Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery

M. Angela Sasse
Department of Computer Science
University College London
London, WC1E 6BT, UK
+44 20 7679 7212
a.sasse@cs.ucl.ac.uk

ABSTRACT
This paper reviews past and current work on usability of security mechanisms. Given that most users interact with computer security on a daily basis, it is astonishing how little interest the CHI community has taken in the design of security systems. Many usability problems associated with security mechanisms could be avoided through application of basic usability knowledge and methods. At the same time, the design of security systems raises some issues that cannot be met with existing CHI knowledge and methods. In conclusion, I will outline the research challenges for improving usability of security systems.

Keywords
Computer Security, password, biometrics, user cost, task analysis,

INTRODUCTION
My research interest in usability of security mechanism started in 1996, when an international telecoms company asked us to investigate why their employees *"could not remember their passwords"*. The company's concern was prompted by the escalating cost of the helpdesk operation through which passwords were being re-set. Anne Adams conducted an interview and questionnaire study with people inside and outside the company; when we published the results in Adams & Sasse (1999), the conclusion was that users

- could not cope with the proliferation of passwords,
- received little instruction, training or support; and
- were not motivated to behave in a secure manner.

We placed the blame for this state of affairs on the computer security community, stating - acerbicly and somewhat uncharitably – that computer security was the last area of IT where user-centered design and user training were foreign concepts. In fact, security researchers Zurko & Simon (1996) had recognized the necessity to apply user-centered design principles to security several years earlier. Today, the security community in general has accepted the importance of what they commonly refer to as the "human factor in security" since one of their most influential exponents, Bruce Schneier (2000) wrote that

> *"Security is only as good as it's weakest link, and people are the weakest link in the chain."*

Reformed social engineer Kevin Mitnick (2002) has provided a plethora of examples of how easily the majority of – under-educated and untrained users – can be duped into behavior that compromises their own (or their organization's) security. Our own work was motivated by the realization that unusable security systems were not only expensive, but ineffective (Sasse et al., 2002). The increasing complexity of systems and applications, and the spread of networked systems and e-commerce has increased the possibilities for attacks. This means the need for good security behaviour from home and corporate users is higher than ever; the reality in most organizations is that security behavior and culture is in a dismal state (Sasse et al. 2001).

In the face of these developments, the security community is nothing if not receptive to guidance from CHI experts on how to improve usability and effectiveness of security systems. This raises the question– what can we offer them?

Based on the published evidence, the answer would have to be - "not a lot". Even though most users interact with security mechanisms on a daily basis, the CHI community can muster less than a dozen publications on the topic; half of those come from my own research team. As a result of this curious lack of interest, a key aspect of everyday technology has been allowed to evolve into a usability disaster. What can we do to recover from this situation? In this paper, I argue for a two-pronged approach. Firstly, we need to provide examples and hard evidence that application of basic CHI knowledge can improve not only usability, but also effectiveness and efficiency of security mechanisms. Secondly, we need to recognize that the design of security systems raises some issues for which, to date, CHI does not have answers ready. Further research is needed in a number of areas, such as the development of policies that govern the use of a particiular technology, and on the longer-term impact of technology on users' habits, motivation and self-image, as well as collective behavior and organizational culture.

APPLYING BASIC HCI PRINCIPLES TO SECURITY

In an earlier paper (Sasse et al., 2001), I made a first attempt to demonstrate how exisiting CHI knowledge and principles can lead to the design of effective and usable security systems. As with any technology implementation, characteristics of

- the prospective users,
- their goals, and the task through which they achieve them, and
- the physical and social context in they perform the tasks

set constraints to which the design solution must provide a good fit. The combination and interaction of several characteristics often leads to conflicting constraints; optimization based on well-understood priorities helps to identify the solution that will work best in practice.

Current security mechanisms fail to acknowledge even very obvious constraints and CHI design principles. Minimizing users' workload –physical, but especially mental - is such a principle. Consider the some key characteristics of human memory

- Items stored in memory decay over time – this means that we cannot retrieve items we don't use with 100% accuracy, or at all.
- Non-meaningful items are harder to recall than meaningful ones (such as words or place names).
- Unaided recall is hard (much hard than cued recall).
- We cannot "forget on demand" items we no longer need.
- When retrieval is attempted, similar items compete and thus interfere with each other.

The most widely used mechanism in computer security - password authentication – requires 100% correct unaided recall of non-meaningful items. With the proliferation of passwords, which often have to be changed, the task users face is simply beyond the capability of human memory (unless a password is used so frequently that automaticity kicks in). Furthermore, users receive no feedback when an attempt fails – they cannot tell whether the failure is due to a typing error, and entering a different password. Several applied psychologists have made attempts to devise ways of improving memorabilty of passwords (e.g. Spector & Ginzberg, 1994; Zviran & Haga., 1990), but their proposals have not caught on because they rely on meaningful items, which reduces cryptographic strength of passwords. Security practitioners are very reluctant to make changes to the established mechanism when the password problem begins to outstrip support resources. They look for fixes outside the mechanism *("all right then, write the password down, and just keep it somewhere safe"*, or automatic password reminder facilities), deliberately ignoring the fact that these fixes creates different, but nevertheless significant security risks. Application of CHI principles, however, would lead to the recognition that users need more support for infrequently used passwords, and lead to mechanisms that provide cued recall, allow for some error, and/or provide feedback when error occurs.

CHI acknowledges that users' behavior is essentially goal-driven, and the importance of designs that support users' tasks and workflow. For most users, most of the time, security is a *enabling* task, and this has a profound consequences for users' perception of, and behavior towards, security (see next section). Application of basic task design principles determines that performance criteria for the security mechanism must be chosen in line with the *production* task, and the actions required for the security mechanisms should not interfere with those required for the production task. In most security implementations, however, a general mechanism is chosen to secure the system, without any consideration of the users' tasks and the organization's workflow. The study by Whitten & Tygar (1999) showed how designing a user interface to a security tool (PGP) with no consideration of users' tasks can render it completely ineffective. Adams & Sasse (1999) found that security often conflicts with production tasks and productivity goals. In such cases, users respond by circumventing security mechanisms, and perceive security as something that makes their life difficult. Task and workflow analysis should form the basis of the design of security systems, and not just the interfaces. A usable interface on a mechanism that requires the user to push anything his hands are engaged elsewhere is useless. If users have to respond to enquiries from customers in great haste, a login mechanism with which provides cued recall through a 4-step procedure involving graphics that take a long time to download is not a viable option.

All technology has to function in a specific physical and social environment. Biometrics are sometimes mistakenly promoted as a general solution to the usability problem in security (e.g. Nielsen, 2000) because users are identified through a physical characteristic (such as fingerprint, iris, face, or voice) and do not have to remember any password, PIN, or token. However, like all security mechanims, specific biometrics will only work in certain user-task-enviroment contexts, and not others. Air pollution and hand grease can affect fingerprint sensors, cameras used in iris and face recognition systems require constant lighting and positioning. Biometrics are not acceptable to some users altogether, and to others in some application contexts.

Currently, security policies fail to acknowledge that users' behavior is governed by social and cultural conventions. If a user has forgotten a password, but needs to log in to complete an urgent task, he will ask a colleague. Security policies stipulate that users should not share their passwords. Refusing the request in such a situation, however, makes the colleague appear uncooperative, and means she does not trust her colleague. Kabay (1996) identified the need to employ knowledge from social psychology in the design and enforcement of security policies. CHI has only recently started to consider that users' beliefs, attitudes, motivation, and values provide important constraints for technology design; we currently have tried and tested knowledge and methods for addressing these.

NEW RESEARCH CHALLENGES

Security is, in several aspects, different from other technology design problems. One key problem mentioned in the previous section is the role of security of an enabling task. Security is not a goal most users strive for; rather, it is seen to get in the way of their production tasks. Current CHI knowledge can be applied to avoid making this state of affairs worse: when selecting a security mechanism, we can minimize users' physical and mental load, ensure the mechanism fits with tasks, and takes account of the physical and social context. To achieve this kind of "fit", security practitioners will have to re-think their current approach of to securing systems through general, "maximum strength" mechanisms and policies.

Security and CHI practitioners will need to work together to understand how trade-offs between performance on production tasks and security should be made. Usability for individual users needs to be balanced against the security requirements of an organization, which in turn need to be based on a proper risk analysis. Performance in security is harder to evaluate than other areas, because recording of certain data (e.g. password typed in) would create additional vulnerability. Brostoff & Sasse (2001) demonstrated that testing the performance of a security mechanism in isolation from the task and context in which it is to be used is a waste of time. The challenge is to create test-beds and test environments in which performance of new security mechanisms, and the impact on the production task, can be evaluated in context.

Whilst a well-designed security mechanism will not put off users, it will not entice them, either. In many home and organizational contexts, users lack the motivation to expend the extra effort. Weirich & Sasse (2001) identified a set of beliefs and attitudes held by users who do not comply. The reason fall into 2 main categories

1) Users do not believe the threat to security is "real", and therefore see no need to expend effort required.
2) Users do not believe their behavior makes any significant difference – "a determined attacker will get in anyway", and/or "nobody else follows the rules, why should I?"

Both lines of argument lead to the cost/benefit equation – people will not expend effort if they do not perceive or expect a (potential) benefit for themselves. If it comes to securing their homes, many users will make the effort if they believe themselves to be at risk. In many work environments, however, the users' and organization's goals are not aligned.

To date, many security practitioners have tried to address this problem by enforcing desired user behaviors through sanctions. This approach may work to some extent in the military sector (from which, not surprisingly, many security mechanisms and security staff hail). Most organizations, however, cannot afford to take the same approach – (1) it is too expensive to enforce regulations on a regular basis, and (2) the creative, flexible knowledge workers modern organizations seek to attract would not put up with this kind of treatment.

Adams & Sasse (1999) argued that user training and motivation would help users to *"do the right thing"*. The data from Weirich & Sasse (2001), however, suggest that education and training measures will not work unless users *believe* that they, or people they are about, are at risk. Furthermore, being seen as security-conscious is not exactly desirable in most people's perception: users who follow computer security rules are currently seen as "paranoid" and "anal". Forcing users to behave in a manner that conflicts with their self-image is likely make matters worse by pushing users from "can't be bothered" non-compliance to acts of covert hostility, i.e. sabotage. The image of security needs to be improved – towards something seen as desirable, part of professional image. Changing user perception in this way will require a long and well-thought campaign using social marketing techniques, within organizations and in society in general. Posters in workplaces ("Have you locked your screen?") and rewards for good security behavior are some examples.

A key insight that has emerged from our research over the past 6 years is that employing any measures - such as improving user interfaces to security mechanisms, or mounting education campaigns - will have little effect lasting effect if used in isolation.

Security is a socio-technical system and needs to be designed as such. CHI aims to match technology to human characteristics, but currently does not have a method that aims to design (rather than just specify) desirable user behavior in tandem with technology. As a first step in this direction, Brostoff & Sasse (2001) have adapted Reason's (1990) model of human error (a socio-technical model for improving safety behavior in organizational contexts) to security. Reason's model is a good starting point because safety and security share the "enabling task" problem. Two key differences are that the benefits of safety are more obvious to most people, and that safety does not have adversaries who actively seek to attack.

A key challenge for the future will be to design interactions with security that foster good security behavior, and break bad security habits that have formed over a long period of time. Accompanying education measures cannot be aimed at individual users, the organizational security culture needs to be changed at same time. Unlike many other technologies, security requires managers to be seen to be "leading by example", and enforce user behavior, and be seen to enforce it. Risks and rationale for required behavior have to be transparent to motivate users to do the right thing.

Another key challenge is to understand which mechanisms are acceptable to which users under which circumstances. Outside military environments, acceptability of a security mechanism is necessary conditiona for its effectiveness. Amongst emerging security mechanisms, this is in particular an issue for biometrics. Biometrics have the potential to reduce the physical and mental load on users in many situations (in a recent study, I found that convenience was a huge factor in acceptance) but the fact that a user is identified uniquely means it harbors risks in terms of privacy and identity theft. Users make cost (risk) and benefit (convenience, or "greater good") assessment – relevant factors influencing perception need to be explored prior to implementation

FURTHER WORK

To address the challenges involved in designing usable security, CHI needs to address a number of issues. Clearly, we need to integrate knowledge socio-technical systems research, safety-critical system design, and social psychology into mainsteam design approaches. Furthermore, we need be aware aware that the policies governing the use of a technology need our attention as much as the technology itself.

A final observation is that the CHI research community may be too focussed on novel technologies, and not interested in monitoring effectiveness and efficiency of technologies once they have become widely used. There seems to be an implicit assumption that technologies that are widely used are, by definition, usable. Examples such as password security and email show how technologies that worked well enough when first introduced can evolve into usability disasters over time and with extended use. Unlike with new technology that has obvious flaws, users will not notice problems that build up over time. In this respect, usability is like security – only ongoing monitoring and adaption will keep the menace at bay.

REFERENCES

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

Baker, D.B. (1996) Fortresses Built Upon Sand. in *Proceedings of the 1996 New Security Paradigms Workshop*. Arrowhead, CA.: ACM Press.

Brostoff, S. & Sasse, M. A. (2000): Are Passfaces more usable than passwords? A field trial investigation. In S. McDonald, Y. Waern & G. Cockton [Eds.]: People and Computers XIV - Usability or Else! Proceedings of HCI 2000 (September 5th - 8th, Sunderland, UK), pp. 405-424. Springer

Brostoff, S. & Sasse, M. A. (2001): Safe and sound: a safety-critical design approach to security. Proceedings of the New SecurityParadigms Workshop 2001 (Sept. 10-13, Cloudcroft, NM), pp. 41-50. ACM Press.

Clark, D. &. Wilson, D. (1987) A Comparison of Commercial and Military Computer Security Policies. In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA.

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

Haskett, J. A. (1984). Pass-algorithms: a user validation scheme based on than knowledge of secret algorithms. *Communications of the ACM, 27*(8), 777-781.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D. (1999) The Design and Analysis of Graphical Passwords. *Proceedings of the 8th USENIX Security Symposium*, August 23-36, 1999, Washington, D.C., USA

Kabay, M. E. (1996): Developing and Implementing Organizational Policy. In *The NCSA Guide to Enterprise Security*, Chapter 11. McGraw-Hill.

Lemos, R (2000) *Laptop thieves usually not after data.* http://www.zdnet.com/zdnn/stories/news/0,4586,2629471,00.html

Lipson , D. A. and Fisher, H. F. (1999) Survivability-a new technical and business perspective on security. *Proceedings of the 1999 workshop on New Security Paradigms*, September 22 to 24, 1999, Caledonian hills Canada

Menkus, B. (1988). Understanding the use of passwords. *Computers and Security, 7*(2), 132-136.

Mitnick, K. (2002). *The Art of Deception*.

Nielsen, J. (2000). Security & Human Factors. Jakob Nielsen's Alertbox, November 26, 2000 http://www.useit.com/alertbox/20001126.html

Reason, J. (1990) *Human Error*. Cambridge University Press. Cambridge, UK

Sasse, M. A., Brostoff, S. & Weirich, D. (2001), Transforming the 'weakest link': a human-computer interaction approach to usable and effective security. *BT Technology Journal*, 19 (3), 122-131.

Schneier, B. (2000), *Secrets and Lies*, John Wiley & Sons, 2000.

Spector, Y., & Ginzberg, J. (1994). Pass sentence - a new approach to computer code. *Computers and Security, 13*(2), 145-160.

Whitten, A. & Tygar, J.D. (1999) Why Johnny can't encrypt: A usability evaluation of PGP 5.0*, Proceedings of the 8th USENIX Security Symposium,* August 1999, Washington.

Zurko, M.E. and Simon, R.T. (1996), "User-centered security", Proceedings of the 6th New Security Paradigms Workshop, CA.

Weirich D. & Sasse, M. A. (2001): Pretty Good Persuasion: A first step towards effective password security for the Real World. *Proceedings of the New Security Paradigms Workshop 2001* (Sept. 10-13, Cloudcroft, NM), pp. 137-143. ACM Press.

Zviran, M. and Haga, W. J. (1990). "Cognitive Passwords: The Key to Easy Access Control." *Computers and Security* **9**(8), 723-736.