Mental Models of Computer Security Risks

Farzaneh Asgharpour
School of Informatics
Indiana University
Bloomington, Indiana, USA
fasgharp@indiana.edu

Debin Liu
School of Informatics
Indiana University
Bloomington, Indiana, USA
deliu@indiana.edu

L. Jean Camp
School of Informatics
Indiana University
Bloomington, Indiana, USA
ljcamp@indiana.edu

ABSTRACT

Improved computer security requires improvements in risk communication to naive end users. Efficacy of risk communication depends not only on the nature of the risk, but also on the alignment between the conceptual model embedded in the risk communication and the recipients' perception of the risk. The difference between these communicated and perceived mental models could lead to ineffective risk communication. The experiment described in this paper shows that for a variety of security risks self-identified security experts and non-experts have different mental models. We illustrate that this outcome is sensitive to the definition of "expertise". We also show that the models implicit in the literature do not correspond to experts or non-expert mental models. We propose that risk communication should be designed based on the non-expert's mental models with regard to each security risk and discuss how this can be done.

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: Invasive software, Unauthorized access; K.4.4 [**Electronic Commerce**]: Security; D.2.2 [**Des-ign Tools and Techniques**]: User interfaces; H.1.2 [**User/ Machine Systems**]: Human factors, Human information processing, Software psychology; D.2.2 [**Design Tools and Techniques**]: User interfaces; D.m [**Miscellaneous**]: Software psychology

General Terms

Design, Security, Human Factors

Keywords

Security, Privacy, Mental Models, Card Sorting, Risk Communication, Behavioral Economics, Psychology of Security

1. INTRODUCTION

The growing reliance on online services, the exponential growth of security breaches [7], zombies, and botnets [20] suggest a need for better security practice by average users. Better risk communication about privacy and security risks is needed to change user behavior. Risk communication typically consists of messages designed by security experts to inform a community of non-experts.

Effective security risk communication requires both communicating risk information and motivating the appropriate risk behaviors. One may think that since experts know the risks their mental model is the most reliable mental model for designing risk communication instruments. The key point is that the purpose of risk communication is not conveying the perfect truth to the users, but rather prompting them to take an appropriate action to defend their system against a certain threat. While mitigation of a risk requires knowledge of the nature of the risk, efficacy of the risk communication requires the experts to understand the mental model of their target group.

The mental models approach is a risk communication method based on the conceptual models of recipients of risk communication. A mental model is a simplified internal concept of how something works in reality. This concept is case specific and is subject to change due to life experience, stigmatization, perception, and individual information processing strategies [25]. The mental models approach has improved risk communication in environmental as well as medical risk communication [16, 26]. Mental models have been explored in privacy research [12].

An examination of the security literature has found five widely used conceptual models implicit in language or explicit in metaphors [5]. These conceptual models form the basis of our exploration into mental models:

Physical Safety: The physical concept of security is implicit in descriptions of 'locks' and 'keys'. This concept implies individual and localized control.

Medical Infections: The model of security incidents as medical infections is grounded in the patterns of diffusion of malicious code infectious diseases, and the importance of heterogeneity in the larger network [18]. Some studies of network security have stressed the concept of the network as an ecosystem of security.

Criminal Behavior: Computer security violations can be crimes or may seem to be criminal. The concept of computer risks as risk of being a victim of crime implies that users or machines are targeted.

Warfare: The warfare concept of computer security implies the existence of a determined implacable enemy. It

has the potential to leverage horror by leveraging the horrors of war [11].

Economic Failure: Security and network or software vulnerabilities can be seen as market failures [2, 23, 28]. Vulnerabilities, in particular, can be seen as externalities [6]. Computer security failures cause downtime and costs [8, 14].

The mental models approach has not been formally evaluated in terms of its applicability to security risk communication. In this formal evaluation, we have a series of questions to answer. First, do the mental models implicit in the security literature correlate with the mental models of experts or non-experts? Second, do the mental models of experts (who create risk communication) correlate with the mental models of lay users (who receive risk communication)? Third, how sensitive is the correlation between experts' and non-experts' mental models to the definition of expertise?

In order to answer the above questions we have performed two card sorting [15] experiments. The two experiments differ in definition of expert and non-expert. Here we describe complete analysis of the first and second experiment and compare the two.

As a preliminary result, our study approves that the concepts of security as embedded in literature are not well matched to the mental models of experts or non-experts. We found that experts and non-experts have significantly different mental models. Our results proved sensitive to the definition of expert. The more stringent the definition of the expert and non-expert the greater the distance between their mental models.

Section 2 summarizes the related work in risk communication. Section 3 explains the details of our experimental setup. Section 4 covers the data analysis and findings. Section 5 concludes the paper

2. RELATED WORK

Mental models have been used to examine user behavior in terms of privacy. Diesner et al. [12] have studied the mental models of data privacy in India by conducting interviews.

Acquisti and Gross [1] have shown that individuals have unrealistic risk assumptions in online social networks. Their study shows that people's privacy concerns are only a weak predictor of their membership to the network.

Mental models have been widely used in human-computer interaction and usability [22]. In HCI, a mental model is a set of assumptions or beliefs about how a system works. People interact with systems according to their beliefs and assumptions about the system [24, 25]. Norman [25] suggests that the usability, functionality and learnability of the conceptualized model of the designer depend on the alignment between the conceptualized model of the design and the mental models of the end users. From these three factors, the functionality, and learnability of the risk communication refer to its potential to prompt the target group to take the desired action to mitigate the addressed risk.

Cosantine and Lockwood [9] define four criteria for usability of a product: learnability, retainability, efficiency of use and, user satisfaction. Learnability and retainability are the two criteria pointing to the role of mental models in usability. In other words, to the extent that a correct mental model could be learned and retained by a user, the user will be more effective.

Morgan [21] has applied mental models to a wide range of environmental applications. Bostrom [3] has applied mental models in home hazards. Fischoff [13] proposes using mental models to minimize over-confidence in individual perceptions of personal safety, such as shown by Acquisti [1] in case of privacy. Keller [17] proposes using mental models to mitigate the availability heuristic which produces irrational risk behavior.

In our previous work [5] we initiated the idea of using mental models in security risk communication. In risk communication the concept of mental models is subtly distinct from the concept of mental models in usability. This work is grounded in mental models as it has been developed in environmental risk communication [10]. The goal of mental models in environmental research is to enhance risk awareness about household toxic and alter consumer behavior [21]. Like computer security, environmental risks are much more complex in households. Paint stripper and other chemical hazards are, like computers, more easily regulated in the work place than home.

3. EXPEIMENT

3.1 Card Sort

Due to the complexity of human knowledge acquisition and psychology, the discovery of implicit mental models is a difficult task. This task could be done using various elicitation techniques such as Teachback Interviews, Repertory Grid, Goal-Oriented Approach, Grounded Theory and Card Sort [4]. Card sorting [7, 27] is a structured elicitation technique done by requiring a subject to sort a pile of cards with words written on them into different piles.

There are two kinds of card sorting: closed and open. In a closed card sort a subject must choose to classify label of each card into a set of predefined groups. In an open card sort no labels are given and the subject can sort the words into arbitrary groups according to that subject's perception. The benefit of the card sort technique is that it is easy for the subjects to perform. We applied a closed card sort to evaluate the mental models of lay users and experts with regard to security risks.

3.2 Experiment Design

We designed an experiment to answer the following questions:

1. What are the mental models of experts and non-experts with regard to a set of security risks (given in the experiment)?
2. Do the mental models implicit in the security literature correlate with the mental models of experts or non-experts?
3. To what degree do the mental models of experts correlate with the mental models of lay users?
4. How sensitive is the correlation between experts' and non-experts' mental models to the definition of expertise?

We used the card sorting technique to answer the first two questions. To find the correlation between people's mental models and their level of expertise in security we repeated

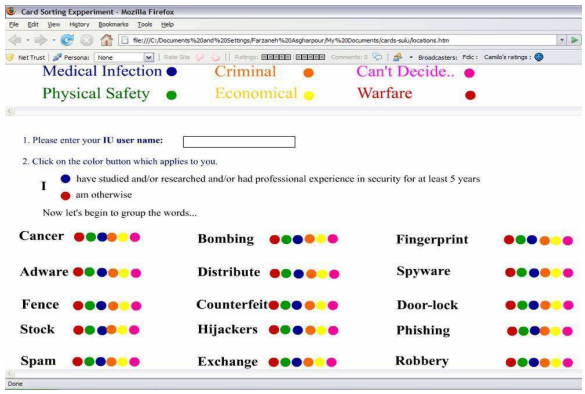

Figure 1: Screenshot of the card sorting experiment

the same card sorting experiment twice, each time with a different definition of "expert" and "non-expert". Throughout the paper we refer to the two implementations of the experiment as experiment 1 and 2. We addressed the third question by comparing the results of the two experiments. In this section, we first explain the shared setup of the card sort experiment and then describe the differences between experiment 1 and 2.

Experimental Interface: We developed a closed card sort experiment to estimate a mental model for each security risk. To recruit a large population of participants, we performed the experiment online. Details about the recruitment process and participants follow.

The participants were given six label and color pairs: physical security-green, medical infection-blue, warfare-red, criminal behavior-orange, economics failure-yellow, and "I can't decide"-purple. The participants labeled a word by changing its color to correspond to the color of the label. Each word was accompanied with six colored buttons. Clicking on each button changed the color of the corresponding word into the color of the selected button. Figure 1 shows a screen-shot of the experiment's interface. To avoid effecting the participants' decisions, we did not follow any specific cultural pattern in associating colors with labels. For instance, the color green is associated with peace for some people and with the environment for others. The arbitrary color selection made the participants refer to the instructions frequently. This can lead to subjects being more careful in assigning colors to words.

The experiment was developed using Macromedia Flash and PHP.

Words and Labels: A closed card sort experiment requires first and foremost a set of words and labels. We asked the participants to group the given words into these six labels: physical security, medical infections, criminal behavior, economic failure, warfare and "I can't decide". We instructed them to label a word with "I can't decide" if they could not decide, had no impression, or felt the word fit none of the other categories.

The words related to each mental model were selected using Webster's Thesaurus. For instance, the words selected for security as crime are synonyms to "theft" according to Webster's Thesaurus. See Table 3 for the word list. The participants were allowed and encouraged to look up the words with which they were not familiar. There were 29 security related words, 6 physical security, 9 disease, 9 criminal behavior, 7 economic failure and 6 warfare-related words.

Levels of Expertise: We considered two levels of expertise in security: expert (E) and non-expert (NE). Experiment 1 and 2 differ in the definition of expertise. In both experiments the definitions of expert and non-expert were given in the instruction section. The participants declared their expertise according to the given definitions.

In experiment 1 participants declared their expertise according to the following definitions.

Expert (E_1): A person who knows the technical definitions of all the security-related words.

Non-Expert (NE_1): One who does not know the technical definition of the security risks and at most knows some practical aspects of the risks.

In experiment 2, participants declared their expertise according to the following definitions.

Expert (E_2): One who has at least five years experience in security as a researcher, student or practitioner.

Non-Expert (NE_2): Otherwise

Since E_2 is a more restricted definition of expert, throughout the paper we refer to E_1 and E_2 as weak-expert and strong-expert respectively. For consistency, we refer to NE_1 and NE_2 as weak-non-expert and strong-non-expert respectively.

Participants: The first experiment included 22 experts and 49 non-experts. The second experiment included 11 experts and 27 non-expert participants. In both experiments the participants were 18-50 years old. They were faculty, staff, graduate and undergraduate students in informatics or computer science departments. Our target participant was someone who had some previous knowledge or experience with computers so they were familiar with the general notion of computer security.

Why two experiments? The reason for having two implementations of the card sorting experiment is to find the correlation between the definition of expertise and the related mental models. The second experiment illustrated a need for more detailed repeated experiments, but answered our immediate concerns.

4. ANALYSIS

The methodology and definitions introduced in this section apply to both experiments.

For each group of participants, experts and non-experts, we calculated the matrix of intra-similarity between the words. First the original data were tabulated. Each time a participant marked a pair of words with the same color, we count that as a vote for similarity between the two words.

Therefore, as an example, if most of the participants mark the words "trade" and "stock" with the same color, then we can say these two words are highly similar. In contrast, if only a few participants assign the words "war" and "fever"

Table 1: List of Words Given in the Card Sorting Experiment (the first three words under each mental model are the *Obvious Words*)

Crime	**Medical**	**Physical**	**Warfare**	**Economic**	**Security**
Theft	*Epidemic*	*Fence*	*War*	*Trade*	Identity theft
Housebreaking	*Fever*	*Door-lock*	*Bombing*	*Export*	Hijackers
Kidnapping	*Illness*	*Shield*	*Destroy*	*Stock*	Cookies
Fingerprint	Cancer	Inviolability	Terror	Distribute	Adware
Counterfeit	Detoxification	Invulnerability	Attack	Exchange	Spyware
Robbery	Nausea		Suicide	Endorse	Phishing
Mugging	Inflammation			Advertise	Spam
Vandalism	Contagious			Risk	DoS attack
Injection	Sore				Drive-by-download
					Trojan
					Keystroke logger
					Junk mail
					Virus
					Worm
					Hacking
					Binder
					Exploit
					Zombie
					Authentication
					Click fraud
					Password
					UserID
					Firewall
					Backdoor
					Blacklist
					Spoofing
					Dropper
					Address book
					Honeypot

Table 2: Number of weak-non-experts labeling each pair of words with the same color (Partial NSM)

	Cancer	Bombing	Fingerprint	Adware
Cancer	49	4	1	2
Bombing	4	49	1	5
Fingerprint	1	1	49	12
Adware	2	5	12	49

with the same color, we interpret this result as these two words being dissimilar. This way, we developed two 66 × 66 matrices, one for experts and one for non-experts. We named these two matrices *Expert's Similarity Matrix* (ESM), and *Non-expert's Similarity Matrix* (NSM). As an example, Table 1 shows part of the NSM matrix in experiment 1. For instance, according to this table 12 weak-non-experts consider "Adware" and "Fingerprint" as similar words.

In order to reveal underlying perceptual dimensions that participants use to distinguish among these words, we show the symmetric matrices via multidimensional scaling map.

4.1 Methodology

We use the multidimensional scaling (MDS) [10] method to locate the expert's and non-expert's similarity matrices, ESM and NSM, into a two dimensional space. The multidimensional scaling (MDS) method is used to find structure in a set of distances (dissimilarities). MDS assigns objects to specific points in a conceptual space such that the distances between points in the space match the given dissimilarities of the data. The dimensions of this conceptual space can be used and interpreted to further understand the data [19]. Since MDS considers either relative distance or similarity between observations, one can equally map the observations either using similarity or dissimilarity matrix. MDS could transform one matrix into the other using matrix operations. Applying MDS we map the words from the card sort into a two dimensional space and then, considering relative distances between the words, assign mental models to each security risk.

We use the software SPSS (Statistical Package for the Social Sciences) to convert the similarity matrices into the distance matrices. Even though we derived the set of related words for each mental model from Webster's Thesaurus, the participants sometimes labeled the words differently from our original assignment. Therefore, we were motivated to highlight some of the mental models words as *Obvious Words*. (Table 3 shows a list of three obvious words under each mental model). We distinguish these words as obvious words since for each group of three words, at least 85% of the participants have labeled all the words with the same mental model. For instance, 90% of all the participants labeled the words "illness", "epidemic", and "fever" as medical infections. Throughout the paper, we refer to each set of obvious words under a specific mental model as an *Obvious Mental Model*. For instance, "illness", "epidemic", "fever" is the Obvious Medical Mental Model.

For each risk r, in the set $R = \{r_1, r_2, ..., r_{29}\}$ of the given risks in our card sort experiment, we define the expert-distance between r and an obvious mental model $M = \{w_1, w_2, w_3\}$ as

$$D_E(M, r) = \sum_{1 \leqslant i \leqslant 3} d_E(w_i, r) \quad (1)$$

Where $d_E(M, r)$ is the expert-distance between w_i and r according to the expert distance matrix. We define the non-expert-distance, $D_{NE}(M, r)$, similarly.

Finally to each risk r we assign the expert/non-expert mental models according to the following definition. Suppose that the risk r has the following expert/non-expert distances from the obvious mental models:

$$D_1 \leqslant D_2 \leqslant D_2 \leqslant D_4 \leqslant D_5 \quad (2)$$

The expert/non-expert mental models were assigned to any risk r based on the relative distance to r. Therefore, the mental model of r is M_1 with the minimum distance, D_1, from r.

4.2 Findings

4.2.1 Maps

The similarity matrices ESM and NSM define the corresponding dissimilarity matrices EDM and NDM. Figures 2 and 3 show the MDS maps of the dissimilarity matrices considering all the security and the obvious words in the experiment 1. Figures 4 and 5 show the MDS maps of the dissimilarity matrices considering all the security and the obvious words in the experiment 2.

- Both weak-experts and weak-non-experts isolate the medical mental model from the rest of the words. Therefore, medical mental model is not well matched to the mental models of weak-experts and weak-non-experts.

- Weak-experts exclude the warfare and the economics failure mental models, whereas non-experts do not.

Considering Figures 4 and 5, in experiment 2

- In the strong-expert and strong-non-expert maps, the medical mental model is isolated from the rest of the words. With the exception of the risk "Virus" for strong-non-experts, the medical mental model is not well matched to the mental models of strong-experts and strong-non-experts.

- Criminal, physical and economic mental models are closer to computer security than other mental models for strong-non-experts.

- Criminal, physical and warfare mental models are closer to computer security than other mental models for strong-experts.

4.2.2 Mental Models

Based on the methodology explained in Section 4.1, for each risk r and each group of participants, the mental model with minimum distance from r is assigned as the mental model of that risk r. We apply this criteria and find the mental models of experts and non-experts in each experiment. Figures 6 and 7 illustrate the results.

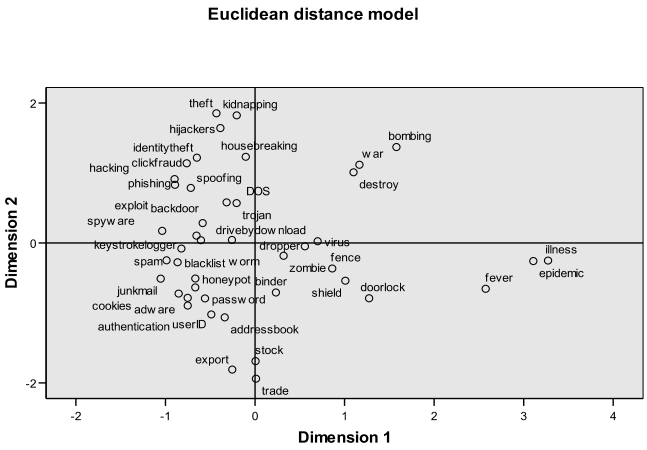

Figure 2: MDS Map for Weak-Experts

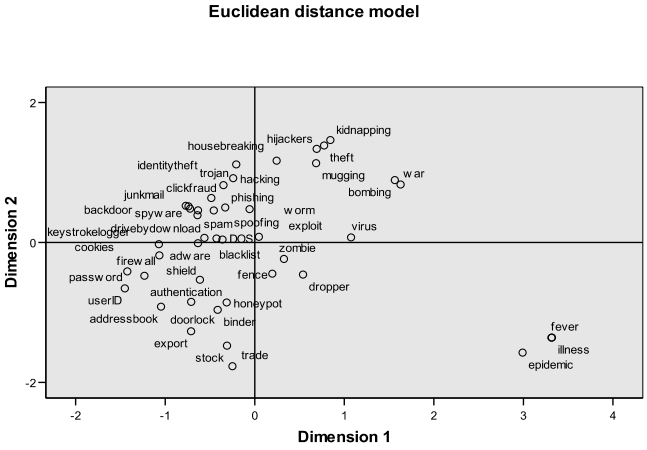

Figure 4: MDS Map for Weak-Non-Experts

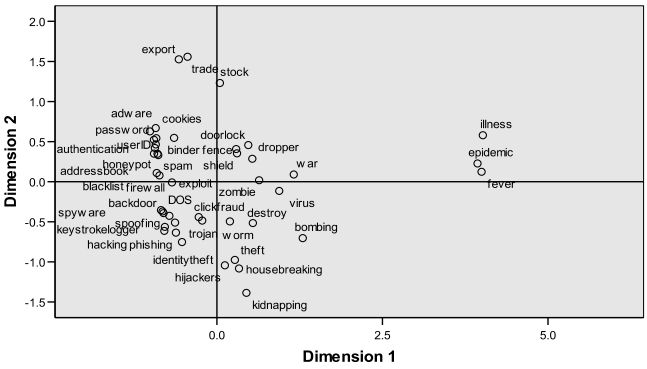

Figure 3: MDS Map for Strong-Experts

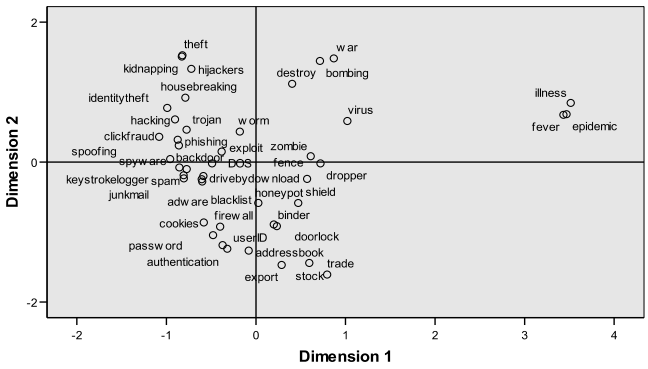

Figure 5: MDS Map for Strong-Non-Experts

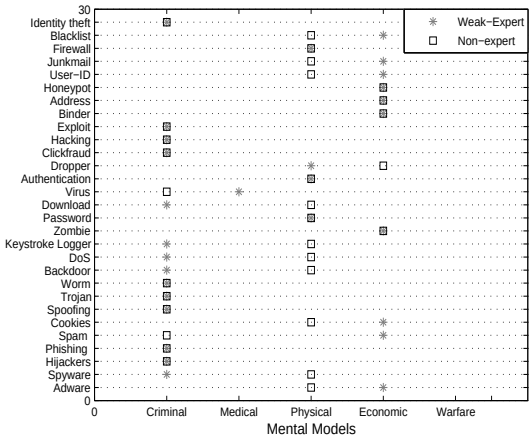

Figure 6: Mental models of weak-experts and non-experts in Experiment 1

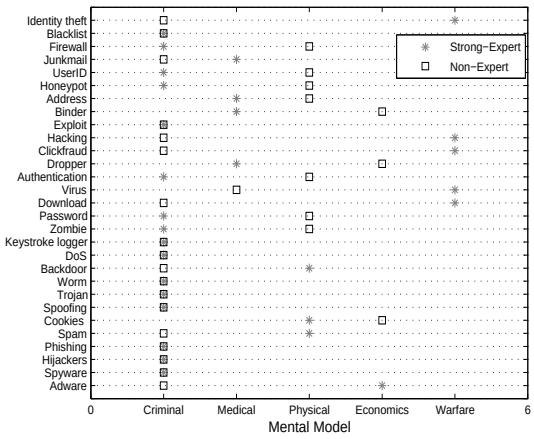

Figure 7: Mental models of strong-experts and non-experts in Experiment 2

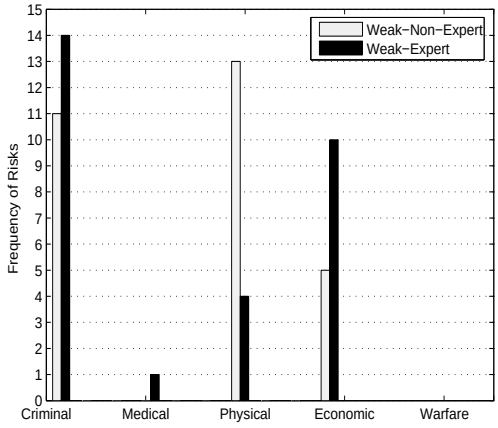

Figure 8: Distribution of Mental models For Security Risks in Experiment 1

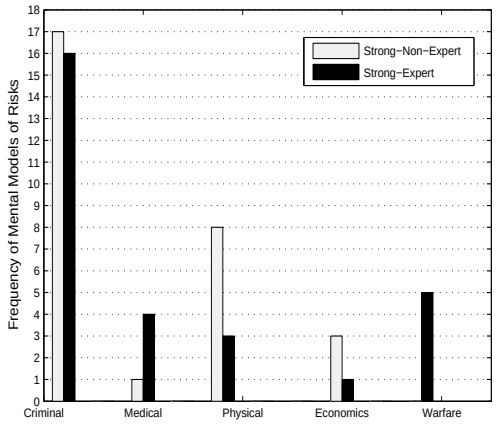

Figure 9: Distribution of Mental models For Security Risks in Experiment 2

Table 3: percentage of 29 risks assigned to each MM

MM	W-Expert	W-NE	S-Expert	S-NE
Criminal	48%	38%	55%	59%
Physical	14%	45%	11%	28%
Warfare	0%	0%	17%	0%
Economic	34%	17%	3%	10%
Medical	3%	0%	14%	3%

4.3 Discussion

Referring to our findings illustrated in Figures 8 and 9, the distribution of mental models among experts and non-experts in the two experiments are significantly different.

Considering figures 6 and 7 weak-experts and non-experts have two different mental models for 13 different risks, whereas in the case of strong experts and non-experts they have different models for 18 different risks. Non-experts in both experiments reject the warfare mental model, whereas strong experts have 17% increase in choosing warfare mental model compare to weak-experts. These facts approve that the more stringent the definition of expertise resulted in a greater distance between expert and non-expert mental models. This arguable supports our assertion that the mental models embedded in risk communication be targeted for non-experts rather than based on the models of the communicating experts.

Both experiments show a significant difference between experts and non-experts in choosing physical mental model as their first mental model. However, in both experiments non-experts choose either the physical or criminal mental model. This strongly suggests the use of criminal and physical security metaphors in risk communication to lay users.

The core suggestion of this paper is to communicate security risks to each group of computer users according to their mental models of the risk. For example, strong-experts mark passwords as corresponding to a criminal model, while both weak and strong non-experts conceive of passwords as belonging to the physical realm. Therefore, non-experts perceive password risk as closer to the risk of a lost key; while experts perceive passwords as more closely corresponding to

subverted credit card numbers.

One of the labels given in card sorting experiment was "I can't decide". The participants choose this label for words they didn't know and words that fit no other category. Almost 50% of both weak and strong experts labeled "firewall", "userID" and "cookies" as "I can't decide". This percentage dropped to 40% in the case of weak and strong non-experts for "firewall" and "userID". The average of "I can't decide" for all the security risks, in the case of experts was 40% and in the case of non-experts was 30%. These facts suggest that the five mental models implicit in the security literature do not correlate with the mental models of experts and non-experts.

5. CONCLUSION

This paper reports our main contribution in exploring the mental models of security experts and non-experts with regard to security risks. Previously these models had been implicit in security risk communication. Our goal is to evaluate these implicit mental models, make them explicit and, use them in a systematic manner for risk communication. These experiments were a first step.

Our experiments suggest that for almost 45% of the risks in the case of weak-experts and 62% in case of strong-experts, experts and non-experts have two different mental models. The results from the two experiments suggest that people's mental models of security risks strongly correlates with their level of expertise in security. We propose that computer security risk communicators should match lay users's mental models.

As the first step, we used a quantitative approach to estimate the mental models of computer users with regards to some common security risks. Our current work continues with qualitative interviews with experts and non-experts. We have initial designs of risk communication that use these mental models in visual narrative mechanisms and have completed an initial test with 16 participants.

6. ACKNOWLEDGEMENTS

We would like to thank professor Youn-Kyung Lim (Indiana University-Bloomington) for her helpful comments on this paper and Christian Briggs (Ph.D. student at Indiana University-Bloomington) for his suggestions on our experiment's interface.

7. REFERENCES

[1] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *Privacy Enhancing Technologies*, pages 36–58, 2006.

[2] A. Arora, R. Telang, and H. Xu, editors. *Optimal Policy for Software Vulnerability Disclosure*, Minneapolis, MN, 2004. Third Workshop on the Economics of Information Security.

[3] A. Bostrom, B. Fischhoff, and M. G. Morgan. Characterizing mental models of hazardous processes: A methodology and an application to radon. *Journal of Social Issues*, 48(4):85, 1992.

[4] T. A. Byrd, K. L. Cossick, Cossick, and R. W. Zmud. A synthesis of research on requirements analysis and knowledge acquisition techniques. *MIS Quarterly*, 16(1):117–138, March 1992.

[5] L. J. Camp. Mental models of security. *IEEE Technology and Society*, 2006.

[6] L. J. Camp and S. Lewis. *The Economics of Information Security.* Kluwer Academic, Boston, MA, 2004.

[7] H. Cavusoglu, B. Mishra, and S. Raghunathan. A model for evaluating it securiy investments. *Communications of the ACM*, 47(7).

[8] J. P. Choi, C. Fershtman, and N. Gandal, editors. *Internet Security, Vulnerability Disclosure, and Software Provision*, Cambridge, MA, 2005. Fourth Workshop on the Economics of Information Security.

[9] L. L. Costantine and L. A. Lockwood. *Software For Use - A Practical Guide to the Models and Methods of Usage Centered Design.* Reading MA: Addison-Wesley.

[10] T. Cox and M. Cox. *Multidimentional Scaling.* Boca Raton, Florida: Chapman and Hall/CRC, 2001. 2nd edition.

[11] D. Denning. *Information Warfare and Security.* Addison-Wesley Publication, Boston, MA, 1998.

[12] J. Diesner, P. Kumaraguru, and K. M. Carley. Mental models of data privacy and security extracted from interviews with indians. *55th Annual Conference of the International Communication Association*, 2005. New York, NY.

[13] Fischhoff. Characterizing mental models of hazardous processes: A methodology and an application to radon. *Journal of Social Issues*, 15(2):37–45, 1995.

[14] D. E. Geer. Security of information when economics matters. *Verdasys, Inc.*, May 2004. available online, at http://www.verdasys.com/resources/resources.html.

[15] W. Hudson. Playing your cards right: Getting the most from card sorting for navigation design. *HCI & Higher Education Column: People: HCI & the web*, 12(5):56–58, Sep 2005.

[16] H. Jungermann, H. Schutz, and M. Thuring. Mental models in risk assessment: Informing people about drugs. *Risk Analysis*, 1981.

[17] C. Keller, M. Siegrist, and H. Gutscher. The role of the affect and availability heuristics in risk communication. *Risk Analysis*, 26(3):631639, 2006.

[18] J. Kephart, D. Chess, and S. White. Computers and epidemiology. *IEEE Spectrum*, 1993.

[19] J. Kruskal and M. Wish. *Multidimensional Scaling.* Sage Publication, 1978.

[20] B. Laurie and R. Clayton. Proof-of-work' proves not to work. *Third Workshop on the Economics of Information Security, Minneapolis, MN*, 2004. available online, at http://www.dtc.umn.edu/weis2004/clayton.pdf.

[21] M. G. Morgon, B. Fischhoff, A. Bostrom, and C. J. Atman. *Risk Communication: A Mental Models Approach.* Cambridge University Press, Cambridge, UK, 2001.

[22] J. Nielsen. *Usability Engineering.* Academic Press, San Diego, CA, 1993.

[23] D. Nizovtsev and M. Thursby, editors. *Economic Analysis of Incentives to Disclose Software Vulnerabilities*, Cambridge, MA, 2005. Fourth Workshop on the Economics of Information Security.

[24] D. Norman. *The Design of Everyday Things.* New

York: Doubleday/Currency, 1983.

[25] D. Norman. *Some Observations on Mental Models In Mental Models eds. D. Gentner and A. Stevens, LEA*. 1983.

[26] C. F. Ronnfeldt. Three generations of environment and security. *Journal of Peace Research*, 34(4):473–482, 1997.

[27] S. L. Schensul, J. J. Schensul, and M. D. Lecompte. *Essential Ethnographic Methods*. AltaMira Press, Lanham, MD, 1999. ch. 1.

[28] R. Telang and S. Wattal, editors. *Impact of Software Vulnerability Announcements on the Market Value of Software Vendors, an Empirical Investigation*, Cambridge, MA, 2005. Fourth Workshop on the Economics of Information Security.