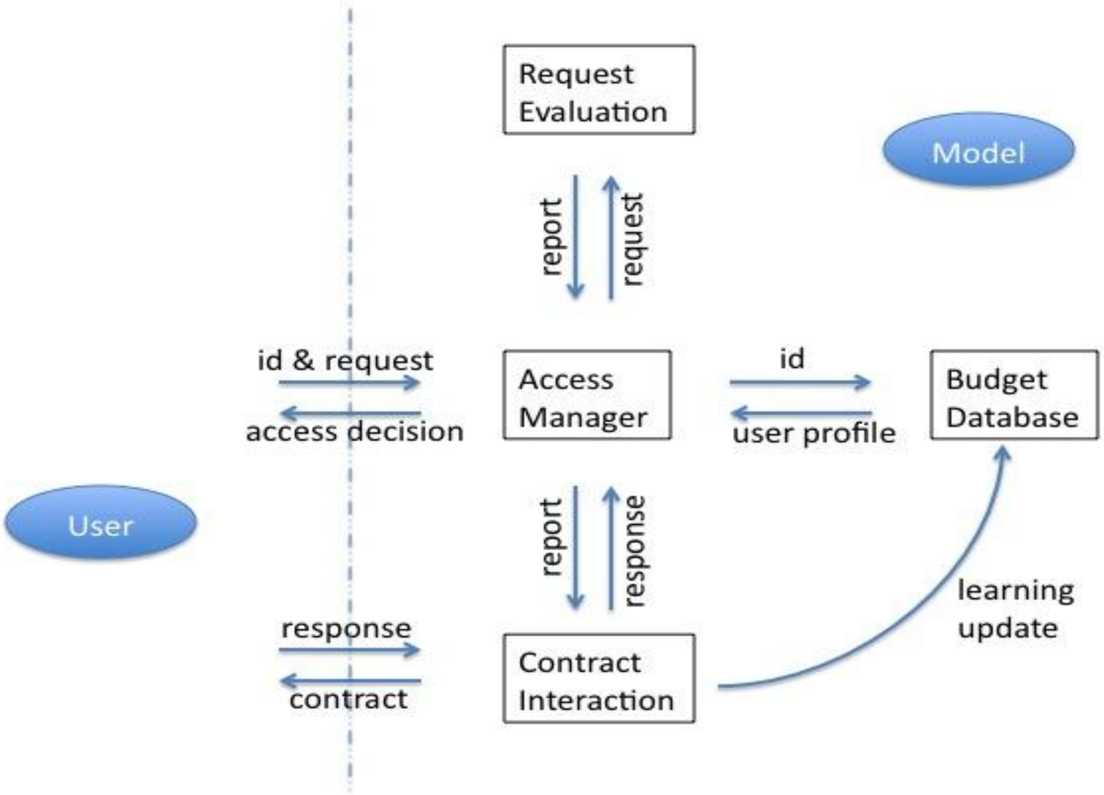
Bring Incentives to Access Control

Debin Liu, L. Jean Camp, and XiaoFeng Wang
School of Informatics and Computing
Indiana University

Goal

- Risk- and Incentive-Based (RIB) Access Control model
    - Regulate users' purposeful risky behavior
    - Limit aggregated risk
    - Prevent risk-generating human errors
    - Incentivize users for low-risk accesses

Model Structure



Incentive Contract

- A contract provides two things:
  - the price in allowance points that the user should pay for the access request,
  - The reward tokens the user can receive by performing some risk-mitigating behavior.

- The reward of performing risk-mitigating behavior, *r*, could be a function of
  - risk-mitigating behavior *r(e)*,
  - generated risk consequence *r(k)*.

Risk-Mitigating Behaviors

- Denoted as *e*.
- Include technical behaviors and knowledge on
    - risk mitigation,
    - fraud identification,
    - security control,
    - data protection,
    - resource management,
    - and etc.

Effort-Based Contract

- A contract based on risk control efforts level
  - *r(e)*
  - requires that the organization has the ability to observe and verify user's risk-mitigating behaviors;
  - can induce the user to put forth the efficient risk-mitigating behaviors without incurring extra costs.

Game Equilibrium

- RIB model proposes a contract ***r***, while a user chooses an optimal ***e***, such that the following equations are satisfied

$$\min_{e}[c(e) - r(e)]$$

$$\min_{r}[k(e) + r(e)]$$

- The contract and selection of ***e**** form a Nash Equilibrium in the contract game.

Consequence-Based Contract

- A contract based on consequence
  - *r(k)*
  - Organizations are sometimes capable of observing the outputs and consequence of users' activities.
  - The consequence *k* is a noisy signal of the risk-mitigating behaviors.

Game Equilibrium

- User will choose an ***e*** that minimizes

$$c(e) - \sum_{1 \leq i \leq n} p_i(e) r(t_i)$$

- Organization needs to generate a contract ***r*** such that the user's optimal choice will minimizes

$$\sum_{1 \leq i \leq n} p_i(e) k(t_i) + \sum_{1 \leq i \leq n} p_i(e) r(t_i)$$

Preliminary Experimental Evaluation

- Three rounds of human-subject experiments

- The 1st round
  - as benchmark
- The 2nd round
  - Controlled by effort-based contract incentive mechanism
- The 3rd round
  - Controlled by consequence-based contract incentive mechanism

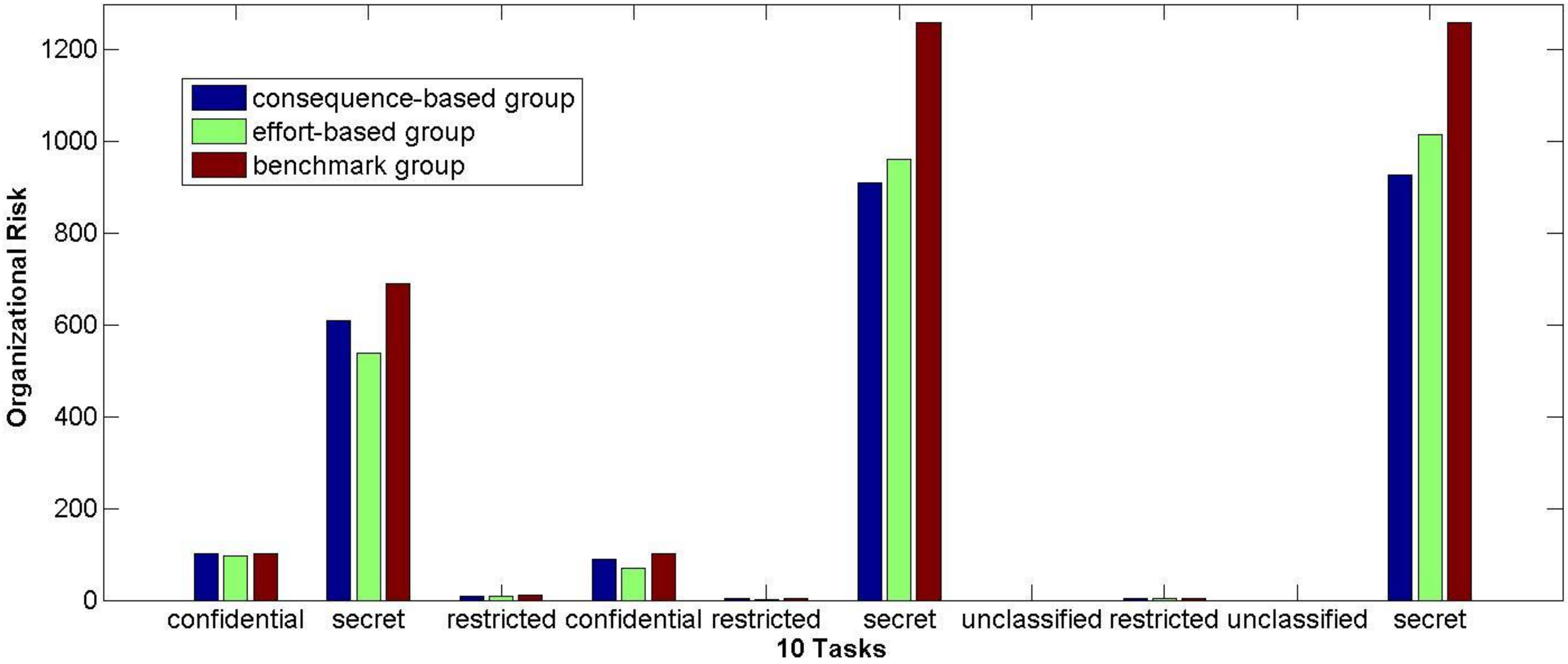
Recruitment

- 36 participants
- Voluntarily recruited
- Randomly and equally assigned into three groups
- An interesting finding from background survey:
  - 61% of the participants chose to scan their personal computers immediately upon seeing a virus warning,
  - while only 52% did so to their organization's computers.
  - This echoes the hypothesis about the existing misalignment between employees' incentives and their organizations' interests.

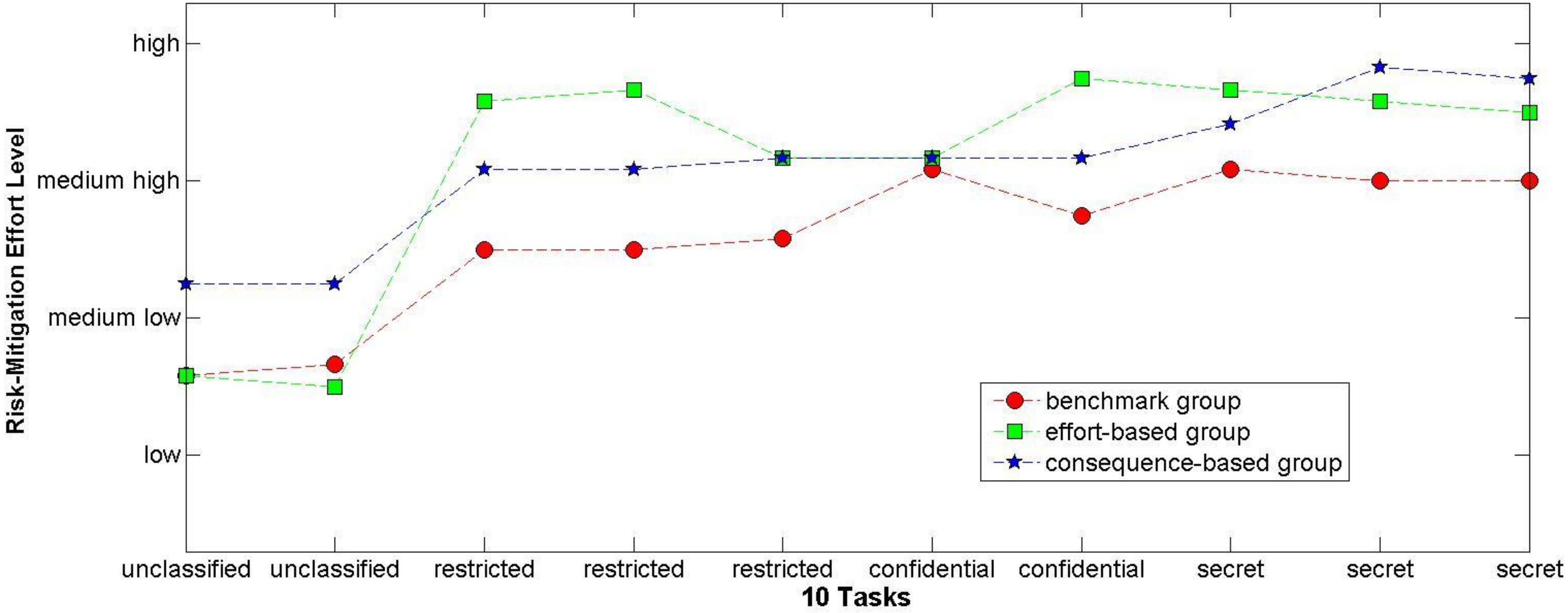
Task Descriptions

- Sending ten documents, each of which was attached to a different email;
- Participants were told that with a certain probability, these emails could be intercepted by untrusted parties.
- They were suggested, but not required, to encrypt the emails or the documents, or both:
  - encrypting both email and document as the high level risk-mitigating behavior (Level 3),
  - encrypting only the document as the medium high level risk-mitigating behavior (Level 2),
  - encrypting only the email as the medium low level risk-mitigating behavior (Level 1),
  - no encryption as the low level risk-mitigating behavior (Level 0).

Organization's Risk Postures



Average Personal Risk-Mitigating Behavior Levels


high
medium high
medium low
low
Risk-Mitigation Effort Level
unclassified
unclassified
restricted
restricted
restricted
confidential
confidential
secret
secret
secret
10 Tasks
● benchmark group
■ effort-based group
★ consequence-based group