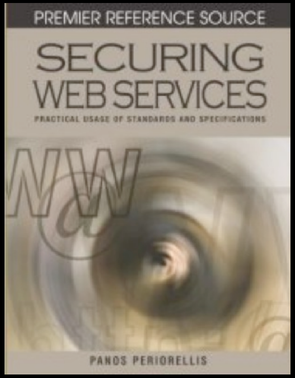
Why (Managing) IT Security is Hard and Some Ideas for Making It Easier

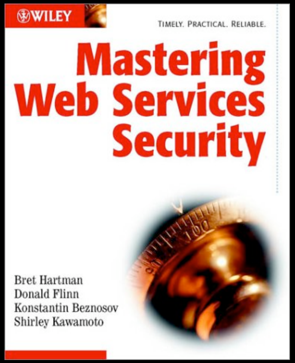
Konstantin (Kosta) Beznosov

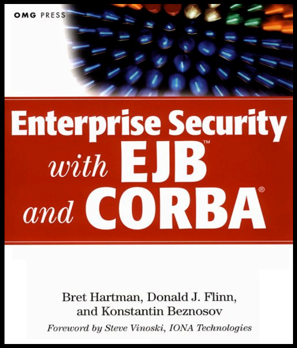
Laboratory for Education and Research in Secure Systems Engineering
Department of Electrical and Computer Engineering
University of British Columbia, Canada

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)
  - 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






OMG PRESS
Enterprise Security with EJB and CORBA
Bret Hartman, Donald J. Flinn, and Konstantin Beznosov
Foreword by Steve Vinoski, IONA Technologies

University of British Columbia

founded in 1908
ranked among the world top

- 40 institutes, by the *Shanghai Jiao Tong University*
- 27 universities, by *Newsweek* magazine in 2006
- 38 universities, by the *Times Higher Education Supplement* in 2005

airplanes vs. cars

- flying is fast
- driving is slow
- why isn't everybody flying?

IT Security is Critical

IT Security is Costly

organizations worldwide spent in 2007

$1.55 trillion on IT

7-9% on IT security

$108 billion

Forrester Research

Cyber crime market worldwide

$105 billion

John Viega, Mcafee

why aren't secure systems everywhere?

almost completely insecure, or “secure” **but**

- too expensive and error-prone to build
- too complex to administer
- inadequate for real-world problems
- forever

examples

what can be done about it?

improvements towards

1. inexpensive and error-proof to build
2. effective and inexpensive in administration
3. adequate for problem domains
4. easy and inexpensive to change and integrate

Outline

- HOT Admin
- JAMES
- SQLPrevent

HOT Admin

a broad empirical study of IT security practitioners and their environment

HOT Admin:
Human **O**rganization and **T**echnology Centred Improvement of IT Security **Admin**istration

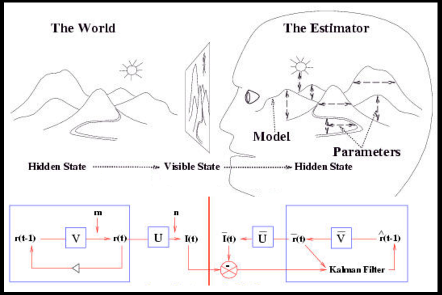
- Purpose
  - Tool evaluation: methodology
  - Tool design: guidelines & techniques

H

O T

Work Plan

Field study



Models

Techniques & Methodologies

Validation & Evaluation

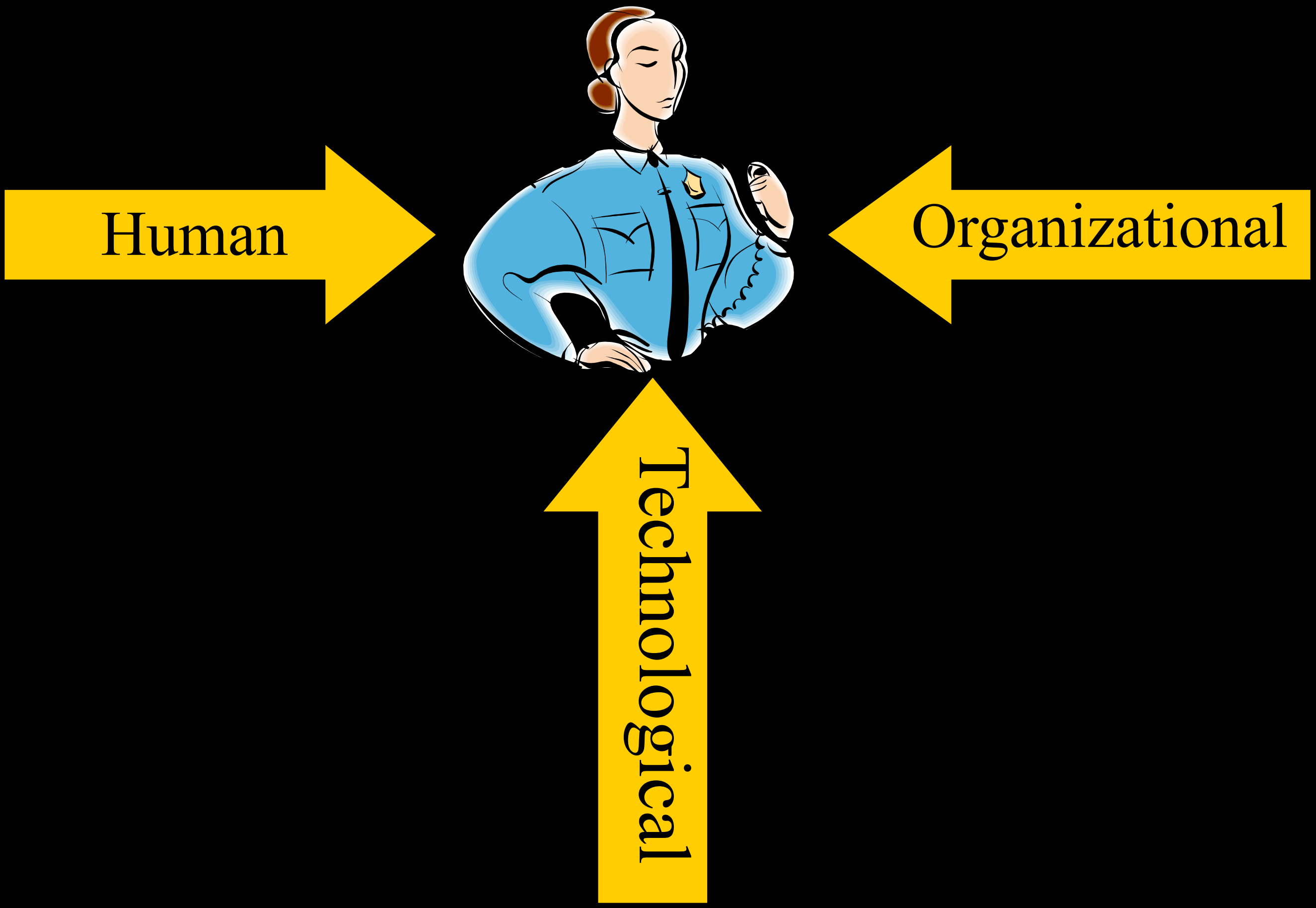
sponsors and partners

Entrust®

NSERC CRSNG

SAP®

Human Organization and Technology Centred

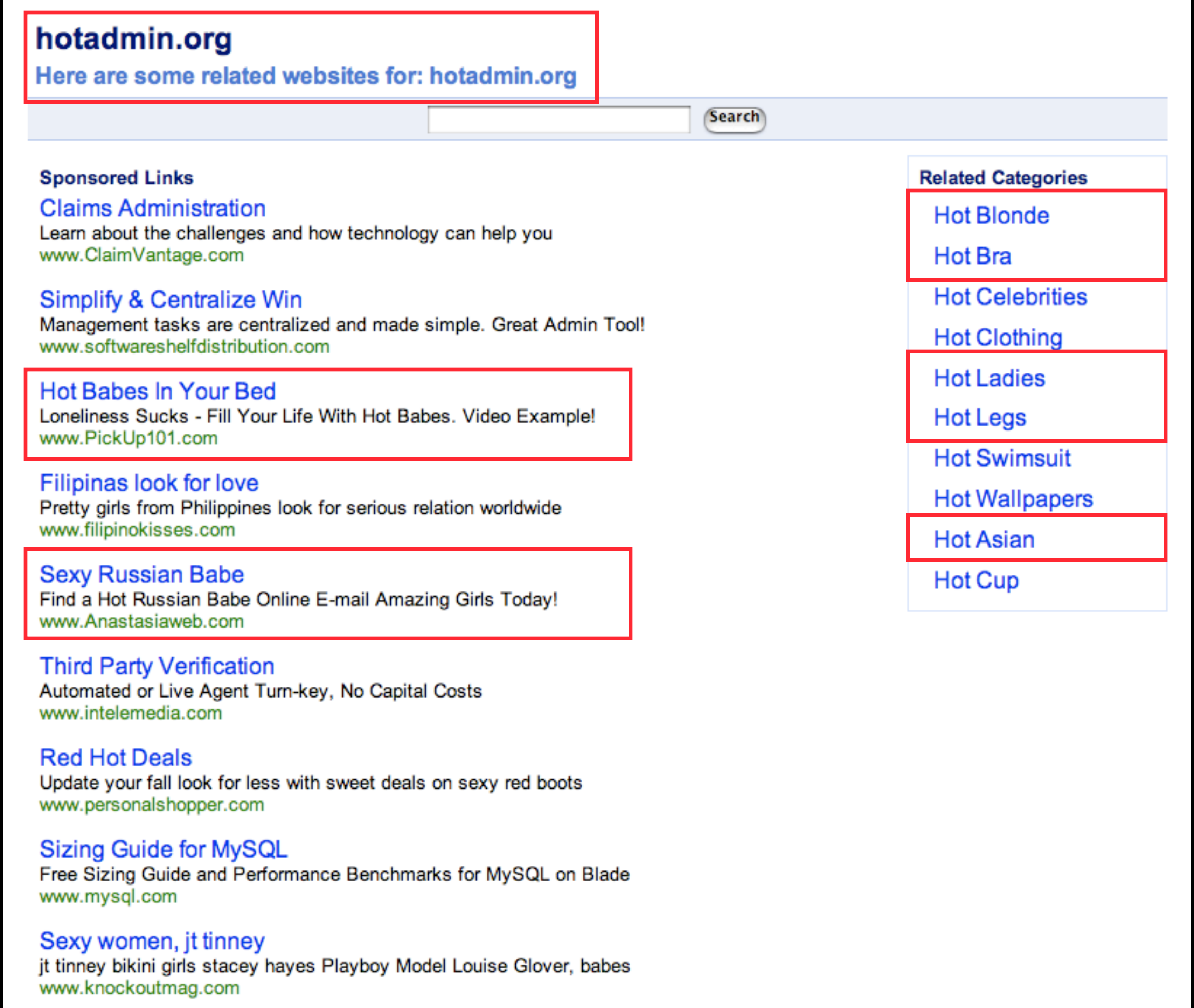


Human

Organizational

Technological

hotadmin.org



hotadmin.org

Here are some related websites for: hotadmin.org

Sponsored Links

Claims Administration
Learn about the challenges and how technology can help you
www.ClaimVantage.com

Simplify & Centralize Win
Management tasks are centralized and made simple. Great Admin Tool!
www.softwareshelfdistribution.com

Hot Babes In Your Bed
Loneliness Sucks - Fill Your Life With Hot Babes. Video Example!
www.PickUp101.com

Filipinas look for love
Pretty girls from Philippines look for serious relation worldwide
www.filipinokisses.com

Sexy Russian Babe
Find a Hot Russian Babe Online E-mail Amazing Girls Today!
www.Anastasiaweb.com

Third Party Verification
Automated or Live Agent Turn-key, No Capital Costs
www.intelemedia.com

Red Hot Deals
Update your fall look for less with sweet deals on sexy red boots
www.personalshopper.com

Sizing Guide for MySQL
Free Sizing Guide and Performance Benchmarks for MySQL on Blade
www.mysql.com

Sexy women, jt tinney
jt tinney bikini girls stacey hayes Playboy Model Louise Glover, babes
www.knockoutmag.com

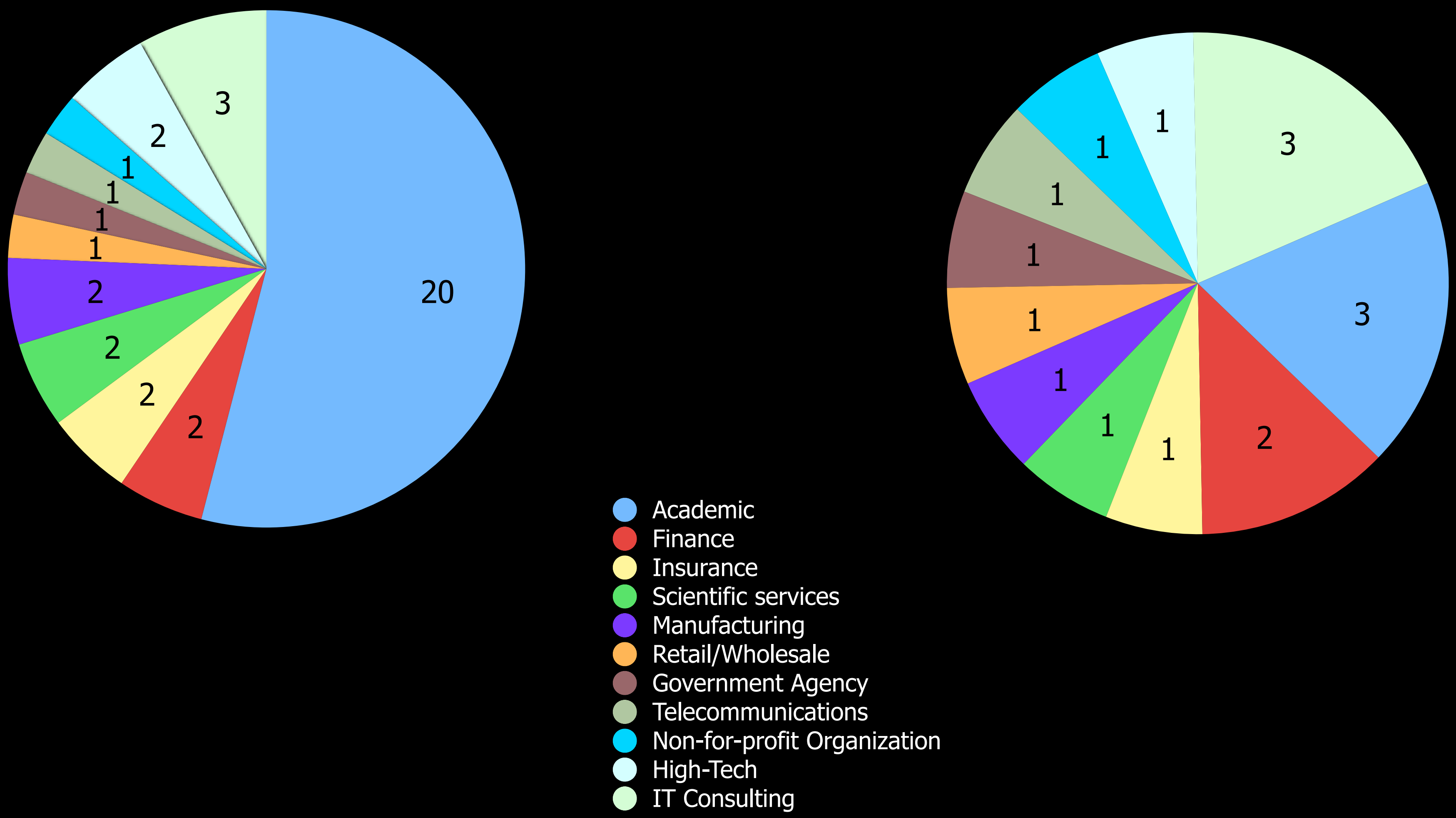
Related Categories

Hot Blonde
Hot Bra
Hot Celebrities
Hot Clothing
Hot Ladies
Hot Legs
Hot Swimsuit
Hot Wallpapers
Hot Asian
Hot Cup

methods summary

- data collection
  - online questionnaire
    - demographics
  - in situ semi-structured interviews
    - two interviewers
  - participatory observations
    - 75 hours in academic organization IT department
    - policy development and IDS deployment
- data analysis
  - qualitative description
    - constant comparison, inductive analysis
    - coding: selective, open, axial, theoretical

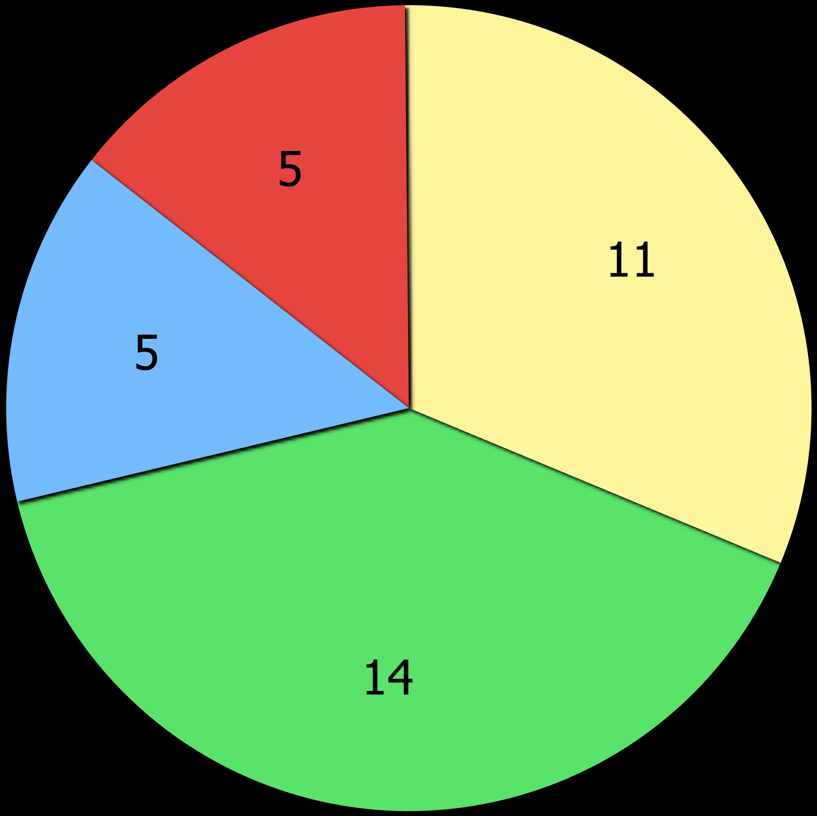
industry sectors



36 interviews

16 organizations

job types



- 🟦 IT Manager
- 🟥 Security Manager
- 🟨 Security Specialist
- 🟩 IT (with security tasks)

findings to date

no security admins!

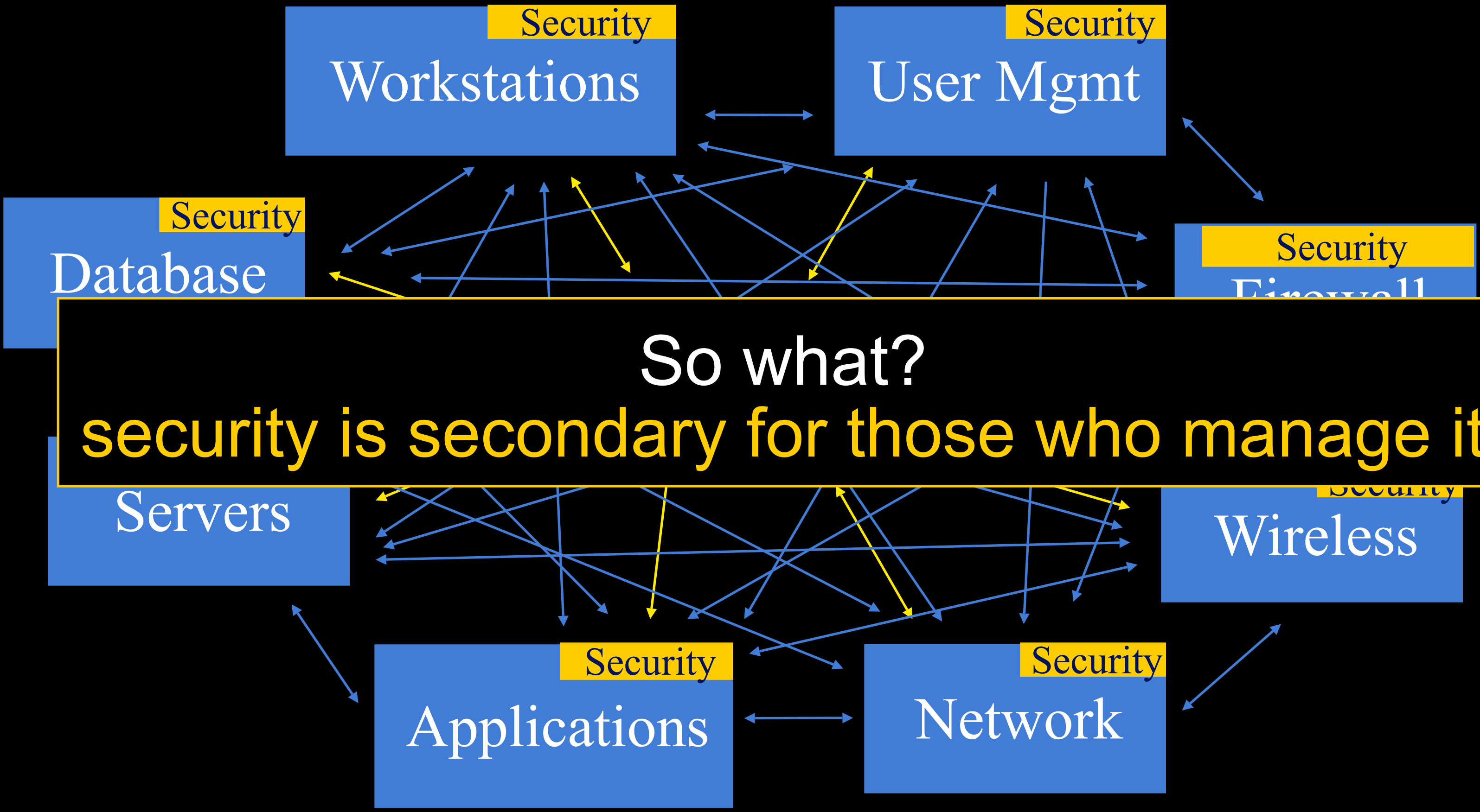
- system analysts
- application analysts
- business analysts
- technical analysts
- system administrators

- application programmers
- auditors
- IT managers
- security leads
- network leads

``… *what makes me [a security] analyst is that I'm also involved in developing the policies and procedures … an analyst is also someone who's doing a certain amount of troubleshooting and someone who's, I guess, a little bit more portable in terms of what their daily responsibilities are going to be like.*''

Study Participant

loosely coordinated teams



So what?

security is secondary for those who manage it

"I have a security team that I work with. They don't report to me but I actually work with them and they sort of are represented by the different areas."

Study Participant

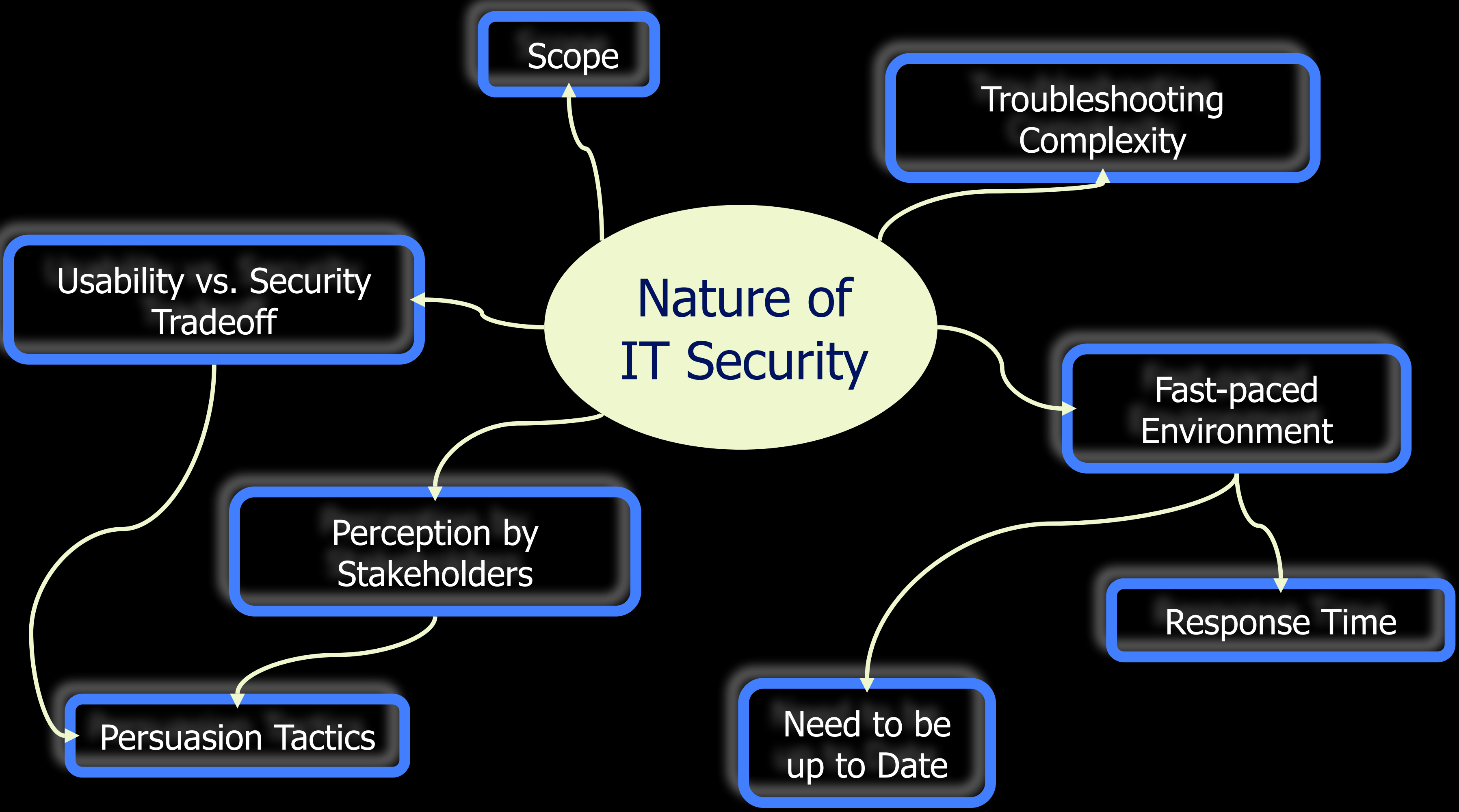
skills they practice

- pattern recognition
- inferential analysis
- use of tacit knowledge
- bricolage
  - Dictionary: “construction or creation from a diverse range of available things”
  - Origin: mid 20th century: French, from bricoler ‘do odd jobs, repair.’

So what?

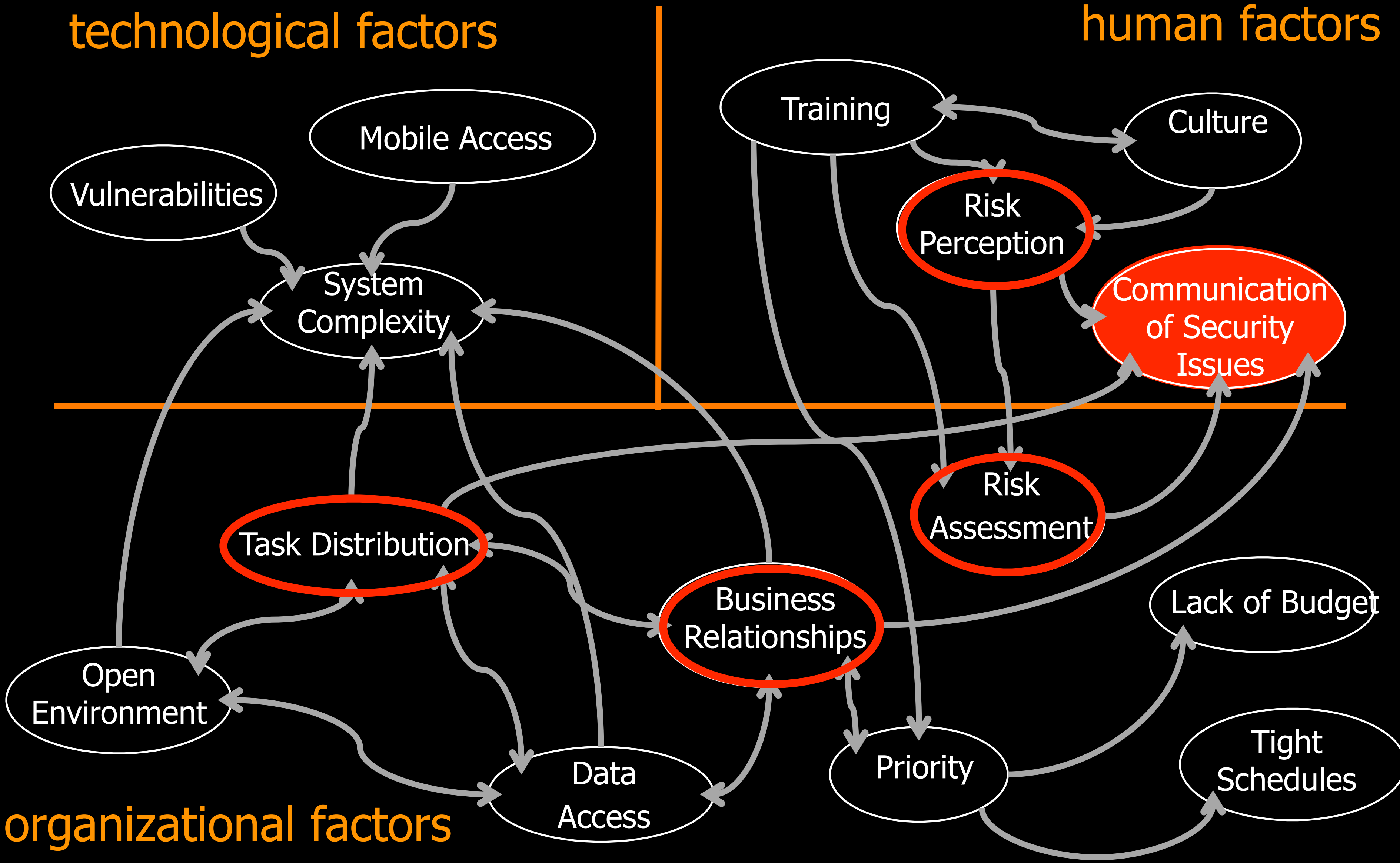
- finding gaps in tool support
- tool improvement
- new usability testing methods

model of differences



For more information:

A. Gagné, K. Muldner, K. Beznosov, “Identifying Security Professionals' Needs: a Qualitative Analysis”, to appear in the Proceedings of the *Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.



technological factors

human factors

organizational factors

Mobile Access

Vulnerabilities

System Complexity

Training

Culture

Risk Perception

Communication of Security Issues

Risk Assessment

Task Distribution

Business Relationships

Lack of Budget

Open Environment

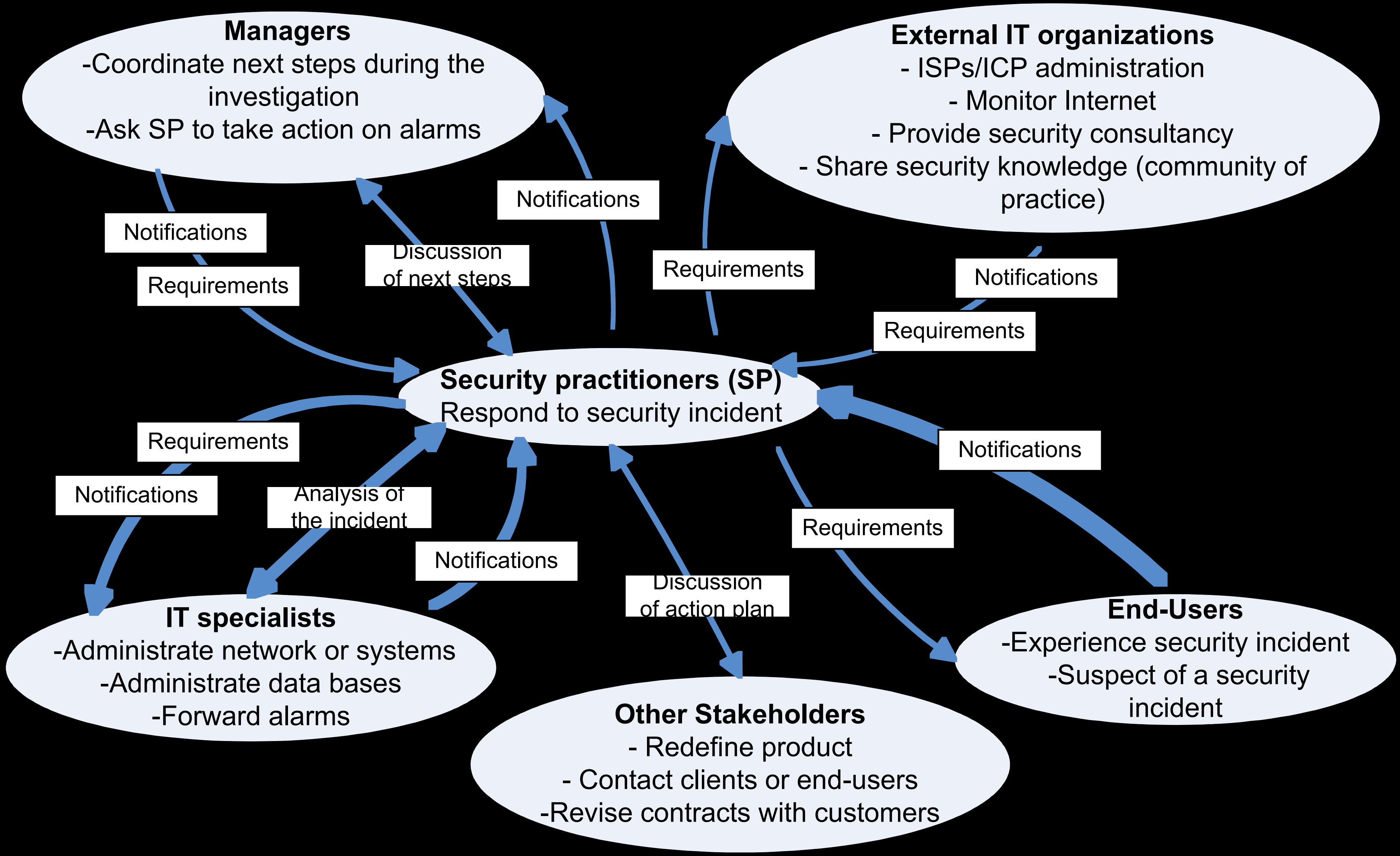
Data Access

Priority

Tight Schedules

R. Werlinger, K. Hawkey, K. Beznosov, “Human, Organizational and Technological Challenges of Implementing IT Security in Organizations”, to appear in the *Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.

Interactions During Incident Response



Managers
-Coordinate next steps during the investigation
-Ask SP to take action on alarms

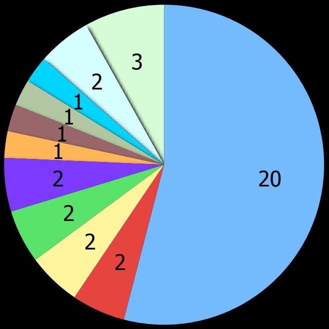
External IT organizations
- ISPs/ICP administration
- Monitor Internet
- Provide security consultancy
- Share security knowledge (community of practice)

Security practitioners (SP)
Respond to security incident

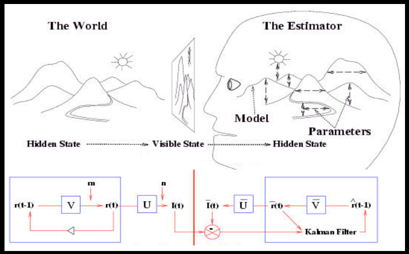
IT specialists
-Administrate network or systems
-Administrate data bases
-Forward alarms

Other Stakeholders
- Redefine product
- Contact clients or end-users
-Revise contracts with customers

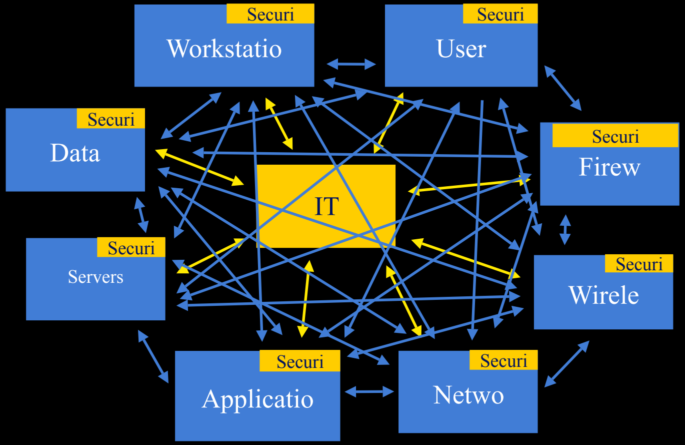
End-Users
-Experience security incident
-Suspect of a security incident

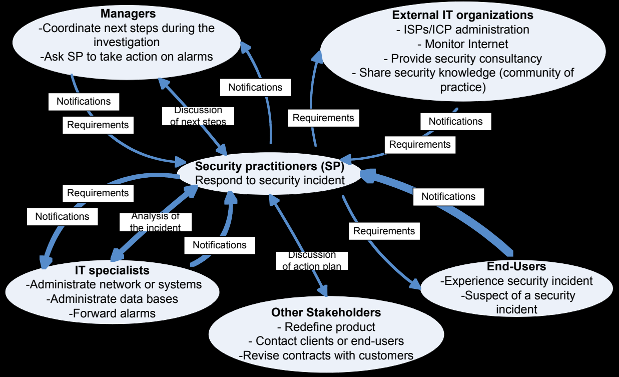


Field study

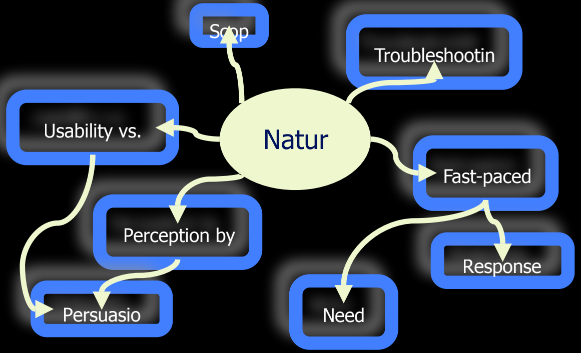


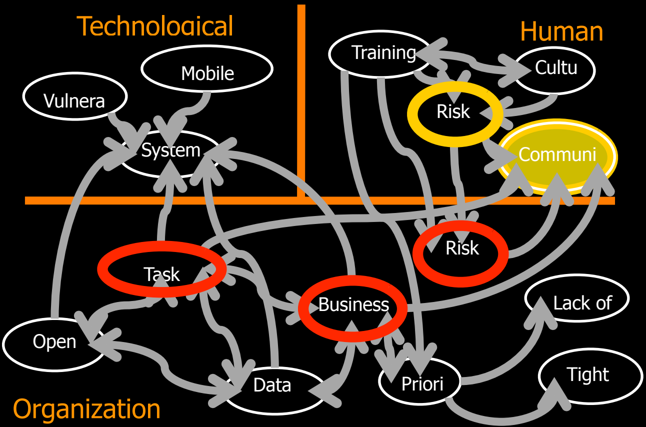
Models





Managers
-Coordinate next steps during the investigation
-Ask SP to take action on alarms
External IT organizations
- ISPs/ICP administration
- Monitor Internet
- Provide security consultancy
- Share security knowledge (community of practice)
Notifications
Notifications
Requirements
Discussion of next steps
Requirements
Notifications
Requirements
Security practitioners (SP)
Respond to security incident
Requirements
Notifications
Notifications
Analysis of the incident
Notifications
Requirements
Discussion of action plan
IT specialists
-Administrate network or systems
-Administrate data bases
-Forward alarms
End-Users
-Experience security incident
-Suspect of a security incident
Other Stakeholders
- Redefine product
- Contact clients or end-users
-Revise contracts with customers

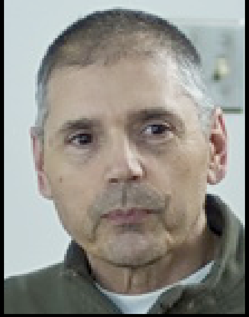


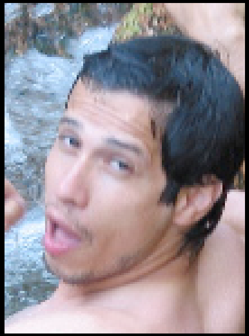


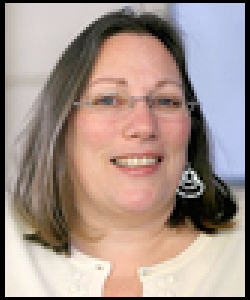
selected project publications

- K. Hawkey, K. Muldner, K. Beznosov, "Searching for the Right Fit: A case study of IT Security Management Models," to appear in *IEEE Internet Computing Magazine*, May/June 2008.
- D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, "Towards understanding IT security professionals and their tools," in the *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pp. 100-111, Pittsburgh, PA, July 18-20 2007.
- A. Gagné, K. Muldner, K. Beznosov, "Identifying Security Professionals' Needs: a Qualitative Analysis", to appear in the *Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.
- R. Werlinger, K. Hawkey, K. Beznosov, "Human, Organizational and Technological Challenges of Implementing IT Security in Organizations", to appear in the *Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.
- K. Beznosov and O. Beznosova, "On the Imbalance of the Security Problem Space and its Expected Consequences," *Journal of Information Management & Computer Security*, Emerald, vol. 15 n.5, September 2007, pp.420-431.
- K. Hawkey, D. Botta, R. Werlinger, K. Muldner, A. Gagné, K. Beznosov "Human, Organizational, and Technological Factors of IT Security" presented at *Research Landscape session of the ACM SIG CHI conference*, April 5-10, 2008, Florence, Italy.
- R. Werlinger, K. Hawkey, K. Beznosov "Security practitioners in context: Their activities and collaborative interactions" presented at *Work in Progress poster session of the ACM SIG CHI conference*, April 5-10, 2008, Florence, Italy.

hotadmin.org


David Botta


Rodrigo Werlinger


Kirstie Hawkey

Kasia Muldner

Kosta Beznosov

Sid Fels

Pooya Jaferian

Fahimeh Raja

Brian Fisher

André Gagné

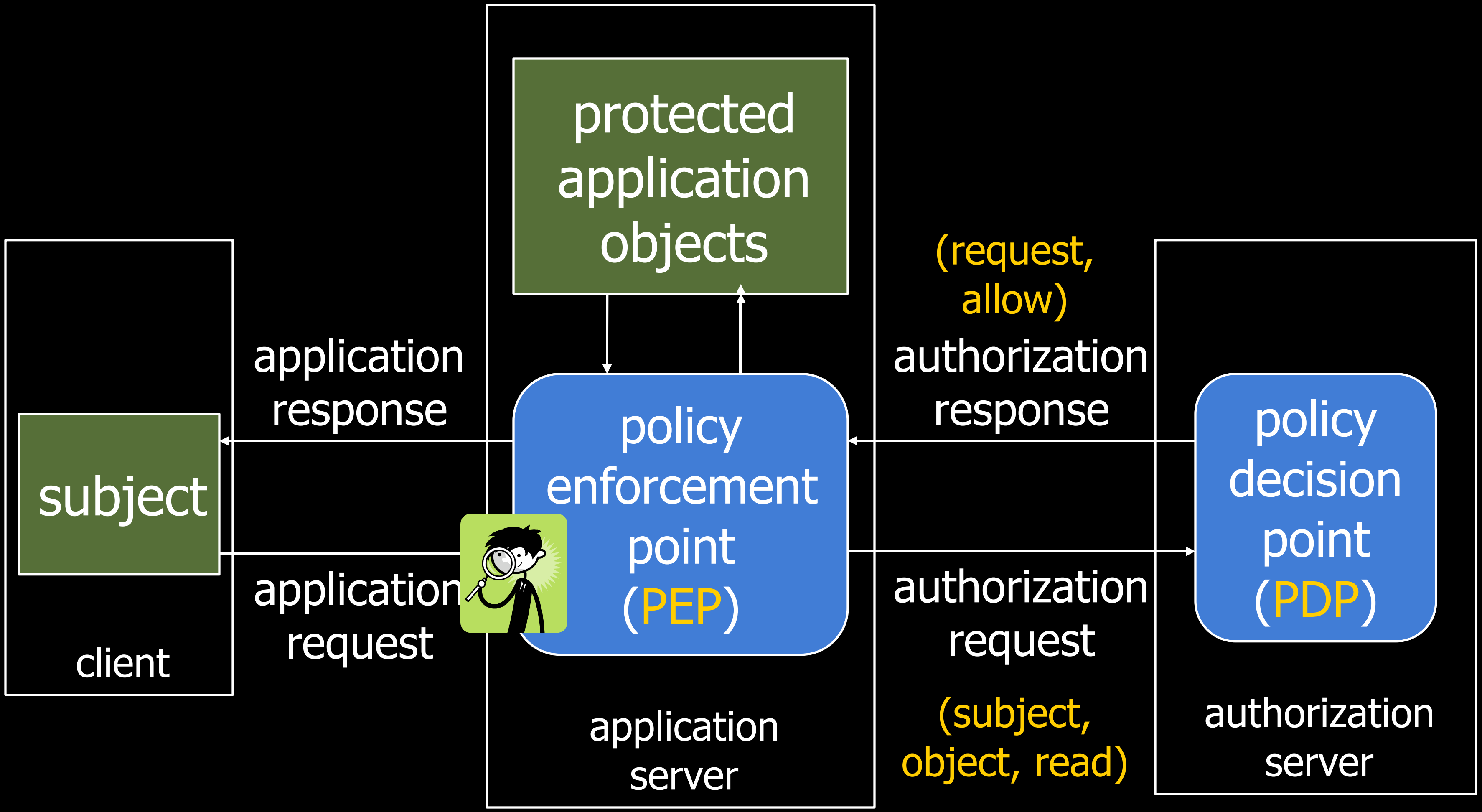
JAMES

flooding and recycling authorizations

departing assumptions

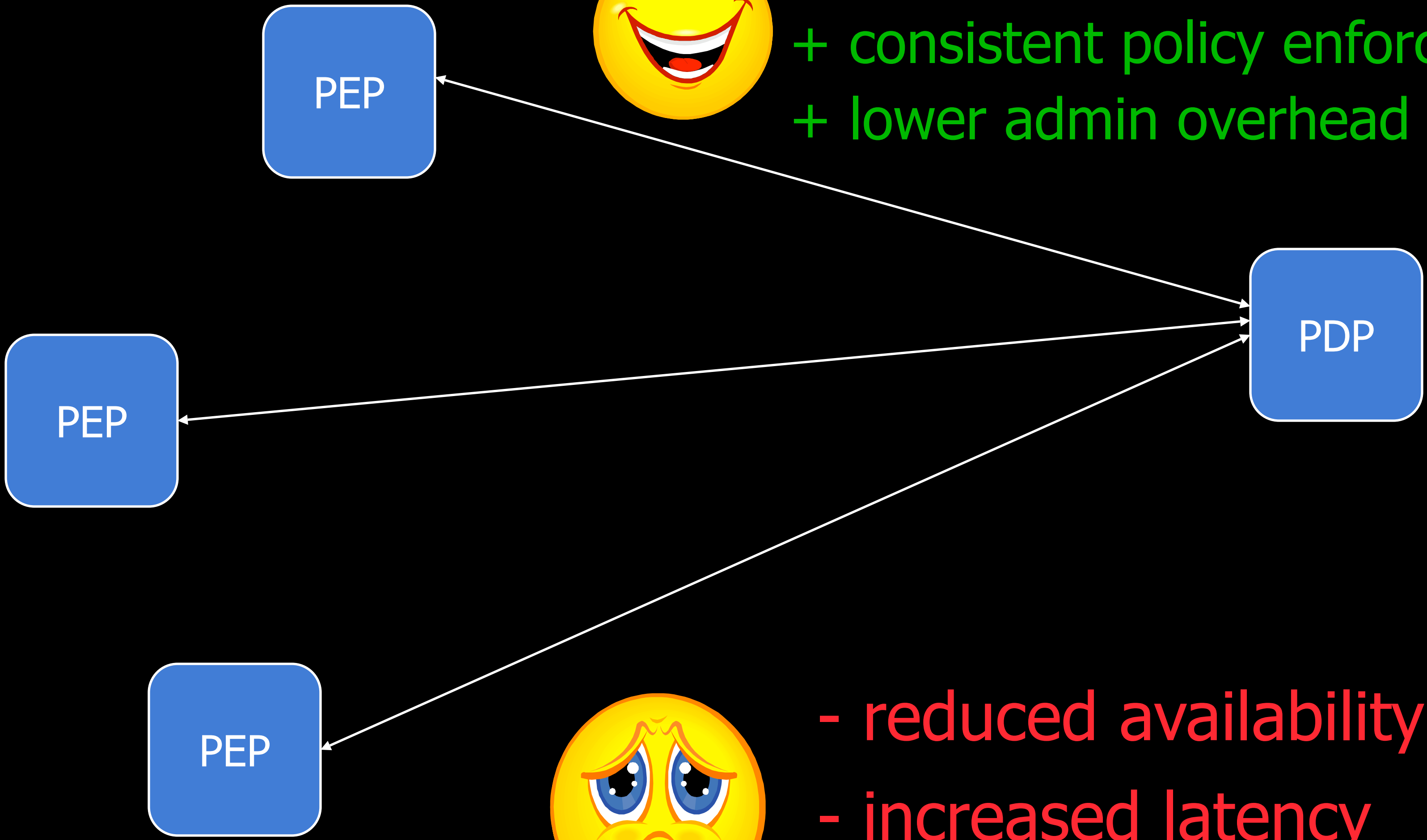
- processor resources virtually free
- commodity computing most cost-effective
- network bandwidth virtually unlimited
- human time/attention expensive

a typical authorization architecture



also known as request-response paradigm
applied by IBM Access Manager, Entrust GetAccess, CA SiteMinder, etc.

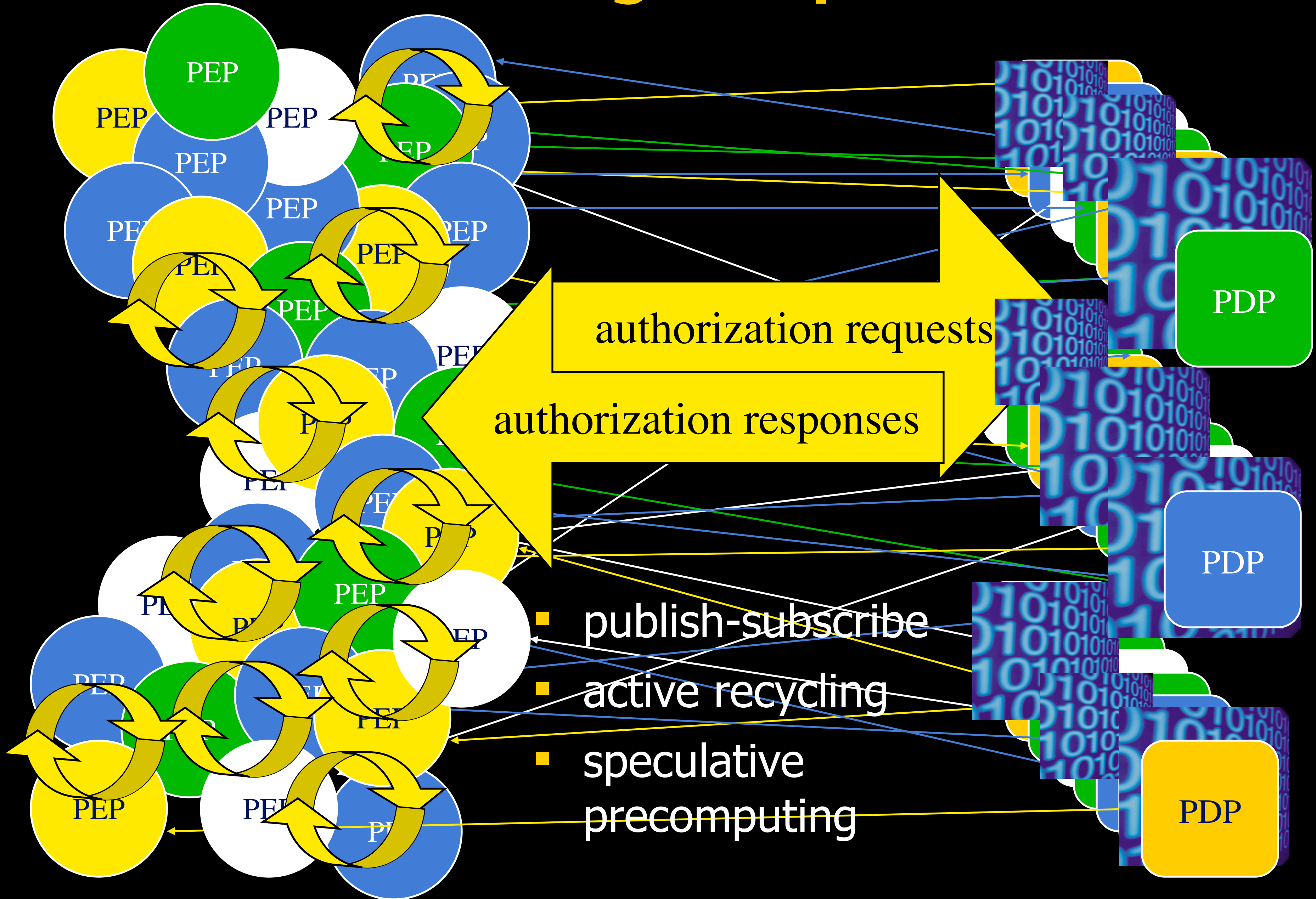
request–response paradigm



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

- reduced availability
- increased latency
- reduced scalability

addressing the problem

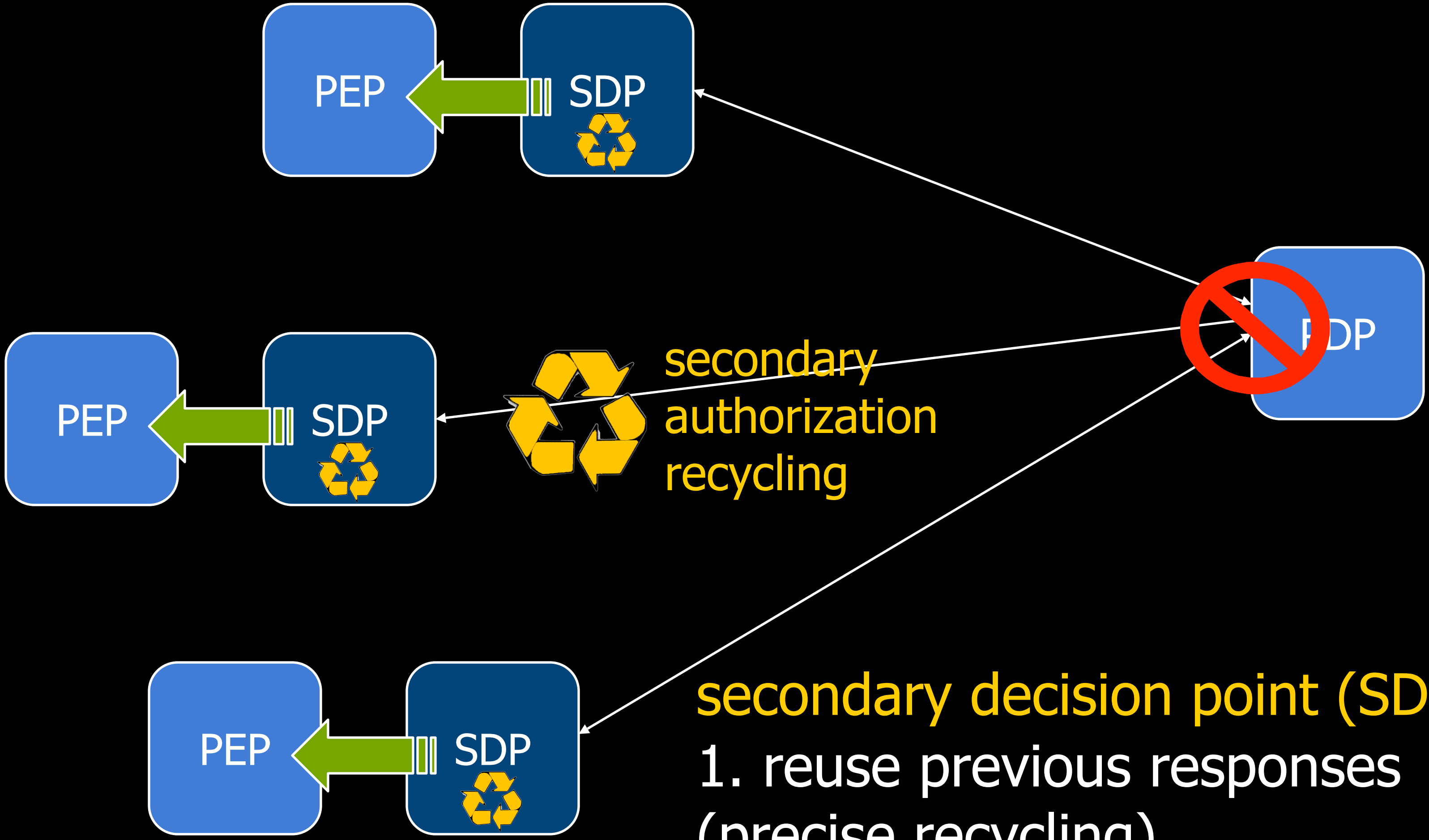


authorization requests

authorization responses

- publish-subscribe
- active recycling
- speculative precomputing

secondary and approximate authorization model (SAAM)



secondary
authorization
recycling

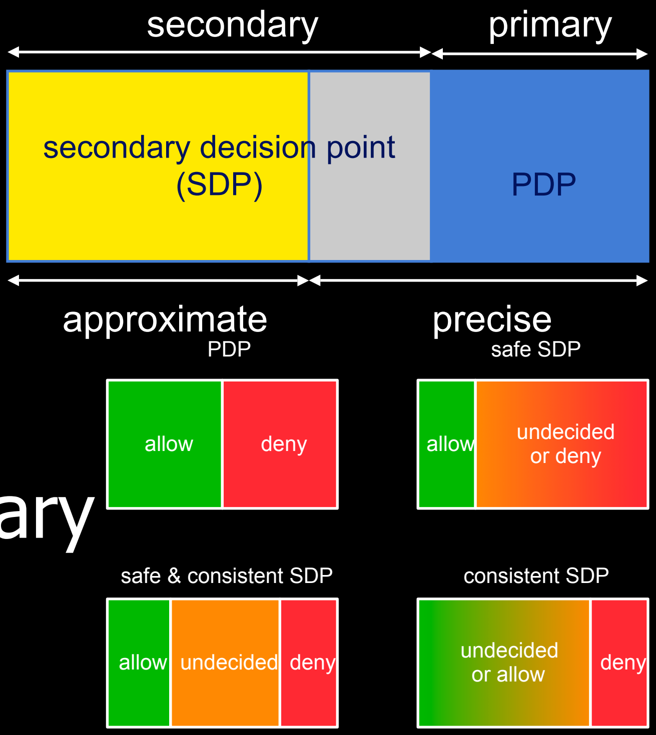
secondary decision point (SDP)

1. reuse previous responses (precise recycling)

2. infer approximate responses (approximate recycling)

SAAM summary

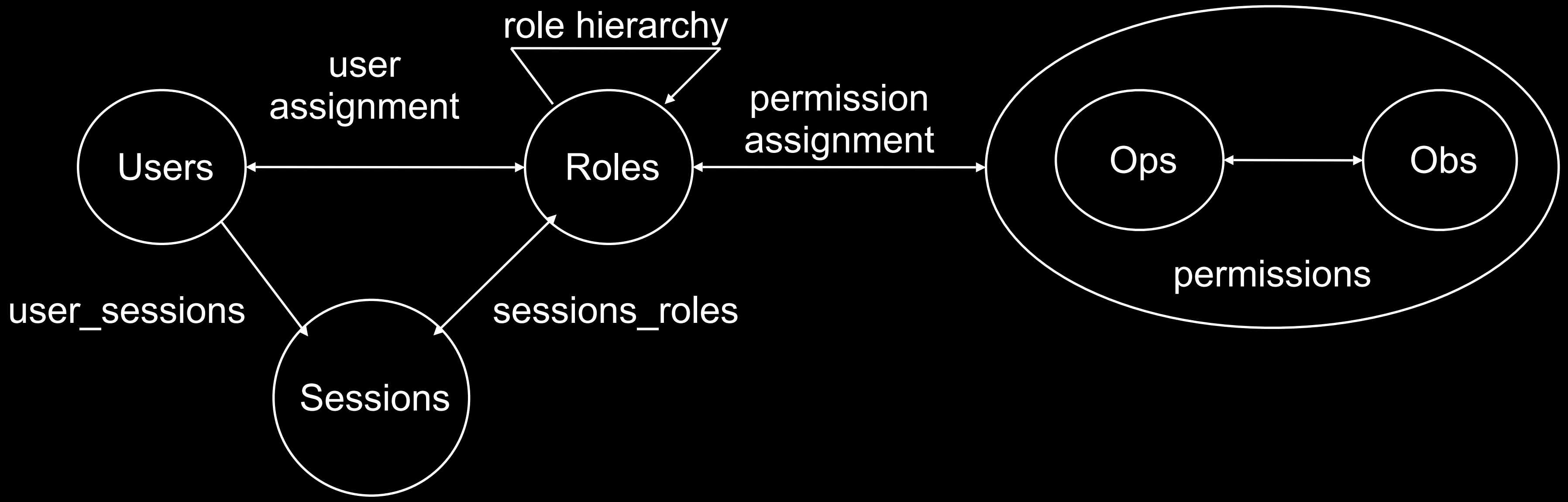
- basic elements
  - authorization requests <s, o, a, c, i>
  - authorization responses <r, i, E, d>
- responses can be
  - primary or secondary
  - precise or approximate
- secondary decision point
  - implemented at PEP
  - uses primary to compute secondary
  - can be safe and/or consistent



selected project publications

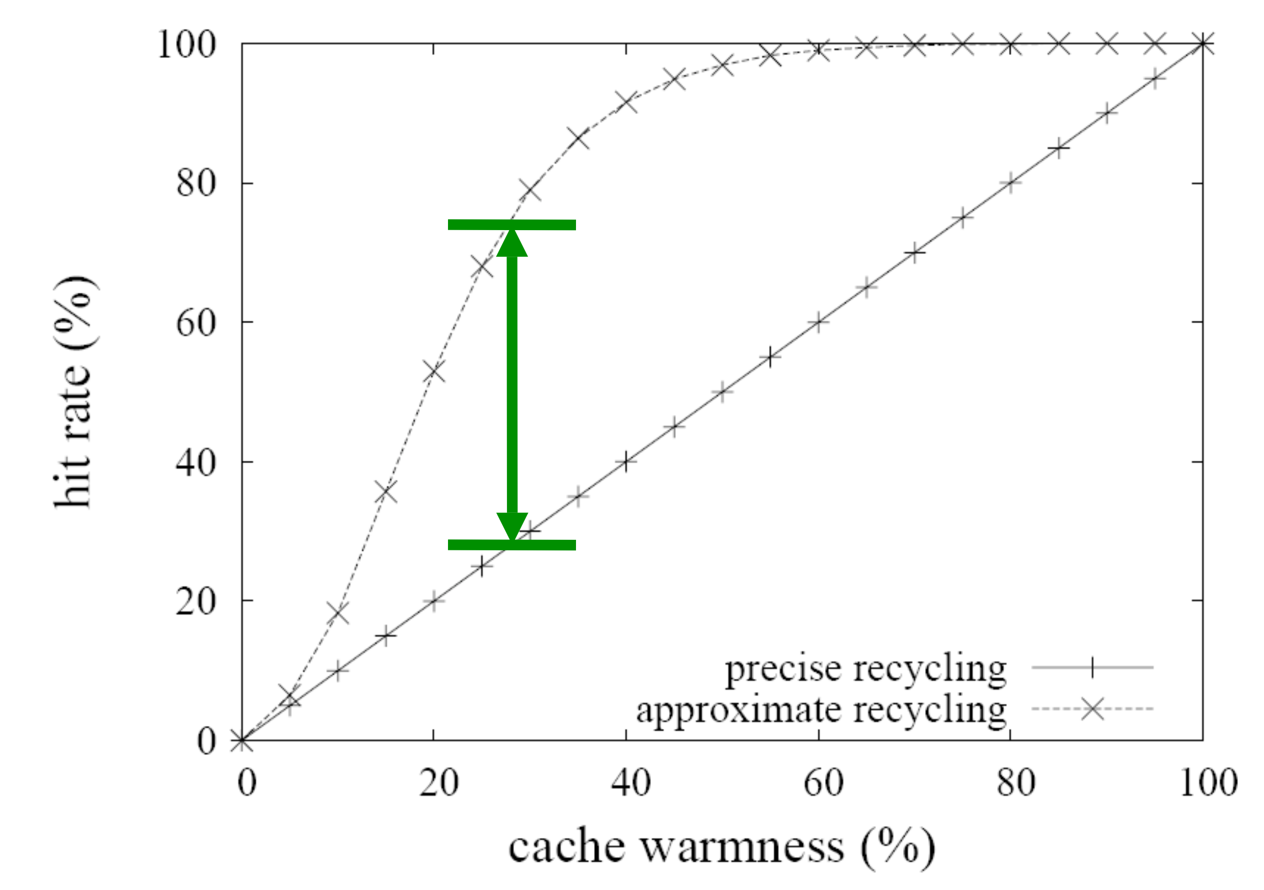
- SAAM for RBAC
  - Q. Wei, J. Crampton, K. Beznosov, M. Ripeanu, “Authorization Recycling in RBAC Systems” to appear in Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Estes Park, Colorado, 11-13 June 2008.
- SAAM for Bell-Lapadula
  - J. Crampton, W. Leung, K. Beznosov, “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 SAAM
  - Q. Wei, M. Ripeanu, K. Beznosov, “Cooperative Secondary Authorization Recycling” 14 pages, to appear in the IEEE Transactions on Parallel and Distributed Systems, on 2008-05-08.
  - 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.
- 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.

SAAM$_{RBAC}$: SAAM for RBAC

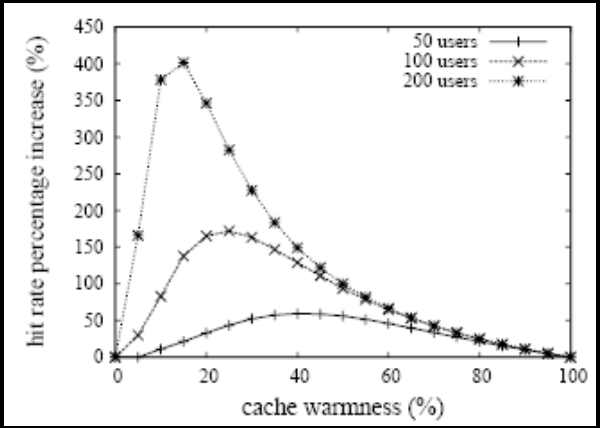


improvements in availability

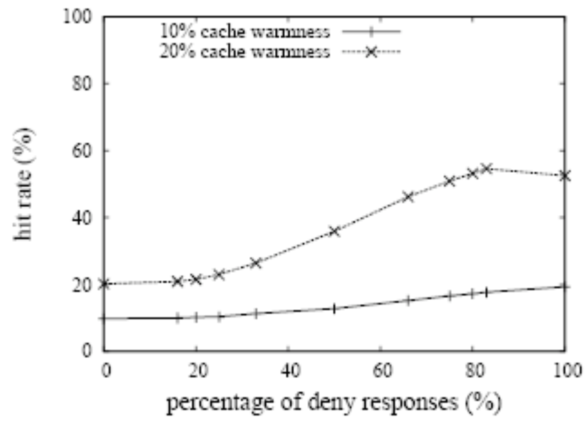
100 subjects, 1000 objects, 50 roles



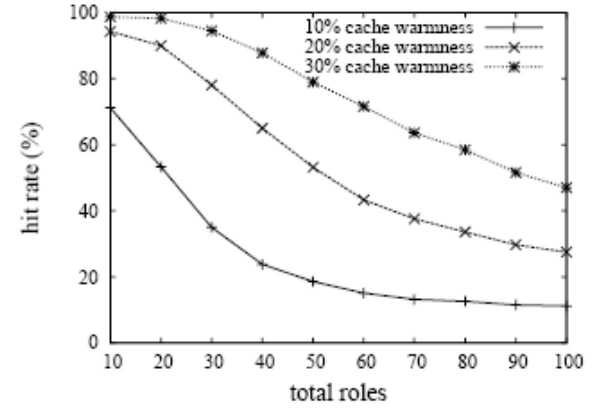
the impact of various system parameters



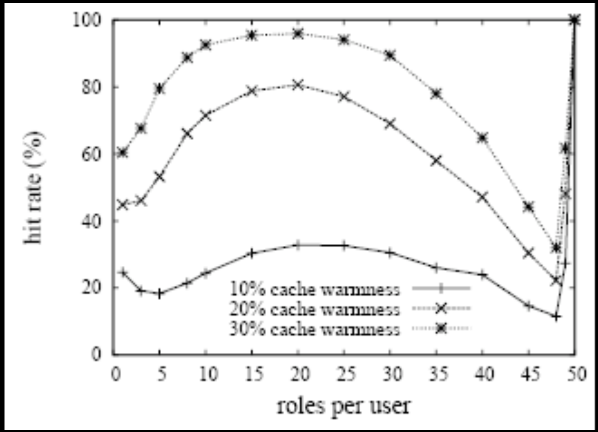
total users



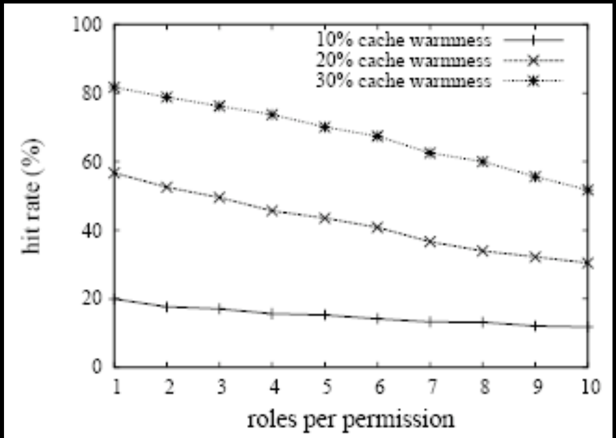
deny responses



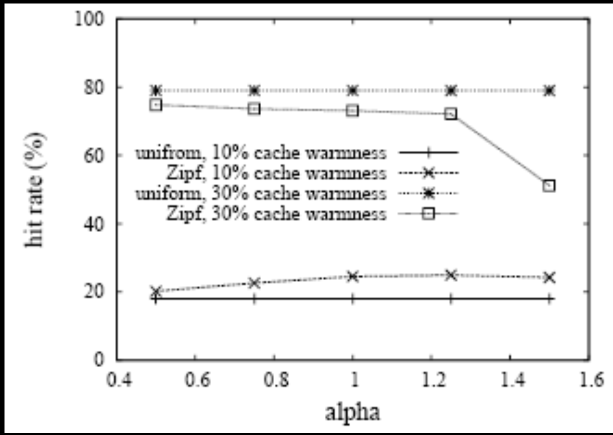
total roles



roles per user



roles per permission

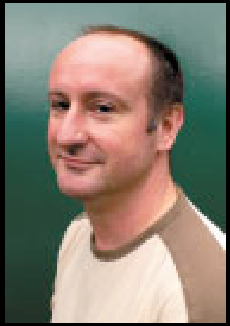


request distribution

project team

Qiang Wei

Matei Ripeanu



Jason Crampton
Information Security
Group at Royal Holloway
University of London

Kosta Beznosov

SQLPrevent

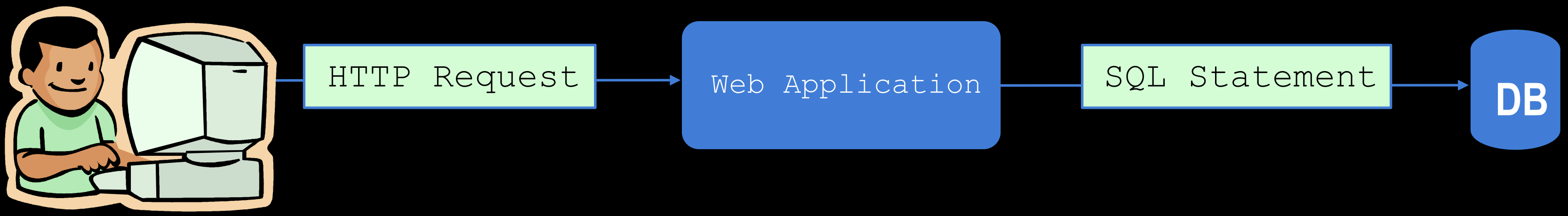
Effective Dynamic Detection and Prevention of SQL Injection Attacks Without Access to the Application Source Code

OWASP top 10 web security threats

1. Cross Site Scripting
2. SQL Injection
3. Malicious File Execution
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Information Leakage and Improper Error Handling
7. Broken Authentication and Session Management
8. Insecure Cryptographic Storage
9. Insecure Communications
10. Failure to Restrict URL Access

source: http://www.owasp.org/

how SQL injection attack (SQLIA) works



HTTP Request

Web Application

SQL Statement

DB

HTTP Request

```
POST /prodcut.aspx HTTP/1.1
product_id=2 ; SHUTDOWN
```

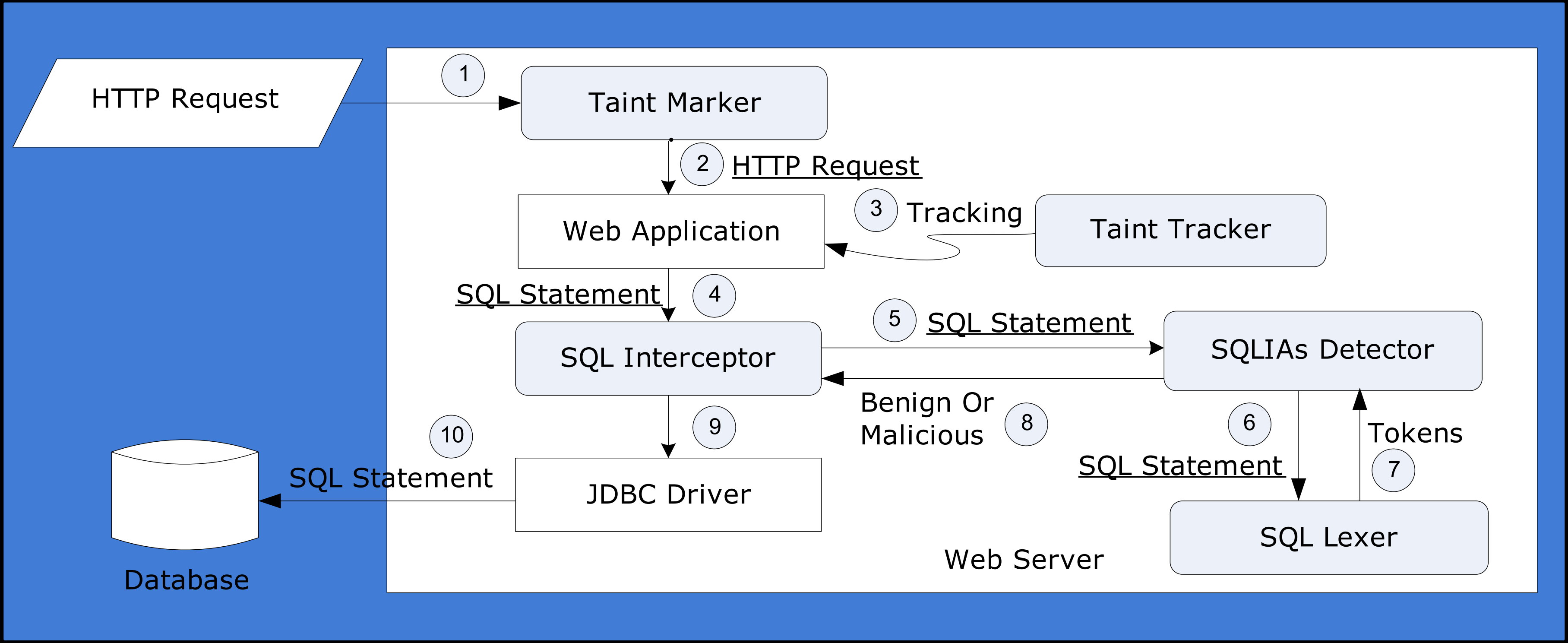
Web Application Program Logic

```
"SELECT * FROM product WHERE id="+ request("product_id")
```

SQL Statement

```
SELECT *  FROM product WHERE id=2 ; SHUTDOWN
```

System Architecture



Resulted SQL Statement: sql

```
Update books set book_name='UPDATE',
price= 1000
WHERE book_id=123
```

Tainted Data must only appear in literal

performance overhead

subject	overhead (%)			
	detection		**prevention**	
	Avg	Std Dev	Avg	Std Dev
Bookstore	0.8	0.4	2.7	1.0
Employee	1.3	0.7	3.1	1.1
Classifieds	1.0	0.4	2.6	0.8
Events	2.1	0.6	2.7	1.2
Portal	1.7	0.4	2.0	0.7
Average	**1.4**	**0.5**	**2.6**	**0.8**

SQLPrevent with dynamic taint analysis

- Reduces false positives and false negatives
- Imposes low performance overhead
- Requires no access to application source code
- Enables easy deployment by two config. changes

project team

San-Tsai Sun

Kosta Beznosov

summary

Why (Managing) IT Security is Hard

- HOT Admin

Some Ideas for Making It Easier

- JAMES
- SQLPrevent

lersse.ece.ubc.ca