

# MITIGATING INADVERTENT INSIDER THREATS WITH INCENTIVES

Debin Liu  
XiaoFeng Wang  
L. Jean Camp

School of Informatics  
Indiana University

# Insiders

- ▣ within an organization
- ▣ with legitimate access to organizational resources
- ▣ e.g. an employee, contractor, consultant, or any person who has a relationship with or position of trust within the organization

# Statistics

- ▣ US companies lose 5% of their annual revenues to internal fraud <sup>1</sup>
- ▣ Half of survey participants experienced an insider incident <sup>2</sup>
- ▣ 80% of publicized data breaches <sup>3</sup>
- ▣ 91% of global financial services firms were concerned about insider threats <sup>4</sup>
- ▣ \$7.2 billion in fraudulent trades by a rogue insider <sup>5</sup>

# Insider Type

## ▣ Malicious Insiders

- the individuals with varying degrees of malicious intent to cause harm
- motivated by seeking profit

## ▣ Inadvertent Insiders

- do not have malicious intent
- do not responsibly manage security
- most IT experts agree that most leaks of information and security breaches are not criminal but the result of accidents and human errors <sup>6</sup>



# Research Goal

- ▣ Design a risk management mechanism using incentive engineering
  - align incentives between users and organization
  - encourage the users to self-manage their risks
  - discourage the users against risky actions
  - mitigate the inadvertent insider threats

# Scenario

- ▣ An inadvertent insider
- ▣ Use company resources
- ▣ Download a football screensaver
- ▣ Two websites with different risk rating
- ▣ Warning pop-up for the risky website
  
- ▣ Inadvertent insider only motivated by his personal gain

# Core Problem

- ▣ Risk communication not effective
- ▣ The incentives are incorrectly aligned for the inadvertent insider
  - incentive engineering
  - shift the cost of risk

# Risk Budget Mechanism

- ▣ Every user is assigned a bucket of risk points
- ▣ A risky activity will cost him some points
- ▣ User gets punishment, if
  - run out of budget before having task done
- ▣ Or user gets reward, if
  - job done before using up his points
  - the more points surplus the more rewards



# Budget Assignment

- ▣ Budget size determined
  - by the organization
  - based on
    - ▣ task description
    - ▣ organization's preference
    - ▣ user's access rights
    - ▣ user's security preference
- ▣ Budget size implies a risk limit

# Points Payment

- ▣ Inadvertent insiders only take actions based on their privileges and access
- ▣ Organization knows all the possible actions a user can take
- ▣ Organization can associate a risk rating with each action

# Punishments

- ▣ An incentive against risk-seeking behaviors
- ▣ Enforced by the organization
- ▣ Triggered by the risk budget exhaustion
- ▣ In the form of
  - an audit
  - a mandatory training program
  - a loss of access
- ▣ Translate exhausted budget into a cost

# Rewards

- ▣ A measure to reward the user
  - The fewer risk points consumed the more rewards the user will get
- ▣ In the form of
  - more access
  - monetary award
  - symbolic award
  - welfare
    - ▣ accumulated
    - ▣ redeem



# In Practice

- ▣ An employee
  - Internet surfing
  - documents downloading
    - ▣ a daily risk budget  $B$
    - ▣ spend  $p_j$  to visit a website  $w_j$  that costs  $p_k$  to perform the downloading
    - ▣ spend  $p'_j$  to visit another website  $w'_j$  that costs  $p'_k$  to download
    - ▣  $p_j, p_k, p'_j$  and  $p'_k$  are set by the organization based on its perception and evaluation of potential risks
    - ▣ assuming  $B > (p_j + p_k) > (p'_j + p'_k)$
    - ▣ we expect she voluntarily chooses the second website, which incurs lower risks, under our risk budget mechanism

# Experimental Configuration

- ▣ Two human-subject experiments
  - based on a firefox browser extension
- ▣ The 1<sup>st</sup> experiment
  - as benchmark
  - to understand users' risk behaviors
- ▣ The 2<sup>nd</sup> experiment
  - to study the change of risk behaviors

# Recruitment

- ▣ 40 participants
- ▣ Voluntarily recruited from the undergraduates at Indiana University
- ▣ Randomly and equally divided into two group
- ▣ None of them have majors in computer related fields

# Task Descriptions

1. Search for the websites offering free screen savers downloads from the web
2. From the search results, choose five websites: website-1, website-2, website-3, website-4 and website-5
3. From website-1, please take a screenshot of an animal screensaver
4. From website-2, please take a screenshot of a nature screensaver
5. From website-3, please take a screenshot of a sport screensaver
6. From website-4, please take a screenshot of a space screensaver.
7. From website-5, please take a screenshot of a flower screensaver.
8. Thank you. You have completed the experiment



# Website Rating

- ▣ Those that have been previously visited are trusted
- ▣ Those that have not been previously visited are considered untrusted
- ▣ The ratings of an untrusted website comes from McAfee SiteAdvisor

# Experiment One


Screensavers – The Very Best from screensaver.com: Free and Custom Developed Screen Savers

http://www.screensaver.com

Latest Headlines

**[JavaScript Application]**  
The website you are trying to visit is considered risky.  
Are you willing to continue?

Cancel OK

 **Nothing but the best!**

NEW RELEASES SPECIAL PICK MOST POPULAR SEASONAL FAVORITES SCREENSAVER LIBRARY


Search Screensavers  Search

[Tech Support](#) | [Contact Us](#) | [About Us](#) | [Links](#) | [Free Games](#) [Club Log-In](#)


## Screensaver Favorites

Featured Screensaver

**Living 3D Dolphins**

 Swim with the dolphins in this deep sea adventure! This free

**3D Falling Leaves**

 Watch as your cares drop away like the brilliantly colored leaves

**PLAY FREE Games on Your Desktop!**

# Experiment Two

- ▣ 20 participants completed the same task under the additional constraint of their risk budgets
- ▣ If they successfully accomplished their tasks
  - receive \$10 plus a bonus
  - bonus based on the remaining risk points
- ▣ If any participant exhausted a risk budget
  - compensation forfeited
- ▣ If any participant failed to complete the experiment in time allowed
  - compensation forfeited


# Experiment Two

Screensavers | Download Free Screensavers

http://www.a

g Started Latest Headlines Get

**Halloween Screensavers**  
Get free Halloween screensavers  
Choose from 1000's of screensavers  
AllHalloweenScreensavers

 **[JavaScript Application]**  
The website you are trying to visit is considered risky.  
This visit to this website will cost 18 risk points.  
Are you willing to pay these 18 risk points to continue?

Ads by Google

**Download Free Screensavers**

[Home](#) | [Seasonal](#) | [What's New](#) | [Bookmark](#) | [Make Your Own](#) | [Free Content](#) | [Link To Us](#) | [Get The Klip](#) | [Advertise With Us](#)  
**Top Screensavers:** [Christmas](#) | [The Matrix](#) | [Thanksgiving](#) | [3D](#) | [Hot](#) | [Living Aquarium](#)

**Screensavers**  
:: [Cartoons](#)  
:: [Models](#)  
:: [3D](#)  
:: [Celebrities](#)  
:: [People](#)  
:: [Anime](#)  
:: [Fantasy](#)  
:: [Sports](#)

No matter what type of screensavers you're looking for, you'll find it here, among our comprehensive free screensaver listings. If you're weary of the lame, boring default screensavers that came with your computer, then try one of the many dazzling free screensavers we offer here. [Click Here](#) to bookmark our site in Internet Explorer or press **Ctrl+D** in Netscape!

[Free Screensavers](#)  
The Best Free Screensavers Site - Download 1000's Of

**Screensaver Search**  
enter keywords

**Live Saver Search**

**Top 10 Searches**  
[fairys](#)

**Top Downloads**  
[Living 3D Waterfalls 3.0](#)  
[Living 3D Dolphins](#)  
[Living Marine Aquarium 2](#)  
[Lightning Storm 3D](#)



# Firefox Browser Extension

1. Detect a new page being loaded;
2. Check the domain name of a webpage;
3. Maintain a list of target high risk websites and their reputations;
4. Pop up a warning message when a high risk website was about to be visited;
5. Ask for confirmation or rejection of the visit choice from the participant;
6. Record the experimental results;

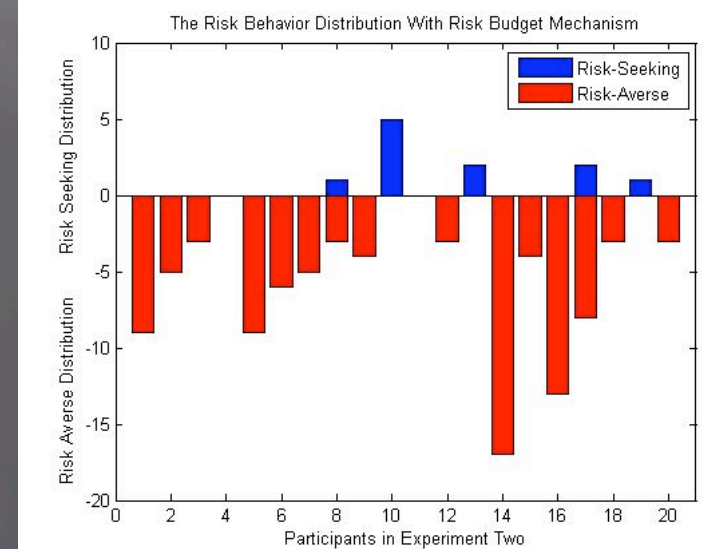
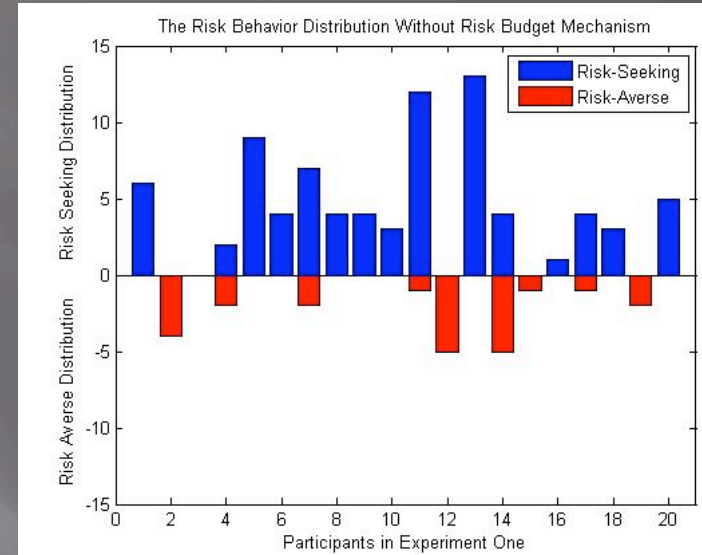
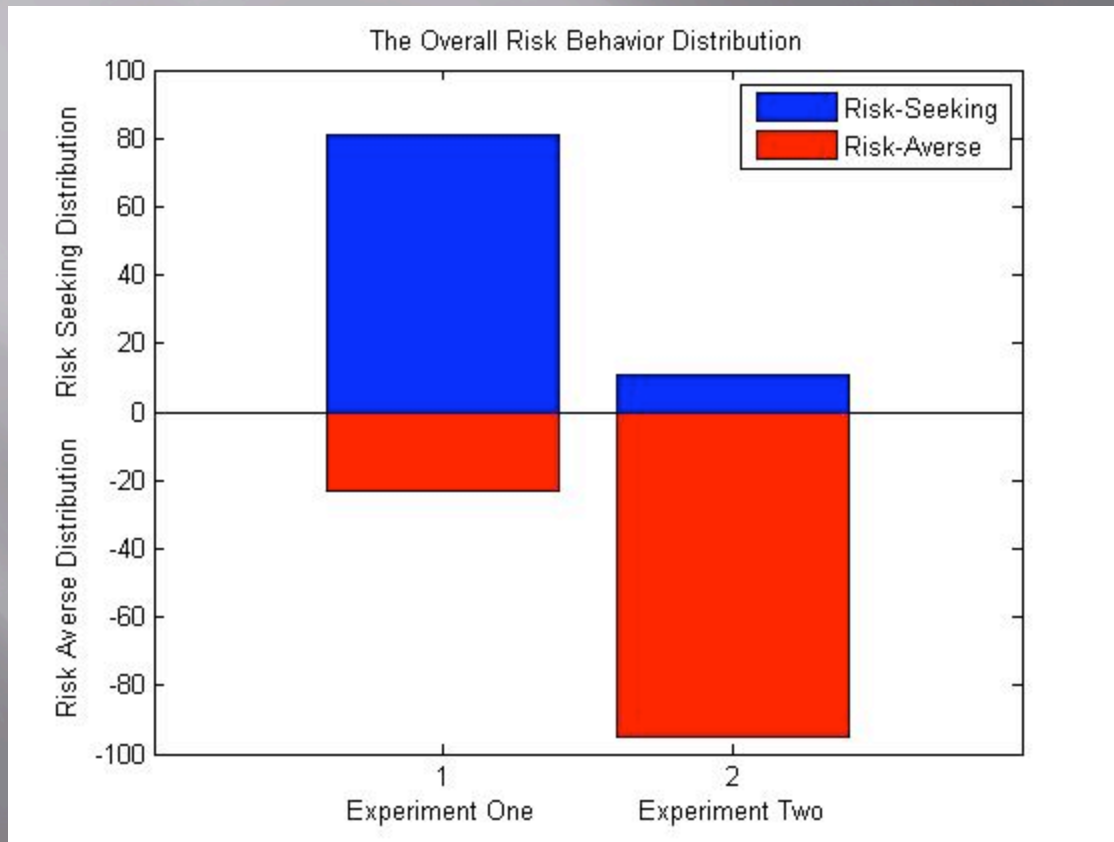
(In experiment two, the extension also took the following actions:)

7. Generate a price based on a website's reputation;
8. Track participants risk budgets balance.

# Data

- ▣ 1<sup>st</sup> experiment
  - 104 pop-up warning messages
  - 81 risk-seeking decisions
  - 23 risk-averse decisions
- ▣ 2<sup>nd</sup> experiment
  - 106 pop-up warning messages
  - 11 risk-seeking decisions
  - 95 risk-averse decisions

# Risk Behaviors



# Risk Boundary

- ▣ 2<sup>nd</sup> experiment
  - 11 risk-seeking behavior responses
  - average payment was 16 pts
- ▣ 1<sup>st</sup> experiment
  - assuming 16 pts cost
  - 20% participants could exhaust their budget
- ▣ Incentives
  - effectively motivate users against abuse of their privileges
  - help establishes a boundary for organization



# Regulation Friction

- ▣ Regulation friction
  - the efforts made by the users to adopt a risk-averse strategy instead of a risk-seeking strategy
- ▣ Measured this regulation friction using time interval for completing the task
  - 1<sup>st</sup> experiment      5:45
  - 2<sup>nd</sup> experiment      6:00
  - Regulation friction of 4.3% of the time committed in experiment one

# Game Theoretic Analysis

	Risk-Seeking	Risk-Averse
No Reward	$(-P_1, 0)$	$(-P_2, -C)$
Reward	$(-P_1-R_1, R_1)$	$(-P_2-R_2, R_2-C)$

- ▣  $P_1$ : the cost to the organization when a risk-seeking adopted
- ▣  $P_2$ : the cost to the organization when a risk-averse adopted
- ▣  $P_1 > P_2$
- ▣  $R_1$ : the reward to the user when a risk-seeking strategy is adopted
- ▣  $R_2$ : the reward to the user when a risk-averse strategy is adopted
- ▣  $R_1 < R_2$
- ▣  $C$ : the friction between the risk-seeking and the risk-averse strategy

# Game Solution and Application

- ▣  $R_1 < R_2 - C$  must hold
- ▣ (*reward, risk averse*) as equilibrium strategy in the repeated game
- ▣ It's critical to determine the parameters
  - $C$  could be estimated from time difference observation
  - adjust the incentive functions and monitor the risks, until the risk behavior distribution becomes acceptable

# Conclusion and Future Work

- ▣ Inadvertent insiders pose a grave security threat
- ▣ we propose a risk budget mechanism that encourages insiders to behave in a manner aligned with interest of the organization
- ▣ experiment results
  - impacts on rational users' risk attitudes
  - evidently shifts their behaviors
- ▣ in the future
  - study the effectiveness of our approach beyond the scenario of web browsing
  - explore the possibility of combining the idea of risk budgeting with existing access control mechanisms



# References

1. *State CIOs Take Action Now!* The National Association of State Chief Information Officers, 2007.
2. *The 2007 Ecrime Watch Survey*. CMU Software Engineering Institute. 2007.
3. *The report of the Association of Certified Fraud Examiners*. 2006.
4. *Insider Threats Remain IT's Biggest Nightmare*. Infoworld, September 22, 2007.
5. *Notes on a Scandal: Lessons in Operational Risk Management from Societe Generale*. Diamond Management and Technology Consultants Financial Services Practice. 2008.
6. *Homeland Defense Journal*. 2007.

Thank you for your time!

Questions?