DOT/FAA/CT- 05/20

Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

Human Factors Considerations for Passwords and Other User Identification Techniques

Part 1: Literature Review & Analysis

Kenneth Allendoerfer, NAS Human Factors Group, ATO-P
Shantanu Pai, L-3 Communications, Titan Corporation

September 2005

Technical Report

This document is available to the public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. A copy is retained for reference by the William J. Hughes Technical Center IRC.

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the objective of this report. This document does not constitute FAA certification policy. Consult your local FAA aircraft certification office as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center’s full-text technical reports web site: http://actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No. DOT/FAA/CT-05/20	**2. Government Accession No.**	**3. Recipient's Catalog No.**

4. Title and Subtitle
Human Factors Considerations For Passwords and Other User Identification Techniques Part 1: Literature Review & Analysis

5. Report Date
September 2005

6. Performing Organization Code
ATO-P

7. Author(s)
Kenneth Allendoerfer, NAS Human Factors Group, ATO-P and
Shantanu Pai, L-3 Communications, Titan Corporation

8. Performing Organization Report No.
DOT/FAA/CT-05/20

9. Performing Organization Name and Address
Federal Aviation Administration
NAS Human Factors Group, Bldg 28
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

12. Sponsoring Agency Name and Address
Federal Aviation Administration
Human Factors Division, AAR-100
800 Independence Ave., S.W.
Washington, DC 20591

13. Type of Report and Period Covered
Technical Report

14. Sponsoring Agency Code
AAR-100

15. Supplementary Notes

16. Abstract

All users need proper authorization before they can access National Airspace System (NAS) equipment. Current systems employ a variety of user identification systems and techniques such as usernames, passwords, and smartcards. Current procedures and policies place a variety of sometimes contradictory requirements on the Technical Operations workforce. This report describes the human factors and usability issues faced in the use of these identification techniques. Issues include the number of passwords a user must remember, the frequency by which the passwords must be changed, the complexity of the passwords, and social issues like trust and accountability. This report discusses the human factors research literature examining these topics and makes recommendations for making passwords easier to use in general. The report also provides an analysis of ways in which NAS maintenance tasks and systems differ from the typical information technology environment studied in the literature. The report discusses ways that these differences may affect decisions regarding passwords and other user identification technology. Finally, the report proposes a study in which information will be gathered from field personnel to provide a more specific, targeted analysis of how passwords and other user identification techniques can be made simpler and more usable in the NAS.

17. Key Words
Biometrics, Memory, Passwords, Tokens

18. Distribution Statement
This document is available to the public through
the National Technical Information Service,
Springfield, Virginia, 22161

19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 35	**22. Price**

Table of Contents

List of Illustrations

Figure Page

Executive Summary

Within the Federal Aviation Administration (FAA), Air Traffic Organization Technical Operations Services personnel ensure that the systems that make up the National Airspace System (NAS) function safely and effectively. All users need proper authorization before they can access NAS equipment. Current systems employ a variety of user identification techniques such as usernames, passwords, and smartcards.

The purpose of our research is to examine the human factors aspects of user identification systems, relate these to the FAA maintenance tasks, environment, and user characteristics, and develop recommendations for addressing human factors issues, such as memory limitations and ease of use. In this report, we present a literature review and analysis of human factors considerations for passwords and other user identification techniques. We relate this analysis to the FAA Technical Operations (TO) domain and provide recommendations for improving the use of passwords in the field. We also describe areas for further investigation.

The first and most common approach is known as knowledge-based identification, which uses something users *know* for authentication. Knowledge-based identification systems require users to memorize passwords and sometimes usernames and recall these when accessing the system. The security of a knowledge-based system is affected by an organization's policies and practices. There are many ways that passwords can be compromised such as snooping, spyware, guessing, and brute force attacks. The consequences for forgetting a password can be serious for an organization in terms of lost productivity, effort spent managing passwords, and in potential intrusion and loss of security.

Users feel cognitive pressures that make it difficult to remember passwords such as the length, complexity, frequency of change, frequency of use, and the number of passwords. Users also feel social pressures, such as concerns about identity, trust, and accountability, that affect whether or not they follow secure password techniques. As a result of the cognitive and social pressures, users adopt coping strategies such as writing passwords down, sharing passwords among a group of users, using words that are easy to guess, and using the same password on multiple systems.

A second approach is called token-based identification, which uses something a user *has* for authentication, such as a smartcard, key, or badge. The advantages of token-based systems over knowledge-based systems are that users are more likely to remember their token and that the token itself is hard to duplicate and share. Tokens do have some human factors issues such as forgetting or misplacing the token but these are generally easier to address than with passwords. Token-based systems are more expensive than password systems because additional hardware and administration are needed.

A third approach is called biometric identification, in which a physical or behavioral characteristic of the user is used, such as a fingerprint, an iris scan, or a voice recognition. The advantages of biometrics over knowledge- or token-based systems is that there is nothing for the user to forget and the biometric identifier is extremely difficult to share or duplicate. The main human factors issue facing biometric systems is the acceptability of such systems because of concerns about the personal nature of the information they use. In addition, biometric

identification systems require finding alternate techniques for users who lack the required characteristic, such as disabled people.

The TO environment differs in many ways from the traditional office environment that is typically studied in the literature. These differences include safety-critical systems, 24-hour operations, the number of systems, the variety of facilities and locations, unusual working postures and environments, and the age of many NAS systems. These issues should be considered during any system acquisition or policy-making process.

Recommendations for improving the human factors of passwords include increased training, increased enforcement and testing, reducing the number of passwords that must be remembered, allowing users to use clues and other techniques for remembering passwords, known as mnemonics. A future field study is proposed in which human factors engineers will collect specific data from field personnel about the systems, environments, and techniques used in the field and will provide more specific recommendations for the technical operations environment.

1. Introduction

Within the Federal Aviation Administration (FAA) Air Traffic Organization (ATO), Technical Operations (TO) Services personnel ensure that the systems that make up the National Airspace System (NAS) function safely and effectively. NAS systems include automation, communications, navigation, surveillance, and information technology systems. TO[1] personnel maintain current NAS systems and are responsible for the integration and transition of new systems. They work at many types of facilities:

- the National Operations Control Center (NOCC) located in Herndon, VA;
- three Operations Control Centers (OCCs) located in Atlanta, GA, Olathe, KS, and San Diego, CA;
- Air Route Traffic Control Centers (ARTCCs);
- Terminal Radar Approach Control (TRACON) facilities;
- Air Traffic Control Towers (ATCTs); and
- Automated Flight Service Stations (AFSSs).

AF personnel manage and maintain more than 44,000 pieces of equipment and systems at over 6,000 facilities and locations.

All users need proper authorization before they can access a NAS system. Current systems employ a variety of user identification systems and techniques. Identification is the process of associating an individual with an identity (Jain, Hong & Pankanti, 2000). It can be in the form of authentication, sometimes known as verification, in which a person provides an identity (e.g., username) and some confirmation (e.g., password). Authentication processes determine if users are who they claim to be. Identification can also be in the form of recognition in which the user makes no identity claim and the system determines who the person is automatically by matching the user's face or other characteristic to a database of authorized (or unauthorized) people.

Once authenticated or recognized, users are granted access and privileges based on what the system allows. Some systems give the same level of privileges to all authenticated users. Others allow user access to different functions or sections of a system based on their level of authority or job responsibilities. For example, a system administrator typically can access all areas of a system whereas a regular user is prevented from installing software, formatting hard drives, or other activities that are potentially destructive and not part of their normal job.

Identification systems fall into three categories: knowledge-based, token-based, and biometric identification systems (Miller, 1994). Depending on the nature of the systems being secured, an organization may use several techniques or combinations of techniques with different requirements. For example, safety critical environments like TO use knowledge-based identification systems with strict requirements for passwords. These requirements increase

[1] With the transition to the ATO, many functions once performed by the FAA Airway Facilities organization now fall under the ATO Technical Operations Services (ATO-W) service unit. Other functions now fall under the individual domain service units. To avoid confusion and unfamiliar terms, in this document we use the term technical operations (TO) in its general sense to refer to any personnel engaged in maintaining, monitoring, and controlling NAS equipment regardless of their position in the FAA organizational structure.

security because complex passwords are less prone to attack from intruders[2]. At the same time, these requirements may increase users' memory and cognitive load. Other user identification methods, such as smartcards and biometric techniques, may introduce other human factors issues such as user acceptance or difficulty providing biometric characteristics due to physical changes or limitations.

The purpose of our research is to examine the human factors aspects of user identification systems, relate these to the TO tasks, environment, user characteristics, and develop recommendations for addressing human factors issues, such as memory limitations and ease of use. In this report, we present a literature review and analysis of human factors considerations of passwords and other user identification techniques. We relate this analysis to the TO domain and provide recommendations for improving the use of passwords in the field. We also describe areas for further investigation.

2. Knowledge-Based Identification Systems

Knowledge-based identification systems use something users *know*, such as a password or personal identification number (PIN), to authenticate the user. For example, most traditional office systems require users to create alphanumeric passwords that satisfy criteria determined by the system administrator. Automated teller machines (ATMs) typically require a four-digit PIN. Depending on the system and the policies of the organization, passwords and PINs may be created by users or assigned by the system administrator. Knowledge-based approaches are widespread in the FAA and industry and will receive the majority of our attention in this report. In the last section, we discuss knowledge-based techniques that are not based on the traditional username/password model.

2.1 Security of Passwords

Knowledge-based identification systems require users to memorize their passwords and recall them when accessing the system (Sasse, Brostoff, & Weirich, 2001). Knowledge-based systems depend on the complexity, also called entropy, of the passwords and the secrecy of the users. Complexity refers to how difficult it is for an intruder to "crack" the password by guessing or brute force (Boroditsky & Pleat, 2001). A complex password is typically eight or more characters long, prohibits dictionary words, and includes special characters. For example, a password such as "J23$ERtN" is less likely to be guessed compared to a simple password such as "october66." Words such as a spouse's name are easy to guess and do not make secure passwords. Secrecy refers to users keeping a password confidential to only themselves and perhaps the system administrator. When users share their passwords with each other or write their passwords down, the secrecy is reduced.

[2] In common usage, the term "hacker" has come to mean a person who seeks to enter someone else's computer systems for purposes of vandalism, theft, fraud, or just thrills. However, "hacker" is also commonly used to describe a talented programmer or engineer who may be self-taught or may be known for developing practical solutions to difficult problems. To avoid confusion in this report and avoid offending the many legitimate hackers with whom we work, we use the term "intruder" to mean a person who enters a computer system without authorization.

The security of a knowledge-based system also depends on an organization's policies and practices. An organization may establish a policy that passwords must be changed on a specific schedule (e.g., every 90 days) and follow specific complexity requirements (e.g., minimum six characters, including two digits). The organization can encourage good practices through periodic training, memoranda, and in some cases, sanctions for employees caught breaking the rules. In many current systems, administrators enforce password policies using the system itself. For example, the system may be programmed to allow users to only create passwords that conform to the complexity requirements and may force them to change passwords at the required rate. System-enforced password policies, however, cannot guarantee password secrecy. There are no systems that can prevent a user from writing down their password.

Before discussing the human factors aspects of passwords, we believe it is important to understand how passwords are compromised and why various password policies are enacted. In the sections that follow, we discuss several methods that intruders use to illegitimately obtain passwords and access to computer systems.

2.1.1 Snooping, Spying, and Stealing

A simple way to obtain someone's password is to watch or listen to them while they enter it. In information security slang, watching someone while they type their password is called "shoulder surfing." Computers located in public areas, such as internet cafes, or being used in public areas, such as a laptop on an airplane, are especially susceptible. Snooping can also be accomplished electronically. A small video camera could be located unobtrusively and record finger movements. A wiretap can record telephone conversations and touchtone button presses. Spyware can record users' keystrokes and other actions.

A similar method is to steal or borrow an object or device where passwords are stored. This could be as simple as looking for sticky notes attached to a screen or stealing someone's day planner or personal digital assistant (PDA). The more in plain sight and unguarded an object is, the easier it is for an intruder to use it to steal passwords. In this case, social considerations contribute to the passwords being stolen. Users may believe they are in a secure environment and that "nothing will happen to me."

Another method is for the intruder to use someone's computer while the owner is on a break or has left for the day. Users may not always log off or may forget to lock their screens. The intruder simply sits down at the computer and scans the hard drive for likely filenames (e.g., "My Passwords") or looks in history and cookie files stored by web browsers. In addition, the intruder could also install spyware such as a keystroke logger.

2.1.2 Spyware

"Spyware" is slang for software that records information about users, usually without their knowledge. In a typical case, users unintentionally install spyware when they visit certain websites or install unapproved software. Spyware may be used in conjunction with social engineering techniques to trick users into installing the spyware. For example, a user may download legitimate software from the internet and install it on their computer. In addition to the legitimate software, however, the installation package also includes software that spies on the user’s sensitive data. The data recorded by spyware can be records of websites visited or, more seriously, of every keystroke made by the user. In this case, social considerations contribute to the passwords being stolen. Unscrupulous people tricked users into believing that the software was legitimate.

2.1.3 Social Engineering

“Social engineering” is a euphemism for deception. Social engineers are con men who trick others into revealing passwords, opening locked doors, and otherwise compromising security. A common social engineering technique is to call an employee, typically one with lower authority like a secretary, and claim to be someone in higher authority, such as an IT manager. The target gives away information or allows access out of a desire to be helpful, fear of reprimand, or even boredom (Jones, 2003).

“Phishing” is slang for social engineering via e-mail or other electronic means. The phisher sends an e-mail claiming to be an authority, such as a bank or online service, and says that there is a problem with the target’s account or computer. The target is asked to help fix the problem by providing their username and password.

“Spoofing” is slang for creating a system that looks legitimate but is really a way to steal sensitive information. Spoofing is often used in conjunction with phishing. In a typical spoof, the target receives an e-mail purporting to be from a trusted source. The e-mail may look completely legitimate, containing graphics and logos from the trusted source. The e-mail explains that the target’s account “needs updating” or may describe an “unadvertised sale.” The e-mail contains a link that seemingly takes the target to the legitimate site. Instead, the target is taken to a different site, often hosted in a foreign country, that has been made to look identical to the real site. The target logs to the spoof site which records the login information. For added realism, the spoof site may then forward the target to the real site. Only the website address gives any indication that the spoof site is illegitimate. Spoofing can be very sophisticated and even savvy users can be fooled (Neumann, 2000).

Education is the best protection against social engineering. Users must be aware of the different techniques that social engineers use, know how to spot an illegitimate e-mail or website, and know techniques for reporting possible social engineering attacks. All social engineering techniques use social pressures to compromise security.

2.1.4 Guessing

Despite being prohibited by most password security policies, people use common words for their passwords. The words they choose are often easy to guess, such as the name of a family member, a birth date, or even just “password.” A potential intruder may try to break into a system by guessing several likely candidates first before turning to more sophisticated methods. In this case, cognitive pressures contribute to the passwords being compromised. It is easy to remember a birth date so that is what users often choose.

Protection against lucky guessing is the main reason that many security policies prohibit using personal information and common words for passwords. Many systems have built-in measures that lock accounts after several unsuccessful attempts, such as the so-called “three strikes and you’re out” rule. Even with these measures in place, however, Pinkas and Sander (2002) found that lucky guessing is a very common method for intrusions.

2.1.5 Dictionary Attack

A dictionary attack is fairly difficult from a technical perspective and is associated with more organized, deliberate intruders (Pinkas & Sander, 2002). In a typical case, an intruder first obtains an encrypted password file from a system. This could be accomplished by social engineering, theft, or any other method. Having this file alone does not help the intruder much because modern encryption algorithms protect the contents of the file itself (Pinkas & Sander, 2002). However, the intruder can get around this by using the system’s encryption algorithm to create a file containing all the words in the dictionary in their encrypted forms. By comparing the encrypted dictionary and the encrypted password file, the intruder is able to identify regular words used as passwords.

Protecting against dictionary attacks is the main reason that many security policies prohibit the use of English words. Avoiding dictionary attacks also inspires policies to break up words with numbers or symbols as in “myp8ssword.” Dictionary attacks are successful mainly because of cognitive pressures on the users. It is easier to remember an English word than it is to remember random letters so users naturally choose words.

2.1.6 Brute Force

In a brute force attack, an intruder tries all possible combinations to crack a password. The more complex a password is, the more secure it is against brute force attacks. For example, when using a standard US keyboard, 26 lowercase letters, 26 uppercase letters, 10 digits, and 32 symbols are available. If all of these characters are available for use in a random, 8-character password, the number of possible combinations is 94^8 or six quadrillion (6.1×10^{15}). Even if a intruder could try 100 million combinations per second, it could take almost two years to obtain such a password by brute force (though, according to the laws of probability, the intruder has a decent chance of finding the password within the first year). However, it is extremely difficult for people to generate and remember random sequences. As a result, the search space for the brute force attack is actually much smaller than this. Intruders will normally begin the process with English words and other non-random sequences because these have a higher chance of success.

For a brute force attack to be successful, given the number of unsuccessful attempts required, security must normally be compromised in some other manner first. For example, an intruder might load software on a machine that disables the 3-strike-rule.

Protecting against brute force attacks is the main reason that security policies mandate the use of long passwords, both upper and lowercase, with symbols and numbers. In addition, frequently changing passwords helps protect against brute force attacks because of the long time required to complete one. Brute force attacks are successful mainly because of cognitive pressures on users. It is easier to remember words, birth dates, and other personal information than it is to remember a random string of letters and numbers. As a result, users allowed to choose their own passwords normally do not choose randomly, which makes the system more susceptible to brute force.

2.2 Cognitive Pressures

All knowledge-based identification systems rely on human memory, which in some ways is nearly limitless. People can remember hundreds of names, thousands of words, and tens of thousands of facts. People can remember huge amounts of information for decades and can retrieve information in fractions of seconds. In other ways, however, human memory is very limited. People forget names, faces, appointments, and their lunch boxes all the time. The study of how human memory functions and why people forget has been a focus of psychology since the earliest days of the field (Baddeley, 1990).

It can be very difficult for people to remember passwords, especially long and complex ones commonly required by modern information security polices. For example, Carstens, McCauley-Bell, and Malone (2000) asked participants to create their own passwords that followed common guidelines:

a. the password must be at least seven characters in length,

b. the password must have a combination of letters, digits, and symbols,

c. the password cannot use the same term more than twice,

d. password must not spell out a dictionary word or a proper noun, and

e. password cannot be relevant data, such as social security number, street address, or birth date.

They found that after one day of use, participants failed to correctly recall their passwords 50% of the time. In a similar study, Dhamija and Perrig (2000) found that participants could correctly recall a password one week after creating it only 70% of the time. The precise magnitude of the problem with forgotten passwords is not important. The key insight is that people have serious problems recalling passwords, even over relatively short periods of time.

Remembering passwords is made even more difficult when users access multiple systems with different passwords. For example, in their survey of British Telecommunications (BT) employees accessing multiple systems, Sasse et al. (2001) found that 80% of participants reported completely forgetting their password as the cause of their most recent login problem. In addition, about 18% of the participants reported confusing passwords across multiple systems. The average number of passwords used by BT employees was 16.

In the following sections, we describe five factors that exert pressure on human memory and affect how people can learn and remember passwords. Many of these cognitive pressures result directly from password security policies put in place to protect against guessing, dictionary, and brute force attacks. The pressures have cumulative and interaction effects. Mandating long, complex passwords may not cause problems if there is only one password and it rarely changes. However, mandating long, complex passwords for multiple systems that must be changed every month is very likely to cause problems.

2.2.1 Length

The classic study by Miller (1956) showed that human short-term memory has a capacity of seven “chunks” of information, plus or minus two. A chunk, in the traditional psychological view, is an integrated, meaningful set of information. The integration of the chunk helps a person recall the individual pieces of the chunk and recalling one piece helps the person recall the rest. For example, the list of letters “HARD TO RECALL” is much easier to remember than the list “AORR CL LATHDE,” even though both lists are exactly the same length, contain exactly the same letters, and have exactly the same spacing. In the first list, the letters are grouped into three meaningful chunks (i.e., words) whereas in the second list, the letters are organized into three meaningless groups. In the first list, recalling “HA” helps the recall of “RD” because the letters are chunked together into the word “HARD.” In the second case, recalling “AO” does not help with recall of “RR” because “AORR” is not a useful chunk.

To learn a list of items that do not form chunks, a person can use a variety of memorization techniques. The most common technique is rote rehearsal. Simply repeating the list items to oneself multiple times will increase memory for the list. However, rehearsal requires conscious, time-consuming effort and is still prone to errors and forgetting over time. Other techniques to use are rhymes, mental imagery, and other mnemonics that add richer meaning to the list items. In the example above, a good mnemonic would be to make a sentence out of the letters of the list, such as “All Old Red Roosters Called Larry Long Ago Took Home Duck Eggs.” Learning the meaningful (though a bit weird) sentence is more reliable in the long run than learning the list by rote rehearsal. However, coming up with a new mnemonic each month for each password can be challenging and time consuming.

More than 36% of IT organizations require a password eight characters or longer (Rainbow Technologies, 2003). Long passwords will be difficult to learn for many people, especially when those passwords carry other complexity requirements. Some people (the minus side of “plus or minus two”) are even going to have trouble learning passwords longer than five characters unless those passwords can be easily made into meaningful chunks (Miller, 1956).

2.2.2 Complexity

The closer a password is to truly random, the most difficult it is to crack by brute force. While few information security policies go as far as mandating truly random passwords, many prohibit the use of English words and may require using uppercase and lowercase letters, symbols, and digits. These requirements increase the randomness or “entropy” of the passwords and increase the number of possibilities that must be attempted in a brute force attack.

However, the closer to random a password is, the harder it is for people to form chunks. Short, random passwords, like 4-digit ATM PINs, are fairly easy to remember but long, random ones are exceedingly difficult (Sasse et al., 2001). Mnemonics become harder to develop the more random the password becomes. The main method for remembering a random password is through frequent, effortful rote rehearsal or writing the password down.

2.2.3 Frequency of Change

Passwords that change frequently are more difficult to crack by brute force because of the time such attacks require. Passwords that change frequently are also more resistant to attack because a stolen password has an automatic expiration date. If the intruder does not act immediately, the password may soon become worthless, even if the user does not know that the password has been stolen. In some national security applications, passwords change every day or even every minute. Few civilian password policies, however, mandate such frequent changes. Common techniques require that passwords are changed every 30 or 90 days.

The more frequently a password must be changed, the harder it will be to remember. In particular, old passwords will create what is known as proactive interference. Proactive interference occurs when old information gets mistakenly recalled in place of newer information (Baddeley, 1990). For example, suppose a password is "tinavg1p" for 90 days and then the user changes it to "t1inavgp" by swapping the location of the "1." When the user tries to recall the new password, he or she has a good chance of recalling the old password by mistake because it was used so often, for so long, and is so similar to the current one.

In addition to the effects on memory, frequent password changes create workload. Users must think of new passwords that conforms to all of the organization's requirements but that are also easy to remember. Second, users may need to rehearse the new passwords or develop a mnemonic. This is not trivial to do for many people (Sasse et al., 2001). With long, random passwords, the time needed to truly commit the password to memory may be substantial. Third, the user must go through the password change process which itself requires effort and takes time. If the user must change passwords for multiple systems around the same time, such as on last day of the quarter, the effect on a user's workload and other tasks may be substantial.

2.2.4 Frequency of Use

Passwords that are used every day are easier to remember than those used occasionally. In psychological terms, the person rehearses the password each time he or she uses it to log in. The more times a password is rehearsed, the more likely it is to be recalled. However, a person may not use every password they own every day, every month, or even every year. A password that has not been used in the last 12 months stands a 60% chance of being forgotten (Sasse et al., 2001).

2.2.5 Number of Passwords

An industry survey of over 3,000 IT workers found that the average IT worker manages 5.5 passwords but nearly one quarter of them manage more than 8 (Rainbow Technologies, 2003). The more passwords a person must remember decreases the chances for remembering any specific password. Having multiple passwords also increases the chance of interference among similar passwords. This is especially true for systems that are not used frequently.

2.3 Social Pressures and Attitudes

Cognitive aspects are not the only human factors considerations faced by users of knowledge-based IT security systems. Social aspects and user attitudes also play a major role (Sasse et al., 2001; Weirich & Sasse, 2001, 2002). Some of social factors and attitudes that affect users' password practices are listed below.

- *Identity*. People normally try to avoid doing things that would cause them to be viewed negatively by themselves or others. People who rigorously protect their passwords by steadfastly refusing to write them down or share them could be seen as paranoid, conformist, or "nerds." If it is important to me that others see me (and I see myself) as easy going and trusting, I am going to resist doing things that make me feel or seem paranoid. For example, if a person I believe to be an authority figure asks me what my password is, I am more likely to reveal it because I do not wish to seem overly suspicious.

- *Trust*. Sharing passwords among co-workers can be seen as a sign of trust. If a user refuses to share a password with a co-worker, it could be seen as a serious sign of distrust. Because mutual trust is a component of successful teamwork, policies that promote distrust normally should be avoided.

- *Informal work procedures*. A group of co-workers typically develops informal procedures and workarounds to deal with occasional situations that arise during day-to-day work. Some of these may contradict official password policies. For example, despite a policy that forbids sharing passwords, a user may be home sick and may ask a co-worker to log into his or her account and check e-mail. Users who follow these informal procedures are normally acting in good faith; they are trying to be helpful, practical, and are trying to get a job done. However, they are also reducing the overall security of the system.

- *Accountability*. Users often are fully aware of the password rules but still continue to violate them. According to Weirich and Sasse (2001), these users do not expect to be held accountable for breaking the rules because "they regard the regulations as unrealistic and their behavior as common practice." In addition, higher paid, more senior employees may believe that they are too busy or too important to be expected to follow petty password rules and that the IT department does not have authority to tell them what to do (Sasse et al., 2001).

- *Double-binds*. If users do not follow good security practices, their systems are more vulnerable. However, if users do follow good security practices, their systems may become more appealing targets. That is, a potential intruder may learn that a system is tightly protected and come to believe that there must be something very valuable in that system or may view the extra protection as a challenge. Users may believe that rigorously following the rules draws too much attention to them and their systems.

- *Nobody will target me*. Many users believe they or their systems are not important enough to merit serious attention from intruders.

- *They could not do much damage anyway*. Some users believe that even if their password were stolen, not much damage could be inflicted. In some cases, the users may be correct in this belief but many users may not be aware of the many ways their system and their data could be exploited.

- *Reputation*. Some users believe that rigorous password protection is not truly justified or necessary but they still follow the rules to preserve a professional reputation for themselves and their organization. Others do not see following information security rules as being related to their professional reputation.

Any organization developing information security procedures needs to consider each of these factors. Some can be addressed through training and examples. Others can be addressed by increasing monitoring, enforcement, and accountability for those found to be breaking the rules. Issues of identity and trust, however, will be more resistant to change because they are based in deeply held beliefs about oneself and how one should behave toward others. They are the main reasons why social engineering can be so effective. A solution to these problems may be reduce the need (or perceived need) for sharing passwords in the first place.

2.4 Consequences of Forgetting or Losing Passwords

To a single user in an office environment, the costs of forgetting a password are fairly light. The user will probably need to complete some paperwork, make a phone call, or possibly have an embarrassing discussion with a supervisor. Many systems will allow users to reset their own passwords by asking for other information (e.g., mother's maiden name, city of birth) and sending the new password to a known e-mail address (Vanguard Password Reset, 2003). No matter how easy the process, the user will experience some frustration and lose some productivity.

To the whole organization, however, forgotten passwords have significant costs. Depending on the number of systems and employees, managing usernames and passwords can be a full-time job for help desks. For example, at the FAA William J. Hughes Technical Center in 2004, a facility populated with engineers, programmers, and other highly technical people, there were approximately 1,700 Lotus Notes password resets out of 2,500 accounts. Many of these resets were associated with upgrading from one version of the software to another. There were roughly 650 password resets out of 2,500 Novell Network accounts and 100 resets out of 700 Microsoft Network accounts. There is no information regarding how those resets were distributed (e.g., did 20% of the accounts require 80% of the resets?), however the numbers give a rough idea as to the scope of the password management issue in a large organization. Even if each reset cost as little as 10 minutes of productivity and IT labor, the resets for just these three systems cost the Technical Center over 400 labor hours in one year.

In TO, the consequences of a forgotten password are more serious. A maintainer cannot afford to be locked out of an essential system in a safety-critical environment due to a forgotten password. A maintainer cannot afford to have their duties, such as returning a mission critical component to service after a repair, delayed while a password is reset or a system administrator is contacted. Because the NAS is a 24-hour operation, many TO personnel work night shifts and independently with low staffing levels. A forgotten password on the overnight shift could mean an interruption in service due to unavailability of staff authorized or trained to reset passwords.

For these reasons, forgetting passwords is a serious issue in TO that needs to be carefully evaluated.

Even worse than the consequences for forgetting a password are the consequences of an intruder stealing or cracking a password. Intruders do not necessarily come from outside the organization. An intruder is simply someone who accesses a system when he or she is not authorized to do so. In an FAA office environment, a stolen password could result in relatively minor offenses like reading someone's private e-mail or it could result in very serious crimes like identity theft or the destruction of government property. In TO, a stolen password could allow an intruder to compromise the safety or efficiency of the NAS by damaging systems or corrupting data. For this reason, password security in TO is a focus of agency IT security policy.

2.5 Coping Strategies

Traditional usability principles seek to reduce the likelihood of human error and hide complicated processes and obstacles. A system without a password is usable, but not very secure whereas a system that requires a new login every minute would be very secure but unusable (Cranor & Garfinkel, 2004). When a system is prone to errors and complex to use, users often take matters into their own hands by building workarounds and cheat sheets (Boroditsky & Pleat, 2001); password systems are no different. Users often violate password policies because forgetting a password can lead to serious consequences but complex passwords are difficult to remember (Weirich & Sasse, 2002). For example, users may write their passwords on a sticky note and leave it on their desk or make a list of passwords in their PDA or in a file on their computer.

The cognitive pressures, the social pressures, and the consequences of forgetting a password exert pressure on the users. Users do not want to forget their passwords but many times the password policies and systems are constructed so that some forgetting is inevitable for nearly everyone. To avoid forgetting passwords, to satisfy the social factors, and comply with at least *some* of organization's password policies, requirements users may adopt one or more coping strategies listed below.

- *Writing passwords down*. Adams and Sasse (1999) found that 50% of 139 business persons surveyed wrote down their passwords. An industry survey of over 3000 IT workers found that 55% reported writing down their passwords at least one time (Rainbow Technologies, 2003). Writing down a password may not always be wrong. If the system is in a secured room, writing an extremely long group password and taping it to the system may be worthwhile as this may discourage users from disclosing it over the phone (Yan, Blackwell, Anderson, & Grant, in press).

- *Sharing one password among a group of co-workers with similar responsibilities.* System administrators may sometimes assign a password to a group of individuals with similar responsibilities and authorization levels. This is usually true in organizations that encourage shared responsibilities and teamwork (Adams & Sasse, 1999). This technique also diffuses accountability and reduces the ability to audit the use of passwords (National Institute of Standards and Technology, 1985). In an industry survey, 44% of IT workers reported sharing passwords (Rainbow Technologies, 2003). This strategy helps alleviate both cognitive and social pressures.

- *Using an easily guessed word like a family member's name or a birth date* (Boroditsky & Pleat, 2001). The Brown, Bracken, Zoccoli and Douglas (2004) survey found that two-thirds of their participants created passwords based on personal characteristics like their own initials or birth dates, with most of the remainder relating to relatives or friends.

- *Using the same password on multiple systems*. Cyota Online Service Stats (2005) found that 44% of users of online banking services, which deal with very sensitive information, use the same password on multiple systems. Brown et al. (2004) found that 66% of more than 200 college students used the same passwords on multiple systems even though the students averaged fewer than five systems apiece.

- *Using the shortest and simplest password that the system will accept*. While not a true violation, this coping strategy prevents an identification system from being as secure as it could be.

- *Changing a password when required, then immediately changing it back*. This coping strategy is prevented by many systems that track previous passwords.

- *Making a new password by making a minor change to the original password*. For example, user might change the password "HackOnThis1" to "HackOnThis2." Some systems also prevent this automatically by requiring a maximum amount of overlap between subsequent passwords.

- *Relying on subordinates to remember passwords.* There are no technical means to prevent this coping strategy; only policies and education can prevent this.

- *Using mnemonics*. For example, a user might select a password using the first letter of each word of a meaningful sentence. Depending on the mnemonics being used, this coping strategy can be used effectively without reducing overall security.

Coping strategies are not necessarily negative but they are indicative of the pressures being experienced by users. Most coping strategies lead to a lower overall security level and are seen as negative by the organization. However, coping strategies are positive from the users' perspective. They reduce cognitive and social pressures and decrease the chances that a user will feel the consequences of forgetting a password. By instituting stricter requirements for passwords, information security policies may be inadvertently lowering overall security. Stricter requirements add pressure on the users which will likely lead to more use of coping strategies which, in turn, will lower overall security (see Figure 1). Many of these strategies are explicitly prohibited but this is no assurance that people do not use them. The goal of any policy should be to maximize overall security.

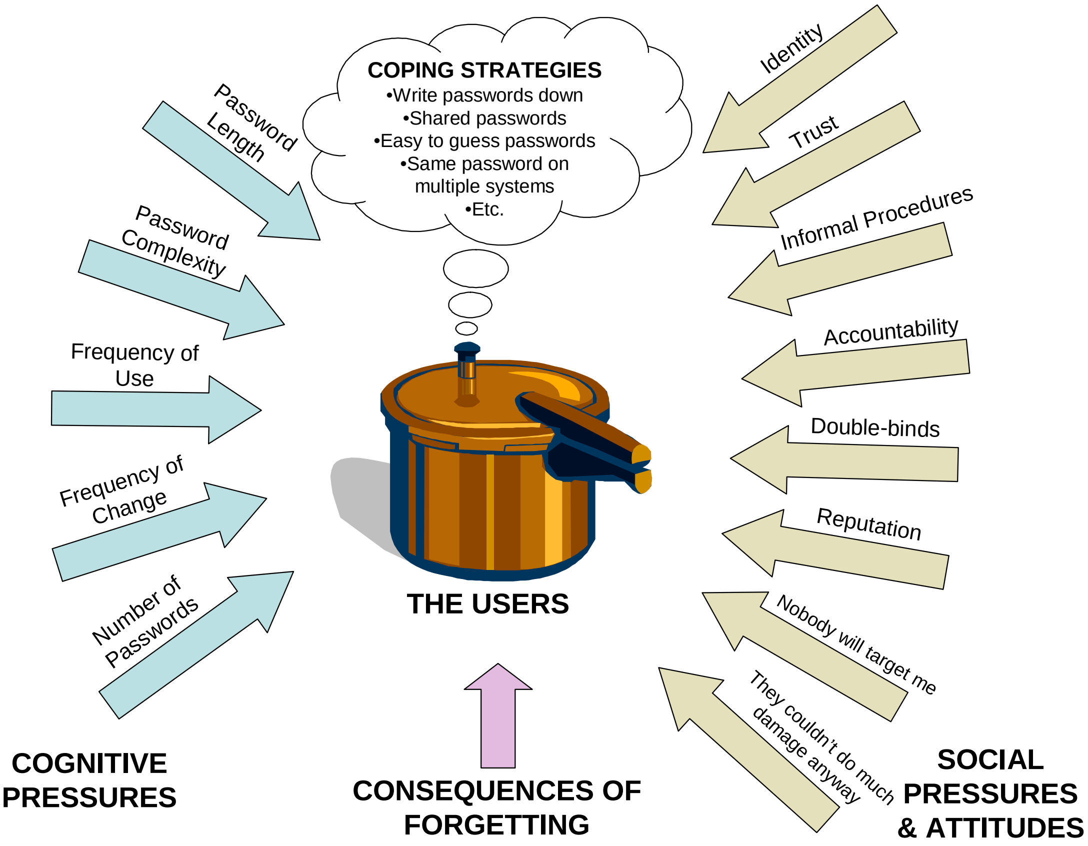

Figure 1. The pressures on users regarding passwords.

Not all coping strategies have equal effects but all have the potential to reduce password security by moving users away from the theoretical ideal of long, random passwords that change frequently. Some coping strategies can be prevented by the password management system itself. For example, a system may be configured to accept only passwords that meet the organization's policies for length and complexity. However, no system or technology can prevent a user from writing a password down.

2.6 Other Knowledge-Based Techniques

Though passwords and PINs form the majority of knowledge-based identification systems, there are other techniques under development or being used in limited areas. These may be promising alternatives once the technology is commercially mature and has been more widely tested. These technologies attempt to make the task simpler by relying on characteristics that people find particularly easy to recall.

2.6.1 Recognition-Based Passwords

Almost all password systems are based in recall in which a user fills in a blank. However, a century of memory research shows that humans are generally much better at recognition than recall (Baddeley, 1990). Recognition is a form of remembering in which the person chooses items from a list. Recall relies on fill in the blank questions, recognition relies on multiple choice.

There is a growing literature on the use of recognition-based passwords, especially recognition of pictures rather than words. At least one commercial product is available based on this technique, known as Passfaces (RealUser Corporation, 2005). Passfaces makes use of people's remarkable ability to remember human faces very accurately for long periods of time. Passfaces presents users with a list of pictures of human faces and asks the user to indicate pictures that are part of the user's personal list. Human factors research has shown that this technique decreases login failures over traditional passwords by as much as a third and even when used less frequently than passwords (Brostoff & Sasse, 2000).

Dhamija and Perrig (2000) allowed users to select a set of 5 photos or artwork from a set of 25. The probability of an intruder cracking a set of pictures by lucky guessing was the same as a PIN. However, after one week, the chance of the user accurately recognizing his or her set of pictures was 90-95% whereas the chance of accurately recalling a password or PIN was 65-70%.

Weinshall and Kirkpatrick (2004) presented participants with a password composed of a set of pictures, randomly selected from a database of 20,000, arranged in sets of 2 to 9 images. During the authentication process, participants were shown several groups of images and were asked to select the one image in each group that was in the original training set. Accuracy rates varied from 70% to 90% over a three month period while the probability of an intruder succeeding at guessing the correct pictures was less than 0.001.

The primary human factors considerations of these techniques involve understanding how people choose pictures or words to recognize. If an intruder knew that the target user liked dogs, the intruder would be likely to select a picture of a dog as a reasonable first guess. This issue is not significantly different from users creating passwords out of easily guessed information.

2.6.2 Challenge Questions

Challenge questions are another knowledge-based technique. A challenge question is based on personal information that is difficult to forget, such as "What is your mother's maiden name?" or "What is your eye color?" A series of these questions may be very difficult for an intruder to guess correctly. Which questions are used and the sequence of questions could change every login, making the system difficult to crack by brute force or lucky guessing. Challenge questions are currently common in the banking industry to authorize telephone transactions and on websites to reset a forgotten password.

The primary security consideration of challenge questions is that the answers can be obtained relatively easily by spying, stealing, and social engineering. Certain questions, like mother's maiden name, are so commonly used that a motivated intruder might determine this information ahead of time. A successful challenge question system would need to use a series of questions using information that is very difficult to obtain without knowing the target person personally.

Two important human factors consideration for challenge questions are the time it takes to complete the process and the privacy of the information. To provide a high level of security, a series of challenge questions must be asked. The process will naturally take longer to complete than typing in one password. This may reduce productivity and increase frustration. However, the reduction in forgotten passwords and time spent resetting them may compensate for the slower authentication process in the long run.

A second human factors consideration is that the system must store the right answers to the challenge questions. In the case of a series of questions, this could be a substantial amount of information. Many people are reluctant to provide personal information due to privacy considerations and fear of identity theft.

3. Token-Based Identification Systems

Token-based identification systems use something the users *have* to make an identification (Jain et al., 2000). Magnetic swipe cards, keys, infrared card readers, radio frequency readers, and smartcards fall under this category. One of the important advantages of token-based identification systems is that they do not require users to remember a password. They do, however, require that users remember their token.

Tokens employ different methods to prevent tampering or forgery. At the simplest level, a token must be physically manufactured. The more complex the manufacturing process is, the harder it will be for a potential intruder to forge or duplicate a token. In addition, the token can have security mechanisms built into it. For example, tampering with some types of radio frequency identity (RFID) tokens sends an alarm notification to the RFID reader or notifies the security personnel that the token needs to be revalidated (Activewave RFID Applications & Solutions, 2004). RFID based tokens may facilitate tracking of lost badges through a built-in sensor (Activewave RFID Applications & Solutions). This sensor can also send a signal when badges are swiped by employees.

Smartcards, which are plastic cards incorporating small memory chips, can be exceedingly hard to crack because of the amount of information that can be stored on the chip and the encryption that can be applied. The difficulty of manufacturing smartcards makes them attractive solutions for many information security applications.

All token-based systems require some sort of infrastructure for issuing the tokens and for reading them. For example, a system based on magnetic swipe cards requires a reader at each access point and a device to encode new cards and replace lost ones. Depending on the technology used, token-based systems can involve significant expenditures on hardware and administration. Finally, as with password systems, the organization must set policies for issuing and renewing tokens.

3.1 Human Factors Issues

Token-based identification systems have several inherent human factors weaknesses. Most importantly, users may forget, misplace, or damage their token. Like passwords, as the number of tokens increases, the chances for forgetting or misplacing a token increases. The chances of users adopting negative coping strategies (e.g., attaching every token to one lanyard that users wear around their necks) also increases. Like a forgotten password, a missing or damaged token typically requires the user to contact the system administrator, file paperwork, and obtain a new token. The administrator will be required to process the paper work, deactivate the lost token, and issue a new one. In case of a lost or damaged key, a locksmith may have to be called in to replace the now compromised lock.

Physical distribution of tokens makes them easy to share with others. They are easily identified and portable, which may make them targets for theft. If a token is lost or stolen, the person recovering the token has the same access as the owner until the owner realizes that the token is missing. For tokens that are rarely used, owners may not realize that a token is missing until they try to access the system and cannot.

The hardware at access points needs some level of administration and maintenance. Depending on the configuration, a single malfunctioning card reader might prohibit all users from accessing a system or facility. In addition, as in password systems, token-based systems employed in 24-hour time critical environments like TO must address how systems can be accessed or new tokens can be issued during non-business hours when the people normally responsible for administering the tokens are unavailable.

To restrict system access to rightful owners of the tokens, token-based identification systems may add multiple authenticating factors to the identification process. For example, users of some token-based systems may be required to enter a PIN or password in addition to using the token. This process adds another level of complexity making it difficult for intruders who have stolen or forged a token to gain access. At the same time, this procedure requires users to memorize passwords and is subject to the password limitations discussed in the previous section.

4. Biometric Identification Systems

Biometric identification systems identify individuals based on their distinguishing physiological and/or behavioral characteristics (Miller, 1994). A biometric identification system uses a pattern recognition system to make a personal identification by verifying the authenticity of a specific physiological characteristic, such as fingerprint, retinal pattern, iris, face, wrist vein, hand geometry, or a behavioral characteristic, such as handwriting, signature, or speech (Jain et al., 2000).

4.1 Complexity of Biometric Identification Systems

An ideal biometric identification system would have the following characteristics (Jain et al., 2000):

a. It is *universal* so that all people possess the characteristic.

b. It is *unique* in that no two people can have the same characteristic.

c. It is a *permanent* characteristic and can be neither changed nor altered.

d. It is *presentable* in that the physiological or behavioral characteristics can be easily provided to a sensor and is easily quantifiable.

The biggest security advantage of biometric identification systems is that they are extremely difficult to forge. Despite what happens in spy novels, there is no way to create an artificial retina and a retina from a dead person deteriorates rapidly (National Center for State Courts, 2002). In addition, unlike knowledge-based and token-based systems, users of biometric identification systems do not need to remember or keep track of anything. The physical or behavioral characteristic is with them all the time. Biometric identification systems, however, have been more expensive to install and maintain than password systems (Boroditsky & Pleat, 2001).

4.2 Human Factors Issues

When compared with knowledge-based or token-based identification system, biometrics-based identification systems have a human factors advantage because users are not required to recall passwords or keep track of tokens. Users carry the physiological or behavioral characteristics used in biometric identification all the time. However, there are other human factors issues associated with biometric identification systems.

4.2.1 Maturity of Technology

Biometric systems have some technological barriers to overcome. For example, accuracy and verification time still can be problems. For example, Coventry, Angeli and Johnson (2003) found a series of problems with different biometric technologies. A prototype face recognition system simply failed to recognize participants 10% of the time, even through the participants were in its database. Seventeen percent of the participants failed in more than half their attempts to use a fingerprint scanner. The verification time with an iris scanner varied from as low as 2.2 seconds to a high of 33.5 seconds. These results show that even if the users do everything right, there is still a chance that the identification will fail or take a long time. These failures and delays caused by the technology could potentially increase workload and cause frustration for the users. Again, in a time-critical environment, delay may not be acceptable.

Research efforts aimed at increasing the accuracy and decreasing the time for verification are underway. For example, Fox, Gross, Chazal, Cohn and Reilly (2003) integrated three separate biometric identification systems employing speech, static face images, and lip motion features to obtain a maximum accuracy of 100%. Apart from high accuracy, integration of separate biometric characteristics may be helpful when temporary physical changes prevent users from using the biometric systems. For example, when a user is not able to provide a finger print due to a cut, the system may identify him based on an iris scan or speech recognition, thereby ensuring continuous availability of the system.

4.2.2 Physical Changes and Disabilities

Temporary physical changes such as cuts, burns, or blisters on the finger may prevent users from providing a fingerprint for scanning (Proctor, Lien, Schultz & Salvendy, 2000). Face recognition mechanisms may fail when users grow a beard or wear glasses (International Biometric Group, 2002). A voice recognition system may have difficulty recognizing a user recovering from a cold. Physical changes associated with illness or aging may also affect the accuracy of the identification (Turner & Blackburn, 2002). Finally, not all users will possess the physical or behavioral characteristic. For example, a disabled user may not have use of the proper hand needed to present to a hand geometry scanner.

4.2.3 Training and Usability Factors

To achieve higher levels of identification accuracy, biometric technologies typically need users to present the characteristics in a specific way. These requirements vary between manufacturers and technologies. For example, an iris scanner may require that users hold their eyes very still for a period of time. The users may require some training and experience before they can keep their eye still long enough. Until they reach this point, users will be more prone to errors and accompanying delays.

4.2.4 User Acceptance

Social and psychological factors come into play while considering biometric identification systems. For example, iris scanners may make users uncomfortable because they are inherently protective of their eyes (Miller, 1994). Collecting information like fingerprints may make users uncomfortable because of the association between fingerprints, law enforcement, and a surveillance society ("Big Brother"). Users may feel that their physiological or behavioral characteristics are private and personal and they may resist providing these data to the organization (Turner & Blackburn, 2002).

Biometric systems seem to be becoming more acceptable with time. For example, in a survey of ATM users, 78% of the respondents said that having biometric access to ATMs would be acceptable to them (Westin, 2002).

5. Issues for the TO Environment

Different working environments may warrant different approaches to user identification. For example, the TO environment is unusual in that it houses more than 44,000 pieces of equipment at over 6,000 locations. The FAA custom built many of its NAS systems or purchased commercial-off-the-shelf (COTS) products and modified them for FAA use (Ahlstrom & Muldoon, 2003). As a result, there is a lack of consistency in the system security approach as well as the method used for authenticating users. For example, TO personnel may be required to set up passwords for different systems following different password requirements and policies. As a result, they are forced to remember many passwords. Although requiring users to recall a username and a password for one system may be reasonable, users find it difficult to remember usernames and password for multiple systems.

The following characteristics make the TO environment different from the common corporate IT environment. These differences should be considered in selecting technology and policies for user identification systems:

a. Safety is the main concern of the FAA and the TO personnel. A reduction in NAS safety due to an information security breach is unacceptable. As a result, the overall information security profile for FAA systems must be higher than most corporate or industrial systems.

b. TO personnel provide 24-hour service to ensure safe operation of the NAS. However, not all facilities are staffed at all times and different authorization levels may be needed at different times of day. Any interruption in service may have safety implications. In addition, many TO facilities are staffed and monitored at all times.

c. Because TO operations are safety and time critical, identification systems need to establish user identity as quickly as possible. A slower system may not be acceptable.

d. TO personnel may handle several systems in a single day. For example, TRACON specialists may interact with up to fourteen systems on a daily basis, whereas TO specialists at an ARTCC will monitor and interact with up to 25 systems (Ahlstrom & Muldoon, 2003). Each system may have different identification mechanisms.

e. TO personnel often work at sites far from their home base. Returning to their base to retrieve a misplaced token may not be feasible, especially when the task is time or safety critical.

f. Awkward working postures (e.g., on a ladder or in a cabinet) may prevent TO personnel from providing biometric data such as a retinal scan or hand geometry.

g. TO personnel may work in outdoor environments under variable weather and lighting conditions. In addition, they may need to wear gloves or other protective clothing while working.

h. Many of the systems maintained by TO were built during eras with lower expectations for information security. The legacy equipment may not accommodate all possible identification technologies.

i. The TO environment is not a homogeneous entity and is organized into different domains and regions, each with its own responsibilities and ways of operating (Ahlstrom & Muldoon). Each domain has a unique configuration of systems and equipment. For this reason, a NAS-wide guideline or policy regarding user identification systems may be difficult to establish. Policies may need to be tailored for individual domains.

j. Although many TO systems are safety and time critical, not every system has equal security concerns and most facilities already have multiple security measures in place (e.g., property security, door access, 24 staffing). Most FAA systems are only accessible over the FAA intranet and many are connected only to internal, closed networks. Recommendations developed for more externally open IT environments may need to be reconsidered for TO.

Hence, a survey of policies and practices associated with use of identification systems is necessary to understand the current use of identification systems and how TO personnel manage access for multiple systems. For example, TO personnel may interact with 25 different systems, each requiring its own password. Apart from understanding the current state of identification systems in the TO environment, the survey will also highlight problem areas, if any, from the human factors point of view. The current state of the art in identification systems will then be reviewed to determine an appropriate fit between technologies, policies and practices, and the requirements imposed by the TO environment, users and tasks.

Although usability of identification mechanisms may be improved through technology, policies, practices, and the willingness of users to follow the practices still remain issues. Ideally, to maintain security of the systems, users need to be persuaded rather than forced to adhere to information security practices and the policies and practices need to address the users, tasks, and environment as well as security. A field study will allow us to evaluate current password practices from a human factors point of view and identify factors that lead to non-adherence to safe practices for authentication and make recommendations to mitigate these issues. The feasibility of these recommendations may also be assessed.

6. Recommendations

Organizations may spend a considerable amount protecting information systems through the use of technology (Brostoff & Sasse, 2002). Because humans are integral parts of the overall information security profile, technological or other measures targeted at securing the systems are less effective when human factors is not considered.

The priority given to information security by an employee depends on that employee's duties and where that employee is in the organizational structure (Besnard & Arief, 2004). Although maintaining security is an obvious part of a system administrator's job, users may not hold themselves responsible for the security of the system. Identifying and authenticating users delays and creates workload for users who want to use systems to accomplish their primary job duties (Weirich & Sasse, 2002). From a user's perspective, the ideal number of authentications required in their day-to-day activities is zero. For this reason, it is important that organizations create strategies aimed at making security usable, especially for individuals for whom information security is not a primary job function. Techniques that reduce the cognitive or social pressures on users, described in the following sections, make information security easier for users, reduce the impact of information security on the actual business of the organization, and increase overall security by discouraging negative coping strategies.

6.1 Training and Awareness

Many authors in the IT security literature recommend increasing training for employees on password security and launching awareness campaigns (Adams & Sasse, 1999; Cranor & Garfinkel, 2004; Orgill, Romney, Bailey, & Orgill, 2004; Sasse et al., 2001). From a human factors perspective, we certainly endorse these recommendations. However, we caution organizations against expecting increased training and awareness to result in large, fast improvements in compliance and overall security. There is little evidence in the literature that more training or increased awareness measurably improves users' behavior in the long run. The research shows that, in general, employees know the rules and understand the consequences of forgetting their passwords. Employees break the rules to cope with the powerful cognitive and social pressures that we have discussed throughout this report. Increased training and awareness may indeed reduce some of the social pressures and may help protect against social engineering. Unfortunately, the only way that increased training is likely to reduce cognitive pressures is by providing training on mnemonics to facilitate recall in knowledge based systems.

6.2 Enforcement and Testing

Increasing enforcement of IT security policies or increasing the consequences if employees are caught violating the policies may improve the overall level of information security. About 75% of the1230 organizations surveyed by Ernst and Young suggest that rigorous monitoring and enforcement of regulations have a positive impact on maintaining information security (Ernst & Young, 2004). From a human factors perspective, however, increased enforcement is likely to have little effect on cognitive pressures and is likely to have a mixed effect on social pressures. Increased enforcement is likely to increase employees' sense of accountability and increase their understanding of the consequences of breaking the rules. It may also strengthen an us-versus-them dynamic between the users and the information security staff, which may compound existing pressures of identity and trust. The organizations enforcing information security policies should be aware that users may want to comply with the policies but simply cannot because of the other cognitive and social pressures placed on them.

We encourage organizations to take a somewhat softer approach by instituting non-punitive security testing following the so-called "tiger team" or "white hat" approach. In this approach, trusted experts are hired to attempt to break into systems using whatever techniques and tools are available to them. The findings of such "attacks" are normally not used to punish employees but rather to identify holes. For example, a tiger team might call employees and attempt to use social engineering to obtain their passwords. The results of the audit could be presented to the employees (without identifying information and no threat of sanctions) as an illustration of the importance of secure practices. Such an audit could be part of a larger training or awareness program. Unfortunately, such audits are expensive to conduct and the organization is still left with the question of how to fix the identified problems. Users would need to be aware that periodic audits such as these could occur. The awareness of the audits alone may be enough to increase compliance with information security policies.

6.3 Fewer Passwords

Some experts in information security literature believe that using one password to access two or more systems is a very bad idea (Brown et al., 2004; Cyota Online Service Stats, 2005). Doing so, they argue, allows a single security breach to affect multiple systems instead of just one. While this argument is reasonable on its face, we believe that maintaining dozens of passwords (or, worse, instituting a policy that requires a different password on every system) creates unacceptable cognitive pressure on users. If users must remember more than even five or six different passwords, they will almost inevitably write their passwords down (Brown et al., 2004). Writing passwords down increases the risk for future security breaches. Stealing a day planner or PDA could result in the compromise of many systems. In addition, writing down and keeping track of multiple passwords creates workload and frustration for users, takes them away from their actual tasks, and reduces job satisfaction.

In our opinion, organizations can improve their overall information security by allowing the same password to be used on multiple systems and by allowing fewer, stronger logins. Fewer passwords reduce the cognitive pressure on users, increasing the likelihood that they will keep their passwords in their heads not their PDAs. With fewer passwords to remember, the organization could afford to make the remaining logins more complex, change more frequently, or that use an identification technique other than passwords, such as graphical passwords, challenge questions, tokens, or biometrics.

6.4 Clues and Mnemonics

If users insist on writing down their passwords, they can be encouraged to add a level of protection by writing down only clues to the password, like the first and last letter, rather than the password itself. If the passwords are recorded in a file or on a PDA, the password file itself can be protected with a password.

Passwords can be recalled more easily if users have the freedom to add meaningful data to them. For example, in the second stage of their experiment, Carstens et al. (2000) found that when passwords contained meaningful data, such as user's first and last initials, the recall rate increased from 50% to 72%. Interestingly, these passwords met the stringent complexity guidelines discussed earlier. Participants were better able to recall the passwords because meaningful data in the passwords could be grouped and chunked together. Organizational policies may need to be amended to allow for password guidelines that permit use of meaningful data for the user, however still enable organizations to have complex passwords.

Mnemonics can be very effective in improving recall (Baddeley, 1990). However, many users do not know about mnemonics or do not have experience applying them to passwords. It is here that training and awareness could have some positive effect on cognitive pressures. Some examples of mnemonics follow:

- *Use the first letter of each word of a phase to form the password.* For example, "My dog Spot eats two bowls of food every day" can become "MdSe2bofed," a very secure password. This technique also can be used in reverse, in which a random sequence is created and then words are associated to the letters. This is similar to "Every Good Boy Deserves Favor" which musicians use to learn the lines of the treble clef or "Kings Play Chess On Fancy Glass Stools" which biology students use to learn the levels of the taxonomy of species.

- *Use rhymes*. Ancient storytellers remembered long epic poems by rhyming and rhymes help children learn to sing and speak. Rhymes can be easily applied to passwords even if nonsense words are used. For example, "DemTem1Blem" sounds like a line from a nursery rhyme but is very easy to remember and conforms to most password policies.

- *Rehearse aloud*. When developing a password, users may think it is sufficient to rehearse the password in their heads. It is much more effective to rehearse the password by speaking it aloud. To maintain security, of course, this rehearsal needs to be done alone. Singing the password to a familiar tune is even more effective.

- *Use visualization*. In this technique, a person associates visual image with the information being memorized. A common technique is for the person to first learn a list of related concrete words, known as pegwords, and then associate those words with the letters of the password. For example, a person can easily learn a list of pegwords such as "Kennedy Johnson Nixon Ford Carter Reagan Bush." Then the user visually associates the letters of the password with the pegwords (John F. Kennedy eating a letter “W,” Lyndon B. Johnson with an “X” on his shirt, Richard M. Nixon carrying an “H,” etc.). Creating elaborate visualizations like this may seem like too much effort to learn a simple password. However, this technique is commonly used by performers who entertain audiences with their abilities to quickly and accurately learn information and can be extremely effective.

- *Use puns and shorthand*. E-mail, instant messaging, and vanity license plates have created visual puns, shorthand, and abbreviations using letters, numbers, and symbols. For example, “CUL8R” (for “see you later”) and “;-)” (for a winking, smiling face) are common typographical jokes used in e-mail. In combinations, this type of pun can be used to create passwords that are hard to crack but easy to remember.

- *Password visits.* Passwords that are used infrequently are frequently forgotten. To improve the likelihood of actually recalling the password when it is truly needed, frequently logging into each system and then logging back out will help keep passwords fresher in the users’ memories. Depending on the number of systems, however, making regular password visits would take time away from users’ primary tasks.

7. Future Research

Building on the analysis and recommendations discussed so far, we plan to pursue additional research into the human factors considerations of user identification systems. In particular, we need to understand how the general information security literature applies to the TO domain. We will generate additional recommendations that are tailored for the TO environment as needed.

7.1 Field Visits

In March 2005, we visited multiple TO facilities to better understand the current operational requirements of user identification systems in use. Findings from those visits are available in Part 2 of this report (Allendoerfer & Pai, 2005). The existing literature on the human factors of information security can be difficult to apply to the TO domain, especially to TO tasks that are different from traditional IT and systems that are not computers.

We examined and categorized the user identification systems, policies, and practices currently used by TO personnel. We were interested in obtaining operational information that potentially has human factors implications. This included information pertaining to the work environment, the number of systems accessed by each user, the number of different passwords used, password selection criteria across different systems and sites, frequency with which users access systems, common causes and consequences of authentication problems, and user acceptability of identification systems.

7.2 Proposed Demonstration of Recommendations

The objective of the overall project is to examine identification systems from a human factors perspective and to develop recommendations for the TO environment. Some of these recommendations involve the implementation of new policies or technology. However, before a recommendation can be pursued further by the FAA, a demonstration of the feasibility or suitability of the recommendation may be necessary.

Existing recommendations for identification technologies in other domains, especially those aimed at mitigating human factors issues, may or may not apply directly to the TO environment. For example, a fingerprint scanning system may work very well in an office environment but its success on a radar tower is not known. Alternately, we may recommend that password policies allow users to include meaningful initials in their passwords to make them easier to recall. However, recall may depend on factors such how often users access the system, length of the password, and number of different passwords memorized by the users. A demonstration of the recommended technology or practice will help us better understand the implications of our recommendations.

At the same time, the feasibility of the recommendation needs to be assessed. For example, a policy change to allow users to include meaningful initials in their passwords may mean reprogramming of the system databases, and this could be very tedious or expensive. In addition, the management and administrative staff may be requested to provide feedback on the recommendations.

7.3 Revisions to the Human Factors Design Standard (HFDS)

The HFDS (Ahlstrom & Longo, 2003) is a comprehensive compilation of human factors practices and principles integral to the procurement, design, development, and testing of the FAA systems, facilities and equipment. Although the HFDS includes guidelines for use of passwords, it does not cover other forms of identification such as biometrics or token-based systems and their relative advantages. Research findings from this study may be incorporated in the HFDS so that other FAA as well as non-FAA systems may use them as a guideline for selecting identification systems for use in authentication.

References

Activewave RFID Applications & Solutions. (2004). *RFID applications and solution - Airport security*. Retrieved July 12, 2004, from http://www.activewaveinc.com/applications_airport_security.html

Adams, A., & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM, ACM 42*, 41-46.

Ahlstrom, V., & Longo, K. (2003). *Human factors design standard* (HF-STD-001). Atlantic City International Airport, NJ: Federal Aviation Administration, William J. Hughes Technical Center.

Ahlstrom, V., & Muldoon, R. (2003). *Function key and shortcut key use in airway facilities* (DOT/FAA/CT-TN03/07). Atlantic City International Airport, NJ: Federal Aviation Administration, William J. Hughes Technical Center.

Allendoerfer, K., & Pai, S. (2005). *Human factors considerations for passwords and other user identification techniques part 2: Field study, results and analysis* (DOT/FAA/CT-05/27). Manuscript in preparation.

Baddeley, A. D. (1990). *Human Memory: Theory and Practice*. Boston, MA: Allyn & Bacon.

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

Boroditsky, M., & Pleat, B. (2001). Security at the edge: Making security and usability a reality with SSO. *Passlogix, Inc*. Retrieved June 2, 2004, from www.activetechs.com/solutions/ security/sso/security_at_the_edge.pdf

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

Brostoff, S., & Sasse, M. A. (2002). Safe and sound: A safety-critical approach to security. *Proceedings of the New Security Paradigms Workshop 2001 (NSPW 01), 2001*, 41-50.

Brown, A., Bracken, E., Zoccoli, S., & Douglous, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology, 18*, 641-651.

Carstens, D., McCauley-Bell, P., & Malone, L. (2000). Development of a model for determining the impact of password authentication practices on information security. *Proceedings of the International Ergonomics Association /Human Factors and Ergonomics Society 44th Annual Meeting,44,* 342-345. .

Coventry, L., Angeli, A., & Johnson, G. (2003). Usability and biometric verification at the ATM interface. *Proceedings of the 2004 Conference on Human Factors in Computing Systems,* 153-160.

Cranor, L., & Garfinkel, S. (2004). Secure or usable? *IEEE Security and Privacy, 2*(5), 16-18.

Cyota Online Service Stats. (2005). *Key online services statistics*. Retrieved March 8, 2005, from http://www.cyota.com/product_1_15.asp

Dhamija, R., & Perrig, A. (2000). *Déjà Vu: A user study using images for authentication*. Retrieved March 8, 2005, from http://www.sims.berkeley.edu/%7Erachna/papers/usenix.pdf

Ernst & Young. (2004). *Global information security survey*. Retrieved March 8, 2005, from http://www.ey.com/global/download.nsf/Austria/2004_global_info_sec_survey/$file/2004_Global_Information_Security_Survey_2004.pdf

Fox, N., Gross, R., Chazal, P., Cohn, J., & Reilly, R. (2003). Person identification using automatic integration of speech, lip, and face experts. International Multimedia Conference. *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications,* 25-32.

International Biometric Group. (2002). *One face in 6 billion*. Retrieved July 18, 2004, from http://www.biometricgroup.com/in_the_news/discover.html

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*, 91–98.

Jones, C. (2003). *Social engineering: Understanding and auditing*. Retrieved March 28, 2005 from http://www.sans.org/rr/whitepapers/engineering/

Miller, B. (1994). Vital signs of identity. *IEEE Spectrum*, *31*, 22-30.

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

National Center for State Courts. (2002). *Individual biometrics - Retinal scans*. Retrieved July 27, 2004, from http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html

National Institute of Standards and Technology. (1985). Password usage. *Federal Information Processing Standards Publication 112*. Washington, DC: Author.

Neumann, P. (2000). Risks to public in computers and related systems. *ACM SIGSOFT Software Engineering Notes, 25,* 15-23.

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004, October). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. *Proceedings of the ACM Special Interest Group in Information Technology Education 2004 (SIGITE ’04) Conference*, 177-181.

Pinkas, B., & Sander, T. (2002). Securing passwords against dictionary attacks. *Proceedings of the 9th ACM Conference on Computer and Communications Security, 9*, 161-170.

Proctor, R., Lien, M., Schultz, E., & Salvendy, G. (2000). Human factors in information security methods. *Proceedings of the International Ergonomic Association/Human Factors and Ergonomic Society 44th Annual Meeting*. San Diego, CA.

Rainbow Technologies. (2003, June). *Password survey results*. Retrieved March 28, 2005 from http://mktg.rainbow.com/mk/get/pwsurvey03

RealUser Corporation. (2005). *Passfaces* [Computer software]. Retrieved from http://www.realuser.com

Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' - A human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*, 122-131.

Turner, A., & Blackburn, D. (2002). Biometrics: Separating myth from reality. *Corrections Today*, *64*, 140-141.

Vanguard Password Reset. (2003). *Reducing costs by allowing authorized users to reset forgotten passwords*. Retrieved July 19, 2004, from http://www.techsearch.co.kr/products/WP_passwordreset.pdf

Weinshall, D., & Kirkpatrick, S. (2004). Passwords you'll never forget but can't recall. *Proceedings of the 2004 Conference on Human Factors in Computing Systems*, 1399-1402.

Weirich, D., & Sasse, M. (2001). Persuasive password security for the real world. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI2001)*, 2001, 139-140.

Weirich, D., & Sasse, M. (2002). Pretty good persuasion: A first step towards effective password security for the real world. *Proceedings of the New Security Paradigms Workshop 2001*, 137-143.

Westin, A. (2002, December). Biometrics in the mainstream: What does the U.S. public think? *Privacy and American Business Newsletter, 9*(8), (Available from the Center for Social & Legal Research, 2 University Plaza Suite 414, Hackensack, NJ 07601)

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (In press.). *The memorability and security of passwords*. Retrieved March 8, 2005, from http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf

Acronyms

AFSS	Automated Flight Service Stations
ARTCC	Air Route Traffic Control Center
ATCT	Air Traffic Control Towers
ATM	Automated Teller Machine
ATO	Air Traffic Organization
BT	British Telecommunications
COTS	Commercial Off-the-Shelf
FAA	Federal Aviation Administration
HFDS	Human Factors Design Standard
NAS	National Airspace System
NOCC	National Operations Control Center
OCC	Operations Control Center
PDA	Personal Digital Assistant
PIN	Personal Identification Number
RFID	Radio Frequency Identity
TO	Technical Operations
TRACON	Terminal Radar Approach Control