To Download or Not to Download: An Examination of Computer Security Decision Making

Jefferson B. Hardee | North Carolina State University | jbhardee@ncsu.edu
Ryan West | SAS Institute | ryan.west@acm.org
Christopher B. Mayhorn | North Carolina State University | chris_mayhorn@ncsu.edu

Imagine you are in the middle of studying for tomorrow's test when your antivirus software prompts you with a message indicating new virus definitions are available. Would you update the antivirus software now or later or not at all?

Imagine now that you're browsing online and you receive an instant message (IM) with a friendly greeting and a Web page link from one of your IM buddies. She asks that you follow the link to see an amusing picture. You're not busy at the moment but would you click on the link?

These vignettes illustrate the kinds of computer-security situations that people encounter on a daily basis. They are often mundane, seemingly small decisions that hide the potential for a security incident. While new authentication mechanisms can replace passwords to offer more secure and user-friendly security, any computer security situation that involves an action or decision from the user is open to risk. Therefore, understanding how users perceive and make security decisions is fundamental to designing security features that users will use and use well.

USABILITY OF SECURITY MECHANISMS

There has been a growing focus on the usability of security mechanisms over the past few years. Some authors suggest that regardless of how good security technology is, it is the "people problem" that must be overcome for successful security [4]. Previous studies have shown that security mechanisms for encryption, authorization, and authentication are difficult for users to understand or use. Most of the attention in this work has been on the interaction between the user and the system.

PUTTING THE "HUMAN" BACK INTO THE HUMAN-COMPUTER SECURITY INTERACTION

There have been fewer articles that focus entirely on the human side of the user-security interaction of late. Schultz, Proctor, Lien, and Salvendy [5] offer a taxonomy of human error in user-security interaction. In addition, several authors have explored perceived risks and safety behaviors in online shopping as they relate to Internet usage and various demographic variables [2]. Most of this work focuses on general perceptions or behaviors rather than specific security decisions and how they are made. Thus, there is a critical need for empirical research that bridges the gap between security decision making and the factors that influence likely action.

Thus, to complement much of the existing research in the area of computer security, the present study was designed to focus on the "human problem" by

SPECIAL SECTION HCI & SECURITY

experimentally manipulating a number of factors that might influence computer security decisions. A series of decision-making scenarios were designed to systematically vary by decision domain, risk, and gain-to-loss ratio in an effort to determine how computer users might respond to potential security decisions. One question that motivates this research is whether users differ when they make computer versus non-computer decisions. For this reason, the current study included both decision domains for the purpose of contrasting computer-based decisions with the baseline of non-computer decision making. Thus, if no differences arise, the large behavioral literature on non-computer decision making can be used to inform security practitioners about potential user behavior. Armed with this knowledge, practitioners may be able to develop more usable security software mechanisms.

A TEST OF DECISION MAKING WITHIN COMPUTER AND NON-COMPUTER DOMAINS

Fifty-six students enrolled at a public university volunteered to participate in a study that used a 2x2x3 repeated measures factorial design. The variables manipulated were decision domain (computer vs. non-computer), risk (high vs. low), and gain-to-loss ratio (high gains/low losses, equal gains/losses, low gains/high losses). A decision-making task composed of 24 decision scenarios was constructed such that 12 scenarios were within the computer domain and 12 were composed of non-computer-related decisions. In addition, the scenarios were equally divided within those two categories as being high or low risk. Risk was defined as the likelihood of suffering harm or loss; thus high-risk scenarios were associated with a greater probability of harm or loss. Conversely, low-risk scenarios contained a minimal probability of harm or loss. Finally, scenarios were equally divided to represent the three gain-to-loss ratios where some scenarios contained more gains than losses and others contained more losses than gains, or equal gains and losses. Two scenarios were developed to represent each of the six risk and gain-to-loss ratio combinations for a total of 12 computer and 12 non-computer scenarios.

DECISION MAKING AND TECHNOLOGY USAGE

The study used performance on a scenario-based decision task to draw conclusions about how risk and gain-to-loss ratio might affect decision-making within the domains of computing and non-computing security decisions. Each scenario presented a problem, and each participant was asked to choose between two decision-making options. For example, should one open an unfamiliar email attachment from an unfamiliar sender or delete the email? Following this question, participants were asked to assume

Overall

Gains	#	Comments	Losses	#	Comments
Time/Convenience	66	7.8%	Time/Inconvenience	303	50.5%
Protecting Information	293	34.4%	Money/Property Loss	111	18.5%
Protecting Money/Property	397	46.7%	Social/Emotional	54	9.0%
Social/Emotional	42	4.9%	Unsatisfied Need	65	10.8%
Protecting Self or Others	48	5.6%	Information loss	58	9.7%
Other	5	0.6%	Other	9	1.5%

Computer Decisions

Gains	#	Comments	Losses	#	Comments
Time/Convenience	41	9.2%	Time/Inconvenience	146	45.8%
Protecting Information	232	51.9%	Money/Property Loss	37	11.6%
Protecting Money/Property	162	36.2%	Social/Emotional	34	10.7%
Social/Emotional	9	2.0%	Unsatisfied Need	50	15.7%
Protecting Self or Others	0	0.0%	Information loss	49	15.4%
Other	3	6.0%	Other	3	0.9%

Non-Computer Decisions

Gains	#	Comments	Losses	#	Comments
Time/Convenience	25	6.2%	Time/Inconvenience	157	55.9%
Protecting Information	61	15.1%	Money/Property Loss	74	26.3%
Protecting Money/Property	235	58.2%	Social/Emotional	20	7.1%
Social/Emotional	33	8.2%	Unsatisfied Need	15	5.3%
Protecting Self or Others	48	11.9%	Information loss	9	3.2%
Other	2	0.5%	Other	6	2.1%

Table 1: Coding Scheme and Descriptive Data for Qualitative Comments

that they had made the more conservative of the two decisions. Under this assumption, they were asked to make comments about the gains and losses of the decision.

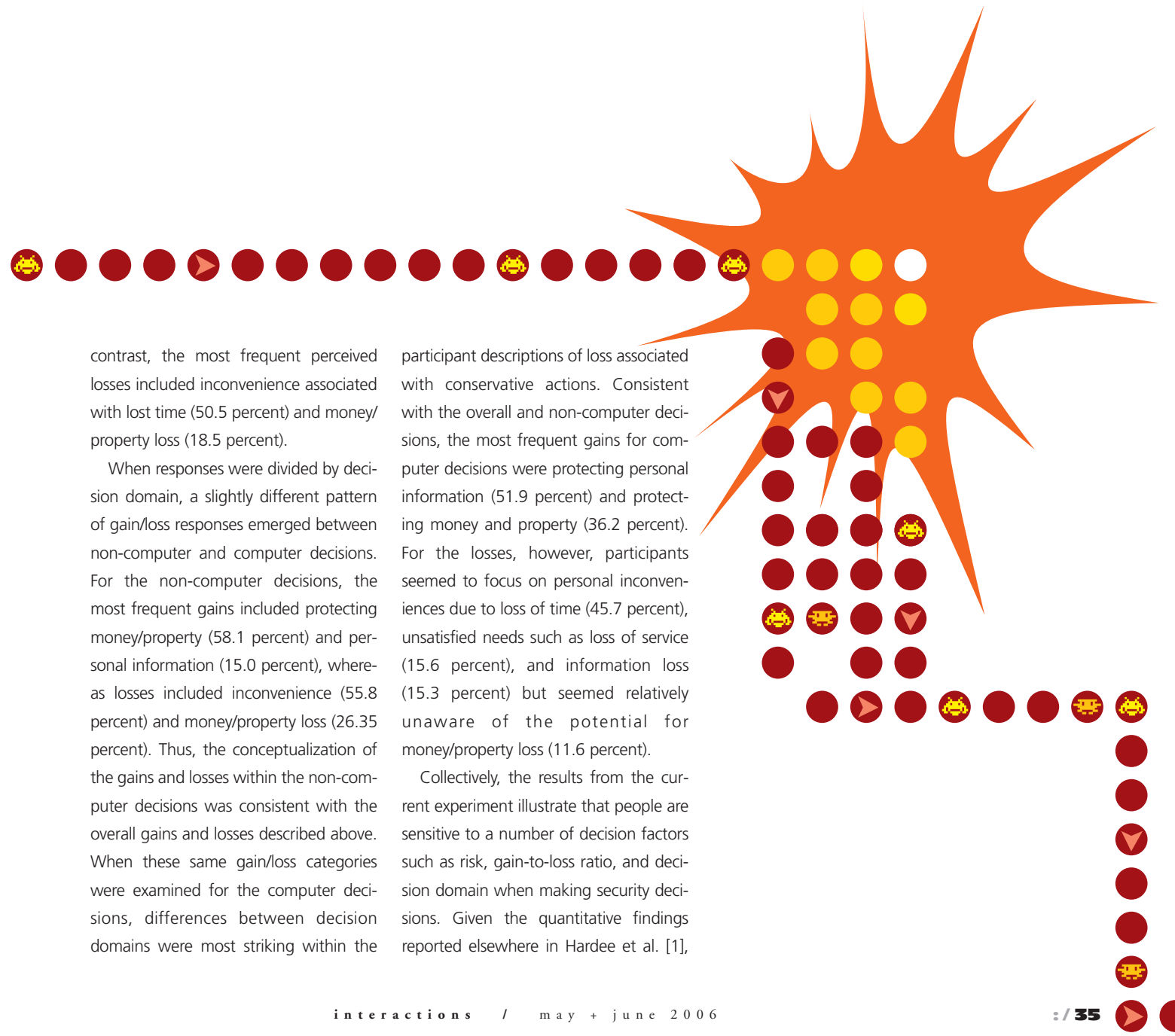
A survey was constructed to assess the participant's behavior, knowledge, or experience with respect to certain domains (available from the first author upon request). Analyses revealed that all participants were relatively frequent users of technology and that they had adequate experience to make informed decisions on the scenario-based decision task.

FINDINGS

While performance on the quantitative decision-making task and the survey data is described elsewhere [1], this article focuses on participants' qualitative comments to determine what variables were considered as either gains or losses during the decision task.

To determine how participants assessed the relationship between gains and losses, their comments associated with the most conservative decision option were examined. Table 1 reflects the coding scheme that was developed to categorize how participants conceptualized gains and losses overall, then within the computer and non-computer decision domains. Two independent raters used the coding scheme to evaluate each of the 1,451 open-ended responses given by the participants and inter-rater reliability was 94.8 percent.

Overall, participants made 851 comments to describe general gains and 600 comments to describe general losses. As reflected in Table 1, the most frequent gains cited included protecting money and property (46.6 percent) followed by protecting information (34.4 percent). By



contrast, the most frequent perceived losses included inconvenience associated with lost time (50.5 percent) and money/property loss (18.5 percent).

When responses were divided by decision domain, a slightly different pattern of gain/loss responses emerged between non-computer and computer decisions. For the non-computer decisions, the most frequent gains included protecting money/property (58.1 percent) and personal information (15.0 percent), whereas losses included inconvenience (55.8 percent) and money/property loss (26.35 percent). Thus, the conceptualization of the gains and losses within the non-computer decisions was consistent with the overall gains and losses described above. When these same gain/loss categories were examined for the computer decisions, differences between decision domains were most striking within the participant descriptions of loss associated with conservative actions. Consistent with the overall and non-computer decisions, the most frequent gains for computer decisions were protecting personal information (51.9 percent) and protecting money and property (36.2 percent). For the losses, however, participants seemed to focus on personal inconveniences due to loss of time (45.7 percent), unsatisfied needs such as loss of service (15.6 percent), and information loss (15.3 percent) but seemed relatively unaware of the potential for money/property loss (11.6 percent).

Collectively, the results from the current experiment illustrate that people are sensitive to a number of decision factors such as risk, gain-to-loss ratio, and decision domain when making security decisions. Given the quantitative findings reported elsewhere in Hardee et al. [1],

the most conservative decisions occurred when it was apparent that risk was high. Moreover, participants' perceptions of the gain-to-loss ratio was important in driving the decision process such that more conservative decisions occurred when losses were perceived as being greater or equal to gains. Also, there was no difference between computer and non-computer decisions when risk and gain-to-loss ratio were held constant. Perception of risk greatly impacted computer decisions.

The current results are informative because they supplement the results of Hardee et al. by revealing that participants consistently conceptualized the nature of gains across decision domains in terms of protecting information, money, and property; however, conceptualization of loss information varied by decision domain. While non-computer decision losses were described in terms of inconvenience and money/property loss, losses within the computer domain appeared to focus more on personal inconvenience such that decision-makers were relatively unaware of risks to money and property loss.

SOFTWARE DESIGN RECOMMENDATIONS

Drawing on the present results and past research [1], a number of general recommendations can be made to assist security software designers in making their products more usable. Given the nature of the text-based scenarios developed for this study, recommendations for designers will be limited to factors that can easily be manipulated to improve the likelihood that users will make secure decisions by altering the wording or decision frame of their product.

- Explicit text should be used to identify the highly risky nature of the decision and the consequences of the outcome.
- Efforts to highlight the greater potential for losses should be made.
- To facilitate conservative decision making, the severity of the loss and the likelihood of the incident should be made available simultaneously to the user.
- In computer-security tasks, users need to be reminded of the potential to lose money and property.
- Emphasize potential losses and directly contrast these with an estimate of time investment to mitigate user's perceptions of time loss as an inconvenience.

APPLYING THE RECOMMENDATIONS TO SECURITY WARNINGS

These recommendations might prove useful in developing more effective security software by honing the attributes of warning messages received by users. The main purpose of warnings is to decrease harm from hazards to people and property. Because technology-based warning-delivery systems have received attention as a possible outlet for improving safety in a number of domains [6], the application of this knowledge to security warn-

ings seems to be a natural extension of previous work in the area of risk communication. Given the recommendations for altering the wording of computer security warnings listed above, the following examples might be easily implemented to resolve the security dilemmas represented by the opening vignettes that illustrated everyday computer decision making. For the vignette that described an interaction with antivirus updating, a warning message that simply alerts the user to the presence of an update may not be effective. A more effective warning might explicitly describe the potential for loss (e.g., a tangible financial figure for the cost of one's computer system) should a virus be contracted and contrast this with an estimate of time investment necessary to update the software. For the vignette that described a potentially harmful Web-page link nested within an instant message, a warning message that pops up to inform the user of the likelihood of virus transmission via this mode of communication might be more effective than the minimal warnings that users currently receive.

CONCLUSIONS

Combining the evaluation approach described in this article with potential alterations of security warnings should allow designers to improve security systems. By supplementing preexisting knowledge from the literature with suggestions from the people who are actually using these security programs, the likelihood of successful application and usability should improve. Much work remains, however. Empirical investigations into the effectiveness of the new security warning messages based on the design recommendations described above are essential to assisting security practitioners to design usable software to protect online safety. Moreover, future research in this area might focus on whether user characteristics such as personal computing experience or situational factors such as stress and time pressure influence the likelihood of making conservative computer security decisions.

REFERENCES **1.** Hardee, J. B., Mayhorn, C. B., & West, R. T. (submitted). *You downloaded WHAT?: Computer-based security decisions*. 50th Annual Meeting of the Human Factors and Ergonomics Society. Santa Monica, CA: HFES. **2.** Milne, G. R., Rohm, A. J., & Bahl, S. (2004). *Consumers' protection of online privacy and identity*. The Journal of Consumer Affairs, 38(2), 217-232. **3.** Miyazaki, A. D., & Fernandez, A. (2001). *Consumer perceptions of privacy and security risks for online shopping*. The Journal of Consumer Affairs, 35(1), 27-44. **4.** Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley & Sons. **5.** Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). *Usability and security: An appraisal of security issues in information security methods*. Computers and Security, 20 (7), 620-634. **6.** Wogalter, M. S., & Mayhorn, C. B. (2005). *Providing cognitive support with technology-based warning systems*. Ergonomics, 48(5), 522-533.

ABOUT THE AUTHORS

Jefferson B. Hardee is a graduate student pursuing his MS in the Ergonomics/Experimental Psychology program at North Carolina State University in Raleigh, North Carolina. He received his BS in computer science from North Carolina State University in 2003.

Ryan T. West is a user experience researcher who has studied enterprise-class systems administration at Microsoft and now SAS Institute. Ryan has a PhD in cognitive psychology from the University of Florida.

Christopher B. Mayhorn is an assistant professor in the Ergonomics/Experimental Psychology Program at North Carolina State University in Raleigh, North Carolina. He received his PhD in cognitive/experimental psychology from the University of Georgia in 1999.