Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security

M A Sasse, S Brostoff and D Weirich

The security research community has recently recognised that user behaviour plays a part in many security failures, and it has become common to refer to users as the 'weakest link in the security chain'. We argue that simply blaming users will not lead to more effective security systems. Security designers must identify the causes of undesirable user behaviour, and address these to design effective security systems. We present examples of how undesirable user behaviour with passwords can be caused by failure to recognise the characteristics of human memory, unattainable or conflicting task demands, and lack of support, training and motivation. We conclude that existing human/computer interaction knowledge and techniques can be used to prevent or address these problems, and outline a vision of a holistic design approach for usable and effective security.

1. Introduction

With the exponential growth of networked systems and applications such as eCommerce, the demand for effective computer security is increasing. At the same time, the number and seriousness of security problems reported over the past couple of years indicates that organisations are more vulnerable than ever. In many of the reported cases, user behaviour enabled or facilitated the security breach. The security research community — which hitherto largely ignored the human factor — now acknowledges that:

> '... security is only as good as it's weakest link, and people are the weakest link in the chain.' [1]

The opposition recognised and exploited this state of affairs earlier. Kevin Mitnick, arguably the world's most famous hacker, testified to the US Senate committee that he had obtained more passwords by tricking users than by cracking. In his new role as security evangelist, he never ceases to point out that:

> '... the human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain.' [2]

The first implication of this new perspective on security is that the traditional security approach — to address the problem by developing ever more complex technology — is not sufficient. We agree with this conclusion. However, labelling users as the 'weakest link' implies that they are to blame. In our view, this is a repeat of the 'human error' mindset that blighted the development of safety-critical systems until the late eighties [3]. Consider the following examples of users violating password rules.

- Ambushing

  A user is told that his password has expired, and he must change it immediately or be locked out of the system — he feels stumped, and ends up choosing his wife's name. This is exploited by a colleague who wants to look at files he has no permission to access. He tries out the user's family members' names to get into the system, and succeeds. Many password systems 'ambush' users without warning. People have difficulty designing and memorising strong passwords, and they have even more difficulty under pressure.

- Conflicting goals

  An aircraft designer needs to access six different systems; company policy states she must have a different password for each. The system only accepts strong passwords, and requires a change each month. Recently, she was reprimanded by her boss for missing an important deadline — she worked on a Sunday but could not get to some files because she could not recall the right password and could not get help. She now keeps a note with her current passwords under her mouse mat, where an industrial spy working as a contract cleaner finds it and uses the passwords to download confidential design drawings. The security

mechanism and policy created an impossible memory task (at least without instructions or training). When failure at the memory task interfered with her work, the organisation failed to recognise and address it. The user was left with two conflicting goals and forced to relegate security to second place.

- Requested disclosure

  A hacker calls company employees and tells them that he works for IT support and needs their password to update some programs on their machine. Since no admin accounts have been set up on many PCs in this company, IT support staff often need to ask users for their passwords when they want to get into these machines. This is a contextual issue — if systems are set up so users are regularly asked to disclose their passwords, it is difficult for them to distinguish in which context disclosure is safe, and when it is not.

These examples illustrate issues that are often overlooked in security design. As Adams and Sasse [4] pointed out, security has largely ignored usability issues; many users of security systems face unattainable or conflicting demands, and receive no support or training. A human/computer interaction (HCI) design approach takes into account that users and technology work together completing a task (in order to achieve a goal) in a physical and social context. Any specific user, technology, task and context may bring constraints to the design problem. In the remainder of the paper, we systematically examine the following issues involved in security design, and outline how HCI knowledge can be employed to address them:

- technology,
- user,
- goals and tasks,
- context.

While these issues can affect any security mechanism, we are using examples from our research on one specific mechanism — passwords — to illustrate them. Our recommendations are based on an analysis of the relevant literature, and empirical findings from the following four studies.

- Study 1

  By use of questionnaires, 144 BT employees (half at management grade or above) were asked both to describe the cause of the last password problem they encountered that led to a password reset, and also to report their number of overall passwords at work and how they used them.

- Study 2

  This study analysed six months of password reset logs from the BT password helpdesk.

- Study 3

  In-depth interviews on attitudes to passwords were conducted with 17 users (10 were BT employees, 6 were PhD students at UCL, and one a systems administrator working in finance). The interviews lasted between 30 and 60 minutes and were subsequently transcribed for analysis.

- Study 4

  32 students used a Web-based system to practise and submit assessed coursework [5]. System logs of the passwords and passfaces (see section 3.1) used allowed us to study not only frequency of logins and login failures, but also what caused the wrong selection.

2. Technology

There are five ways to authenticate users (see Rejman-Greene [6]); most security mechanisms use a two-step procedure in which identification and authentication are combined. An example of such a combination are cash cards (token-based identification) combined with a PIN (knowledge-based authentication). By far the most common access control mechanism in computing is the combination of a userid (identification) and password (authentication).

Most password systems are implemented in the same way.

- Userid and password

  The mechanism issues a userid for every new user, and also a password (which can be changed by the user to one of their choice). The password is supposed to be a secret shared between the user and the computer only, it should not be disclosed or written down.

- Log-on

  To log on, the user has to enter their userid and password, which the system processes and compares to the entries it has stored. If it finds a match, the user will be given access to the computer system, but if there is no match, the user will not be allowed access, and may have to contact a system administrator to have a new password issued. Many systems suspend an account after 3 or 5 unsuccessful login attempts, and bar further attempts until the account has been re-set.

From a technical point of view, the password mechanism is a low-cost option, the risks of which are well understood. It is also a mechanism with which many users are familiar. However, there are also a number of usability issues connected to its use.

- Number of passwords

  Password mechanisms are usually implemented on a per-system basis. This means that users need to log into each password-protected system individually; the time required to log into a number of systems several times a day can add up. Some operating systems store userid and password and automatically use it on the user's behalf (for example to mount remote volumes).

- Password policies

  The growing number of systems with which users have to interact creates memory problems (see section 3.1). The problem is often exacerbated by password policies, usually based on the Federal Information Processing Guidelines [7]. These rules state, for instance, that:

  — passwords must be strong, i.e. a pseudo-random mixture of letters, numbers and characters,

  — users should have a different password for each system,

  — passwords should be changed at regular intervals, and accounts of users who do not comply deleted or suspended.

- Varying systems

  There is great variability of userids and passwords across different systems, e.g. Unix takes up to 8 characters, Windows 95/98 up to 14, and Windows 2000 up to 127. Some systems have highly elaborate content restrictions (e.g. "there must be at least three non-letter characters in the password, and letter 4, 5, or 6 must be such a character"), but these vary from system to system.

The result is a huge demand on users' memory:

- users not only have to remember passwords, but also the system and userid with which it is associated,
- users have to remember which password restrictions apply to which system,
- users have to remember whether they have changed a password on a particular system, and what they have changed it to.

It is thus not difficult to accept that many users cannot cope. As a result, the cost of re-setting passwords has reached significant levels in BT and elsewhere. In response to rising cost and user protests, many organisations give users permission — or even direct them — to write their passwords down and keep them in a safe place. This violates the first principle of knowledge-based authentication — that the password should exist only in two places — in the system (in encrypted form) and the users' mind.

A technical solution to reduce the number of passwords is a single sign-on (SSO) login system, which many companies are starting to deploy. This reduces not only users' memory load, but also the total amounts of time users spend on logins. If SSO is not feasible (e.g. because of cost), allocating users a single userid for all systems, standardising password rules, and enforcing them consistently, can improve the situation somewhat. Most security policies decree that users should have different passwords for different systems, to limit the number of systems compromised if an unauthorised person gets hold of a password. From a usability point of view, allowing users to have the same password on different systems is desirable because it increases frequency of use and memorability (see section 3). Ultimately, this makes for more effective security because it gives users a chance to have strong passwords they can remember, and a strong password reduces the chances of it being compromised in the first place.

3. User

3.1 Memorability issues

The user characteristic that has the primary impact on password design is memorability. There is a huge body of research on human memory, but the most important issues related to passwords can be summarised as follows:

- the capacity of working memory is limited,
- memory decays over time — this means people may not recall an item, or not recall it 100% correctly,
- recognition of a familiar item is easier than unaided recall,
- frequently recalled items are easier to remember than infrequently used ones, and retrieval of very frequently recalled items becomes 'automatic',
- people cannot 'forget on demand' — items will linger in memory even then they are no longer needed,
- items that are meaningful (such as words) are easier to recall than non-meaningful ones (sequences of letters and numbers that have no particular meaning),
- distinct items can be associated with each other to facilitate recall — however, similar items compete against each other on recall.

Knowledge-based authentication mechanisms, such as passwords, require users to memorise items and recall them when accessing a specific system. Asking users to recall a single password and userid for one system may seem reasonable, but with the proliferation of passwords, users are increasingly unable to cope.

Password problems

Before study 2 (the analysis of password resets), BT security staff believed that the rising number of password resets was due to a small number of careless 'repeat offenders' — by their own definition, employees who ask for a reset 6 or more times a month. Study 2 found that 91.7% of resets were caused by 'normal users', i.e. more than 90% of users cannot cope with the password mechanism in the way they were expected to, which is a rather damning result in terms of usability of password mechanisms. The study also found that 30% of the 'repeat offender' helpdesk calls could be traced back to temporary staff, and were largely due to administrative (rather than memory) problems.

Study 1 (BT employee questionaires) is the first systematic study of passwords in a population of real users during their normal work. The average number of passwords per user was 16. We asked users to describe the cause of their last password problem, as well as the frequency with which they used the password. The responses were then categorised according to these frequencies into three groups — light use (from once per year to just under once a month), medium use (from once a month to once a day) and heavy use (used more frequently than once a day). The results are shown in Fig 1. Our data supports the findings from the Web survey by Adams et al [8], in which users reported that infrequently used passwords are the ones that are most often forgotten.

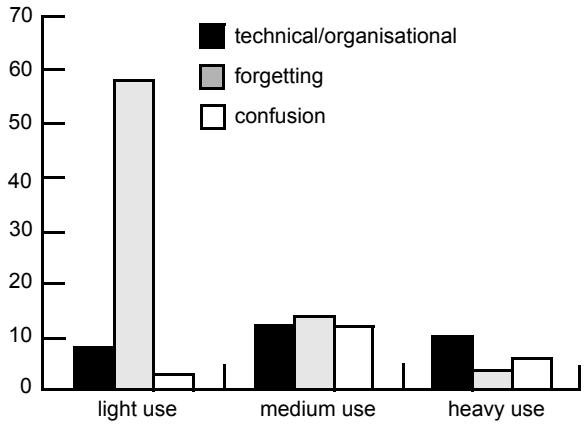

Fig 1 Frequency and cause of problems with passwords.

Study 1 also demonstrated the effect of password content. Figure 2 illustrates problems with a voicemail system using a six-digit PIN. The proportion of reported incidences where this PIN could not be remembered was very high — even when it was moderately or heavily used. While frequently used computer passwords can be recalled after periods of non-use, even heavily used PINs are forgotten after short periods of non-use.

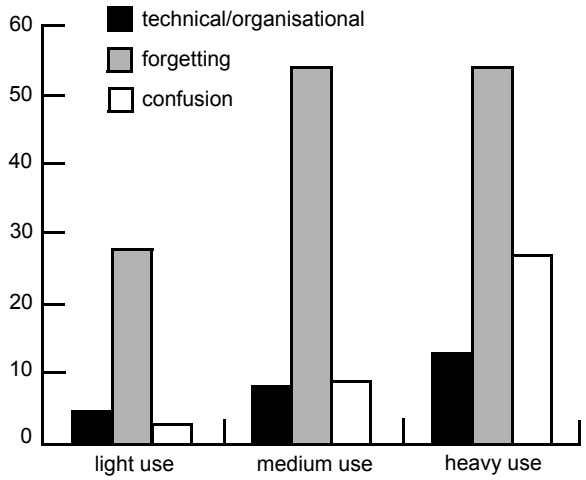

Fig 2 Frequency and causes of problems with a 6-digit PIN.

In the discussion to date, login failure has been usually described as 'users forgetting passwords'. Studies 3 and 4 found, however, that users hardly ever drew a complete blank — the login usually failed because:

- they recalled the password partly, but not 100% correctly,
- they recalled a different password from the one required, i.e. a previously used password for the same machine, or a password for a different machine.

This shows the basic memory mechanisms (described above) in action — items decay in memory unless they are frequently recalled, and recall of similar items causes interference. The likelihood of 100% correct recall of infrequently used items is extremely low. This means that a password mechanism that demands 100% accurate recall every time is an extremely bad match for infrequently used systems. That the results for 6-digit PINs are even worse confirms the importance of password content. It also indicates that a token-PIN combination, often touted as a more usable replacement for passwords, is likely to cause more problems with infrequently used systems than a standard password.

Heavy- or medium-use passwords were more often confused than lightly used passwords (see Fig 1). Heavily used passwords were more often confused than they were forgotten, and PINs are more frequently confused with each other than passwords (see Fig 2). Frequency of execution is one of the key considerations when matching technology to users' tasks (see section 4), but has to date rarely been taken into account in security. Our findings provide a powerful argument that existing mechanisms are a bad match for systems that are not accessed on a daily basis, and that this causes the vast majority of password problems.

The results from studies 1 and 2 suggest that the other major cause of password resets are forced password changes. 13% of all reported password problems occurred just after changing a PIN. Moreover, the more frequently the PIN was used, the more problems occur after changing it. Approximately the same number of problems occurred just after changing medium and heavily used passwords, whereas there were fewer problems with infrequently used passwords. There has been no systematic investigation of the impact of forced password changes on numbers of resets and password strength. The studies reported in this paper provide some evidence that they make a significant contribution to password problems. The qualitative data in study 3 suggests that password quality declines with frequency of forced changes — as users become increasingly desperate in their quest for a password or PIN that stands out, their choices become more guessable.

Can passwords be strong **and** memorable?

Both security [1] and usability experts [9] have stated that recalling strong passwords is a humanly impossible task because strong passwords are non-meaningful items and hence inherently difficult to remember. However, what makes a password easy to guess or crack is the fact that it is meaningful to many other people, as well as the password owner. It is possible to create passwords that are strong and meaningful — pseudo-random combinations of letters, numbers and characters that are meaningless to anyone but the password owner/creator. Many systems administrators use system-generated passwords for maximum security, and generate a sentence that describes, for instance, their opinion of a particular character in Star Trek (e.g. m,1aNib7 becomes 'Me, I am NOT impressed by SevenofNine'). They can manage a reasonable number of passwords by having different themes for different systems. For heavily used passwords, these pass algorithms seem to work well [10]. Zviran and Haga [11] obtained good recall results using a similar method with ordinary users, by giving them instructions to concatenate several words and interspersing them with characters for user-generated passwords (e.g. BF$gat0 for Black Forest Gateau). As part of our own research, we have incorporated a related set of rules into an on-line password tutorial. We have not completed an objective performance test (in terms of password strength and recall rates), but have received feedback that these rules helped users with password construction ('finally, I have a way of generating passwords the system will accept!') and recall.

Alternative knowledge-based authentication systems

One of the most fundamental HCI principles is to avoid unaided recall wherever possible, since it is known to place a considerable burden on users' cognitive load and overall ability to perform. There are authentication mechanisms that use cued recall and recognition, for example:

- composite weak authentication — many banks ask their customers to identify themselves by providing several weak but memorable items — this method may be used in combination with a password, and/or as a back-up method if the password has been forgotten,
- cognitive passwords [12] involve a series of questions about the user's personal preferences and history — after a certain number of correct answers, the user is considered to have passed authentication,
- associative passwords [11] employ word pair or phrase associations in a similar manner (e.g. Dear-God, Spring-Step, Black-White) while avoiding word association stereotypes — Ellison et al [13] refer to systems such as these that use the contents of episodic memory as employing personal entropy,
- the pass sentence mechanism [14] is an unaided recall mechanism in the first place — however, if the user does not get the secret completely right, the user is prompted with questions about the pass sentence, and when the user answers enough questions correctly, login is allowed.

Systems based on recognition of visual items for authentication have received much attention recently:

- v-GO® [15] presents users with a visual scene — to authenticate, the user clicks on certain objects in the scene in particular order, and is then able to create a story using the objects in the scene, a mnemonic technique which aids the user in recalling the correct sequence of objects (v-GO® appears to have had only cursory analytic evaluation),
- both Deja Vu [16] and Passfaces™ [17] present users with panels of images, from which they have to recognise and select their pass images, the most significant difference between the two systems being the content of the images — Deja Vu employs randomly generated art, while Passfaces uses photographs of strangers' faces in an attempt to exploit people's ability to process and remember faces.

These systems have performed well in laboratory-style tests, producing recall rates of up to 80% even after up to 3 months of non-use [18, 19]. However, these results must be treated with caution because users in these trials were given one set of cues — this means there are no similar cues with which to confuse them. Unpublished trials with multiple cues indicate that problems similar to those with passwords occur when users are given several similar visual clues, or have to change them. In addition, the graphics involved in these systems require significant bandwidth and processing resources; when these are not present, login time can increase significantly, which in turn interferes with users' tasks (see section 4).

3.2 User knowledge and motivation

Adams and Sasse [4] investigated users' perceptions of password mechanisms to identify the human and organisational factors that can have an impact on the security and usability of password mechanisms. They found that many users' knowledge was shockingly inadequate, which leads to them constructing their own, often wildly inaccurate models of possible security threats and the importance of security. This, in turn, gives rise to a wide variety of user behaviour that is undesirable in terms of security. Studies 1 and 3 confirmed this state of affairs. It is therefore not surprising that 'user education' has appeared on top of the to-do list of many security departments. However, this will require more than pushing documents to users.

From the task perspective (see section 4), security is an enabling task, i.e. one that needs to be completed in order to be able to perform the main task. Authentication is an enabling task that needs to be completed to get to the resources required to do real work. It is easy to see that for many users today, security is something that gets in the way of real work, especially when mechanisms are difficult to use, and/or the need for security is not obvious. Users have to be motivated to make the additional effort that is required to use security mechanisms properly. Small business or home users can be motivated to a certain extent by education about the risks of not bothering with security. This allows them to make an informed choice about their behaviour, based on an assessment of the risks to them personally and the effort required to reduce these risks. This is different for large organisations (see section 5). Users are generally less concerned about security of their organisation's computer systems, and often choose to follow existing policies only selectively or not at all.

In order to develop effective means of educating and motivating users with respect to password mechanisms, we tried to understand the mindset of users at which such measures will be targeted. In study 3, we identified 7 issues that lead to undesirable password behaviour.

- Identity issues

  People who exhibit good password behaviour are often described as 'paranoid', 'pedantic' or 'the kind of person who doesn't trust anybody' —even by themselves. Some participants are proud of the fact that they do not understand security ('I'm not a nerd'), or do not comply with regulations ('I don't just follow orders').

- Social issues

  Sharing your password is considered by many users to be a sign of trust in their colleagues — you share your password with people you trust, and somebody refusing to share their password with you is effectively telling you that they do not trust you. The same goes for other password-related behaviour, such as locking your screen when you leave your computer for a few minutes — you are telling your colleagues next to you that you do not trust them.

- 'Nobody will target me'

  Most users think the data stored on their system is not important enough to become the target of a hacker or industrial spy. Hackers, for example, are assumed to target 'rich and famous' people or institutions. Some users accept that hackers might target somebody like them just to get into the overall system and try to get further from there, but clearly do not regard this as very likely, purely because of the number of users that could be targeted this way.

- 'They could not do much damage anyway'

  Most users do not think that somebody getting into their account could cause any serious harm to them or their organisation.

- Informal work procedures

  Current password mechanisms and regulations often clash with formal or informal work procedures (e.g. if you get ill and cannot come in, somebody in your group should be able to access your account and take care of your customers).

- Accountability

  Most users are aware that their behaviour does not fully comply with security regulations. However, they do not expect to be made accountable because they regard the regulations as 'unrealistic' and their behaviour as 'common practice'. In addition, they know that there is always a chance that a hacker will break into their system, however well they behave. They can always claim that it was not their misbehaviour that led to the break-in. Some users realise that they might be held accountable for past behaviour (e.g. writing down their password) if somebody gets into their system now.

- Double-binds

  If a computer system has strong security mechanisms, it is more likely to come under attack from hackers who want to prove themselves, and who will in the end find a way to get in. If it has weak security, inexperienced hackers who try to break into many systems without targeting one specifically might get in. Similarly, if you follow rules (e.g. lock your screen), people will think you have valuable data on you computer, and are more likely to try to break in. If you do not follow regulations, it is easier for somebody to break in.

An additional interesting result of study 3 was that there are users who show good behaviour even though they are of the opinion that this is not necessary. They follow regulations because they perceive it as necessary to maintain their professional reputation, or because they believe that any security failure involving their employer would ultimately reduce its standing in the business world. This insight provides a potential basis for further educational and motivational measures. A more drastic approach would be to link organisational security to users' personal data, by providing access to payroll, health records and personal email — all users in study 3 stated such data was worthy of good security behaviour.

4. Goals and tasks

Consideration of user's goals and tasks is the key element of a user-centred approach to design. Technology is not an end in itself, but should work in tandem with users to achieve an individual's or organisation's goals; these goals need to be identified to ensure that user/system interaction is designed to be effective, i.e. produces the required output. Goals are achieved through the completion of tasks; technology designers study tasks to ensure that user/system interaction is designed to be efficient, i.e. can be completed as quickly as possible and without waste of resources. An analysis of goals and tasks typically identifies:

- the goals (desired output),
- fundamental tasks (without which the desired output cannot be achieved),
- enabling tasks (which have to be completed in order to be able to carry out a fundamental task),
- performance criteria for each task (e.g. speed of completion, maximum number of errors),
- frequency with which each task is carried out,
- resources required by users and technology to carry out the task.

The insights gained through such analysis provide essential input into the design process. Fundamental tasks, for instance, are given priority in terms of visibility and feedback, and frequent tasks need to be particularly efficient in execution. Another fundamental principle of good design is to apportion tasks to users and technology in line with their strengths and weaknesses (e.g. limitations of human memory, see section 3.1).

4.1 Tasks and passwords

Many of the problems users have with security mechanisms can be explained in terms of a bad match between the mechanisms and users' goals and tasks. Users' behaviour is essentially goal-driven. If the benefits of an enabling task are not obvious to users, they will view it as something that gets in the way of completing the fundamental task, and find ways of cutting it out if possible. The studies by Whitten and Tygar [20] and Adams and Sasse [4] described this phenomenon for PGP encryption and password mechanisms, respectively. Whether or not it is possible to bypass an enabling task, the extra effort required will foster resentment in users, and feed the perception that security is 'not sensible' because it interferes with real work. This, in turn, reduces user motivation (see section 3.2), which in the longer terms leads to an erosion of security culture (see section 5.2).

All our studies provided evidence of how badly matched password mechanisms currently are to users' capabilities and their tasks. This is because password mechanisms, and the policies that govern their use, are currently designed and chosen as general mechanisms to protect access to systems, and without reference to the work that is being performed. Infrequently used passwords, for example, would be better served by a mechanism that does not require 100% accurate recall of strong memory items, i.e. accepts partly successful authentication, a combination of weak items, or relies on recognition (see section 3.1). More tolerant mechanisms would also work better in conjunction with high-speed, high-pressure tasks, which have an increased likelihood of user slips.

Current mechanisms generally do not acknowledge the cost of authentication failure for fundamental tasks. Users and organisations can suffer significant losses as a result of not being able to access a system needed for a fundamental task because of authentication failure. If there is no contingency when legitimate users are unable to gain access, they are left to invent their own, such as borrowing a colleague's password — there was plenty of evidence for this in studies 1 and 3. There may be help desks or system administrators, but if a re-set takes 15 mins to complete, and an important customer wants a quote now, this is not a valid contingency.

Consequently, security must be designed as an integral part of the system that supports a particular work activity in order to be effective and efficient. Decisions about system and file access must be based on how tasks and workflow are organised in the real world. In modern organisations, many tasks are assigned to teams, and teamwork and collaboration are encouraged. If users are then given individual passwords, and unable to access each other's files even though they are needed for shared tasks, password disclose will become common. Finally, a task-centred design recognises that support resources, such as instructions and help, need to be available at the point where users need them. Instructions for constructing and memorising a strong password, for instance, should be available when a password needs to be chosen or changed

— and the instructions, as well as labels on any tools, need to be compatible with users' vocabulary [20].

5. Context

An effective and efficient design of a user/technology interaction will be largely determined by the goals of that interaction and the tasks required to complete it. Beyer and Holtzblatt [21] identified a host of physical and social factors that need to be considered and accommodated to design an effective system. This section presents a number of points that are relevant to password security.

5.1 Physical environment

The physical environment in which password mechanisms are used can influence user behaviour. Adams and Sasse [4] found that if the physical security environment has obvious flaws, users may feel that it is not worth bothering with passwords ('after all, anyone can get in here'). A strong physical security environment can lead to complacency, which needs to be counteracted by reminding users of risks facing the organisation (see section 5.2).

Presence of others is an important consideration:

- users may worry about how they appear to others (e.g. 'paranoid', see section 3.2),
- many users become nervous when they feel observed by others, which can have a negative impact on their ability to recall and enter passwords accurately — many people feel under pressure when there is a queue of other users waiting to use a cash dispenser, for instance, and feel embarrassed that others can see they have a problem, perhaps feeling embarrassed because others:

  — can observe their ineptitude,

  — may assume that they are trying to gain access to something they are not entitled to.

5.2 Social and organisational environment — security culture

Study 3 provided in-depth data that showed that good password behaviour can lead to social repercussions (see section 3.2). Users who behave according to regulations are seen as 'paranoid' or 'pedantic', and anybody not willing to share their password with colleagues might be regarded as untrusting, and possibly even untrustworthy. All this points to an important area of further research. For effective security, organisations must develop a culture in which passwords are not only integrated into people's work (see section 4), but security is adopted as a shared concern by all employees. In many organisations, there is a wide gap between security policies and widespread insecure behaviour. Password rules that are unworkable in practice cannot be enforced and are thus not taken seriously; since security provides the rationale for password rules, it also ends up not being taken seriously. Highly paid key staff often feel that they are too busy to obey 'petty' password rules, and those in charge of security are often not in a position to enforce compliance from these staff. A sinister side-effect on security culture is that being able to flaunt password regulations becomes a badge of seniority.

The first step towards recovering security culture is to ensure that password mechanisms are not unworkable. Security design has to integrate all aspects of security, from the technical to the user interface and user training, with the organisation's work practices and overall culture. We believe that security policies, and the way in which they are presented and enforced, are a fundamental leverage point that makes it possible to move towards such an integration of security and overall organisational culture. However, it will take significant work in terms of user education and motivation to achieve a state where all members of the organisation accept their role in, and responsibility for, the security of an organisation. We have adapted the use of fear appeals [22] as a means of convincing users that good security behaviour also serves their own interest [23]. The main points of this approach are threefold.

- Impact of security on business

  Emphasise the importance of security for the organisation's business. Show how the organisation's reputation and business would be affected if it becomes known that employees engage in behaviour which, for instance, might endanger confidentiality of customer data. Most employees realise that lost business means jobs in danger. This gives the fear appeal (and the associated punishment) a rational motivation that will raise users' acceptance of it.

- Punishment

  Appropriately punish behaviour, not its consequences. Make it clear that you can not monitor all the employees all the time, but that you will make detailed enquiries about their past behaviour in case of a break-in through their account. This behaviour will definitely be punished, whether it led to the actual break-in or not.

- Security awareness

  Report security transgressions, rather than trying to keep them secret in an attempt not to lose face. Currently, there are few rewards for security-conscious behaviour; if regulations are to be taken seriously, failure to observe them must be dealt with, and seen to

be dealt with. This is effectively learning by negative reinforcement, which can only be effective if security failures are made known to users.

6. Conclusions

6.1 Do passwords have a future?

We have identified a considerable number of usability issues with password mechanisms. At the same time, our analysis has revealed that many problems are due to the way in which passwords are currently implemented.

- Single sign-on

  Organisations can fight password inflation by moving away from designing security on a per-system basis. SSO, a single userid, and password rules that are consistent across systems, can help achieve this. Also, security must be designed as an integral part of users' work, rather than get in the way.

- Reducing forced changes

  Judicious changes to password policies can make strong passwords manageable. Organisations can curb password inflation by reducing forced changes, and sanctioning use of the same password for several systems. In our view, this entails fewer risks than abandoning the cardinal principle of knowledge-based authentication and moving to wholesale writing down of passwords, as Schneier suggests [1]. Passwords that are written down are harder to protect than those that are memorised.

- Alternatives

  There are alternative mechanisms to the two-step password procedure which requires a strong item to be recalled, and these would be more suitable for infrequently used passwords.

- Password management

  There are techniques for designing and managing a certain number of strong passwords; these techniques need to be made available when users need them.

- User motivation

  User education will only work if users are motivated.

Nielsen [9] suggests that passwords are a usability nuisance that will be abolished by wide-scale introduction of biometric authentication. Biometric systems may be a good fit for some user/tasks/context configurations, but not all of them (see Rejman-Greene [6]). We predict that knowledge-based authentication, in a more appropriate form than today, will be used in the foreseeable future.

6.2 Does security need special usability?

Whitten and Tygar [20] suggested that security needs a usability standard that is different from those applied to 'general consumer software'. We disagree with this view — after all, Whitten and Tygar themselves used standard HCI methods to uncover the usability problems in the user interface of PGP. In this paper, we have outlined how existing HCI knowledge and tools, properly applied, would go a long way towards addressing usability issues in security.

If there are gaps in the HCI repertoire when it comes to designing usable security, they are in the area of:

- user motivation,
- a method that integrates the different aspects that affect usability of security.

We have adapted the fear appeals from cognitive therapy to make security instructions more persuasive [24], and are currently trialling policies, tutorials and user interfaces that incorporate persuasion. To devise a design method for the whole socio-technical system that is security, we are currently adapting Reason's framework [3] for the design and maintenance of safety-critical systems [23]. Safety and security protect the interests of both individuals and organisations in the long term. However, they also compete for resources with fundamental tasks in the short term, and are likely to be sacrificed for short-term gain. This tendency can only be overcome by making security a visible and integral part of an organisation's long-term goals and its daily activities.

Acknowledgements

The work reported in this paper is a result of a long-term collaboration with colleagues at BT, especially Marek Rejman-Greene in BTexact Technologies. Sacha Brostoff and Dirk Weirich were funded through BT/EPSRC Industrial CASE studentships.

References

1 Schneier B: 'Secrets and Lies', John Wiley and Sons (2000).

2 Poulsen K: 'Mitnick to lawmakers: People, phones and weakest links', (March 2000) — http://www.politechbot.com/p-00969.html

3 Reason J: 'Human Error', Cambridge University Press, Cambridge, UK (1990).

4 Adams A and Sasse M A: 'Users are not the enemy', Communications of the ACM, 42, No 12 (December 1999).

5 Brostoff S and Sasse M A: 'Are Passfaces more usable than passwords? A field trial investigation', in McDonald S et al (Eds): 'People and Computers XIV — Usability or Else', Proceedings of HCI, Sunderland, UK, pp 405—424, Springer (September 2000).

6 Rejman-Greene M: 'Biometrics — real identities for a virtual world', BT Technol J, 19, No 3, pp 115—121 (July 2001).

7 FIPS: 'Password Usage', Federal Information Processing Standards Publication (May 1985).

8 Adams A, Sasse M A and Lunt P: 'Making passwords secure and usable', in Thimbleby H et al (Eds): 'People and Computers XII', Proceedings of HCI'97, Bristol, Springer (August 1997).

9 Nielsen J: 'Security and Human Factors', Alertbox (November 2000) — http://www.useit.com/alertbox/20001126.html

10 Haskett J A: 'Pass-algorithms: a user validation scheme based on knowledge of secret algorithms', Communications of the ACM, 27, No 8, pp 777—781 (1984).

11 Zviran M and Haga W J: 'A comparison of password techniques for multilevel authentication mechanisms', The Computer Journal, 36, No 3, pp 227—237 (1993).

12 Zviran M and Haga W J: 'Cognitive passwords: the key to easy access control', Computers and Security, 9, No 8, pp 723—736 (1990).

13 Ellison C, Hall C, Milbert R and Schneier B: 'Protecting secret keys with personal entropy', — http://www.counterpane.com/personal-entropy.pdf

14 Spector Y and Ginzberg J: 'Pass sentence — a new approach to computer code', Computers and Security, 13, No 2, pp 145—160 (1994).

15 Passlogix® Inc — http://www.v-go.com/nav.asp?sec=company&loc=who

16 Dhamija R, Perrig A and Deja V: 'A User Study — Using Images for Authentication', Proceedings of the 9th USENIX Security Symposium, Denver, Colorado (2000).

17 Passfaces™ — http://www.idarts.com/

18 Valentine T: 'An evaluation of the Passface™ personal authentication system', (Technical Report) Goldmsiths College, University of London (1998).

19 Valentine T: 'Memory for Passfaces™ after a long delay', (Technical Report) Goldsmiths College, University of London (1999).

20 Whitten A and Tygar J D: 'Why Johnny can't encrypt: A usability evaluation of PGP 5.0', Proceedings of the 8th USENIX security composium, Washington (August 1999).

21 Beyer H and Holtzblatt K: 'Contextual design', Morgan Kauffmann (1997).

22 Rogers R W: 'A protection motivation theory of fear appeals and 22 change', The Journal of Psychology, 91, pp 93—114 (1975).

23 Brostoff S and Sasse M A: 'Safe and sound: a safety-critical design approach to security', to be presented at the 10th ACM/SIGSAC New Security Paradigms Workshop, Cloudcroft, New Mexico (September 2001) (in press).

24 Weirich D and Sasse M A: 'Pretty good persuasion: a first step towards effective password security for the real world', to be presented at the 10th ACM/SIGSAC New Security Paradigms Workshop, Cloudcroft, New Mexico (September 2001) (in press).

Martina Angela Sasse holds a Master's degree in Occupational Psychology and a PhD in Computer Science, and is currently a Reader in Interaction Design in the Department of Computer Science at University College, London. Her main areas of research are design and usability issues of ubiquitous multimedia systems. She has researched the usability aspects of security in collaboration with BT since 1996, and co-written several papers on the topic with her PhD students Anne Adams, Sascha Brostoff and Dirk Weirich.

Sacha Brostoff obtained a BSc in Phychology from Manchester University in 1995 and an MSc in Ergonomics from Birkbeck College, University of London, in 1996.

He is currently completing his PhD research (on the usability of authentication mechanisms) in the Computer Science Department at University College, London.

Dirk Weirich obtained a BSc in Computer Science with Cognitive Science from University College, London, in 1997.

He is currently completing his PhD research (on methods for improving user behaviour with password mechanisms) in the Computer Science Department at University College, London.