THE UNIVERSITY OF BRITISH COLUMBIA

JAMES: Junk Authorizations for Massive-scale Enterprise Services

Konstantin (Kosta) Beznosov

Laboratory for Education and Research in Secure Systems Engineering

lersse.ece.ubc.ca

outline

- the problem
  - context
  - target environment
  - limitations of point-to-point architectures
- the approach
- summary & future work

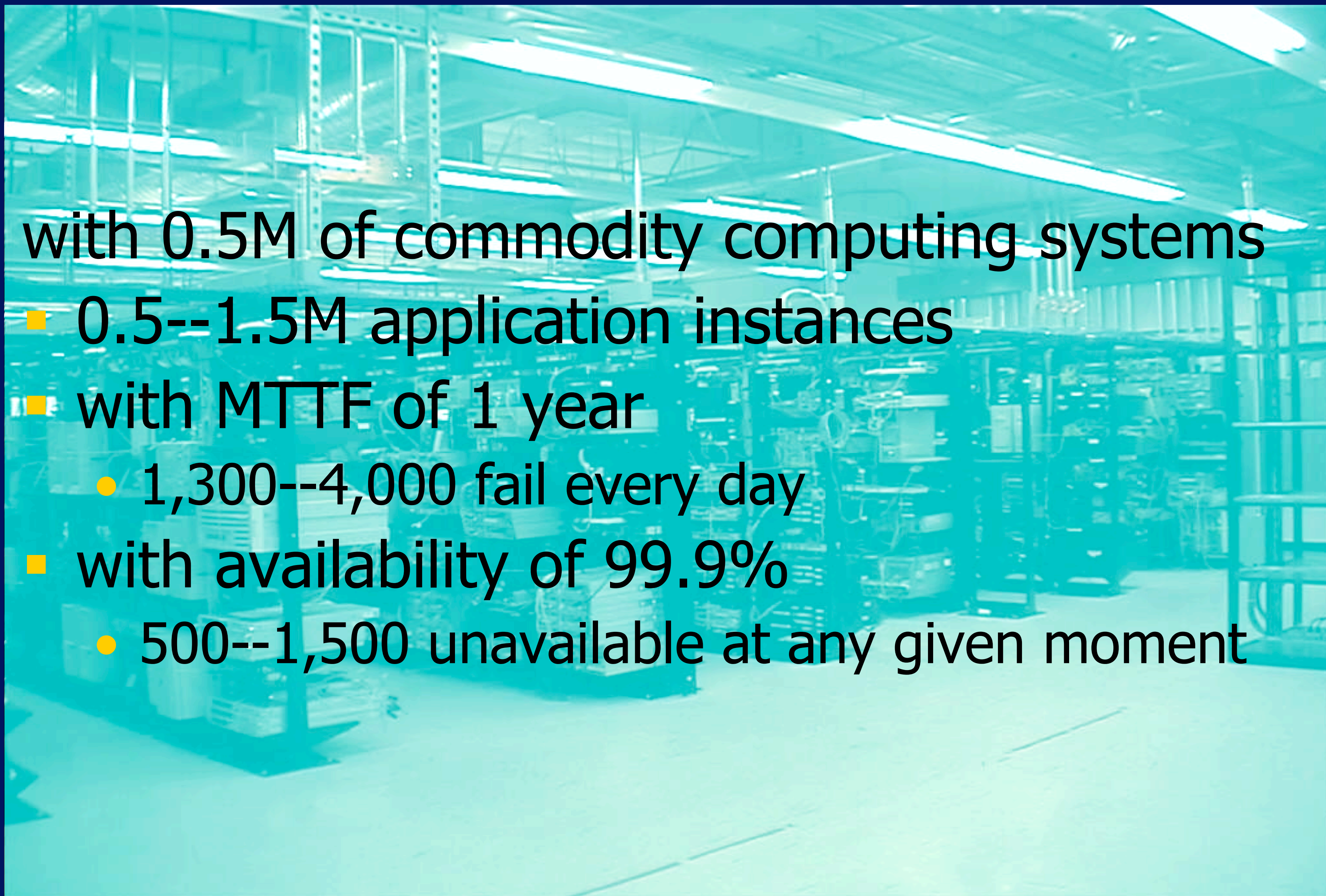
the problem

context

- processor time virtually free
- human time/attention expensive
- commodity computing most cost-effective

target environments

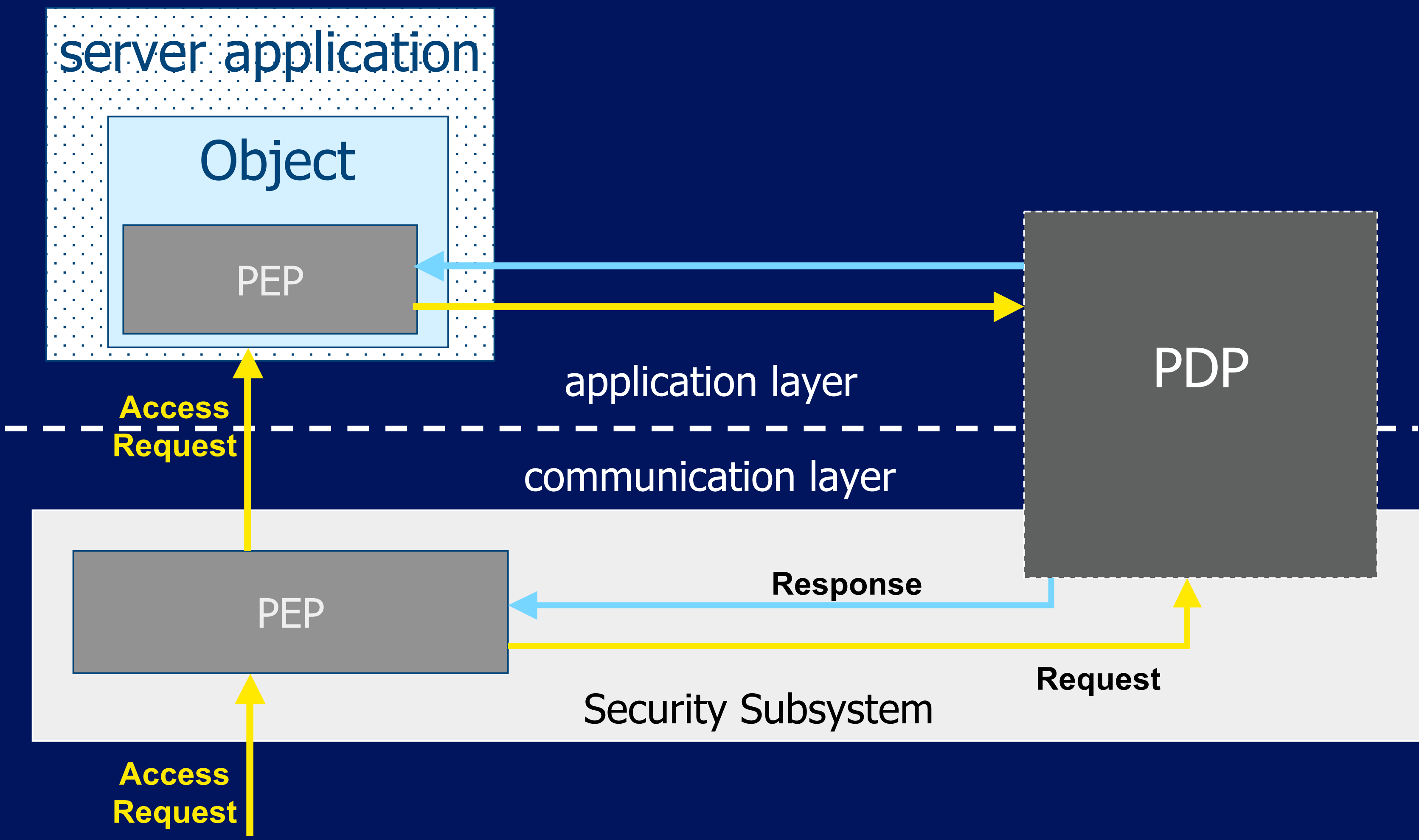
target environments



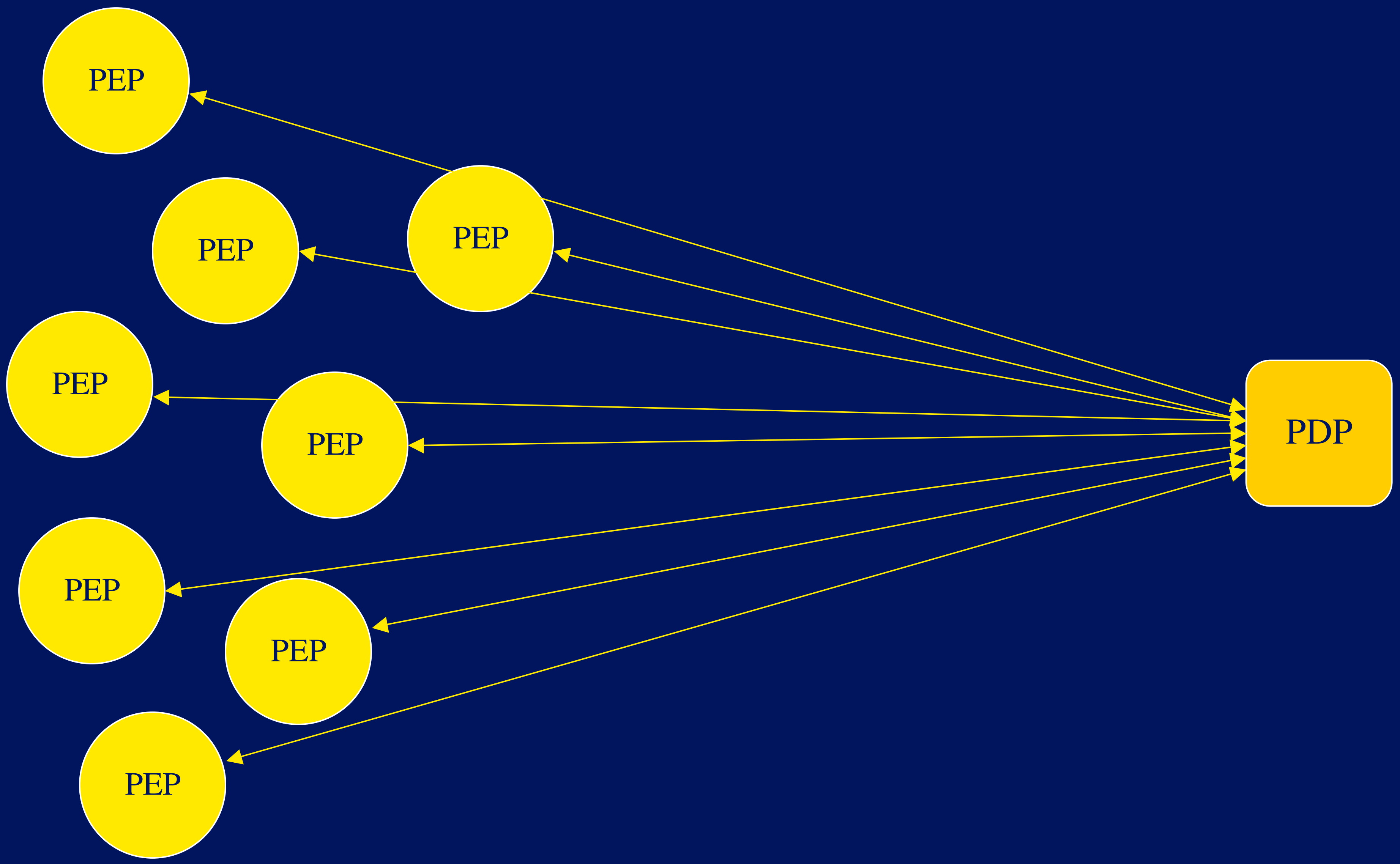
with 0.5M of commodity computing systems

- 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

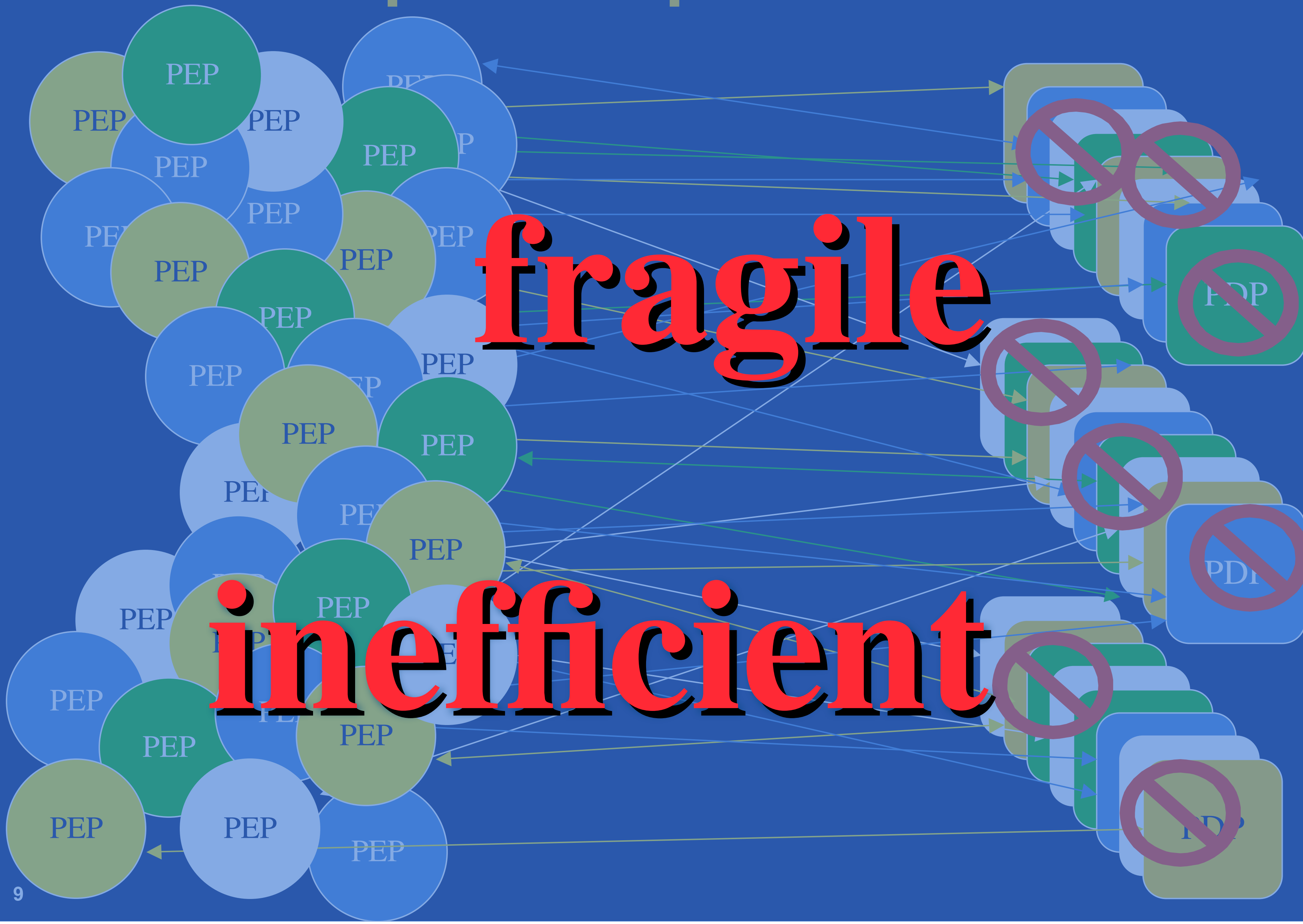
request-response paradigm



enables PDP reuse



results in point-to-point architectures



addressed problem

point-to-point authorization architectures at massive scale

- become too fragile, requiring costly human attention, and
- fail to reduce latency by exploiting the virtually free CPU resources and high network bandwidth

THE UNIVERSITY OF BRITISH COLUMBIA

the approach

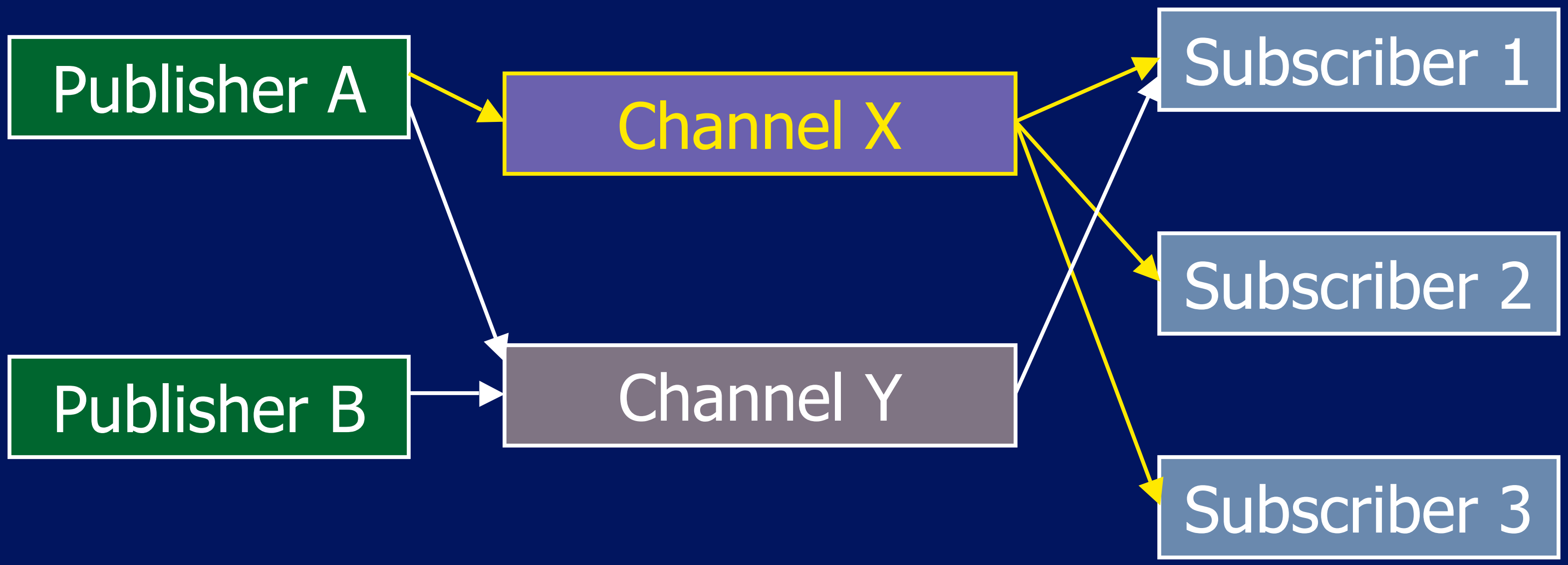
addressing the problem

1. decouple PEPs from PDPs with publish-subscribe architecture(s)

2. recycle policy decisions

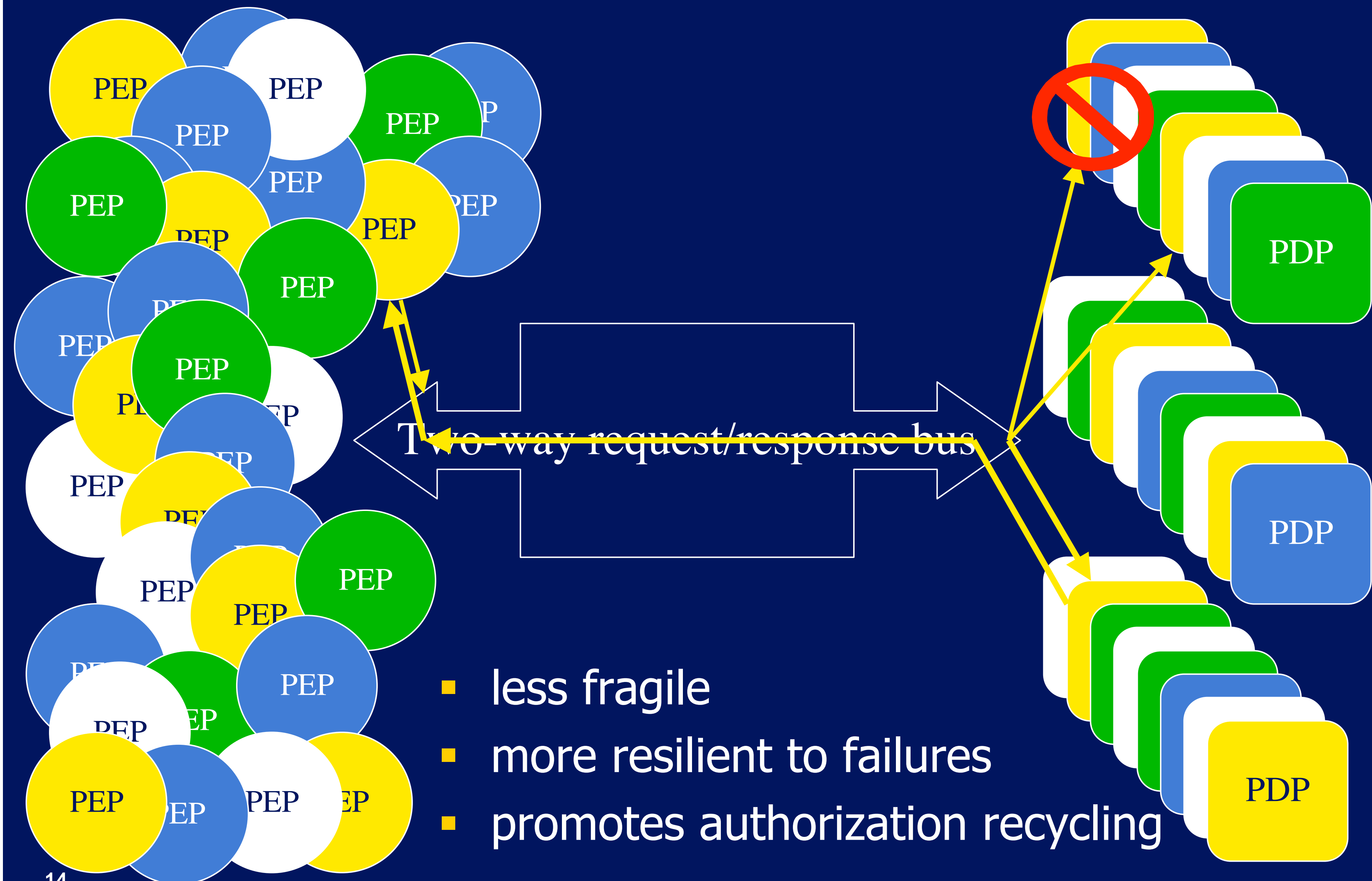
3. flood PEPs with speculatively computed (junk) authorizations

publish-subscribe architecture



Used properties:
- many-to-many
- asynchronous

publish-subscribe for policy decisions

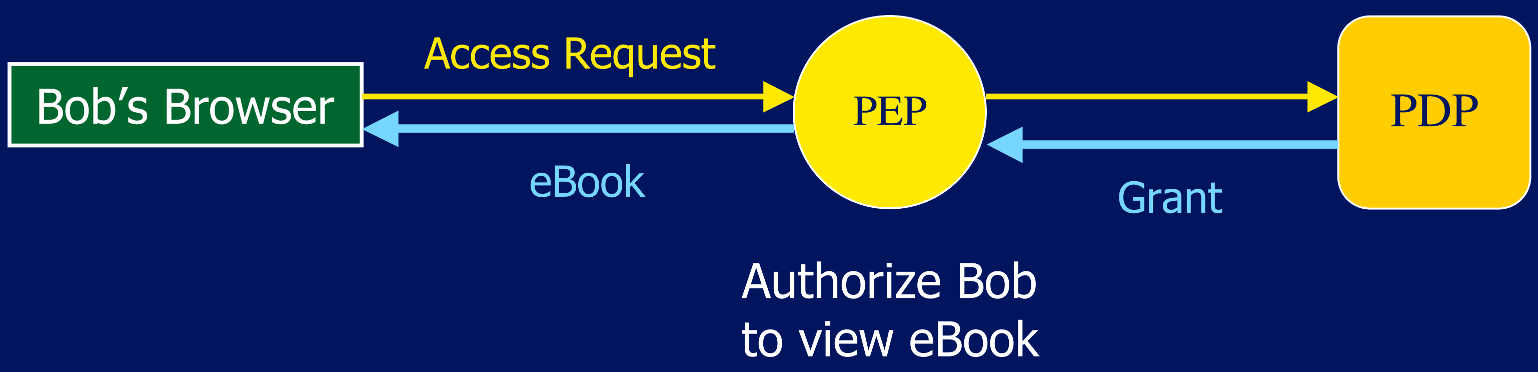


- less fragile
- more resilient to failures
- promotes authorization recycling

recycling authorizations

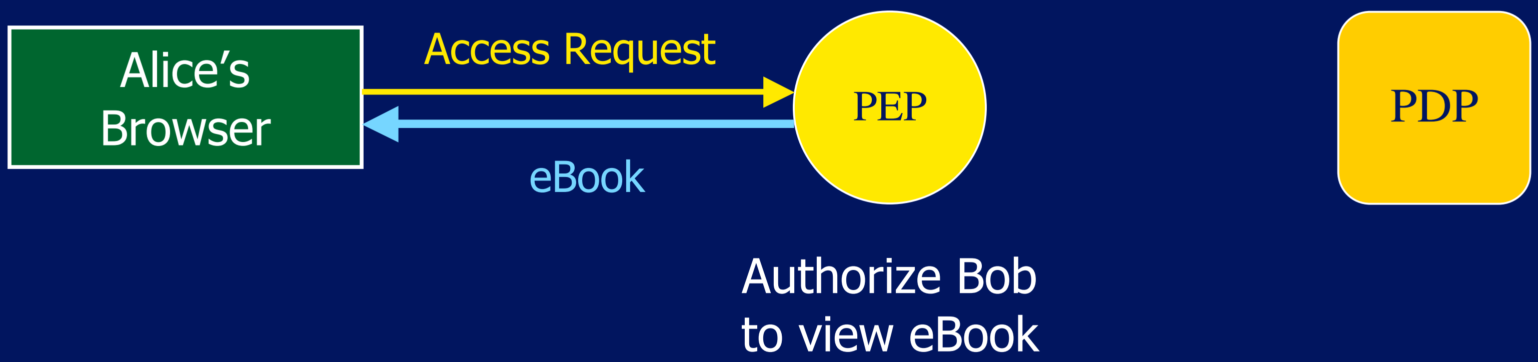
Bob is a *customer*

- He gets authorization to view "Software Design"



recycling authorization

- Alice *preferred customer*
  - More privileges than Bob
  - System recycles the authorization for Bob and allows Alice to view the book



THE UNIVERSITY OF BRITISH COLUMBIA

Secondary and Approximate Authorizations Model (SAAM)

basic elements

- request <s, o, a, c, i>
  - s -- subject
  - o -- object
  - a -- access right
  - c -- context
  - i -- identity of the request

  <{id="Bob", role="customer"}, {id="eB-23"}, view, {date="05-08-15"}, 6112>
- response <r, i, E, d>
  - r -- response identity
  - i -- identity of the request
  - E -- evidence
  - d -- decision

  < 934598438, 6112, [ ], allow > -- direct (from PDP) response

  < 943498843, 6115, [6112], allow > -- indirect/precise response

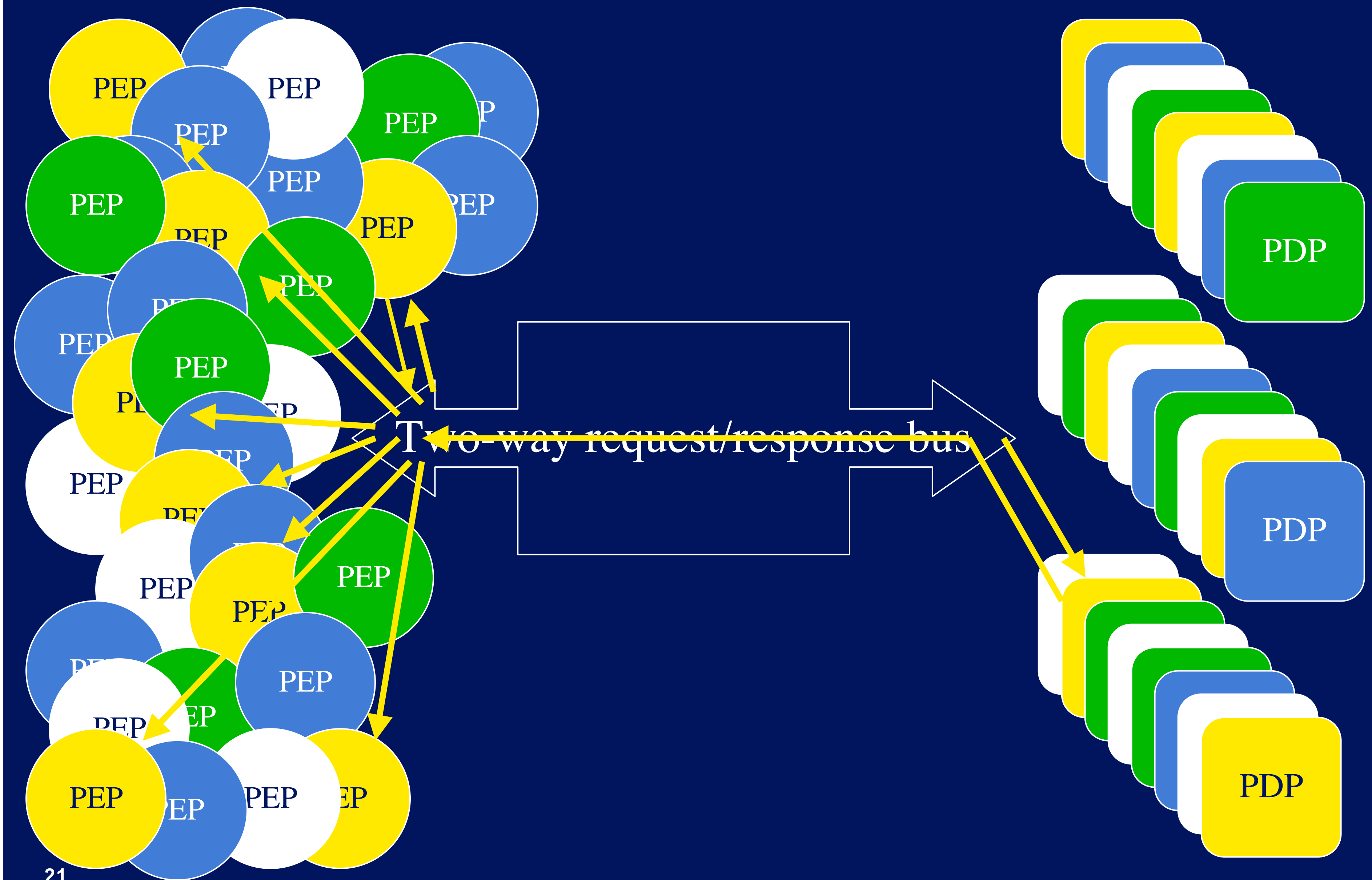
  < 990923124, 6120, [6112], allow > -- indirect/approximate response

recycling authorizations

- secondary authorizations
  - re-using decisions made for other, but equivalent, requests
  - example <s, o, a, c, i> <s, o, a, c, i’>
- approximate authorizations
  - re-using decisions made for other, but similar, requests
  - examples
    - preferred customer ≥ customer ≥ visitor
    - row ≤ table
    - read ≤ modify

back to JAMES

flooding with speculative authorizations



summary

- problem
  - context and assumptions
    - human time/attention is too expensive
    - CPU resources are virtually free
    - commodity computing is most cost effective
  - target environments
    - massive-scale enterprises with 10^5 machines
  - limitations of point-to-point architectures
    - too fragile, high latency, too expensive to maintain
- approach
  - decouple PEPs and PDPs with publish-subscribe
  - recycle authorizations
    - secondary and approximate authorization model (SAAM)
  - flood with junk authorizations

current status and future work

- current work
  - $SAAM_{BLP}$, $SAAM_{RBAC}$, $SAAM_{significant}$
  - simulation
  - P2P-based authorization recycling
  - publish-subscribe for authorizations
- future work
  - speculative authorizations

THE UNIVERSITY OF BRITISH COLUMBIA

An Overview of The Ongoing Research at LERSSE

Konstantin Beznosov
http://konstantin.beznosov.net

What's LERSSE?

Laboratory for Education and Research in Secure Systems Engineering

- Research group at
  the Department of Electrical & Computer Eng.
  UBC
- People
  - Faculty
    - Konstantin Beznosov, lead (computer security)
    - Sidney Fels (Human Computer Interaction), lead of HCT Lab
  - 2 Ph.D. students
  - 5 Master students + 2 joining in September

http://lersse.ece.ubc.ca

Research Directions and Projects

1. engineering security mechanisms
   - *CORBA Security, RAD,* AAS, **RAD JACCet**, *SDMM, attribute function, EASI, composable authorization engines,* **JAMES**, **AC mech. eval.**
2. access control models & languages
   - CORBA-RBAC, RelBAC *XACML v1.0*, **SAAM**, **probabilistic trust**
3. engineering secure software
   - **agile security assurance**
4. network security
   - **MC-SSL**
5. critical infrastructure interdependencies
   - **CITI interdependencies**
6. usable security
   - **HOT Admin**

Legend: **current**, **presented**, past, *back in industry*

agile security assurance

problem

mismatch between agile development & security assurance

contributions

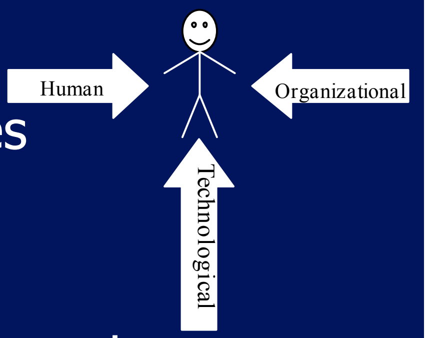
1. **examined** (pain points)
2. **classified** assurance methods
3. **alleviated** (tools, knowledge codification, new methods research, intermittent assurance)

Further research

- tool support
- knowledge classification
- new assurance methods

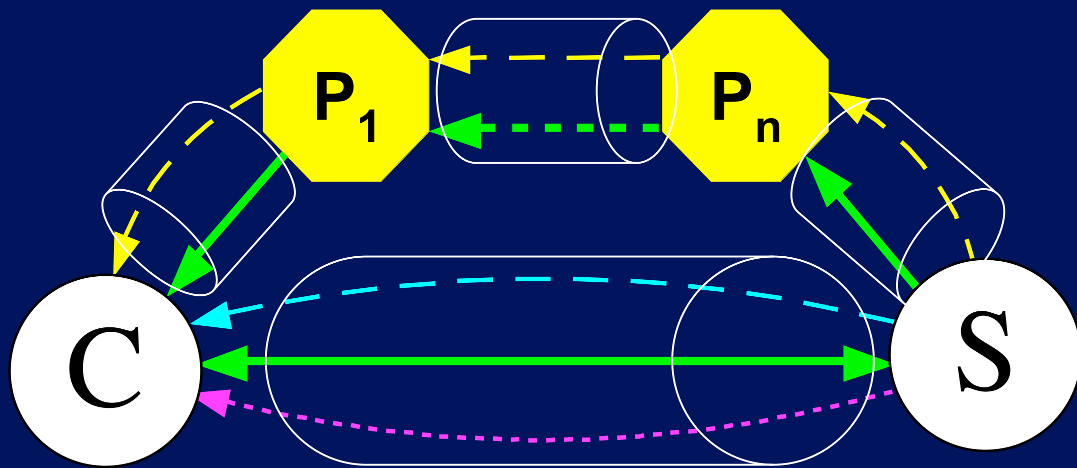
HOT Admin: Human, Organization, and Technology Centred Improvement of IT Security Administration

- purpose
  1. evaluation methodology for sec. admin. effectiveness
  2. guidelines and techniques to design sec. admin. tools
- problem addressed
  - conflict of human, organizational, and technological forces
- approach
  - resolve the conflict through harmonizing the forces



- work plan (3 years)
  1. pilot studies to fine-tune the methodologies
  2. inventories and an initial analysis through field research
  3. development of models
  4. design of techniques and methodologies
  5. validation and evaluation of the project's key results.
- team
  - Kosta Beznosov (security), Sid Fels (interfaces),
    Lee Iverson (collaborations), Brian Fisher (interaction)

multiple-channel SSL



- end-to-end security with partially trusted proxies
- selective data protection