2017

Mining the Mind – Applying Quantitative Techniques to Understand Mental Models of Security

Nik Thompson
Curtin University, nik.thompson@curtin.edu.au

Tanya Mcgill
Murdoch University, T.Mcgill@murdoch.edu.au

Mining the Mind – Applying Quantitative Techniques to Understand Mental Models of Security

Nik Thompson
School of Information Systems
Curtin University
Perth, Western Australia
Email: nik.thompson@curtin.edu.au

Tanya McGill
School of Engineering and Information Technology
Murdoch University
Perth, Western Australia
Email: t.mcgill@murdoch.edu.au

Abstract

Mental models, informal representations of reality, provide an appealing explanation for the apparently non-rational security decisions of information technology users. Although users may be attempting to make secure decisions, the use of incomplete or incorrect information security mental models as a shortcut to decision making may lead to undesirable results. We describe mental models about viruses and hackers drawing on data from a survey of 609 adult IT users and link these to security behaviours and perceptions. We find that there are potentially just a small number of common security beliefs and suggest that accommodating mental models during security design may be more beneficial to long-term security than expecting users to change to accommodate security requirements.

Keywords information security, mental models, human factors, home computer, mobile device

1 Introduction

Mental models are informal representations of reality that people use to understand their environment and interactions. Craik (1943) theorised that mental models are the way in which humans interact with the world and suggested that rather than relying on formal rules and logic, people often make decisions based on their general knowledge and understanding of the situation.

Because individuals have limited working memory, mentals models serve to minimise the load on memory with simplified and selective representations of reality encoded in the models (Johnson-Laird et al. 1998). Thus, these models are not intended to be complete – suggesting that simply arming people with more information may not directly translate to more refined solutions to problems where responses are driven by models. In a domain like information security, where information technology (IT) users may be overwhelmed by a large amount of technical information, it is reasonable for behaviours to be guided by readily accessible mental models of the situation. In fact, even for more knowledgeable users, more specific and detailed information may be less easily retrievable than a basic mental model.

The law of small numbers (Tversky and Kahneman 1971) also plays a role. Individuals may believe that their own limited experience of information security is fully representative of all the threats faced. Consequently, having "played the odds and won", that is, emerging unscathed in spite of poor security decisions (Camp 2009) will further reinforce their incomplete and perhaps unrepresentative mental models of the situation. This perspective provides an appealing explanation for the abundant situations in which individuals make security related decisions that may not be easily explained by logical reasoning or inference.

"Folk" models which form through personal experience or stories shared among people in a community (Keil 2010) may influence decisions so strongly that the mental model prevails even when faced with conflicting evidence. In August of 1994, the Moura Mine disaster resulted in the deaths of 11 miners in Queensland, Australia. A subsequent investigation revealed that a gas explosion had been caused by coal in an advanced stage of heating – evidence of which had been available for six weeks prior to the disaster yet was either minimised or overlooked (Windridge 1996). This has been attributed to a flawed folk model which held that coal takes six months to heat up to a dangerous level (Chapman and Ferfolja 2001). As the warnings of coal heating were inconsistent with the mental model, they were dismissed, leading expert individuals toward an incorrect course of action that was not guided by the evidence in front of them. In an information systems context, warning signs and evidence of security threats may be far less prominent. In fact, a great deal of research goes into trying to address the large scale findings that IT users often fail to attend to security warnings (Akhawe and Felt 2013). A further challenge is faced when users may take in security information, but fail to act on it if it is not aligned to their mental model of the situation (Egelman et al. 2008).

This study was designed to identify beliefs about viruses and hackers that contribute to mental models and estimate their prevalence in the IT end user population, giving insights into kinds of beliefs that users may call upon when making security decisions. We also attempt to describe a set of prototype models and sort users into these models to perform exploratory analysis linking mental models to security behaviour.

2 Related Work

Mental models have been successfully used for risk communication in other disciplines, such as drug risks (Jungermann et al. 1988), however they have failed to achieve widespread utilisation in the information systems domain. Human computer interaction (HCI) practitioners are perhaps the most familiar information systems professionals with the concept of mental models. Nielsen (1990) describes two important elements of mental models: firstly the mental model is based on beliefs rather than facts, and may therefore be imperfect or unclear. Secondly, individuals will each have their own mental model; different users might even create different models of the same situation as the model is based on their own understanding of reality. Usability issues arise when there is a mismatch between the mental model of the developer and that of the technology user.

Mental models have received some attention in behavioural security research. Camp (2009) identified five possible mental models that may be used to communicate information security risk. These include Physical Security (e.g. locking doors and guarding assets), Medical (e.g. security hygiene can prevent infection spread), Criminal (e.g. end users are targets of opportunity), Warfare (e.g. perimeter security and constant diligence) and Market (e.g. costs versus benefits of security behaviours).

Beliefs are the basic component of mental models and a particular mental model held may be viewed as a set of these beliefs. The early work in deriving mental models of security has been largely qualitative in nature (e.g. Bravo-Lillo et al. 2011; Wash 2010) as extensive interviews and discussions are the ideal environment to explore beliefs and perceptions, when little is known about them. However, to gain a broader, more generalisable understanding of mental models of security and the roles they play larger scale quantitative studies are needed.

Wash (2010) conducted a qualitative study into how home computer users perceive various security threats. An iterative methodology was followed in which semi-structured interviews were conducted through several rounds of refinement. Respondents were selected by the researcher to ensure a large variability and no prior training in computer security. Thus, the sample was not intended to be generalised to the entire population of home computer users, but rather selected to reveal a wide range of mental models and perceptions. Through this study he described folk models around computer viruses and hackers. Four models of viruses were described: that viruses are Bad, Buggy Software, Cause Mischief or Support Crime. Similarly, four models of computer hackers were described: that hackers are Graffiti Artists, Burglars, Criminals or Contractors (to organised crime).

Subsequent research attempted to implement these mental models into a simulation environment. Guided by the premise that behaviour is predicted by not only level of knowledge but also its structure, Blythe and Camp (2012) showed that a simulated agent programmed with a mental model can make similar decisions to a human. This supports the view that mental models may function like simulations in the mind, allowing an individual to step though a situation before acting. Estimation of how prevalent these models may be in the general population was described as an area for future work (Wash 2010), and it is this gap that we aim to address in the current paper.

As mental models form from information that an individual believes to be true (Johnson-Laird et al. 1998), an expert mental model may differ from a non-expert user's. Prior research confirms the difference in beliefs and security behaviours of expert and non-expert users and suggests that in order to deliver effective security advice, the users must first be understood (Ion et al. 2015). All users may have the motivation to protect themselves against threats, but only those which they believe are real and are part of their mental model (Wash and Rader 2011). It is possible that security advice (created by experts) may be incompatible with the mental models and belief structures of non-expert users, leading to some of the insecure behaviours observed. Wash and Rader (2011) suggested that there is a need to ultimately eliminate the need for users to become more like security experts. This could be a reality if we understand how prevalent different belief structures and models are, and tailor security solutions based on this understanding.

More recently, Wash and Rader (2015) made a step toward quantifying some of the beliefs that may be part of mental models. They created a survey instrument to measure beliefs about viruses and hackers, and administered this to a Qualtrics survey panel of 1,993 United States based IT users. They gathered data about three virus related beliefs ("Viruses create visible problems", "You can protect against viruses", "Viruses are caught on the Internet") and two hacker related beliefs ("Hackers target home computer users", "Hackers target others") that were not considered to be mutually exclusive. They were able to report on the prevalence of these beliefs in the wider IT user population. They also attempted to group respondents using clustering approaches. This suggested that certain patterns of beliefs (i.e. mental models) may be shared by a larger number of respondents. However, with their results yielding a large number of possible clusters and a small number of beliefs measured (e.g. four possible groups of users were used to describe the two hacker beliefs) further work is required to elaborate on these prototype models before findings may be translated or generalised to real world situations.

3 Research Method

This study was designed to extend prior work and attempt to estimate the prevalence of beliefs about hackers and viruses held by IT users. The target population for the study was people who use IT (such as computers, tablets and smartphones) for personal use. The unit of analysis was the individual user. Data was collected through an anonymous online questionnaire.

In order to obtain a large and diverse sample, a third party recruitment firm was contracted to identify potential participants in the United States. The recruitment firm contacted potential participants by email and invited them to participate by completing the web based questionnaire. All participants were 18 years or over and were advised that completion of the questionnaire was voluntary, and that responses were anonymous.

The questionnaire collected general background and demographic information about respondents followed by a set of questions based around virus and hacker beliefs derived from the work of Wash (2010) with the objective of quantifying the prevalence of his theorised folk models of security. Virus and hacker beliefs were separated into individual items. The types of beliefs measured about viruses were: Virus Creator, Virus Purpose, Virus Effect and Virus Transmission. The types of beliefs measured about hackers were: Hacker Identify, Hacker Purpose, Hacker Target, Hacker Effect and Hacker Work. For every type of belief an "Other" option was also created to accommodate the possibility that the mental model profiles were incomplete. For instance Wash (2010) described three possible beliefs of Virus Effects: General Bad things, Annoying Problems or Information Stolen. Virus Effect was represented in our questionnaire as four items, three representing the original beliefs and "Other". Respondents were asked to rank these in order of their perceived importance. The full list of these items is presented in Appendix 1.

For each user, the data collection yielded 19 data points about virus beliefs and 17 data points about hacker beliefs. The current exploratory analysis did not require such granular data and these data points were collapsed into categories. For virus beliefs, four categorical variables were created to encode the respondent's highest ranked choice for Virus Creator, Purpose, Effect and Transmission. Similarly for hacker beliefs, five categorical variables encoded the highest ranked choice for Hacker Identity, Purpose, Target, Effect and Work.

In order to facilitate exploration of relationships between mental models and security behaviour, items to measure security behaviour, perceived severity and perceived vulnerability when using mobile devices such as smartphones and tablets were included for approximately half of the participants[1]. Security behaviour was measured using five items which asked the participant to state whether or not they performed the behaviour. The items were chosen as representative of recommended personal computing security behaviours and were scored as 1 for "Yes" or 0 for "No" or "Unsure". A composite variable was calculated as the sum of the responses to the five items. Both perceived severity and perceived vulnerability are proposed as determinants of security behaviour in research based on Protection Motivation Theory (Rogers 1975; 1983). There is evidence to support their role (Crossler and Bélanger 2014; Liang and Xue 2010; Woon et al. 2005) and it may be that these perceptions are influenced by mental models of security. Items to measure them were therefore also included in the study. Six items were used to capture each construct, and they were each measured on a 7 point Likert scale from 1 "Strongly Disagree" to 7 "Strongly Agree". Details of the items are available from McGill and Thompson (2017). Composite measures of perceived severity and perceived vulnerability were calculated as the mean of the items.

4 Results

Data screening was undertaken to identify respondents who had not sufficiently engaged with the study; 629 responses remained after removing responses with zero variance or those where completion took either below half of the minimum estimated completion time or twice the maximum estimated completion time (Huang et al. 2012). Of these, 20 were found to have only partially answered the mental models questions, leaving a final usable sample size of 609. The gender distribution of the sample was 61.7% female and 37.6% male.

4.1 Prevalence of Virus and Hacker Beliefs

Initial data analysis of the 609 responses revealed that certain beliefs were strongly held by a large proportion of the users. For the virus data set, most users believed that the creators are either mischievous or criminal and that the purpose and effect of viruses are related to information theft. There was no strong preference for how viruses were transmitted with an almost even distribution across the three choices. Table 1 reports the beliefs that respondents ranked as most relevant in the virus data set. For space reasons only the two most popular beliefs are included, therefore the row totals do not account for 100% of the respondents.

[1] The remaining participants answered the same items, but about home computer and laptop use rather than mobile device use, so were not included in the analysis.

Category	Belief (Percent)	Belief (Percent)
Virus Creator	Mischievous (49%)	Criminal (34%)
Virus Purpose	Gather Info (67%)	Disruption (17%)
Virus Effect	Info Stolen (69%)	Annoying (15%)
Virus Transmission	Running File (39%)	Automatically (32%)

Table 1: Summary of virus beliefs

In the hacker data set there was more variance, but again certain beliefs appear to be more prominent in the population. Hacker Purpose mirrors the findings in the virus data set with strong support for finding information as the purpose of hacking. More than half of the respondents believed that anyone can be a target of hackers, and that the effect is severe, causing lots of problems. These findings suggest that users are indeed concerned about their personal information, and aware that it may be a target. Respondents generally believed that hackers work either as part of an organised crime group or independently. Finally, the most common belief of hacker identity is also that they are part of an organised crime group, although results in this area are more evenly split across the three beliefs. As with the previous example, we summarise hacker beliefs in a table form below, including the two most common beliefs for each category.

Category	Belief (Percent)	Belief (Percent)
Hacker Purpose	Find Info (82%)	Mischief (14%)
Hacker Target	Anyone (54%)	Based on opportunity (35%)
Hacker Effect	Lots of problems (76%)	Possible computer problems (22%)
Hacker Work	Organised Crime (48%)	Independent (37%)
Hacker Identity	Organised Crime (39%)	Criminals (31%)

Table 2: Summary of hacker beliefs

4.2 Association Rule Mining

Association rule mining was the first technique employed to identify mental models. Association rule mining may be understood from the perspective of shopping basket analysis. Retailers mine transaction records, to learn which sets of items are commonly purchased together by their customers. For instance, the recommended items presented to shoppers at an e-commerce site are based on evidence that other shoppers have previously bought the items together; that is, they are somehow associated. To evaluate the usefulness of these "item sets" that are revealed, a number of metrics are employed, including confidence. Confidence percent is an indicator of how certain we are that when one item is present the associated item will also be present. If, out of ten shopping baskets that contain bread, four also contain milk, then there is a four out of ten or 40% confidence in this rule.

Emergence of a set of frequently held beliefs may indicate that a particular mental model is more prevalent. Though individuals may hold multiple mental models, evidence of associations would highlight which beliefs tend to be linked, and are stronger in the population. For instance, Wash (2010) discussed folk models of viruses and hackers in terms of sets of beliefs although he did not report how many users possessed each model. Thus, association rule mining was employed to explore any potential associations between beliefs held.

For this analysis, RapidMiner Studio v7.5 (RapidMiner Inc. 2017) was utilised. To perform association rule mining, the data must be presented as a series of true/false items. This is akin to searching the shopping basket looking for items that tend to occur together. Data were pre-processed to convert the categorical variables into binominal data and to map these values to true/false type statements. For example "Virus Creator = Organised Crime" or "Virus Creator ≠ Young Technical Geeks".

Next, the FP-Growth algorithm was applied to this data to look for frequent item sets. This process applies the FP-tree data structure to identify frequent item sets (Han et al. 2000). This was executed with a confidence parameter of 85% set as the threshold.

Mining of the virus beliefs data yielded a handful of potential rules, all of which led to only two (similar) outcomes: "Virus Effect = Information gets stolen", and "Virus Purpose = Gather Information". These do not appear to reveal any further insights into the patterns of user beliefs, beyond what is already apparent from the prevalence data described in Section 4.1. As high confidence rules may occur by chance, further analysis is needed to determine whether there is statistical independence of the antecedent and the outcome of the rule (McNicholas et al. 2008). Based on this analysis, we concluded that the potential rules were not of interest.

Data from the hacker beliefs were subjected to the same treatment and rule mining. Again, the small number of potential rules converged on only two beliefs: "Hacker Purpose = To look for Information" and "Hacker Effect = Lots of Computer Problems". It is apparent that beliefs about information theft and data security are commonly held, however similar to the virus data, further investigation revealed that the potential rules were not of interest. It was concluded that association rule mining was not successful with this data set and that the relations between virus or hacker beliefs may be more complex than a direct correlation between certain beliefs held. The next stage of exploratory analysis was to discern if an unsupervised (i.e. machine led) data mining approach might reveal some groupings of response data that would suggest patterns of mental models.

4.3 Clustering

Clustering is an unsupervised data mining approach in which items are grouped together such that members of a cluster are more similar to each other than they are to items outside their cluster. This may be performed with no a priori knowledge of the cluster characteristics, and subsequent analysis is required to determine if the proposed clusters are actually meaningful. Thus, out of the myriad cluster models and possible solutions, the "correct" one, if any, must often be determined by experimentation. This clustering was also performed in RapidMiner Studio v7.5.

The mental model data being analysed was represented with a single variable for each belief to encode the view held by the respondent. As this data is categorical in nature, k-medoids clustering was applied (Kaufman and Rousseeuw 1987). The k-medoids algorithm nominates the "most centred" data point in each cluster and iteratively scans through all other data points, deciding which cluster to assign them based on their similarity to the centre. As a rule of thumb, an attempt was made to find a value for k (number of clusters) such that there would be no needlessly small clusters, and that the number of clusters was low. This is in order to attain the most generalisable and simple solution and to reduce the risk of over-fitting (i.e. modelling random error or noise instead of the underlying relationship).

For the virus data set, possible solutions were found with either two or three clusters. The three cluster model consisted of one large and two smaller clusters. These superficially appeared to represent three sets of beliefs, although more detailed analysis revealed that there were minimal differences between the smaller clusters and a two cluster model was considered more appropriate. A two cluster model was accepted which yielded n=466 and n=143.

With beliefs about hackers, the results were less clear-cut. The clustering models that were explored often did not converge on a solution that had much real-world explanatory power. After removing the two factors that had the least predictive relevance, Hacker Target and Hacker Effect, the k-medoids algorithm was once again applied to the remaining data set. Two clusters were found with a reasonably even split of n=319 and n=290.

Evaluation of the "quality" of a cluster model is subjective. Numerical measures such as Davies-Bouldin index (Davies and Bouldin 1979), typically built into data mining tools, evaluate intra-cluster similarity and inter-cluster differences. These values describe how close together data points are grouped into clusters, however shed little light onto whether there is any inherent meaning in the groupings. As there was no ground truth against which to compare our models, descriptive measures discussing the observable patterns within the clusters were employed to understand the exploratory work. In the next section we describe the clusters in terms of the beliefs that are commonly held by members of each cluster and suggest prototype models to explain the perspective of each set of users.

4.4 Mental Models about Viruses

Virus mental model cluster 1 hold the *Criminal Enterprise* mental model of viruses and 76% of the sample belong to this cluster. Members consider virus creators to be either mischievous (50%) or criminal (35%) in nature. Consistent with criminal activity being traditionally associated with activities such as theft or fraud, those with this mental model strongly believe that the purpose of a computer virus is to gather information (82%). Unsurprisingly, they also overwhelmingly associate

the effect of a virus infection to be that information is stolen (84%). The mode of transmission of the virus is seen as being automatic in nature or installed by a hacker (41%) and to a lesser extent by running a file (30%).

Cluster 2 hold the *Mischief* mental model of viruses, and the remaining 24% of the sample belong to this cluster. Although holding similar views of virus creators to those in Cluster 1, that is, that they are mischievous (45%) or criminals (31%), beliefs around virus purpose diverge more clearly. Those holding the *Mischief* mental model do not consider information theft as a primary purpose of viruses. Rather they rank disruption (54%) and mischief (22%) as the main purposes. In keeping with a perception of *Mischief*, the perceived effect of a virus is that the "Computer runs badly" (48%) or there are "Annoying problems" (27%). Although respondents describe potentially frustrating situations, these views suggest that those in this cluster may perceive a lower severity of virus infection. Finally, the mode of transmission of viruses is seen to be largely from "Running infected files" (71%). Rather than seeing themselves as potential victims of a criminal enterprise, those holding this mental model may simply consider malware and viruses as annoyances – perhaps even a hazard of regular internet use.

4.5 Mental Models about Hackers

Hacker mental model cluster 1 hold the *Independent* model of hackers and 52% of the sample belong to this cluster. They believe that the hacker identity is primarily young techies (40%) or criminals in general (33%). Those with the *Independent* mental model believe that the purpose of hacking is most commonly to find information (72%), but also to a lesser extent for general mischief (21%). They believe that hackers generally work independently (70%) and this appears to be the defining characteristic of this mental model.

Cluster 2 hold the *Organised Crime* model of hackers and the remaining 48% of the sample belong to this cluster. Members consider the identity of hackers to mostly be organised crime (58%), followed by criminals in general (29%). The perceived purpose of hacking for this cluster is almost universally to find information (93%). They also universally (100%) believe that hackers work as part of organised crime units. It is likely that the identity of a hacker and their work unit are prominent characteristics of a user's mental model about hackers.

Beliefs about the targets and effect of hacking were not used as variables for clustering, as these had little predictive power and their inclusion made little difference to the outcome of the clustering model. Cluster 1 and Cluster 2 both consider that hackers target anyone (57% and 52%) and are opportunistic (34% and 36%). Similarly, both clusters also consider that the effect of a hack is to cause a large number of computer problems (73% and 78% respectively).

4.6 Influence on Behaviour

As discussed in Section 2 above, mental models are believed to play a role in security behaviour (e.g. Camp 2009; Wash and Rader 2011). There has, however, been little research directly measuring whether this is the case. In order to explore whether the mental models identified in this study were associated with users' security behaviour, and how any associations might relate to perceptions of severity or vulnerability, exploratory analyses were undertaken to evaluate our mental model data alongside more traditional user security behaviour data. Table 3 shows the mean levels of security behaviour and security perceptions for the two virus belief clusters. As can be seen, the *Criminal Enterprise* cluster had higher average levels of security behaviour, perceived severity and perceived vulnerability. To further explore these potential differences, non-parametric Mann-Whitney U tests were used to determine if there were significant differences in security behaviour or perceptions between people holding different mental models of viruses. Mann-Whitney U tests were used rather than t-tests as the data did not meet the assumption of normality. The Mann-Whitney U test tests the hypothesis that two independent samples are likely to derive from the same population, and does not require the assumption of normal distributions. No significant differences in levels of security behaviour were found between those in the *Criminal Enterprise* cluster and those in the *Mischief* cluster ($U=6{,}714.0$, $Z=-1.200$, $p=0.230$). Levels of perceived severity were, however, significantly higher for those in the *Criminal Enterprise* cluster ($U=5{,}964.5$, $Z=-2.441$, $p=0.015$), but levels of perceived vulnerability were not significantly different ($U=6{,}989.5$, $Z=-0.730$, $p=0.465$). Users in both clusters believe that they can be a target and their levels of perceived vulnerability are not significantly different. Similarly, there is no significant difference between the levels of security behaviours undertaken. However, users in the *Criminal Enterprise* cluster had significantly higher levels of perceived severity, indicating that if users believe that criminal enterprises are responsible for security issues the threats may be perceived as more severe than if they are believed to be a result of mischief.

	Criminal Enterprise (N=236)		Mischief (N=63)		Significant Difference?
	Mean	SD	Mean	SD	
Security behaviour	2.26	1.65	1.97	1.36	No
Perceived severity	5.85	1.30	5.54	1.27	Yes
Perceived vulnerability	4.71	1.42	4.53	1.24	No

Table 3. Virus belief cluster comparison

Table 4 provides a similar comparison for the two hacker belief clusters. As can be seen, the *Organised Crime* cluster had higher levels of security behaviour, perceived severity and perceived vulnerability. The differences between clusters were significant for security behaviour (U=9,587.5, Z=-2.123, p=0.034) and perceived severity (U=9,564.5, Z=-2.147, p=0.032). The difference in the levels of perceived vulnerability were not, however, significant (U=9,833.5, Z=--1.761, p=0.078). Again, users in both clusters believe they are relatively vulnerable, with no significant differences observed in levels of perceived vulnerability between the clusters. This finding is consistent with the results reported in Section 4.1 where 54% of respondents reported that the target of a hack could be anyone and 35% reported that targets were determined based on opportunity. Users in the *Organised Crime* cluster, however, have significantly higher levels of perceived severity than those who believe that hackers are *Independent*. Mirroring this trend, the levels of security behaviour are higher for those in the *Organised Crime* cluster.

	Independent (N=157)		Organised Crime (N=142)		Significant Difference?
	Mean	SD	Mean	SD	
Security behaviour	2.01	1.56	2.41	1.61	Yes
Perceived severity	5.64	1.35	5.95	1.21	Yes
Perceived vulnerability	4.55	1.37	4.82	1.39	No

Table 4. Hacker belief cluster comparison

5 Discussion and Conclusion

We have presented a set of prototype mental models that can be used to describe users in terms of commonly held beliefs. For viruses these are the *Criminal Enterprise and Mischief* models, with the *Criminal Enterprise model more prevalent*. For hackers these are the *Independent* and *Organised Crime* models, which are were of almost equal prevalence. Prior work has shown that the mental model held by an individual influences their reasoning and decision making. For instance, people who hold a simplistic view of electricity as something that flows like water may employ a mental model of a garden hose. These individuals then go on to connect a battery to a bulb with a single wire, so that electricity from the storage tank (battery) may trickle through the wire to the bulb (Tarciso Borges and Gilbert 1999). Holding an incomplete or flawed mental model may lead a user to make decisions that they believe are rational and sensible, but may be flawed (Keil 2010). This provides a new perspective to explain the apparently non-rational choices that users make.

Our exploratory analysis of differences in security behaviour between those holding different mental model of security threats addresses Wash and Rader's (2011) call for more research on how mental models influence security behaviour. The results not only show that mental models can be associated with different levels of security behaviour, but provide a starting point as to how this may occur. For example, users who believe virus creators to have criminal intent, rather than being merely mischievous, have higher levels of perceived severity of threat and this has been shown in many studies to influence security behaviour (e.g., Posey et al. 2015; Siponen et al. 2014; Vance et al. 2012). Similarly, users who hold the *Organised Crime* model of hackers have higher levels of perceived severity of threat. Linking mental models of security to the body of quantitative research using models such as Protection Motivation Theory (Rogers 1975; 1983) provides a promising way forward.

A limitation of our work is that the data gathered about security beliefs is constrained to a set of beliefs described in previous research. Expanding this to a larger set of data points may improve the outcomes of the data mining and provide deeper insights into IT users' mental models. Another interesting area for future work may be to examine the kinds of situations in which mental models or heuristics are employed during security decision making and contrast this with the use of more methodical approaches. It is possible that the environment and context influence the decision making strategies employed and thus have an impact on IT users' behaviour.

Prior work has shown that incorrect mental models can lead to insecure behaviours (Egelman et al. 2008) and suggests that some of the widespread security issues faced by the public may be heightened by mismatches between developers' perspectives and those of end users. For example, it is possible that some of the rising issues concerning the insecurity of Internet of Things devices may be in part due to users not viewing such devices with the same mental model as applied to a regular computer, even though there are many commonalities.

Research suggests that security experts (e.g. developers) hold different mental models to non-experts (e.g. users) (Ion et al. 2015; Wash and Rader 2011). HCI designers have recognised the issues that arise when developers and users possess different models and attempt to mitigate this risk during design. However, this does not appear to be done in information security. Instead of attempting to simply lay the blame on the end user, or expecting them to change, developers can do their part. Wash and Rader (2011) suggest that the need for users to become more like security experts in order to be more secure may be alleviated by changing mental models. Mental models however, resist change, and this can be a significant roadblock for any intervention that requires the users to adjust their beliefs (Duffy 2003). Therefore, we not only support the suggestions of Wash and Rader but also propose that developers should learn about the mental models held by users. By understanding the beliefs that users already hold, developers may tailor an experience and environment that is consistent with users' expectations and may enable them to make security decisions that are as effective as the users believe they are.

6 References

Akhawe, D., and Felt, A.P. 2013. "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness," in: *Proceedings of the 22nd Usenix Security Symposium*. USENIX, pp. 257-272.

Blythe, J., and Camp, L.J. 2012. "Implementing Mental Models," in: *Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops*. IEEE, pp. 86-90.

Bravo-Lillo, C.C., Downs, L., and J Komanduri, S. 2011. "Bridging the Gap in Computer Security Warnings: A Mental Model Approach," *IEEE Security & Privacy* (9:2), 03, pp 18-26.

Camp, L.J. 2009. "Mental Models of Privacy and Security," *IEEE Technology and Society Magazine* (28:3), pp 37-46.

Chapman, J.A., and Ferfolja, T. 2001. "Fatal Flaws: The Acquisition of Imperfect Mental Models and Their Use in Hazardous Situations," *Journal of Intellectual Capital* (2:4), pp 398-409.

Craik, K. 1943. "The Nature of Explanation." Cambridge, Cambridge University Press.

Crossler, R.E., and Bélanger, F. 2014. "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument," *Data Base for Advances in Information Systems* (45:4), pp 51-71.

Davies, D.L., and Bouldin, D.W. 1979. "A Cluster Separation Measure," *IEEE Transactions on Pattern Analysis and Machine Intelligence* (PAM-1:2), pp 224-227.

Duffy, F.M. 2003. "I Think, Therefore I Am Resistant to Change," *Journal of Staff Development* (24:1), p 30.

Egelman, S., Cranor, L.F., and Hong, J. 2008. "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*: ACM, pp. 1065-1074.

Han, J., Pei, J., and Yin, Y. 2000. "Mining Frequent Patterns without Candidate Generation," *ACM SIGMOD Record* (29:2), pp 1-12.

Huang, J.L., Curran, P.G., Keeney, J., Poposki, E.M., and DeShon, R.P. 2012. "Detecting and Deterring Insufficient Effort Responding to Surveys," *Journal of Business and Psychology* (27:1), pp 99-114.

Ion, I., Reeder, R., and Consolvo, S. 2015. " "... No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices," in: *Symposium on Usable Privacy and Security (SOUPS)*. pp. 327-346.

Johnson-Laird, P.N., Girotto, V., and Legrenzi, P. 1998. "Mental Models: A Gentle Guide for Outsiders," *Sistemi Intelligenti* (9:68).

Jungermann, H., Schütz, H., and Thüring, M. 1988. "Mental Models in Risk Assessment: Informing People About Drugs," *Risk Analysis* (8:1), pp 147-155.

Kaufman, L., and Rousseeuw, P. 1987. *Clustering by Means of Medoids*. North-Holland.

Keil, F.C. 2010. "The Feasibility of Folk Science," *Cognitive Science* (34:5), pp 826-862.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp 394-413.

McGill, T., and Thompson, N. 2017. "Old Risks, New Challenges: Exploring Differences in Security between Home Computer and Mobile Device Use," *Behaviour & Information Technology*, DOI: 10.1080/0144929X.2017.1352028.

McNicholas, P.D., Murphy, T.B., and O'Regan, M. 2008. "Standardising the Lift of an Association Rule," *Computational Statistics & Data Analysis* (52:10), pp 4712-4721.

Nielsen, J. 1990. "A Meta-Model for Interacting with Computers," *Interacting with Computers* (2:2), pp 147-160.

Posey, C., Roberts, T., and Lowry, P.B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp 179-214.

RapidMiner Inc. 2017. "Rapid Miner 7.5." Retrieved 1 June 2017, from https://rapidminer.com/

Rogers, R.W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), pp 93-114.

Rogers, R.W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in: *Social Psychophysiology,* J.T. Cacioppo and R.E. Petty (eds.). New York: Guilford Press, pp. 153-176.

Siponen, M., Mahmood, A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp 217-224.

Tarciso Borges, A., and Gilbert, J.K. 1999. "Mental Models of Electricity," *International Journal of Science Education* (21:1), pp 95-117.

Tversky, A., and Kahneman, D. 1971. "Belief in the Law of Small Numbers," *Psychological Bulletin* (76:2), p 105.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3), pp 190-198.

Wash, R. 2010. "Folk Models of Home Computer Security," *Proceedings of the Sixth Symposium on Usable Privacy and Security*: ACM.

Wash, R., and Rader, E. 2011. "Influencing Mental Models of Security: A Research Agenda," *Proceedings of the 2011 Workshop on New Security Paradigms*: ACM, pp. 57-66.

Wash, R., and Rader, E. 2015. "Too Much Knowledge? Security Beliefs and Protective Behaviors among United States Internet Users," in: *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* Ottawa, Canada.

Windridge, F. 1996. "Warden's Inquiry: Report of an Accident at Moura No 2 Underground Mine on Sunday, 7 August 1994." Brisbane, Department of Mines and Energy.

Woon, I., Tan, G., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in: *Proceedings of the Twenty-Sixth International Conference on Information Systems*. Las Vegas: pp. 367-380.

Appendix 1 – Questionnaire Items

Virus belief items

The following questions were used to capture participants' understanding and experience of computer viruses.

Viruses are created by :					
Criminals	Mischievous hackers	Bad people	They are not created on purpose	Corporations	Other
Purpose of viruses is to :					
Gather information for identity theft or fraud	Cause mischief and annoy people	No real purpose	Disrupt/corrupt government or business systems	Other, not mentioned above	
The effect of virus infection is that :					
Information gets stolen for criminal purposes	Annoying problems are caused for users	The computer runs badly	Other, not mentioned above		
Viruses are transmitted by :					
Automatically spread or installed by hackers	Passively caught by viewing shady websites or emails	By inadvertently downloading and running an infected file	Other, not mentioned above		

Hacker belief items

The following questions were used to capture participants' understanding and experience of computer hackers.

Hackers are usually :					
Young technical geeks	Criminals	Professional organized criminals	Other, not mentioned above		
The way hackers work is :					
Independently	To impress friends	No real pattern	As part of a criminal organization	Other, not mentioned above	
Hackers break in to :					
Cause mischief	Look for financial and personal information	Other, not mentioned above			
The effect of a break in is :					
Lots of computer problems, software might have to be reinstalled	Possible computer problems	No harm to computer, it will run fine			
Hackers usually target					
Anyone, it doesn't matter	Opportunity, it could be me	Not me, they only look for rich important people	Not me, they only look for large databases of information		

Copyright