Human Factors Considerations for User Identification on Air Traffic Control Systems

Kenneth Allendoerfer
Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City Int'l Airport, NJ 08405
+1-609-485-4864
kenneth.allendoerfer@faa.gov

Shantanu Pai
Titan Corporation
5218 Atlantic Avenue
Mays Landing, NJ 08330
+1-609-625-5669
spai@titan.com

Vicki Ahlstrom
Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City Int'l Airport, NJ 08405
+1-609-485-5643
vicki.ahlstrom@faa.gov

ABSTRACT

The Federal Aviation Administration (FAA) airway facilities (AF) workforce maintains the automation, surveillance, navigation, and communications systems that make up the National Airspace System (NAS). NAS systems employ a variety of user identification techniques and policies which place cognitive and social pressures on the AF workforce. This poster describes ongoing FAA research examining the human factors issues AF personnel face in the use of information technology (IT) security. Issues include the number of passwords personnel must remember, the complexity and frequency by which passwords must be changed, and employee accountability. This poster provides an analysis of ways in which the AF environment, tasks, and users differ from the common IT environment described in the literature. We discuss ways that these differences may affect decisions regarding passwords and other IT security techniques.

1. INTRODUCTION

The Federal Aviation Administration (FAA) provides air traffic control (ATC) services in the United States. The National Airspace System (NAS) includes automation, communication, navigation, and surveillance systems that are maintained by specialists from FAA Technical Operations Services, commonly known as airway facilities (AF). AF specialists certify, monitor, and control NAS equipment to ensure that it is available for pilots and controllers and provides accurate and reliable information.

Because the NAS affects aviation safety, national security, and the nation's economy, access to NAS equipment is closely monitored and controlled. However, the various systems were acquired by the FAA at different times, from many vendors, and built to meet a variety of requirements. There are many AF facilities, each with some autonomy to determine its own information technology (IT) security policies and practices. As a result, AF specialists use a variety of user identification techniques and technologies and follow numerous different procedures.

The consequences for forgetting a password or losing a token can be serious in terms of lost productivity, effort spent resetting passwords or obtaining new tokens, and in the potential for intrusion and outages. AF specialists 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. Specialists also feel social pressures that affect whether or not they follow secure password techniques such as concerns about identity, trust, and accountability. As a result these pressures, AF specialists 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.

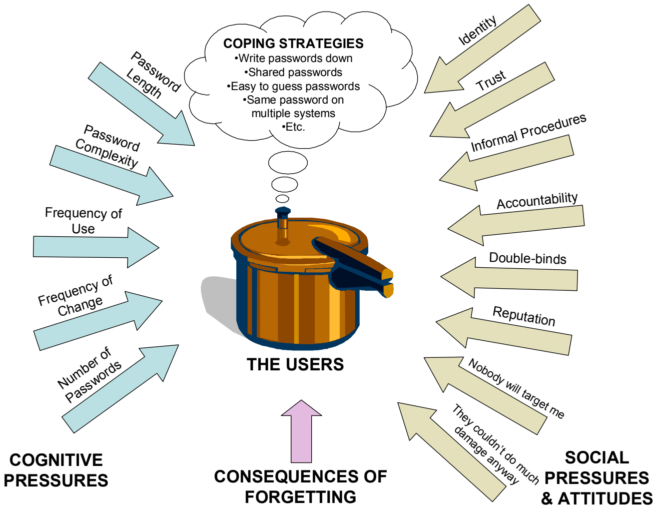

Figure 1. Pressures on AF users regarding passwords.

The purpose of our ongoing research is to examine the human factors aspects of user identification in general, relate these to the AF tasks, environment, and user characteristics, and develop recommendations.

2. SPECIAL CONSIDERATIONS

The existing research on the human factors aspects of passwords, tokens, and other IT security techniques usually examines corporate IT environments that utilize standard hardware and software, well-known user interfaces, and common tasks. This research applies to AF in many respects but there are also numerous differences that must be considered.

First, AF is a very large and diverse operation. AF personnel are responsible for more than 44,000 pieces of equipment at over 6,000 locations. Most NAS systems were custom built for the FAA using specialized hardware and software often during eras with lower expectations for IT security. The equipment may not accommodate all possible technologies or policies. AF specialists may be required to set up passwords for different systems following different procedures and requirements.

Second, a breach of security that allows an intrusion or an outage of the NAS could cost lives. AF personnel provide 24-hour service but not all facilities are staffed at all times and different authorization levels may be needed at different times of day. Because many AF maintenance actions are time critical, user identification systems must work extremely quickly and reliably.

Third, AF personnel may work with as many as 25 different systems during a single shift, each with its own user interface and IT security requirements. Moving frequently between systems increases the cognitive pressure on specialists and their workload in managing passwords.

Fourth, AF personnel often work at locations far from their home office. Returning to the office to repair a malfunctioning token or reset a forgotten password may not be feasible, especially when the specialist is working to accomplish a safety- or time-critical maintenance action.

Fifth, some AF specialists regularly work in postures and environments that are not well suited to existing IT security techniques. For example, a maintenance procedure may require a specialist to stand on a ladder to access a radar antenna. Specialists also may work in outdoors under bad weather and lighting conditions. They may need to wear gloves or other protective clothing. Environments such as these make typing passwords difficult and providing a biometric scan unsafe or impossible. This reduces the number of user identification options that can be considered.

3. RECOMMENDATIONS

The following recommendations are based on recommendations from the existing human factors in IT security literature and on our analysis of how the existing literature applies to AF.

3.1 Training and Awareness

Some in the IT security literature recommend increasing training on password security and launching awareness campaigns [3] and we endorse those recommendations. However, we caution AF against expecting large, quick increases in compliance or overall security due to increased training and awareness. We could not locate evidence showing that more training would substantially improve users' IT security behavior in the long run. In AF, many of these behaviors are entrenched and result from deeper organizational issues. In general, AF specialists know the rules and understand the consequences but they willfully break the rules because of the powerful cognitive and social pressures.

3.2 Enforcement and Testing

Increasing enforcement of policies and consequences for violations may improve overall IT security. From a human factors perspective, however, increased enforcement is likely to have little effect on the cognitive pressures that specialists feel and have a mixed effect on the social pressures. It is likely to increase specialists' sense of accountability but it may also strengthen an us-versus-them dynamic between field personnel and the headquarters organizations that set policy.

We advocate that AF take a softer approach by instituting non-punitive security testing following the so-called white hat approach. For example, a white hat attacker might email AF specialists and attempt to obtain their passwords. The results of the attack could then be presented to the employees as an illustration of the importance of secure practices. Unfortunately, such attacks are expensive to conduct and the organization would still be left with how to fix the problems.

3.3 Fewer Passwords

Some of the IT security literature argues that using one password to access two or more systems is a very bad idea [2]. Doing so allows a single security breach to affect multiple systems instead of one. We believe, however, that having dozens of passwords creates unacceptable cognitive pressure on users. If AF specialists must remember more than five or six different passwords, they will inevitably write them down regardless of what the official policy says. Writing passwords down increases the risk for future security breaches.

In our opinion, AF can improve overall security by allowing passwords to be used on multiple systems. This reduces the cognitive pressure on users and will allow the remaining logins to be made more complex, change more frequently, or use an identification technique other than passwords, such as graphical passwords, challenge questions, tokens, or biometrics.

3.4 Mnemonics

Passwords can be recalled more easily if users have the freedom to add meaningful data to them. For example, Carstens, McCauley-Bell and Malone [1] found that when passwords contained meaningful data, such as users' first and last initials, the recall rate increased from 50% to 72%. Interestingly, these passwords met stringent complexity guidelines. Participants were better able to recall the passwords because meaningful data in the passwords could be grouped and chunked together. AF policies may need to be amended to allow for password requirements that permit use of meaningful data for the user but that still allow complex passwords. Mnemonics can be very effective in improving recall. Unfortunately, many AF specialists do not know about mnemonics and have no experience applying them. Providing AF personnel with practical tips on ways to improve their memories for passwords may have beneficial effects.

4. REFERENCES

[1] 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.

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

[3] 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.