The True Cost of Unusable Password Policies: Password Use in the Wild

Philip Inglesant & M. Angela Sasse
Department of Computer Science
University College London
Gower Street, London WC1E 6BT, UK
{p.inglesant, a.sasse}@cs.ucl.ac.uk

ABSTRACT

HCI research published 10 years ago pointed out that many users cannot cope with the number and complexity of passwords, and resort to insecure workarounds as a consequence. We present a study which re-examined password policies and password practice in the workplace today.

32 staff members in two organisations kept a password diary for 1 week, which produced a sample of 196 passwords. The diary was followed by an interview which covered details of each password, in its context of use.

We find that users are in general concerned to maintain security, but that existing security policies are too inflexible to match their capabilities, and the tasks and contexts in which they operate. As a result, these password policies can place demands on users which impact negatively on their productivity and, ultimately, that of the organisation.

We conclude that, rather than focussing password policies on maximizing password strength and enforcing frequency alone, policies should be designed using HCI principles to help the user to set an appropriately strong password in a specific context of use.

Author Keywords

Passwords; Password Policy; Usable Security

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): D.4.6 Security and protection, K.6.5 Authentication.

General Terms

Human Factors; Security

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.
Copyright 2010 ACM 978-1-60558-929-9/10/04....$10.00.

INTRODUCTION

Despite a growing number of graphical and biometric authentication mechanisms, passwords remain the most familiar and commonly-used form of user authentication in organisational settings. In this paper, we investigate the impact of passwords, and their associated security policies, on individual users' productivity and experience. Password policies govern not only construction and lifetime of individual passwords, but also work with other contextual factors to define the numbers of passwords users are expected to remember and the frequency with which they have to use them.

Over 10 years ago, Adams & Sasse [1] found that password policies that do not meet users' work practices caused high levels of dissatisfaction, and led to insecure practices and low security motivation.

Since then, we have seen studies of passwords using controlled [22] and survey methodologies [10, 23], which provide some understanding of the policy factors that make passwords easier to generate, remember, and use, in ways which are appropriate to the situation. So - has this understanding been applied in practice? Has anything changed?

We investigated password use in two major organisations. Our study combines two forms of methods: a highly-structured diary study to capture "what happens during the day", and retrospective interviews following up on the context around the passwords identified in the diary. By focussing on the password as the object of interest, we have been able to "look around" instances of password use, to identify problems in using passwords governed by specific policies a specific context, and to understand how users cope with them. We are not simply concerned with the extent to which users comply with policy, but to identify ways in which policy impacts - positively or negatively - on users' daily practice of password use.

In this way, we are able to understand more about contextual issues of password use:

1. What specific aspects of password policy cause problems for users?
2. What coping strategies do password users adopt to overcome those problems?

3. How do those coping strategies affect productivity, the security of the specific systems, and organisation’s risk management in general?
4. Are there unexpected password issues not covered by existing policy?

Based on our results, we make three key observations:

1. When users cannot cope with the demands of strict password policies, it a) reduces their productivity, and b) leads them to adopt coping strategies - which usually reduce security.
2. Although passwords are usually considered in terms of authentication for a service or a device, today they are encountered in many other ways in the workplace – and existing password policies do not cover these. As a result, users adopt ad-hoc solutions, which are usually insecure.
3. Security depends on the context of use. Context - including virtual workstations, Single Sign-on, and home and mobile working - impacts not only the frequency of password use, but also on the risks associated with it.

Organisations that continue to ignore HCI design principles and impose unusable password policies pay a price in the cost/benefit trade-off between the risk of loss versus the cost of complying with security [12]. Password policies should be as strong as needed, not more. Forcing users to comply with policies which meet the maximum theoretical risk is a huge cost, not only in monetary terms but also in terms of the most valuable resource any organisation has - the goodwill of organisation members.

BACKGROUND

Password policies are currently set at the organisational level, with them aim of preserving the confidentiality, integrity and availability of the organisation’s systems and data. There is a growing body of evidence that people cannot cope with the password policies imposed on them [1, 7], and that, given the choice (that is, without imposed restrictions) users choose the weakest password they can get away with [10].

The User Cost of Password Policies

Factors in password policy that increase the user effort include: password strength, type (character restrictions); numbers of passwords the user has to remember; and frequency of changing passwords.

Conversely, factors which can be expected to mitigate the load on users are: Single Sign-on (SSO); password synchronization - a single password covering multiple services; and systems designed to help users cope with passwords in a secure way, such as local password management.

Factors which place a load on the user

Strong passwords - in the sense of password length and character set size - take many orders of magnitude longer to crack than shorter, simpler passwords [14]. But - given the choice - users tend to avoid non-alphanumeric symbols [10, 13], and passwords which contain such symbols are significantly harder to recall and more likely to be written down [23]. Allan [2] calculates a “*breaking point*”; there is a maximum effective entropy - a pessimistic calculation puts this at about 18bits - for all types of password; exceeding this is likely to cause users to write passwords down, so that trying to increase password entropy by strengthening the policy will be counter-productive.

Another consideration is that strong passwords offer no protection against phishing or key-logging [10, 12]. Frequent change and non-re-use of passwords across sites are the common password policy recommendations to mitigate such risks, but these measures are arguably of marginal benefit [12].

Being required to devise high-strength passwords, with high frequent changes, over many passwords which are required to be distinct from one another, combines into a heavy load for the user [14, 23]. Organisational policy generally has no control over numbers of additional “private” passwords users may have, but organisations can reduce the need for multiple passwords within the workplace through technical measures, such as Single-Sign On (SSO), or use of alternative authentication mechanisms, such as biometrics. The former has become more common over the past 10 years, but adoption of alternatives to passwords has been slow.

The Impact of Password Policies

In this section, we examine the current guidelines on how to select password policies, and the user load results from different policies. Recent guidelines by the US National Institute of Standards and Technology [14] organise aspects of password policy around identified risks in the compromise of password-based authentication systems. Among the recommendations which impact on users, they cover:

1. Secure transmission of passwords, to mitigate password capture;
2. Construction of strong passwords, and a (high) limit on the frequency of guesses, to mitigate guessing and cracking;
3. Password expiration and avoidance of recently-used passwords, to mitigate the use of compromised passwords; and
4. Use of Single Sign-On and local password management, to enable stronger policies while reducing the load on the user.

Other points which a password policy should consider include:

1. Timeouts and screen locking, to mitigate opportunistic mis-use of an unattended desktop; and
2. Rules about sharing passwords - traditional advice [9] suggests that this is to be avoided, but others [1] found situations in which password sharing might be appropriate in the workplace [1] or for personal banking [20].

Password Policies in the Context of Use

Password policies need to be understood in the concrete reality of daily use - which Dourish et al. have called "*security in the wild*" [7]. In this real-life context, password use is a secondary task, and an interruption to the user's primary task [4]. Moreover, password use does not occur in isolation, but works alongside other access control mechanisms and factors in the context of use.

What Passwords Do People Actually Choose?

Password policy sets out the constraints within which users must operate; users choose passwords within those limits, in ways which we aim to understand more. For example, do they conform minimally or maximally to password construction rules?

It might be expected that people will choose a strong password for a sensitive application. Evidence for this is mixed; Zviran & Haga [23], in a large quantitative analysis of password choice, did not find any correlation between password length and composition and data sensitivity. However, we believe that there are issues around password choice which can only be uncovered by an in-depth study of password use in actual practice.

Choosing a weak password might be entirely rational, from a user's point of view; the direct costs of attacks might be small and uncertain, but the indirect costs of additional effort are immediate and certain. Herley [12] provides important new insights into people's implicit cost/benefit calculations in deciding whether or not to follow security rule. As he argues, e-commerce users understand the risks, and they judge the likely personal cost from password cracking or theft to be low.

However, in this paper we are specifically concerned with password use in organisations. The costs of a password breach might include significant losses for the organisation, and serious consequences for the individual's continued employment.. Adams & Sasse [1] argue that most users within organisations are security-conscious; insecure practices are not the result of a relaxed attitude, but are the result of ad-hoc attempts to deal with an unmanageable load and conflicting demands.

The Problem for Policy-Setters and Policy-Users

It is clear that, to be effective, security policies need to be written to balance the organisation's security requirements against the ability of users to perform security tasks [14]. To achieve this balance, those responsible for setting policies need to understand the users' primary task and context of operation, as well as the risks. As the same time, it may not always be possible to produce an ideal solution; there will always be some conflict between security and the smooth working of users' primary tasks.

METHODOLOGY

Aims of the Study

We want to understand users' experiences of password use in organisational settings. It cannot be assumed that organisational use has the same costs and benefits, for users or for the organisation, as in studies of individual performance with passwords or use of passwords by consumers. From the organisation's viewpoint, passwords are subject to password rules and policies which are under their control, as decided by policy setters - Chief Information Security Officers or other senior managers.

From a detailed study of daily password use, we aimed to understand more about specific problems faced by users in conforming to password policies, and the strategies which they adopt to cope with these issues.

Overall Approach

The research was conducted within the context of a large project to model different aspects of organisational security policies [21]. For that purpose, we sought quantitative data about how long passwords take to enter, how often different types of password are used, and an understanding of the context of use.

Our research is also a rich source of qualitative data, particularly the transcripts of voice recordings of debrief sessions following each participant's diary keeping.

Our approach differs from previous research in two ways. First, by taking the *password* itself as the object of study, rather than the user and their experience with passwords in general, we were able to study the contextual factors that surround the password. Second, we wanted to study users' daily experiences with those passwords.

We asked our participants to record actual password events that occurred in their working day; we hoped that this would record problems and their immediate impact, and provide a cue for discussing practices and lived experiences resulting from particular password policies in subsequent semi-structured interviews. In retrospect, our approach was successful in identifying password practices, but less so in bringing to light specific events.

Organisation A	
A large research-intensive university; participants are administrators, and lecturers or researchers in disciplines removed from Computer Science and HCI, and teaching staff:	
Administrative staff	7
Lecturing and research (non-Computer Science/HCI)	8
Organisation B	
A large financial services organisation. Participants are members of a security team and Human Resources administrators. The security team members are of interest to us as a sample of more security-aware users	
HR Administration	5
Security team	12

Table 1: Participants in the diary & interview study

Three Forms of "In the Wild" Data

Capturing the situated actions of people interacting with technology requires detailed recording of events as they occur. However, video recording was not an option due to the sensitive nature of passwords, and our initial attempt at shadowing with pencil-and-paper recordings was cut short because Organisation B thought shadowing staff was commercially too sensitive. It was important for us to develop a methodology which interfered as little as possible with users' flow of work. We thus adopted a combined approach, using diary studies to record users' actual use of passwords, as accurately as possible within the limitations of self-reporting, followed by an interview.

Diary Study

Diary studies are an established method to investigate technology in use in HCI [5, 15]. It is important to be clear, however, that in contrast to those studies, in our case the diary was highly structured, apart from space for free-text responses where participants were asked to give the background task - such as starting work - and specific reason for password use - such as authenticating to a particular service.

Debrief Interviews

The debrief interviews were structured around a questionnaire to capture details of users' passwords, but administered by the researchers and voice-recorded, with participants encouraged to discuss the reasons for their questionnaire responses in depth. In this way, our method is between ethnography and quantitative methods. Our diary study provides data which are amenable to quantitative analysis, for example around the frequencies of various kinds of password events.

Organisation A	
Length	7 or 8 characters
Character sets	At least one character from 3 of 4 classes
Character classes are upper case letters, lower case letters, digits, and non-alphanumeric characters	
Passwords must not consist of words or proper names, including known foreign-language words, or variants produced by exchanging I's, L's and O's for 1's and 0's	
Expiry	4 months
History	Must not be *similar* to previous 12 passwords
Password management	Password synchronisation - one password for many organisational systems
Impending password expiry is signalled to users by an email sent to their organisational address	
Organisation B	
Length	Minimum 6 characters
Character sets	Identical to Organisation A
Passwords must not include parts of the user's name or other common words	
Expiry	90 days
History	Must not be *identical* to previous 9 passwords
Password management	SSO for most organisational systems
Impending password change is signalled to users by a warning at log-on time for two weeks prior to expiry	

Table 2: Password policies in the two organisations

Sampling

Because we were concerned with organisational password policies, we recruited participants from among staff members within two organisations. Over a period from December, 2008 to August, 2009, we recruited 32 participants who each kept the diary for 4-5 working days - see Table 1. Participants were all volunteers and were compensated with gift certificates. We recorded 17.4 hours of interviews from these participants. Although this is a relatively small sample size, it is appropriate for an in-depth analysis of diaries and qualitative data.

Analysis

The forms collected during the structured interviews were digitised into a relational database; this relatively formal data structure allowed for rapid extraction of data.

Data quality

Where a participant kept a diary for more than 5 days, only the first 5 days were included in the quantitative analyses, although all days were nevertheless recorded for the information they provide for qualitative analysis. 4 participants kept a diary for only 4 days each. All 4 were part-time workers, and the 4 days comprised their work days over the study period; we have included their entries. For 2 participants, we felt that the diary data was unreliable and have discarded it from the quantitative results, but nevertheless used the debrief in the qualitative analysis. This left 982 password events suitable for analysis.

As well as the paper record of password details taken during the interviews, we had the transcripts and recordings of the interviews, and so were able to double-check the questionnaire data. We identified 26 passwords from 14 participants which were recorded in the diaries but for which details were not reported in the debriefs, due to error or for reasons such as an extension of the diary after the debrief. We also noted 3 passwords recorded in the debriefs but not recorded in the questionnaire results. These were excluded from the quantitative and qualitative analyses.

We collected 196 separate passwords in total in the diaries. However, some passwords are fixed by the architecture to be identical to others, as a single password for use across many systems. Some participants recorded these as separate passwords while others chose to record them as one. This applies to 52 passwords, leaving 144 unique passwords.

Qualitative and quantitative analysis

We analysed the data quantitatively and qualitatively in terms of different uses for each password, to understand specific triggers for password use. The basic method was to identify common issues and correlations quantitatively, and to add depth by focussed qualitative analysis. Our questionnaire and diaries used 5-point Likert-style scales, in some cases labelled.

The transcribed recordings were analysed using a variant of Grounded Theory [6]. We used Atlas TI [19] to aid our qualitative analysis. Unlike classic Grounded Theory, we did not develop a single "core" code, but instead we identified common themes around each of the following clusters of codes:

1. Sensitivity of passwords, and factors which affect it;
2. Estimated strength of passwords and why participants consider passwords to be strong or weak;
3. Coping with the demands of password policies, both for devising passwords and for remembering them;
4. Similarity of passwords with other passwords used by participants;
5. The "ecology", or context, surrounding each password.

Each of these clusters of codes was then used to build a "meta-code" and re-coded for common factors between participants.

RESULTS

Our analyses of daily practices around passwords, and their impact on users, produced findings that we can categorise under three headings:

i. Conflict between password policies and the capabilities of users, and the problems this creates;

ii. The ways users find to cope with this conflict; and

iii. The impact on security of different contexts of use.

Conflict Between Password Policies and Users' Needs

We examined users' perceived needs for compliance with secure practices, and found that users are cogent in their understanding of security needs, but nevertheless find the demands imposed by password policies too difficult.

We begin by showing some of the features of password policies that create burdens for users. Later, we consider the strategies which users adopt to attempt to cope with these demands; however, each coping strategy introduces its own problems, as we shall see.

Our findings support those of Adams & Sasse [1] that the majority of users are security-conscious, and can understand the need for secure behaviour. On the other hand, forcing them into behaviours which they perceive as too stringent creates a conflict between their perception and the enforced practice.

The Burden of Changing Passwords

Regular password changing is recommended by NIST [14] and mandated in both organisations, with the intention of mitigating the risk from compromised passwords: the risk of a password being compromised increases with its lifetime.

Users rarely change their password unless forced to do so. We asked participants how often they change their passwords. Apart from those passwords (network and others - 40 in total) for which change is enforced, only 10 of the 144 unique passwords are changed more than once per year, and even of those, 5 are only changed because the participants forget them.

In minimising password change, participants are being completely reasonable: changing passwords places a heavy burden on users, both in devising a new password and also in learning them.

The Burden of Devising Passwords

Generating new passwords which must conform to a strict security policy is a non-trivial interruption to users' activities.

Password policies are highly restrictive - but users are unclear about what the rules are. In Organisation A, users changing a password were surprised that to find the system would not allow anything it deemed *similar* to the users' 12 previous passwords. This meant they were unable to apply their usual method for constructing passwords:

> *so it's got to the point where it's ... so difficult to make one up, and difficult to remember, that I have to write it down.*

The need to invent new passwords which are not obviously similar to previous ones challenges the mental resources of users:

> *this one we do have to keep changing all the time, and it gets harder to, to think of things*

The Burden of Learning Passwords

Passwords which are used very frequently are remembered easily; 59 unique passwords were said to be remembered "automatically" in this way. This is so, even for the complex passwords in Organisation A:

> *no I don't forget my... I never, I don't think I've ever forgotten my [Organisation] one, not because I've got such a wonderful memory but just because you type it so often.*

Thus, requiring strong passwords *might* be acceptable, *if* users were able to keep to one password which is used frequently for almost all uses within the organisation. Unfortunately, this does not overcome the problem of remembering it in the first few days; this learning period can be especially challenging for part-time staff; one reported using a clue as a reminder on Monday mornings following a change.

Moreover, it is not always the case that the organisational password is used frequently, while others are used less often: in Organisation A, some departments have a local password, which means that the main organisational password is used only occasionally - this was the case for two of our participants.

The Burden of Forgetting

Forgetting a password is always an interruption; but, in some cases, "remembering by reset" might be a reasonable strategy in situations such as returning from vacation or for infrequently-used passwords.

Unfortunately, in the case of Organisation A, arranging a password reset is more complicated. A participant described a typical scenario:

> *first I go through a series of passwords that I use, and hope it's one of them, and when it locks me out, I swear at [Information Systems], and it has to be reset completely*

which entails a call or visit to the helpdesk[1]; but once the password is reset, it takes up to two hours before it has propagated to all the systems.

The effort and, more importantly, the time delay involved in resetting passwords raises a genuine *fear of forgetting*; considering the disruptions it causes to users' tasks and productivity; another participant reported:

> *I get emails, think I'm too busy to open that, and then I did it yesterday and I was down to you've got 10 more days ... I've just been too busy to risk forgetting the password or having two hours where I can't log in ... that's happened to me before.*

Coping with Password Policies

Users develop strategies to cope with matching password needs to security requirements. when the requirements of the policy exceed users' capabilities, they are forced to develop more complex - or, alternatively, less secure - coping techniques.

Coping with Choosing Passwords

Most users we observed had developed (sometimes quite imaginative) strategies for generating passwords – such as using paired words from a cycle of non-English words. Of course, if a strong password is mandatory, then users are forced to be imaginative.

Paradoxically, upper limits on password length or character set - which reduce the possible password strength -, as well as fixed passwords, also block users from using their preferred scheme. This is notably the case for the main password in Organisation A, which must be 7 or 8 characters; bank passwords and some e-commerce (such as train company) passwords also restrict the character set.

The most obvious scheme to generate passwords is to re-cycle an old one, perhaps making some small change. Users see "good" passwords (that are memorable and conform to the policy) as a "resource", which they continue to use for new applications even if the original use is no longer allowed. Of the 144 unique passwords, we found 14 currently also used for other work-related passwords, 17 re-used for personal uses, and 22 not identical but similar to other passwords - a total of 53. This is in addition to the 52 passwords which are *forced* to be identical by the architecture of the system.

Re-use does not necessarily mean people are using the same or similar passwords for "everything"; only two of our participants admitted to doing so, even though in Organisation B that would be quite possible.

[1] A self-reset is now available, but was not, at the time of this research

Writing Passwords Down

An obvious - and potentially risky - response to the demand to learn a new password is to write the password down.

Of the 15 participants in Organisation A, 9 admitted to writing down the main organisational password, either for the first few days of use or if, because of the nature of their work, they only use the organisational password occasionally.

It could be considered small progress since the findings of Adams & Sasse [1] that most users who write down passwords now do so apologetically, and keep it in some “safe” place, such as a diary. Even though this is some progress, passwords in a “safe” place at home or work are still at risk from attackers [12, 18], and, since wallets and diaries can be lost, the coping strategy is not always effective.

For comparison, none of the participants from Organisation B wrote down their network or PC login password, and the reason seems clear - although forced to change their passwords as in Organisation A, small, easily remembered changes are allowed. Unfortunately, this can lead to new problems - the user remembers the basic password, but may fail to remember the variations.

Users Want To Be Secure, But Do Not Always Know How

We have said that few participants showed a relaxed attitude, eg., using the same password for everything. At the same time, users need to balance what they perceive to be reasonably strong passwords against the need to remember them, especially if they are not frequently used.

Yet choosing a reasonably strong yet memorable password is not easy. At least 3 participants - out of 5 non-security specialist participants in Organisation B - described their SSO password in terms which show that they are very weak - for example “*an item that is on my desk ... and then add a number to it*” - even for what they admit are sensitive applications. These participants nevertheless described the passwords as secure or fairly secure. Whereas Organisation A frustrates users by enforcing an overly-strong policy, Organisation B appears to offer little guidance to non-specialist users about appropriate password choice.

Such passwords are clearly guessable, but even apparently strong passwords might be guessable by someone with personal knowledge of the user - names or initials of relatives and significant dates are a popular scheme. Such passwords pass the stringent checking used in Organisation A; this reliance on a technical approach of enforcement, then, not only does not help users to learn how to make better passwords, but also does not always detect poor ones.

The Importance of the Context of Password Use

A core HCI principle is that, to be accepted by users, security policies must fit with an individual or organisation’s primary task [1, 4]. However, it has been less noted that the organisational context also covers aspects of the security architecture which have the potential to make life easier or more demanding for users.

Context impacts the frequency and ease of password use - and, consequently, on the ability of users to become familiar with complex passwords - as well as on the sensitivity of passwords and risks from security breaches.

We typically think of passwords as authentication for a PC or online service. However, in daily use passwords encompass many other reasons for use, and the same password is often used for many services, by user choice or by the architecture of the authentication system.

For our questionnaire, we started with an *a priori* set categories of password use, but from our analysis we expanded this to at least 14, including some which are not often considered when password policies are designed. Space prevents us discussing each category in detail here, but notable categories are well-known uses such as access to company or third-party service and login to a local PC; emerging uses such as Single Sign-On and login to an online virtual desktop; and less-considered uses such as work-related social networking, access to personal HR information, and password-protecting shared files and other resources.

Frequency of Use: Single sign-on vs. Single Password

The context of use is exemplified by the differences between use of Single Sign-On and single passwords. Both organisations have password architectures which require the use of the same password for multiple services. However, in Organisation A, this is a unified organisational password, not true Single Sign-On (SSO): users are required to re-enter the password for each service - and also following timeouts of each service, a major source of frustration for those who have to work on a number of different online services.

Organisation B, in contrast, has true SSO in most instances. This might be expected to reduce password use. On the other hand, company policy is that staff should lock their PCs when leaving their desks, which generates an additional set of usages - 317 in the diaries, by far the largest number of usages, in fact, although each one requires only a password, not the userId - participants report that this is not a large interruption: they are not actually interrupted by the password entry, but are returning from getting a drink or some similar break.

Sensitivity Varies with the Context of Use

Sensitivity - in the sense of “*what bad things could happen from unauthorised access*” - depends on what an attacker could actually do with a password; and that, in turn, depends on the level of access which the password gives. In Organisation A, access control is implemented in particular services; for example, in a student records system, only authorised staff are able to enter student marks, although all staff access the same system.

If a password is used to logon locally to a PC, then whether this is sensitive or not depends, naturally, on the data stored on the computer and that, in turn, on whether the PC stores data locally or is essentially a front-end to a virtual online desktop - an increasingly common architecture which is widely used in both organisations. Access to network filestore can be controlled - in Organisation B, a dedicated team ensures correct authorisation to shared and personal filestore. The actual data which might be visible is therefore controlled, and also depends on the area of work - and can change, as people move onto different projects. On the other hand, some staff have access to drives which are shared among other members of their department - and which therefore contain data which may need further protection, by passwords or other access control.

Use of Passwords for File Sharing

There is one type of password which emerged from our findings that exemplifies unsophisticated security practices which create serious risks: passwords used for protecting *shared files* and *shared web spaces*. Although file passwords account for a relatively small number of events in our password diaries, such passwords are used extensively among numbers of people. Our research found situations in which shared passwords have become the *de facto* method of controlling access to shared resources.

There are two categories of shared password – long-term and ad-hoc ones. Long-term passwords are shared among many recipients, and used many times - participants in both organisations reported this practice, even for access to sensitive information. Where files are genuinely shared among users, this might be an appropriate practice [1]; however, at least some of the passwords we found shared in this way are extremely weak, and unchanged for years: the difficulty of distributing the new password to a number of users discourages changing.

With ad-hoc shared passwords, participants devise one-use file passwords which consist mainly of single words chosen at random (for example, the name on a passing truck, or an item on the sender's desk); the password is emailed to the intended recipient. We found that shared passwords did not conform to the organisational password policies. Adding the password is often the last obstacle to completing a time-critical task (such as sending a monthly report or update), and so users are keen to "just get it done".

DISCUSSION

The conflicts and the issues we have uncovered with passwords in actual use, can be traced fundamentally to ill-considered password policies, in terms of 1) factors which are covered in the policies: insisting on passwords which are unfeasibly strong, or changed too frequently; and 2) factors which are *not* considered in the policies: the different uses of passwords, and other contextual issues

A large-scale web study found that users choose weak - mainly lowercase-only - passwords whenever they can [10]. [11] argues that this failure to use strong passwords is a rational choice, if the direct losses associated with a breach are small compared with the user costs of choosing a strong password.

However, unlike many consumer transactions on the web, breaches such as the loss of student records or details of staff benefits could have incalculable costs. Weak passwords are not a rational choice in those cases. Our users understood this; if they continue to choose weak passwords, it is not because they are irrational or lax, but because devising and remembering a strong password is a considerable effort and an interruption to their primary task.

In our study, both organisations prevent users from choosing such weak passwords - at least for their main password. However, this additional password strength comes at a cost, not only for the users but also for the organisation, in terms of time lost and, paradoxically, a potential loss of security.

The True Cost of Unusable Password Policies

We have shown that factors in password policy lead to frustration when users are unable to comply with password policies; such policies clearly do not meet their needs, and they are forced to adopt coping strategies.

We focus on Organisation A because it provides such a clear example of impact of an excessively strict password policy on the experience of users. Because the policy is very restrictive in the passwords it allows, users are unable to use their normal password methods for choosing passwords. However, if - as is likely - their normal methods for choosing passwords are weak, then this is not, in itself, necessarily undesirable. Unfortunately, in the case of Organisation A, the checking is excessive; this does not guarantee that the password cannot be cracked (that would be impossible), but it does guarantee that users are frustrated in quite reasonable password choices.

But once they have chosen a password which is strong enough, and have learnt it, users still do not have a password "resource" they can continue to use. This is because, when change is enforced, unlike in Organisation B, small changes to passwords are not accepted. Unless users can discover some unintended loophole to thwart the checking, the entire process of choosing has to start again. Users then have a double load: both to choose a new password which is acceptable to the policy, and to learn it.

Thus, the unusability of the policy arises from the *combination* of the requirement for the password to be excessively strong *and* for it to be changed frequently *and* for the new password to differ significantly from previous passwords. In comparison, Organisation B does require frequent change, but is much more lenient in the requirements for password strength and, crucially, allows for new passwords to be minimally different from previous ones.

Adding to the emotional pressure on users, and impeding their primary goals, is their awareness that, should they forget their password, this will require a reset, with a delay of two hours during which their access to essential organisational services will be lost; in many cases they are unable to work during this time.

Faced with this conflict, it is not surprising that a majority of participants from Organisation A admit to writing these passwords down, not in disregard of security policies, but as the only workable coping strategy. Indeed, writing passwords down is half-accepted by the Organisation A policy, which merely says "*don't keep a record of your userid and password together*". This is not a solution; our point is that writing down is a *response* to an unusable policy.

Strength and Change Frequency is the *Wrong* Focus

We have seen that Organisation A enforces passwords which are strong to the point that users are frustrated in their reasonable password choices.

However, the password strength may not be the most important factor in preventing unauthorised access. For many personal mobile devices, the number of password attempts is limited, so that online cracking is unfeasible. For almost all online applications, the number of attempts is also limited. There remains, however, the risk of offline attacks, for example if the password file, even with hashed or encrypted passwords, has been captured.

But password strength does nothing to prevent phishing or key-logging [11]. The other key aspect of Organisation A's policy - password change - is designed to mitigate these risks, along with the risk of "brute force" attacks. Whether a single-character change, as allowed by Organisation B, would be sufficient to deter a serious attacker is uncertain. Clearly, if a computer is compromised by a key-logger, merely changing the password will not fix the problem. What *is* certain is that requiring users to make major changes to their existing passwords creates conflict for the user, between their primary goals and the requirements of the policy.

Nor, as we have seen, does the Organisation A policy provide much protection from passwords being guessed by those with special knowledge of the user. And, crucially, the Organisation A policy greatly *increases* the threat from passwords left written down.

Returning finally to the costs and benefits to the user and to the organisation, it might seem that an employing organisation gains all the benefits from strong password policies, while the staff members, as users, carry all the costs. It should be clear from what we have said, however, that this is spurious: even if staff are willing, or able, to work the extra hours to overcome time lost through password problems, this is at the expense of goodwill and effectiveness.

CONCLUSIONS AND A WAY FORWARD

We have looked in detail at a snapshot of events for a sample of password users; but every minute taken in unnecessary password use needs to be multiplied by orders of magnitude to account for all the password uses even within one organisation. This is the true cost of unusable password policies. Against the world-view that "*if only [users] understood the dangers, they would behave differently*" [12], we argue that "if only security managers understood the true costs for users and the organisation, they would set policies differently". We conclude with some suggestions for how this might be achieved.

Towards Holistic Password Policies

The vision of a holistic approach for security policies is not new; Sasse et al. [16] outlined what such a policy should contain. In moving to a holistic approach, there is no single ideal policy, as the ongoing debate about writing passwords down [12, 17] indicate.

Focussing on frequency of password changing, or password strength, without considering the user in their context of work, is clearly not holistic. Technical means can force people to change their passwords frequently; if this leads to weaker passwords, technical means can enforce strong passwords. If users then forget those passwords, technical services can be provided to assist password resets - and the cycle starts again. It becomes, as Herley [12] puts it, "*an existing system [that] can only be kept going with constant patching*". This does nothing to encourage security awareness, but introduces usability problems which antagonise users.

Beautement et al. [3] propose the model of the *Compliance Budget* to understand how users balance the effort of complying with a security behaviour required by an organisation, against their own benefits in the context of their production goals. This offers a positive way forward, since the organisation can manage users' compliance budget through good security design and a security-aware organisational culture.

In the age of cloud computing, it becomes technically feasible to brute-force passwords, but the cost is a constraining factor. Simple lower-case passwords must be at least 12 letters long to keep within a cost of $US1million; if uppercase, numbers, and non-alphanumerics are added, 10 characters is the minimum needed to do so [8]. If policies continue in their current spirit, we can expect these longer and/or more complex passwords to become mandatory for everything. Our findings show that users already struggle with the burden generated by current restrictions - which are significantly less - and so we could expect the behaviours we observed to be magnified, leading to overburden and collapse. This puts all the more urgency on reserving these strong password requirements for contexts in which brute-force cracking is a realistic risk. Rather than a *one-size-fits-all* approach, we argue for a flexible password policy tailored to mitigate the risks users actually face. This flexibility needs to extend beyond technical issues, to allow for the differing security needs of different work groups. Alternatively, perhaps the cloud will provide the motivation to finally move to a different authentication mechanism.

ACKNOWLEDGMENTS

The authors would like to acknowledge the contribution of Simon Arnell of HP Labs in the collection of this data, the assistance of the other members of the Trust Economics project (funded by the Technology Strategy Board), in particular Robert Coles, and the very helpful suggestions of four anonymous reviewers. Sincere thanks to all participants for their time in keeping the diaries and discussing their password use so helpfully.

REFERENCES

1. Adams, A. & Sasse, M. A. Users Are Not The Enemy. Communications of the ACM 42, 12 (December) (1999), 41-46
2. Allan, A. Passwords Are Near the Breaking Point: Gartner Research Note (2004) http://www.indevis.de/dokumente/gartner_passwords_breakpoint.pdf
3. Beautement, A., Sasse, M. A., and Wonham, M. The Compliance Budget: Managing Security Behaviour in Organisations, ACM Press (2008)
4. Brostoff, S. & Sasse, M. A. Safe and Sound: A Safety-Critical Approach to Security In Proc. NSPW 2001 (2001)
5. Brown, B. A. T., Sellen, A. J., and O'Hara, K. P. A Diary Study of Information Capture in Working Life In Proc. CHI 2000, ACM Press (2000), 438-445
6. Charmaz, K. Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis, SAGE Publications, London, UK; Thousand Oaks, CA, USA; New Delhi, India (2006)
7. Dourish, P., Grinter, R. E., Delgado de la Flor, J., & Joseph, M. Security in the wild: user strategies for managing security as an everyday, practical problem. Personal and Ubiquitous Computing 8, 6 (2004), 391-401
8. Electric Alchemy Cracking Passwords in the Cloud: Insights on Password Policies (2009) http://news.electricalchemy.net/2009/10/password-cracking-in-cloud-part-5.html
9. Federal Information Processing Standards Password Usage (Withdrawn February 2008) (1985) http://www.itl.nist.gov/fipspubs/fip112.htm
10. Florêncio, D. & Herley, C. A Large-Scale Study of Web Password Habits In Proc. WWW 2007 (2007)
11. Florêncio, D., Herley, C., and Coskun, B. Do Strong Web Passwords Accomplish Anything? In Proc. HotSec 07 (2007)
12. Herley, C. So Long and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users In Proc. NSPW 2009 (2009)
13. Morris, R. & Thompson, K. Password security: a case history. Communications of the ACM 22, 11 (1979), 594-597
14. National Institute of Science and Technology NIST Special Publication 800-118: Guide to Enterprise Password Management (Draft): Recommendations of the National Institute of Standards and Technology (2009) http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
15. Palen, L. & Salzman, M. Voice-Mail Diary Studies for Naturalistic Data Capture under Mobile Conditions In Proc. CSCW 2002, ACM Press (2002), 87-95
16. Sasse, M. A., Brostoff, S., & Weirich, D. Transforming the weakest link - a human/computer interaction approach to usable and effective security. BT Technology Journal 19, 3 - July (2001), 122-131
17. Schneier, B. Secrets and Lies: Digital Security in a Networked World, Wiley Indianapolis, IN, USA (2000)
18. Schneier, B. Write Down Your Password (2005) http://www.schneier.com/blofg/archives/2005/06/write_down_your.html
19. Scientific Software Development, 2006, 'ATLAS.ti The Knowledge Workbench', Berlin, Germany
20. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., and Furlong, M. Password Sharing: Implications for Security Design Based on Social Practice In Proc. CHI 2007, ACM Press (2007), 895-904
21. Trust Economics http://www.trust-economics.org/
22. Yan, J., Blackwell, A., Anderson, R., & Grant, A. Password Memorability and Security: Empirical Results. IEEE Security & Privacy 2, 5 - September/October (2004), 25-31
23. Zviran, M. & Haga, W. J. Password Security: An Empirical Study. Journal of Management Information Systems 15, 4 (1999), 161-185