Making Passwords Secure and Usable

Anne Adams[1], Martina Angela Sasse[2] & Peter Lunt[3]

[1] *Department of Computer Science, UCL, Gower Street, London. WC1E 6BT*
tel no:- +44 171 419 3462
fax no:- +44 171 387 1397
Email :- A.Adams@cs.ucl.ac.uk
(Contact for correspondence on submission.)

[2] *Department of Computer Science, UCL, Gower Street, London. WC1E 6BT*
tel no:- +44 171 380 7212
fax no:- +44 171 387 1397
Email :- A.Sasse@cs.ucl.ac.uk

[3] *Department of Psychology, UCL, Bedford Way, London. WC1E 6BT*
tel no:- +44 171 387 7050 ext. 5401
Email :- p.lunt@ucl.ac.uk

To date, system research has focused on designing security mechanisms to protect systems access although their usability has rarely been investigated. This paper reports a study in which users' perceptions of password mechanisms were investigated through questionnaires and interviews. Analysis of the questionnaires shows that many users report problems, linked to the *number of passwords* and *frequency of password use*. In-depth analysis of the interview data revealed that the degree to which users conform to security mechanisms depends on their perception of *security levels, information sensitivity* and *compatibility with work practices.* Security mechanisms incompatible with these perceptions may be circumvented by users and thereby undermine system security overall.

Keywords : Security, Passwords, Grounded Theory, Organisational Factors

1 Introduction

Most organisations try to protect their systems from unauthorised access, usually through passwords. Considerable resources are spent designing secure authentication mechanisms, but the number of security breaches and problems is still increasing (DeAlvare, 1990; Gordon, 1995; Hitchings, 1995). Unauthorised access to systems, and resulting theft of information or misuse of the system, is usually due to hackers "cracking" user passwords, or obtaining them through social engineering. System security, unlike other fields of system development, has to date been regarded as an entirely technical issue - little research has been done on usability or human factors related to use of security mechanisms. Hitchings (1995) concludes that this narrow perspective has produced security mechanisms which are much less effective than they are generally thought to be. Davis & Price (1987) point out that, since security is designed, implemented, used and breached by people, human factors should be considered in the design of security mechanism. It seems that currently hackers pay more attention to human factors than security designers do. The technique of social engineering, for instance - obtaining passwords by deception and persuasion - exploits users' lack of security awareness. Hitchings (1995) also suggests that organisational factors ought to be considered when assessing security systems. The aim of the study described in this paper was to identify usability and organisational factors which affect the use of passwords. The following section provides a brief overview of authentication systems along with usability and organisational issues which have been identified to date.

1.1 Background

Confidentiality is a key element in information security, with user authentication as the main mechanism to obtain this (Parker, 1992). Authentication procedures have traditionally been divided into two different stages. *User identification* (User ID) initially identifies the user interacting with the system. As it is merely a means of specifying who the user is, this id does not have to be secured. At the second - *user authentication* stage - the user has to be verified as the legitimate user of the ID; the *password* used as the means of authentication has to be secret.

Originally, passwords were *system-generated* to ensure users employed "secure" combinations of characters. Most users, however, found these passwords hard to remember, and therefore tended to write them down. Furthermore, security risks were identified in the distribution of system-generated passwords. Both of these reasons have lead to *user-generated passwords* as the most widely used process for password production. In addition to one-word passwords, there are a number of other authentication mechanisms currently in use:

- Passphrases (phrase required instead of a word);
- Cognitive passwords (question-and-answer session of personal details);
- Associative passwords (a series of words & associations) and
- Personal Identification Numbers (PINs).

This paper investigates user-ID and user-generated passwords, the most widely-used password mechanisms. The level of security provided by this can vary greatly, depending on the individual user's password design expertise and security awareness. The US Federal Information Processing Standards (FIPS, 1985) suggest that there are several criteria that should be used to assure different levels of password security. *Password composition*, for example, relates the level of a password's security to the size of the character set from which it has been chosen. An alpha-numeric password is therefore more secure than one composed of letters only. Short *password lifetime* - i.e. changing passwords frequently - is suggested to reduce the risk associated with undetected illicit use of a "compromised" password. Finally, *password ownership* is noted as an important aspect of its security. The FIPS suggest that individual ownership:

- increases individual accountability;
- reduces illicit usage;
- allows establishment of system usage audit trails;
- reduces the requirement for frequent password changes dues to group membership fluctuations.

There is indeed evidence that many users do not follow secure password construction. DeAlvare (1988) found that once a password is chosen, a user is unlikely to change it until it has been

shown to be compromised. This research was continued in 1990 to show that, if allowed, most users will tend to construct passwords that contain as few characters as possible. These observations cannot be disputed, but the conclusion that these observed behaviours are due to users being inherently careless and therefore insecure ought to be reconsidered. Security departments try to counteract users' "inherently insecure" behaviour with system-based mechanisms such as password expiry and construction restrictions, assuming that forcing users to comply with security measures will reduce insecure behaviour. Again, the notion that desired behaviour can be enforced may work in a military environment, but this fits less well with modern organisations and work practices.

The guiding principles of system security have determined the type of security problems identified and their approach to possible solutions. The tendency is to respond to security problems by enforcing more restrictive authentication regimes, such as:

- increasing change regimes (change password once a month);
- longer and more complex passwords (alpha-numeric & required length);
- reduction in allowed input error rates.

Whether these mechanisms have resulted in more secure user behaviour has not been empirically confirmed. Anecdotal evidence suggests that their effect may be the opposite of what was intended: the more restrictive mechanisms are, the more likely it is that users will circumvent them, resulting in behaviours which are even less secure. The reason for this apparent paradox is usability as more restrictions in authentication mechanisms create more usability problems. Carroll (1996) pointed out that the very characteristics which make a password more secure also make it less memorable. This has produced efforts to identify mechanisms for generating memorable yet secure passwords (DeAlvare, 1988; Barton and Barton 1988). The impact of these recommendations seems to have been limited; most users do not seem to be aware of them.

1.2 Usability issues in password systems

The aim of this study is to identify human and organisational factors which impact on the security and usability of password systems. *Security* is defined as reducing unauthorised access to information or systems; *usability* in the password domain is defined in terms of memorability and perceived overheads. The study was conducted in two parts. In the first part of the study, a detailed questionnaire on security and usability of password authentication systems was designed to elicit descriptions of user behaviour and problems related to the use of passwords. The web-based questionnaire was completed by 139 respondents, half of which were employees in Organisation A, the other half were Internet users from around the world. The questionnaire results are reported and discussed[1] in Section 2. The quantitative research seeks to identify relationships between users password memorability, frequency of password usage, automaticity in entering a password and perceptions of the need for security levels. The issues most frequently raised in the questionnaires were followed up with in-depth semi-structured interviews with 30 users, 15 from Organisation A and 15 from Organisation B. Section 3 explains how the interviews have been analysed using a qualitative method from social sciences called grounded theory, and presents the resulting model of system and organisational factors along with their impact on security and usability. Implications of the findings are discussed in Section 4 and recommendations made for improving authentication processes.

2 Questionnaire study

2.1 Method

2.1.1 Participants

139 responses were received, half of which were from organisation A. The other half from organisations throughout the world. Participants were recruited via email and web interest groups which could be argued restricted subject sampling to technologically biased respondents. It should be

[1] Further relationships were reviewed but few of any interest were found

noted however that respondents were varied in both computer (less than 1 year to 10 years) and password (1 to over 10 passwords - some stating over 30 passwords) experience. For security reasons, participants' personal details were automatically anonymised and personal detail sections of the questionnaire were not always completed.

2.1.1 Instruments

As there has been little previous research on this particular issue, a pilot questionnaire was used to obtain initial quantitative and qualitative data. Although this questionnaire took a broad approach to the subject area, it focused on password related user behaviours, in particular memorability problems. Results from the open ended sections of the questionnaire, however, suggested that this narrow approach was not addressing key problems with password usage as a user authentication device.

2.1.1 Procedure

The questionnaire was placed on the web and once completed was anonymised before being automatically returned, via email, for analysis.

2.2 Results

The significant relationships observed in the study are summarised in Table 1. There is a significant ($P<0.05$) correlation between *"infrequently used passwords"* and *"frequent memory problems"* with the same password, and between *"frequently used passwords"* and *"infrequent memory problems"*. There is also a significant ($P<0.005$) correlation between *"have to think first"* (before password recall) and *"frequent memory problems"* with the same password. The opposite end of this relationship is between *"automatic"* (password recall) and *"infrequent memory problems"*. An interesting point is the significant ($P<0.05$) correlation between *"desire to decrease security"* and *"frequent memory problems"* with the same password.

	Responses	**Correlation Coefficient**	**Significance**
Password usage by Memory problems	137	-.2204	P<0.05
Automaticity by Memory problems	136	-.6338	P<0.005
Required security changes by Memory problems	122	-.2079	P<0.05

Table 1: Mean correlation coefficients[2] between automaticity, memorability and frequency of password usage

50% of respondents wrote their passwords down in one form or another. It was also found that 50% of respondents using more than one password had produced a method to construct "related" passwords, i.e. all or most of their passwords had a common theme or domain. In fact, this applied to all users who answered these question - almost half left these questions blank.

The results clearly suggest that password memorability is partially reliant on frequency of use, which produces automaticity. This would tie in with observations on *encoding specificity* and the *implicit vs. explicit* memory models (Graf and Mandler, 1984; Graf and Schacter, 1985). Encoding specificity suggests that to retrieve information efficiently, the form of password construction should match the retrieval procedure; a semantically meaningful password should be retrieved semantically). The explicit *vs*. implicit memory model suggests that semantically stored passwords (those that have a meaning) are best for explicitly retrieved material (thinking about the item to be recalled). However, if a password is frequently used and therefore automatically (implicitly) retrieved, a structural construction (the shape of the word or the position of keys on the keyboard) is more effective for retrieval purposes.

[2] (All variables in above analysis are means for all password systems using a 2-tailed Significance using a Spearman's Rho test for ordinal related data)

The open-ended sections of the questionnaire suggested there were other factors which influenced user behaviour or led to user problems. It was concluded that further qualitative analysis was required to comprehensively investigate relevant issues.

3 Qualitative analysis

3.1 First-pass analysis: method

The first set of 15 semi-structured in-depth interviews lasted approx. 30 minutes and were conducted with users in Organisation A. Respondents had varying levels of password expertise, both over period and frequency of use. Participants were asked a series of semi-structured questions that covered issues of password generation and recall along with more general system and organisational factors. The interview format allowed participants to introduce new issues to the discussion that they regarded as important.

3.2 First-pass analysis: results

The initial analysis of the interviews and free-format answers in the questionnaire was guided by *frequency* and *fundamentality* of the issues raised by the users. This produced 4 factors influencing effective password usage. Problem areas for password usability were *multiple passwords, password content, users' perceptions of security* in the organisation and *information sensitivity*.

3.2.1 Multiple passwords

Many users have to remember *multiple passwords*, i.e. they have to use different passwords for different applications and/or change password frequently because of password expiry mechanisms. A high number of passwords reduces memorability, increases insecure work-practices (e.g. writing passwords down) and poor password design (e.g. using *password* as their password), as illustrated in the following quotes:

> *"Constantly changing passwords results in very simple choices which are easy to guess or break within seconds of using* 'Cracker'[3]. *Hence there is no security."*

> *"But basically because I was forced into changing it every month I had to write it down."*

Many users devise their own method for beating memorability problems such as *related passwords* - linking their passwords via some common element. Such methods are devised in response to password expiry mechanisms, and by users who have to have different passwords for different applications. Many of these users consciously implemented their own security by varying elements in these linked passwords (e.g. *tom1, tom2, tom3).* However the results show that, rather than improving memorability and security, this decreases password memorability. This has been identified as due to the within-list interference (Wickens, 1992) of related passwords which causes users to write passwords down which in turn reduces password security levels.

3.2.2 Password content

Password content is defined here as the character content of the password reviewed in terms of its memorability and security. Initial results found that users' knowledge of secure password design was very inadequate. This leads users to create rules and judgements on password design strategies which are anything but secure. Words contained in the dictionary and names are the most vulnerable form of password. These results showed that many users do not realise this:

[3] A password dictionary checker

*"I mean I would have thought that if you picked something like your wife's Christian name or something then the chances of a complete stranger guessing ********* in my case were pretty remote."*

3.2.3 Security perceptions

Analysis of the results revealed that users perceptions of security levels and potential threats was a key element in motivating their work-practices. Without clear feedback from the organisation, users construct their own model of *security threats* and *importance of security*. The two extracts below illustrate users' misconceptions in their perceptions of both organisational security and possible breaches:

"I don't think that hacking is a problem I've had no visibility of hacking that may go on. None at all."

"I think that security problems are more by word of mouth than computer problems"

3.2.4 Information sensitivity

The study identified that users' security behaviour often depends on their perceptions of the *information sensitivity*. Users identified certain systems as worthy of secure password practices, whilst others were perceived as "not important enough". In the absence of guidance, users concluded that confidential information about individuals (personnel files, email) was sensitive; but commercially sensitive information, such as customer records and financial data, were often not regarded as sensitive. Some users stated that they liked the classification of printed documents (e.g. *Confidential, Not for Circulation*). This indicates that users need guidance on information sensitivity and rules for levels of protection.

3.3 In-depth analysis: grounded theory

The initial approach to the qualitative analysis ignored a wealth of information in the data. Further analysis using *grounded theory* methods (Glaser & Strauss, 1967; Strauss & Corbin, 1990) enabled us to resolve apparent contradictions and inconsistencies in users' statements. This analysis of the qualitative and quantitative data was then used to build a model of users' password behaviour. Social science methodologies have been used for some years in HCI particularly in the field of CSCW (Suchman, 1987; Fafchamps, 1991). Unlike other social science methodologies, 'grounded theory' (Strauss & Corbin, 1990) provides a more focused, structured approach to research (closer in some ways to quantitative methods) which is why it has been termed a post positivistic method (Stevenson & Cooper, 1997). We have not found any published examples of its application to HCI problems, but found it matched the requirements of this study for a number of reasons:-

1. This study uncovered a complex web of variables interacting to produce users' password behaviour. Grounded theory was able to descriptively relate these variables in a way that enabled possible intervention points to be identified.
2. In a field where there has been little previous research, the direction of the study could be biased by the researcher. Grounded theory enables research to be grounded in the data obtained so that the validity of the theories produced are increased.
3. The structured format of grounded theory encourages the building of a framework and theories that are grounded in the data which then improves the external validity of the research conducted.

The analysis provided a step-by-step account of password usage problems and possible intervention points. A framework of password usage was produced which was substantiated by a further 15 in-depth interviews in organisation B. As the findings from the various studies are too numerous to discuss in detail, we only provide a top level diagram of the model (see Figure 3) and a description of it through a detailed walk-through (see Table 2). Items that are of particular interest in the efficiency of password usage are also presented (Sections 3.4.1 & 3.4.2).

3.4 In-depth analysis: results

3.4.1 Security perceptions: solving apparent contradictions

Several of the interviews show users identifying one perception of their behaviour and then later stating the opposite. Such contradictions make it hard to establish relationships between factors which influence user behaviour. Contradictory statements could be caused by users' being unsure of their own descriptions, or discussing complex issues which involve several factors. The application of grounded theory techniques for analysing the free-format statements on the questionnaires and the interview data identified the latter as the case. An example of an apparent contradiction is shown in Figure 1.

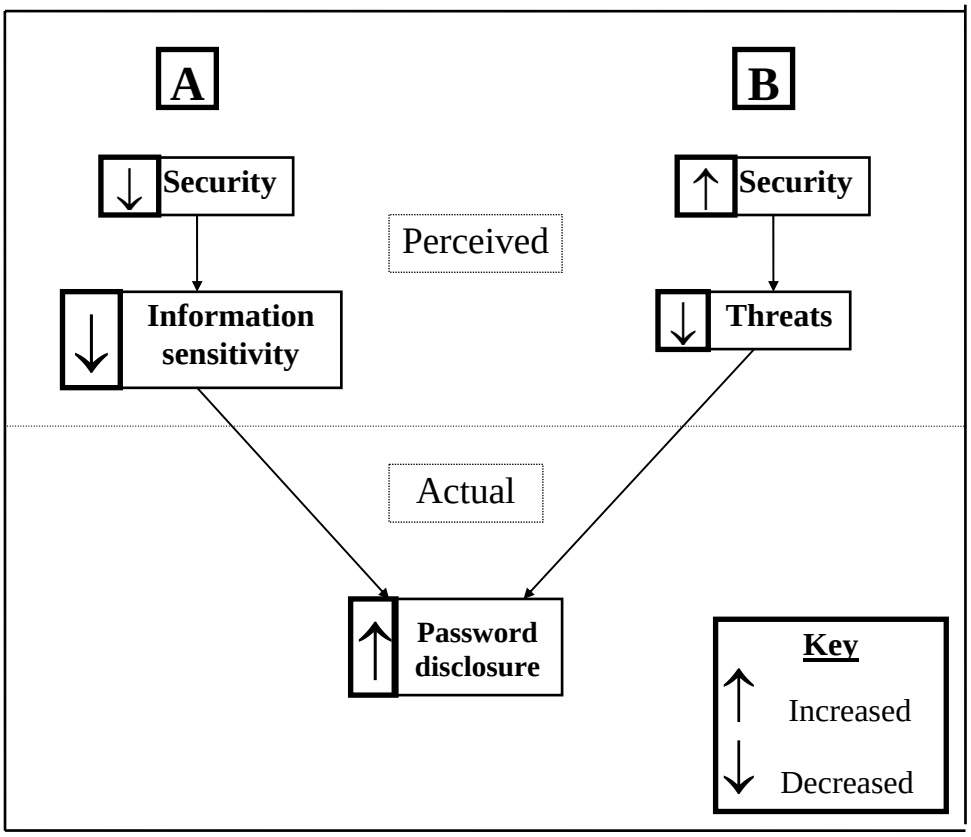

Figure 1: User behaviours produced by perceptions of security levels

A) If users perceive the organisation's general security level as low (decreased), this decreases their perception of how sensitive the information protected is. This, in turn, increases insecure work procedures such as password disclosure. (*"Well, if the information isn't important, why make a big fuss about keeping your password secret?")*

B) If users perceive the organisation's general security level as high (increased) this then decreases their overall perception of threats to the information. This, in turn, also increases insecure work procedures such as password disclosure (*"Well, security for getting into the site is so tight, there's no harm in writing down my password and leaving it on my desk."*)

3.4.2 Work practices: the full story

The analysis revealed the importance of compatibility between work practices and password procedures. Organisation A forced users to have individually owned passwords for group working. This was perceived as incompatible with working procedures whilst *shared passwords* for teams, with shared information, was considered a compatible replacement (see section A in Figure 2). Further research with users in a comparative organisation (see section B in Figure 2) revealed almost the opposite problem and yet the same cause: Enforced group passwords for individual personal

information were passionately rejected by users, perceived as incompatible with the nature of the work and information involved in it.

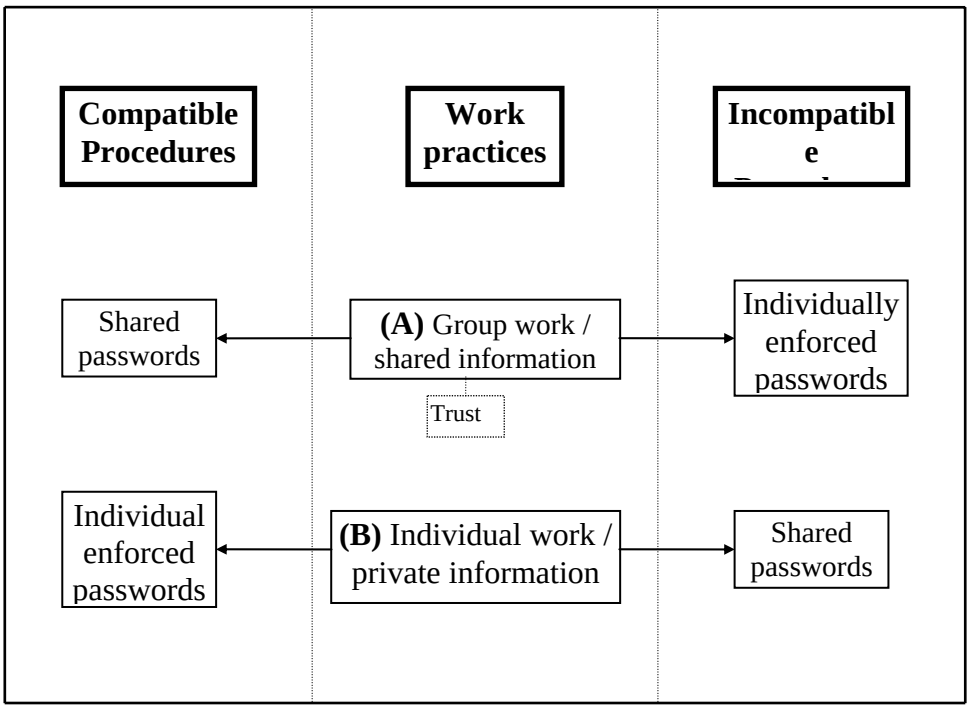

Figure 2: Users perceptions of work practices & system procedures compatibility

This analysis using the grounded theory approach has enabled detailed models of password usability and security to be formulated (see Figure 3). Table 2 provides a rule-based version of the model represented in Figure 3.

Figure 3: High level story-line of password usage

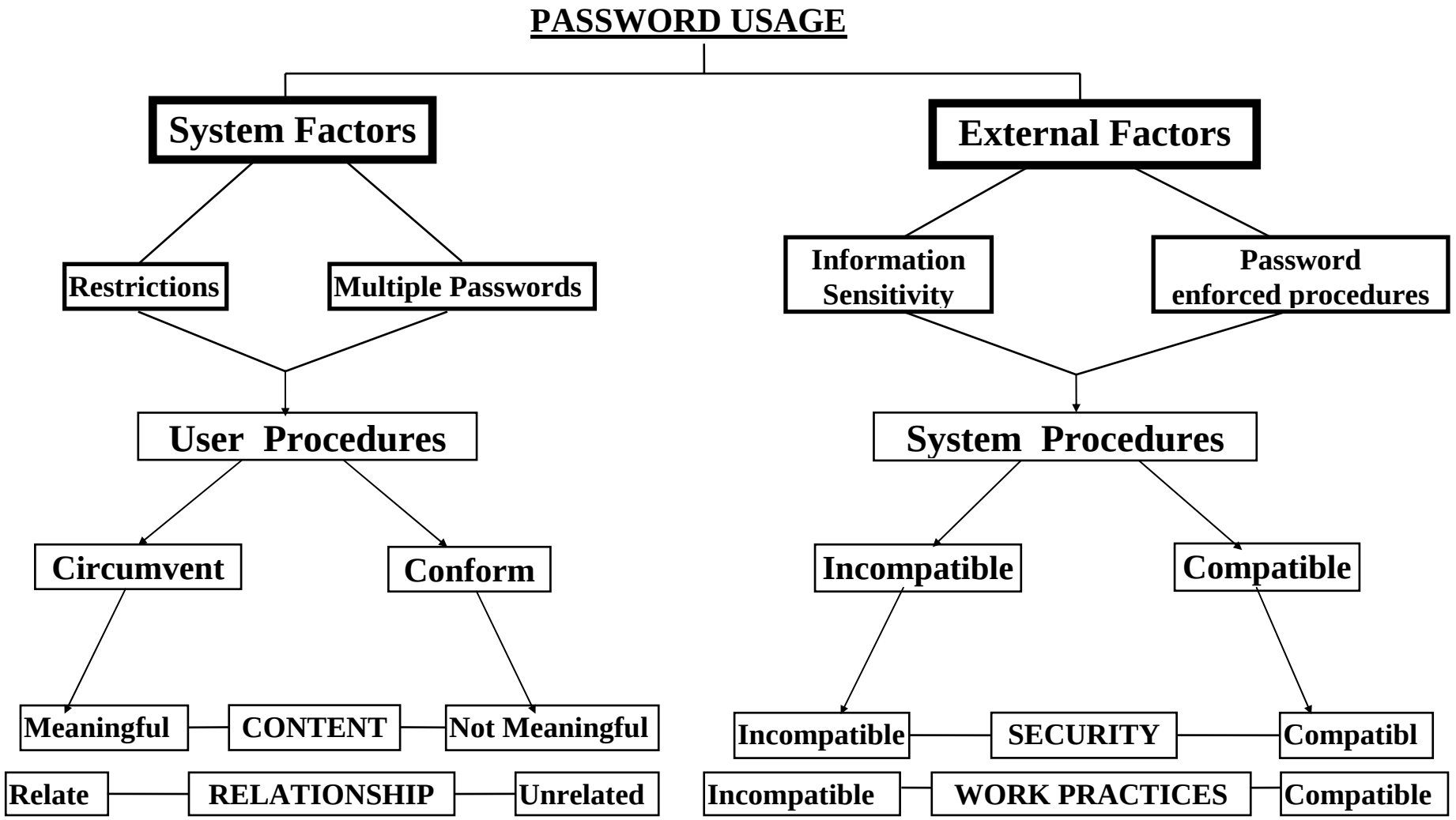

Table 2 : PASSWORD USAGE [High Level Story-line - Walkthrough]

1. SYSTEM FACTORS

A) ARE:-

1. Password restriction mechanisms
2. Passwords for multiple applications and multiple changes over time.

B) Have USER PROCEDURES that:-

1. CONFORM with system factors to produce:-
   a) UNRELATED PASSWORD CONTENT these are:-
      I. Non-words
      II. Words that contain unrelated elements and that are not automatically meaningful.
   b) MULTIPLE PASSWORDS which are:-
      I. Passwords that are totally independent and not related in anyway to one another.
2. CIRCUMVENT system factors to produce:-
   a) RELATED PASSWORD CONTENT these are:-
      I. Meaningful words either personally or generally identifiable.
      II. Related content within the password (e.g.abc123)
   b) RELATED PASSWORDS (JOINED PASSWORDS) these are:-
      I. Related elements across multiple passwords. Either across passwords for applications or across changes in passwords for a single application or both.

2. EXTERNAL FACTORS

A) ARE:-

1. Information's perceived sensitivity or importance.
2. Enforced password practice so that passwords are perceived to be allocated to the individual or the group.

B) Have ORGANISATIONAL PROCEDURES that are:-

1. COMPATIBLE with users perceptions to produce:-
   a) COMPATIBLE SECURITY these are:-
      I. Where sensitive information has a high security where there are high perceived threats
      II. Where unimportant information has a low security where there are low perceived threats.
   b) COMPATIBLE WORK PRACTICES these are:-
      I. Where employees work individually with personal or sensitive information and have individual passwords.
      II. Where employees work in groups sharing information and have group or shared passwords.
2. INCOMPATIBLE with users perceptions to produce:-
   a) INCOMPATIBLE SECURITY that is:-
      I. INSECURE
         i) Where sensitive information is poorly secured with low security levels.
         ii) Where Perceived threats are also high with non-sensitive information and low security.
      II. SECURE
         i) where non-sensitive information is well secured with high security levels. With perceived threats being high or low.
   b) INCOMPATIBLE WORK PRACTICE that are:-
      I. Where group work with shared information has perceived individual enforced passwords.
      II. Where individual work with personal or sensitive information has perceived group enforced passwords.

4 Discussion

This analysis has identified two main problem in password usage; *password mechanisms* that users perceive as forcing them to produce behaviours that circumvent them and *organisational factors* that are perceived as incompatible with working procedures. These problems are due to a lack of communication between security departments and users - users do not understand security issues and system departments lack an understanding of users' perceptions, tasks and needs. Resulting perceptions (by security departments) of users' as 'inherently insecure' and of security mechanisms and procedures (by users) as illogical are then increased, de-motivating naturally secure user behaviours. In this section we examine the consequences of this in detail and discuss intervention points for improving communications.

4.1 Users lack security knowledge

Parker (1992) points out that a major doctrine in password security, adopted from the military, is the *need-to-know principle*. The assumption being that the more known about a security mechanism, the easier it is to attack. Part of the defence is therefore to information only to those who "need to know". A similar approach to security is taken by many business organisations today: those responsible for system security argue that explaining the rationale behind security mechanisms increases its vulnerability. Many security departments see users as "inherently insecure" which produces a tendency to tell users as little as possible. One clear finding from this study is that "insecure" user behaviour is often caused by a lack of understanding. This can be seen in a number of user observations with password content, security perceptions and information sensitivity (see 3.2).

In many organisations, system-generated passwords have been replaced by user-generated ones. This means that the responsibility for creating secure passwords has been shifted to the users; but the "need-to-know" policy of many security departments means that known rules for creating secure passwords are rarely communicated to users. Many users are being asked to complete a skilled design job without adequate training and little on-line guidance. Our data shows that, lacking basic knowledge, users make their own judgements about which practices are secure, and these judgements are often wildly inadequate.

The grounded theory analysis also revealed that many users confused user identification (user ID's) and the password sections of the authentication process. Without knowledge of the authentication process, users assumed that these ID's were another form of password to be secured and recalled in the same manner. This maybe due to the fact that many user ID's are often non-words without meaning. Even if the user ID's are related to the users' name, they differ in format for the varying applications used. This in turn increases users' perceived mental workload associated with passwords. Lack of understanding here increases the perceived overhead, which in turn reduces users' motivation to comply with suggested behaviour.

Finally, users have a poor understanding of password security breaches and risks. Users perceived threats to be low because of a lack of visible risk feedback. Users' lack of understanding also lead to the general misconception that password cracking was completed on a personal basis: perceptions of threats were found to decrease as they perceived their insignificance in the system.

4.2 A lack of user-centred design in system security

This study has identified that many mechanisms designed to improve system security can in practice decrease it. Lack of communication with users also leads to a lack of a user-centred design of security mechanisms. Many mechanisms create overheads for users or require user behaviour which is unworkable. It is hardly surprising to find that many will try to circumvent such mechanisms.

Change regimes are employed to reduce the impact that an undetected security breach could have on an organisation. However, our findings suggest that change regimes reduce overall password security. Users required to frequently change their passwords were found to be producing passwords with less secure content and disclosing their passwords more frequently. Requiring users to have a large number of passwords (for multiple applications and change regimes) creates serious usability problems. Reduced memorability causes password disclosure and crackable passwords (see Section 3.2.1). Many users feel they are forced into circumventing security procedures which decreases their security motivation. Hackers using social engineering techniques rely on a lowered security motivation among users to breach security mechanisms.

Ultimately, a lack of user-centred design in password mechanisms forces users to circumvent procedures. Users are aware that their behaviour is insecure and it is this awareness that decreases their security motivation. The grounded theory model has identified that this can then lead to a spiralling decline in users secure behaviour ("*oh well my behaviours are not secure anyway so it doesn't really matter how lax I become*.")

4.3 Motivating users security awareness

The analysis revealed that users' perception of security threats was motivating or de-motivating as far as their security behaviour was concerned. A lack of organisational feedback on security issues was also found to de-motivate users' security awareness. However, one of the major factors de-motivating users was a lack of user-centred design in security mechanisms.

It has been suggested by the US Federal Information Processing Standards (FIPS, 1985) that individual ownership of passwords increases accountability and decreases illicit usage of passwords, because of the possibility of audit trailing - a by product of authentication. We found, however, that most users are not aware that auditing of system use can be linked to passwords. Further evidence shows that this is probably for the best, since those users who did realise this possibility circumvented auditing by using another person's password - not necessarily because their actions broke rules, but *"just in case, so someone else gets the blame if things go wrong"*. FIPS (1985) states that shared passwords for groups are insecure. However, our results indicate that they should be used if work is carried out by a team. If a password mechanism is incompatible with users' work practises, they perceive the security mechanism as "not sensible" and will circumvent it (e.g. by disclosing it to other group members). This can lead to a perception that all password mechanisms are "pointless", and are therefore circumvented.

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 behaviours e.g. because of obvious external threats or information sensitivity. These findings are supported by research within Organisation B, where both physical and computer security levels were low and security threats were evident. In this situation, users demonstrated exemplary behaviour with their own passwords. We would argue that the "need-to-know" policy ought to be reconsidered and users ought to be told of past or existing (attempted) breaches of security.

5 Conclusions

5.1 Increase communication between users and security experts

The technical bias towards security mechanism 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 organisations which seek to encourage work practices such as teamwork and shared responsibility. Such organisations require support for *trust* and *information sharing*. The authoritarian approach has also led to security departments' reluctance to communicate with users. Informing users about security mechanisms and threats is seen as lowering security by increasing the possibility of information leaks. Ultimately, this has lead to a two fold problem:-

1. Users' lack of security awareness.

2. Security departments' lack of knowledge about users produces security mechanisms and systems which are not usable.

These two factors lower users' motivation to produce secure work practices. This then reinforces security departments' belief that users are "inherently insecure" and leads to the introduction of stricter mechanisms. Communication between security departments and users is therefore often restricted to "ticking off" users caught contravening the rules. This type of relationship is not suitable for modern distributed and networked organisations which encourage communication and collaboration. This

vicious circle needs to be broken by improving communication between security departments and users, along with training and user-centred design of security mechanisms.

5.2 Users and password behaviour

Insecure work practices and low security motivation have been identified by information security research (DeAlvare, 1990; Ford, 1994; Gordon, 1995) as a major problem which must be addressed. There is, however, no identification by those same researchers as to the cause of these user related problems. Instead, the blame has been squarely placed on the user with a lack of security motivation as the reason. It is assumed that users naturally lack security motivation and that this state will not be changed until they have been made aware of, or forced into completing, secure actions. This assumption, however, suggests that humans start, as do computers, from a blank sheet that is programmed into a certain action. The truth is that human behaviour is far more complex than simple conditioned responses. Forcing users to complete an action, may only make them circumvent the whole procedure giving the *appearance* that they have completed that action.

The results from this study suggest that if users show insecure security behaviours and have a low security motivation, it is often due to the security mechanisms employed. These mechanisms have not been assessed in terms of their compatibility with users' work practices, organisational strategy and usability - factors which we would expect to be considered during the design and implementation of most systems today. Designers of security mechanisms must realise that human and organisational factors are a key issue in security design. Social engineers understand this and have used it to their advantage, increasing system security breaches. Unless security departments understand how their mechanisms are used in practice, they will always be doomed to produce mechanisms which look secure on paper but fail in practice.

5.3 Recommendations

The construction of secure passwords can be assisted by the recommendations given below under "content" and "password relationships". Users' motivation to apply these relies on the recommendations set out in "security perceptions" and "work practices".

Password Content

- Give on-line instruction and training on how to construct usable/secure passwords. This will show users that they need not circumvent security mechanisms in order to construct memorable passwords.
- Give on-line feedback to users on what constitutes an insecure password. This will hopefully aid in users' knowledge of what not to use in their password design procedures.

Password Relationships between Multiple Passwords

- Multiple passwords decrease overall security and memorability which in turn increases users' overheads.
- If multiple passwords have to be used, a maximum of 4 or 5 is recommended to reach the extent of most users' memory abilities for totally different multiple passwords. This number is reduced if passwords are used infrequently.
- If more passwords are needed, then users should be advised that they can join the passwords (produce several passwords that have related content) to reduce the number. They should also be advised that this could cause memory interference problems unless joint passwords are identical which will increase memorability and security (by reducing password disclosure). A possible solution could be presented in a physical format with smart card technology giving a second barrier of security which could be used for various systems.

Security Perceptions

- Give on-line feedback to users of how crackable their password is. This will identify for users the importance of constructing secure passwords and help them to identify those more highly crackable.
- Relay to users the possible threats to the organisations system and information. This will increase the users' concept of perceived threats and thus the need for security measures.

This measure is especially necessary on sites where security is high and the site is isolated. Users perception of threats to security is especially low under these conditions.

- State the role that password security plays in combating perceived threats.
- Make explicit the level of sensitivity that different information has. This will reduce the degree of arbitrary judgements made by users.
- State how security levels relate to information sensitivity. This will indicate how well the security conforms to organisational procedures.

Work Practices

- Relate enforced password practice to organisational procedures. This will mean that users will identify how relevant security is to their working practices with shared information having shared passwords and individual work having personal passwords. If this is not to be adhered to, reasons must be given to the user as to why it is necessary for the security mechanisms to circumvent working procedures.

REFERENCES

Barton, B.F. & Barton, M. S. (1984) "User-friendly password methods for computer-mediated information systems. *Computers and Security*, **3**, 186 - 195.

Carroll, J.M (1996) "Computer Security" 3rd ed. Butterworth-Heinemann, MA.

DeAlvare, A. M.(1988) "A Framework for Password Selection" *Unix Security Workshop II*. Portland. Aug 29 - 30

DeAlvare, A. M.(1990) "How Crackers Crack Passwords OR What Passwords to Avoid" *Unix Security Workshop II*. Portland. Aug 27-28

Davis, D. and Price, W. (1987) "Security for Computer Networks" John Wiley & Sons, Chichester.

Fafchamps, D (1991) "Ethnographic workflow analysis: Specifications for design." In Bullinger, H. J. (eds). Human aspects in computing: Design and use of interactive systems and work with terminals, Elsevier, pp. 709-715.

FIPS (1985) "Password Usage" Federal Information Processing Standards Publication. May 30.

Ford, W.(1994) "Computer communications security: Principles, standard protocols and techniques" Prentice Hall. NJ

Glaser, B. & Strauss, A. (1967) "The discovery of grounded theory". Aldine, Chicago.

Gordon, S.(1995) "Social Engineering: Techniques and Prevention", *Computer Security*, 1995

Graf, P. & Mandler, G. (1984) "Activation makes words more accessible, but not necessarily more retrievable." *Journal of Verbal Learning and Verbal Behavior*, **23**, 553-568.

Graf and Schacter (1985) "Implicit and explicit memory for new associations in normal and amnesic subjects" *Journal of Experimental Psychology: Learning, Memory and cognition*, **11**, 385 - 395.

Hitchings, J. (1995) "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology." Computers & Security, **14**, 377-383.

Parker, D. B. (1992) "Restating the foundation of information security" in "IT Security: The Need for International Co-operation" G. G. Gable & W.J. Caelli (eds). Elsevier Science Publishers, Holland.

Strauss , A. & Corbin, J. (1990) "Basics of qulitative research: Grounded theory procedures and techniques" Sage, London.

Stevenson, C. & Cooper, N. (1997) "Qualitative and Quantitative research." The Psychologist: Bulletin of the British Psychological Society, April. 159-160

Suchman, L. (1987) "Plans and Situated Action: The problem of Human-Machine-Communication" Cambridge Univerity Press. Cambridge.

Wickens, C.D (1992) “Engineering Psychology and Human performance” (2nd ed.) Harper Collins, NY.