WORKING
PAPER

# Toward A Cognitive Analysis of Insider Threats

## An Examination of User Password Choice

JOEL B. PREDD AND ANDREW M. PARKER

WR-688

June 2009




INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

# PREFACE

## ABOUT THIS DOCUMENT

Managing organizational security risks requires understanding how people behave when working in the context of organizational security policies and systems. Experience has shown that systems and policies developed without this understanding are at best ineffective, and at worst can increase the risks to the confidentiality, availability, and integrity of an organization's information. Developing this understanding requires the theories and methods of social science to construct an evidence base that can inform the construction of behaviorally-aware security policies and practically effective security systems.

The paper represents an early step toward developing such an evidence base. The paper applies behavioral decision theory to develop hypotheses about how users choose passwords, and uses those hypotheses to suggest novel ways to help users choose passwords that are both memorable and secure. Behavioral experiments are proposed that could test the hypotheses and evaluate the new approaches. The paper examines a specific choice – user password choice – to highlight the more general importance of an explicitly cognitive perspective on human behavior in security contexts.

This research was funded by the Department of Homeland Security through an Institute for Information Infrastructure Protection (I3P)-sponsored study on Human Behavior, Insider Threat and Awareness. Other publications from this study include:

J. B. Predd, S. L. Pfleeger, J. Hunker and C. Buford, "Insiders Behaving Badly", IEEE Security and Privacy, vol. 6, no. 4, pp. 66-70, Jul/Aug, 2008.

## THE RAND HOMELAND SECURITY PROGRAM

This research was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment (ISE). The mission of RAND Infrastructure, Safety, and Environment is to

improve the development, operation, use, and protection of society's essential physical assets and natural resources and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Homeland Security Program research supports the Department of Homeland Security and other agencies charged with preventing and mitigating the effects of terrorist activity within U.S. borders. Projects address critical infrastructure protection, emergency management, terrorism risk management, border control, first responders and preparedness, domestic threat assessments, domestic intelligence, and workforce and training.

Questions or comments about this report should be sent to the corresponding author, Joel Predd (Joel_Predd@rand.org). Requests for information about the I3P Insider Threat Study can be directed to the project leader, Shari Lawrence Pfleeger (Shari_Pfleeger@rand.org). Information about the Homeland Security Program is available online (http://www.rand.org/ise/security/). Inquiries about homeland security research projects should be sent to the following address:

Andrew Morral, Director
Homeland Security Program, ISE
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5414
Andrew_Morral@rand.org

**CONTENTS**

Preface....iii
About this Document....iii
The RAND Homeland Security Program....iii

Figures....vii

Glossary, List of Symbols, Etc....ix

I. Introduction....1
Outline....3

II. A choice model for password selection....4
Modeling password selection as a choice between strong and weak alternatives....4
Choices have different outcomes....6
This model makes two additional assumptions....8

III. How do users choose, and what can organizations to about it?....11
Hypothesis 1: Users will choose stronger passwords when they perceive a compromise of their account to be more likely or consequential....12
Hypothesis 2: Users will choose stronger passwords when they perceive security risks to be more tangible and less abstract....16
Hypothesis 3: Users will choose stronger passwords when they have chosen stronger passwords in the past....20
Hypothesis 4: Users will choose passwords that are based on the first examples that come to mind....22
Hypothesis 5: The strength of user password choices will vary depending how the choice is framed....25

IV. Conclusion....28
The Analysis Could Be Extended to Other Choices Made By Non-Malicious Insiders....28
Behavioral Experiments Could Support the Development of Organizational Risk Models and Responses....28

Bibliography....30

**FIGURES**

2.1 Conceptualizing password alternatives in terms of strength and memorability .....5

2.2 Salient Classes of Password Alternatives .....6

2.3 Outcomes of Password Choice .....10

## GLOSSARY, LIST OF SYMBOLS, ETC.

| Symbol | Definition |
|---|---|
| **BDT** | **Behavioral decision theory** |

# I. INTRODUCTION

Organizational security policies empower or requires users to make choices – for example, to open an email attachment, to visit a website, to encrypt a sensitive email, to backup data, or to select a new password. Though the nature of the decisions depends in part on the organization, the user's role within the organization, and the organization's security policies, all users face decisions as a result of the policies set forth by their organizations.

A user's decision (malicious or otherwise) to open an email attachment, to choose a weak password, or to send sensitive data without encryption can threaten the confidentiality, integrity and availability of the organization's systems and information. Predd et al. (2008) define an insider as someone with legitimate access to an organization's computers and networks, and an insider threat as an insider's action that puts an organization or its resources at risk. Thus, many user decisions can create insider threats.

Understanding how users make such decisions offers hope for facilitating more security-aware user behavior, for creating more behaviorally-aware security policies and, more generally, for managing the risk of insider threats. Security researchers and professionals are generally aware of how they believe users should decide, but there is a lack of evidence concerning how and why users actually decide when organizational security policy presents a choice. Such an understanding may suggest ways to manage the risk of threatening insider behavior.

Behavioral decision theory (BDT; Kahneman, Slovic, & Tversky, 1982; Fischhoff, 2005) provides empirically robust insights into how and why individuals make decisions, including how individual decision-making differs from models characterizing rational choice. The BDT approach of contrasting a descriptive understanding of how individuals actually decide with theoretical models of how individuals should decide has suggested ways to help individuals make better choices in a variety of contexts, including controlling domestic radon, considering mammography, and improving diet (Bostrom, Fischhoff, & Morgan, 1993; Silverman et

al., 2001; Wisdom, Downs, & Loewenstein, 2008). Pfleeger and Atlee (2006) suggested applying BDT to software-related decisions, including security. More recently, Schneier (2008) discussed applications of BDT to security.

In this paper, to illustrate how BDT can shed light on ways to improve security, we apply BDT to analyze a specific decision usually placed on users by security policy: choosing a password. Choosing a password has been widely observed to involve a trade-off between memorability and security. Passwords that are easy for users to remember are often cryptographically weak (i.e., it is easy for someone to determine the password using computer-supported guesses). On the other hand, strong (i.e., high entropy, random) passwords are often difficult for users to remember. Though an extensive body of research addresses password mechanisms and systems, surprisingly little is known about the psychological mechanisms underlying how and why users choose passwords. To shed light on this question, we analyze user choices in simplified model that frames password selection as a choice between cryptographically weaker, easier-to-remember passwords and stronger, harder-to-remember alternatives. This framing proves useful, because it highlights the outcomes that must be weighed when the user is trying to make a "reasoned" choice, and allows us to leverage findings from BDT to develop hypotheses about how and why users choose passwords. The hypotheses suggest unexplored response mechanisms that may productively affect user decision making, and we propose behavioral experiments that could test the hypotheses and evaluate the responses.

This paper's use of this password selection example serves three broader objectives:

1. To frame a classic insider security problem as an individual choice. In doing so, we illustrate how other insider threats can be similarly characterized.
2. To demonstrate how BDT suggests both behavioral explanations for an insider threat and novel response mechanisms. We expect that similar insights could be leveraged to address other insider behavior.

3. To propose empirical studies, including behavioral experiments that could test the theory and evaluate different responses. The proposed experiments respond to the increasingly voiced need to understand human behavior in security contexts (e.g., Karat et al., 2005; Bishop et al, 2008; Wybourne et al., 2009)

Our analysis focuses on cognitive factors shaping user decision-making, and thereby complements research that considers the relationship between security and usability (Cranor and Garfinkel, 2005). Sasse et al. (2001), to cite one example, employ the principles of human-computer interaction to identify contextual factors that affect user password behavior, including the conflict between enabling security tasks (like choosing a password) and necessary job tasks, the number of different passwords a user must remember, the frequency with which the organization requires a password to be reset, the individual's peer group members' perception of security, and a broader organizational security culture. These findings are demonstrably important, but in many organizations, security policy still requires users to choose passwords. Therefore, an explicitly cognitive perspective may be necessary to explain what context alone cannot. Our focus on user choices is what distinguishes this research from and makes it complementary to usability research on password practices.

**OUTLINE**

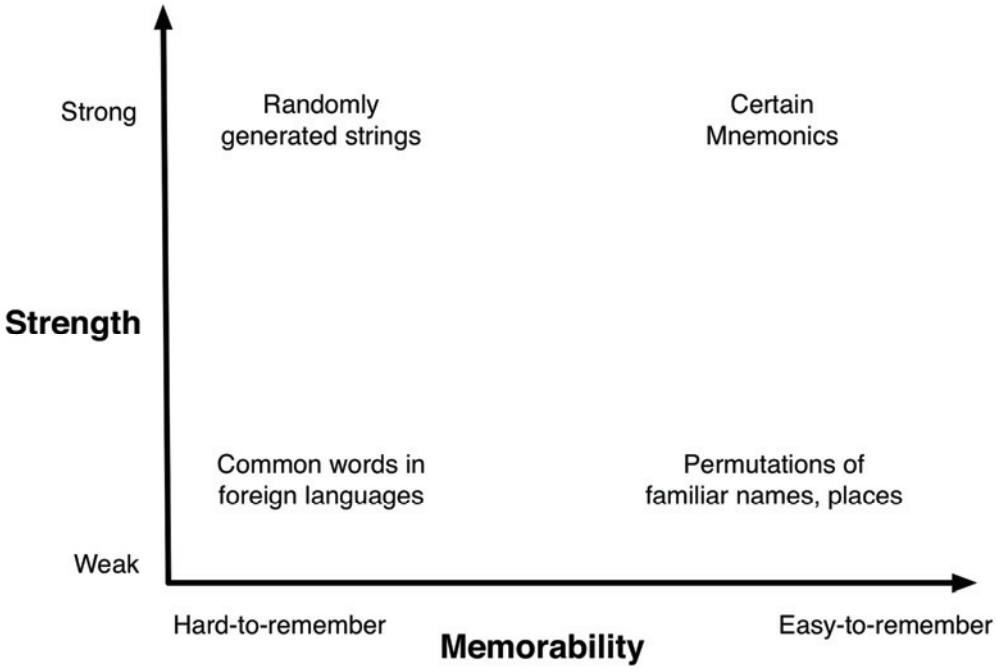
The remainder of this paper is organized as follows. In Section II, we describe a simple model that poses password selection as a choice. In Section III, we apply normative and behavioral decision theories to develop hypotheses about how and why users actually choose passwords. For each hypothesis, we discuss general findings from the behavioral decision-making literature that motivate the hypothesis, describe response options that may be productive if the hypothesis is supported, and sketch empirical studies that could test the hypothesis or evaluate responses. Finally, in Section IV, we summarize the main conclusions and discuss generalizations to other insider threats. Related work is discussed throughout the paper.

## II. A CHOICE MODEL FOR PASSWORD SELECTION

### MODELING PASSWORD SELECTION AS A CHOICE BETWEEN STRONG AND WEAK ALTERNATIVES

Users who are empowered to choose their own passwords must select from a large number of possible options. Each alternative password has a variety of attributes that in theory a user could consider when choosing. We conceptualize alternative passwords in two dimensions, with a strength dimension varying between cryptographically weak and strong and a memorability dimension varying between easy-to-remember and hard-to-remember. Figure 2.1 illustrates this representation of passwords, and positions four types of passwords in the corners of the two-dimensional space: a randomly-generated string is an example of a strong and hard-to-remember password, and simple transformations of a user's first name might be characterized as weak and easy-to remember. A common word in an unknown foreign language might constitute a hard-to-remember, weak password, and some mnemonic passwords can be both strong and memorable as suggested by Yan et al. (2004).

**Figure 2.1 Conceptualizing password alternatives in terms of strength and memorability**




In theory, a user chooses among all passwords in this space. In practice, it seems reasonable to assume that most individuals choose among a subset for which strength and memorability are negatively correlated – especially in the absence of systems or policies that facilitate choices that are both memorable and strong.[1] In Figure 2.2, this choice set is shaded gray.

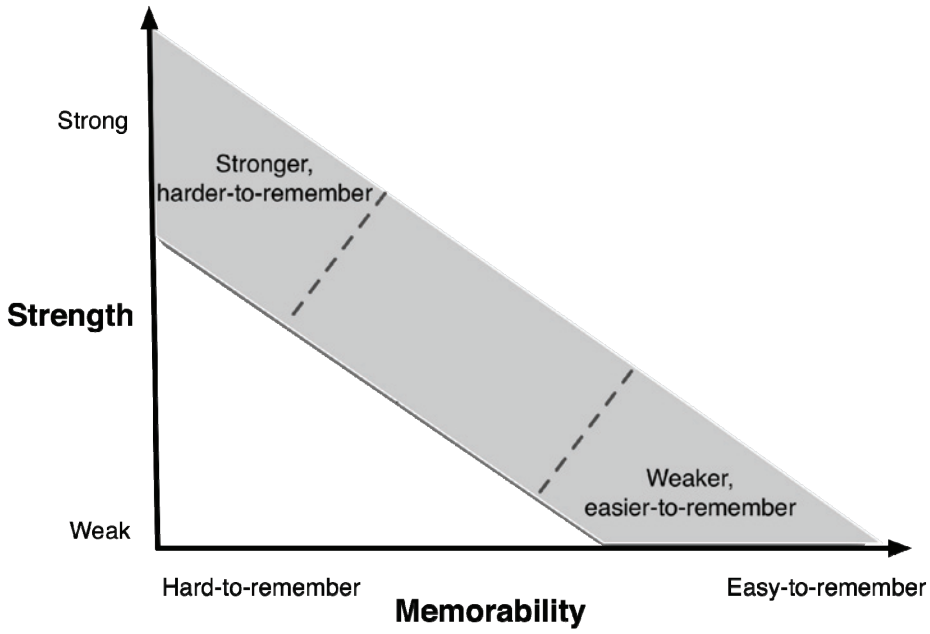
The extremes of this choice set – stronger, harder-to-remember passwords and weaker, easier-to-remember passwords – represent exemplar

---

[1] Adams and Sasse (1999) suggest that the trade-off between memorability and security is false or that it is artificially introduced by password mechanisms that are poorly integrated into the organizational context. Furthering the false choice argument, Yan et al. (2004) provide empirical evidence that some mnemonic passwords can be both memorable and strong. These insights notwithstanding, memorability and security may be *perceived* as negatively correlated for users selecting their own passwords. This is suggested by the 10% of users reported in an experiment conducted by Yan et al. to be non-compliant with password policies despite targeted password selection instructions.

password classes that may be particularly salient to the user. Users may readily construct easy-to-remember permutations of familiar names or places; and highly impersonal, relatively random passwords may be understood by users to be strong even if they require effort to generate and remember. The two password classes are denoted in Figure 2.2.

**Figure 2.2 Salient Classes of Password Alternatives**




The salience of these extremes motivates a choice model that conceives user password selection as a choice between passwords in the two classes. Clearly, a binary choice model is limited descriptively since users actually choose among all possible passwords as discussed above. However, we posit that the abstraction is sufficient to generate useful insights about user behavior. Thus, we assume that when selecting a password, a user chooses passwords in one of two classes corresponding to relatively stronger, harder-to-remember passwords and weaker, easier-to-remember passwords.

**CHOICES HAVE DIFFERENT OUTCOMES**

This choice model requires defining the outcomes of the choice. As is obvious from our formulation, two focal consequences of password choices are security and memorability. A user account made vulnerable

due to a weak password choice is at risk of being compromised by malicious attackers and a compromised account exposes the system and information that the organization sought to protect with the password. Hard-to-remember passwords may frustrate users and limit their productivity by requiring them to spend time recalling their password or to work with help desks to reset their accounts.[2]

However, there are other outcomes beyond these most salient ones. By virtue of being a member (e.g., an employee) of the organization, the users may suffer losses (e.g., to their job, professional reputation,[3] etc.) if the organization suffers due to a compromised account. Similarly, the organization may suffer productivity (or profit) losses indirectly through productivity losses experienced by the user. Relatedly, the user may have personal information stored on the organization's systems, and thus, a compromised account may put the user's personal information at risk. Finally, Ives et al. (2004) highlights that a consequence of reusing weak passwords is that a compromise of one account can put other accounts (e.g., individual personal accounts) at risk.[4]

In principle each of the aforementioned consequences could occur for passwords in both classes, since logically the user's password

---

[2] Extensive research on human memory exists (e.g., Miller, 1956), establishing some measure of the difficulty of remembering different types of passwords. In the context of password selection in particular, Yan et al. (2001) conducted an experiment and found that users perceived random passwords to be harder to remember than both self-selected and mnemonic passwords, and that a written record of random passwords was kept longer on average than written records of self-selected passwords. Rosencrance (2003) reports that 51% of all surveyed users require IT help to access applications because they forget passwords. Survey results reported in Sasse et al.(2001) suggest that passwords are often partially remembered and confused with other passwords.

[3] Sasse et al. (2001) report a user for which password choice was a matter of professional reputation.

[4] Many researchers have noted that another consequence of choosing strong passwords is that users may write the passwords down on an easily-compromised piece of paper. We choose to interpret writing passwords down as a user solution or response, rather than as a consequence in itself. We discuss this response in more detail in Section III.

choice affects only the likelihood of the outcomes -- not their eventuality or perceived value. In particular, a user may forget even a weaker, easier-to-remember password, and a brute force password cracker could luckily discover a randomly-generated password.[5] A user may be merely more likely to forget a strong password than a weak one, and by definition, the likelihood of compromising a user account via password cracking is greater for a weak password. Further, the outcomes ostensibly have the same value if they occur (regardless of the choice). Thus, a user's decision affects the likelihood of the outcomes occurring, not their eventuality or value.

Figure 2.3 offers a depiction of the different outcomes in our password choice model. Each rectangle represents a different possible outcome (i.e., consequence) of password choice. Arrows link those outcomes that are dependent; conceptually, the outcome at the beginning of an arrow must occur before the outcome at the end of the arrow can occur. Shaded outcomes are more likely given a stronger, harder-to-remember password choice than a weaker, easier-to-remember password choice, but all outcomes are possible for both choice alternatives.

**THIS MODEL MAKES TWO ADDITIONAL ASSUMPTIONS**

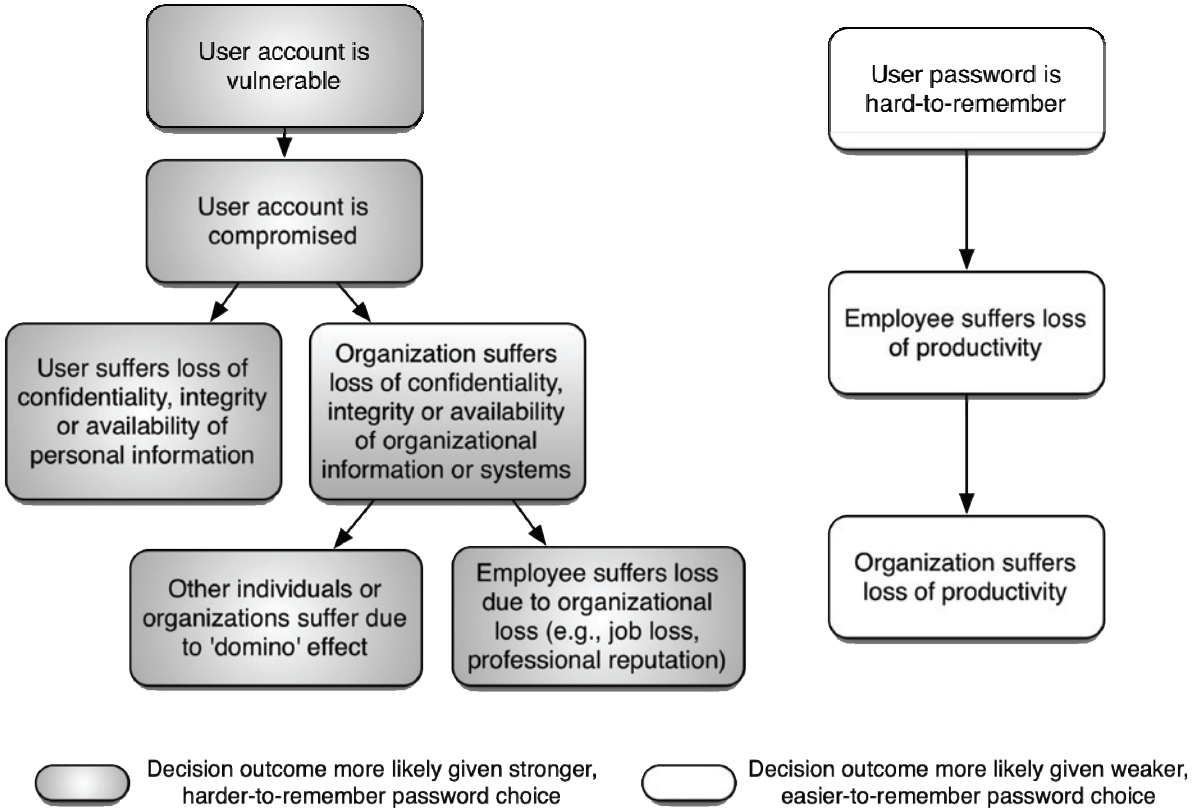
Beyond the binary choice abstraction, this model makes two additional assumptions, and it is important to consider the extent to which these assumptions affect the foregoing analysis. First, the model assumes that the user can distinguish stronger from weaker passwords. Crucially, the model does not assume a particular definition of password strength, and our analysis is insensitive to whatever formalism we might apply to discriminate between the two types. For example, the insights of BDT could be leveraged if we were to define a strong password mathematically in terms of entropy and if we defined strength in terms of adherence to criteria specified by a given security policy (e.g., "a

[5] In the experiments discussed in Yan et al. (2004), some users with self-selected passwords required password resets, and 8% of random passwords were cracked using a permuted dictionary attack.

strong password has eight characters, including at least one digit or punctuation mark"). This assumption limits the analysis to situations where the user has been provided with and understands instructions about how the organizational password policy defines strong passwords.

Relatedly, the model assumes the users are aware of the choice and have the resources to choose. Usability research employing the principles of human-computer interaction has identified a number of contextual effects that may distract the users from or limit their engagement in decision-making. As cited in the Introduction, Sasse et al. (2001) identified a number of factors including conflicting task demands -- the incongruence resulting from the fact that password selection and management are keeping users from doing their "real" job tasks -- as explaining why some users engage in risky behavior, such as choosing weak passwords and sharing passwords. This assumption limits the analysis to situations where the choice is real and the user is engaged in decision-making.

**Figure 2.3 Outcomes of Password Choice**



## III. HOW DO USERS CHOOSE, AND WHAT CAN ORGANIZATIONS TO ABOUT IT?

There is considerable evidence that individuals choose weak passwords and that password reuse is common. For example, Brown et al. (2004) report on a study that categorized students' passwords according to the information that was used to construct the password. The study found that 15% of passwords chosen by college students were constructed using their own names and that 45% of students use their names in some way to derive their passwords. 78% of all passwords referred either to the individual, their relatives or their pets, and 75% of passwords referenced the personally identifiable entity without any modification or transformation. Further, Brown et al. (2004) report that college students have on average 8.18 uses ("systems") that require passwords, with 1.84 uses per unique password. In a related study, Gaw and Felten (2006) report similar but slightly higher password reuse rates. Florencio and Herley (2007) report similar conclusions in a much larger study of web password habits.

Why are weak password choices so pervasive? And, what can be done to facilitate user choices that more fairly balance security and memorability?

In this section, we apply normative (i.e., theoretically rational) and descriptive (i.e., behaviorally accurate) decision theories to our model to develop cognitive hypotheses about user password choice. For each hypothesis, we first discuss motivating findings from BDT and then discuss what response options may be productive if the hypothesis were true. Though some of the hypotheses and response options are intuitively appealing, there is in general a lack of empirical evidence establishing causal relationships between user passwords choices and the hypothesized moderating factors. Toward developing such an evidence base, we discuss ways one might empirically test each hypothesis or evaluate the proposed responses through behavioral experiments. Absent other motivating forces, such an evidence base may be needed before it would be advisable for organizations to make significant investments in the proposed responses.

**HYPOTHESIS 1: USERS WILL CHOOSE STRONGER PASSWORDS WHEN THEY PERCEIVE A COMPROMISE OF THEIR ACCOUNT TO BE MORE LIKELY OR CONSEQUENTIAL.**

**Theory**

This hypothesis reflects a basic assumption of normative decision theories, and as we will describe below, can be seen as the basis for many currently practiced or proposed responses. Generally speaking, normative models for rational choice presume that decisions depend on the decision-maker's perceived value – or utility – of the different outcomes (e.g., those in 2.3), as well as the perceived likelihood of those outcomes given a particular choice. And despite some systematic departures (presented in the sections below), people do tend to choose options for which they perceive greater likelihood of achieving greater value for themselves and others they care about (Kahneman et al, 1987). In all cases, a "rational" individual, applying the principle of expected utility maximization, chooses the alternative that provides in the greatest expected utility – determined by multiplying the perceived value and likelihood of each outcome and summing across all outcomes associated with the alternative.

In the context of password selection, both the value and likelihood of the different outcomes are dependent on the user's context. For example, the value of a strong password may depend on the value of the information it protects; the value of enhancing productivity with an easy-to-remember password depends may depend on the user's role within the organization. Similarly, the relative likelihood of these outcomes may depend on the nature of the organization, role of the individual, the importance of the information, and other factors.

Preferences for different password choices may be understood in such normative terms. For example, the security community's preference for strong passwords may result from the expected cost of a compromised account's sufficiently outweighing the expected cost of having to remember a hard password. However, individuals may perceive consequences differently from the security community (or the organization), and a worst-case scenario (i.e., one that heavily emphasizes the risk of compromise for the organization) may ignore differences across individual decisionmakers and contexts. For some

individuals and organizations (e.g., a cashier at a small family grocery), information protected by a password may seem so inconsequential or an attack may seem so unlikely that choosing a weak password is reasonable. For other individuals and organizations (e.g., people trusted with sensitive information), the expected utility comparison supports conventional security wisdom about the importance of strong passwords. Even within a given context, perceptions may differ across individuals and organizations. In theory, variations in user perceptions of outcome values and likelihoods may predict the variation in user choices.

This theoretical discussion motivates the hypothesis that users will choose stronger passwords when they perceive a compromise of their account to be more likely or more consequential. Consistent with this hypothesis, Adams and Sasse found in interviews and surveys that users do a better job of implementing and following security policies when they understand the goals of the policies and the security threats faced by the organization. Gaw & Felten (2006) report survey data suggesting that some users are more likely to avoid reusing personal passwords for accounts protecting financial data. In a large survey of personal web passwords, Florencio and Herley (2007) show clear differences between the bit strength of passwords chosen for the NY Times website and financial sites PayPal and Fidelity. We are unaware of any studies that associate measures of users' perceived likelihood or value with objective measures of password strength or memorability.

**Potential Responses**

Hypothesis 1 suggests several ways that organizations can affect user password choices, and in fact many currently proposed responses rely on this hypothesis. First, the hypothesis reflects classic responses of changing the objective or actual consequences and likelihoods of memorability outcomes. For example, Topkara et al. (2007) describe a method for helping users generate secure and memorable passwords through mnemonics. Mnemonic passwords leave the basic password mechanism unchanged, and may affect decision making by reducing the memorability cost of choosing a strong password. Password mechanisms

that are based on easily-recalled personal facts, opinions, or interests,(Zviran and Haga, 1990), on word associations (Zviran and Haga, 1993) and on pass sentences (Spector and Ginzberg, 1994) similarly reduce the likelihood of forgetting or having to reset strong passwords, while relying on a slightly modified password system. Proactive password checking (e.g., Spafford, 1991; Yan, 2000; Vu et al., 2008) involves imposing restrictions on the passwords users can choose, with the idea of constraining the strength of available choices. Writing down passwords has the effect of eliminating memorability costs altogether, though doing so introduces a new risk associated with the easily compromised piece of paper. Biometric methods and schemes that employ pictures as passwords (Suo et al., 2005; De Angeli et al., 2005) restructure the decision entirely in serving as an alternative to password authentication systems.

Second, the hypothesis suggests trying to shape users' perception of outcome values or likelihoods, reflecting the sentiment, "if only users appreciated the 'true' value and likelihood of a compromised account, they would put greater effort into constructing stronger passwords." Efforts to educate users about the costs of weak passwords and about techniques for choosing strong and memorable passwords fit in this category. Notably, training is not sufficient to change user behavior completely: Yan et al. (2004) provide evidence that compliance is greater with training, but that 10% of users choose weak passwords despite instructions. Third, Hypothesis 1 suggests introducing additional incentives (or disincentives) to encourage (discourage) individuals to choose particular alternatives and avoid others. Normatively, this approach affects decision-making by adding weight (in the form of a valued consequence) to whatever choice is favored by the incentive.[6] In the context of password selection, the idea of adding outcomes is consistent with studies by Sasse et al. (2001) that suggest that bad password-related behavior is in part due to users' not being

[6] As suggested by the framing hypothesis discussed below, it may be practically important how an incentive is framed – for example, as a reward or as avoidance of a punishment.

held accountable for bad practices. Given that passwords are meant to be kept secret, incentive structures that require others in the organization to assess password strength may raise their own issues. However, users could be rewarded based on proxies such as the measured strength of their password, or penalized if their account is compromised via a password breach. Proactive password checking systems (e.g., Spafford, 1991; Yan 2000) that check the strength of passwords in near real-time may facilitate incentives by providing immediate feedback (and hence learning) regarding the likelihood of an account's being compromised with a chosen password.[7]

Related to accountability, a somewhat controversial intervention would be to disclose the hardness of users' passwords to co-workers, in addition to the number of password resets they require over the course of a particular year. Publicizing this information might introduce choice outcomes associated with peer pressure, to the extent that users may want to keep such metrics within socially acceptable bounds. Naturally, this approach could have unintended consequences in terms of organizational culture, etc., and would need to be explored.

**Testing the Hypothesis**

Despite recent attempts to quantify password practices, it is important to note that Hypothesis 1 and its potential responses depend on psychological mechanisms (formation of perceived value and likelihood) that have rarely been evaluated empirically in the context of insider threat or password choice. In contrast, the empirical focus to date has tended to be on behavioral outcomes (e.g., password strength and memorability, reuse, recall times, retry attempts, etc.), presuming the psychological mechanisms.[8] One exception is Sasse and colleagues

---

[7] And to make matters worse, surveys by Sasse et al. (2001) suggest that users are woefully unaware of consequences of security behavior.

[8] Vu et al. (2007) studied the affect of different password restrictions on time and number of attempts to create passwords, in addition to login time and memorability.

(Adams & Sasse, 1999; Sasse, Brostoff, & Weirich, 2001), who interviewed users regarding their perceptions and attitudes towards passwords and security risks. Building on these efforts, a potentially fruitful empirical strategy would start with a descriptive analysis, explicitly characterizing password choice as a decision, including mapping out (a) how users psychologically structure the password choice problem (e.g., what they perceive as potential options and consequences), (b) their perceived values and likelihoods of different consequences, given specific choices, and (c) how this differs across naturally-occurring contextual variables. Once this groundwork has been laid, follow-on experiments could test whether (a) through (c) are affected by the application of the response strategies described above. The basic mapping exercise (and the measurement strategy that can derive from it) will provide greater insight into the strength and weaknesses of different response strategies.

**HYPOTHESIS 2: USERS WILL CHOOSE STRONGER PASSWORDS WHEN THEY PERCEIVE SECURITY RISKS TO BE MORE TANGIBLE AND LESS ABSTRACT.**

**Theory**

People tend to perceive some consequences more acutely than others, and often discount consequences to abstract stakeholders and abstract outcomes. Jenni and Loewenstein (1997) demonstrate one such phenomenon, labeled the "identifiable victim effect," whereby "society is willing to spend far more money to save the lives of identifiable victims than to save statistical victims" (p. 236). More generally, as stakeholders or consequences become less identifiable, immediate, and certain, they tend to hold less sway in decisions. Some of this may be driven by perceived abstractness in likelihood. Outcomes that happen with certainty are overweighed, relative to those that happen probabilistically (Kahneman & Tversky, 1979), prospects with well-understood likelihoods are preferred over those with ambiguous or undefined likelihoods (Ellsberg, 1961), and outcomes that are more easily imagined or recalled feel more likely (and

are hence given greater weight) than those that are less vivid (Tversky & Kahneman, 1974; Kahneman & Tversky, 1982). Discounting abstractions may also happen because of how consequences are valued, with immediacy and concreteness playing a key role. Outcomes that happen immediately are preferred to those that happen with a delay (Loewenstein & Elster, 1992; Roelofsma & Keren, 1995) and objects that are currently owned are valued more highly than those that are unowned (Thaler, 1980).

From the perspective of a user choosing a password, the relative certainty and ease of remembering the password may be a more salient consequence than the distant chance of the password's being attacked with some probability at some future time. Indeed, the user will be required to use the password immediately, and will certainly bear the cognitive burden and productivity losses if effort is required to recall or reset a hard-to-remember password. Moreover, as suggested by Figure 2.3, much of the security risk is experienced indirectly by the user through the organization, and productivity losses are experienced by the organization indirectly through the user.[9] Thus, the user experiences the memorability consequences more proximally than the security outcomes.

This discussion suggests the hypothesis that users will choose stronger passwords when they perceive security risks to be more tangible and less abstract. Consistent with this hypothesis, Adams and Sasse (1999) assessed a lack of experience with security breaches to be a reason for decreased user's perceived risk. Further, they note that commercially-sensitive information was seen as less sensitive than personal information. This is also consistent with Hypothesis 2, to the extent that personal information is less abstract and more tangible for the average user than commercially-sensitive information. Once again,

---

[9] Decisions that require an individual to trade-off outcomes to self and outcomes to others (e.g., the organization) have been characterized as *ethical dilemmas*. See Loewenstien (1996) for a discussion of BDT applied to ethical decision-making.

we are unaware of any causal evidence to link risk tangibility with measures of strength or memorability.

**Potential Responses**

If true, this hypothesis suggests response options that aim to make security risks more tangible and less abstract to users who choose passwords. For example, publicizing password breaches within the organization -- or at other organizations -- to all users could help users perceive security risks as more tangible. Additionally, providing a vivid account (e.g., a narrative describing the user whose password was breached, their responsibilities within the organization, etc.) could promote a more tangible appreciation for security risks than users receive through more abstract references to "security." A related approach would be to have an internal website that publicized known attempts to attack the organization's networks. If viewed by users, such a site could help users perceive security risks as more tangible – a process that could be incorporated into training or into the password changing mechanism.

The opposite approach – increasing the abstraction and decreasing the tangibility of choice outcomes associated with password memorability – may prove more controversial. For example, users could be asked to choose passwords for their anonymous co-workers, rather than for themselves. In such a scenario, the user choosing passwords for their anonymous co-worker would still appreciate the value of a memorable password, even though he or she would not experience the memorability costs directly. In the opposite way that an abstract appreciation for security may lead users to discount security risks, distancing the user from memorability outcomes may make them discount those costs so that they make fairer security-memorability trade-offs. (To avoid the obvious outcome of having employees who know other employees' passwords, one could require the user to edit a fixed number of characters from the one chosen by their anonymous colleague.)

**Testing the Hypothesis**

Simple empirical studies could be devised to test Hypothesis 2. For example, one could compare the strength of passwords chosen by users more likely to hear about password attacks (e.g., members of security or IT departments) with the strength of passwords for other users (e.g., administrative or clerical staff). If the password strength of aware users is stronger than for unaware users, this would lend some support to the hypothesis. To be conclusive, one would need to experimentally manipulate this exposure. At a minimum, one should control for individual differences (e.g., familiarity with security risks, comfort with technology, education, etc.) that could also explain the variation between the groups. Another variable of interest may be the time since the individual's past exposure to a security breach.

Another approach would be to examine how the strength of the password choices varies with individuals' mental models of security risks (e.g., Camp and Liu, 2009; Farahmand et al., 2008). For example, computer security risks may necessarily be more abstract (e.g., the users may feel as though they understand them less than other risks), and there may be danger in users' superimposing a simplistic and concrete (and possibly inaccurate) alternate mental model (e.g., it's like locking your front door). The hypothesis would be supported if users with mental models similar to an expert model chose stronger passwords than users who adopted alternate, simpler models. Controlling for individual differences would also be necessary for this approach.

Simple experiments and quasi-experiments could be also devised to test the effect of the proposed responses. One could measure the strength of user passwords before and after an effort to publicize security incidents. An opportunistic experimental design would measure the strength of passwords today, and then after a major cyber-security incident that gains the attention of the national media. In both cases, Hypothesis 2 would be supported if the strength of passwords after the change were significantly stronger than the strength of passwords before the change.

Finally, similar experiments could be conducted to assess the affect on chosen password strength when users choose for co-workers

instead of themselves. Each user could first be asked to reset his or her own password, and then be asked to choose a password for an anonymous co-worker. The strength of both choices could be compared, and the hypothesis would be supported if the strength were greater when individuals chose a password for others.

**HYPOTHESIS 3: USERS WILL CHOOSE STRONGER PASSWORDS WHEN THEY HAVE CHOSEN STRONGER PASSWORDS IN THE PAST.**

**Theory**

Past decisions act as a powerful guide for people making new decisions. In particular, people have a tendency to judge options relative to their current situation. For example, Kahneman and Tversky (1979) pointed out that people often frame predicted consequences as gains or losses relative to their current state. Furthermore, because people quickly adapt to the consequences of those decisions (Thaler, 1980), and when making a sequence of decisions, they can arrive over time at choices that they themselves may not favor, given a larger perspective. For example, by slowly incrementing the payoffs and odds in a series of choices between simple gambles (e.g., 11/24 chance of winning $4 vs. 10/24 chance of winning $4.25), Tversky (1969) was able to get people to choose progressively lower-probability gambles. Eventually, people ended up choosing options that were actually less preferred when compared directly to their starting point (i.e., 7/24 chance of $5 lost out to 11/24 chance of $4). This study suggests that in sequential choices people will tend to focus on relative changes in their well-being rather than on an absolute state. This tendency is sometimes called a recent decision bias.

Users are perhaps most frequently asked to choose a password in the context of a password change or reset. In those contexts, the recent decision bias suggests that users may judge the memorability or security of their new password relative to their current password. Regardless of strength, a new password will be less memorable than an old, well-used password. Moreover, the user's current password may provide a reference point for password strength if he or she is unaware of successful cracking attempts on it. Thus, a user subject to a recent decision bias

may be set up to favor weaker, easier-to-remember passwords when asked to reset an existing password that is normatively weak.

**Potential Responses**

This hypothesis suggests giving users opportunities to practice choosing passwords. For example, an organization could develop games or exercises around artificial scenarios in which users are rewarded for choosing strong and memorable passwords. The hope would be that when users actually chose passwords, they would recall passwords chosen in the game and use those "recent decisions" as examples from which to judge strength and memorability. Such an exercise would augment more traditional training by giving users actual practice (and feedback) in choosing passwords. Naturally, one would have to advise users not to reuse passwords chosen during such a game for their actual passwords, especially if those choices are made public.

**Testing the Hypothesis**

An initial approach to testing Hypothesis 3 would be to compare the strength of users' passwords before and after a password change. A positive correlation between the strength of users' password choices at both times would be consistent with the hypothesis.[10] There would be greater support for the hypothesis if there were a positive correlation even when controlling for individual dispositional factors like attitude or familiarity with security.

A similar approach would be to compare the strength and memorability of user passwords across different personal and work-related scenarios. Through a carefully designed survey instrument, one could acquire qualitative, self-assessments of users' passwords for personal banking and email systems, for social networking services, for

---

[10] Adams and Sasse (1999) assert that "users required to change their passwords frequently produce less secure password content" (p. 44), supporting a contextual effect associated with the frequency of password reset requests. Though related, this research does not consider the historical strength of user password choices.

inconsequential bulletin board services, and for organization "work" systems. Correlations in the strength of passwords chosen by an individual in different scenarios would be consistent with Hypothesis 3. Once again, this test would require controlling for individual differences that could provide alternative explanations for the findings.

Finally, it would be straightforward to develop a controlled experiment to test the effect of the proposed games or exercises that allowed users to practice choosing passwords. A set of users could be randomly selected to participate in a game or sequence of games. At the next password change following the exercise, the strength of passwords chosen by users who participated could be compared to the strength of passwords chosen by users who didn't participate.

**HYPOTHESIS 4: USERS WILL CHOOSE PASSWORDS THAT ARE BASED ON THE FIRST EXAMPLES THAT COME TO MIND.**

**Theory**

The tendency of current decisions to be influenced by recent decisions is exacerbated by a general tendency of people to tend to stick with the status quo, or "doing nothing or maintaining one's current or previous decision" (Samuelson & Zeckhauser, 1988, p. 7). This is exemplified by the greater uptake of organ donation in countries where one has to opt-out of the program (hence, making it the status quo), rather than having to explicitly opt-in (e.g., Abadie & Gay, 2006).[11] This bias toward the status quo is further increased as the number of options available to the decision maker increases (Samuelson & Zeckhauser, 1988). As noted by Ritov and Baron (1992), the tendency may reflect both comfort with one's current position and reluctance to do anything about changing it.

---

[11] Similar effects have been shown with health plans and retirement planning (Samuelson & Zeckhauser, 1988; Choi et al., 2001).

As discussed in Section II, a user's actual choice is among all possible passwords, a complex decision by measure of the number of alternatives the decision-maker can consider. For a user subject to the default bias, a natural and efficient way of choosing in this situation is to select the password that first comes to mind (or simple variations thereof). Simple variations of the user's existing password or of personal passwords constitute a natural status quo that individuals may be inclined to accept to avoid the complexity of choosing an alternative.

**Potential Responses**

Many password systems have the capability to disallow users from reusing old passwords or simple variations thereof. Though disallowing password reuse eliminates a natural default choice, it would not avoid the recent decision bias discussed previously; users may still judge the memorability and security relative to old passwords. More importantly, there may be more productive, less defensive ways to leverage this people's tendency to select defaults.

For example, one can envision a password changing system that allowed the user first to choose one of (say) ten randomly generated passwords and then to edit the chosen one in whatever way the user thought would improve its memorability. (One can easily imagine more sophisticated systems that only allowed a fixed number of user edits, or edits of a particular type.) Whereas requiring users to construct a password from scratch may encourage users to reuse easy-to-remember passwords (the natural default), this approach may help avoid bad security-memorability trade-offs by providing alternate defaults (a password picked from a list), simultaneously leveraging people's tendency to stick with defaults.[12]

---

[12] Forget et al. (2008) apply principles of Persuasive Technology (Forget et al., 2007) to propose a related idea of improving password strength by placing randomly selected characters in randomly selected positions in a user's chosen password. This approach still requires the user to choose an initial password, and interestingly, experiments revealed circumstances in which users chose weaker initial passwords to

**Testing the Hypothesis**

To the extent that a user's previously used or current passwords are likely the first to come to mind, the pervasiveness of password reuse stands in support of this hypothesis. Adams and Sasse (1999) report that 50% of their survey respondents use common elements across passwords. As cited above, Brown et al. (2004) report that college students have on average 8.18 uses ("systems") that require passwords, with 1.84 uses per unique password.

A controlled experiment could test the effect that providing editable, cryptographically-strong default passwords has on user password choices. Users could be divided into two groups. Users in the control group would choose their passwords according to the organization's existing policies. Users in the experimental condition would pick their favorite from among a set of 10 randomly generated exemplar passwords and then edit the choice to improve memorability. Password strength and memorability measures could be used to compare the strength of users' choices in each group. We would hypothesize that the strength of passwords chosen by users in the experimental condition would be significantly stronger and that memorability would be comparable.

Incidentally, we are unaware of any evidence about the causal relationship between disallowing transformation of old passwords (a classic response) and password strength; similar behavioral experiments could be conducted to test their effectiveness.

---

circumvent the memorability costs associated with randomized modifications. Our idea leverages the default bias by allowing users to edit system-generated strong defaults rather than having the system modify a weak user choice.

**HYPOTHESIS 5: THE STRENGTH OF USER PASSWORD CHOICES WILL VARY DEPENDING HOW THE CHOICE IS FRAMED.**

**Theory**

People's choices often depend on how the decision and its consequences are characterized. This influence is particularly troubling when the differences in characterization are objectively irrelevant. The now classic Asian Disease Problem is an example of such "framing effects:"

> *"Imagine that the U.S. is preparing for the outbreak of an unusual Asian disease, which is expected to kill 600 people. Two alternative programs to combat the disease have been proposed. Assume that the exact scientific estimate of the consequences of the programs are as follows:*
>
> *If Program A is adopted, 200 people will be saved.*
>
> *If Program B is adopted, there is a 1/3 probability that 600 people will be saved, and 2/3 probability that no people will be saved.*
>
> *Which of the two programs would you favor?" (Tversky & Kahneman, 1981, p. 453)"*

In this condition, 72% of respondents chose Program A and 28% chose Program B. A second group saw the exact same options, but phrased in terms of people dying (e.g., in Program B, there is a 1/3 probability to nobody will die, and a 2/3 probability that 600 people will die). In this second condition, only 22% chose Program A and 78% chose Program B.

Levin and Gaeth (1988) demonstrated an even more basic form of framing when they presented people with ground beef that was labeled either as 80% lean or 20% fat. The lean framing was judged by study participants as substantially lower in quality than the fatty framing.

Both of these examples contrast positive and negative framing of attributes or consequences (Levin, Schneider, & Gaeth, 1998), and demonstrate the general findings that (a) people tend to react more favorably when options are describe positively than when they are described negatively, (b) losses are typically given more weight than corresponding gains, and (c) people tend to be risk averse for gains and risk seeking for losses (Kahneman & Tversky, 1979).

Given our model of password choice, there are in fact several equivalent ways password choice can be framed. It can be framed (a) in terms of password strength, in which the user decides between stronger and less-strong alternatives; (b) in terms of password weakness, in which the user decides between weaker and less-weak options; (c) in terms of ease-of-memorability, in which the user decides based on how easy the password is to remember; (d) in terms of difficulty of memorability, in which the user decides based on how difficult the choice is to remember; or (e) in terms of some trade-off between security and memorability. Most password mechanisms are not explicit in framing the choice for the users, and in fact, the users are generally left to determine for themselves how the choice is framed. The theory suggests a user's password choices will depend on how the choice is framed by the user.

**Potential Responses**

Hypothesis 5 suggests assuming some control for how the password choice is framed by the user. The use of password strength meters by some websites is consistent with this approach and implicitly frames the decision in terms of strength: the user is obliged to understand their choices by how it increases or decreases a graph of password strength. However, the theory suggests alternatives, such as password weakness meters, password memorability meters, or a combination of password strength or weakness meters with memorability meters. Without additional research, it is unclear what approach would yield the best security-memorability trade-offs.

**Testing the Hypothesis**

Once again, simple experiments could be devised to test hypothesis and evaluate responses. Users could be randomly assigned to one of several groups whose choices were alternately framed. The control group would choose a password without any explicit guidance, and experimental groups could be provided password strength meters, password weakness meters, password memorability meters, or a combination of strength, weakness and memorability meters. The hypothesis would be supported if

password memorability and strength varies across the groups, and the recommended strategy would correspond to whatever group yielded the best security-memorability trade-off.

# IV. CONCLUSION

In this paper, we conducted an analysis of password choice, an insider threat that is introduced when organizational security policy requires users to make decision. Behavioral decision theory was leveraged to establish hypotheses about the psychological mechanisms underlying how and why users choose and to suggest response options that may be productive if the hypotheses were supported. For each hypothesis, behavioral experiments were proposed that could contribute to an evidence base that would facilitate an understanding of how different response options affect user choices.

## THE ANALYSIS COULD BE EXTENDED TO OTHER CHOICES MADE BY NON-MALICIOUS INSIDERS

This paper's narrow focus on password choice frames a classic insider security problem as an individual choice. This decision-theoretic framing suggests behavioral explanations for an insider threat, provides a coherent framework for developing new responses mechanisms, and suggests behavioral experiments that may validate the theory and evaluate different responses. Indeed, similar analysis and experiments could be conducted for other choices that users face as a result of organizational security policy -- for example, whether to open an email attachment, to visit a website, to encrypt a sensitive email, and to backup data. Such analysis may complement the contextual understanding of user behavior that is provided by usability research, by providing the cognitive perspective necessary to explain what context alone cannot.

## BEHAVIORAL EXPERIMENTS COULD SUPPORT THE DEVELOPMENT OF ORGANIZATIONAL RISK MODELS AND RESPONSES

Some of the research on the economics of information security has taken an *organizational perspective* to develop risk models that integrate a variety of threats, including those that arise from malicious outsiders and from malicious and non-malicious insiders. A

distinguishing feature of our work is that it takes a *user perspective* to analyze a specific risk that arises when organizational security policy requires insiders to make a choice. The present analysis may contribute to the broader understanding of the economics of information security, since analyses of human decision-making and behavior associated with specific risks may provide insights that enrich higher-level organizational risk models

**BIBLIOGRAPHY**

Abadie, A., and S. Gay, "The Impact of Presumed Consent Legislation on Cadaveric Organ Donation: A Cross-Country Study," *Journal of Health Economics*, Vol. 25, 2006, pp. 599-620.

Adams, A., and M. A. Sasse, "Users are Not the Enemy," *Communications of the Association for Computing Machinery,* Vol. 42, No. 12, 1999, pp. 40-46. http://doi.acm.org/10.1145/322796.322806

Arkes, H. R., and C. Blumer, "The Psychology of Sunk Cost," *Organizational Behavior and Human Decision Processes*, Vol. 35, 1985, pp. 124-140.

Bishop, Matt, Dieter Gollman, Jeffrey Hunker, and Christian Probst, "Abstracts Collection - Countering Insider Threats," *Dagstuhl Seminar Proceedings 08302*, July 2008, ISSN 1862-4405. http://drops.dagstuhl.de/opus/volltexte/2008/1796/

Bostrom, A., B. Fischhoff, and M. Granger Morgan, "Characterizing Mental Models of Hazardous Processes: A Methodology and an Application to Radon," *Journal of Social Issues*, Vol. 48, 1992, pp. 85-85.

Brown, Alan, Elisabeth Bracken, Sandy Zoccoli, and King Douglas, "Generating and Remembering Passwords," *Applied Cognitive Psychology*, Vol. 18, No. 6, 2004, pp. 641-651. http://www3.interscience.wiley.com/cgi-bin/abstract/109082556/ABSTRACT

Camp, L. J., and D. Liu. "Bringing Mental Models to Computer Security Risk," *Risk Analysis*, accepted, 2009.

De Angeli, Antonella, Lynne Coventry, Graham Johnson, and Karen Renaud, "Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems," *International Journal of Human-Computer Studies*, Vol. 63, No. 1-2, July 2005, pp. 128-152,

Ellsberg, D., "Risk, Ambiguity, and the Savage Axioms," *The Quarterly Journal of Economics*, Vol. 75, 1961, pp. 643-669.

Farahmand, Fariborz, Mikhail Atallah, and Benn Konsynski, "Incentives and Perceptions of Information Security Risks," *International Conference on Information Systems (ICIS) 2008 Proceedings*, http://aisel.aisnet.org/icis2008/.

Fischhoff, B., "Decision Research Strategies," *Health Psychology*, Vol. 24, No. 4, 2005, pp. S9-S16.

Florencio, D. and C. Herley, "A Large-Scale Study of Web Password Habits," In *Proceedings of the 16th International Conference on World Wide Web* (Banff, Alberta, Canada, May 08-12, 2007). WWW '07. Association for Computing Machinery, New York, NY, 2007, pp. 657-666. http://doi.acm.org/10.1145/1242572.1242661.

Forget, A., S. Chiasson, P. C. van Oorschot, and R. Biddle, "Improving Text Passwords Through Persuasion," *Proceedings of the 4th Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, July 23-25, 2008). SOUPS '08, vol. 337. ACM, New York, NY, 1-12. http://doi.acm.org/10.1145/1408664.1408666

Forget, A., S. Chiasson, and R. Biddle. *Persuasion as Education for Computer Security*, Ottawa, Canada: Carleton University, 2007: http://www.scs.carleton.ca/~schiasso/Forget_ELearn2007_PersuasionAsEducation.pdf

Gaw, Shirley and Edward W. Felten, "Password Management Strategies for Online Accounts," *Symposium on Usable Privacy and Security (SOUPS) Conference Proceedings*, July 2006. http://cups.cs.cmu.edu/soups/2006/proceedings/p44_gaw.pdf

Ives, Blake, Kenneth Walsh, and Helmut Schneider, "The Domino Effect of Password Reuse," Communications of the Association for Computing Machinery, Vol. 47, No. 4, 2004, pp. 75-78. http://portal.acm.org/citation.cfm?id=975817.975820

Kahneman, D., and A. Tversky, "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica*, Vol. 47, 1979, pp. 263-291.

Kahneman, D., and A. Tversky, "The Simulation Heuristic," in D. Kahneman, P. Slovic, and A. Tversky, eds., *Judgment Under Uncertainty: Heuristics and Biases*, New York: Cambridge University Press, 1982.

Kahneman, D., J. L. Knetsch, and R. H. Thaler, "Fairness and the Asumptions of Economics," in R.W. Hogarth and M.W. Reder, eds., *Rational Choice: The Contrast Between Economics and Psychology,* Chicago: University of Chicago Press, 1986.

Karat, Clare-Marie, John Karat, Carolyn Brodie, "Why HCI Research in Privacy and Security is Critical Now, *International Journal of Human-Computer Studies*, Vol. 63, No 1-2, July 2005, pp. 1-4.

Kirkpatrick, L. A. and S. Epstein, "Cognitive-experiential Self-Theory and Subjective Probability: Further Evidence for Two Conceptual Systems," *Journal of Personality and Social Psychology,* Vol. 63, 1992, pp. 534-544.

Levin, I. P., and G. J. Gaeth, "Framing of Attribute Information Before and After Consuming the Product," *Journal of Consumer Research*, Vol. 15, 1988, pp. 374–378.

Levin, I. P., S. L. Schneider, and G. J. Gaeth, "All frames are not created equal: A typology and critical analysis of framing effects," *Organizational Behavior and Human Decision Processes*, Vol. 76, 1998, pp. 149–188.

Loewenstein, G., "Behavioral Decision Theory and Business Ethics: Skewed Trade-offs Between Self and Other," in D. M. Messick and A. E. Tenbrunsel eds., *Codes of conduct: Behavioral Research Into Business Ethics*, New York: Russell Sage Foundation, 1996, pp. 214-227.

Loewenstein, G., and J. Elster, *Choice over time,* New York: Russell Sage Foundation, 1992.

Messick, D. M., and K. Sentis, "Fairness, Preference, and Fairness Bias," in D. M. Messick and K. S. Cook, eds., *Equity Theory: Psychological and Sociological Perspectives,* New York: Prager Publishers, 1983.

Pfleeger, Shari Lawrence and Joanne M. Atlee, *Software Engineering: Theory and Practice*, third edition, Upper Saddle River, NJ: Prentice Hall, 2006.

Predd, Joel, Shari Lawrence Pfleeger, Jeffrey Hunker, and Carla Bulford, "Insiders Behaving Badly," *IEEE Security and Privacy*, Vol. 6, No. 4, July 2008, pp.66-70, ISSN:1540-7993.

Roelofsma, P. H. M. P., and G. Keren, (1995). "Framing and Time-Inconsistent Preferences," in J.-P. Caverni, M. Bar-Hillel, F. H. Barron, & H. Jungermann, eds. *Contributions to Decision Making,* New York, NY: Elsevier Science B. V, 1995.

Samuelson, W. and R. Zeckhauser, "Status Quo Bias in Decision Making," *Journal of Risk and Uncertainty*, Vol. 1, 1988, pp. 7-59.

Sasse, M.A., S. Brostoff, and D. Weirich, "Transforming the 'Weakest Link' – a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal*, Vol. 19, No. 3, 2001, pp. 122-131, ISSN: 1358-3948.

Schneier, Bruce, *The Psychology of Security*, January 18, 2008, http://www.schneier.com/essay-155.html.

Shafir, E., "Choosing Versus Rejecting: Why Some Options Are Both Better and Worse Than Others," *Memory and Cognition*, Vol. 21, 1993, pp. 546–556.

Silverman, E., S. Woloshin, L. M. Schwartz, S. J. Byram, H. G. Welch, and B. Fischhoff, "Women's Views on Breast Cancer Risk and Screening Mammography: A Qualitative Interview Study," *Medical Decision Making*, Vol. 21, No. 3, 2001, p. 231.

Spafford, Eugene, *Opus: Preventing Weak Password Choices*, West Lafayette, Indiana: Department of Computer Sciences, Purdue University, CSD-TR 92-028, June 1991. http://ftp.cerias.purdue.edu/pub/papers/gene-spafford/spaf-OPUS.pdf.

Spector, Yishay and Jacob Ginzberg, "Pass-Sentence – a New Approach to Computer Code," *Computers & Security*, Volume 13, No. 2, April 1994, pp 145-160.

Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen, "Graphical Passwords: A Survey," *21st Annual Computer Security Applications Conference (ACSAC 05) Conference Proceedings*, Tucson, Arizona: IEEE Computer Society, December 2005, pp. 463-472. http://www.acsac.org/2005/papers/89.pdf

Thaler, R., "Toward a Positive Theory of Consumer Choice," *Journal of Economic Behavior and Organization*, Vol. 1, 1980, pp 39-60.

Topkara, Umut, Mikhail J. Atallah, and Mercan Topkara, "Passwords Decay, Words Endure: Secure and Re-usable Multiple Password Mnemonics," *Proceedings of the 2007 ACM Symposium on Applied Computing*, 2007, ISBN: 1-59593-480-4.

Tversky, A., and D. Kahneman, "Judgment Under Uncertainty: Heuristics and Biases," *Science Magazine*, Vol. 185, 1974, pp. 1124-1131.

Tversky, A., and D. Kahneman, "The Framing of Decisions and the Psychology of Choice," *Science Magazine*, Vol. 211, 1981, pp. 453-458.

Vu, Kim-Phuong L., Robert W. Proctor, Abhilasha Bhargav-Spantzel, Bik-Lam (Belin) Tai, Joshua Cook, and E. Eugene Schultz, "Improving Password Security and Memorability to Protect Personal and Organizational Information," *International Journal of Human-Computer Studies*, Vol. 65, No. 8, August 2007, pp. 744-757.

Weirich, Dirk, and Martina Angela Sasse, "Pretty Good Persuasion: A First Step Towards Effective Password Security in the Real World," New Security Paradigms Workshop, *Proceedings of the 2001 workshop on New Security Paradigms*, Cloudcroft, New Mexico, session 7, 2001, pp. 137-143. ISBN: 1-58113-457-6.

Wisdom, J., J. Downs, and G. Loewenstein, "Promoting Healthy Choices: Information vs. Convenience," paper presented at the Annual Meeting of the Society for Judgment and Decision Making, Chicago, IL, November 2008.

Wybourne, Martin, Martha Austin, and Charles Palmer. *National Cyber Security, Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior*, An Industry, Academic Government Perspective, 2009.
Institute for Information Infrastructure Protection (I3P).
http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf

Yan, Jianxin Jeff, Alan Blackwell, Ross Anderson, and Alasdair Grant, "Password Memorability and Security: Empirical Results", *IEEE Security and Privacy*, Vol. 2, No. 5, 2004, pp. 25-31.

Zviran, M., and W. J. Haga, "A Comparison of Password Techniques for Multi Level Authentication Mechanisms," *Journal of Computing*, Vol. 36, 1993, pp. 221-237.

Zviran, M. and W. J. Haga, "Cognitive Passwords: The Key to Easy Access Control," *Computers and Security*, Vol. 9, 1990, pp. 723-736.