Pace University
DigitalCommons@Pace

Cornerstone 3 Reports : Interdisciplinary Informatics

The Thinkfinity Center for Innovative Teaching, Technology and Research

12-1-2010

Security@Web: Teaching Security with Alignment in Trust on the Web (FINAL REPORT)

Li-Chiou Chen
Seidenberg School of CSIS, Pace University

Mary Long
Lubin School of Business, Pace University

Follow this and additional works at: http://digitalcommons.pace.edu/cornerstone3

Part of the Digital Communications and Networking Commons

Recommended Citation
Chen, Li-Chiou and Long, Mary, "Security@Web: Teaching Security with Alignment in Trust on the Web (FINAL REPORT)" (2010). *Cornerstone 3 Reports : Interdisciplinary Informatics.* Paper 45.
http://digitalcommons.pace.edu/cornerstone3/45

This Report is brought to you for free and open access by the The Thinkfinity Center for Innovative Teaching, Technology and Research at DigitalCommons@Pace. It has been accepted for inclusion in Cornerstone 3 Reports : Interdisciplinary Informatics by an authorized administrator of DigitalCommons@Pace. For more information, please contact rracelis@pace.edu.

December 14th, 2010

Thinkfinity Cornerstone 3: Interdisciplinary Informatics - Grant Application (3nd Round)

Final Project Report

Security@Web: Teaching Security with Alignment in Trust on the Web

PI: Li-Chiou Chen, Associate Professor of Information Technology, Seidenberg School of CSIS
Co-PI: Mary Long, Professor of Marketing, Lubin School of Business

Email: { lchen, mlong} @ pace.edu

Project web site: http://csis.pace.edu/~lchen/secureweb/

Project Goals

A) Please outline your original goals.

This proposed project, Security@Web, will develop a course module that raises students' awareness of information security on the web. The project will also entail a research component examining the relationship between perceptions of trust and attitudes towards security. The research and course module will be informed by interdisciplinary research from both marketing and information security and therefore foster collaboration between the two participating schools.

Progress

B) What progress have you made towards your original goals on your project to date?

We have achieved all the original goals, including developing a web security course module and designing/conducting a web trust/security survey. During spring 2010, we focused on reviewing previous literature and forming our own theory of students' perceptions of trust and security risk on the web. An exploratory survey conducted in two marketing classes provided additional insights. During summer 2010, we designed our course module based on this preliminary work. In addition, we developed a student survey and test sites to assess students' perceptions of web site trust and security. During fall 2010, we piloted the survey in four sessions of CIS101 classes, one Seidenberg computer security class, one Lubin marketing class and one Lubin UNV101 class. We utilized the course slides we developed for debriefing after the survey.

C) What activities have been completed to contribute to meeting/progressing toward these goals?

Our progress is shown in the various education and research activities including theory development, exploratory study, course module development, survey development and course activities.

Theory Development

By researching previous literature, we formed a fundamental understanding of the concept of trust, in particular, web trust, and computer security risk. Trust has been defined in numerous ways in both the marketing and IT literature. Trust continues to be an elusive concept, defined and measured in numerous ways. As the study of business exchanges has shifted from physical goods to services and from bricks and mortar to online, the antecedents and definitions of trust continue to evolve. Trusting beliefs are often categorized by three attributes -- competence (ability of the trustee to do what the truster needs), benevolence (trustee caring and motivation to act in the trustee's interests), and integrity (trustee honesty and promise keeping) (McKnight, Choudhury and Kacmar 2002). Perceived security risk refers to an individual's judgment of the risk involved in a certain computer related activity. For example, students might provide their personal information to their school web site since they think that the school site is very secure and they sense a low security risk on the site. Perceived security risk can be measured based on the individual's perceived probability of risk, perceived consequences, and perceived controls (security countermeasures). Understanding how individuals perceive the exposure and the effects of risk is considered an important part of analyzing and managing technology-induced risk (Morgan 1981). However, risk perception of computer security has yet to be fully studied although the general perception of risk has been found to greatly impact individual computer decisions (Hardee et al. 2006). Research has empirically verified that higher perceived security control is positively related to trust in e-commerce websites (Chellappa & Pavlou 2002; Chen & Barnes 2007; Suh & Han 2003), users intention of purchasing (Bhatnagar et al. 2000; Ranganathan & Ganapathy 2002; Salisbury et al. 2001; Suh & Han 2003) and in willingness to use online banking (Liao & Cheung 2002).

Exploratory Study

We conducted an exploratory study to investigate the factors that students consider when evaluating whether or not a website is secure and trustworthy. We developed a short online questionnaire which included two sections of questions. In section one, students were asked to list the five websites they use the most and why they go to these sites. In section two of the survey, they were asked several open-ended questions: (1) When

would you trust a website? What are the signs and indications of a trustworthy website?; (2) Other than looking at the website itself, how else do you evaluate the trustworthiness of a website?; (3) How do you know a website is secure (i.e., your information is protected)? What are the signs and indications of a secure website?; (4) Other than looking at the website itself, how else do you evaluate the security of a website?

Course Module Development

We developed a course module in web security and trust, which was incorporated in classes during Fall 2010. The course module consisted of a short lecture on web security and a set of quiz questions to assess students' knowledge in web security. The module takes about half an hour of class time. We gave the course module slides and the knowledge quiz to the instructors who helped us with the web survey on security/trust. The slides were used for debriefing after the web survey. The slides can be downloaded from our project web site http://csis.pace.edu/~lchen/secureweb/.

The course module introduced the following topics to students:

- Common computer threats on the web
- Practices against web security threats
- Web security cues and technology
- Anti-phishing strategies

Second Web Survey Development

Based on our results from the exploratory study, we designed a second web survey to elicit students' awareness of web security and trust in a web site. The survey asked the students to browse through a bookstore web site and express their perceptions of security and trust of this web site. The questions measured students' perceptions of the following concepts on 7-point Likert scales: perceived security, trusting belief, intention to adopt security measures and intention to transact with the web site. The data collected from this survey will be used to validate the following hypotheses:

Hypothesis 1: Users' perceived security of a web site has a positive impact on their trusting belief.

Hypothesis 2: Users' perceived security of a web site has a negative impact on their intention to adopt security measures.

Hypothesis 3: Users' perceived security of a web site has a positive impact on users intention to transact with the site.

Hypothesis 4: Users' trusting belief of a web site has a negative impact on their intention to adopt security measures.

At the end of the survey, the survey also asked students 10 questions to assess their knowledge of web security. Below is a sample question from this knowledge quiz:

What is the function of a security padlock on a web site? (The correct answer is A)

A. to prove that the web site is genuine and the information transmitted is encrypted

B. to guarantee users' privacy

C. to explain its security method and privacy policy

D. to prove that the person who logs in is a legitimate user

Course Activity

The exploratory study was conducted in two undergraduate marketing classes in the Lubin School. Students were directed to complete an anonymous online survey about their Internet experiences. The classes were MAR 322 Marketing Research (26 students) and MAR 499 Advanced Marketing Management (27 students). The survey was done during class time and framed as an example of marketing research and demonstration of an online survey software (Qualtrics.com). The order of questions on security and trust were reversed for half the sample to eliminate order bias. After completion of the online surveys, students were debriefed and given the opportunity to comment on the study.

The second web survey was conducted in four CIS101 (CIS101 Introduction to Computing) classes, one Seidenberg class (CIT251 Computer Security Overview), one Lubin marketing class (MAR344 Customer Relationship Management) and one Lubin UNV101 class (UNV101 First Year Seminar: Introduction to University Community). We have collected 91 effective samples from the survey. The results of this study will be used to validate our hypotheses about students' perceptions of trust and security risk on the web. The survey is exempted for IRB review approved by Pace IRB #10-67.

We also distributed the web security course slides and answers to the security knowledge quiz to all the instructors who participated in this survey. This information was used for debriefing after the survey.

D) What activities have not been completed? Please indicate why they have not been completed.

Although we have completed all the activities proposed in this project, we are continuing to analyze the data collected from the survey to discover further research results. We will analyze the data utilizing statistical software and prepare the study for future publications.

Outcomes & Impacts

E) Please outline the outcomes you have received as a result.

All of our project outcomes and activities can be found in our project web site http://csis.pace.edu/~lchen/secureweb/. Below is a list of presentations and publications supported by the Thinkfinity grant:

- Li-Chiou Chen and Mary M. Long (October 2010) "Savvy or Naïve?: Factors that Students Consider when Evaluating the Trustworthiness and Security of Websites," presented at Direct/Interactive Marketing Research Summit, San Francisco, CA..
- Li-Chiou Chen and Gaurav Bansal, "An Integrated Model of Individual Web Security Behavior," Proceedings of the Sixteenth Americas Conference on Information Systems, Lima, Peru, August 12-15, 2010.
- Li-Chiou Chen and Mary M. Long, "Perceived Online Security and Trust from a Student Perspective: An Exploratory Study," Proceedings of the Global Business and Technology Association. ISBN: 1-932917-06-3, Spring 2010.

F) Has your project impacted students? If so, how many?

In general, the results of our study and the course module impacted students in terms of increasing their awareness about web security. In particular, during Spring 2010, the students in both MAR 322 Marketing Research and MAR 499 Advanced Marketing Management learned about designing an exploratory survey on web trust and security risk perception. During Fall 2010, students in various classes learned basic web security knowledge through our survey and knowledge quiz. These classes include CIS101 Introduction to Computing, CIT251 Computer Security Overview, MAR344 Customer Relationship Management, and UNV101. In total, the project impacted about 53 students during Spring 2010 and about 91 students in Fall 2010. We expect to distribute our course module slides and knowledge quiz information to more instructors in the future to broaden the impact.

G) Has your project impacted other faculty members? If so, how many?

There are 5 faculty directly involved in the surveys and the course modules including the PI and Co-PI. Faculty who participated in the survey have received course materials for teaching basic web security awareness.

H) Were there any unintended outcomes achieved?

None.

I) Do your outcomes reflect the change or benefit you were hoping to receive?

Yes, the outcomes of our project reflect the benefit that we planned to achieve. During the debriefing of students for both the exploratory and second survey, it was apparent that many Lubin students were not aware of objective signs of web security. After viewing the module and slides on security, many of the students admitted that this was an eye-opener and that it had heightened their awareness of security issues. In addition, Seidenberg students who took the Computer Security Overview class were more suspicious and cautious with the web site presented in the second survey than the CIS101 students. This observation implies that web security awareness might depend upon the computing environment as well as user education, which could be fostered via the teaching materials that we designed.

Thinkfinity Goals & Future Plans

J) How has your project furthered the Thinkfinity Cornerstone you selected?

Our project has certainly furthered the Thinkfinity Cornerstone III: Research in the Interdisciplinary Programs. We created a teaching module that was deployed in both the Seidenberg and Lubin Schools and also created a research instrument to study web security and web trust combining the expertise from both the Computing discipline and the Marketing discipline. Our publications support the research effort that we have accomplished and our course activities support the education goal that we are trying to achieve.

K) Describe your future plans for sustaining the program or project.

We plan to further analyze the survey data and submit the results for publication. In addition, more runs of surveys are planned in the next year to produce more solid support for our research hypotheses. The support we received from this Thinkfinity grant enabled us to build up a foundation in the education and research of web security and trust. The project is sustainable in the future since it has already created a set of teaching materials in web security awareness and a research instrument in the form of a user survey of web security and trust.

References

McKnight, D.H., Choudhury, V., & Kacmar, C. (2002). Developing and Validation Trust Measures for E-Commerce: An Integrative Typology. Information Systems Research, 13 (3), 334-359.

Morgan, M. G. (1981). Probing The Question of Technology-Induced Risk. IEEE Spectrum, 18(11) 58-64.

Hardee, J. B., West, R., & Mayhorn C. B. (2006). To Download or Not to Download: An Examination of Computer Security Decision Making. ACM Interactions 32-27.

Chellappa, R., & P.A. Pavlou. (2002). Perceived Information Security, Financial Liability, and Consumer Trust in Electronic Commerce Transactions. Journal of Logistics Information Management, Special Issue on 'Information Security', 11(5), 358-368.

Chen, Y. H., & S. Barnes. (2007). Initial Trust and Online Buyer Behavior. Industrial Management and Data Systems, 107, 21-36.

Ba, S. (2002). Establishing Online Trust Through a Community Responsibility System. Decision Support Systems, 31, 323-336.

Suh, B. & Han, I. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. International Journal of Electronic Commerce, 7(3), 135-161.

Bhatnagar, A., Misra, S., H. R. Rao. (2000). On Risk Convenience, and Internet Shopping Behavior. Communications of the ACM, 43(11), 98-105.

Ranganathan, C. & Ganapathy, S. (2002). Key Dimensions of Business-To-Consumer Web Sites. Information and Management, 39 (6) 457-465.

Salisbury, W., Pearson, P., Pearson, A.,& Miller, D. (2001). Perceived Security and World Wide Web Purchase Intention. Industrial Management & Data Systems, 101, 165 -176

Liao, Z., & Cheung, M. T. (2002). Internet-Based E-Banking and Consumer Attitudes: An Empirical Study. Information & Management, (39), 283-295