

Department of Information Systems & Decision Sciences

BEAR STEARNS RESEARCH GRANT

Application & Guidelines (2/1/2008)

PURPOSE and OVERVIEW

To provide research support to Information Systems & Decision Sciences (ISDS) full time, permanent faculty for research projects carried out at the Bears Stearns IT Research Center that will eventually lead to high quality academic publications.

The funds available from this grant could be used to pay for research expenses such as stipends to research assistants, paying human subjects for research, buying hardware and software for research, paying for data access, and other research related expenses for research projects based out of Bears Stearns IT Research Center.

GRANT AMOUNT: Up to \$5000 per faculty member over a three year period.

ELIGIBILITY CRITERIA

To be eligible applicants must:

- Be full time, permanent ISDS faculty member on the Tampa, Sarasota or Lakeland campus.
- Have exhausted his/her startup funds and research overhead funds. In case of any remaining startup funds, all research expenses related to the proposed project that is permissible to be charged to the startup fund must be charged to that fund.
- Have submitted working papers for all previously completed projects supported by Bear Stearns Research Grants to the ISDS Chair
- Recipients of Bear Stearns Research Grants, who had previously signed the undertaking on page 8, are ineligible to apply if they did not fulfill the requirements of the undertaking.
- Have no other active research grant (USF or external) for the same scope of work
- Be contractually committed to continue as a USF employee for the following academic year.

To be eligible projects must:

- Not have overlapping funding for the scope of work described in this proposal from any other source during the term of the grant.
- Have exhausted all other sources of funding including the Gaiennie Fund, if doctoral students are involved in the scope of work described in the proposal.
- Be housed at the Bears Stearns IT Research Center.
- Not be designed primarily for curriculum or educational development, e.g., preparation of textbooks or course materials, or evaluation of educational experiments, etc.

EVALUATION CRITERIA

Application competitiveness is strengthened by addressing the following:

- Importance of the problem being addressed in the research project
- Extent to which the project is original and innovative in concept and/or approach
- Clarity and soundness of objectives/hypotheses and methods
- Anticipated contribution to the literature
- Potential for publication of the research output in high quality academic outlets in the applicant's field
- Recent research record of the applicant in terms of quality of publications, working papers, and presentations at research conferences

APPLICATION REVIEW PROCEDURES

Each proposal will be reviewed by an ad hoc committee of three ISDS faculty members, who would be best qualified to evaluate the proposal. The ISDS Chair will normally appoint the committee. In case of any conflict of interest, the ISDS Chair will designate an ISDS faculty member to appoint a committee and manage the review process. If deemed appropriate and necessary by the committee, comments about the proposal that might be particularly helpful or informative may be forwarded to the applicant. The identity of the committee members will not be known to the applicant.

Deliverables

At the end of the project, a working paper must be submitted to the ISDS Chair.

RESEARCH COMPLIANCE

The following conditions require special clearance before research may be undertaken. Please indicate on the first page if the proposed research will require approval by the Institutional Review Board (IRB).

USE OF HUMAN SUBJECTS IN YOUR RESEARCH

Researchers proposing to use human subject participants in the course of their research study are required to submit an application to the Institutional Review Board (IRB) for review and approval ***before initiating each project and before funding will be released***. This requirement encompasses a variety of research activities that can range from the simple use of data and surveys or interview procedures to more complex and invasive protocols such as clinical trials and treatment interventions. Please consult the IRB homepage for contacts and more detailed information: <http://www.research.usf.edu/cs/>.

ADDITIONAL CONDITIONS

- The Bear Stearns Research Grant will be awarded on a rolling basis, and this program will continue as long as funds are available.
- The ISDS Department Chair has the right to cancel this program with an advance notice of one month.
- The ISDS Department Chair reserves the right to make changes to this program.
- For the purpose of accounting, each year will be from July 1st to June 30th of the following year.
- Any unused funds cannot be rolled over to another project or to the next three year cycle.
- All expenses on the Grant have to be approved by the ISDS Chair.

APPLICATION SUBMISSION PROCEDURES

Applicants should submit a signed electronic copy (using this document) to the ISDS Department Chair.

APPLICATION LIMIT- Multiple proposals from an applicant will be accepted, but the total funding during a three year cycle will not exceed \$5000 across multiple proposals funded.

LENGTH OF APPLICATION - Limit identified sections of the application to the size or length indicated in the application.

Application for the
Bear Stearns Research Grant

Title of Proposal: An integrated model of information security and risk management

Name of Faculty Member: Manish Agrawal

Names of Project Team Members: Manish Agrawal, Kaushal Chari, Varol Kayhan

E-mail address: magrawal@coba.usf.edu

If your project will include the use of human subjects you must receive approval from the USF Institutional Review Board (IRB) prior to initiating the study. Indicate below whether IRB approval is required for your project:

IRB approval required? (Yes)

Will you be receiving research funding from any source (USF or external)? (No)

If Yes, indicate funding amount and source below. Note: to be eligible for the Bear Stearns Research Grant, there should be no overlap between the proposed research project and work that is funded from another source

Funding amount: N/A

Source: _____

PROJECT SUMMARY/ABSTRACT

Limit: 200 words, double-spaced

Provide an overview of the proposed project, including the importance of the problem to be addressed and the expected contribution to knowledge in your field. Include objectives/hypotheses, methodology and anticipated results.

Organizations are making significant investments to protect their IT infrastructure from security breaches and to comply with regulations such as Sarbanes-Oxley. In response, research has focused on security-related issues such as optimal information security investments (Gordon and Loeb 2002), and the value of Intrusion Detection Systems (IDS) (Cavusoglu, Mishra et al. 2005). The question however remains if organizations are making the right types of investments in security technologies. What is therefore also needed are measures to quantify security (Littlewood, Brocklehurst et al. 1993). For example, the studies cited above provide a theoretical treatment of security issues, with model parameters left to be estimated through empirical research. Gordon and Loeb (2002) recommend that the maximal investment on information security should not exceed approximately 37% of the value of the resource being protected. However, they do not provide any guidelines as to how the security dollars should be spent to obtain maximum protection. (Cavusoglu, Mishra et al. 2005) model IDS in terms of the detection rate P_d and the false alarm rate P_f and find that an IDS is useful only when P_d exceeds a critical value. While this result may be interesting, it is useful only when accurate estimates of P_d are available. These examples highlight the need for empirical research to determine security risks, and to verify the effectiveness of security technologies.

In the proposed research, we will first empirically determine the probability of breaches for various information security controls. We will then provide an approach that is grounded in empirical data for assessing the probability of security breaches for various security configurations. Finally, we will develop an analytical model for determining the optimal security configuration.

EXPECTED OUTCOMES OF PROJECT

Single-spaced outline format is permitted

a. Publication Plan – Briefly describe the tangible results of your project and how you plan to publish/disseminate the results of your project. Include names and Web addresses of potential journals or other academic outlets along with an indication of the level of quality of the outlet (ranking in field, acceptance rates, etc.).

The research is being targeted for submission to the MISQ special issue on information security. Preliminary results will also be submitted to the INFORMS CIST conference at Washington D.C. If we are unable to meet the deadline for the MISQ special issue, we may submit the research paper from the proposed research to ISR.

It is well known that MISQ and ISR are premier journals for MIS research.

b. Proposal Budget – Provide a budget for the proposal by listing all the expense items and the amount requested.

The research requires expert assistance in setting up the target hosts and instrumentation for data collection. In addition, student participants will be offered rewards to expend effort to compromise the system.

\$3,000: To pay an experienced consultant for systems configuration, vulnerability development, and setting instrumentation for data collection.

\$2,000: Participation and reward fee for 3 subjects from the White Hatters Club.

PROJECT DESCRIPTION

An Integrated Model of Information Security & Risk Management

Introduction

In the proposed research, we aim to develop an integrated model of information security and risk management that integrates tradeoffs between the cost of various kinds of risks for any given IT infrastructure and the cost of IT controls. We propose a methodology grounded in empirical data to determine the optimal security configuration for the given IT infrastructure. Literature relevant to the proposed research is sparse. Recent research has focused on issues such as optimal information security investments (Gordon and Loeb 2002), value of specific controls such as IDS (Cavusoglu, Mishra et al. 2005). While Gordon and Loeb (2002) theoretically determine the optimal investment in security, they do not specify the controls to use. The proposed research will determine the optimal set of controls.

Model

Table 1: Notations

T	Set of transaction types.	r_t^l	Transaction loss rate of transaction type $t \in T$.
F	Set of farms. A farm is a collection of computers running identical applications for load balance and fault tolerance.	c_t^l	Unit cost of transaction loss rate of transaction type $t \in T$.
F_t	Set of farms used in processing transaction $t \in T$.	c_i^s	Unit cost of general control of type $i \in G$.
N_f	Set of nodes (i.e., computers) in farm $f \in F$.	c_{pj}^s	Unit cost specific control of type $j \in S$ used at node p .
k_{ft}	Number of sub-transactions spawned from a single transaction of type $t \in T$ at farm $f \in F$.	l_p^i	Loss amount when there is an integrity breach in node p .
r_t^d	Desired transaction rate of transaction of type $t \in T$ (in transactions per minute).	l_p^c	Loss amount when there is a confidentiality breach in node p .
r_{ft}^e	Expected transaction rate of transaction of type $t \in T$ (in transactions per minute) based on vulnerability at farm f .	Q_p	Capacity of node p in transactions per minute.
r_t^m	Minimum transaction rate of transaction of type $t \in T$ supported (in transactions per minute).	y_i	= 1 if general control of type $i \in G$ used in the IT infrastructure; 0 otherwise.
G	Index set of general control types such as a perimeter router.	Z_{pj}	=1 if specific control of type $j \in S$ used at node p ; 0 otherwise.
S	Index set of specific control types such as a host-specific firewall.	$v_p^a([y_i]_{i \in G}, [z_{pj}]_{j \in S})$	Failure probability of node p due to availability breach, given p is shielded by controls $[y_i]_{i \in G}$ and $[z_{pj}]_{j \in S}$.
$v_p^c([y_i]_{i \in G}, [z_{pj}]_{j \in S})$	Failure probability of node p due to confidentiality breach, given p is shielded by controls $[y_i]_{i \in G}$ and $[z_{pj}]_{j \in S}$.	$v_p^i([y_i]_{i \in G}, [z_{pj}]_{j \in S})$	Failure probability of node p due to integrity breach, given p is shielded by controls $[y_i]_{i \in G}$ and $[z_{pj}]_{j \in S}$.

$$\text{Problem P1: } Z1 = \text{Min} \sum_{t \in T} c_t^l (r_t^d - r_t^m) + \sum_{\substack{p \in \cup_{f \in N_F} N_f}} l_p^c v_p^c([y_i]_{i \in G}, [z_{pj}]_{j \in S})$$

$$+ \sum_{\substack{p \in \cup N_F \\ f \in N_F}} l_p^i v_p^i ([y_i]_{i \in G}, [z_{pj}]_{j \in S}) + \sum_{i \in G} c_i^s y_i + \sum_{\substack{p \in \cup N_F \\ f \in N_F}} \sum_{j \in S} C_{pj}^s z_{pj}$$

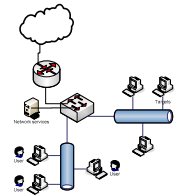
St. $\sum_{t \in T} r_{t, f}^d k_{t, f} \leq f([Q_p]_{p \in N_f})$ for all $f \in F$
 $\sum_{t \in T} r_{t, f}^e k_{t, f} \leq f([v_p^a]_{i \in G}, [z_{pj}]_{j \in S}]_{p \in N_f}, [k_p]_{p \in N_f})$ for all $f \in F$
 $r_{t, f}^e \geq r_{t, f}^m$ for all $f \in F_t$
 y_i and z_{pj} are 0/1 integer; $r_{t, f}^d, r_{t, f}^e$ and $r_{t, f}^m \geq 0$.

The objective function captures the tradeoffs between the cost of security breaches and the cost of controls. There could be breaches in availability, confidentiality or integrity (U.S. Code, Sec. 3542). The first two constraints determine the transaction rates with no risk and with availability breach risk. The function f is specific to the IT configuration used, and can be easily computed (Highleyman, Holenstein et al. 2003). When the model is solved optimally, the optimal assignments of controls (such as firewalls, packet filtering routers, etc.) are determined that minimize loss due to security breaches. While most model parameters are easy to determine, the distributions of v_p^a , v_p^c and v_p^i , (which are IT infrastructure specific) are hardest to determine. We will empirically determine the probability of breaches for various information security controls using an experimental study.

Experimental Study

A team of motivated hackers will attempt to compromise the security of specified hosts. Targets for confidentiality, availability and integrity (i.e., top level objectives) will be defined on these hosts. For example, the target for availability is the response time for connection requests. The hackers will be considered to have achieved their target if they increase response time to five times the normal response time.

Figure 1: Experiment setup



Subjects

Three hackers (subjects) will be selected from the USF White Hatters Club as the red team for the experiments (Wood and Bouchard 2001). This is a group of motivated students who represent USF at various information security competitions around the country. Each subject will have a user account on a host and will seek to compromise a specified target host on the same subnet (Figure 1).

Each subject will be paid for participation and will also be eligible to win additional performance based monetary rewards based on points earned. Specifically, subjects will be rewarded points based on their successes at compromising

the higher level goals such as confidentiality, integrity and availability as well as for reaching intermediate goals. Multiple subjects will help us determine an accurate distribution of multiple breach probabilities.

System Configuration

There will be three separate identical systems, and each subject will be assigned to one dedicated system with goal of compromising the assigned system. Two types of target machine configurations will be used during the experiments.

The first configuration will represent a Linux based server while the second configuration will represent a Windows desktop client (Table 2). These configurations are representative of the common deployments of the respective

Table 2: Nodes used in the experiments

Server	Desktop
OS: Linux (Centos) Web server: Apache DBMS: MySQL Application environment: PHP	OS: Windows XP Browser: IE Software: Office XP

platforms. Custom built applications with defined vulnerabilities will also be added to the server node. Common misconfigurations found in “real-world” installations will also be introduced in the systems.

Experimental Procedure

Subjects attack targets to expose vulnerabilities. A preliminary hierarchy of vulnerabilities (Figure 5) has been developed based on common vulnerabilities, e.g. (McClure, Scambray et al. 2003), and will be further refined based on the opinion of security experts. Each attack goal has a flag associated with it. Points for flags associated with goals higher in the hierarchy (such as a confidentiality breach) will be significantly greater than points for flags lower in the hierarchy. Subjects will first attack unprotected hosts (i.e., without being shielded by any controls) to capture multiple flags and expose various vulnerabilities in the system. The subjects would then launch attacks on each node shielded by just one control.

The primary data collected from experiments would be the self-reported time expended for each attack (successful or unsuccessful), which is a surrogate for effort expended during attacks (Littlewood, Brocklehurst et al. 1993). From the attack patterns in Figure 2, it would be possible to extract the time spent on attacks into three different graphs based on high level attack objectives. Statistical properties such as stationarity and independence of increments will be verified. If independence of increments is verified, then an exponential model based on a non-homogeneous Poisson process (Goel and Okumoto 1979) could be used to determine the probability of breaches.

Figure 2: Example flag capture pattern

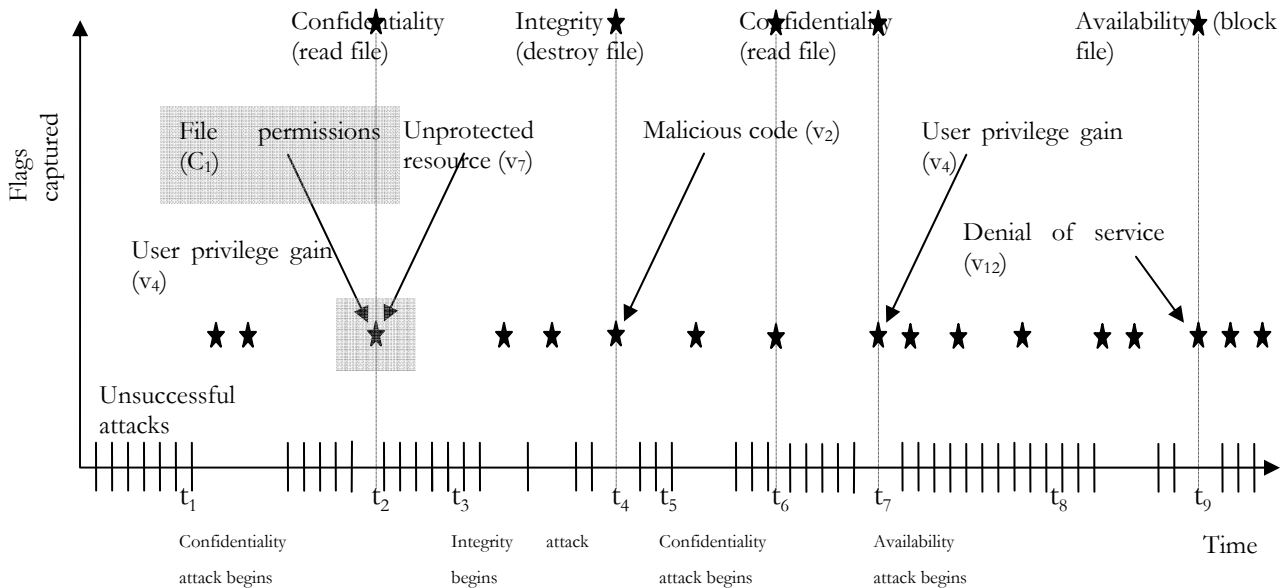


Figure 3: Confidentiality (without controls)

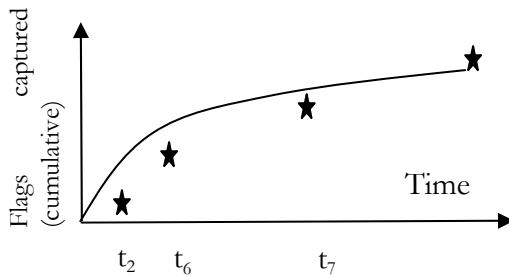
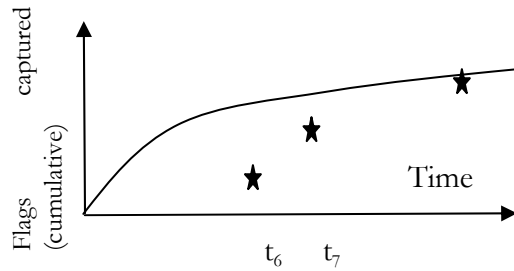


Figure 4: Confidentiality (after control 1)

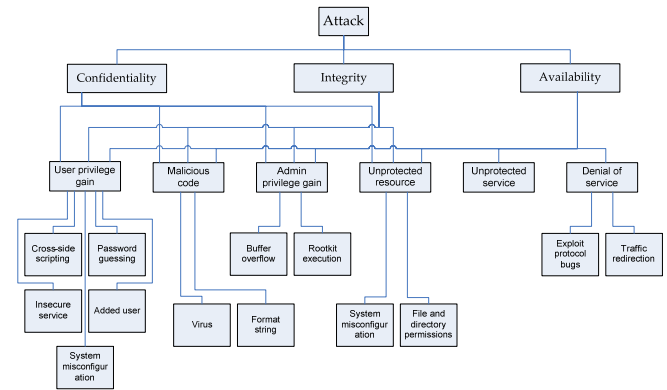


For example, consider the pattern of flags captured in Figure 2. At time t_1 , the attacker starts an attack to breach confidentiality. The attacker captures some intermediate flags exploiting user privileges but fails to violate confidentiality (for example, the compromised user account does not provide a path to the specified documents). However, at time t_2 , the attacker identifies an unprotected resource that leads to breach of confidentiality. Similarly, at time t_3 , the attacker initiates an attack on integrity and succeeds in breaching integrity at time t_4 . The time intervals in the sets $\{(t_2 - t_1), (t_6 - t_5), (t_7 - t_6)\}$, $\{(t_4 - t_3)\}$, $\{(t_9 - t_8)\}$ are indicators of effort required for compromising confidentiality, integrity and availability.

The flag capture pattern in Figure 2 can be used to estimate reliability parameters as shown in Figure 3 for the unprotected host. Control C_1 protects against the unprotected resource vulnerability that led to the first confidentiality breach and Figure 4 shows the fitted curve for reliability after control C_1 is placed.

The conditional probabilities of availability, confidentiality and integrity breaches associated with control i shielding node p (i.e., $v_p^a(x_i)$, $v_p^c(x_i)$ and $v_p^i(x_i)$) can be computed for each node type- control pair using data in graphs such as those displayed in Figure 4. For each control type there will be three separate graphs (i.e., for availability, confidentiality, and integrity). Note that $v_p^a(x_i)$, $v_p^c(x_i)$ and $v_p^i(x_i)$ can be used to compute the value of control i . In the case of multiple controls shielding a given node, the same approach as described above

Figure 5: Initial computer system attack classification and flag tree



could be utilized to compute $v_p^a([y_i]_{i \in G}, [z_{pj}]_{j \in S})$, $v_p^c([y_i]_{i \in G}, [z_{pj}]_{j \in S})$ and $v_p^i([y_i]_{i \in G}, [z_{pj}]_{j \in S})$. Consider two controls a and b , that can shield the following vulnerabilities $\{v1, v3\}$ and $\{v1, v5\}$ respectively, and assume further node p has vulnerabilities $\{v1, \dots, v8\}$. The remaining vulnerability after applying controls $a \in G$ and $b \in S$ to node p would be $v_{ab}^p = \{v1, \dots, v8\} - \{v1, v3\} - \{v1, v5\}$. Thus in graphs related to unprotected case, we only consider the time to breach those vulnerabilities that remain in set v_{ab}^p . From these times, similar graphs such as in Figure 4 can be generated, and the breach probabilities estimated. For various control combinations we can estimate the breach probabilities for various nodes. Note that the use of multiple subjects will enable us to determine mean parameter values for estimating breach probabilities. Once $v_p^a([y_i]_{i \in G}, [z_{pj}]_{j \in S})$, $v_p^c([y_i]_{i \in G}, [z_{pj}]_{j \in S})$ and $v_p^i([y_i]_{i \in G}, [z_{pj}]_{j \in S})$ are numerically computed, we could solve the model corresponding to P1 to determine the optimal set of controls.

The experiments are likely to yield us a rich set of data, and we will be able to perform sensitivity analysis as well as analyze attacker behavior. In conclusion, our methodology could be used for any given IT system configuration

References

- Cavusoglu, H., B. Mishra, et al. (2005). "The value of intrusion detection systems in information technology security architecture." Information Systems Research **16**(1): 28-46.
- Goel, A. L. and K. Okumoto (1979). "Time-dependent error-detection rate model for software reliability and other performance measures." IEEE Transactions on Reliability **R-28**(3): 206-211.
- Gordon, L. A. and M. P. Loeb (2002). "The economics of information security investment." ACM Transactions on Information and System Security **5**(4): 438-457.
- Highleyman, B., P. J. Holenstein, et al. (2003). Breaking the Availability Barrier: Survivable Systems for Enterprise Computing, 1st Books Library.
- Littlewood, B., S. Brocklehurst, et al. (1993). "Towards Operational Measures of Computer Security." Journal of Computer Security **2**: 211-229.
- McClure, S., J. Scambray, et al. (2003). Hacking Exposed: Network Security Secrets & Solutions, McGraw-Hill.
- National Institute of Standards and Technology (2004). FIPS 200: Minimum security requirements for federal information and information systems. Gaithersburg, MD, National Institute for Standards and Technology: 17.
- Ross, R., S. Katzke, et al. (2007). NIST Special publication 800-53: Recommended Security Controls for Federal Information Systems. Gaithersburg, MD, National Institute of Standards and Technology: 188.
- U.S. Code. 44. **Section 35**.
- Wood, B. J. and J. F. Bouchard (2001). Red team work factor as a security measurement. First Workshop on Information-Security Rating and Ranking.

ABBREVIATED CURRICULUM VITA

Limit: 2 pages, single-spaced outline format is permitted.

Include an abbreviated CV with education (baccalaureate to last degree awarded) including institution, discipline, degree and year; relevant professional positions held including institution and years of service; your most recent and relevant publications, working papers, projects and/or presentations including title, date, and name of publication/conference.

Education

SUNY Buffalo
Ph.D. in Information Systems (2002)
"eCommerce sourcing: Drivers, business value and intermediation"
Master of Science, Computer Science (coursework complete, anticipated 2008)
Indian Institute of Technology, Kanpur, India (1986–1992)
Master of Technology, Electrical Engineering
Bachelor of Technology, Electrical Engineering

Professional positions

August 2002 – Present: Assistant Professor, Department of Information Systems and Decision Sciences, College of Business Administration, University of South Florida
August 2001 – July 2002: Instructor, Department of Information Systems and Decision Sciences, College of Business Administration, University of South Florida
October 1992 – June 1997: Indian Police Service, Ministry of Home Affairs, Government of India

Journal papers

"A Framework for Security Analysis of Internet Technology Components Enabling Globally Distributed Workplaces", Shamik Banerjee, Manish Gupta, **Manish Agrawal** and H.R. Rao, ACM Transactions on Internet Technology, (Accepted, to appear, 2008)
"Software Effort, Quality and Cycle-Time: A Study of CMM 5 Projects", **Manish Agrawal** and Kaushal Chari, IEEE Transactions on Software Engineering, 33(3), pg 145 – 156, March 2007 (top 100 downloads, IEEE digital library Feb, Apr 2007)
"Multi-issue automated negotiations using agents", Kaushal Chari and **Manish Agrawal**, INFORMS Journal on Computing, 19 (4), pg. 588-595, Fall 2007
"Market reactions to e-business outsourcing announcements: An event study", **Manish Agrawal**, Rajiv Kishore and H.R. Rao, Information and Management, 43(7), pg 861-873, October 2006 (October- Dec 2006, ranked 22 in Science Direct listing of hottest 25 articles in the area of computer science, all journals (Aug 2007))
"Issues in IT-Offshore Outsourcing Coordination", S. Banerjee, **Manish Agrawal** and H. R. Rao, Journal of Marketing and Communication, 1(3), pg. 59-68, Jan. 2006
"Matching Intermediaries for information goods in the presence of Direct Search: An examination of switching costs and obsolescence of information", **Manish Agrawal**, G. Hariharan, Rajiv Kishore and H.R. Rao, Decision Support Systems, 41(1), pg. 20-36, Nov. 2005
"Ecommerce systems sourcing: An empirical examination of key determinants", Rajiv Kishore, **Manish Agrawal** and H.R. Rao, Journal of Management Information Systems, 21(3), pg. 47-82, Winter 2004-2005, Winter 2004-2005
"A behavioral model of digital music piracy", R.D. Gopal, G.L. Sanders, S. Bhattacharjee, **Manish Agrawal** and S.C. Wagner, Journal of organizational computing and electronic commerce, Vol. 14, No. 2, pg 89-105, 2004
"A Comparison of B2B E-Service Solutions", Dan Jong Kim, **Manish Agrawal**, Bharat Jayaraman and H. Raghav Rao, Communications of the ACM, Dec. 2003, pg 317 - 324
"Demystifying wireless technologies: Navigating through the technology maze", **Manish Agrawal**, K. Chari and Ravi Sankar, Communications of the AIS, Vol 12, article 12, Sep. 2003, pg 166-182

“Impact of Mobile computing terminals in law enforcement”, **Manish Agrawal**, H.R. Rao and G.L. Sanders, Journal of organizational computing and electronic commerce, Vol. 13, No. 2, Feb. 2003, pg. 73-89

“A Testbed for Modeling the Interactions of Application Service Providers (ASPs) with Clients through e-Marketplaces”, **Manish Agrawal**, H.R. Rao, R. Kishore and S. Upadhyaya, Vision, 5(1) Jan-June 2001.

Conference papers

“Information Market Based Decision Fusion”, Johan Perols, Kaushal Chari and Manish Agrawal, Utah Winter Conference, Feb. 2007

“Information Market Based Decision Fusion”, Johan Perols, Kaushal Chari and Manish Agrawal, ICIS 2006, Milwaukee, WI, Dec. 2006

“Information Fusion and Information Markets in Multi-Agent Systems”, Johan Perols and Manish Agrawal, WITS 2005, Las Vegas, Dec. 2005

“Impact of Learning Negotiation Support Systems on Overcoming Cognitive Limitations in Negotiations”, Manish Agrawal and Kaushal Chari, WEB 2005, Las Vegas, Dec. 2005

“Software Effort, Quality and Cycle-time: A Study”, Manish Agrawal and Kaushal Chari, INFORMS CIST 2005, New Orleans, Oct. 2005

“Business Process Integration using Web Services”, Kaushal Chari, Manish Agrawal and Saru Seshadri, Web 2004, Washington D.C., Dec. 2004

“A Conceptual Approach to Information Security in Financial Account Aggregation”, Hernant Padmanabhan, Lokesh Pandey, Manish Agrawal, H.R. Rao, and Shambhu Upadhyaya, Sixth International Conference on Electronic Commerce, Delft, The Netherlands, Oct. 2004

“Design and Evaluation of Software Agents for Online Negotiations”, K. Chari and Manish Agrawal, ICEIS-2004, Porto, Portugal

“Not just products: An examination of the evolution of IT offshore outsourcing”, Manish Agrawal, H.R. Rao and V. Sridhar, Informis 2003, Atlanta, GA

“A Framework for the Comparison of Business-to-Business E-Service Solutions”, Manish Agrawal, H.R. Rao, B. Jayaraman and Dan Kim, CIST 2001, Miami, FL

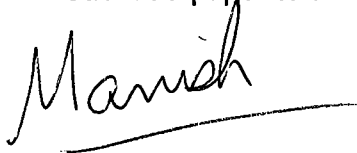
“The role of Intermediaries in Information Services Outsourcing: A testbed for simulation”, Manish Agrawal, R. Kishore and H.R. Rao, AMCIS 2001, Boston, MA

“A comparative analysis of e-commerce governance mechanisms”, Manish Agrawal, H.R. Rao and R. Kishore, AMCIS 2000, Long Beach, CA

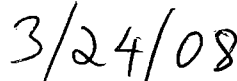
“Mobile computing terminals in law enforcement: An exploratory investigation of the Buffalo Police department”, Manish Agrawal, H.R. Rao and G.L. Sanders, PICMET 1999, Portland, OR

Undertaking: The applicant, if awarded Bear Stearns research Grant, agrees to the following:

- Acknowledge Bear Stearns IT Research Center as a funding source in all research publications generated from the proposed work.
- Maintain a project abstract and links to working papers from this project at the Bear Stearns IT Research Center webpage.
- Submit a paper to a Tier 1 journal of his/her field at the conclusion of the project.



Applicant Signature



Date Signed.