Persuasive Password Security

Dirk Weirich
Computer Science Department
University College London
Gower Street
UK - London WC1E 6BT
D.Weirich@cs.ucl.ac.uk

Martina Angela Sasse
Computer Science Department
University College London
Gower Street
UK - London WC1E 6BT
A.Sasse@cs.ucl.ac.uk

ABSTRACT
Users of password-protected systems have to be persuaded to follow certain regulations to keep systems secure. This paper describes the results of a first study of the mental models, metaphors, attitudes and skills users hold with respect to password mechanisms. It shows that users are currently not motivated to adopt proper password practices. They do not believe that they ultimately can stop somebody from getting into the system, or that somebody getting in could cause them any serious personal harm. We recommend a novel approach to the design of training and online support, which is based on an appropriate use of fear appeals.

Keywords
Security, passwords, discourse analysis

INTRODUCTION AND MOTIVATION
In the past, research on computer security mechanisms has focused almost entirely on technical issues. In recent years, there has been an attitude shift in the computer security community. Humans are now generally considered to be the weakest link in the security chain [1,2], and practitioners in the field look to HCI as a provider of usable solutions.

[3] makes clear that security mechanisms need a usability standard that is different and ultimately more stringent than that applied to most other forms of software. However, making systems secure requires more than just improved user interfaces. Users need to be better educated about security issues. At the moment, they construct their own, often wildly inaccurate model of possible security threats and the importance of security [2]. This, in turn, leads to behaviour that strongly undermines the security of the systems in question: users choose passwords that are cryptographically weak, write them down and store them in insecure locations and easily disclose their passwords to other people. Security policies usually threaten punishment for this kind of behaviour, but are hardly ever enforced. Hackers easily exploit insecure password practices, in particular those skilled in social engineering [1].

Even if the usability of password mechanisms improves in the future, and users become better educated in their use, there is still one further point that needs to be addressed. For most users, security is an enabling task that creates additional overheads. This means that users need to be *motivated* to make the additional effort to use passwords in a manner that maximises the overall security of the system in question.

RESEARCH APPROACH
The aim of our research is to develop means of persuading users to adopt proper password behaviour. Our overall approach can be outlined in three steps:

1. We look at five factors influencing users' behaviour: their mental models, metaphors, attitudes and social and technical skills. In order to elicit these from a specific user group, we conduct interviews which are then analysed using the method of discourse analysis as proposed by Potter and Wetherell [4] (see [5] for a related use of discourse analysis in HCI).
2. We identify those mental models, metaphors, attitudes and skills that lead to proper password behaviour.
3. Finally, we look at ways of guiding users into adopting the elements discovered in step 2. In order to do this, we undertake changes to the discourse about security mechanisms, especially in tutorials and training; the password mechanism itself; and the security policy for the system.

STUDY
We carried out 17 semi-structured in-depth interviews comprising questions concerning various aspects of password security. Ten of the participants worked for a technology company, 6 were Ph.D. students, and 1 was a systems administrator working in finance. The interviews lasted between 30 and 60 minutes and were subsequently transcribed and analyzed using discourse analysis.

Study results
The following is a list of the most important factors influencing security behaviour that we have identified:

- *Identity issues*: Participants exhibiting good password behaviour are often described as '*paranoid*' – even by themselves. Some participants are proud that they do not understand security ('*I'm not a nerd*') or do not comply to regulations ('*I don't just follow orders*').
- *Social issues*: Sharing your password is regarded by many participants as a gesture of '*trust*' in their social interactions – you share your password with people you trust, and somebody refusing to share their password with you is effectively telling you that they don't trust you.
- *'Nobody will target me'*: Most participants regard the information on their system as 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.
- *'They could not do much damage anyway'*: Most participants do not think that somebody getting into their account could cause any serious harm.
- *Accountability*: Most participants are aware of the fact that their behaviour does not fully comply with security regulations. However, they do not expect to be made accountable for this, since they regard the regulations as unrealistic and their behaviour as common practice. In addition, they know that there always is a chance that a hacker will break into their system, however well they behave. They can always claim that it was not their misbehavior that led to the break-in. However, a few participants realize that they might be made accountable for improper behaviour in the past (e.g. writing down their password), if somebody gets into their system now.
- *Good behaviour without a reason*: There are a number of participants who make the attempt to exhibit good password behaviour despite the fact that they are of the opinion that this is not strictly necessary or justified. They follow regulations because they perceive it as necessary in order to maintain their professional reputation, or because they believe that any security failure involving their employer would ultimately reduce the standing of the employer in the business world.

RECOMMENDATIONS

There are a number of recommendations that can be made from the data we have collected and analyzed. Here, we focus on the proper use of *fear appeals* to motivate users to behave in an adequate fashion. This is also the subject of a field trial we are currently carrying out.

Roger's protection motivation theory [6] states that *fear appeals* will be successful when they convince a person that (1) the problem is serious and may affect the person; (2) it can be avoided by taking appropriate action; (3) the person is capable of performing the necessary behaviour required to avoid the problem.

The results of our study show that some or all of these points are not fulfilled for a large number of participants. They do not think it is likely they will be targeted, and if they are, they do not expect any serious damage to be caused. In addition, they believe that even if they behaved properly, a determined hacker could still get in. Finally, they know that their employers can not monitor their every action, so bad password behaviour will usually go unnoticed. They can also always claim that it was not their misbehaviour that let the hacker into the system. This means that for a fear appeal to work, a lot of organizations would be recommended to undertake a number of changes to existing policies and the current discourse about password security in training and online support:

- Do not present the problem as one of a hacker getting into an account and doing serious damage.
- Instead, present it as one of the organization's reputation being tarnished if it were to be known to the outside world that its employees behaved in a fashion that was not security-conscious. This gives the fear appeal (and the associated punishment) a rational motivation which will raise users' acceptance of it.
- Appropriately punish behaviour, not its consequences. In other words, 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.

REFERENCES

1. Schneier, B. Secrets and Lies. John Wiley & Sons (2000).
2. Adams, A. and Sasse, M.A. Users are not the enemy. Communications of the ACM, Vol. 42, No. 12 (December, 1999).
3. Whitten, A. and Tygar, J.D. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. 8th USENIX security composium (Washington, August 1999).
4. Potter, J. and Wetherell, M. Discourse and social psychology. Sage Publications Ltd (London, 1987).
5. Rimmer, J., Wakeman, I., Sheeran, L.,Sasse, M.A. Examining users' repertoire of Internet applications. In Sasse, M.A. and Johnson, C. (Eds.): Human-Computer Interaction – INTERACT '99 (1999).
6. Rogers, R.W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In Cacioppo, J. and Petty, R. (Eds.): Social Psychophysiology. Guilford Press (NY, 1983).