This document is an author-formatted work. The definitive version for citation appears as:

D. S. Carstens, P. McCauley-Bell, L. C. Malone, and R. F. DeMara, "Evaluation of the Human Impact of Password Authentication Practices on Information Security," *Informing Science Journal*, Vol. 7, No. 1, August, 2004, pp. 67 – 85.

Link: http://inform.nu/Articles/Vol7/v7p067-085-229.pdf

Evaluation of the Human Impact of Password Authentication Practices on Information Security

Deborah Sater Carstens
Florida Institute of Technology, Melbourne, FL, USA

carstens@fit.edu

Pamela R. McCauley-Bell, Linda C. Malone, and Ronald F. DeMara
University of Central Florida, Orlando, FL, USA

mcbell@mail.ucf.edu

lmalone@mail.ucf.edu

demara@mail.ucf.edu

Abstract

The research objective was to develop a model for evaluating the human impact that password authentication issues are having on the security of information systems. Through distributing a survey and conducting an experiment, , researchers created a model for predicting the vulnerability that a particular set of conditions will have on the likelihood of error in an information system. The survey consisted of over 250 respondents. The experiment consisted of 30 subjects and the analysis utilized a $\chi 2$ goodness of fit test. The findings indicate that human error associated with password authentication can be significantly reduced through the use of

passwords which are comprised of meaningful data for the user and that meet the information technology community requirement for strength of password. Future research will be performed to further validate and enhance the developed model and to develop human factor password guidelines.

Key Words: Human Error, Information Security

Introduction

The increase in computing and networking expansion as well as increases in threats has enhanced the need to perpetually manage information security within an organization. Although there is literature addressing the human side of information security, events such as 9/11 and the war on terrorism has created more of a burden for organizations, government and private industry, enhancing the need for more research in information security. Carnegie Mellon's Computer Emergency Response Team (2004) has collected statistics showing that 6 security incidents were reported in 1988 compared to 137,529 in 2003. A survey by the Federal Bureau of Investigation (FBI) suggested that 40% of organizations surveyed claimed that system penetrations from outside their organization have increased from the prior year by 25% (Ives, Walsh, & Schneider, 2004). The U.S. Department of Homeland Security (2002) is concerned with the need for information security measures. Therefore, the Federal Information Security Management Act of 2002 was put into place for the purposes of protecting information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability of information. The government has an information security responsibility ranging from protecting intelligence information to issuing social security numbers for each citizen. Private industry must also be concerned with information security as it is vital for the livelihood of any company to protect customer's personal information along with the management of each company's supply chain (Olivia, 2003).

Earlier research identified the presence of human error risks to the security of information systems (Wood & Banks 1993, Courtney as cited in NIST, 1992). A survey conducted by one of the authors, identified password issues as the second most likely human error risk factor to impact an information system. The significance of this is enhanced when realizing that passwords are the primary source of user authentication for the majority of personal and private information systems. The past research findings of password issues as a human error risk factor has been further identified as a threat to security by the University of Findlay Center for Terrorism Preparedness (2003), who developed a vulnerability assessment methodology to better help organizations identify their weaknesses in terms of information security.

Extensive password requirements can overload human memory capabilities as the number of passwords and their complexity level increases. The exponential growth in security incidents (Carnegie Mellon Computer Emergency Response Team, 2004) requires a comprehensive approach to the development of password guidelines which do not exceed human memory limitations yet maintain strength of passwords as necessitated by the information technology (IT) community. The IT community consists of network administrators or security officers who are directly responsible for information security in terms of integrity, confidentiality, and availability of information. In earlier investigations, over 50% of incidents that occur within government and private organizations have been connected to human errors (NIST, 1992). The impact of human error on information security is an important issue that left unresolved can have adverse affects on industry. This research is focused on measuring the impact of password demands as a means of authentication and mitigating the risks that result when these demands exceed human capabilities.

Literature Review

Information Security

Information security involves making information accessible to those who need the information, while maintaining integrity and confidentiality. The three categories that are used to classify information security risks are confidentiality, integrity, and accessibility or availability of information (U.S. Department of Homeland Security, 2002). A security breach in confidentiality is defined as sources not intended to have knowledge of the information have been provided with this knowledge. An example of this category would be sending sensitive data to the wrong person. A security breach in integrity is an incident where there is an unauthorized or incorrect change made to an information source. An example of this category is a financial accounting error causing the

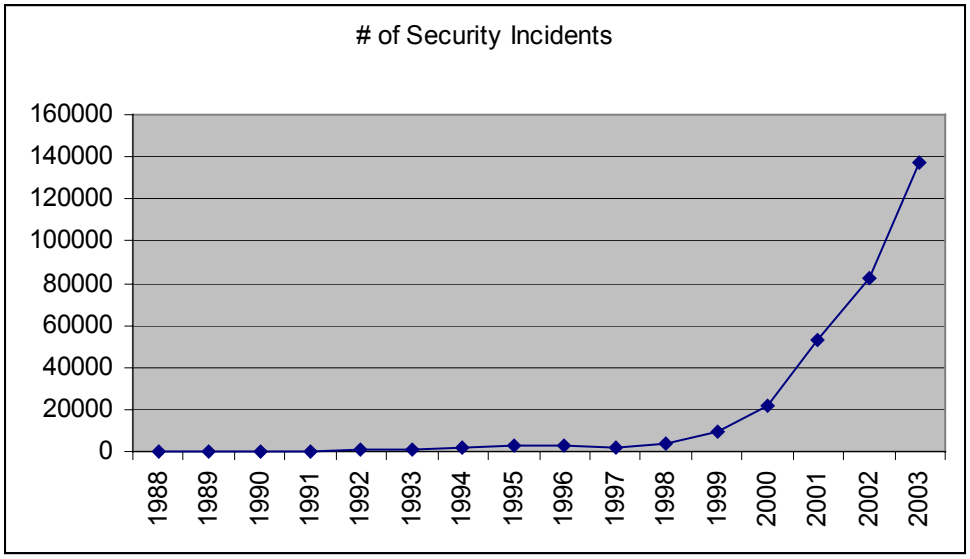

Figure 1. Growth in the Number of Security Incidents
(Carnegie Mellon Computer Emergency Response Team, 2004)

information in the database to be inaccurate. A security breach in accessibility occurs when either access for those entitled to a system is denied or access is given to those who are not authorized to access the system. An example of this category would be an authorized user of a system who is unable to access a system due to forgetting their password. Therefore, a human error security incident is defined as any human error-related event that compromises information as defined by the above categories (Carstens & McCauley-Bell 2000). The exponential growth in security incidents as seen in Figure 1 illustrates the increasing importance of information security for organizations (Carnegie Mellon Computer Emergency Response Team, 2004). In spite of the growing number of security incidents and the Federal Information Security Management Act of 2002, network vulnerabilities continue to exist (Carlson, 2004). To better help organizations reform, the U.S. Government Accounting Office identified five categories that need to be ad

dressed by agencies to protect networks. The categories include access control, system integrity, cryptography, audit and monitoring, and configuration control. Although the Federal Information Security Management Act of 2002 exists along with the newly identified information security categories, organizations are still struggling with specific ways to improve security.

Human Error in Information Security

Kaplan-Leiserson (2003) discusses a study performed by KPMG, now BearingPoint, which suggests that 70% of security breaches at companies are due to actions taken by employees either indirectly or directly. Accidental or deliberate errors by individuals have adverse impacts through increasing an organization's vulnerability (Dutta & McCrohan, 2002). Earlier research by Wood and Banks (1993) suggested that human error has been indicated as the primary factor causing up to 52% of corporate information damage due to information security incidents. In the past, the information technology community has focused extreme attention on reducing or eliminating the risk of malicious outsiders invading company proprietary information databases. However, research has indicated that human error makes up as much as 65% of incidents causing economic loss for a company and that only 3% or less of the time are security incidents caused by external threats such as computer hackers (Lewis, 2003; McCauley-Bell & Crumpton, 1998; NIST, 1992). Although, external malicious attacks can be costly to organizations, these intentional acts causing security breeches are among the lowest risk of information security incidents (Lewis, 2003). There is only a minimal effort to address the human factors issues or human error risks in information security which is among the highest risk of information security incidents (Carstens & McCauley-Bell, 2000; McCauley-Bell & Crumpton, 1998; Wood & Banks, 1993).

Earlier research by one of the authors identified the following categories of information security-related human errors: configuration errors, password issues, incorrect access, input errors, not following procedures, insecure program(s), workload issues, ignorance, and failure to upgrade. This research also indicated that the results of these human error problems cause there to be a compromise in integrity of information, distribution of improper, inaccurate, or confidential information, inability to deliver services, information system interruption, significant economic loss, and loss of life. There were many key human error problems also identified such as a lack of inadequate training, lack of awareness regarding the importance of data and the associated risks for insecure behavior, time pressures (stress and overload on users and system administrators), lack of responsibility/accountability felt by users (for example, disabling a virus protection program because it slows down their computer), employees sharing internal data to external groups, lack of checks/balances, etc. This research also identified several activities which may mitigate the risks of human error consisting of training, automating system functions, increasing accountability perceived by the user, reminders of prominent risks, increasing staffing levels, and having a defined security policy (Carstens & McCauley-Bell, 2000).

In an effort to reduce the risk of security breeches, it is important to create a level of awareness to the users of systems of the associated risks (Kaplan-Leiserson, 2003; Kyas, 1997; McCauley-Bell & Crumpton, 1998). Actions that have been successful in organizations in reducing human error-related information security incidents are training for users and increasing automated functions in a computer (Kaplan-Leiserson, 2003; McCauley-Bell, Carstens, Wilson, Grimsley, & Malone, 2000). An example of increasing automated functions within a computer would be to have a pop up menu appear on an employee's computer screen giving notification that it is time to change their password. Since the human factors discipline has been successful in resolving human errors with human-computer interaction (HCI), these risks can be mitigated through the application of human factors-related interventions (Carstens & McCauley-Bell, 2000; McCauley-Bell & Crumpton, 1998; Preece, Roger, Sharp, Benyon, Holland, & Carey, 1994).

Short-term Memory

In developing a model for evaluating the human impact that password authentication issues are having on the security of information systems, understanding Miller's (1956) Chunking Theory is useful. Miller's Chunking Theory classifies data in terms of chunks and states how the capacity

of working memory is 7±2 chunks of information. A chunk of data is defined as being a letter, digit, word or a different unit such as a date. A chunk is further described as a set of adjacent stimulus units that are closely tied together by associations in the user's long-term memory. Therefore, research suggests that merely turning information into a meaningful chunk of data can increase a person's short-term memory capacity. This occurs because chunking data places the input into subsets that are remembered as single units. A person's short-term memory capacity would be reduced if a person tried to remember isolated digits or letters rather than grouping or recoding the information into chunks of data. Chunking then becomes useful in creating a meaningful sequence of stimuli within the total string of data which then serves as an integral representation of data that is already stored in long-term memory. Golbeck (2002) suggests that schemas can serve as the basis for chunks because they provide a meaningful method for grouping information. A schema is defined as a mental model that makes it easier for users to recall an item. Newell, Shaw, and Simon (1961) suggest that highly meaningful words are easy for a person to learn and remember than less meaningful words. Meaningful (Newell et al., 1961) is defined by the person's number of associations with the word, frequency of the word, familiarity with the sequence orders of the letters, or the ability for the word to elicit an image. Another study conducted by Loftus, Dark, and Williams (1979) tested short-term memory retention among ground control and student pilots through examining communication errors. The findings of this research further support Miller's work, as recall was better when material was chunked. Precezewski and Fisher (1990) studied the format of call signs made up of any series of letters and digits used by the military in secured radio communications. The findings indicate that the size of the chunks influenced the accuracy of short-term retention. Furthermore, mixing letters and digits within one chunk was more difficult to recall than just having letters or digits make up the chunk. This research also then suggests that memory is enhanced when the person can make meaning of the material. Wickens (1992) suggests that chunking should be used whenever possible because of working memory limitations. System designers or in this case, system password guideline designers, should not exceed the low end of Miller's 7±2 scale. Wickens (1992) views chunking as a strategy or mnemonic device that may be taught. Therefore, this strategy or mnemonic device is most useful in the application of helping organizations and individuals develop passwords that do not exceed human memory limitations.

Methodology

This research is currently ongoing and the methodology for this study consists of the following:

- √ Survey
  - Evaluate user practices in determining passwords.
  - Determine vulnerabilities produced through user actions.
- √ Limited case study of a large federal agency
  - Test the usefulness of individuals customizing their passwords utilizing meaningful data and mnemonic devices in password development.
  - Determine the human impact that password authentication issues have on information security.

Survey

A password information security survey was distributed to over 250 participants to determine how the number of passwords an individual has to recall impacts the security of an information

system. This research was conducted to address the human side of information security and more specifically the human impact to information security. The 250 participants were made up of university students and employees. There were three sections incorporated into the design of the survey. Section one of the survey concentrated on understanding individuals' work and school passwords. Examples of work and school passwords are computer passwords, company credit card pin codes, voice mail security codes, facility access codes, etc. Section two of the survey concentrated on understanding individuals' personal passwords. Examples of personal passwords are computer passwords, ATM pin codes, on-line banking passwords, home security access codes, answering machine codes, etc. The third section of the survey concentrated on the demographics of the participants in relation to their gender, age, educational level, etc. A copy of the twenty-three-question survey can be found in the Appendix. The results of this survey were analyzed to aid researchers in the development of the password guidelines utilized in the federal case study experiment.

Federal Case Study Experiment

A limited case study was performed at a large US government agency in which 30 participants opened three password protected Microsoft Word ™ 97 documents five days a week for three weeks. The purpose of the study was to determine the level of password remembrance when an individual developed a password utilizing generic instructions versus specific instructions that required individuals to utilize mnemonic devices. Therefore, the experiment contained three stages that tested different password difficulty levels. Difficulty levels for each stage of the experiment were established through the amount of meaningful data that was contained in participants' passwords as well as participants' ability to chunk the data for ease of remembrance. The guidelines followed by each participant ensured the use of secure passwords as necessitated by the federal agency information technology personnel. A brute force calculation of the shortest passwords utilized in the study was calculated to further ensure the passwords were considered secure.

Stage one required participants to choose their own passwords that satisfied stringent password guidelines. Microsoft Word ™ 97 document password files were not encrypted and can be printed out in plain text. The "protected" file can be inserted a new document and read. However, for the purposes of this study, the Microsoft Word ™ 97 document passwords were sufficient.

The guidelines listed below were used for stage one:

1. Passwords must be at least 7 characters in length.
2. Passwords must have a combination of symbols.
3. Password can not use the same term more than twice.
4. Password must not spell out a dictionary word or proper noun.
5. Password can not be relevant data such as individual's social security number, street address, birth date, etc.

The second and third stages of this experiment required participants to form their passwords through the use of chunking meaningful data together that enabled the passwords to utilize mnemonic devices. The second stage utilized three passwords which were ten characters consisting of their first and last initials using a combination of both uppercase and lowercase letters and their federal agency start date using different types of symbols as day, month, and year separators. The third stage of this experiment had participants utilize three passwords that were the same as the passwords utilized in stage two but with an additional two characters consisting of their mother's first name initial in uppercase and maiden name initial in lowercase.

The security of the password guidelines utilized in each stage were also assessed through application of the multiplicative rule to calculate how many guesses it would take an individual to identify the simplest proposed password (Mendenhall & Sincich, 1994). Results indicate that the expected number of attempts required exceeds one trillion equiprobable guesses from the uninformed attacker. Moreover, brute force attacks are frequently disbarred by limiting the number of unsuccessful login retries. In particular, most systems typically lock out individuals after they complete trying their password three times. Nonetheless, a very determined intruder may attempt access into all user accounts in succession after failing. This is an idealized analysis since it assumes all letter choices are random for any character positioning, but in practice this analysis is optimistic because the recommended guidelines suggest nonrandom letter choice. However, this analysis does still provide a rough estimate of the robustness of the recommended password guidelines. Even if we subtract out 215,000, which is the number of dictionary words in the English language according to Merriam-Webster's Collegiate Dictionary (1998), from Equation (1) and recalculate Equation (2), it would still take a person approximately 16 trillion times [(1E14-215,000) divided by 3 and again by 2] to Log-on to get the correct answer. Therefore, the possibility of guessing the correct password is still considered to be a sufficiently small number. The calculation that determined it would take someone over a trillion guesses before breaking the code of the shortest password in terms of character length tested in this research using the multiplicative rule is below:

- Letters in the alphabet = 26 X 2 (Available uppercase and lowercase letters)
- Amount of available one digit numbers (0-9) = 10
- Number of symbols available ≅ 40
- Character length of smallest password tested in experiments = 7

$$26 \times 2 + 10 + 40 \cong 100 \quad (1)$$

$$(100)^7 = (1E2)^7 = 1E14 \quad (2)$$

1E14 equals the different combinations of 7 tokens (where a token can be a number, letter, or symbol). Since the assumption is that there are 3 retries before a User Id is disabled, 1E14 will be divided by 3 retries and divided once more by 2 signifying a person on average will only have to go through 50% of the different usernames before guessing the correct password as shown in Equation (3).

$$(1E14/3)/2 = 1E14/6 = 16 \text{ trillion} \quad (3)$$

Therefore, it would take approximately 16 trillion times before a person has to Log-on to get the correct answer. The question that arises is how long it would take a person to Log-on 16 trillion times. If a person can only Log-on just once a day, it would take a person about 50 Billion years to guess the correct combination. Even if a person could Log-on every second of everyday, it would take 600,000 years to guess the correct combination. This is calculated by taking 50 Billion years divided by the number of seconds in a day (86,400) which is approximately equal to 600,000 years. Therefore, all four-password guidelines that ranged between seven to twenty-two characters in length can be considered secure from a brute force attack standpoint.

Measurement of participant's performance was determined through asking each participant five days a week to answer four questions. The individuals answered the questions through self report. The exact same questions were asked to each participant throughout the length of the experiment. A $\chi 2$ goodness of fit test was used to determine which set of password guidelines were easier for participants to remember and which passwords required participants to refer the most to a piece of paper to aid in recalling passwords. The four questions asked are listed below:

1-Did you remember all 3 passwords? (Requires a yes or no answer)

2-Did you have to look at a sheet of paper to remember the passwords? (Requires a yes or no answer)

3-How many passwords did you forget?

4-How many times did it take you to successfully open the password protected file?

The results to questions number three and four were omitted since there were many inconsistent responses. An interview of participants was conducted to ensure that these questions were the actual cause of confusion for the participants. The inconsistent responses resulted from participants counting typing errors as both forgotten and remembered passwords, where as the intent would have been that typing or input errors do not constitute a forgotten password. Also, participants who remembered at least one of their passwords and had even accessed their password protected word file successfully but had to refer to a sheet of paper to recall the remaining passwords would list that all three passwords were forgotten. These same individuals would claim that all three of their passwords were forgotten every time they referred to the sheet of paper since all three of their passwords were listed on the paper and then would respond correctly to the question regarding the number of passwords actually remembered. Therefore, the last two questions were omitted from the analysis of this research.

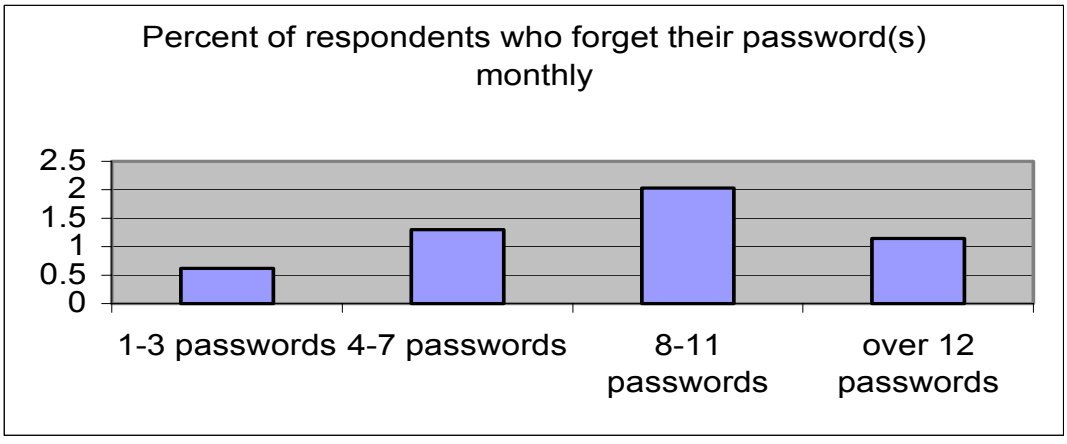

Figure 2. Percent of respondents (255 respondents to this survey question) who forgot their work or school passwords at least once a month. Respondents with only 1-3 passwords forgot a password approximately once every two months whereas respondents with 8-11 passwords forgot a password approximately twice every month.

Results

Survey Results

The survey results indicate that those individuals with eight to eleven work or school passwords are at greatest risk for not remembering their passwords at least once a month as seen in Figure 2. Therefore, these individuals resort to writing down their work or school passwords on a piece of paper to refer to when inputting system passwords as seen in Figure 3. Figure 4 contains the breakdown of difficulty levels of individuals' work or school passwords such as passwords comprised of one word, more than one word, unfamiliar or familiar numbers, and string of numbers, letters, and/or symbols. The results from the work or school password section of the survey were utilized to develop the password guidelines for the federal case study experiment.

The survey analysis also consisted of an analysis of the presage variables to look at the effects. The interesting effects identified are displayed in Figure 5, 6, and 7. Figure 5 looked at the difference in men and women in regards to the percent of each gender that writes their personal password on paper. There were less than one percent of males and females who write their passwords down on paper. However, it is interesting that of the individuals surveyed, females ac-

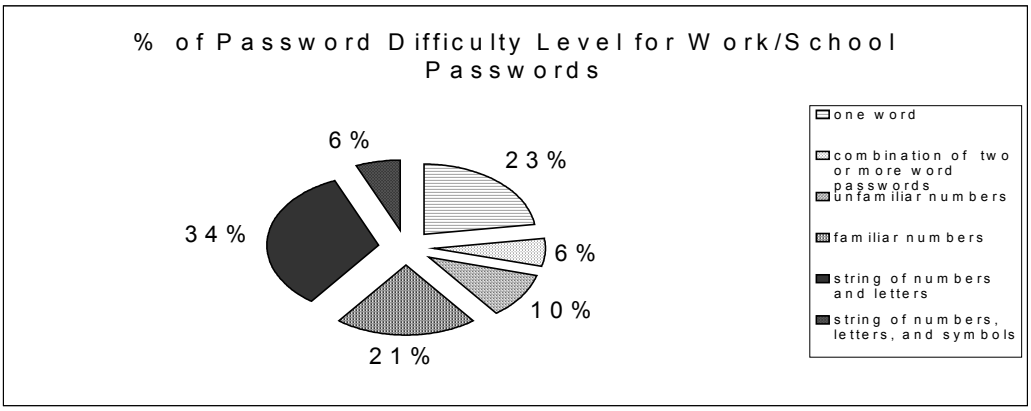

Figure 4. Percent of respondents (220 respondents to this survey question) with passwords that were comprised of one word, combination of two or more words, unfamiliar numbers, familiar numbers, string of numbers and letters, or string of numbers, letters, and symbols.

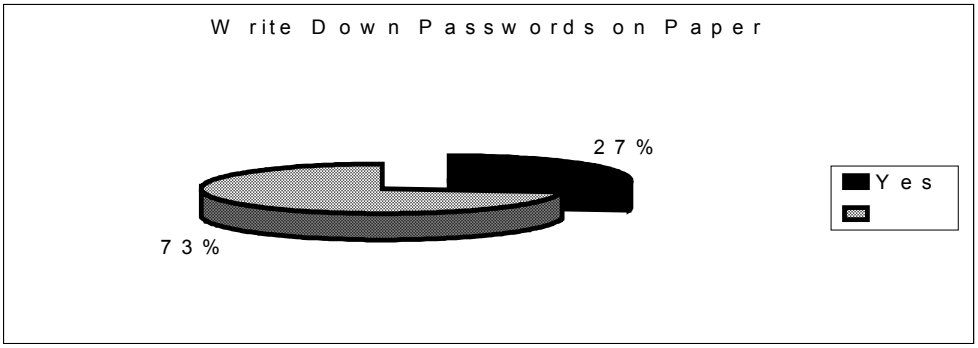

Figure 3. Percent of all survey respondents (257 respondents to this survey question) who wrote down their work or school passwords on paper to refer to when inputting their system passwords.

counted for two-thirds and men only one-third of the individuals who write their passwords on paper. The research indicates that .24% of females write their personal password on paper while only .12% of males write their personal password on paper. Furthermore, the analysis included looking at any differences between part-time, full-time, and individuals that are not employed. Figure 6 displays the results that suggest that part-time employees have on average 3.77 work or school passwords. Full-time employees have on average 3.02 work or school passwords. Indiv-

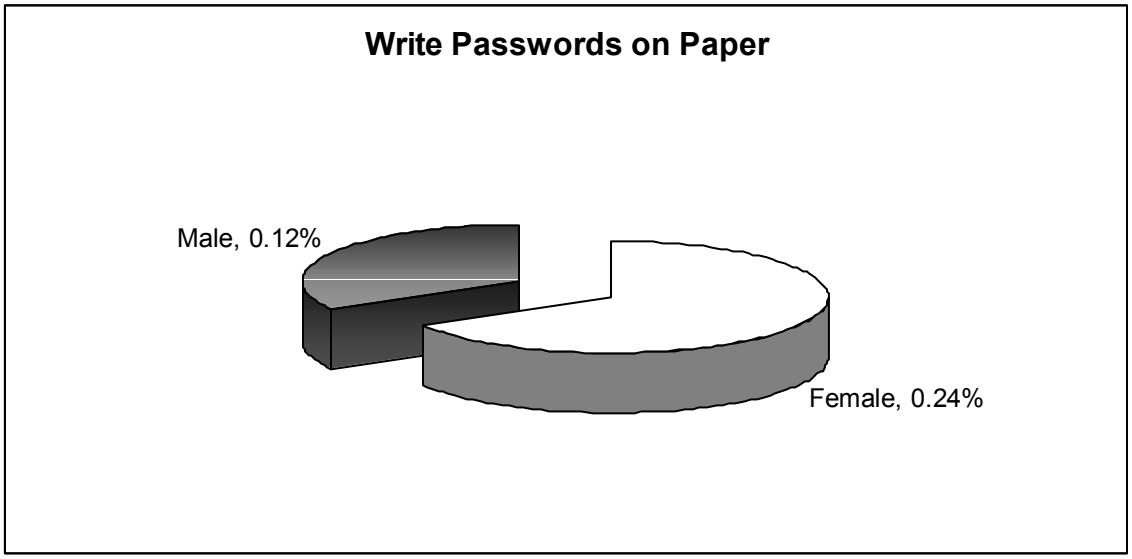

Figure 5. Percent of males and females who write their personal passwords on paper for recall purposes.

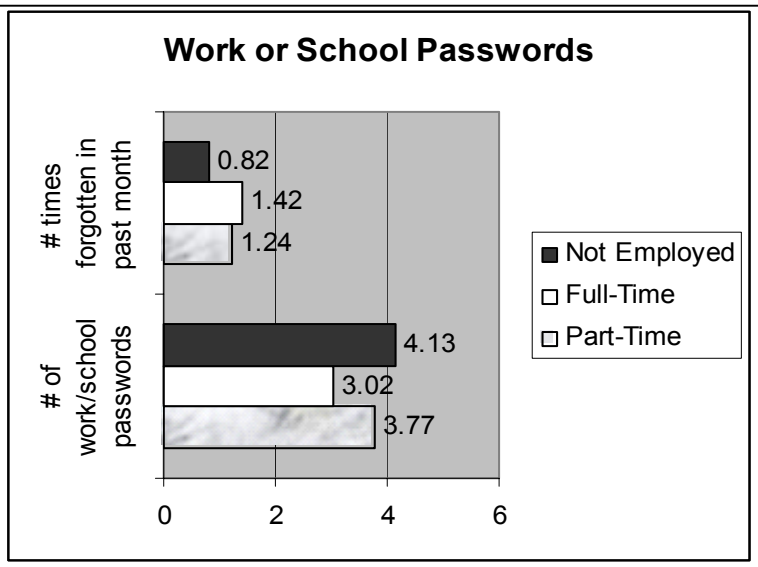

Figure 6. The average number of work or school passwords owned by individuals who are not employed, full-time, or part-time are displayed. Also, the number of times on average individuals has forgotten their password in the last month is shown.

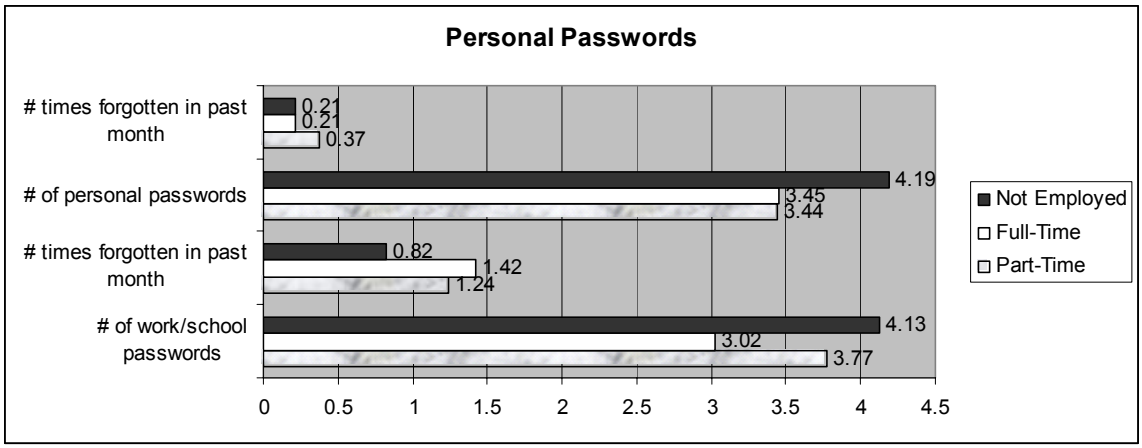

Figure 7. The average number of personal passwords owned by individuals who are not employed, full-time, or part-time are displayed. Also, the number of times on average individuals has forgotten their password in the last month is shown.

iduals who are not employed had the most average number of passwords being 4.13. Figure 6 also displays the results that indicate that part-time employees forgot their password on average 1.24 times in the last month, full-time employees forgot their password on aver age 1.42 times in the last month, and individuals employed only forgot their password on average .82 times in the last month. Figure 7 shows similar results as Figure 6 except the focus is on personal passwords. The results suggest that part-time employees have on average 3.44 personal passwords and forgot their passwords on average .37 times in the last month. Full-time employees have on average 3.45 personal passwords and forgot their passwords on average .21 times in the last month. Individuals not employed have on average 4.19 personal passwords and forgot their passwords on average .21 times in the last month. The results identified have open several opportunities for additional research in further analysis of presage variables in regards to information security.

Federal Case Study Experiment Results

The results of a case study of a large federal agency are presented. Table 1 shows the results of performing a $\chi 2$ goodness of fit test on the answers received from the participants regarding the question "Did you remember all 3 passwords?". The results indicate that stage two, 10 characters in length, and stage three, 12 characters in length, passwords had a significantly higher level of remembrance than stage one passwords.

Table 1

STAGES	% DAYS REMEMBERED ALL PASSWORDS
Stage 1	50.7
Stage 2	66.7
Stage 3	72.7
Stage 1-2-3 $p \leq .001$; Stage 2-1 $p < .01$; Stage 3-1 $p < .001$; Stage 3-2 p= NS	

Table 2

STAGES	% DAYS LOOKED AT PAPER TO RECALL PASSWORD
Stage 1	48.5
Stage 2	29.6
Stage 3	23.5
Stage 1-2-3 $p \leq .001$; Stage 2-1 $p < .01$; Stage 3-1 $p < .001$; Stage 3-2 p= NS were an increased	

Table 2 shows the results of performing a $\chi 2$ goodness of fit test on the answers received from the participants regarding the question "Did you have to look at a sheet of paper to remember the passwords?". The results indicate that individuals referred to a piece of paper to recall a password significantly more with stage one than with stage two and three representing the difficulty individuals experienced in recalling stage one passwords. Through interviewing participants, an

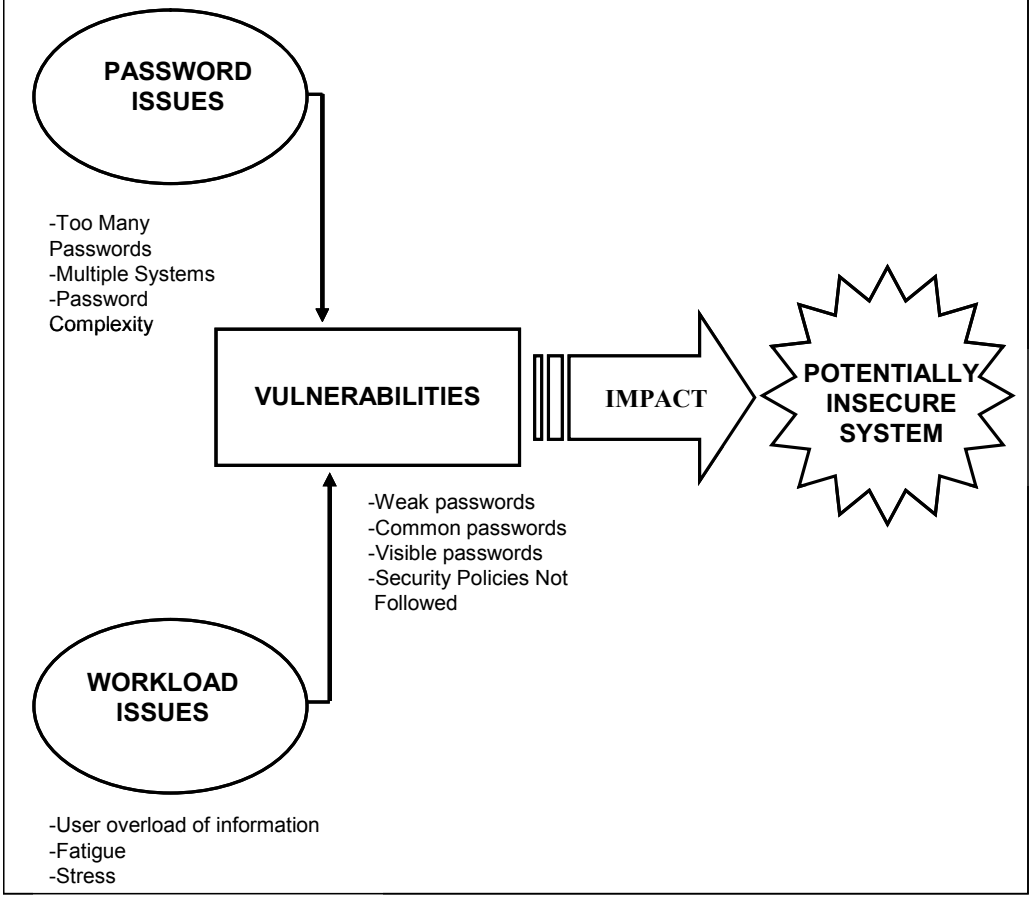

Figure 8. The purpose of the model is to use it in determining the vulnerabilities that password practices are producing on information systems.

explanation for the improvement of individuals recalling stage three passwords the easiest without referring to a piece of paper, may be attributed to a learning curve. Stage two and three passwords were very similar which enabled participants to utilize stage two as training for stage three. Since individuals experienced an increased level of remembrance with less referral to a piece of paper in stage three in comparison to stage two even though there number of characters in stage three passwords, it is reasonable to assume that stage three passwords are probably as easily recalled as stage two (without a learning curve). As expected, the results indicate that a password with meaningful data to the individual is easier to recall even if it contains additional characters. Therefore, the study suggests that the use of mnemonic devices in password development may positively impact information security. An interesting aspect of this experiment is that all three stages of this experiment consisted of passwords that met the stringent guidelines presented in

stage one. This is true since an employee start date meets the fifth requirement of the password guidelines presented in the methodology section since it is not considered to be easily attainable as only the human resource department of an organization houses this data. Overall, individuals were better able to recall the passwords in stage two and three in which the data in the actual passwords could be grouped, or chunked, together as meaningful for the individual. Additionally, the passwords utilized in stage two and three are considered more secure in the eyes of the federal agency's security personnel since the passwords consisted of more characters than the passwords used in stage one.

Implications

The survey and limited federal case study results identified vulnerabilities produced through user actions. The data collected enabled researchers to develop a basic model as displayed in Figure 8 for human factors practitioners and information technology professionals to use in determining the vulnerabilities that password practices are producing on their information systems. This is an initial model and additional research is ongoing to validate and enhance the model. Currently, the model identifies workload concerns that consist of issues faced by humans in their work environment such as an overload of information, fatigue, and stress. Password issues are also addressed in the model to display concerns faced by humans in regards to using passwords such as having too many passwords to remember, too many systems requiring passwords, and too complex of passwords making it difficult for humans to remember their passwords. Together the workload and password issues produce system vulnerabilities such as weak, common, or visible passwords that make it easy for someone not authorized to use a system to gain access. Furthermore, the research also indicates that security policies are not followed adding to the vulnerabilities present. The vulnerabilities then impact the security of a system. Identification of the causes of the vulnerabilities are important as once the causes are known, security personnel can then take the appropriate actions to decrease the vulnerabilities through reducing or eliminating workload and password concerns. The research suggests that vulnerabilities may be reduced though the use of password guidelines that consist of meaningful data for the user which still enable organizations to have strong passwords that hackers would be less likely to breach.

Through simplistic password guideline changes and employee password security training on the use of mnemonic devices in password development, organizations can better guard against human error while maintaining safe practices for user authentication that guard against external threats. As with any research efforts, there are both strengths and limitations of the research. The strength of the survey research was in identifying that those individuals with eight to eleven work or school passwords are at greatest risk for not remembering their passwords at least once a month. This is a significant finding considering the number of individuals that may have eight to eleven passwords given the number of individuals that perform online banking and purchases through various Internet companies. The problem identified as individuals resorting to writing down their passwords is also a significant finding. This very statement confirms the need for human factor password guidelines to assist individuals in the development of passwords that are more easily recalled without the need to refer to paper. The limitation of the survey itself is that more individuals rely heavier on technology yearly and therefore the information collected in the survey becomes outdated. The strength of the experiment is in identifying how even a 12 character length password can be easily recalled when comprised of meaningful information through the use of mnemonic devices. The limitations of the study were in the survey design of the questions as two of the four questions asked could not be part of the analysis due to inconclusive results. The study had the potential to uncover far more information had the survey design contained better questions and had the questions been tested in a preliminary research effort. Due to the limitations of the research, the door is open for future research opportunities.

Future Research

Additional research is underway to determine how passwords influence the human impact in information systems. Due to the limitations in the survey design of the experiment questions and the need to continually survey individuals regarding their password usage as reliance on technology may increase, future research is needed to further validate the original findings. There are also several opportunities for additional research in further analysis of presage variables in regards to information security. Further validation and enhancement to the model previously described in Figure 8 could be altered or expanded based on future surveys and password experiments. Future research will also focus on the link between password and workload issues on human memory limitations. Human factor guidelines for passwords will be created which will enable an individual to choose a strong password which is acceptable to the information technology community yet consist of a password which does not exceed human memory limitations. This research will involve a more in-depth review of the short-term memory literature. If organizations have password guidelines that do not exceed human memory limitations, organizational security policies may be better followed and individuals will no longer have a need to write their passwords on a piece of paper or use the same password for multiple systems. The link between password and workload issues on human memory limitations is that identification of this link between password and workload issues on human memory limitations will enable organizations to better guard against vulnerabilities present in systems and therefore positively contribute to impacting the security of information within systems.

Acknowledgement

Sincere appreciation is given to the US federal government agency for providing subjects and information security experts for the research.

References

Carlson, C. (2004). GAO outlines gaps in security. *eWeek, 21* (12), 29.

Carnegie Mellon Computer Emergency Response Team. (2004) Computer emergency response team statistics. Retrieved May 2004 from http://www.cert.org/stats/cert_stats.html#incidents

Carstens, D. S. & McCauley-Bell, P. (2000). Importance of human error on logistics information security. *Proceedings of the International Society of Logistics Engineer Congress* (Orlando, Florida).

Computer Emergency Response Team (CERT) Coordination Center. (1997). Security of the Internet (New York: The Froehlich/Kent Encyclopedia of Telecommunications), 15, 231-255. Retrieved March 2004 from http://www.cert.org/encycarticle/tocencyc.html#Overview

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45* (1), 67-88.

Golbeck, J. (2002, November). Cognitive load and memory theories. Retrieved March 2004 from http://www.cs.umd.edu/class/fall2002/cmsc838s/tichi/printer/memory.html

Ives, B., Walsh, K., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47* (4), 75-78.

Jaworski, K. (1998). Risk analysis workshop. *ISSA Open Systems Security Conference* (Orlando, Florida).

Kaplan-Leiserson, E. (2003). People and plans: Training's role in homeland and workplace security. *T+D, 57* (9).

Kyas, O. (1997). *Internet security: Risk analysis, strategies and firewalls*. London, England: International Thomson Computer Press.

Lewis, J. (2003). Cyber terror: Missing in action. *Knowledge, Technology & Policy, 16* (2), 34-41.

Loftus, E. F., & Dark, V. J., & Williams, D. (1979). Short-term memory factors in ground controller/pilot communication. *Human Factors, 21*, 169-181.

McCauley-Bell, P., Carstens, D. S., Wilson, T., Grimsley, E., and Malone, L. C. (2000). Understanding human memory limitations and the impact of password authentication practices on information security. *Proceedings of the World Automation Congress* (Maui, Hawaii).

McCauley-Bell, P. & Crumpton-Young, L. (1998). The human factors issues in information security: What are they and do they matter? *Proceedings of the Human Factors and Ergonomics Society 42nd Annual Meeting* (Chicago, Illinois), 439-442.

Merriam-Webster's Collegiate Dictionary 10th ed. (1998).

Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *The Psychological Review, 63,* 81-97.

National Institute of Standards and Technology (NIST). (1992). Computer System Security and Privacy Advisory Board, 1991 Annual Report, 18.

Newell, A., Shaw, J. C., & Simon, H. (1961) *Information Processing Language V Manual*. Edgewood Cliffs, NJ: Prentice-Hall.

Olivia, R. (2003). Will your information survive? *Marketing Management, 12* (1). Business Source Elite Database 10613846.

Perrow, C. (1984). *Normal accidents: Living with high-risk technology*. New York: Basic Books, 3-5, 12, 15-31, 304-305.

Preczewski, S. C., & Fisher, D. L. (1990). The selection of alphanumeric code sequences. *Proceedings of the Human Factors Society 34th Annual Meeting* (Santa Monica, California), 224-228.

Preece, J., Roger, Y., Sharp, H., Benyon, D., Holland, S., & Carey, T. (1994). *Human-Computer Interaction*. Wokingham, England: Addison-Wesley Publishing.

University of Findlay Center for Terrorism Preparedness. (2003). Vulnerability assessment methodology. Retrieved May 2004 from http://seem.findlay.edu/terrorism

U.S. Department of Homeland Security. (2002). Federal information security management act. Retrieved May 2004 from http://www.fedcirc.gov/library/legislation/FISMA.html

Wickens, C. D. (1992). *Engineering psychology and human performance*, 2nd ed. New York: Harper-Collins Publishers. 1-3, 222-231,390,420-423, 424-427.

Wood, C. & Banks, W. (1993). Human error: An overlook but significant information security problem. *Computers & Security, 12*, 51-60.

Appendix
Password Information Security Survey

Instructions: Please answer all 20 questions in the survey. The purpose of this survey is to understand how the number of passwords an individual has to recall impacts the security of a system. Thank you for your participation.

SECTION 1: WORK & SCHOOL PASSWORDS

Examples of work and school passwords are system passwords such as computer passwords, copy machine access codes, voice mail security codes, facility access codes, etc.

1. How many work/school passwords do you have to remember?
   _____

2. Please rate the password difficulty level by writing the number of work/school passwords you have that apply to each below category?

   _____ The password is a word.

   _____ The password is a combination of two or more words.

   _____ The password is made of unfamiliar numbers.

   _____ The password is made of familiar numbers (such as a street address, social security number, birth date, etc.)

   _____ The password is a string of numbers and letters.

   _____ The password is a string of numbers, letters, and symbols.

3. It is likely for a work/school password of mine to be breached? (Please circle one response.)

   Strongly Agree Agree Undecided Disagree Strongly Disagree

4. Do you write down any of your work/school passwords on paper?

   _____ Yes _____ No

5. How often do you change your work/school passwords? (Please circle as many as apply.)

   a). Weekly d). Annually

   b). Monthly e). Never

   c). Quarterly f). Other (please specify) _____

6. How many systems require you to change your work/school passwords? _____

7. If you do change your work/school passwords, do you switch it back to an old password? (Please check one response.)

   _____ Yes _____ No

8. How many times in the last month have you forgotten a work/school password? ____

   Please answer the following two questions if you have forgotten a password in the last month:

How frequently do you use the work/school passwords that were forgotten? (Please specify)

_____

Were the forgotten work/school passwords chosen by you or assigned to you? (Please specify)

_____

9. Please determine the length of your passwords by writing the number of work/school passwords that apply to each below category?

   _____ 1-2 characters _____ 7-8 characters

   _____ 3-4 characters _____ 9 or more characters

   _____ 5-6 characters

SECTION II: PERSONAL PASSWORDS

Examples of personal passwords are system passwords such as computer passwords, ATM pin codes, home security access codes, answering machine codes, etc.

10. How many personal passwords do you have to remember?

    _____

11. Please rate the password difficulty level by writing the number of personal passwords you have that apply to each below category?

    _____ The password is a word.

    _____ The password is a combination of two or more words.

    _____ The password is made of unfamiliar numbers.

    _____ The password is made of familiar numbers (such as a street address, social security number, birth date, etc.)

    _____ The password is a string of numbers and letters.

    _____ The password is a string of numbers, letters, and symbols.

12. It is likely for a personal password of mine to be breached? (Please circle one response.)

    Strongly Agree Agree Undecided Disagree Strongly Disagree

13. Do you write down any of your personal passwords on paper?

    _____ Yes _____ No

14. How often do you change your personal passwords? (Please circle as many as apply.)

    a). Weekly d). Annually

    b). Monthly e). Never

    c). Quarterly f). Other (please specify) _____

15. How many systems require you to change your personal passwords? _____

16. If you do change your personal passwords, do you switch it back to an old password? (Please check one response.)

_____ Yes _____ No

17. How many times in the last month have you forgotten a personal password? ____

    Please answer the following two questions if you have forgotten a password in the last month:

    How frequently do you use the personal passwords that were forgotten? (Please specify)_____

    Were the forgotten personal passwords chosen by you or assigned to you? (Please specify)_____

18. Please determine the length of your passwords by writing the number of personal passwords that apply to each below category?

    _____ 1-2 characters _____ 7-8 characters

    _____ 3-4 characters _____ 9 or more characters

    _____ 5-6 characters

SECTION III: DEMOGRAPHIC INFORMATION

19. What is your gender? (Please circle one response.)

    a). Female b). Male

20. What is the highest-grade you completed? (Please circle one response.)

    a). Grade School d). Bachelor Degree

    b). High School e). Masters Degree

    c). Junior College Graduate f). Doctorate Degree

21. What is your occupation (Please circle as many as apply.)

    a). Administration d). Staff

    b). Student e). Other (Please specify) _____

    c). Faculty

22. How often do you work a week? (Please circle one response.)

    a). Part-time

    b). Full-time

    c). Not employed

23. What is your age category? (Please circle one response.)

    a). 20 or under d). 41-50

    b). 21-30 e). 51-60

    c). 31-40 f). 61 or over

Biographies

NEED DIGITAL PICTURE

Dr. Deborah Carstens has a Ph.D. in Industrial Engineering and B.S. in Business Administration from the University of Central Florida as well as a M.B.A. from the Florida Institute of Technology. She recently began a position as an Assistant Professor of Management Information Systems at the Florida Institute of Technology instructing courses in human-computer interaction, usability, and system design and development. Her research interests are in human error analysis, process and safety optimization, and patient safety. She previously was employed for over ten years at NASA Kennedy Space Center (KSC) where her work included being a principal investigator on human factors research projects, Industrial Engineering for Safety Program Study Manager over research studies conducted on space shuttle activities, and the Process and Human Factors Engineering (P&HFE) Roadmap Manager responsible for the identification of P&HFE technology needs at KSC through to year 2025. During her career at KSC, she was awarded a superior accomplishment award, NASA KSC Graduate Fellowship, and from the Society of Logistics Engineers a Logistics Specialty Award for exceptional achievement in Logistics Management Information Systems.

Pamela McCaulley-Bell is an Associate Professor in the Industrial Engineering and Management Systems Department at the University of Central Florida. She has a Ph.D. in Industrial Engineering, M.S. in Industrial Engineering, and B.S. in Industrial Engineering from the University of Oklahoma. Dr. McCauley-Bell's primary teaching interests at the graduate level are human factors or ergonomics and intelligent systems development. Most recently, she developed an undergraduate course in information security that she taught at the Massachusetts Institute of Technology. She has developed courses in Biomechanics, Ergonomics, Expert Systems and Fuzzy Set Theory. Dr. McCauley-Bell's research interests bring together her background in physical ergonomics, human factors and intelligent system development with the modeling techniques of fuzzy set theory.

Linda C. Malone is a Professor in the Industrial Engineering Department at University of Central Florida. She got her B.S. and M.S. degrees in mathematics and her Ph.D. degree in statistics from Virginia Tech in 1975. She is the coauthor of a statistics text, has authored or coauthored 43 refereed papers, and has a patent pending. She is an associate editor of the Journal of Statistical Computation and Simulation. She has served in various offices in statistical organizations including service on the Board of Directors of the American Statistical Association. She was awarded the honor of Fellow of the American Statistical Association.

Dr. Ronald DeMara received the B.S.E.E. degree from Lehigh University in 1987, the M.S.E.E. degree from the University of Maryland, College Park in 1989, and the Ph.D. degree in Computer Engineering from the University of Southern California in 1992. Since 1993, he has been a full-time faculty at the University of Central Florida and is currently an Associate Professor. He served as Associate Chair and Program Coordinator of the Computer Engineering program, has taught 11 different courses, and developed 4 courses. He has supervised a total of 19 Master students and 4 Ph.D. students. He has completed over 60 publications in conference proceedings, journals and book chapters. He was previously on the technical staff of IBM Federal and Complex Systems Division and a Visiting Research Scientist at NASA Ames Laboratory. He has received the Distinguished Researcher Award and College of Engineering Advisor of the Year award at UCF, and twice received the State of Florida University System's Teaching Initiative award.