



# Information Assurance Projects in UB- School Of Management





# Information Assurance Laboratory



## Overview

- The Information Assurance Laboratory is made up of three distinct computer labs
  - Security Lab, Networking Lab, Forensics Lab
- Students have an opportunity to learn about Information Assurance in a hands-on learning environment in these labs



## Lab Hardware Infrastructure

- (4) Dell PowerEdge Servers
- (16) Windows XP / Linux Workstations
- Dedicated Intrusion Detection System, Web Server, Domain Controller and DHCP server
- Cisco Switches, Routers and Security Device`s
- (3) Forensics investigation workstations

# Education and Community Outreach



- High School Cybersecurity Workshops have been periodically held for local high school students with the purpose of:
  - Educating students about the challenges of computer security and how those challenges can be overcome
  - Encouraging students to further pursue academic studies and careers in Information Assurance

# High School Cybersecurity Workshops

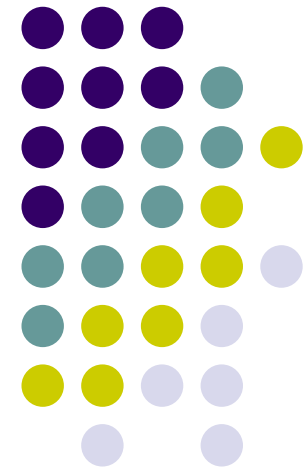


- Workshops have been held for 75 students from local high schools over the past year.
- Hands on activities and live security demonstrations are presented to the students in the Information Assurance Lab.
- Workshops will be adapted for middle school age students in the upcoming year

# AN EXTREME VALUE APPROACH TO INFORMATION TECHNOLOGY SECURITY INVESTMENT

---

Jingguo Wang  
Aby Chaudhury  
H. Raghav Rao



Reference: Wang, J., A. Chaudhury, R. Rao. 2005. "An Extreme Value Approach for Security Investment." *In the Proceedings of The International Conference on Information Systems (ICIS)*, Las Vegas, December 2005.



# Introduction

- Information technology security investment is receiving increasing attention in recent years (Gordon et al. 2005).
- How to efficiently invest in IT security is a big challenge (Ernst & Young 2003, 2004).
- Quantification tools, if applied prudently, can assist in the anticipation and control of direct and indirect computer security cost (Geer et al. 2003; Mercuri 2003).
- In this paper, we propose an approach based on extreme value theory (Gumbel 1958) for IT security investment.



## Related Literature

- There are basically two approaches to determine the effective level of security investment (Cavusoglu 2004).
  - Using traditional risk or decision analysis framework (Gordon and Loeb 2002; Hoo 2000; Longstaff et al. 2000)
  - Using game theory to model the strategic interactions between the organizations and attackers (Schechter and Smith 2003; Longstaff et al. 2000; Cavusoglu, et al. 2004)
- Issues with these models
  - The expected loss value or benefit value cannot fully characterize security failures.
  - Rationality of hackers is hard to capture as they may be motivated by a different value system.



## A Two-Factor Security Model

- The security status of a system ( $\mathcal{F}$ ) depends on:
  - system security level, which is endogenous and measure by the level of security investment  $i$ .
  - system attack level  $a$ , which is exogenous and reflects the risk with which the system confronted.
- $\mathcal{F}$  = probability of system failure = prob. ( $i - a < v$ ),  $v$  is a certain threshold of vulnerability.
- The firm follows a dynamic investment strategy:  $i=i(a, \mathcal{F})$



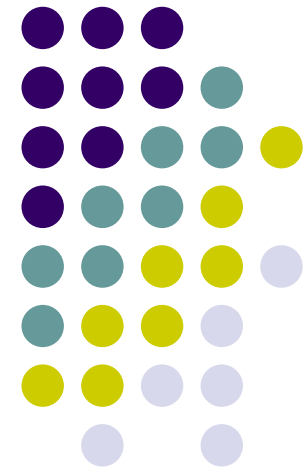
# The Extreme Value Theory

- One of the key requirements for such a dynamic investment strategy is to accurately capture and model the dynamic behavior of attacks.
- By using the extreme value theory, we attempt to address the following issues:
  - What is the probability distribution of high-level attacks (i.e., what is the probability that an attack over a given level will occur during a given year)?
  - What security investment is needed so that the probability of potential system failure is below a certain threshold?
  - What are the factors affecting the behavior of high-level attacks? Are the nature and causes of high-level attacks changing over time? Is it a seasonal phenomenon?

# The Influence of the Physical and Virtual Environment on Transactional Web Usage

---

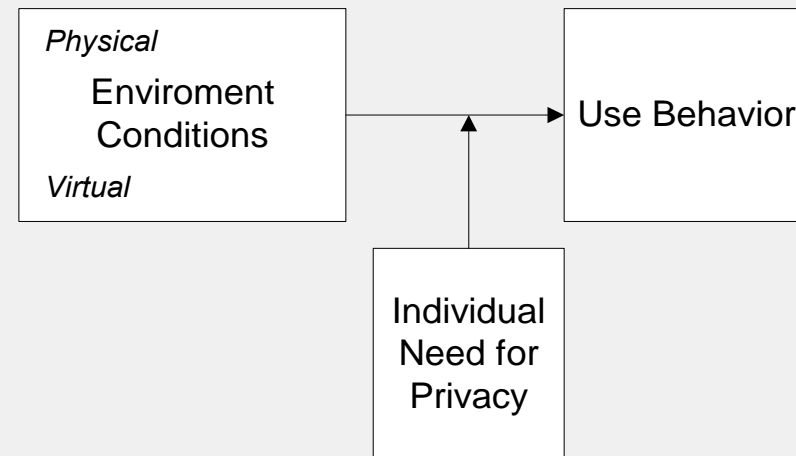
A.D. Rensel, J.M. Abbas, H.R. Rao  
(under review in Journal of AIS; earlier  
version in Proceedings of HICSS)



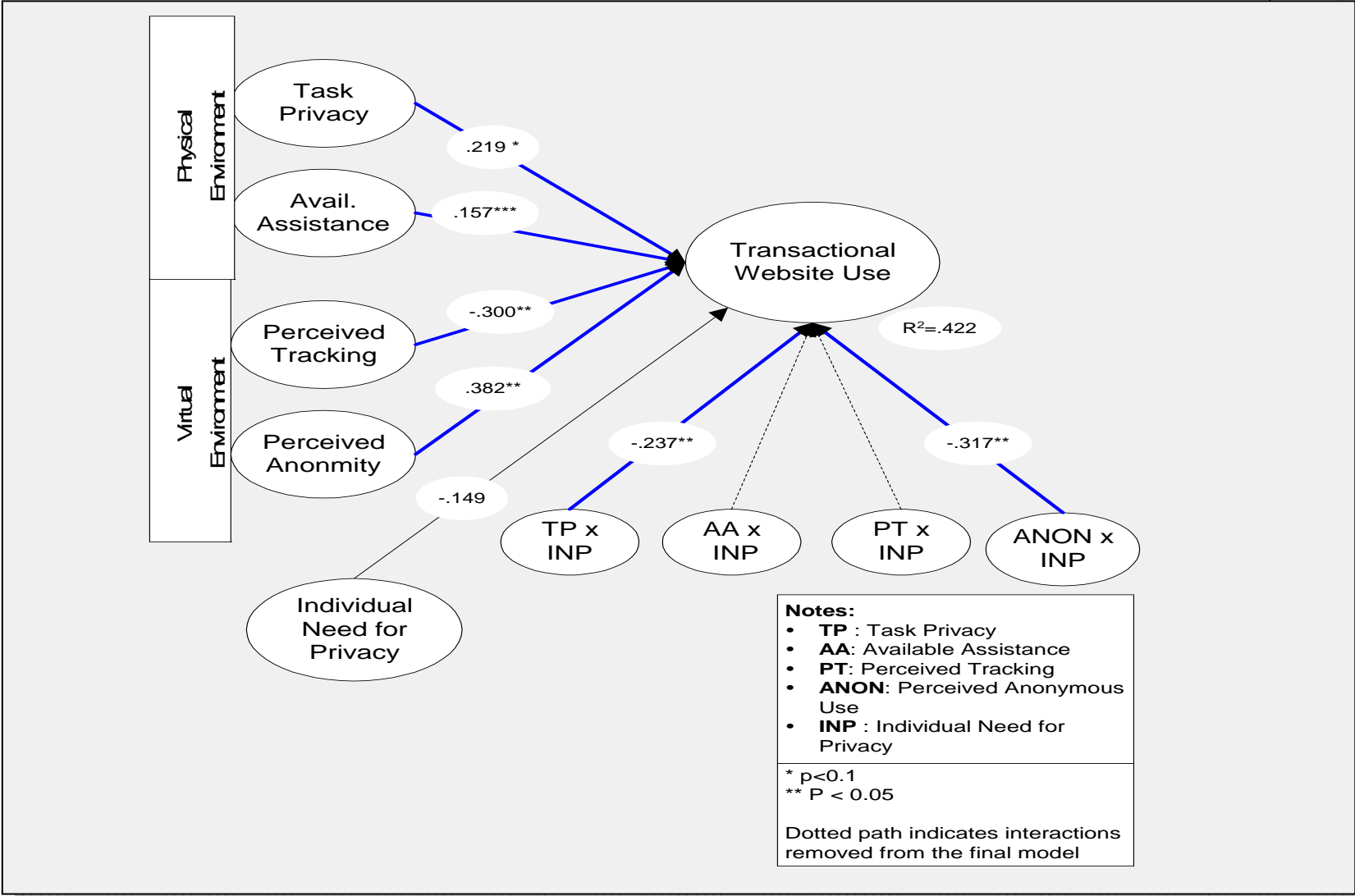


# Introduction

- We are considering the impact of an individuals' perceptions of
  - Physical Environment
  - Virtual Environmenton transactional website use activities.
- Further, we consider the influence of the individual's need for privacy on these relationships.



# Research Model & Results



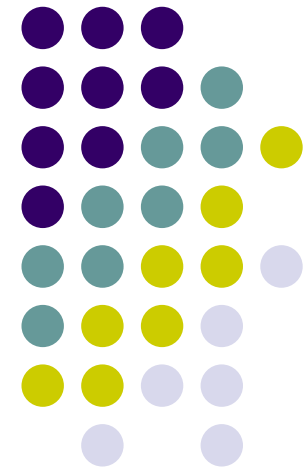
# Conclusions



- Elements in the physical and virtual environment impact public usage behavior
  - Perceived task privacy supports public transactional use
  - Perceived tracking tends to deter public transactional use
  - Perceived anonymity supports public transactional use
- The individual need for privacy (INP) moderates the effect of the environment on transactional use
  - INP decreases the influence of task privacy on transactional use
  - INP decreases the effect of perceived anonymity on transactional use

# Security Protection Design for Honeypot Systems: A Model and Analysis

Chungsuk Ry, H.R. Rao, R. Sharman and  
S. Upadhyaya



An earlier version of this presentation was presented at Web 2004: the Third Workshop on e-Business on December 11th, 2004.



# Introduction

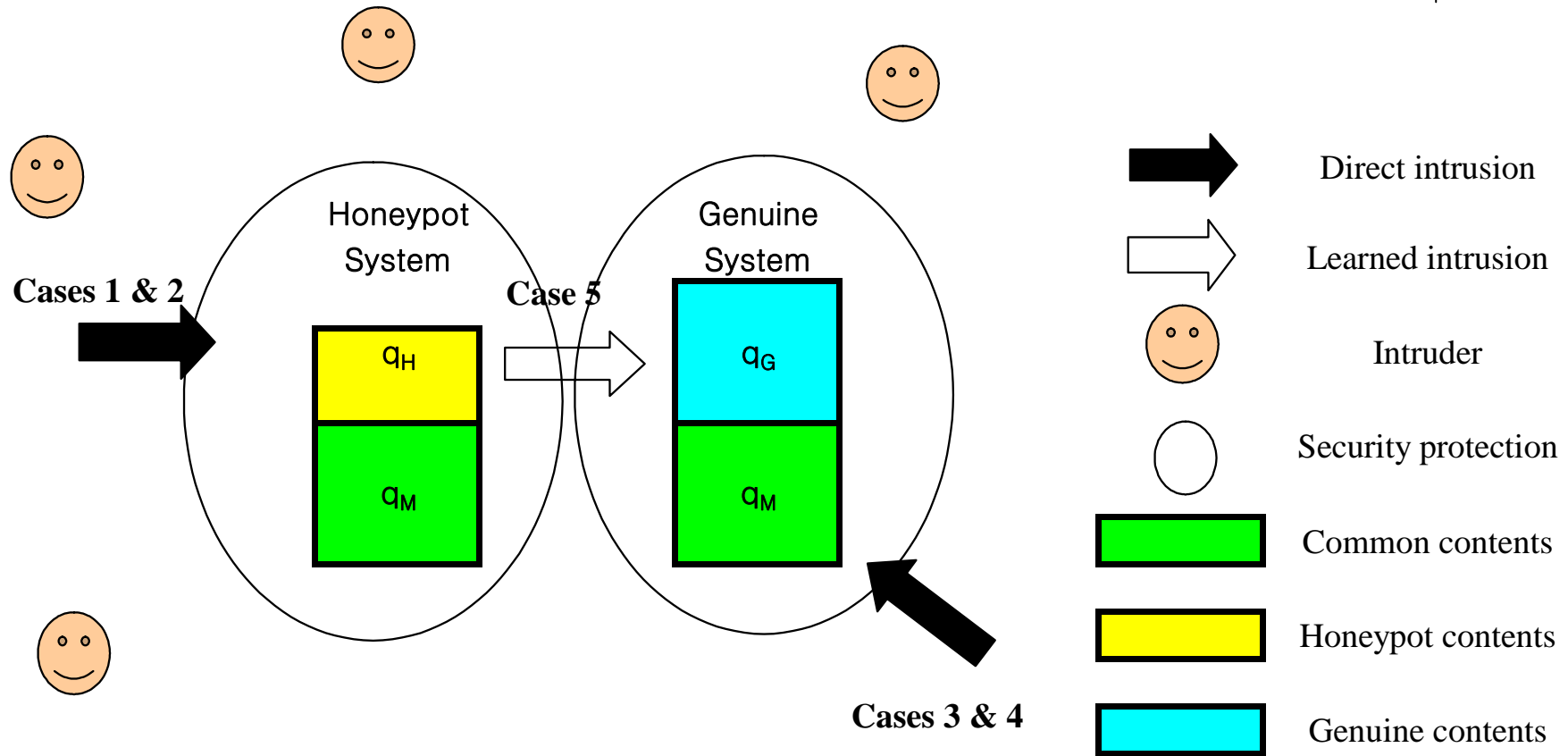
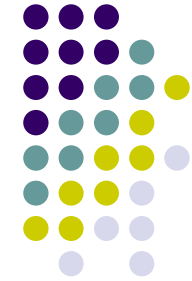
## Research focus

- Importance of information security: technology, intruder's behavior, and economics
  - **Technology**: decoy information system
  - **Intruder's behavior**: intruders' behaviors to enter the information system
  - **Economics**: incentives of the system designer and intruders

## Research objectives

- Examine the intruders' behaviors of invasion into the information system under their own economic incentives
- Analyze the role of the decoy system in protection of the entire information system
- Provide optimal decisions that indicate how the system designer should design the protection of the information system in order to achieve optimal economic performance

# Honeytrap System and Security Management





# Intruder's Behaviors and Profits

Cases	$t = 1$	$t = 2$	Profits
Case 1	Enter the honey-pot system	Do nothing	$v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right)$
Case 2	Do nothing	Enter the honey-pot system	$\rho \cdot \left[ v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H2}}{q_H} + \frac{P_{M2}}{q_M} \right) \right]$
Case 3	Enter the genuine system	Do nothing	$v_G \cdot (q_G + q_M) - e_G \cdot \left( \frac{P_{G1}}{q_G} + \frac{P_{M1}}{q_M} \right)$
Case 4	Do nothing	Enter the genuine system	$\rho \cdot \left[ v_G \cdot (q_G + q_M) - e_G \cdot \left( \frac{P_{G2}}{q_G} + \frac{P_{M2}}{q_M} \right) \right]$
Case 5	Enter the honey-pot system	Enter the genuine system	$v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right)$ $+ \rho \cdot \left[ v_G \cdot (q_G) - e_G \cdot \left( \frac{P_{G2}}{q_G} + \frac{(P_{M2} - P_{M1})}{q_M} \right) \right]$



# Economic Model for Security Management

$$\begin{aligned}
 \text{Maximize}_{P_{H1}, P_{H2}, P_{G1}, P_{G2}, P_{M1}, P_{M2}} \pi = & n_{H1} \cdot e_H \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right) - \left[ c_H \cdot \left( \frac{P_{H1}}{q_H} \right)^2 + c_M \cdot \left( \frac{P_{M1}}{q_M} \right)^2 \right] \\
 & + n_{G1} \cdot e_G \cdot \left( \frac{P_{G1}}{q_G} + \frac{P_{M1}}{q_M} \right) - \left[ c_G \cdot \left( \frac{P_{G1}}{q_G} \right)^2 + c_M \cdot \left( \frac{P_{M1}}{q_M} \right)^2 \right] \\
 & + \sigma \cdot \left\{ n_{H2} \cdot e_H \cdot \left( \frac{P_{H2}}{q_H} + \frac{P_{M2}}{q_M} \right) - \left[ c_H \cdot \left( \frac{P_{H2}}{q_H} \right)^2 + c_M \cdot \left( \frac{P_{M2}}{q_M} \right)^2 \right] \right. \\
 & \left. + n_{G2} \cdot e_G \cdot \left( \frac{P_{G2}}{q_G} + \frac{P_{M2}}{q_M} \right) - \left[ c_G \cdot \left( \frac{P_{G2}}{q_G} \right)^2 + c_M \cdot \left( \frac{P_{M2}}{q_M} \right)^2 \right] \right\} \quad (1)
 \end{aligned}$$

subject to

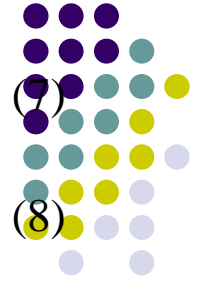
$$v_H \cdot (q_H + q_M) \geq e_H \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right) \quad (2)$$

$$v_H \cdot (q_H + q_M) \geq e_H \cdot \left( \frac{P_{H2}}{q_H} + \frac{P_{M2}}{q_M} \right) \quad (3)$$

$$v_G \cdot (q_G + q_M) \geq e_G \cdot \left( \frac{P_{G1}}{q_G} + \frac{P_{M1}}{q_M} \right) \quad (4)$$

$$v_G \cdot (q_G + q_M) \geq e_G \cdot \left( \frac{P_{G2}}{q_G} + \frac{P_{M2}}{q_M} \right) \quad (5)$$

$$v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right) + \rho \cdot \left\{ v_G \cdot (q_G) - e_G \cdot \left[ \frac{P_{G2}}{q_G} + \frac{(P_{M2} - P_{M1})}{q_M} \right] \right\} \geq 0 \quad (6)$$



$$v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right) \geq v_H \cdot (q_G + q_M) - e_H \cdot \left( \frac{P_{G1}}{q_G} + \frac{P_{M1}}{q_M} \right)$$

$$v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right) \geq \rho \cdot \left[ v_H \cdot (q_G + q_M) - e_H \cdot \left( \frac{P_{G2}}{q_G} + \frac{P_{M2}}{q_M} \right) \right]$$

$$v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H2}}{q_H} + \frac{P_{M2}}{q_M} \right) \geq v_H \cdot (q_G + q_M) - e_H \cdot \left( \frac{P_{G2}}{q_G} + \frac{P_{M2}}{q_M} \right)$$

$$\rho \cdot \left[ v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H2}}{q_H} + \frac{P_{M2}}{q_M} \right) \right] \geq v_H \cdot (q_G + q_M) - e_H \cdot \left( \frac{P_{G1}}{q_G} + \frac{P_{M1}}{q_M} \right)$$

$$v_G \cdot (q_G + q_M) - e_G \cdot \left( \frac{P_{G1}}{q_G} + \frac{P_{M1}}{q_M} \right) \geq v_G \cdot (q_H + q_M) - e_G \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right)$$

$$v_G \cdot (q_G + q_M) - e_G \cdot \left( \frac{P_{G1}}{q_G} + \frac{P_{M1}}{q_M} \right) \geq \rho \cdot \left[ v_G \cdot (q_H + q_M) - e_G \cdot \left( \frac{P_{H2}}{q_H} + \frac{P_{M2}}{q_M} \right) \right]$$

$$v_G \cdot (q_G + q_M) - e_G \cdot \left( \frac{P_{G2}}{q_G} + \frac{P_{M2}}{q_M} \right) \geq v_G \cdot (q_H + q_M) - e_G \cdot \left( \frac{P_{H2}}{q_H} + \frac{P_{M2}}{q_M} \right)$$

$$\rho \cdot \left[ v_G \cdot (q_G + q_M) - e_G \cdot \left( \frac{P_{G2}}{q_G} + \frac{P_{M2}}{q_M} \right) \right] \geq v_G \cdot (q_H + q_M) - e_G \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right)$$

$$v_H \cdot (q_H + q_M) - e_H \cdot \left( \frac{P_{H1}}{q_H} + \frac{P_{M1}}{q_M} \right) + \rho \cdot \left\{ v_G \cdot (q_G) - e_G \cdot \left[ \frac{P_{G2}}{q_G} + \frac{(P_{M2} - P_{M1})}{q_M} \right] \right\}$$

$$\geq v_H \cdot (q_G + q_M) - e_H \cdot \left( \frac{P_{G1}}{q_G} + \frac{P_{M1}}{q_M} \right) + \rho \cdot \left\{ v_G \cdot (q_G) - e_G \cdot \left[ \frac{P_{H2}}{q_H} + \frac{(P_{M2} - P_{M1})}{q_M} \right] \right\}$$

$$P_{H1}, P_{H2}, P_{G1}, P_{G2}, P_{M1}, P_{M2} \geq 0$$

(7)

(8)

(9)

(10)

(11)

(12)

(13)

(14)

(15)

(16)

# Propositions from Numerical Examples



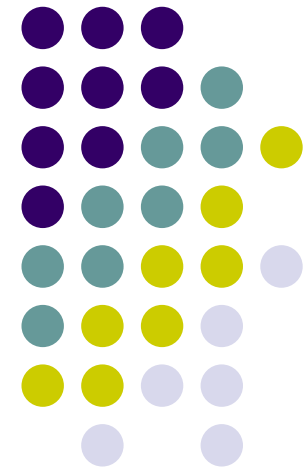
- Proposition 1. When the discount rate for the **system designer's profit** is high, the optimal security strategy is to design higher protection levels during **the earlier time period**.
- Proposition 2. When the discount rate of the **intruder's profit** from information security is high, the optimal security strategy is to design higher protection levels during **the later time period** than during the early time period.
- Proposition 3. When the unique information content of the honeypot system is high, the optimal security strategy is to raise the total protection level for **the honeypot system in the first time period**.
- Proposition 4. When the unique information content of the genuine system is high, the optimal security strategy is to raise the total protection level for **the genuine system all the time**.
- Proposition 5. When the common information content of both honeypot and genuine systems is high, the optimal security strategy is to raise the total protection level for **both systems at the first time period**.

# Exploring the Moderating Effect of Trust and Privacy in the Adoption of Application Service Providers in HealthCare

Ebrahim Randeree

H.R.Rao

Rajiv Kishore



Proceedings, HICSS 2005

Extended Version submitted for AMIS Special Issue



## Abstract

*Understanding the antecedents to the adoption of information technology is important to both technology firms and policy analysts that study the effects of technology adoption on healthcare. This paper uses a transactional cost approach to investigate the role of trust and privacy as moderators in the adoption of Application Service Providers (ASPs) as a new form of information technology outsourcing in the healthcare industry within the current regulatory climate created by HIPAA (Health Insurance Portability and Accountability Act). The analysis utilized a seven-stage measure to capture adoption. Our analysis showed that Transactions costs and the antecedents of transaction costs were highly significant in the ASP adoption process. The direct and moderated effects of Trust and Privacy were not significant.*

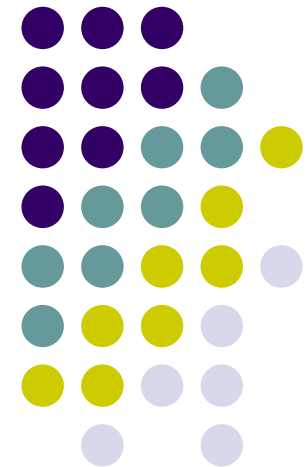
# Managing Security Service Providers: Issues in Outsourcing Security

---

Ebrahim Randeree

H.R.Rao

Rajiv Kishore





## Abstract

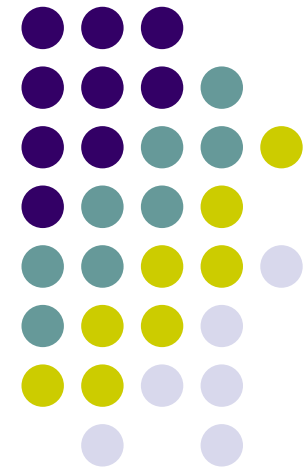
*The issue of trust and risk in outsourced relationships is extended beyond traditional outsourcing models with the introduction of Application Service Providers (ASPs). As ASPs evolve and specialize, Managed Security Service Providers (MSSPs) have emerged as providers of security for firms facing increasing information assurance threats. Building on previous outsourcing literature, this paper develops an integrated model of MSSP adoption; specifically, the paper investigates the issues that impact MSSP acceptance within the current insecure environment. The model identifies contextual variables such as trust, privacy, risk, reputation and relationships with vendors.*

# Information Assurance Issues: Vulnerability to Internet Crime

---

Herath, T.C., Bagchi-Sen S., and Rao, H.R.

**"Vulnerability to Internet Crime and Gender Issues"**, Eileen Trauth (ed), Gender and Information Technology Encyclopedia.

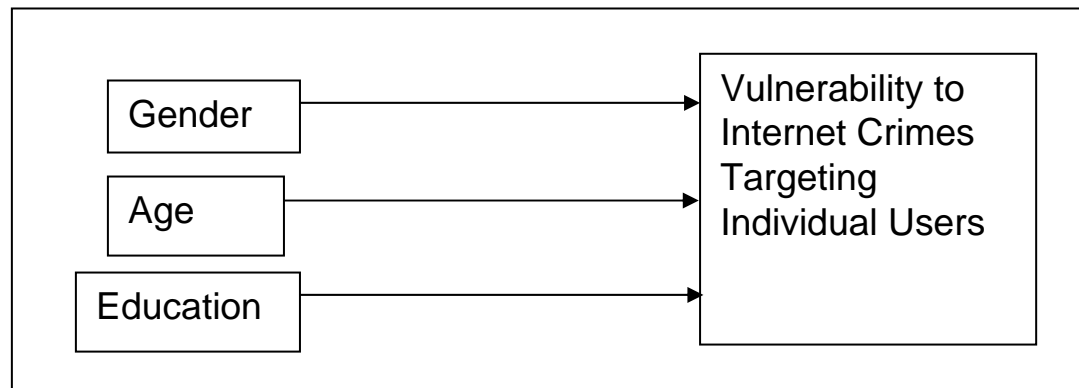




# Introduction

"**Vulnerability to Internet Crime and Gender Issues**", Eileen Trauth (ed), Gender and Information Technology Encyclopedia.

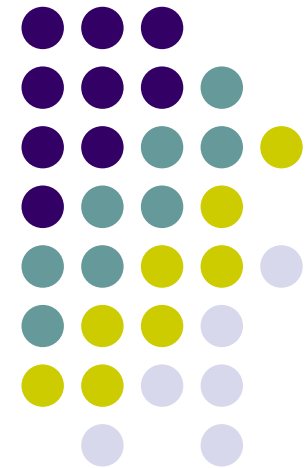
- Considerable research has been conducted to find out whether females are likely to hold negative attitudes toward computers than males resulting in 'technological gender gap'
- Gender differences are observed and studied in a wide range of samples
- exploring whether gender will be one of the factors in understanding vulnerability to Internet crime



# An Investigation of Gender Based Vulnerability Issues in Internet Crimes Across Cultures"

---

Tejaswini Herath,  
H. R. Rao and S. Bagchi-Sen



CANAM grant to conduct the pilot study for a project

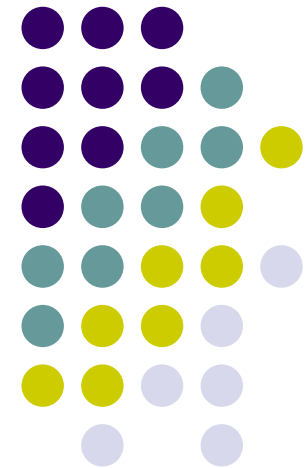
# Abstract



- The study tries to find out if the demographics factors such as sex,, age and education have an impact on awareness of internet crimes
- Study also tries to find out if cultural differences may have an impact on awareness and practices related to information assurance
- Canada is selected for the cross-cultural study mainly because it offers a comparable environment due to widespread use of Internet and at the same time there are significant differences between the two countries due to different culture as well as different legal and government policies.

# Repeated Use of E-Gov Websites: A Satisfaction and Confidentiality Perspective

S. Chai, Herath, T.C., Insu Park and Rao,  
H.R.



# Abstract

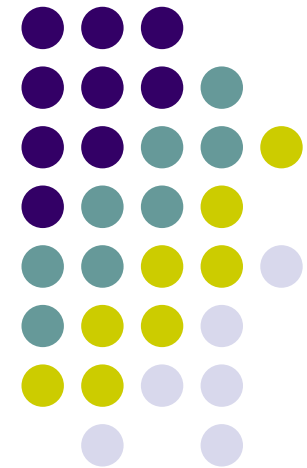


- This paper develops an integrated framework with level of confidential information required as a factor affecting users' privacy concerns and e-government satisfaction derived from service performance.
- Study provides important managerial implication that actions must be taken to enhance security measures that will make users more comfortable using the services through the web for success of e-government initiatives

# Intrusion Countermeasures Security Model based on Prioritization Scheme for Intranet Access Security

---

Manish Gupta, H. R. Rao, S. Upadhyaya



Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, June 2003.



## Contributions of Paper

- **Framework for Effective Response Mechanism to Intranet security violations**
- **RBAC and Prioritization based Vulnerability assessment scheme**
- **Enhance Alert Engine performance**
- **Faster turn-around time-to-detection**
- **Improvises for better quality of security and overall manageability of information assets on Intranet.**
- **Proposed model can be used as a plug-in for an Alert Engine**
- **Dynamic monitoring and Learning Capability**

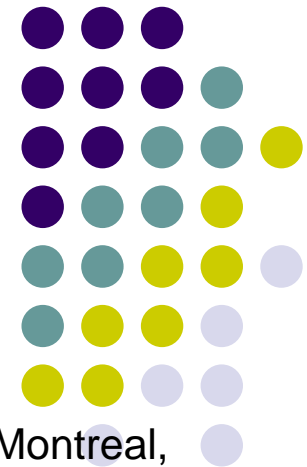


# Contents

- **Components of the framework**
  - Access Priority Scheme
  - Access Priority and criticality Matrices
  - Implementation Methodology (Integration, Algorithm and ERD)
- **Other additions**
  - Cost Benefit Analysis and multi-variate representation of the proposed model
  - A detailed functional example of implementation and integration of the model
  - Literature Survey and comparison with other models

# Electronic Banking and Information Assurance A Survey and Synthesis

Manish Gupta, H. R.Rao, S. Upadhyaya



- Proc. of the 5th International Conference on Electronic Commerce Research, Montreal, CA, October 2002.
- Journal of Organizational and End User Computing, Special Issue on Information Assurance and Security, IDEA Group Publishing, Vol. 16, No. 3, pp. 1-21, July-September 2004.
- Book Chapter: “Advanced Topics in Organizational and End User Computing: Volume 4”, M. Adam Mahmood, IGP, forthcoming.



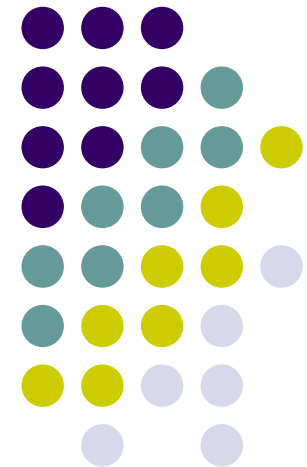
# Components of Paper

- **Detailed Analysis and discussion of E-Banking Information Technology Infrastructure**
  - Applications
  - Site and service Hosting
  - Platforms and Technologies
  - Standards
- **Information Assurance(IA) practices in E-Banking**
  - Existing IA models and standards
  - Security and Privacy Issues
  - In-depth coverage of Information Assurance Issues and combative state-of-art services and mechanisms available
  - Development and Representation of a IA conceptual framework
  - Banking Specific regulations and compliance methodologies

# Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis

---

Manish Gupta, H. R. Rao, S. Upadhyaya



# The Metric Development Framework

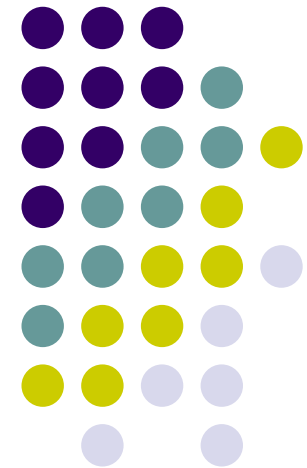


- Different components, architecture and deployed technologies deployed in EBPP systems are discussed understand security underpinnings.
- Information assurance issues in EBPP system analyzed from a workflow and transaction analysis perspective illustrated with numerous workflow/state diagrams.
- an extension of the STRIDE<sup>[1]</sup> threat analysis model and its detailed adaptation with the EBPP system <sup>[1]</sup> (Developed by Microsoft)
- Detailed analysis of threat identification and categorization vis-a-vis EBPP architecture
- The paper develops a framework for the measurement of security levels of any EBPP system, which will help security personnel to ensure a higher level of understanding of information assurance issues and proactively engage in elevating security measures and fraud protection in their organizations.
- A framework for Risk and Vulnerability Assessment and Measurement of a Security Rating of an EBPP System , based on workflow states, to derive an overall vulnerability score for the EBPP system is developed
- A step-by-step procedure is developed to help IT security managers and administrators to understand the metrics that can define proactive and reactive security service delivery levels, and implement the measurement framework that is necessary to demonstrate performance against these metrics.
- A highly effective quantitative risk-assessment model
- A detailed real-world example and implementation of IA metric framework and analysis of results

# Short Term and Total Life Impact Analysis of Worms in Computer Systems

---

Insu Park, R. Sharman,  
H. R. Rao and S. Upadhyaya





# Research Purpose & Focus

- **Purpose**

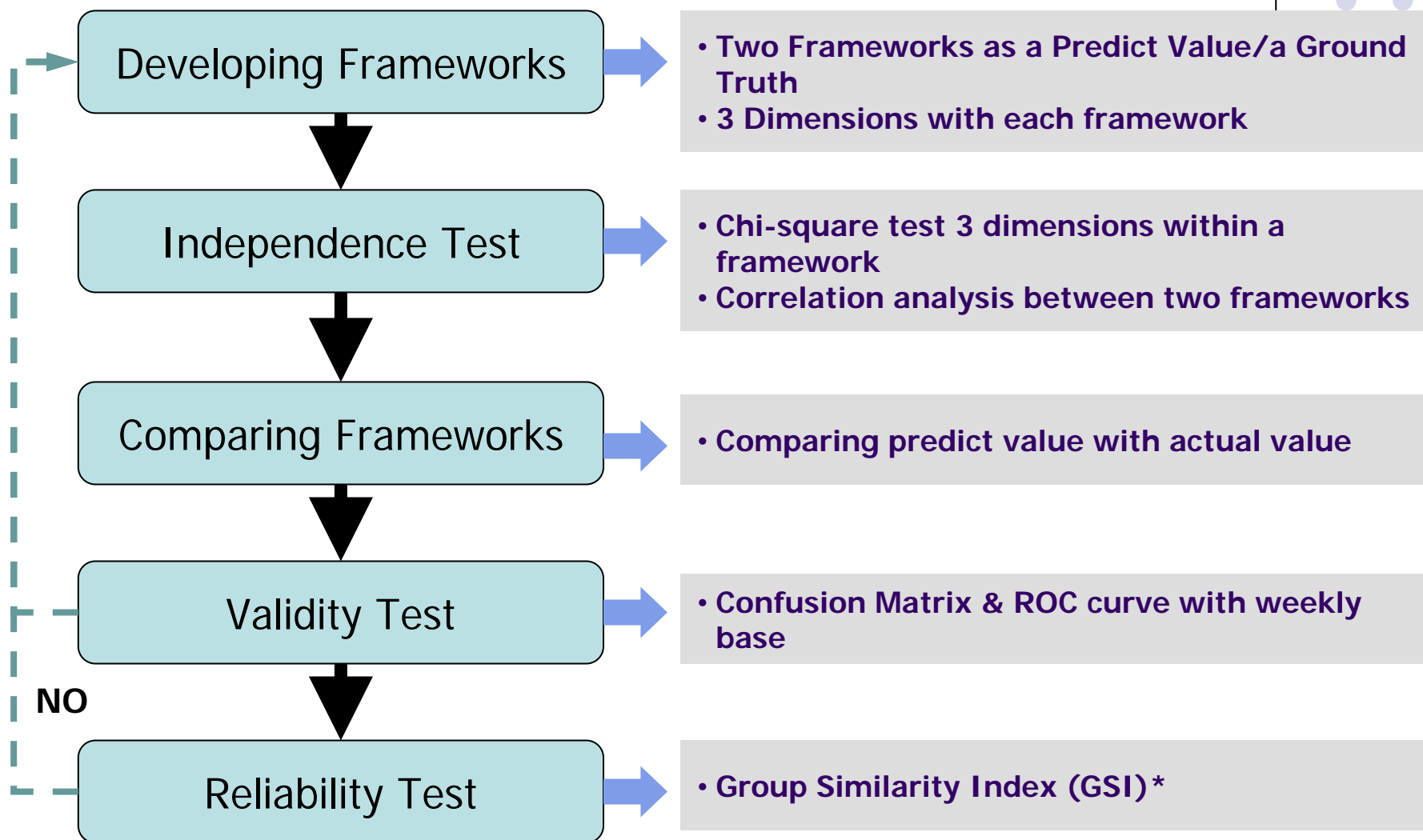
- Developing measures that may be used to discriminate among worms.
- Developing a framework that can allow assignment of a particular worm to a detrimental impact category.
- Examining optimal period to insure the payoff from worms' impact.

- **Focus**

- Detrimental impact of worms *per se* instead of Economic Damage
- The rapidity of spread for the first month
- Number of infections & First week infection



# Classification Process



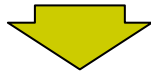
# Frameworks Development



## Framework

### Short Term Impact (STI) framework For predict value

A base ground truth as it relates to data after the virus has run its course.



**Third Dimension** as  
Common Criteria for Two Framework

**Damage Potency:** used to calculate vulnerability, based on the relative damage incurred if a threat exploits a vulnerability



### Total Life Impact (TLI) framework For ground truth (actual value)

A classification based on data available during the early stages in the life of a virus

## Dimensions

- **Early time period hit number (LMH):** For the first month, number of hits we use the acronym log of month hit
  - ⇒ Use the acronym log of **month hit**
- **Tskewness (TSKI):** the degree of inclination toward earlier time periods for the first time period (1st month in this case)
  - ⇒ Adapt the term, 'skewness', from statistics as a way to identify the impact of a virus with regards to time

$$TSKI(V_m) = \frac{3(\bar{Y}_m - Peak_m)}{S_{y_m}} + |Skew\_index_{minimum}|$$

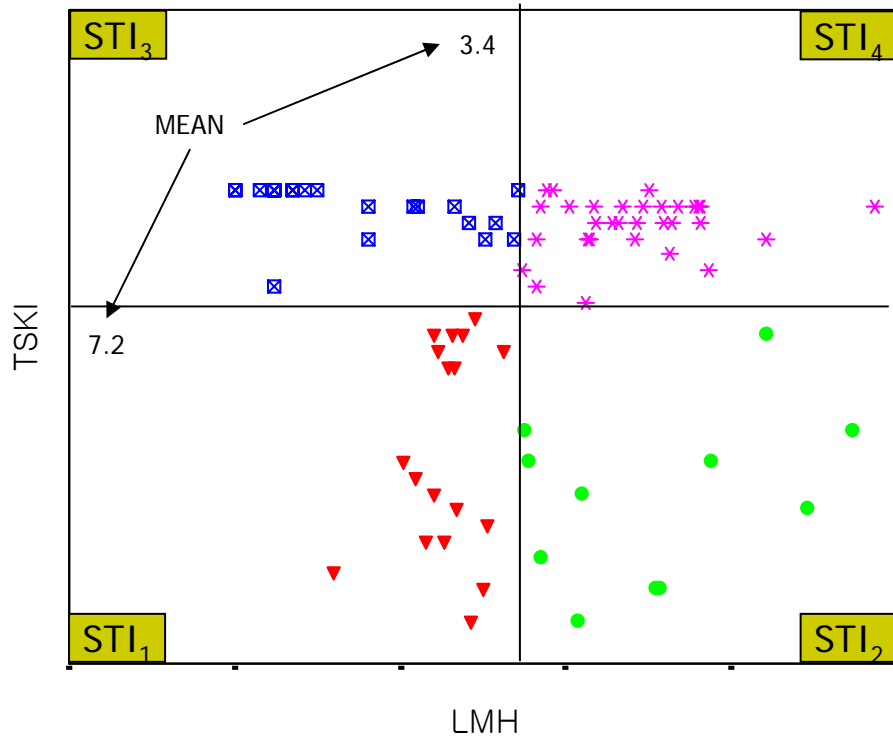
- **Total hit number (LTH):** The total number of hits, or total number of machines infected by the virus, for the life of the virus
  - ⇒ Use the log of **total hit number**
- **Hit density (HT):** The ratio of the hit number of a virus for the first month to the total hit number during its lifespan
  - ⇒ The extent to which first month hits have an impact on the total impact in terms of the total hit number during viruses' lifespan

# Comparing Frameworks

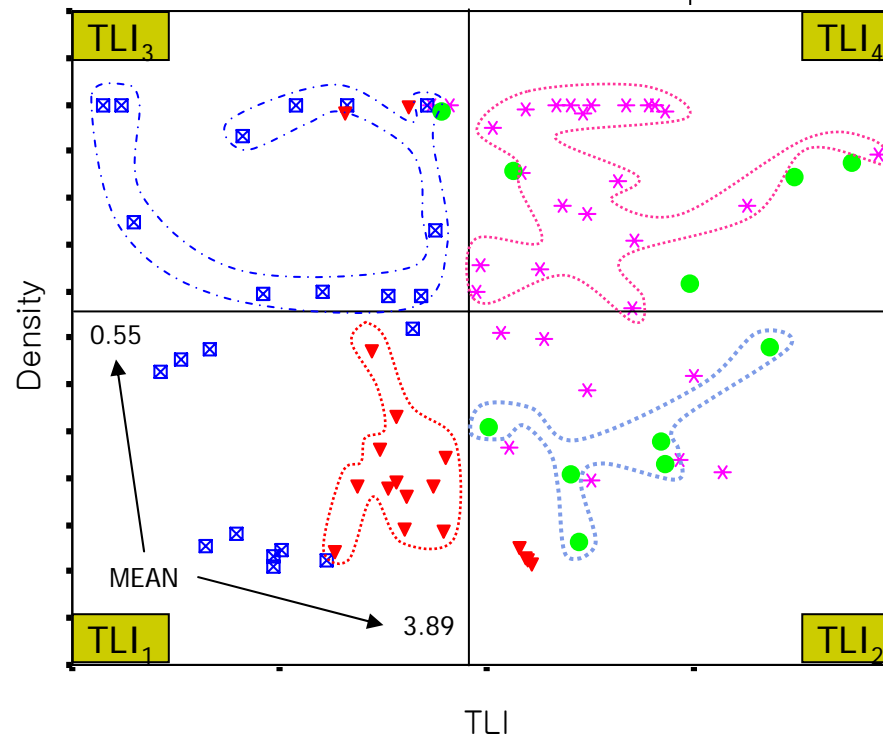
## 2D comparing



Short Term Impact (STI) Framework



Total Life Impact (TLI) Framework



Cell	STI <sub>1</sub>	STI <sub>2</sub>	STI <sub>3</sub>	STI <sub>4</sub>
N	18	11	22	<u>31</u>

Cell	TLI <sub>1</sub>	TLI <sub>2</sub>	TLI <sub>3</sub>	TLI <sub>4</sub>
N	22	18	17	<u>25</u>

Cell	M <sub>1</sub>	M <sub>2</sub>	M <sub>3</sub>	M <sub>4</sub>
N	13 (55%)	6 (33.3%)	12 (71%)	21 (84%)



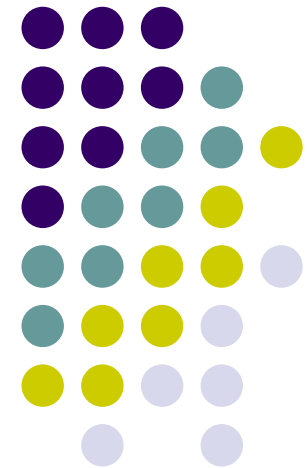
# Conclusions

- Contributions
  - First, this study simplifies factors, which are necessary to categorize worms, into two dimensions: Tskewness and LMH
  - This study applies GSI to our framework for clustering method of worm to enhance validation and reliability.
  - This study shows that
    - A method to predict strength of detrimental impact not just a result of infection of worms with the time
    - Early data can be used for categorizing impacts of worms in organizations with accurate.

# The Effect of Spam and Privacy Concerns on Email Users' Behavior

---

Insu Park, R. Sharman,  
H. R. Rao and S. Upadhyaya



# Purposes & Contributions



- This paper attempts to examine the effect of *privacy concerns* on user's behaviors after they have been exposed to spam e-mail.
- The contributions
- First, this study explains users' coping behavior with regard to spam email as it relates to privacy protection. By paying attention to the underlying psychological processes and motives, the current study also provides insight on how email users behave while protecting their privacy.
- Second, this study provides a theoretical scheme for the users' behavior with regard to spam and privacy. In other words, this study explains the effect of spam email and *privacy concerns* on users' behavior by using a psychometric approach.

# Users' behaviors on spam



- Usage-oriented behavior
  - To describe a behavior that relates to avoiding or reducing email use.
- Protecting-oriented behavior
  - To describe a more active response to spam.
  - a “user’s positive defense behavior to protect their privacy from particular problems such as spam, hacking, and so on.”



# Hypothesis

- **Hypothesis 1:** *The receipt of spam affects privacy concerns.*
- **Hypothesis 2:** *spam experience and privacy concerns affect users' usage-oriented behavior.*
- **Hypothesis 3:** *user's experience with spam does not affect their protection-oriented behavior but privacy concerns do affect their protection-oriented behavior.*



# Implications

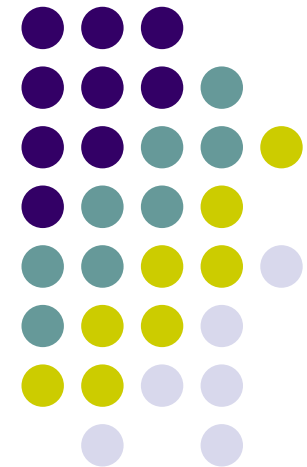
- Explains the use of defense mechanisms in users' privacy protection behavior.
- Presents a theoretical initiative for users' behavior with spam and privacy.
- Reveals that a *spam experience* has a limited impact on users' protection-oriented behavior.
- reveals that an experience with spam has different effects according to users' behaviors
- Shows that *privacy concerns* lead users to resort to dual behavior.

# Managing Private Information Safely on Blogs

Sangmi Chai\*, Jinkyu Lee^, and H.R. Rao\*

\*State University New York at Buffalo  
^Oklahoma State University

S. Chai, J. Lee. H.R. Rao. "Managing Private Information Safe on Blogs."  
The Second Secure Knowledge Management Workshop (SKM), Brooklyn,  
New York, September 28-29, 2006





# Research Questions and Conclusion

## Research Question

- What type of private information is open to the public on the blogs?
- How does one's security awareness affect the decision to post their private information to public?
- What factors stimulate one's security awareness in the context of blog use?
- What are the possible motivations behind sharing one's personal information such as photo, their daily diary and private information on the blog?
- How does the blog provider take care of the users' privacy on the web?

## Conclusion

- The most vulnerable demographic groups to cyber crimes are teenage female bloggers and over 30s female bloggers
- Our test result explains information privacy behavior of bloggers based on their security awareness and experience of security training or exposure.

# Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Children

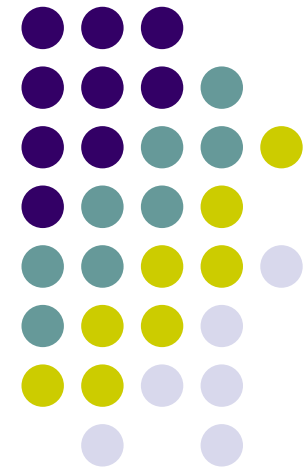
S. Chai\*, S. Bagchi-Sen\*, C. Morrell^, H. R. Rao\* and  
S. Upadhyaya\*

\*State University of New York, Buffalo

^University of Maryland, Baltimore County

*S. Chai, S. Bagchi-Sen, C. Morrell, H.R. Rao and S. Upadhyaya.  
(2006) "Role of Perceived Importance of Information Security: An  
Exploratory Study of Middle School Children's Information Security  
Behavior." The Journal of Issues in Informing Science and  
Information Technology, Vol. 3 pp 127-136*

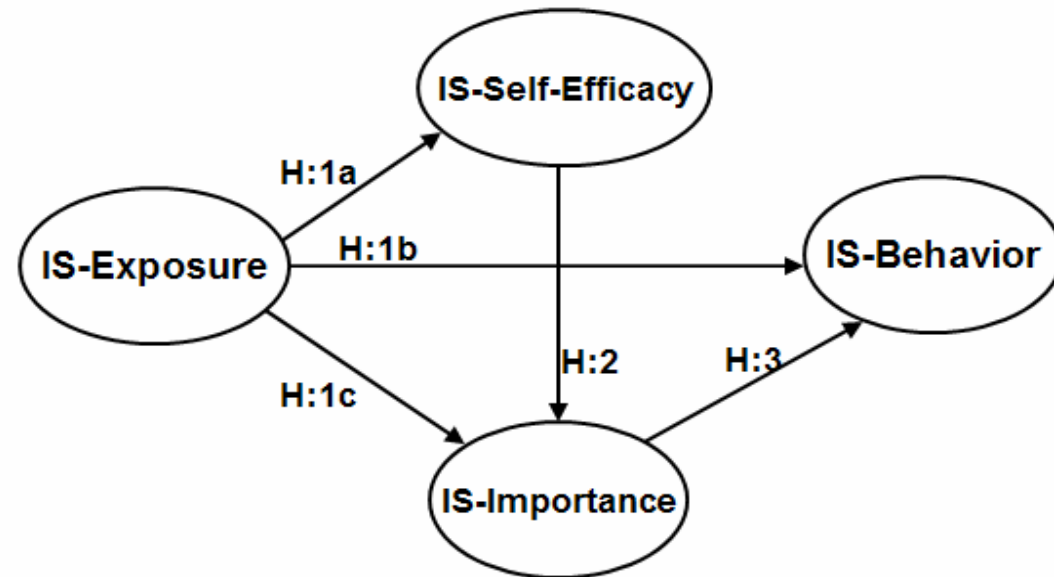
*NSF under grant 0420448*



# Research Question and Model



- To understand the factors that motivate school-age children to pay attention to information security
- To motivate them to use the Internet safely



Students, who have strong self-efficacy toward information security on the Internet and have an exposure of information security from school, parents and media, are more likely to practice information security.

To motivate students' information security behavior, we need to provide more information security education opportunities to students as well as chances for students to be exposed to information security issues. We also need to try to increase their perceived importance of information security.

# Security Practices in Organizations: A Dyadic Investigation of Businesses and their Employees

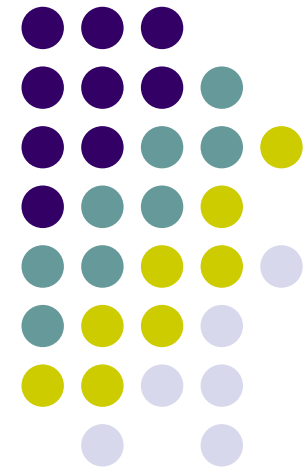
Tejaswini Herath

Advisor: Professor H.R. Rao

Committee Members:

Dr. Debra Street, Department of Sociology

Dr. Shambhu Upadhyaya, Department of Computer Science and Engineering



# Motivation & Background



- Security breaches hamper production and disrupt the workplaces. These security problems also have a negative effect on society at large.
- Cyber Security – A Problem of National importance (PITAC 2005, Department of Homeland Security)
- Several different factors enhance or obstruct the adoption of information security practices by businesses as well as individual employees.
- Goal of this project is to study:
  - (a) organizational contextual factors as they relate to adoption of technologies and policies
  - (b) human factors that affect security behaviors in the organizational setting, and
  - (c) flow of information security practices throughout the organization- a critical aspect of information security.

## Background

- This project is a collaborated effort between The Federal Bureau of Investigation (FBI), Buffalo Division and Center for Excellence in Information Systems Research and Education (CEISARE), SUNY Buffalo
- To understand the security practices in organizations from holistic view - this research considers these issues from both aspects (management and employee)
- We believe that this study will be the first to take a dyadic approach to the issue of security practice adoption.

# Dyadic Survey



- Management Survey
  - Survey information security practices by businesses in Western New York in an attempt to understand and document the severity of cyber crime.
  - Comprehensive security measures and best practices reduce system vulnerabilities – however, there are several different *factors that may enhance or obstruct the adoption of effective information security practices*
- Employee Survey
  - Malicious use by insiders as well as negligence of employees has led to security breaches costing organizations millions of dollars in losses
  - Many recent surveys reveal that although the policies and procedures are in place, many employees including outside contractors ignore them not realizing the importance of their existence.
  - Survey considers end users (employees) who work in very different roles who would be **expected** to be knowledgeable about cyber security relating to internet use as a routine aspect of their job.

# Dyadic Investigation

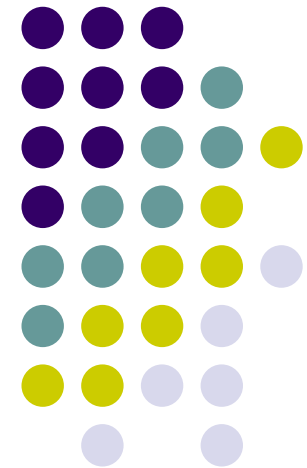


- Dyadic approach strives to investigate if the security policies and practices adopted and implemented by management are widely dispersed within an organization.
- The study will try to understand whether there is a gap between the management perspective and employee perceptions about these practices, and
  - if so, what factors contribute to differences or similarities between management and employees regarding security policies

# Why Phishing Works: An Elaboration Likelihood Perspective

Rui Chen  
Tejaswini Herath  
Jingguo Wang  
H. Raghav Rao

MSS, School of Management, SUNY-Buffalo

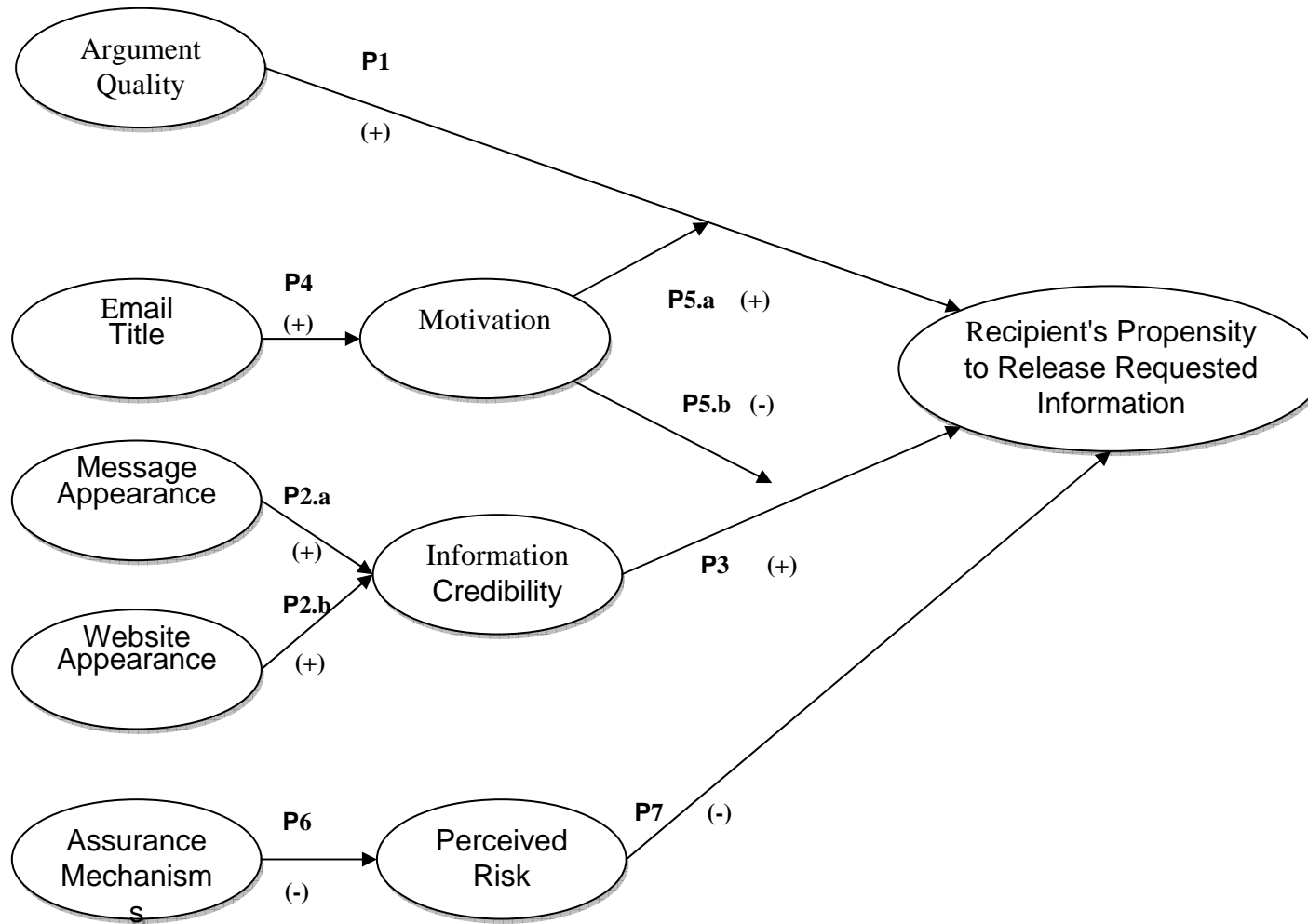
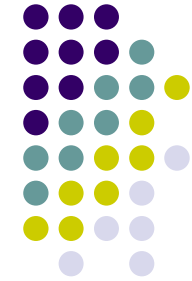


# Introduction



- **Email has become indispensable (Hoffman, 2004), but has also opened new horizons for deception.**
  - Phishing causes 1.2 Billion in 2003 (Gartner Group, 2004). Further it impacts consumer confidence that affects overall e-business
  - The uniqueness of Phishing: Technology provides distance and anonymity; Social engineering; No interaction.
- **Why phishing works, and Why people will click the link and give the information away?**
  - Understand e-mail receiver information process through Elaboration Likelihood Model (ELM) (Petty et.al. 1986) and analyze factors used in design of a phishing e-mail.
- **Phishing research**
  - Models of how phishing works (Jacobson, 2005)
  - Different technologies to fight phishing (spam) – (Hall, 1998; Oppliger, 2005, Warden 2005)
  - Tools will not be completely effective- in addition to technology phishing uses social engineering tactics (The HoneyNet Project & Research Alliance, 2005)
- **Deception**
  - Rich media and Computer-based communication (both Non Verbal and Verbal cues) – ( DePaulo et.al, 2003, Zhou et.al, 2004, Marett et.al., 2004)
  - Phishing – non interactive, different textual cues than current studies

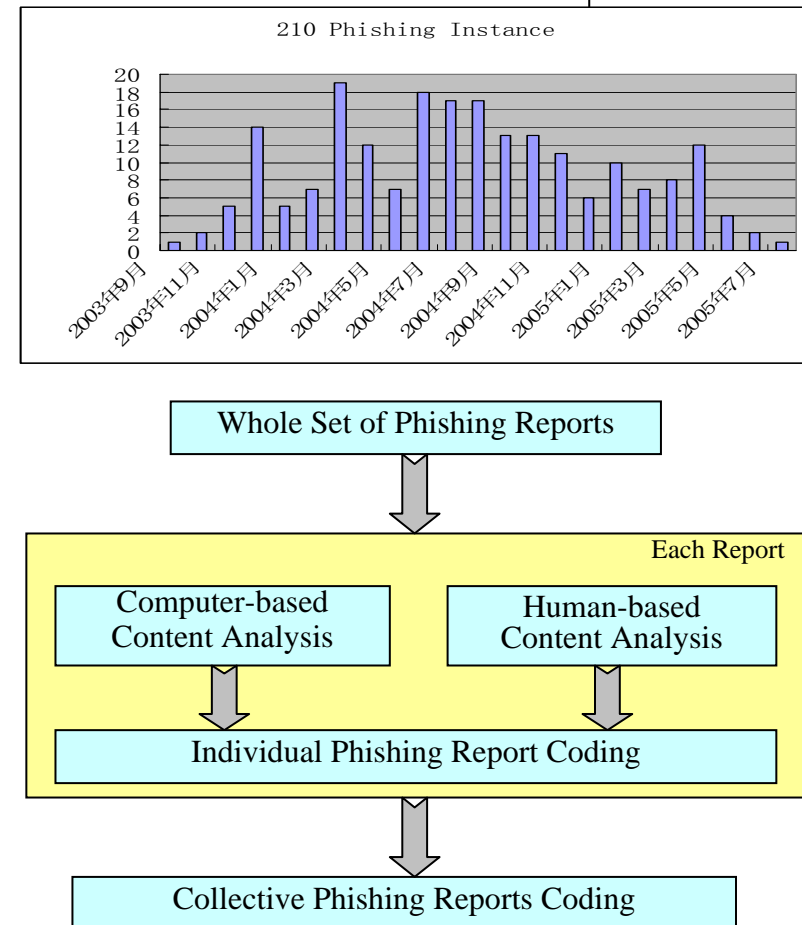
# Why Phishing Works: A Theoretical Framework



# Content Analysis



- Data Source
  - “Phishing Archive” by [Anti-Phishing Work Group](#)
  - Email and Website
- Analysis Process Flow
- Human coding
  - Information assurance mechanism, email /webpage appearance, information requested, and industry type
  - Codebook, code form, and coder training (Neuendorf 2002)
  - Validity and reliability (Krippendorf 1980)
- Machine Coding
  - *Email title and message content*
  - Development of dictionary (Neuendorf 2002)





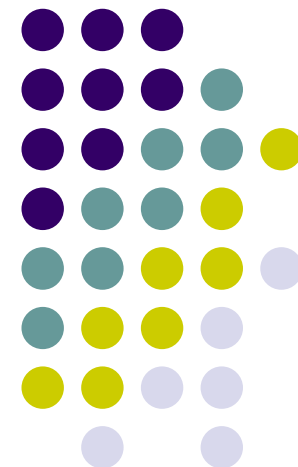
# Future Research

- Validation of the Model
  - Complete Set of Measurement
  - Data Analysis
- Linguistic Style of Phishing Emails
  - Verbal Cues in Deception
  - Linguistic Characteristics of Computer-Mediated Communication
- Phishing Intension Detection → Phishing Filter
  - Phishing Cues
  - Detection Mechanisms
  - Effectiveness Evaluation

# An Examination of Private Intermediaries' Roles in Software Vulnerabilities Disclosure

---

Jessica P. Li  
H. R. Rao



The earlier version of this paper was presented at Secure Knowledge Workshop (SKM) – 2006 in New York City and received best student paper award.

# Motivation



- Software vulnerability disclosure has generated much interest and debate
- Recently some **private intermediaries** have entered this market
  - iDefense, tippingPoint
  - Pay the persons who report the vulnerabilities
  - Provide the discovery information to subscribers
- Two aspects of private intermediaries
  - Self-awareness and self protection, leads to less loss to subscribers
  - Inappropriate information leakage exposes non-subscribers to higher potential attacks
- What are their effects on
  - Optimal timing of disclosure policy made by public intermediaries
  - Vendors' corresponding reaction



# Findings

- **Proposition 1**
  - Public intermediary's optimal disclosure time doesn't change with private intermediary's participation, whether it is an unregulated market or regulated market.
- **Proposition 2**
  - With low information leakage, vendor's optimal patch release time window is increased with the private intermediary's participation.
- **Proposition 3**
  - With low information leakage, as more customers subscribe to the awareness service offered by private intermediary, longer the optimal patch release time window will tend to be.
- **Empirical Evidence**
  - 1493 vulnerability observations from CERT/CC
  - 326 vulnerability observations from iDefense

# Conclusions and Future Research



- Public intermediary's optimal disclosure time does not change with the participation of private intermediaries
- Private intermediaries' service can decrease a vendor's willingness to deliver quick patch where information leakage is low
- Regarding future research, we aim to extend the analysis to scenarios with extensive information leakage