Association for Information Systems
AIS Electronic Library (AISeL)

3-1-2005

Current Research in Information Security and Privacy

Jollean Sinclaire
jsinclar@memphis.edu

Follow this and additional works at: http://aisel.aisnet.org/sais2005

CURRENT RESEARCH IN
INFORMATION SECURITY AND PRIVACY

Jollean K. Sinclaire

The University of Memphis

jsinclar@memphis.edu

Abstract

This paper reviews a range of current MIS research literature to identify research topics in information security and privacy. Results of this study indicate IT security provides the basis of current research in the area of information security and privacy. The results of this study reveal limited research in this area, particularly at the organizational level. One conclusion is that this lack of research results from organizational unwillingness to share information and statistics on security. Another conclusion is that research is needed in the area of information privacy. One area of future research may be organizational privacy policies. Two particular areas of interest may be user perceptions of privacy policies and opt-in/opt-out policies and procedures. Additionally, research related to individuals' concern for information privacy may be less problematic to study than organizational security issues. Research in this area is important because user concern for information privacy has the potential to affect the future of e-commerce.

Keywords
Information security; information privacy

Introduction

This paper reports on a structured review of a range of current MIS research literature undertaken to identify the nature of recent study in information security and privacy. The purpose of this review is to classify and analyze studies from this stream of research and identify today's hot topics in information security and privacy in an effort to detect emerging trends; to acknowledge issues where research exists; and uncover areas where research may be needed. By identifying those topics that are at the foundation of research in information security and privacy, as well as those that are new topics in this area, this paper may also serve to guide future research.

Security and Privacy Research

Because this study was designed to consider articles published by a number of journals, each with a unique perspective, it was necessary to begin with accepted and acceptable definitions of information security and information privacy. Defining information privacy as "the ability of the individual to control personally information about one's self," Stone, Gueutel, Gardner, and McClure (1983) report "this control-oriented definition of information privacy is consonant with many other conceptualizations of the same construct." Corporate IT security is defined by three general security goals: confidentiality, integrity, and availability (Panko, 2004). Therefore, research in security includes but is not limited to security architecture, security policy, cryptography, incident and disaster response, and managing the security function.

It was necessary to delimit what constitutes research in information security and privacy. General interest articles as well as opinion and technical commentary were excluded from consideration. Articles that cite or imply generally accepted research methodologies were included in this study, as were articles of a subjective-argumentative methodology. This study specifically considered the work of researchers representing educational institutions throughout the world and did not consider the work of practitioners or individuals representing commercial firms. However, any research article that was the product of collaboration between both academic and commercial individuals was considered for inclusion in this study.

The Journals

This review of current relevant literature included articles published over a recent two-year period in journals that have been widely and consistently ranked highly as publication outlets for IS research in North America (Whitman, Hendrickson, and Townsend, 1999) (Walstrom and Hargrave, 2001) (Mylonopoulos and Theoharakis, 2001). The specific journals included in the study are listed alphabetically in Table 1. A brief description of each of these journals is given below.

Table 1. Journals and issues included in this study

Journal	Date Range of Included Issues	Number of Issues
Communications of the ACM	Nov. 2002 – Oct. 2004	24 (monthly)
Information & Management	Dec. 2002 – Dec. 2004	16 (8 issues annually)
Information Systems Management	Fall, 2003 – Winter, 2004	8 (quarterly)
Journal of Management Information Systems	Fall, 2002 – Summer, 2004	8 (quarterly)

Communications of the ACM

Communications of the ACM is published by the Association for Computing Machinery. Founded in 1947, "ACM is a major force in advancing the skills of information technology professionals and students worldwide" (CACM, 2003). The 'Information for Authors' page at the CACM web site states, "The Communications of the ACM readership represents approximately 85,000 professionals from every known computing discipline: 80% are computing practitioners working in industry; 20% work in government and academia. The majority of readers have been involved in computing for over 12 years, and 65% have advanced degrees" (Communications of the ACM, online). Established in 1957, this journal publishes the research findings and ideas of the creators and innovators of the latest technology trends. This journal is the "premier computing magazine, internationally renowned and respected for its coverage of both existing and emerging technologies" (Communications of the ACM, online).

Information & Management

Founded in 1978, Information & Management, The International Journal of Information Systems Applications," serves managers, professionals, database administrators and senior executives of organizations which design, implement and manage Information Systems Applications." The goals of this publication are: "To collect and disseminate information on new and advanced developments in the field of applied information systems; To provide material for training and education in administrative data systems; To encourage further progress in information systems methodology and applications; To cover the range of information system development and usage in their use of managerial policies, strategies, and activities for business, public administration, and international organizations; To provide guidelines and insights on how to undertake successful information technology initiatives and learn to avoid failures through the study of success and failure patterns" (Elsevier, online).

Information Systems Management

Information Systems Management is published by Auerback Publications, New York, NY. Founded in 1990, this quarterly journal recently merged with Information Strategy: The Executive's Journal. Publication subjects include business, computer science, management, management information systems, computers and software, and high tech. Read by both practitioners and academicians, this journal publishes research that "presents problem solving strategies and techniques for managers of corporate information systems" (Auerbach Publications, online).

Journal of Management Information Systems

Journal of Management Information Systems, founded in 1984, provides a "forum for the presentation of research that advances the practice and understanding of organizational information systems." This publication offers that it "serves those

investigating new models of information delivery and the changing landscape of information policy making" (Business Source Premier, online).

From these four publications, twenty four articles addressing information security and privacy were selected for inclusion in this study. The number of articles included from each journal is shown in Table 2.

Table 2. Number of research articles per source

Journal	Articles
Communications of the ACM	17
Information & Management	3
Information Systems Management	4
Journal of Management Information Systems	0

Results

Results from this study reveal seventy-four percent of this subset of current research addresses IT information security and twenty-six percent addresses information privacy. Within research on security, twenty-nine percent of the articles address issues of planning, and seventy-one percent of the articles address issues of protection. An analysis of research within the protect function reveals that 50 percent pertains to authentication/verification, twenty-five percent is about types of threats, seventeen percent addresses standards, and 8 percent pertains to firewalls. The research on privacy addresses issues of user perceptions such as trust, privacy seals, and privacy standards, as well as ethical issues related to surveillance. The analysis of research topics is shown in Table 3.

Table 3. Research Topics

Survey of current research	
Information Security	74%
Information Privacy	26%
Research on Information Security	
Plan	29%
Protect	71%
Research on "Protect" Function	
Authentication/Verification	50%
Threats	25%
Standards	17%
Firewalls	8%
Research on Information Privacy	
User Perceptions	67%
Surveillance Issues	33%

The results of this study reveal a lack of research in the area of information security and privacy, particularly at the organizational level. This result is perhaps explained by discussing research by Kotulic and Clark (1999) in which they attempted to study security risk management at the firm level. Before developing questionnaires, Kotulic and Clark (1999) had secured commitments from five firms to pilot test the instruments; however, all five firms declined to participate when the instruments were presented. An additional thirty eight firms were contacted and ultimately one firm agreed to participate in the pilot study. Subsequently, four questionnaires were mailed to 1540 firms; however, only nine firms returned all four instruments for a response rate of less than one percent. Kotulic and Clark (1999) analyzed non-response feedback from seventy four firms to report twenty three percent of those firms stated they do not share any information about computer security policies with outside entities. We may conclude that a lack of research on information security and privacy results from organizational unwillingness to share information and statistics on security.

Another conclusion is that research is needed on information privacy. Results of this study found only six articles related to information privacy. One potential area of future research may be in the area of organizational privacy policies. These policies are generally public information and may be available online. Two particular areas of interest may be user

perceptions of privacy policies and opt-in/opt-out policies and procedures. Additionally, research related to individuals' concern for information privacy may be less problematic to study than organizational security issues and may hold promise because concern for information privacy has the potential to affect the future of e-commerce.

Limitations

The results of this study provide an important although limited snapshot of the nature of current research in information security and privacy. The selection of journals and the selection of the criteria for article inclusion bias the process. However, the journals selected are widely held to be among the top journals in MIS, and selection criteria stem from the consensus definitions and descriptions. A larger problem is the lack of multiple reviewers and classifiers in order to ascertain interrater reliability.

References

Basu, A., & Muylle, S. (2003). Authentication in E-Commerce. *Communications of the ACM*, 46(12), 159-166.

Burmester, M., & Desmedt, Y.G. (2004). Is Hierarchical Public-Key Certification the Next Target for Hackers? *Communications of the ACM*, 47(8), 69-74.

Cam-Winget, N., Housley, R., Wagner, D., & Walker, J. (2003). Security Flaws in 802.11 Data Link Protocols. *Communications of the ACM*, 46(5), 35-39.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7), 87-92.

Di Pietro, R., & Mancini, L.V. (2003). Security and Privacy Issues of Handheld and Wearable Wireless Devices. *Communications of the ACM*, 46(9), 75-79.

Earp, J.B., & Baumer, D. (2003). Innovative Web Use to Learn about Consumer Behavior and Online Privacy. *Communications of the ACM*, 46(4), 81-83.

Frolick, Mark N. (2003). A New Webmaster's Guide to Firewalls and Security. *Information Systems Management*, 20(1), 29-34.

Gordon, L.A., Loeb, M.P., & Sohail, T. (2003). A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM*, 46(3), 81-85.

Gupta, A., Tung, Y.A., & Marsden, J.R. (2004). Digital signature; use and modification to achieve success in next generational e-business processes. *Information & Management*, 41(5), 561-575.

Housley, R., & Arbaugh, W. (2003). Security Problems in 802.11-based Networks. *Communications of the ACM*, 46(5), 31-34.

Ives, B., Walsh, K.R., & Schneider, H. (2004). The Domino Effect of Password Reuse. *Communications of the ACM*, 47(4), 75-78.

Jain, A.K. & Ross, A. (2004). Multibiometic Systems. *Communications of the ACM*, 47(1), 34-40.

Jefferson, D., Rubin, A.D., Simons, B., & Wagner, D. (2004). Analyzing Internet Voting Security, *Communications of the ACM*, 47(10), 59-64.

Kotulic, A.G., & Clark, J.G. (2004). Why there aren't more information security research studies. *Information & Management,* 41(5), 597-607.

Kuechler, W., & Grupe, F.H. (2003). Digital Signatures: A Business View. *Information Systems Management*, 20(1), 19-28.

Liu, C., Marchewka, J.T., Lu, J., & Yu, C. (2004). Beyond concern: a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, 42(1), 127-142.

Martin, D., Wu, H., & Alsaid, A. (2003). Hidden surveillance by Web Sites: Web Bugs in Contemporary Use. *Communications of the ACM*, 46(12), 258-264.

Moores, T. & Dhillon, G. (2003). Do Privacy Seals in E-Commerce Really Work? *Communications of the ACM,* 46(12), 265-271.

Mylonopoulos, N. & Theoharakis, V. (2001). Global Perceptions of IS Journals, *Communications of the ACM*, 44(9), 29-33 (available online at http://www.alba.edu.gr/survey/IS/ISJournals.pdf)

Panko, R.R. (2004). *Corporate Computer and Network Security*. Pearson Education, Inc., Upper Saddle River, NJ

Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in Wireless Sensor Networks. *Communications of the ACM*, 47(6), 53-57.

Rees, J., Bandyopadhyay, S., & Spafford, E.H. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the ACM*, 46(7), 101-106.

Sipior, J.C., Ward, B.T., & Rongione, N.M. (2004). Ethics of Collecting and Using Consumer Internet Data. *Information Systems Management*, 21(1), 58-66.

Smith, H.J., Milberg, S.J., & Burke, S.J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, 20(2), 167-195.

Stone, E.F., Gueutal, H.G., Gardner, D.G., & McClure, S. (1983). A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, 68(3), 459-468.

Turner, E.C., & Dasgupta, S. (2003). Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. *Information Systems Management*, 20(1), 8-18.

Walstrum, K., & Hardgrave, W. (2001), Forums for Information Systems Scholars: III. *Information & Management*, 39, 117-124.

Wang, H., & Wang, C. (2003). Taxonomy of Security Considerations and Software Quality. *Communications of the ACM*, 46(6), 75-78.

Whitman, M.E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, 46(8), 91-95.

Whitman, M.E., Hendrickson, A. R. & Townsend, A. R. (1999). Research Commentary. Academic Rewards for Teaching, Research, and Service: Data and Discourse, *Information Systems Research*, 10(2), 99-109.