USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords.

ANNE ADAMS AND MARTINA ANGELA SASSE

The key element in password security is the crackability of a password combination. Davies and Ganesan [3] argue that an adversary's ability to crack passwords is greater than usually believed. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed (because users do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password lifetime*—changing passwords frequently—is suggested as reducing the risk associated with undetected compromised passwords. Finally, *password ownership*, in particular individual ownership, is recommended to:

- Increase individual accountability;
- Reduce illicit usage;
- Allow for an establishment of system usage audit trails; and
- Reduce frequent password changes due to group membership fluctuations.

QUENTIN WEBB

There is evidence that many password users do not comply with these suggested rules. DeAlvare [1] found that once a password is chosen, a user is unlikely to change it until it has been shown to be compromised. Users were also found to construct passwords that contained as few characters as possible [2]. These observations cannot be disputed, but the conclusion that this behavior occurs because users are inherently careless—and therefore insecure—needs to be challenged.

The Study

A Web-based questionnaire was used to obtain initial quantitative and qualitative data on user behaviors and perceptions relating to password systems. The questionnaire focused mainly on password-related user behaviors (password construction, frequency of use, password recall and work practices) and in particular memorability issues. A total of 139 responses were received, approximately half from employees of Organization A (a technology company), the other half from users in organizations throughout the world. There was a wide range of frequency and duration of password use among respondents. The questionnaire was followed by 30 semistructured in-depth interviews with a variety of users in Organization A and Organization B (a company in the construction sector). Interview questions covered password generation and recall along with systems and organizational issues raised by respondents in the questionnaire. The interview format allowed participants to introduce new issues to the discussion that they regarded as related to password usage. Results from the open-ended sections of the questionnaire were brought together with results from the in-depth interviews to give a wide sample for analysis.

The analysis, using a social science based method called *Grounded Theory* [10], provided a framework of issues affecting user behavior, with a step-by-step account of password usage problems and possible intervention points. Four major factors influencing effective password usage were identified within the framework:

- Multiple passwords;
- Password content;
- Perceived compatibility with work practices; and
- Users' perceptions of organizational security and information sensitivity.

Because the findings from the study are too numerous to discuss in detail here, key points of interest from each factor are presented.

Many users have to remember multiple passwords, that is, use different passwords for different applications and/or change passwords frequently due to password expiration mechanisms. Having a large number of passwords reduces their memorability and increases insecure work practices, such as writing passwords down—50% of questionnaire respondents wrote their passwords down in one form or another.[1] One employee emphasized this relationship when he said "…because I was forced into changing it every month I had to write it down." Poor password design (for example, using "password" as the password) was also found to be related to multiple passwords. "Constantly changing passwords" were blamed by another employee for producing "…very simple choices that are easy to guess, or break, within seconds of using 'Cracker'.[2] Hence there is no security." It is interesting to note here that users, again, perceive their behavior to be caused by a mechanism designed to increase security. At the same time, users often devise their own procedures to increase password memorability and security. Some users devise their own methods for creating memorable multiple passwords through related passwords (linking their passwords via some common element)—50% of questionnaire respondents employed this method. Many users try to comply with security rules by varying elements in these linked passwords (name1, name2, name3, and so forth). However, rather than improving memorability and security, this method actually decreases password memorability due to within-list interference [11], causing users to write down passwords which, of course, compromises password security levels.

Users' knowledge of what constitutes secure password content (the character content of the password) was inadequate. Without feedback from security experts, users created their own rules on password design that were often anything but secure. Dictionary words and names are the most vulnerable forms of passwords, but many users do not understand how password cracking works. Members of the security department in Organization A were appalled to discover that one of their employees suggested: "I would have thought that if you picked something like your wife's maiden name or something then the chances of a complete stranger guessing *********, in my case, were pretty remote."

At the same time, restrictions introduced to create more secure password content may produce less memorable passwords, leading to increased password disclosure (because users write passwords down).

[1]The response was the same for all users who answered these questions—the other 50% of users left these questions blank.
[2]A password dictionary checker.

Many users circumvent such restrictions to produce passwords they find easy to remember. However, the resulting passwords tend to be less secure in terms of content. Even worse, having to circumvent security procedures lowers users' regard for the overall security arrangements in the organization, which, in turn, increases password disclosure.

Another new finding of this study is the importance of compatibility between work practices and password procedures. Organization A employed individually owned passwords for group working that users perceived as incompatible with their working procedures (they advocated shared passwords for themselves). Users in Organization B experienced this incompatibility in reverse: they emphatically rejected the departmental policy of group passwords for individual personal information (such as email).

One reason why Organization A insisted on individual passwords was to establish the users' perception of accountability through audit trails of system usage. We found, however, that most users had not considered the possibility that their actions might be tracked. It is telling that the only user who made the connection cheerfully revealed that he avoided being tracked by using other users' passwords for certain transactions, so that "…if there's any problem, they get it in the neck, not you."

The study clearly showed that users are not sufficiently informed about security issues. This causes them to construct their own model of possible security threats and the importance of security and these are often wildly inaccurate. Users tend to be guided by what they actually see—or don't. As one manager stated: "I don't think that hacking is a problem—I've had no visibility of hacking that may go on. None at all." Another employee observed that "…security problems are more by word of mouth…". This lack of awareness was corroborated by results from the Web questionnaire. A complex interaction between users' perceptions of organizational security and information sensitivity was identified. Users identified certain systems as worthy of secure password practices, while others were perceived as "not important enough." Without any feedback from the organization, users rated confidential information about individuals (personnel files, email) as sensitive; but commercially sensitive information (such as customer databases and financial data) was often seen as less sensitive. Some users stated that they appreciated printed document classifications (for example, *Confidential, Not for Circulation*), indicating their need for information sensitivity guidance and rules for levels of protection in online documentation.

Two main problems in password usage were identified: *system factors*, which users perceive they are forced to circumvent, and *external factors*, which are perceived as incompatible with working procedures. Both these problems are due to a lack of communication between security departments and users: users do not understand security issues, while security departments lack an understanding of users' perceptions, tasks, and needs. The result is that security departments typecast users as "inherently insecure": at best, they are a security risk that needs to be controlled and managed, at worst, they are the enemy within. Users, on the other hand, perceive many security mechanisms as laborious and unnecessary—an overhead that gets in the way of their real work.

Insufficient communication with users produces a lack of user-centered design in security mechanisms.

Users Lack Security Knowledge

Parker [9] points out that a major doctrine in password security, adopted from the military, is the *need-to-know* principle. The assumption is that the more known about a security mechanism, the easier it is to attack; restricting access to this knowledge therefore increases security. Users are often told as little as possible because security departments see them as "inherently insecure." One clear finding from this study is that inadequate knowledge of password procedures, content, and cracking lies at the root of users' "insecure" behaviors.

Both Organizations A and B had replaced system-generated passwords with user-generated ones, thus shifting the responsibility for creating secure passwords to the users. However, known rules for creating secure passwords were rarely communicated to users. Users were asked to complete a skilled design job without adequate training or online feedback. This problem was compounded by the security departments' implicit need-to-know policy on the sensitivity of particular information, potential security breaches, and risks. Users perceived threats to the organization to be low

because of their own judgments of the information's lack of importance or visible threats. This misunderstanding led to the general misconception that password cracking is done on a "personal" basis. They perceived the risk to be low because their role in the system was not important. Organization A decided to provide online support and feedback to users in the process of password design; a cracker program was installed, with constructive advice provided on secure password design for all users whose password was cracked. Online information on threats to password security ("Monthly security report and update") is also being considered.

Finally, we found that users do not understand the authentication process, confusing the user identification (ID) and password sections. Many users assumed IDs were another form of password to be secured and recalled in the same manner. This increased users' perception of the mental workload associated with passwords, which then reduced their motivation to comply with the suggested behavior. The IDs, within the organizations investigated, could have caused this misconception by having no standardized format for different applications and often being non-words without meaning. In response to this finding, Organization A decided to introduce a single sign-on for users with a high number of passwords and is considering the use of smart cards as an identification mechanism. User authentication using physical attributes (biometrics) does not require ID recall, and thus offers a mechanism with reduced mental overhead. The main drawback of these methods is the cost of both installation and monitoring. Organizations also have to consider whether the level and consequences of "false positive" alarms are acceptable to their business. Finally, there is a question of how to combine the specialized equipment required for such methods with remote access to systems, which is an increasing requirement in an age of nomadic professionals.

Security Needs User-Centered Design

Insufficient communication with users produces a lack of a user-centered design in security mechanisms. Many of these mechanisms create overheads for users, or require unworkable user behavior. It is therefore hardly surprising to find that many users try to circumvent such mechanisms.

Requiring users to have a large number of passwords (for multiple applications and change regimes) was found to create serious usability problems. Although change regimes are employed to reduce the impact of an undetected security breach, our findings suggest they reduce the overall password security in an organization. Users required to change their passwords frequently produce less secure password content (because they have to be more memorable) and disclose their passwords more frequently. Many of the users felt forced into these circumventing procedures, which subsequently decreased their own security motivation. Ultimately, this produces a spiraling decline in users' password behavior ("I cannot remember my password, I have to write it down, everyone knows it's on a post-it in my drawer, so I might as well stick it on the screen and tell everyone who wants to know.") Organization A was understandably worried to discover such attitudes, as social engineers rely on password disclosure, low security awareness and motivation to breach security mechanisms. The cost associated with resetting passwords in Organization A was one of the visible consequences, prompting the study that is the basis for this article. Recognizing the impact that cognitive overheads introduced by some password mechanisms have on users' security motivation, the security and human factors groups in Organization A have joined forces to develop a user-centered approach to the design of password and other security mechanisms. Such approaches will also have to take into account that the number of passwords required outside the workplace is constantly growing thus increasing the cognitive load of users.

Motivating Users

A technical bias toward security mechanisms has produced a simplistic approach to user authentication: restricting access to data by identification and authentication of a user. This simplistic approach may work well in military environments, but limits usable solutions to the security problems of modern organizations seeking to encourage work practices such as teamwork and shared responsibility. Such organizations require support for trust and information sharing. The authoritarian approach has also led to security departments' reluctance to communicate with users with regard to work practices. It has been suggested by the U.S. Federal Information Processing Standards (FIPS) [5] that individual ownership of passwords increases accountability and decreases illicit usage of passwords, because of the possibility of audit trailing—a byproduct of authentication. However, both of these assumptions rely on users' perceptions which, as previously mentioned, do not always comply with those of the security departments. FIPS [5] also suggests that shared passwords for groups are insecure. This study has identified that—when users perceive they are using shared passwords for work carried out in a team—this may increase their perceptions of group respon-

sibility and accountability. If a password mechanism is incompatible with users' work practices, they perceive the security mechanism as "not sensible" and circumvent it (for example, by disclosing their password to other group members). This can lead to a perception that *all* password mechanisms are "pointless," circumventing all of them and decreasing overall security. This does not mean that individual passwords should not be used in organizations with team-based working; it is worth considering protecting access to shared information with a shared password while leaving individual passwords for individual activities. The increased mental load of an additional shared password may cause less problems than the spiraling decline in security behavior caused by "incompatible" mechanisms.

It is important to challenge the view that users are never motivated to behave in a secure manner. Our results show that the majority of users were security-conscious, as long as they perceive the need for these behaviors (for example, because of obvious external threats or the perceived sensitivity of the information protected). These findings are supported by research within Organization B, where both physical and computer security levels were low and security threats were evident to users. In this situation, users demonstrated exemplary behavior with their own passwords. We argue that the need-to-know principle should be jettisoned. The main argument of its proponents is that by informing users about the rationale behind security mechanisms, along with real and potential threats to security, they may be lowering security by increasing the possibility of information leaks. This attitude has led to a twofold problem: (a) users' lack of security awareness, and (b) security departments' lack of knowledge about users, producing security mechanisms and systems that are not usable. These two factors lower users' motivation to produce secure work practices. This in turn reinforces security departments' belief that users are "inherently insecure" and leads to the introduction of stricter mechanisms, which require more effort from users. This vicious circle needs to be broken. Communication between security departments ands users is therefore often restricted to "ticking off" users caught circumventing the rules. This approach does not fit with modern distributed and networked organizations, which depend on communication and collaboration. Users have to be treated as partners in the endeavor to secure an organization's systems, not as the enemy within. System security is one of the last areas in IT in which user-centered design and user training are not regarded as essential—this has to change.

Users and Password Behavior

Insecure work practices and low security motivation have been identified by research on information security as major problems that must be addressed [2, 3, 6, 7]. The research presented here does, however, clearly identify the cause of these user-related problems; in the sidebar "Recommendations" we summarize methods for addressing these problems. There is an implicit assumption that users are not inherently motivated to adopt secure behavior, but that such behavior can be achieved through drills and threats of punishment in case of non-compliance. Knowledge from psychology and human-computer interaction indicates that users' behavior is likely to be more complex than a simple conditioned response. This study demonstrates that users forced to comply with password mechanisms incompatible with work practices may produce responses that circumvent the whole procedure. Insecure work practices and low security motivation among users can be caused by security mechanisms and policies that take no account of users' work practices, organizational strategies, and usability. These factors are pivotal in the design and implementation of most computer systems today. Designers of security mechanisms must realize that they are the key to successful security system. Unless security departments understand how the mechanisms they design are used in practice, there will remain the danger that mechanisms that look secure on paper will fail in practice. C

It is important to challenge the view that
users are never motivated to behave in a secure manner.

References

1. DeAlvare, A.M. A framework for password selection. In *Proceedings of Unix Security Workshop II*. (Portland, Aug. 29–30, 1998).
2. DeAlvare, A.M. How crackers crack passwords or what passwords to avoid. In *Proceedings of Unix Security Workshop II*. (Portland, 1990).
3. Davis, C. and Ganesan, R. BApasswd: A new proactive password checker. In *Proceedings of the National Computer Security Conference '93, the 16th NIST/NSA conference*. 1993, 1–15.
4. Davis, D. and Price, W. *Security for Computer Networks*. Wiley, Chichester, 1987.