International Journal of Information Security and Privacy

January-March 2009, Vol. 3, No. 1

Table of Contents

Research Articles

Understanding User Behavior towards Passwords through Acceptance and Use Modelling

Lee Novakovic, Murdoch University, Australia

Tanya McGill, Murdoch University, Australia

Michael Dixon, Murdoch University, Australia

ABSTRACT

The security of computer systems that store our data is a major issue facing the world. This research project investigated the roles of ease of use, facilitating conditions, intention to use passwords securely, experience and age on usage of passwords, using a model based on the Unified Theory of Acceptance and Use of Technology. Data was collected via an online survey of computer users, and analyzed using PLS. The results show there is a significant relationship between ease of use of passwords, intention to use them securely and the secure usage of passwords. Despite expectations, facilitating conditions only had a weak impact on intention to use passwords securely and did not influence actual secure usage. Computing experience was found to have an effect on intention to use passwords securely, but age did not. The results of this research lend themselves to assisting in policy design and better understanding user behavior. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: Ease of Use; Facilitating Conditions; Passwords; Unified Theory of Acceptance and Use of Technology

INTRODUCTION

Computer security is a major issue facing the world we inhabit. Computer systems in a multitude of institutions and organizations hold our personal information. Furthermore, we rely on the safe working of computer systems to not only protect that data, but allow us to take advantage of the benefits technology has to offer. Various kinds of security technology protect these systems. However, the development of security technology has not kept pace with suggested usability guidelines (Nielson, 1990). It has been shown that despite all of the advances in computer security technology, lack of suitable user compliance has led to a marked decrease in the overall levels of security (Adams & Sasse, 1999). Users find security measures difficult to use properly (Adams & Sasse, 1999). It is therefore in the interests of all levels involved with operating and using computer systems that the security measures in place have the appropriate factors affecting acceptance and use studied. The broad aim of the research described in this article was to investigate the effect of the ease of use of passwords on users' intentions to behave securely, and on their actual secure usage of passwords. The help and assistance available to users and its effect on secure usage was also of interest. To address these aims, a model derived from the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis, & Davis, 2003) was developed and tested.

BACKGROUND

Computer security has traditionally focused on securing technology. This encompasses securing it from physical theft, from intrusion (both internal and external threats), compromised integrity and the system's level of availability. This is covered by the basic "Confidentiality, Integrity and Availability" (CIA) security model (Stanton, Stam, Mastrangelo, & Jolton, 2005). This model works well when the sole focus is on securing technology with minimal consideration for the users.

The users of a system are often neglected from consideration when planning the security schema of a network of systems (Adams & Sasse, 1999; Braz & Robert, 2006; Singh, Cabraal, & Hermansson, 2006; Zurko & Simon, 1996). In many instances, the failings of the security plan are seen as a failing of the users (Adams & Sasse, 1999; Zurko & Simon, 1996), rather than the failing of the technology. Since systems are provided for users to use, this shift of responsibility is crucial and the reason for many computer security failings.

A commonly held belief is that there is an inherent trade off between the usability and the security of any given system. However, "if people are unable to use secure computers, they will use computers that are not secure. At the end of the day, computers that are theoretically secure but not usable do little to improve the security of their users…the converse is also true: systems that are usable but not secure are, in the end, not very usable either" (Cranor & Garfinkel, 2005, p. x) .

A commonly used security model is the AAA model. This refers to three parts of computer security: Authentication, Authorization and Accounting (Langsford, Naemura, & Speth, 1983). Authentication can be summarized with the phrase "who you are". Authentication aims to validate who a user claims to be. Once authenticated, a user's credentials may allow them to perform certain actions in certain areas of the system. An example of authorization is the difference between the level of access a regular user has on a system and the level of access an administrator has. Accounting can be summarized with "what you did". Once a user has been authenticated and authorized to do certain tasks, the accounting part records what that person did. Commonly, this is in the form of log files. Whilst all three components (among others) are important to effective computer and network security, authorization and accounting are beyond the scope of this research project. Most problems relating to the usability of security devices and techniques from the user perspective are concerned with the authentication phase (Adams & Sasse, 1999; Braz & Robert, 2006; Patrick, Long, & Flinn, 2003).

There are a number of authentication methods available to users. There are three ways for users to prove their identity to a computer system. These consist of "knowing" something, "having" something or "being" something. Respectively these can be broken down to passwords, security tokens and biometric details.

Despite the fact that they are invariably less secure than ideal, the most prevalent and widespread forms of authentication are the password (or passphrase) and personal identification number (PIN). A password can contain the alphanumeric values and special characters available on a computer system. A PIN is however limited to the ten available digits (0 – 9) (Braz & Robert, 2006). Both schemes offer easy deployment, but are easily forgotten. There are a number of commonly used rules relating to proper password creation and management. These rules are defined as part of the service. Some of these rules include using a minimum of eight characters comprised of alphanumeric characters and special symbols. A password should be easy to remember and able to be typed quickly (Garfinkel, Spafford, & Schwartz, 2003). Further to this, there are a number of rules relating to what should not be in a password. This list includes names (such as spouses and children), favorite sporting teams, favorite fictional character names and unique information about the user (Garfinkel et al., 2003). These are but a few of the recommended constraints on password design.

It is obvious that these requirements are numerous and can demand serious mental effort to create a password that fits all the criteria. For this and other related reasons users find security measures difficult to use properly (Adams & Sasse, 1999) and this can make compliance an issue. Security policies commonly have clauses which demand users change their passwords after a set period of time (Garfinkel et al., 2003; Mainwald, 2003). It has been found that there is a counterproductive effect to these security policies. Demanding passwords be changed frequently and be of strong composition can place too much cognitive load on users. As a result, users choose easy-to-remember passwords, and the system suffers a lower level of security (Adams & Sasse, 1999; Besnard & Arief, 2004; Braz & Robert, 2006). There is also a correlation between the complexity of the password regime and the insecure actions undertaken by users, with 50% of users writing down their passwords (Adams & Sasse, 1999; Besnard & Arief, 2004; Halderman, Waters, & Felten, 2005).

The survey carried out by Adams and Sasse (1999) found that the stricter the restrictions and guidelines on password content, the less memorable the resultant password. It is estimated that a large percentage of helpdesk and support requests are related to password difficulties, often a forgotten password (Brostoff & Sasse, 2000). This inability of the user to effectively deal with the password requirements laid down for them has also been used as a measure of a system's level of usability in relation to security (Brostoff & Sasse, 2000).

Adams and Sasse (1999) also found that users lack security knowledge, and that their lack of knowledge and understanding contributes to their "insecure" behavior. In part this can be traced back to an assumption that the more that is known about a security mechanism, the easier it is to attack. However, their results suggest that lack of knowledge creates more problems than it solves.

As previously mentioned, there are a number of areas in which users fail to act in the most secure way possible. It is important to make the distinction between deliberately malicious users, who may aim to misuse systems or intentionally destroy data and information and users who cause detrimental outcomes to computer security through naïve mistakes, such as poor password hygiene. The latter group of users are the focus of this research. In the survey carried out by Stanton et al. (2005), it was found that 62.5% of participants did not use any punctuation marks in their password, 48.5% of participants had not changed their password in the previous month and that 27.9% wrote down their passwords. This demonstrates the widespread occurrence of naïve mistakes made by users.

The overall security of a system which relies on passwords is not solely dependent on the complexity of user passwords. There exists a multitude of threats to a network's security once a password has been set, regardless of the user's behavior towards it. A "man-in-the-middle" attack could be used to intercept transmitted passwords in network traffic. Password based network security can also be threatened by an exposed password store, such as the "shadow file" on UNIX systems. Data loss of this sort could be through the introduction of malicious code, such as viruses or Trojan horses or theft of hardware and software (Mainwald, 2003).

There are other significant user factors that influence the overall level of security on a computer network and associated systems. These issues are out of the scope, yet complementary to the area of research involving ease of use of passwords. The first such issue is the matter of user error. As information security and the mechanisms which serve this function become increasingly more common, the possibility for user error having an impact becomes more apparent (Zurko, 2005). This could be viewed as a matter of awareness of current security concerns and the effects mitigated through education and training (Mainwald, 2003).

One must not disregard the other "class" of user which can have a great impact on computer security: the system administrator. As this class of user is responsible for the setup and maintenance of a computer network, data backup, maintaining a patching regimen, proper configuration and enforcement of computing policy through technical methods, their action or inaction can have fantastic ramifications on a network's security (Mainwald, 2003).

A system's security is also at risk through users whose confidence and trust is exploited by attackers. This is a process known as "social engineering". Social engineering is a psychological attack on the user, undertaken by tricking them to divulge some information (Orgill, Romney, Bailey, & Orgill, 2004). The effectiveness of social engineering is not due to users being overburdened by the security technologies they are forced to use, it is through a lack of compliance to the security policy. This threat is so serious that some organizations hire individuals to audit their policy by infiltrating their organization (Ceraolo, 1996; Orgill, Romney, Bailey, & Orgill, 2004). Orgill et al.'s (2004) study consisted of a one week experiment, which consisted of infiltrating an organization and convincing employees to participate in a "survey". Of those interviewed, 81.3% willingly gave their username and 59.4% gave their passwords. The study also discovered that of the surveyed employees many were not skeptical or suspicious of the researcher's (posing as an insider of the organization) claims of authority and requests for information.

There also exists a significant social trust component in the area of password sharing and social engineering. The study performed by Weirich and Sasse (2001) showed that divulging one's password to colleagues is a sign of trust between the individuals. Not divulging a password has the unexpected outcome of appearing suspicious of fellow workmates. Similarly, the study performed by Singh, Cabraal and Hermansson. (2006) found that the sharing of bank access codes in married and de facto couples was seen as an expression of trust.

MODELING SECURITY BEHAVIOR

There are a number of models designed for computer security. However, these focus primarily on the technical aspects of computer security, such as access control within a system. Two such models are the Bell and LaPadula Model (1973) and the High-Water Mark model by Weissmann (1969).

As previously stated, the user is the key component to any system. There have been numerous models proposed, such as the Technology Acceptance Model (TAM) (Davis, 1989), to model the acceptance and use of a new technology. However, there has been little emphasis on user behavior studies in the security arena (Adams & Sasse, 1999; Braz & Robert, 2006; Singh et al., 2006; Zurko & Simon, 1996). This however is an important area and more needs to be known about the acceptance and usability of security measures, and models such as TAM can provide a valuable framework for such research.

Technology acceptance relies upon a degree of volition and freedom. However, often in the field of technology, the ability for an individual's free will to play a significant part is limited. Often, system use is mandated, and the user complies, purely due to a requirement for them to do so (Brown, Massey, Montoya-Weiss, & Burkman, 2002). Security is similar in its modus operandi as policies dictate what a user is allowed to do, and how they are required to do it. However, a differentiation needs to be made in relation to security. As stated, security is often a mandatory requirement, but its effective operation relies upon user action. The problem arises that secure user behavior is often hampered by the very system that requires secure behavior. The following section describes the major research that has attempted to model aspects of security behavior.

A study carried out by Aytes and Connolly (2004) proposed a rational choice model to study unsafe computing practices of undergraduate students. They found that users provided with information regarding their insecure actions did little to change their behavior. Cazier, Wilson and Medlin (2007) also investigated the security behaviors of students. They extended TAM (Davis, 1989) to include measures of privacy risk harm and privacy risk likelihood and found that privacy risk factors negatively influenced students' intentions to use technology. TAM was also used by Lu, Hsu and Hsu (2005) to examine the perceived risk of online applications. They surveyed 1,259 users who had used a free trial version of an online antivirus application and found that perceived risk indirectly influenced intentions to use online antivirus tools under security threats.

Lee and Lee (2002) proposed the Theory of Planned Behavior (TPB) (Ajzen, 1991) as a framework to investigate computer abuse. Ng and Rahim (2005) subsequently used a model derived from the TPB to investigate home users' intentions to practice security. The areas of security focused on were users' habits for keeping anti-virus software up-to-date, backing up their critical data and the use of a personal firewall. They found that perceived usefulness of security actions and peer influence were important factors in attitudes to security and decision to practice security.

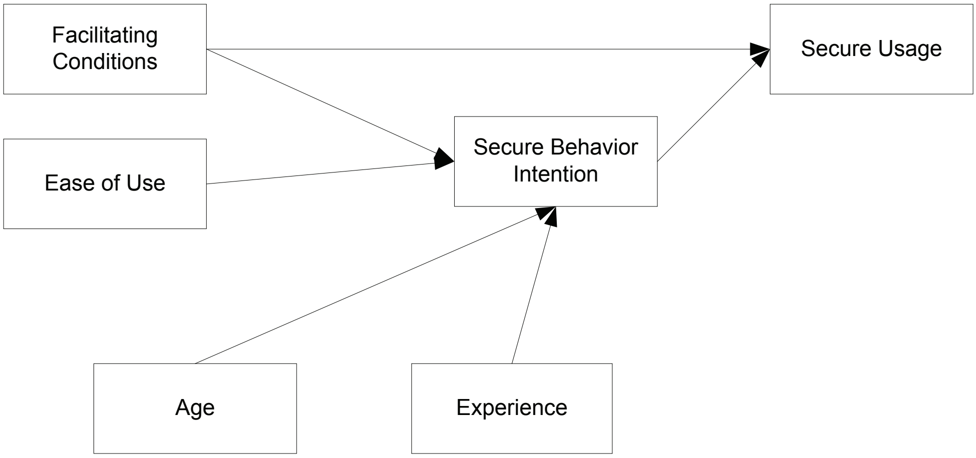
Going beyond user behavior to the behavior of other stakeholders, several studies have proposed and tested behavioral models of security. Woon and Kankanhalli (2007) investigated the intention of programmers to develop applications that are written with security in mind. This study compared models based on the TPB and the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975). They found that a developer's attitude was the biggest factor in their decision to develop applications in a secure manner. Interestingly, given the heavy importance of security, organizations did little to assist their developers, beyond allowing them to go to seminars. Woon and Kananhalli (2007) also found that the help and assistance available to developers had no significant impact on intention to practice secure development of applications.

Knapp, Marshall, Rainer and Ford have undertaken several studies that model the role of top management in security effectiveness (Knapp, Marshall, Rainer, & Ford, 2006; Knapp, Marshall, Rainer, & Ford, 2007). Knapp et al. (2006) proposed and tested a model of the influence of top management support on an organization's security culture and level of security policy enforcement. They found that top management support is a significant predictor of an organization's security culture and level of policy enforcement. Their subsequent study explored the variables through which top management can positively influence security effectiveness. User training, security culture, policy relevance, and policy enforcement were all found to influence security effectiveness (Knapp et al., 2007).

RESEARCH QUESTIONS

The primary objective of the research described in this article is to explore how ease of use of passwords and facilitating conditions, such as the help and assistance available to users, influence user behavior in regards to their passwords. Three research questions were posed. To answer these research questions, a model derived from the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003) was developed (see Figure 1). The UTAUT attempts to forge a unified view of technology acceptance, and was developed through a review and consolidation of models that had previously been proposed to explain information systems usage behavior. The UTAUT is based on eight prior technology acceptance and use models: TRA (Fishbein & Ajzen, 1975), TAM (Davis, 1989), motivational model (Vallerand, 1997), TPB (Ajzen, 1991), a combined theory of planned behavior/technology acceptance model (Taylor & Todd, 1995), model of PC utilization (Thompson, Higgins, & Howell, 1994), innovation diffusion theory (Rogers, 1962), and social

Figure 1. Research model



cognitive theory (Bandura, 1986). The UTAUT captures a wider range of influences than any previous model and was found to account for 70% of the variance in usage in a longitudinal study (Venkatesh et. al., 2003).

The performance expectancy, social influence and voluntariness constructs of UTAUT have not been included in the research model. This research is looking specifically at the concepts of ease of use and facilitating conditions and their effect on intention and usage. Therefore performance expectancy, social influence and voluntariness are outside the scope of the project. Gender, a part of the original UTAUT model, is also not considered a factor of secure computer usage due to it becoming significantly less important as a factor in technology acceptance (Morris, Venkatesh, & Ackerman, 2005) and it was thus not included.

Consistent with the UTAUT and previous research relating to the acceptance of technology, the relationships described below were initially hypothesized in order to answer the research questions.

The first research question of interest was:

What effect does the ease of use of passwords have on users' intentions to use passwords securely and on actual secure usage?

Ease of use (also known as effort expectancy) is the extent to which a user believes that using a system will be free of effort (Davis, 1989). It is defined in this study as the ease of use of passwords. Consistent with the UTAUT and other models of technology and use, the ease of use of passwords should play a role in a user's intention to behave securely. In the current research, ease of use is thought to affect users' intentions to use their passwords in a secure fashion, such that the easier passwords are to use, the more likely users are to intend to act in a secure manner. The following hypothesis was therefore proposed.

H1: *Ease of use will have a positive effect on secure behavior intention.*

It was expected that users' intentions to act securely would have an impact on actual secure usage. Intention influencing actual behavior is a long held relationship and was a key concept in Fishbein and Ajzen's (1975) TRA and Davis's (1989) TAM. In this research, usage is defined as actually using passwords in a secure manner. The following hypothesis was therefore proposed.

H2: *Secure behavior intention will have a positive effect on secure usage.*

The second research question addressed in the study was:

Do facilitating conditions have an impact on secure usage of passwords?

Facilitating conditions is the help and assistance available to users when encountering problems with their passwords, and the usage there of. The help and assistance available to users is considered an essential part of usable security (Besnard & Arief, 2004). Consistent with the UTAUT, it was expected that the facilitating conditions available to users would have a direct effect on their secure usage of passwords. However, as facilitating conditions may also play a role in predicting intention under certain conditions (Venkatesh et al., 2003), any indirect effect via intentions was also of interest. The following hypotheses were therefore proposed.

H3:.*Facilitating conditions will have a direct positive effect on secure usage.*

H4:.*Facilitating conditions will have a positive effect on secure behavior intention.*

The third research question addressed in the study was:

What effect do external factors such as age and experience have on intention to use passwords securely and actual secure usage?

Anecdotally, it is thought that the older an individual the more they will encounter difficulty in using technology. This may be due to lack of confidence and/or lack of skill (Harrison & Rainer, 1992; Janvrin & Morrison, 2000). It was expected that a user's age may have an effect on their intention to use passwords in a secure fashion, as per the results by Morris and Venkatesh (2000). Therefore, the following hypothesis was proposed.

H5: *Age will have a negative effect on secure behavior intention.*

Users' prior general computing experience is expected to have an effect on their intention to behave securely. Taylor and Todd (1995) found significant differences in intention to use technology between experienced and inexperienced users, and Thompson, Higgins and Howell (1994) found that experience had a significant positive influence on use. This distinction is expected to apply in the computer security context. Experienced users are believed to understand the importance of security measures and have a greater intention to behave securely. The following hypothesis was therefore proposed.

H6: *Computing experience will have a positive effect on secure behavior intention.*

METHODS

To answer the research questions posed, data was collected via an online survey. As the primary focus of the survey was how people use their passwords, the potential user base found online was expected to have experience with this topic.

Participants

The target population for this research was all computer users, both in a workplace or home environment. A wide range of age and computing background was desired to get a more complete representation of attitudes towards password security. A link to the survey was posted on a number of websites, each having a wide variety of users. Additional participants were recruited via flyers on university notice boards and word of mouth. A total of 111 responses were obtained.

Data Collection

The software used to create the survey was LimeSurvey (http://www.limesurvey.org). This software allows for the creation of surveys and management of survey data. The gathered data is supplied via a Comma Separated Values (CSV) file. The survey was hosted on a privately run server, accessible by the general internet. Participants were invited to participate in the study by clicking on a link to complete a questionnaire on the web. The questionnaire contained 32 questions and took approximately 10 minutes to complete. Completion of the questionnaire was voluntary and all responses anonymous.

Measurement

Items to measure the constructs of interest were developed for the security domain using instruments from previous research on the UTAUT and other related technology acceptance models as a starting point, with new items being developed as needed. The measurement of each of the constructs is discussed below. The questionnaire completion process was pilot tested by 11 people and slight changes made to clarify questions. The Appendix contains a list of the items included in the final measurement model.

Ease of Use

Ease of use was measured using 8 items. These items are based on items from Pikkarainen, Pikkarainen, Karjaluoto and Pahnila (2004), Brown, Massey, Montoya-Weiss and Burkman, (2002) and Morris and Venkatesh (2000) and were measured on a 5 point Likert scale ranging from “strongly disagree” to “strongly agree”.

Facilitating Conditions

Facilitating conditions refers to the help and assistance that is available to users as they use their passwords. Facilitating conditions was measured using 6 items which are based on items from Aytes and Connolly (2004). Simple statements and a scenario involving a forgotten password were provided and the participants asked to rate their degree of agreement or disagreement using a 5 point Likert scale ranging from “strongly disagree” to “strongly agree”. The scenario posed was: “You have forgotten the password to a computer system, rendering you unable to login and use it, delaying your work”.

Secure Behavior Intention

Secure behavior intention relates to a participant’s intention to use their passwords in a secure fashion. The items used to measure secure behavior intention are based on items from Aytes and Connolly (2004), Ng and Rahim (2005), and Brown et al. (2002). Secure behavior intention was measured using 7 items relating to a scenario based around proper password hygiene. This scenario was: “Good password hygiene recommends a password of 12 characters, alphanumeric (letters and numbers), mixed case and other characters (such as ?, $, ^, #), changed every 30 days and not divulged to any party. A password such as “5gY?r4fTy`/q” satisfies these conditions.” This scenario applied to all the secure behavior intention survey items. Simple statements were provided and the participant asked to rate their degree of agreement or disagreement using a 5 point Likert scale ranging from “strongly disagree” to “strongly agree”.

Secure Usage

Secure usage refers to a participant’s actual usage of their passwords. The same scenario used to measure secure behavior intention was used for this construct. The items used were adapted from Aytes and Connolly (2004). Secure usage was measured using 8 items on a Likert scale. Six items had the scale ranging from “strongly disagree” to “strongly agree”, and the final 2 questions used a scale ranging from “very infrequently” to “very frequently”.

Age

Age was measured as the participant’s age in years.

Experience

Experience was measured as the participant’s general computing experience. It was not limited to their experience with computer security issues. A 5 point scale was used ranging from 1 “Basic (basic word processing, email, web skills)” to 5 “Advanced (Use of programming languages, use of multiple network types, confident user of new systems)”.

DATA ANALYSIS

Structured Equation Modeling (SEM) is a multivariate statistical technique that attempts to explain the relationship between many variables, by evaluating the interrelationships between latent constructs. SEM has the ability to model the interactions of latent constructs. The data analysis in this study was performed using Partial Least Squares (PLS), an alternative estimation approach to traditional SEM. Compared to SEM, PLS is not as sensitive to smaller sample sizes (Hair, Black, Babin, Anderson, & Tatham, 2006).

A two-step approach commonly used in SEM techniques was applied. The approach involves first testing the fit and construct validity of the proposed measurement model and then only once a satisfactory measurement model is obtained, the structural model is estimated. The measurement model is thus “fixed” when the structural model is estimated (Hair et al., 2006). SmartPLS version 2.0 was used to assess the measurement model and the structural model.

Outer loadings of the measurement items were assessed against the suggested cut-off value of 0.4 as suggested by Hulland

(1999). Several items which did not meet the desired 0.4 cut-off were discarded. To ensure the reliability of the measurements, the collected data was tested using three common indicators of reliability. These were Cronbach's Alpha, composite reliability and average variance extracted (AVE). The suggested cut-off value for reliability, when using both Cronbach's Alpha and the composite reliability technique is 0.7, and for AVE it is 0.5 (Hair et al., 2006). Table 1 summarizes the results of the reliability tests and demonstrates that acceptable reliability was obtained for each construct.

Two criteria were used to assess structural model quality: the statistical significance of estimated model coefficients and the ability of the model to explain the variance in the dependent variables. If the model is a valid representation of the influences on secure usage behavior, all proposed relationships in the model should be significant. The bootstrapping technique implemented in SmartPLS 2.0 was used to evaluate the significance of these hypothesized relationships. The R^2 of the structural equations for the dependent variables provide an estimate of variance explained (Hair et al., 2006), and therefore an indication of the success of the model in explaining these variables.

RESULTS AND DISCUSSION

Background Statistics

A total of 111 people (34.2% females and 65.8% males) participated in the study. The youngest participant was 17 years old, and the oldest was 88 years old (with an average age of 35.3 years). The wide age range is indicative of the growing level of participation in computing. The level of computing experience was rated between 1 (basic user) and 5 (advanced user). The average experience, using this scale was 3.49 (min=1, max.=5), indicating a relatively high degree of computer competency.

Figure 2 shows the standardized coefficients for each hypothesized path in the model and the R^2 for each dependent variable. Four of the six hypotheses were supported.

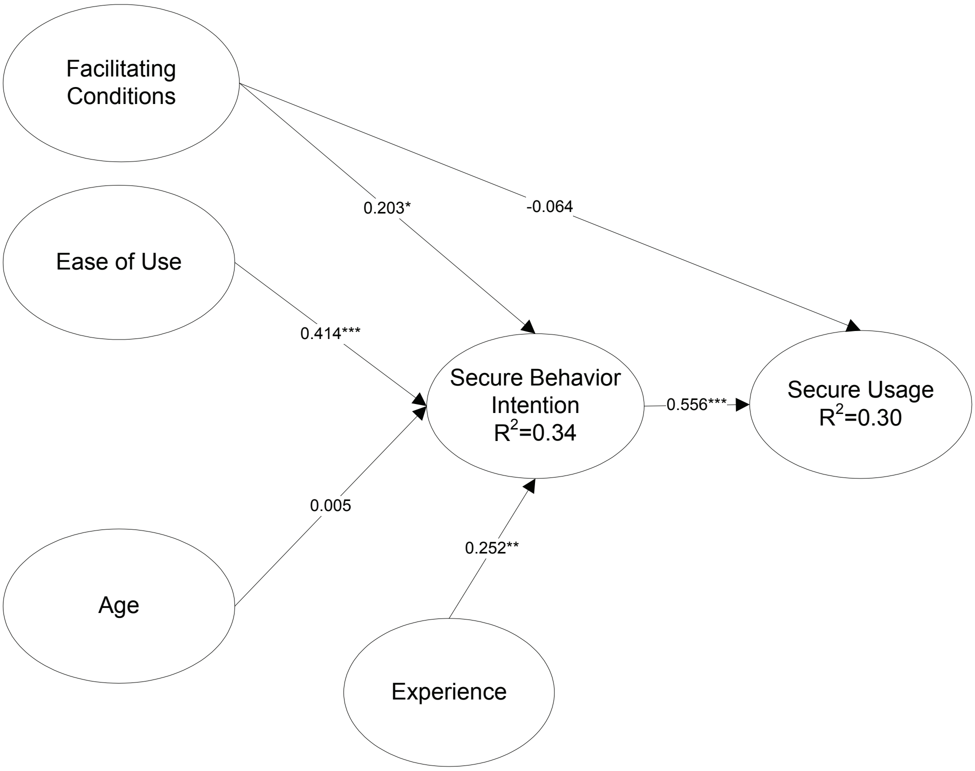
As hypothesized there was a significant positive relationship between ease of use of passwords and secure behavior intention. Thus, support was found for hypothesis

Table 1. Reliability of measurement

	Cronbach's Alpha	Composite Reliability	AVE
Ease of Use	0.85	0.89	0.56
Facilitating Conditions	0.70	0.82	0.61
Secure Behavior Intention	0.81	0.86	0.50
Secure Usage	0.88	0.91	0.62
Age	N/A*	N/A*	N/A*
Experience	N/A*	N/A*	N/A*

** indicates a single item measurement*

Figure 2. Structural model results



* *p* < 0.05
** *p* < 0.01
*** *p* < 0.001

H1. This is consistent with a great deal of literature relating to technology acceptance, that as something is easier to use, the intention to use it rises (Davis, 1989; Venkatesh et al., 2003). Therefore, in the context of this study, as passwords become easier to use, the intention to use them securely becomes higher. This complements previous literature about password use, which has shown that many users found passwords too difficult to use, leading to poorer usage (Adams & Sasse, 1999; Tari, Ozok, & Holden, 2006).

Secure behavior intention was also found to have a positive influence on secure usage. Thus, hypothesis H2 was supported. That is, in the context of passwords, as the intention to use them securely increases, passwords are used more appropriately. This is consistent with previous technology acceptance research which has found that intention leads to actual usage (Davis, 1989; Venkatesh et al., 2003). Or, to look at the situation holistically, as passwords become easier to use, the intention to use them properly rises, which in turn has a positive influence on actual secure usage.

The second research question addressed in the study related to the role of facilitating conditions. Contrary to expectations, facilitating conditions did not directly influence secure usage of passwords, therefore hypothesis H3 was not supported. However, facilitating conditions was found to have a weak significant effect on secure behavior intention. Although hypothesis H4 was supported, post hoc analysis of total effects showed that even though facilitating conditions influenced secure behavior intention, there was no indirect effect on secure usage. Provision of support for secure usage of passwords increased users' intentions to use passwords securely, but didn't increase their actual secure usage. This result is inconsistent with the UTAUT (Venkatesh et al., 2003) which postulates that the influence of facilitating conditions is primarily a direct one and inconsistent with Besnard and Arief's (2004) claim that the help and assistance available to users is an essential part of usable security, but consistent with Woon and Kankanhalli's (2007) study of developers' intentions to develop applications with security in mind which found that facilitating conditions had no significant effect. Also, in a study undertaken by Ng and Rahim (2005) it was found that facilitating conditions had no effect on a user's perception of the task they were performing as being under their control.

The third research question addressed in the study related to the possible effects of external factors such as age and experience on intention to use passwords securely and actual secure usage. The results indicate that age had no significant effect on secure behavior intention. Thus, hypothesis H5 was rejected. It appears that personal computing and associated actions (such as passwords) have become commonplace, and differences due to age may be declining (Munro, Huff, Marcolin, & Compeau, 1997; Parish & Necessary, 1996).

It was hypothesized that computing experience would influence password usage. A significant positive relationship was found between an individual's prior computing experience and their intention to act in a secure way. Consequently, hypothesis H6 was accepted. This result is consistent with prior research (Taylor & Todd, 1995). Post hoc analysis also showed that experience had an indirect influence on secure usage via secure behavior intention ($t = 2.51$, $p < 0.05$). Thus, as users become more experienced, they gain knowledge about the systems they work with and the security implications of usage. With this knowledge, they become more aware of concerns about the possible security implications of their behavior and their intention to behave securely increases, which in turn leads to more secure behavior.

Model's Ability to Explain Variability in Dependent Variables

Although two of the hypothesized paths were not found to be significant, the model showed reasonable explanatory power. The variance in secure behavior intention explained by the model was 34% ($R^2 = 0.34$) and the variance explained in secure behavior was 30% ($R^2 = 0.30$). This compares well with Ng and Rahim's (2005) results and demonstrates the research model's ability to predict secure behavior. Whilst Ng and Rahim did not study the usage of passwords, they tested three common security tasks and the intention of home users to perform each. The variance explained by their model for intention to carry out each of the security tasks was: anti-virus software updating (23%), data backup (18%), and firewall usage (39%).

The model makes a valuable contribution to the field of usable security. Whilst the existing literature has established that users find their passwords hard to use, this model demonstrates that the intention to use passwords in a secure way is predicated upon ease of use. In a more practical sense, it should give food for thought to system administrators and IT managers to review their guidelines regarding passwords.

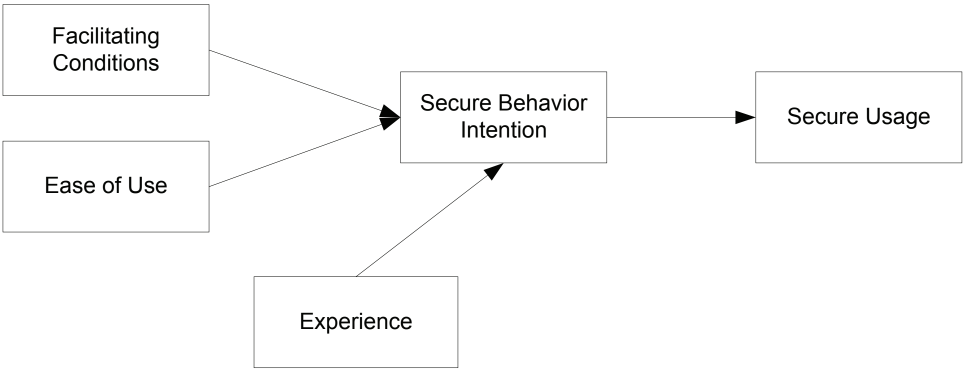
CONCLUSION

This research project aimed to determine the roles of ease of use, facilitating conditions, intention to use passwords securely, experience and age on users' usage of passwords. Data was collected via an online survey, and analyzed using PLS.

Figure 3 presents the research model with non-significant paths removed. The final model demonstrates the fundamental interest of this study, that difficult passwords have an impact on their usage. It also shows that an individual's intention to behave securely is a good indicator of their actual behavior. The model also shows that a user's prior computing experience influences their intention to act securely and though this, their actual secure usage. That is, the more experienced a person is, the more likely they are to behave securely. It is interesting to note that while available assistance had a weak impact on intention to use passwords securely, it did not influence actual secure usage.

The secure usage of computer systems is a key concern for many parties. System administrators' efforts are in vain if the technology reduces the ability of users to act securely. This concern is not just a technical administration and management issue. The dealings of individuals, business, government and society rely on secure transfer of information, and it is vital that the ability to do so is made as effective as possible. The results of this research highlight the importance of ensuring that passwords are easy to use. As one participant stated "Secure passwords are by definition transient and difficult to remember. This is a fundamental flaw in the password mechanism for everyday use". This highlights the main theme of this research and illustrates the false dichotomy often found in application development: it can be secure, or it can be usable.

Figure 3. Relationships supported by this study



REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing, 16*(3), 22-40.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bell, D. E., & LaPadula, L. J. (1973). *Secure Computer Systems: Mathematical Foundations*. Bedford, Massachusetts: MITRE Corporation.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*(3), 253-264.

Braz, C., & Robert, J. (2006). Security and usability: The case of the user authentication methods. In *Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine* (pp. 199-203). New York, USA: ACM Press.

Brostoff, S., & Sasse, M. A. (2000). Are passfaces more usable than passwords? A field trial investigation. In *Proceedings of HCI 2000* (pp. 405-424). Sunderland, UK.

Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., & Burkman, J. R. (2002). Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems, 11*(4), 283-295.

Cazier, J. A., Wilson, E. V., & Medlin, B. D. (2007). The role of privacy risk in IT acceptance: An empirical study. *International Journal of Information Security and Privacy, 1*(2), 61-73.

Ceraolo, J., P. (1996). Penetration testing through social engineering. *Information Systems Security, 4*(4), 37-49.

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: Designing secure systems that people can use*. Sebastopol: O'Reilly.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, WA: Addison-Wesley.

Garfinkel, S., Spafford, G., & Schwartz, A. (2003). *Practical unix & internet security*. Sebastopol: O'Reilly.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate Data Analysis* (6th Edition ed.). Upper Saddle River, NJ, USA: Pearson Education.

Halderman, J. A., Waters, B., & Felten, E. W. (2005). A convenient method for securely managing passwords. In *Proceedings of the 14th International Conference on World Wide Web* (pp. 471-479). New York NY, USA: ACM Press.

Harrison, A. W., & Rainer, K. (1992). The influence of individual differences on skill in end-user computing. *Journal of Management Information Systems, 9*(1), 93-111.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*(2), 195-204.

Janvrin, D., & Morrison, J. (2000). Using a structured design approach to reduce risks in end user spreadsheet development. *Information & Management, 37*(1), 1-12.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy.

Information Management & Computer Security, 14(1), 24-36.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2007). Information security effectiveness: Conceptualization and validation of a theory. *nternational Journal of Information Security and Privacy, 1*(2), 37-60.

Langsford, A., Naemura, K., & Speth, R. (1983). OSI management and job transfer services. *Proceedings of the IEEE, 71*(12), 1420-1424.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2/3), 57-63.

Mainwald, E. (2003). *Network security: A beginner's guide*. New York: McGraw Hill/ Osborne.

Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing workforce. *Personnel Psychology, 53*(2), 375-403.

Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2005). Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior. *IEEE Transactions on Engineering Management, 52*(1), 69-84.

Munro, M. C., Huff, S. L., Marcolin, B. L., & Compeau, D. R. (1997). Understanding and measuring user competence. *Information & Management, 33*, 45-57.

Ng, B. Y., & Rahim, M. A. (2005). A socio-behavioral study of home computer users' intention to practice security. In C. Saunders (Ed.), *Proceedings of The Ninth Pacific Asia Conference on Information Systems*. Bangkok, Thailand: Pacific Asia Conference on Information Systems.

Nielson, J. (1990). Heuristics for User Interface Design. Retrieved 5 February 2008, from http://www.useit.com/papers/heuristic/heuristic_list.html

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In *Proceedings of the 5th Conference on Information Technology Education* (pp. 177-181). New York NY, USA: ACM Press.

Parish, T. S., & Necessary, J. R. (1996). An examination of cognitive dissonance and computer attitudes. *Educational Technology, Research and Development, 116*(4), 565-566.

Patrick, A. S., Long, A. C., & Flinn, S. (2003). HCI and security systems. In *Conference on Human Factors in Computing Systems* (pp. 1056-1057). New York NY, USA: ACM Press.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: An extension of the technology acceptance model. *Internet Research, 14*(3), 224-235.

Rogers, E. M. (1962). *Diffusion of Innovation*. New York: Free Press.

Singh, S., Cabraal, A., & Hermansson, G. (2006). What is your husband's name? Sociological dimensions of internet banking authentication. In *Proceedings of the 20th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artefacts and environments* (pp. 237-244). New York , USA: ACM Press.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Tari, F., Ozok, A. A., & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *SOUPS '06: Proceedings of The Second Symposium on Usable Privacy and Security* (pp. 56-66). New York NY, USA: ACM Press.

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly, 19*(4), 561-570.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1994). Influence of experience on personal computer utilization: Testing a conceptual model. *Journal of Management Information Systems, 11*(1), 167-188.

Vallerand, R. J. (1997). Toward a Hierarchical Model of Intrinsic and Extrinsic Motivation. In *Advances in Experimental Social Psychology* (Vol. 29, pp. 271-360). New York: Academic Press.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: A first step towards effective password security in the real world. In *NSPW '01: Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 137-143). New York, USA: ACM Press.

Weissmann, C. (1969). Security controls in the ADEPT-50 timesharing system. In *AFIPS Conference Proceedings* (pp. 119-133). Santa Monica CA, USA: System Development Corporation.

Woon, I. M. Y., & Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. *International Journal of Human-Computer Studies, 65*(1), 29-41.

Zurko, M. E. (2005). User-centered security: Stepping up to the grand challenge. In *Proceedings of the 21st Annual Computer Security Applications Conference* (pp. 187-202). Washington, DC, USA: IEEE Computer Society.

Zurko, M. E., & Simon, R. T. (1996). User-centered security. In *NSPW '96: Proceedings of the 1996 Workshop on New Security Paradigms* (pp. 27-33). New York NY, USA: ACM Press.

APPENDIX

Final Items Used to Measure Constructs

Ease of use

I find my password(s) are difficult to use?

I find my password(s) impede my ability to do my work?

If I faced multiple systems, each with their own password, I would feel this required a large amount of mental effort

If I faced multiple systems, each with their own password, I would be able to remember each password*

If I faced multiple systems, each with their own password, I would write down each password

If I faced multiple systems, each with their own password, I would see password(s) as being too complicated

Facilitating conditions

The assistance available to me is helpful

I am able to get assistance

I am able to get prompt assistance

Secure behavior intention

I intend to create strong password(s)

I intend to periodically update my password(s) to maintain a high level of password security

I intend to keep my password(s) secret from friends

I intend to keep my password(s) secret from family

I intend to keep my password(s) secret from co-workers (if applicable)

I intend to keep my password(s) secret from system administrators (if applicable)

I intend to avoid creating a written note of my password(s) to aid remembering

Secure usage

I follow these guidelines

I feel these guidelines are too hard

If I followed these guidelines, I feel I would not be able to remember my password(s)

If I followed these guidelines, I would write down my password(s)

If I was mandated to follow these guidelines, I would make additional effort to remember my password(s)

After establishing a user account, do you regularly change your password(s)?

How regularly are you willing to change your password(s)?

Do you ever divulge your password(s) to a family member, friend, colleague or other individual?

Lee Novakovic is in a graduate program with a governmental consumer affairs agency. He has an honours degree in computer science from Murdoch University. His research interests include information security, data communications and human factors in computing.

Tanya McGill is a senior lecturer in information technology at Murdoch University in Western Australia. She has a PhD from Murdoch University. Her major research interests include information technology education and end user computing. Her work has appeared in various journals including Decision Support Systems*,* Journal of Research on Computing in Education*,* European Journal of Psychology of Education*,* Information Resources Management Journal *and* Journal of Organizational and End User Computing.

Michael Dixon is a senior lecturer in information technology at Murdoch University in Western Australia. He holds a PhD from Murdoch University and a MBA in telecommunications management from Golden Gate University. He is also a certified Cisco Certified Network Professional (CCNP), Cisco Certified Design Professional (CCDP), and Cisco Certified Academy Instructor (CCAI). His major research interests include information technology education, data communications and neural networks.