Human Factors of Security Systems: A Brief Review

Andrew Patrick, National Research Council of Canada
(Andrew.Patrick@nrc.ca)

DRAFT

March 19, 2002
Version 1.5

This paper is a working document that summarizes what I have been reading. Most of the ideas and findings come from the work of Angela Sasse and her students at University College London (UCL; http://www.cs.ucl.ac.uk/staff/A.Sasse). This paper will be revised and expanded as I learn more. Comments and discussion are welcome.

Introduction

The human factor is often described as the weakest part of a security system and users are often described as the weakest link in the security chain. In this paper, I review some of the literature on the human factors of security systems and suggest that, rather than blaming users, we should understand the roles and demands placed on them by security systems (Adams & Sasse, 1999). By taking a "root cause" approach, the reasons behind user behaviors can be understood and solutions to security problems caused by human behavior can emerge. The focus of this paper is on password-based access systems, but I also touch upon Public Key Infrastructures (PKI) and the role of computer operators in security problems.

Securing System Access

All security access methods are based on three fundamental pieces of information: who you are, what you have, and what you know (Brostoff & Sasse, 2000). If users can provide proof in some or all of these areas, they are admitted to the system. Most login procedures require users to provide information in two of these authentication areas, and there are various options for the information required. For proving who they are, users can provide their name, email address, or a user ID. Since this information provides no assurance of identity, some system operators are beginning to employ biometrics (such as fingerprints, voice recognition, iris scans, or retinal scans) as methods of user identification. For proving what they have, users can produce service cards (i.e., ATM cards), physical keys, digital certificates, smart cards, or one-time login cards such as the SecurID card (http://www.rsasecurity.com/products/securid/). For proving what they know, users can provide a password or pass phrase, or a personal identification number (PIN). This information is essentially a secret that is shared between the user and the system. A knowledge technique that has been explored recently is to use recognition memory. For example, the Passfaces system requires people to recognize chosen faces from a matrix of random pictures (see below).

Using Passwords

The most common login procedure is for the user to provide a user ID and a shared secret password that they have chosen. Users have been described as the weakest link in security systems because of their behavior when using user ID/password systems. Many studies have shown, for example, that users tend to choose short and/or guessable passwords (Adams & Sasse, 1999). This makes security systems quite vulnerable to crack attacks, where common passwords and dictionary words are tried until a password is broken. In 1998, for example, CERT reported finding a cache of 186,126 account entries with encrypted passwords stolen from a variety of systems, and the intruder had been able to guess 47,642 (26%) of the passwords with a password-cracking tool (http://www.cert.org/incident_notes/IN-98.03.html).

Another very common problem is that users forget their passwords. One estimate is that 50 percent of all help desk calls are password related, and most of these are because a password has been forgotten (Murrer, in Brostoff & Sasse, 2001). Password reset rates have been estimated as one reset per every four or five users per month (Brostoff & Sasse, 2000). The implications of this are large. For example, in a corporation that has 100,000 users this represents about 25,000 resets a month. If each reset takes five

minutes to complete, 12 full-time staff would be needed just to handle the resets. This is obviously a large expense. (The worst time for forgotten passwords is after holidays.)

Probably because of the difficulty remembering, users also have a tendency to write their passwords down. In one study, 50 percent of the user surveyed admitted to writing down their passwords, and the other 50 percent did not answer the question (Adams & Sasse, 1999). Moreover, it is not just novice users who exhibit this behavior. Ronald Reagan carried the authentication codes for the nuclear "football" (a military briefcase that never leaves his side) in his pocket, and lost them during his attempted assassination. Also, Jimmy Carter left his codes in a suit that he sent to the dry cleaners.

Other notorious password behaviors are: (1) users share their passwords with their friends and colleagues, (2) users fail to change their passwords on a regular basis even when instructed to, (3) users may choose the same password (or closely related passwords) for multiple systems, and (4) users are often willing to tell their passwords to strangers who asked for them (asking was the most common technique use by Kevin Mitnick in his infamous security exploits; Sasse, Brostoff, & Weirich, 2001).

Moving Beyond Blame

Before declaring that users are the enemy, we should consider why they do these things. What are users being asked to do that seems to be so difficult? What are they capable of doing? What have they been taught? Simply blaming the users and declaring the problems to be "human error" ignores the causes of the errors and the role of technology in forcing or preventing those errors (Brostoff & Sasse, 2001). This blame approach is similar to the abandoned "human error" approach to airline pilot incidents. In many cases where it appeared that pilot errors were the cause of accidents it was found that the pilots behaved as they did because: (1) the design gave wrong cues about the cause of the problem, (2) they were presented with impossible cognitive or physical tasks, (3) they had insufficient knowledge, or (4) they had insufficient training. Moving away from blaming the pilots towards developing planes and control systems that take into account the pilots' needs and limitations has gone a long way towards improving flight safety. The same approach is required for security systems. Rather than being the main cause of security problems, users are often the inheritors of system defects, poor designs, incorrect installations, faulty operation, and bad management (Brostoff & Sasse, 2001). A careful analysis of the characteristics of security systems from the human factors point of view can be useful for improving the effectiveness of the systems.

One significant demand placed on users of security systems is a requirement to remember multiple passwords. Users are often faced with remembering dozens of passwords or PINs, but human memory is brief and easily confused. A recent study of British Telecom workers revealed that an average of 16 passwords were required for workers to do their jobs (Sasse, Brostoff, & Weirich, 2001). Human memory is also optimized for meaningful content presented in context, while user IDs and passwords are often unrelated and meaningless. Obviously, this high cognitive stress is bound to lead to problems.

Rarely used passwords are easily forgotten. One study show that 60 percent of the problems with infrequently used passwords was forgetting (Sasse, Brostoff, & Weirich, 2001). Also, similar user IDs and passwords can lead to confusion, and this is the most common problem for medium-use passwords. PINs, four or six digit numbers, are particularly difficult to remember and are easily confused even when used frequently (Sasse, Brostoff, & Weirich, 2001).

Another related human factors problem is the content of passwords. Users are supposed to create passwords that cannot be guessed. However, our memory systems are particularly weak at remembering meaningless content. In addition, users are sometimes forced to change their passwords often and rapidly, usually being told that their password has expired and they must change it "now". This pressure to choose passwords quickly means that users may fail to store the new passwords in their memories. It is also difficult to forget old passwords -- we don't forget on command. One study showed that 13 percent of all PIN problems come immediately after a PIN change, and this problem increases with frequently used PINs (Sasse, Brostoff, & Weirich, 2001). These problems occur when users are asked to forget one password and start using another one. In addition, the password content rules can differ between systems (e.g.,

accepting digits only, 8 characters, 14 characters, or up to 127 characters) adding to user confusion during password creation.

Password systems are often not compatible with day-to-day work practices. Users may need to work quickly and this means they need to get their passwords reset quickly if they forget them. If a quick, 24-hours-a-day password reset service is not available, it is no wonder that users choose to write their passwords down. There may also be serious consequences to forgetting passwords such as loss of time, prestige, or the ability to login to a system at all if a three-strikes rule is in place (after three failed login attempts, the user is locked-out of the system). Users may also be working in groups that need to share files and resources. If mechanisms to support information sharing within groups are not in place, users may be forced to share passwords. The result of all of these factors is that for many users the feeling is that security gets in the way of "real work".

The Security Culture

There may also be problems related to the social perceptions and attitudes of the organization towards security. For example, some studies have shown that security-conscious people may be perceived as paranoid or not trusting (Sasse, Brostoff, & Weirich, 2001). Obviously, this may reduce users' willingness to conform to rigorous security requirements.

Individual users may also feel that they are not vulnerable to security attacks. They may feel that they are insignificant and that an attacker would not target them. They may also feel that no one knows anything about them so their passwords can be something familiar, such as their child's name. In addition, they may feel that their information is not important or sensitive and therefore not worthy of protection. Another common attitude is that their account might be vulnerable but it does not affect the entire system (Sasse, Brostoff, & Weirich, 2001).

There are other organizational issues that affect the users interactions with security systems. If password sharing or writing down passwords is common practice in an organization, it will reinforce the behavior of any individual. If administrators routinely ask users for passwords when conducting system maintenance, they may be creating an atmosphere of open password sharing. Also, if the physical security systems are flawed, users may feel that password rules are futile. Finally, Sasse, Brostoff, & Weirich (2001) have documented that some senior users may feel that they are too important to have to deal with such trivial things as passwords and security systems.

Solutions

There are solutions to the security issues caused by the behavior of users, but they are not commonly used (see Adams & Sasse, 1999, for an excellent review). To avoid memory problems caused by multiple unique IDs, organizations can issue each user a single login ID for use on all systems. To alleviate the problem of a remembering multiple passwords, organizations can support synchronized passwords across systems. There may be some reluctance to do this since it means that if one system is compromised all the systems are compromised. However, administrators may have to choose between one strong password used on multiple systems, or many weak passwords, or passwords that are written down somewhere. Having one common password may actually result in a more secure system. A related solution is a single-sign-on system where users are authenticated once and then they are allowed to access multiple systems.

System operators should also be careful about forcing password changes. The number of changes should be kept to a minimum and users should be forewarned about upcoming changes so that their password choice can be well thought out. This will allow users to choose strong passwords and give them time to rehearse and encode the passwords so they are remembered later.

Users should also be educated about their password choices. System operators should clearly explain the password content rules and rationale behind them. User should be given information about how password-guessing schemes work, in particularly how they search for common passwords and dictionary words (Adams & Sasse, 1999). Systems should also check passwords as they are created so that users get

immediate feedback about the quality of the passwords they are choosing. Users can also be taught a technique for generating strong passwords from easily remember phrases (e.g., the phrase "Microsoft is an evil empire!" can be converted into the password "MS-ev1l_emp!").

Another technique is to reduce the memory load placed on users. It is well known that cued recall, where users are prompted for the information they must remember, is more accurate than free recall (Crowder, 1976). This can be used in security systems by requiring personal associates for passwords, such as "dear - god, "black - white", "spring - garden". Performance can also be improved by not asking users to recall at all, but rather to recognize certain material. Recognition is much easier and more accurate than recall (Preece, 1994). This recognition method is used in the "v-Go" system, where users are presented with a visual scene and must remember which objects to click in which particular order. A similar system is "Déjà vu", where a panel of random images is presented to the user and they must select the right images in the correct order. Finally, in the Passfaces system users are presented with 36 faces and they must correctly pick the four faces they have chosen earlier as their "password". There is some evidence, summarized in Figure 1, that Passfaces are easier to remember than passwords, especially after long intervals with no use (Brostoff & Sasse, 2000).

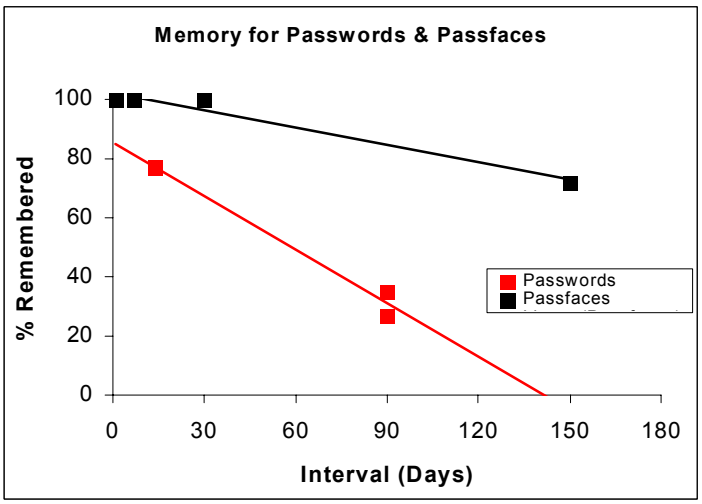

Figure 1: Memory for Passfaces and Passwords
(adapted from Brostoff & Sasse, 2000)

Brostoff & Sasse (2000) recently followed-up these impressive laboratory results with a three-month trial of the Passfaces system. They found that the Passfaces system had a lower reset rate than traditional passwords. However, Passfaces performed quite slowly on older machines because of the intensive graphic operations when presenting the faces, causing significant login delays and user frustrations. Overall, these recognition-based access systems seem promising. However, it is not clear if confusion problems will return when systems like Passfaces are employed widely and users must remember multiple, similar visual cues for multiple systems.

Security administrators should also consider alternatives to the traditional user ID and password pair. For example, deploying physical keys such as smart cards may be particularly useful for situations were passwords are used rarely.

A solution to the user behavior of sharing passwords is to support group accounts and group file permissions as appropriate. This is easily done in some operating systems such as a Unix.

Organizations can also change the social perceptions regarding security. Organizations can increase security awareness by publishing incident reports and explaining the policies in place and the rationale behind those policies. They can also explain the potential impact of security problems on both a personal and economic level. Organizations should also reward security-conscious behavior and punish security

infractions. This should be done proactively, by doing things such as routinely checking for weak passwords, rather than waiting for incidents to happen.

There has been much interest recently in using biometrics, such as fingerprints or voice patterns, for user identification (Jain, Hong, & Pankanti, 2000; Rejman-Greene, 2001), but these systems can have their own problems. Biometrics can be hard to forge but easy to steal (Schneier, 1999). For example, fingerprints can be lifted from objects and used when the owner is not present. Also, the master file of biometric templates can be compromised so that an intruder could replace a legitimate thumbprint file with their own. If the integrity of a biometric has been compromised (e.g., a thumbprint file has been widely distributed) it makes the biometric system unusable forever. Also, a biometric security network can be compromised by packet sniffing and insertion, where an illegitimate biometrics file is inserted in place of a legitimate one that is being transmitted.

Biometrics systems can be based on physical characteristics, such as fingerprints, or behavioral characteristics, such as voice patterns (Markowitz, 2000) or typing styles (Joyce & Gupta, 1990). The performance of behavioral biometrics (in terms of correction rejections and false acceptances) can be affected by circumstances such as health, stress, and other factors. Also, at least one behavioral biometric system, the one based on typing styles, appears to be less acceptable to users, who are afraid that their work performance may be monitored in some way (Brostoff & Sasse, 2000).

Public Key Infrastructure (PKI)

Some proponents have argued that public key infrastructure (PKI) systems may avoid some of the problems caused by user behaviors. However, these systems still depend on the proper behavior of users for various crucial activities (Davis, 1996). For example, the certification authority must authenticate users in a suitable manner, such as a physical identification check. Failures in this authentication process are well known, such as when VeriSign issued Microsoft certificates to an imposter. Also, public key systems require that users authenticate each public key before they use them. Users of PKI systems must also keep their local computer physically secure and protect their private key. Finally, the PKI system is only as good as the pass phrase chosen by the user, and this can have all of the same password problems discussed above.

PKI systems can also suffer from serious usability problems. One study (Whitten & Tygar, 1999) investigated the usability of PGP (Pretty Good Privacy) software and found a number of problems: (1) users did not understand the visual metaphors used for certifying and encrypting, (2) users did not understand the different key types (RSA and Diffi-Helman/DSS), (3) users were not aware of, or did not know how to use, the key server, (4) users did not understand the "validity" and "trust" attributes of keys, and (5) users did not understand what key to encrypt with. Furthermore, the system under test had a number of irreversible actions, such as accidentally deleting private keys, accidentally publishing or revoking keys, or forgetting the pass phrase. The ultimate result of these problems was that, when given a task to send an encrypted, certified e-mail, 25% of the users sent the secret message with no protection.

System Operators as Users

Human factors problems are not restricted to end-users. System operators are also human and therefore have limitations and the potential to make mistakes. Perhaps the most serious behavioral problem of system operators is poor implementation of the system. This may be due to failure to understand the security technology, and/or failure to implement all of the necessary features. In one study, failures during installation and feature selection were the most common sources of security problems in the banking and government sectors (Anderson, 1993).

Another problem seen with system operators is poor operating procedures. This includes not keeping the system up-to-date, not responding to security notices, badly managing their own passwords, cost-cutting, and simple laziness. An interesting research area might be an analysis of factors that contribute to inappropriate system operator behaviors. Finally, operator fraud can be a serious problem in situations where security compromises can lead the financial gain (Anderson, 1993).

Conclusions

Users of password systems are notorious for many bad behaviors, including choosing easily guessed passwords, forgetting their passwords, writing them down, or telling them to friends and strangers. There are often valid reasons for these behaviors, however, and a careful review of the demands being placed on the users and the limitations of human performance can explain some of the unwanted actions. The system characteristics and the nature of the work environment are also important for determining how security systems are used and abused. By adopting a "root cause" approach, system developers and operators can move beyond blaming users towards developing security systems that users can actually use.

References

Adams, A., & Sasse, M.A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM, 42*, 41-46.

Anderson, R. (1994). Why cryptosystems fail. *Communications of the ACM, 37*, 32-40.

Brostoff, S., & Sasse, M.A. (2000). Are Passfaces more usable than passwords? A field trial investigation. *In Proceedings of HCI 2000*, Sept. 5-8, Sunderland, U.K., 405-424 Springer.

Crowder, R.G. (1976). *Principles of learning and memory*. Hillsdale, NJ: Lawrence Elrbaum Associates.

Davis, D. (1996). Compliance defects in public-key cryptography. *Proceedings of the 6th Usenix Security Symposium*, San Jose, CA, 1996, 171-178.

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

Joyce, R., & Gupta, G. (1990). Identity authentication based on keystroke latencies. *Communications of the ACM, 33*, 168-176.

Markowitz, J.A., (2000). Voice biometrics. *Communications of the ACM, 43*, 66-73.

Preece, J. (1994). *Human-computer interaction*. NY: Addison-Wesley.

Rejman-Greene, M. (2001). Biometrics -- Real identities for a virtual world. *BT Technology Journal, 19*, 115-121.

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

Whitten, A. & Tygar, J.D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 9th USENIX Security Symposium*, August 1999. http://www.cs.cmu.edu/~alma/johnny.pdf