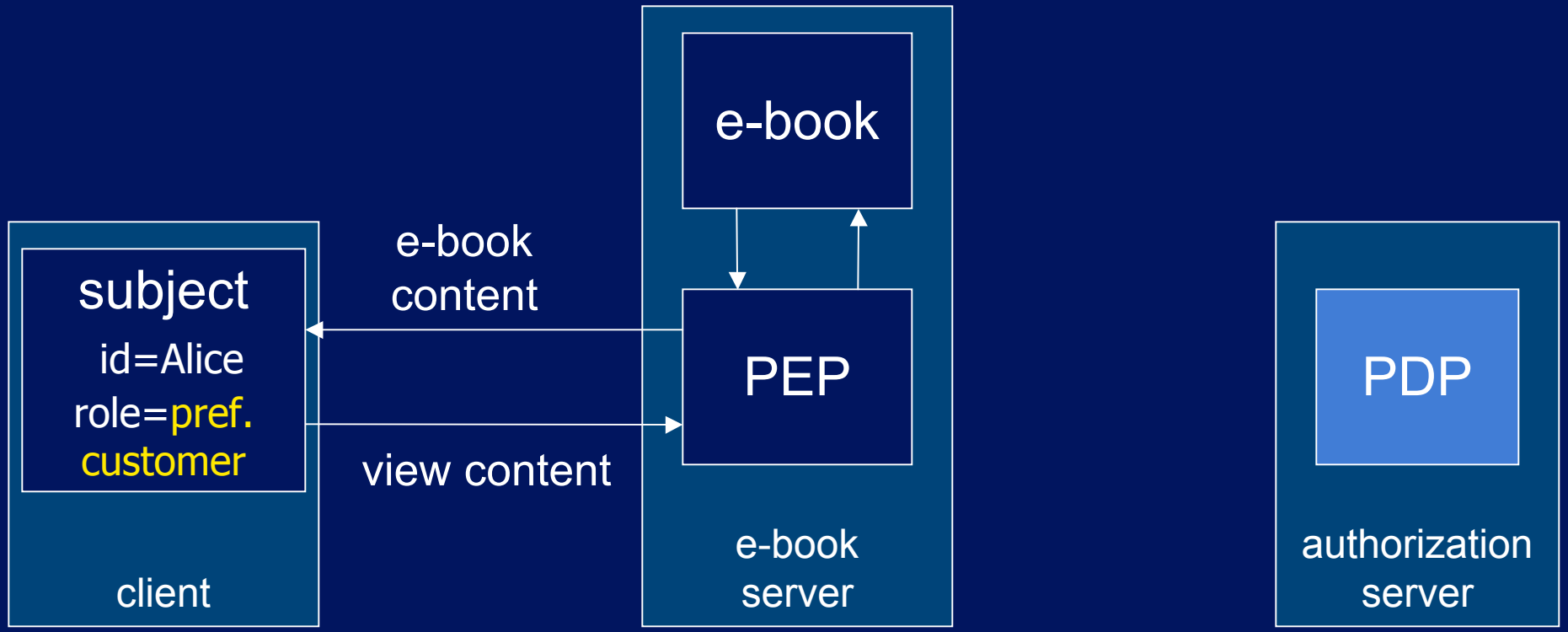
(SAAM)

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

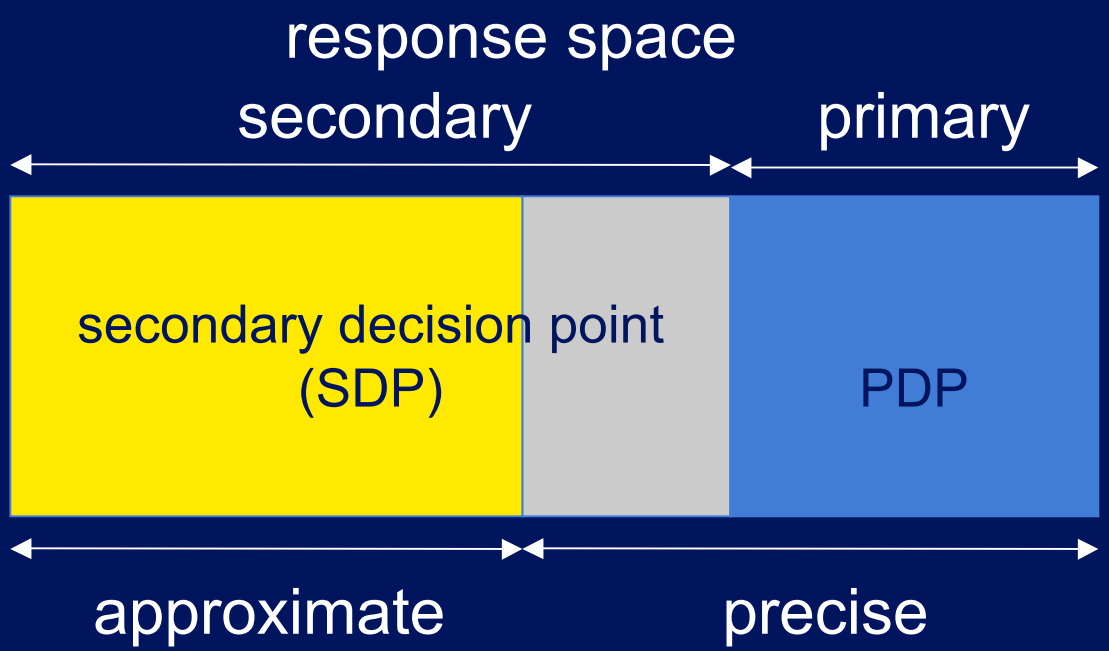
<{id="Bob", role="customer"}, {id="eB-23"}, view, {date="05-08-15"}, 11>

equivalent

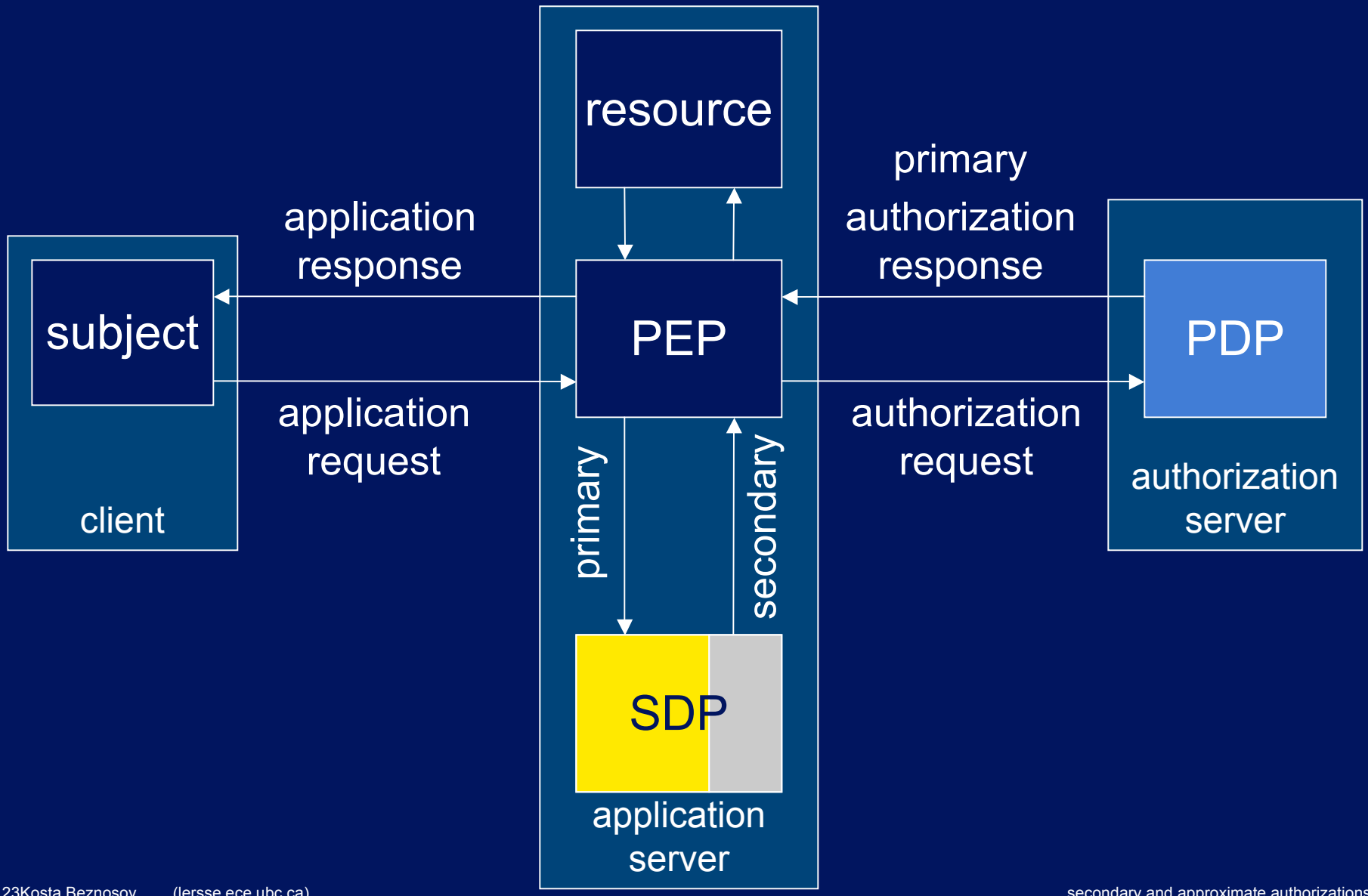
< 2, 11, [1], allow > -- precise response

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

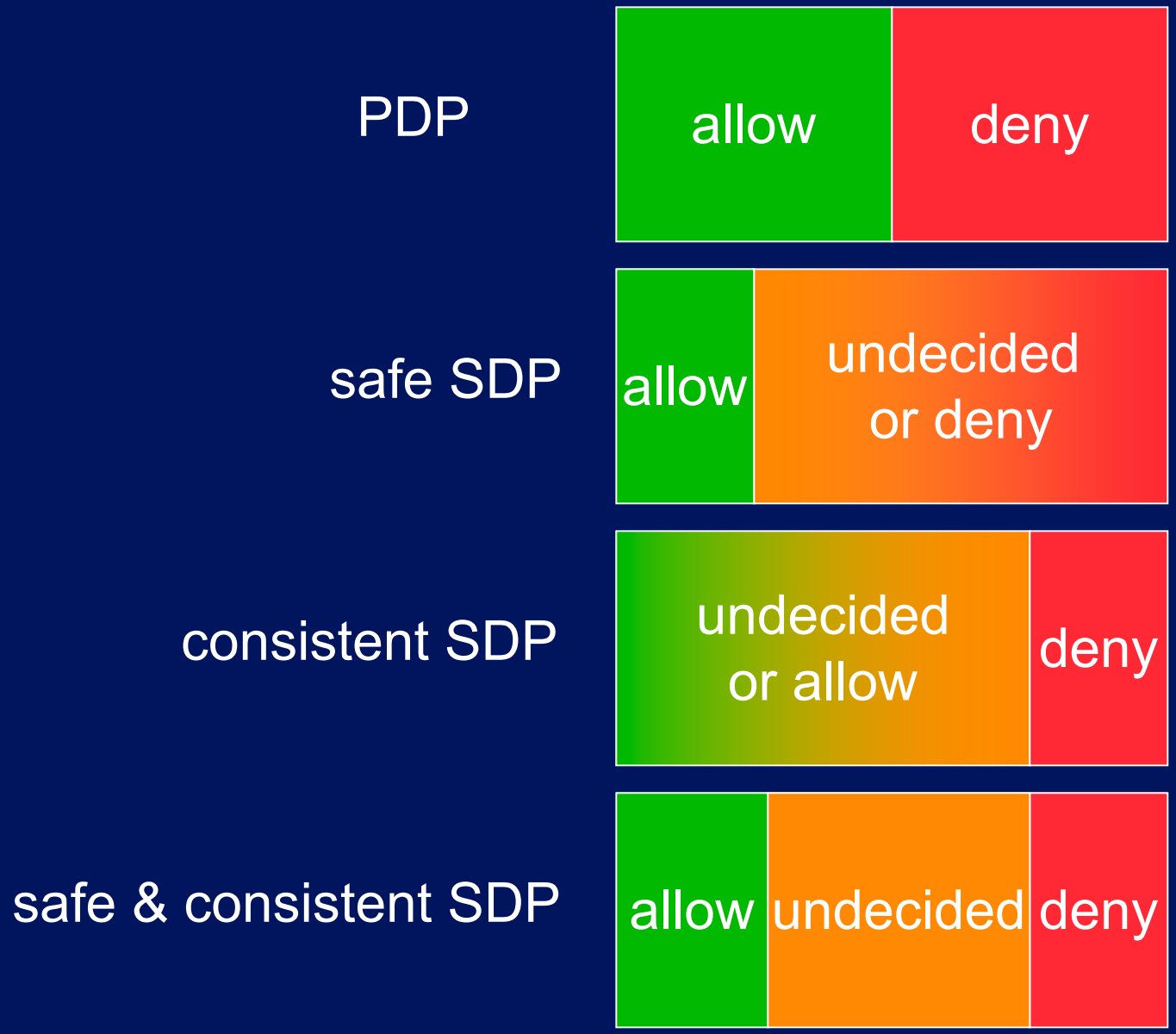
< 3, 12, [1], allow > -- secondary and approximate response



use of secondary decision point

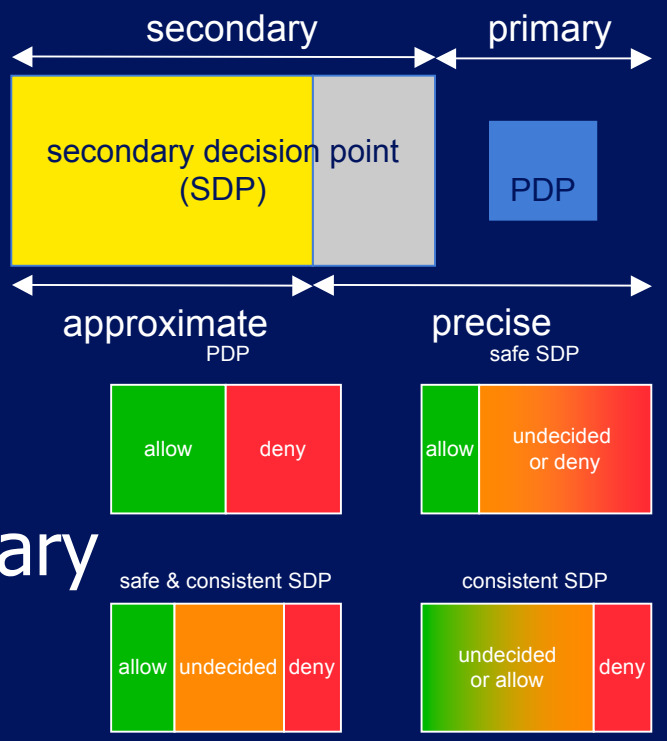


SDP types


PDP
allow
deny
safe SDP
allow
undecided
or deny
consistent SDP
undecided
or allow
deny
safe & consistent SDP
allow
undecided
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



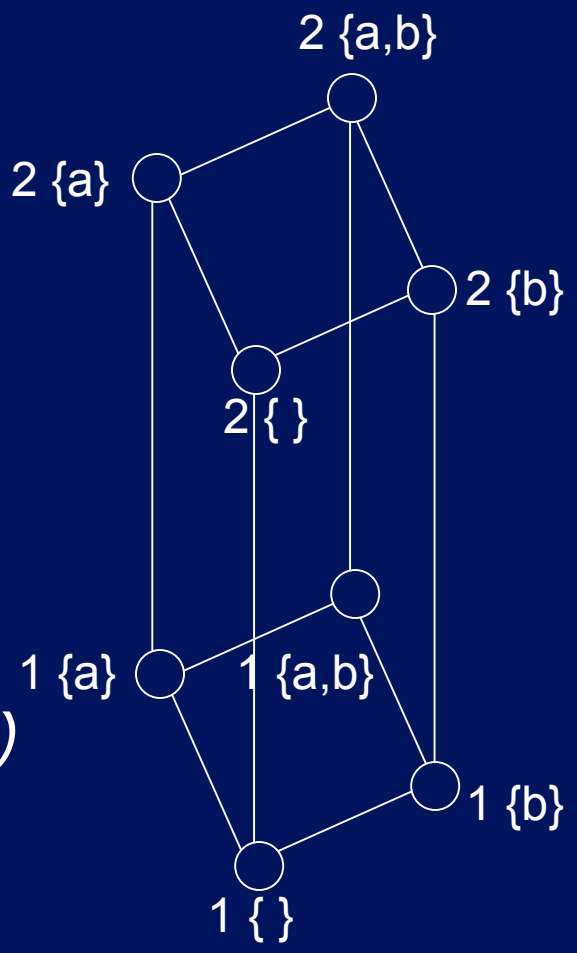
THE UNIVERSITY OF BRITISH COLUMBIA

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

BLP refresher

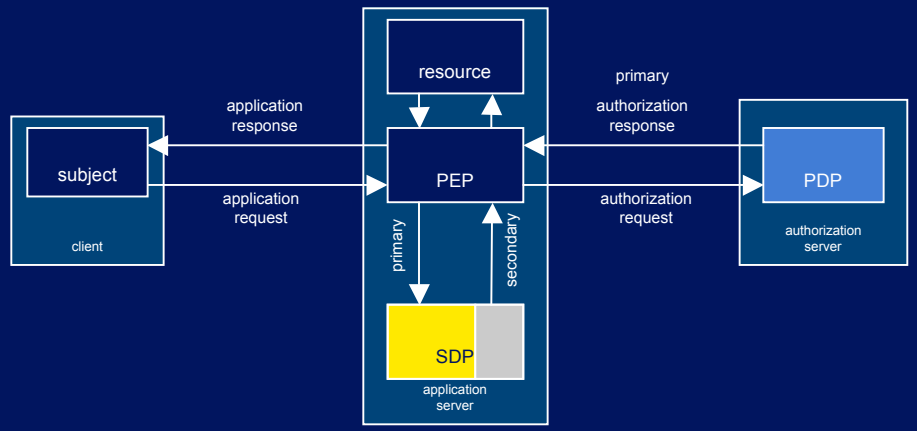
- S : subjects, O : objects
- DAC
- L: lattice of security labels
- λ: $S \cup O \rightarrow L$

- 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 $\Rightarrow \lambda(o) = \lambda(s)$

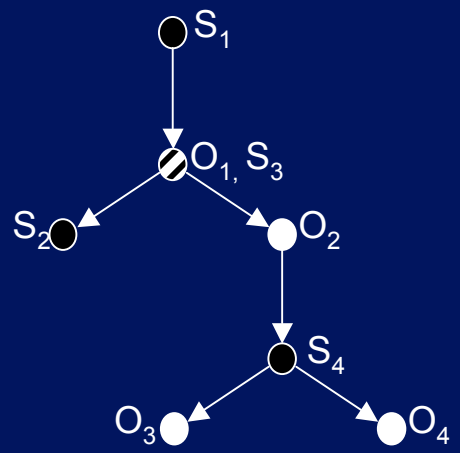


three scenarios

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 $SAAM_{BLP}$?

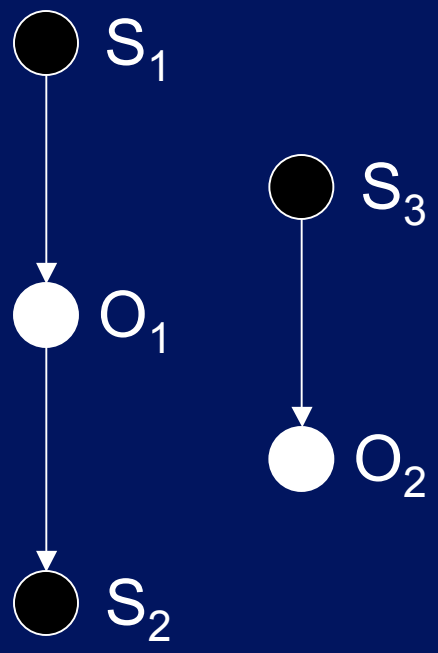


1. dominance graph (DG) -- ADG
2. algorithms for SDP to
   - modify DG based on (primary) authorizations
   - compute secondary authorizations using DG

Dominance Graph

allow

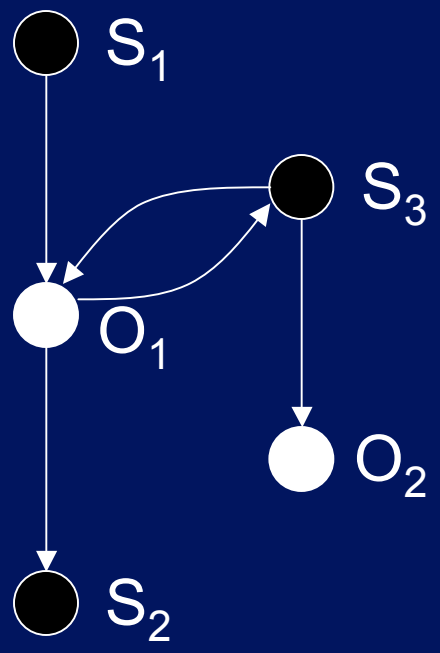
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)



Dominance Graph

allow

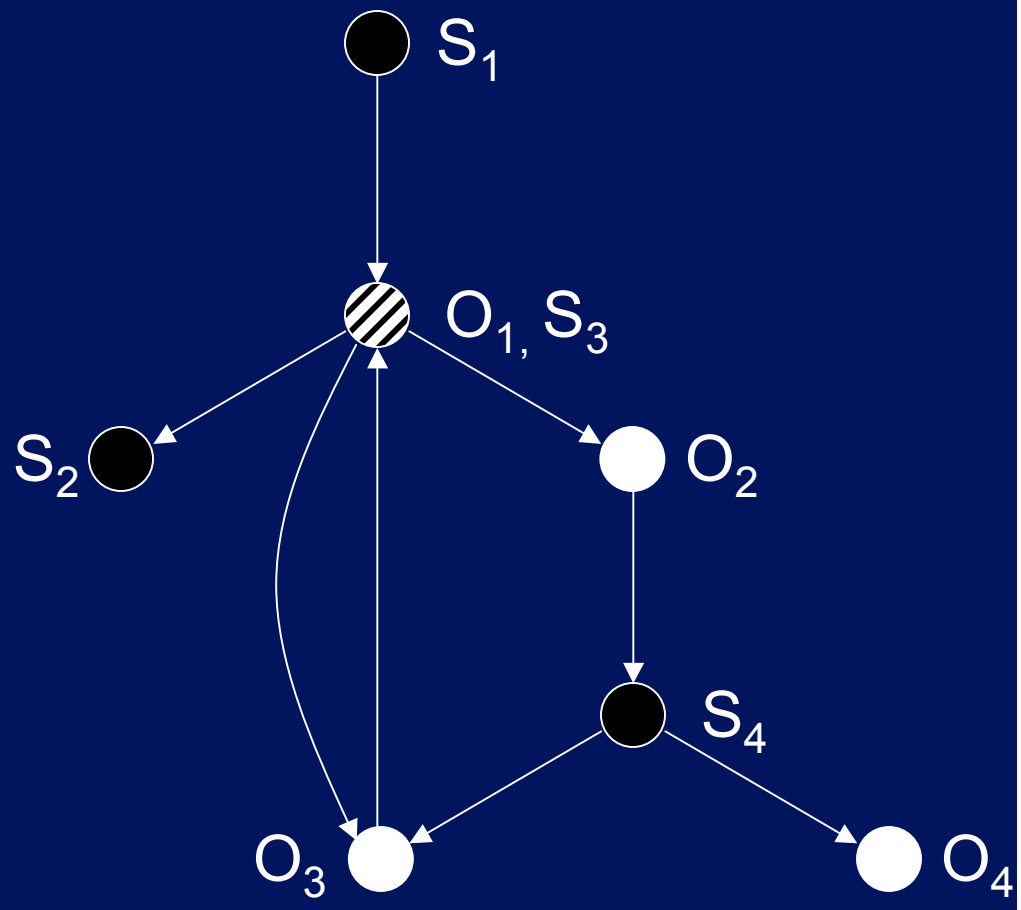
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)



Dominance Graph

allow

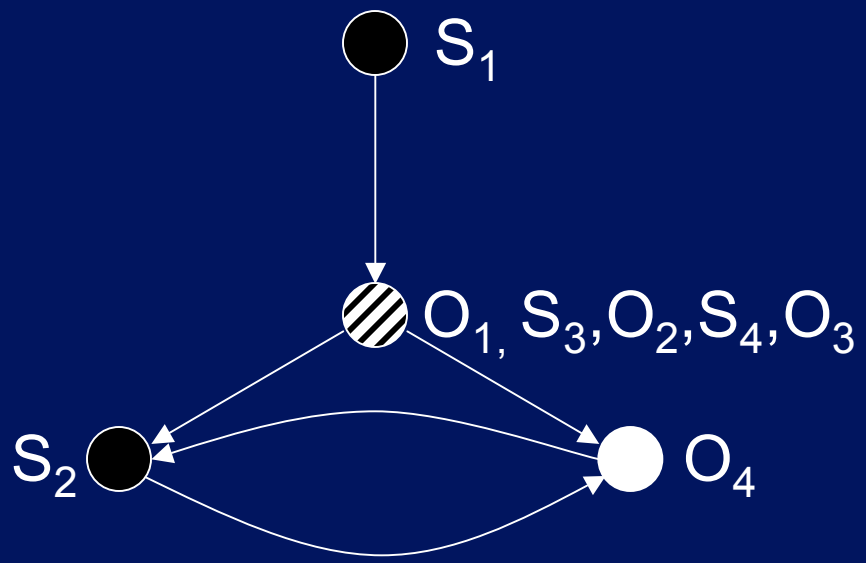
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)



Dominance Graph

allow

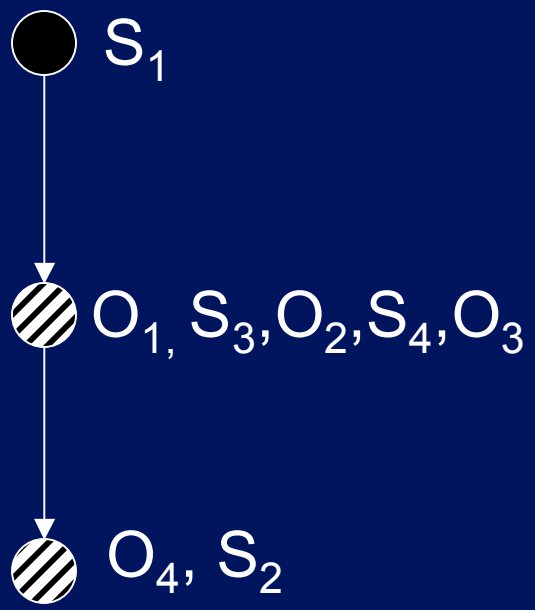
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)
10. (s_2, o_4, write)



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)



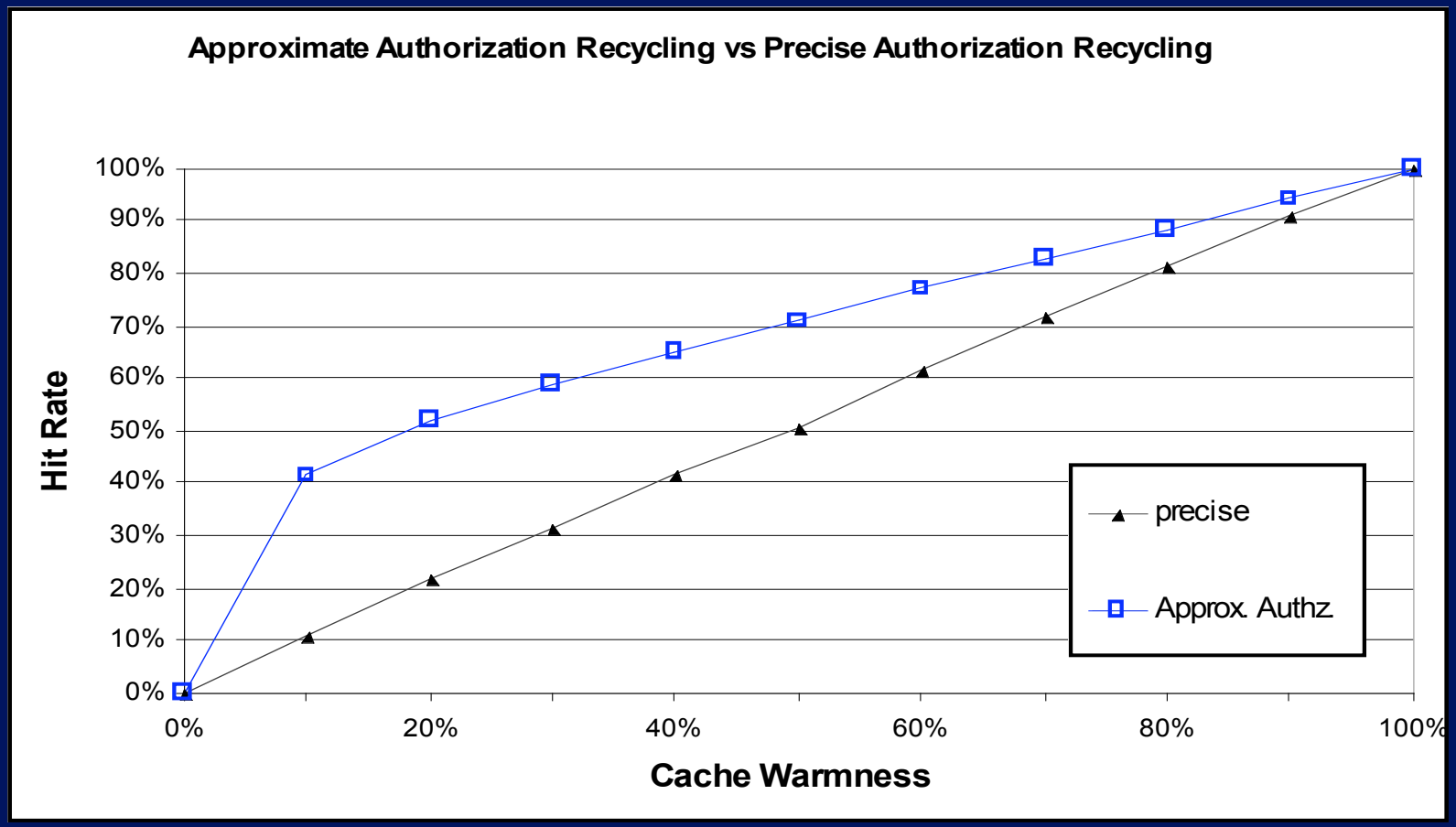
- (S_1, O_4, read)
- (S_4, O_1, write)
- (S_2, O_3, append)
- (S_3, O_4, read)

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

THE UNIVERSITY OF BRITISH COLUMBIA

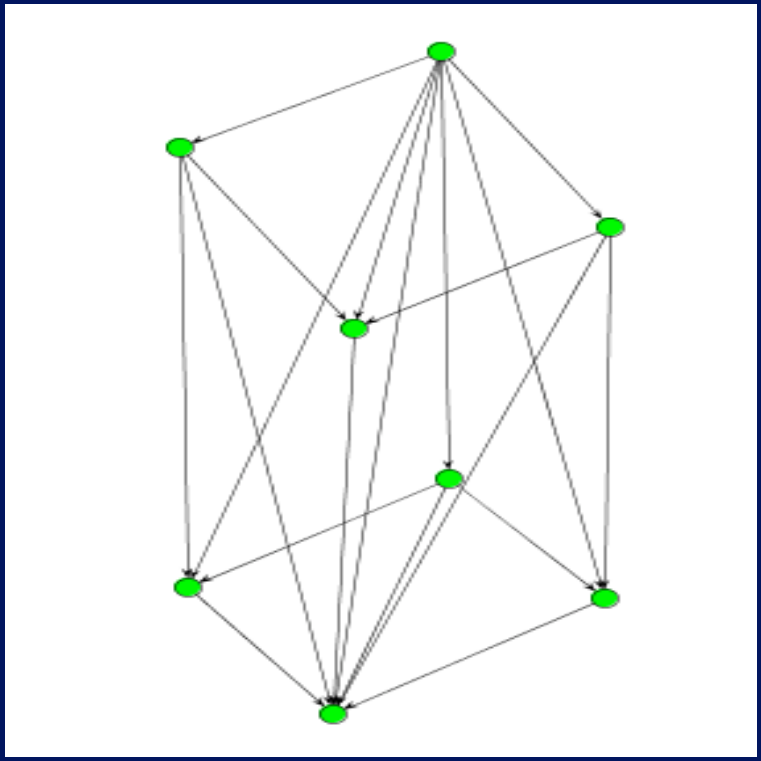
evaluation of $SAAM_{BLP}$

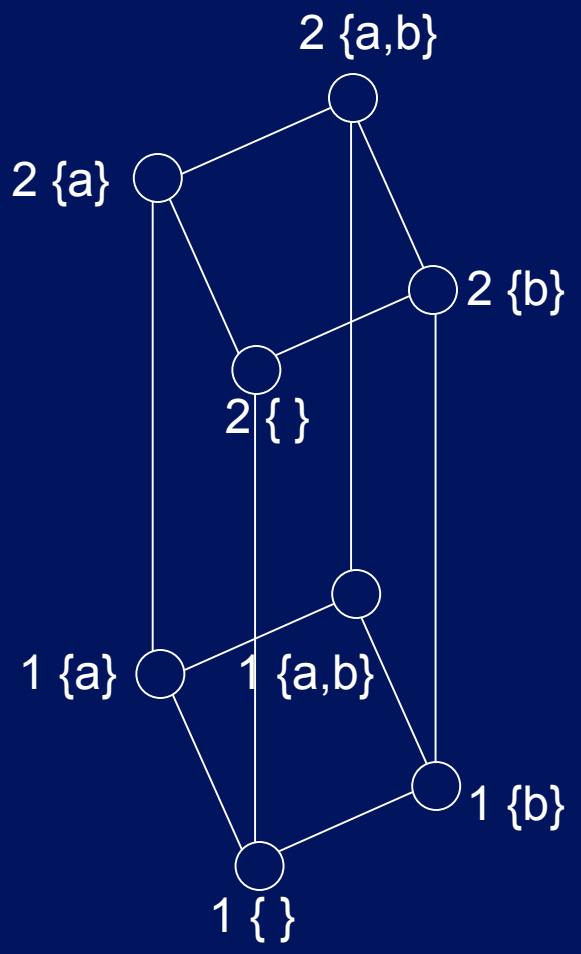
simulation results



100 subjects, 1000 objects, 14 labels security lattice

dominance graph and security lattice



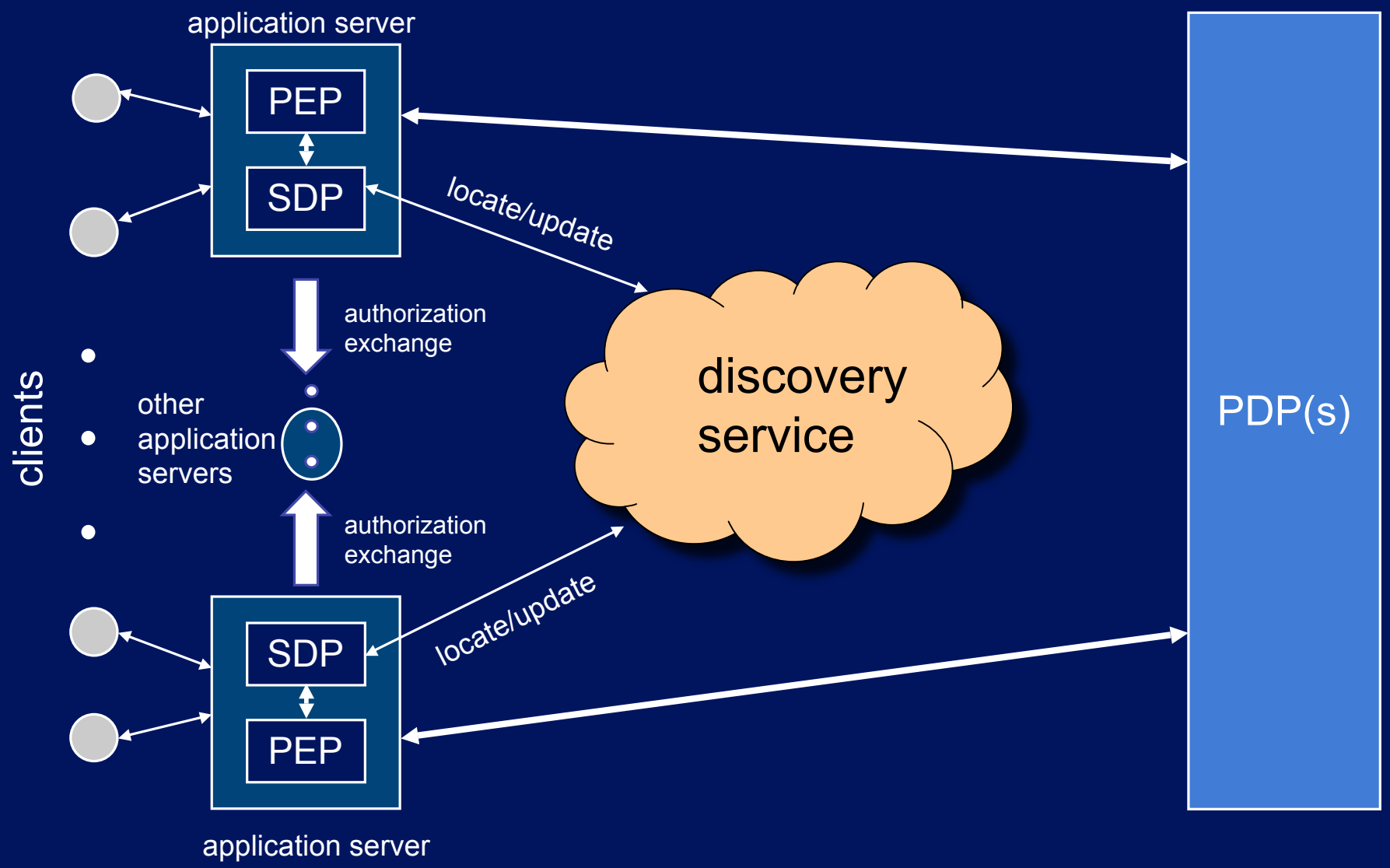


THE UNIVERSITY OF BRITISH COLUMBIA

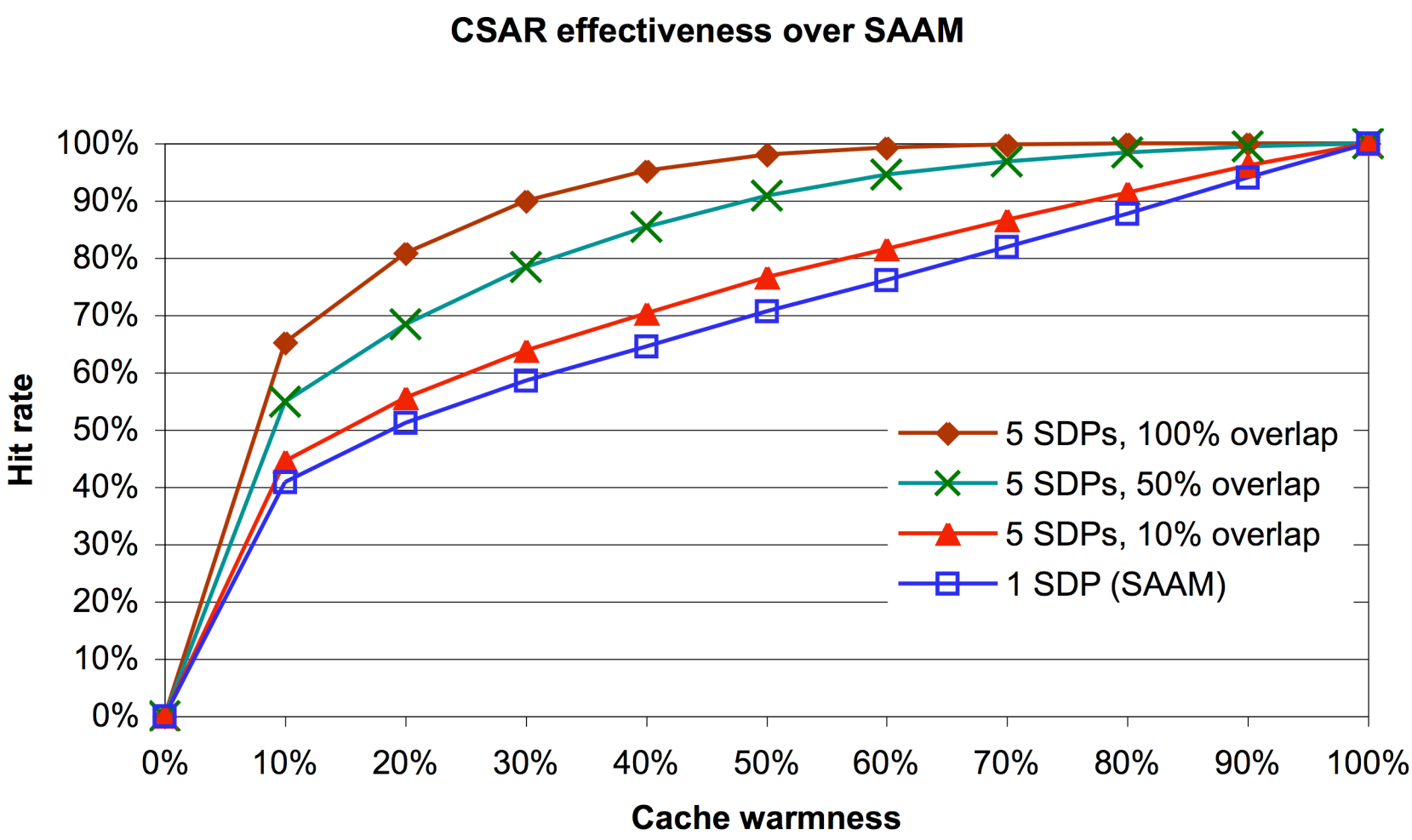
cooperative secondary authorization recycling

(CSAR)

CSAR architecture



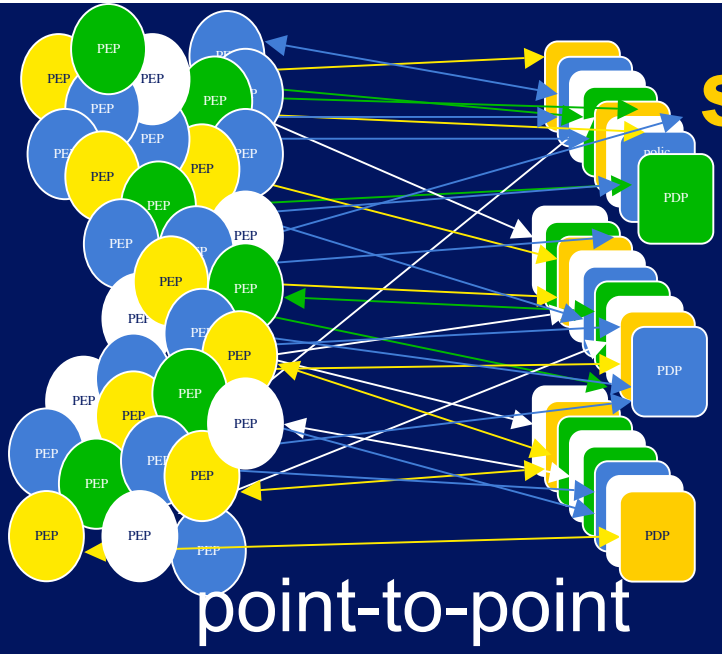
simulation results



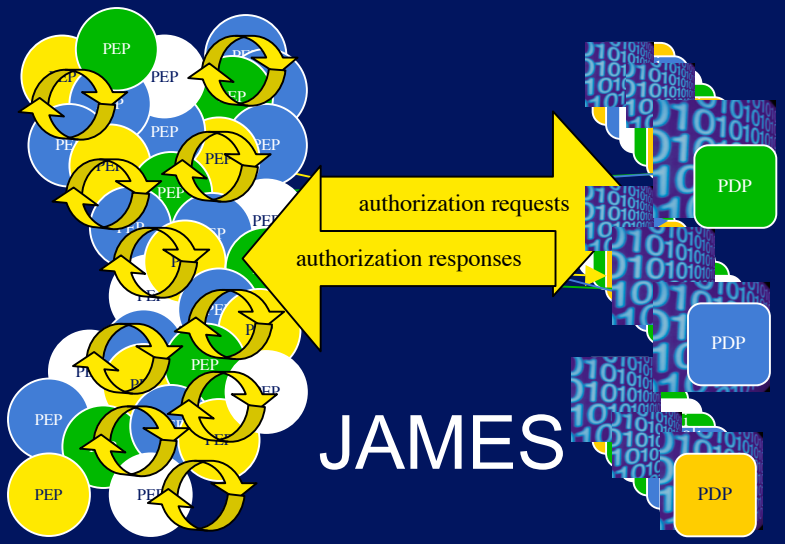
project team

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

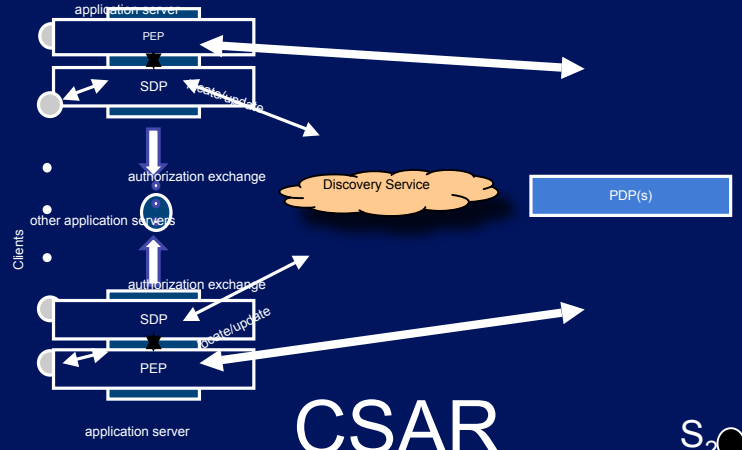
summary



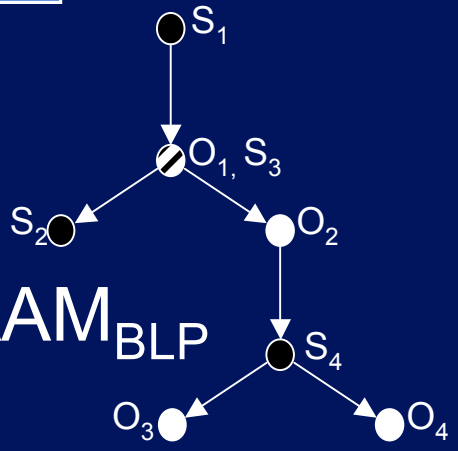
point-to-point



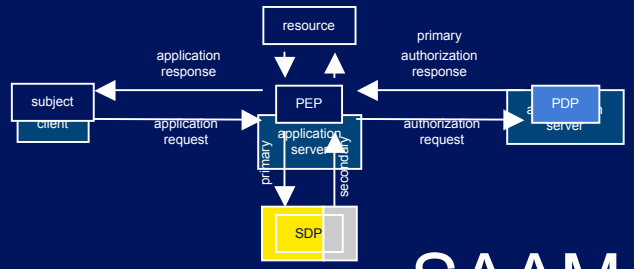
JAMES



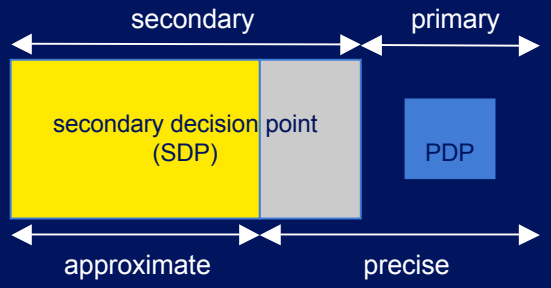
CSAR



$SAAM_{BLP}$



SAAM



related 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.
- J. Crampton, W. Leung, and K. Beznosov, "Secondary and Approximate Authorizations Model and its Application to Bell-LaPadula Policies," In *Proceedings of the Symposium on Access Control Models and Technologies (SACMAT)*, pp. 111-120, Lake Tahoe, California, USA, June 7-9 2006.
- Q. Wei, K. Beznosov, M. Ripeanu, "Cooperative Approximate Authorization Recycling," poster presented at the USENIX Security Symposium, Vancouver, Canada, August 1-3, 2006.

konstantin.beznosov.net