Usability and trust in information systems

M. Angela Sasse
University College London

While the Office of Science and Technology commissioned this review, the views are those of the authors, are independent of Government and do not constitute Government policy.

1 INTRODUCTION

The need for people to protect themselves and their assets is as old as humankind. People's physical safety and their possessions have always been at risk from deliberate attack or accidental damage. The advance of information and communication technology (ICT) means that many individuals, as well as corporations, have additional ranges of physical (equipment) and electronic (data) assets that are at risk. Furthermore, the increased number and types of interactions in cyberspace have enabled new forms of attack on people and their possessions. Consider grooming of minors in chat-rooms, or Nigerian email cons: minors were targeted by paedophiles before the creation of chatrooms, and Nigerian criminals sent the same letters by physical mail or fax before there was email. But the technology has decreased the cost of many types of attacks, or the degree of risk for the attackers.

At the same time, cyberspace is still new to many people, which means they do not understand these risks or recognize the signs of an attack as readily as they might in the physical world. The ICT industry has developed a plethora of security mechanisms, which could be used to mitigate risks or make attacks significantly more difficult. Currently, many people are either not aware of these mechanisms, or are unable or unwilling to use them. Security experts have taken to portraying people as 'the weakest link' in their efforts to deploy effective security (for example, Schneier (2000)). However, recent research has revealed that at least some of the problem may be that security mechanisms are hard to use or are ineffective. This paper summarizes current research on the usability of security mechanisms and discusses options for increasing this usability and the effectiveness of these mechanisms.

Most security mechanisms are based on access control and checking of credentials, and often users are told 'not to trust anyone in cyberspace'. Most people would agree that minors in chat-rooms should not unquestioningly trust that their conversation partners are who they say they are, and that recipients of con mails should not believe the stories put forward as lures. But the solution to the threats from cyberspace cannot simply be 'don't trust anyone'. Trust is an integral part of our social and business interactions: trust that is warranted will, over time, lead to an increase in social capital and a decrease in the cost of economic systems. The review in this paper points out the underlying dilemma between the need for trust in human interactions and the dangers of misplacing trust in the electronic domain. Finally, this paper identifies some usability issues connected to privacy, which is closely linked to security and trust.

2 USABILITY

Usability of security mechanisms was, until recently, an under-researched area. Zurko and Simon (1996) were the first to point out that current security mechanisms make unreasonable demands on many stakeholders. Users, system administrators and system developers struggle with the workload created by many current security mechanisms, and are overwhelmed by the increasing complexity involved in securing systems at all possible levels (hardware, operating system, network, applications). The problems of system administrators and developers will be briefly considered in the conclusions to this section. The main part of the paper, however, focuses on usability of security mechanisms for users.

The definition of a usable system (based on Shackel 1975) requires that

- the intended users can meet a desired level of performance operating it (task performance);
- the amount of learning/practice required to reach that desired level of performance is

appropriate (learnability);
- the system does not place any undue physical or mental strain on the user (user cost); and
- users are satisfied with the experience of interacting with the system.

These considerations have traditionally been applied to an individual user interacting with the technology. However, most interactions between users and security mechanisms take place in the context of a socio-technical system (for example, a corporate environment) with different stakeholders (Checkland 1999). These stakeholders have different goals and views, which sometimes conflict – for example, the organization may put the task performance of the organization as a whole before satisfaction of the individual user. While outside the corporate context, users may have some degree of choice about security mechanisms and whether they employ them, organizations set security policies, which not only govern the selection of security mechanisms, but also specify the behaviour that users are expected to exhibit. Another issue is that key usability principles (for example, providing feedback or forgiveness) are currently not applied to design of security mechanisms, because help offered to the user could also be exploited by a potential attacker. Usability and security are often seen as competing design goals and it is thus not surprising that the results of the few empirical studies that have looked at usability of security mechanisms have been rather damning. Security mechanisms that have been studied include authentication mechanisms, email encryption and web security; the remainder of this section summarizes the findings and discusses how usability of these specific mechanisms could be improved.

2.1 Authentication Mechanisms

Authentication is a cornerstone of most security systems today, and most users interact with these mechanisms on a daily basis. The login is usually a two-step procedure:

1. identification (entering the user_id or account), followed by
2. verification (matching the password stored for that account to what the user enters).

Some mechanisms can operate as a one-step procedure of identification or verification only.

There are three types of authentication mechanisms:

3. knowledge-based authentication (passwords and passphrases, PINs, graphical passwords);
4. token-based authentication (physical tokens such as smartcards or badges); and
5. biometric-based authentication (using users' physical characteristics such as fingerprint, hand geometry, iris pattern or face).

Some security mechanisms may combine two of these mechanisms as part of the two-step procedure (for example, bank card and PIN).

The vast majority of empirical studies on usability and security have looked at authentication mechanisms. This review uses those findings to ground a detailed discussion of the causes of usability problems with security mechanisms and what options are available for improving that situation.

2.1.1 Knowledge-based authentication

Knowledge-based authentication is by far the most common security mechanism used in ICT today. The cardinal rule of knowledge-based authentication is that the verification item (password or PIN) should exist in two places only: in the system (in encrypted form) and in the user's mind, and should not be externalized (written down) or disclosed to anyone else.

Passwords and passphrases. Passwords consist of strings of alphanumeric characters. To prevent cracking attacks,[1] security experts advise that users must have strong passwords (a non-meaningful string of characters drawn from a large character set, mixing letters, numbers and symbols, and upper and lower case) and many company security policies (see also section on user interfaces) mandate the use of strong passwords. Unfortunately, the functioning of human memory makes strong passwords more difficult to recall. In the study by Adams and Sasse (1999), users reported that they had an increasing number of passwords to remember and regularly encountered problems, particularly for infrequently used passwords.

Sasse et al. (2001) confirmed this with a set of objective data on password performance and concluded that the way in which passwords are currently implemented (non-meaningful items, changed regularly, with many similar competing items) conflicts with the characteristics of human memory (items decay over time unless recalled frequently, cannot forget on demand, similar items compete), especially for infrequently used passwords.

Brostoff and Sasse (2000) provide some insight into failed logins based on empirical data.

- 52 per cent of failed logins are due to users entering the wrong password (37 per cent entered their old password for the same system, instead of their current one, 15 per cent entered their password for another system).
- In 12 per cent of failed logins users seemed to have recalled the correct password, but mistyped it on entry.
- 20 per cent of failed logins were due to the users entering the wrong user_id (account name), rather than the wrong password.

Users' inability to cope with the current number and form of passwords is further confirmed by the quality of passwords users chose. In a survey of 1,200 users of bank access control systems (Petrie 2002):

- 90 per cent of respondents reported having passwords that were dictionary words or names, with
- 47 per cent of the sample using a name (their own name or names of their partners, children or pets); and
- only nine per cent of respondents reported using cryptographically strong passwords, as recommended by security policies.

Yan (2001) points out that weak passwords, as used by 90 per cent of respondents in this study, hugely reduce the time and computing power required to crack passwords.

Even in organizations that explicitly instruct users on how to select strong passwords, many do not comply: Yan et al. (2000) report that 32 per cent of students at Cambridge University had passwords that could be cracked with a quick dictionary attack. Dhamija and Perrig (2000) report that despite instruction and admitting to 'knowing better', participants in their study at the University of California at Berkeley picked weak passwords.[2] Similar results have been reported by studies run in corporate environments, for example, Sasse et al. (2001). Other pertinent findings on password quality from this study are that:

- most users try to increase the memorability of passwords by using one password for several systems;
- more than half of passwords consist of a word with a number at the end;
- users only change passwords when forced to; and
- most 'change' the password by increasing the number by one.

Personal identification numbers (PINs). PINs are used to secure access to applications, either in combination with a token for two-step identification (for example, for cash dispensers), or as a one-step authentication (for example, mobile phones, home burglar alarms). Given their wide usage, the lack of available (published) empirical evidence is disconcerting; many financial institutions conduct internal research, but the findings are never published for fear of damaging customer confidence or reputation. There are informally reported numbers, for instance, that one-third of users use their birth date as their PIN (Anderson 2001). There are anecdotal reports that users write the PIN on the card itself, or other materials carried in the same wallet; some banks have also discovered PINs scratched into cash dispensers or materials surrounding them.

This indicates that PINs are even harder to remember than the standard computer password, which also tallies with results from general research on human memory (Schacter 2002). Sasse et al. (2001), comparing problems reported with passwords and PINs in the same corporate environment, conclude that:

1. infrequently used PINs are extremely vulnerable to being forgotten;
2. even frequently (daily) used PINs are forgotten by the majority of users after very short periods (one week) of non-use; and
3. managing multiple PINs, and/or PINs that are frequently changed, creates even more usability problems than managing multiple passwords.

Graphical passwords. Increasing problems with passwords and PINs have led to a spurt in the efforts to provide more usable knowledge-based authentication mechanisms. Psychological research on human memory (Schacter 2002) has established that:

1. human performance at recognition is far superior to unaided recall, and
2. images are processed and stored differently from words, and are easier to recall.

This knowledge has been applied to the design of graphical user interfaces (GUI) for 20 years now, and more recently has been applied to developing graphical passwords, which authenticate users through recognition of images, or features of images. The two leading examples of such systems are *Déjà Vu* (Dhamija and Perrig 2000) and Passfaces™ (Passfaces 2003). With *Déjà Vu,* users select their clues from a set of random art (randomly generated computer art) and, on login, select their images from a set of distractor images. Passfaces™ is based on a large image base of human faces.[3] Users select one face from each of four panels of nine faces and recognize these images from eight distractor faces on login.

Initial evaluation of these systems indicated huge advantages in memory performance compared to standard passwords. Dhamija and Perrig (2000) report that an initial evaluation of *Déjà Vu* demonstrated much better performance than for passwords. A laboratory-based study of Passfaces™ (Valentine 1999a,b) found extremely good recall rates (over 95 per cent successful logins within three attempts), even after a three-month period of non-use.

These results indicate that graphical password systems have a significant performance advantage for infrequently used authentication. Informal reports from commercial trials, however, indicate that this performance advantage disappears rapidly when users have multiple logins using the same type of image or when the images/faces are changed.

Graphical passwords are not suitable for frequently used authentication because they tend to be slow – graphics slow down the login procedure – and to decrease the chances of an attacker guessing the right cue – users have to go through a minimum of three or four rounds of selection. Brostoff and Sasse (2000) report that logins by students to a coursework server dropped by 70 per cent compared to the standard password login, because the graphical login took 30 to 90 seconds to complete, as opposed to five seconds for the password login. Also, frequent use of graphical passwords in public or semi-public environments (such as public libraries or Internet cafes) increases the chances of shoulder-surfing attackers.

Empirical evidence on knowledge-based authentication. Knowledge-based authentication in the form of passwords and PINs is by far the most widely used security mechanism today. From a technical point of view, password systems are cheap to set up. However, empirical research has shown that the cost of operating this mechanism is unacceptable for individual users and organizations alike.

1. The user cost associated with current password systems is unacceptable for most individual users. There is a high mental workload associated with memorizing and recalling multiple passwords, and cost associated with failed logins. Additional user cost arises because many users worry about not being able to recall passwords, which leads to stress and this, in turn, often creates negative perceptions of, and attitudes to, security mechanisms and organizational security in general (Adams and Sasse 1999).
2. When legitimate users fail to authenticate, they are unable to carry out the work activity or gain access to resources or services. Thus, low task-performance on the login task impacts on performance of the production task. This means individual users are prevented from reaching their goals, which is irritating at best, and very distressing if the goal is important and/or users are under time pressures. In corporate environments, failure to complete production tasks has

a negative impact on the productivity of the overall organization.

3. There are further costs to the individual user and the organization when passwords have to be re-set following a failed login. The user has to construct, memorize and recall a new password. The organization incurs further costs because the re-setting of passwords has to be done by system administrators or via specialist helpdesks; some organizations now expend significant resources on re-setting passwords (Sasse et al. 2001). Many organizations use automated password reminder systems, which minimize the costs for both the individual user and the organizations, but re-issuing rather than re-setting passwords contravenes standard security guidelines (FIPS 1985). Automated credential recovery systems (CRS) can be used to re-set passwords without a human operator (Just 2003), but the cost of setting up a secure CRS, and registering credentials, is high for both organization and user.[4]

The attitude of many security experts is that good security does not come cheap. The results from empirical research on knowledge-based authentication show, however, that the strategies that users employ to cope with the ‘inhuman’ workload that knowledge-based authentication creates makes these systems largely ineffective. The vast majority of users do write some or all of their passwords down – and some security departments even encourage their users to do so in a secure manner.[5]

Another, less often discussed, threat arises from users’ attempts to increase memorability by using the same password across several systems. Whilst the increase in risk from doing this may be low in many corporate contexts (where re-use of passwords may be allowed for low-risk systems), Anderson (2001, p. 39) points out that many users do not consider the consequences in every circumstance: “the password you use to authenticate [yourself as] the customer of the electronic banking system … is quite possibly known to a Mafia-operated porn site as well”.

Similarly, users may see little wrong with disclosing the PIN used on a shared office or mobile phone. But if this is the same PIN as used with their bankcard, this practice greatly facilitates theft by colleagues or family members. Given that individuals who are victims of bank fraud are very likely to have been defrauded by somebody known to them, the need for individuals to protect themselves on shared devices, such as home PCs and mobile phones, is overriding.[6]

Any knowledge-based authentication mechanism will create a certain amount of mental workload for individual users, but the workload is manageable if the number of items is kept low, or if items are frequently used (in which case recall becomes automatic). The problems observed arise from the fact that each user interacts with many systems and devices that have to be protected, and their numbers are likely to increase significantly over the next 10 years.

Research on memory (see Schacter (2002) for a summary) suggests that recalling more than two or three strong passwords is beyond the ability of human memory, and even those would be difficult to recall if used infrequently. Possible interventions include:

1. *Reducing the number of passwords*. In corporate environments, a deliberate strategy to reduce the numbers of passwords and PINs is employed. Some companies are deploying single sign-on, for an example, see V-Go (2003). Even simple measures such as standardizing individual users’ user_id across different systems can help to reduce users’ mental workload and numbers of failed logins.
2. *Provide training and support*. If security needs are such that users have to manage a number of strong passwords, specialist instruction and training on how to construct and memorize passwords, for example, on how to construct passwords or passphrases with a high degree of personal entropy (Ellison et al. 2000), can improve their performance. Passphrase (longer, and hence harder to crack) passwords allow users to use meaningful content (Schneier 2000). This increases memorability, but also the chance of mistyping; given an appropriate number of attempts (see below), passphrases would seem particularly suitable for infrequently used authentication. Other types of support could be allowing users to store hints with a high degree of personal entropy (including images and sounds) in a CRS or personal password manager on a device users carry with them (for example, a personal digital assistant (PDA) or mobile phone).
3. *Recognition rather than recall*. The characteristics of human memory mean it is far easier to recognize an item (aided recall) or action than to recall it (unaided recall). This design principle is pervasive in the design of current-generation GUIs (where users recognize the correct command from a limited set of menu items or icons), and there have been attempts to apply

this principle to authentication mechanisms using graphical passwords. Such mechanisms are likely to work particularly well for infrequently used systems, provided the number of clues used is low, or multiple cues are very distinct. The principle can also be applied to text-based knowledge-based systems: for example, through associative passwords (see Zviran and Haga (1993)) or challenge-response authentication.

4. *Move away from 'all-or-nothing' authentication*. Current password logins fail unless the password is entered 100 per cent correctly, for instance, they are not forgiving to user error. Rather than drawing a complete blank, most logins fail because users mis-type passwords, or enter an old password, or the password for a different system. A key usability principle is to provide feedback to users when their actions are unsuccessful. Current password systems do not provide any feedback about why the login failed and possible actions the user could take to recover, because this could help the attacker. Nevertheless, authentication mechanisms can be made more forgiving. Text-based challenge-response systems, for instance, can be set to pass the user on three correct answers, or four correct and one incorrect, etc. Multi-level authentication (Zviran and Haga 1990) can make systems more forgiving by providing backup when access by password and/or PIN (see below) fails; typically, the user will be taken through an automated or human-interaction credential recovery process. This method is widely used in telephone banking, for instance, but many of these systems are vulnerable because they use publicly available knowledge (for example, mother's maiden name) as credentials, as opposed to 'secrets' (Schneier 2000).[7] Even the usability of standard password authentication can be improved by relaxing some policies. Brostoff and Sasse (2003) conducted a three-month trial in which users were free to have as many login attempts as they wanted and they could at any stage ask for a password reminder. They found that, when the initial login attempt failed, only 53 per cent of users managed to recover within three attempts, but almost all users (93 per cent) would persist and manage to login in 10 attempts or less. Increasing the number of login attempts increases the threat of password guessing by a fellow insider (who may also employ shoulder-surfing), but makes no difference to the threat of password cracking by an outside attacker (which is what most firms worry about).

In the light of usability problems with PINs, it is worrying that manufacturers of smartcards and other forms of token-based authentication systems seem to favour using tokens in combination with a PIN, and that PINs have been proposed as a backup for biometric.

2.1.2 Token-based authentication

Whilst knowledge-based authentication is currently the predominant mechanism, token-based authentication has been widely used in the physical domain. Tokens can be used as a one-step process, for example, swipe cards for door access, but this is a fairly weak mechanism since a token may be stolen or found by a potential attacker, who can use it until the loss/theft is discovered and the token is revoked. Therefore, tokens are more often combined with another method in a two-step process, the combination of bank cards and PINs for cash dispensers being the most widely used example. Tokens are becoming increasingly popular, with the token used for authentication, and the knowledge-based item (PIN) for verification, thus reducing the memory load compared to a two-step knowledge-based procedure. There is no published research on usability issues with tokens or smartcards. Tokens such as the SecurID have been used, with apparent success, for remote access by financial institutions. On the other hand, the high cost of replacing lost tokens and/or lost working time has led companies in other sectors to abandon it.

The city of Turin is currently undertaking the first large-scale attempt to issue smartcards to citizens for access to services and payment of local taxes (Torinofacile 2003). Based on 2,655 smartcards issued, the number of tokens that were lost in the post/stolen in the first six months was low (16). The majority of citizens who registered for the card were male, well educated and aged between 19 and 45; the number of cards issued to males was three times higher than for female citizens. Since most home and small business PCs are currently not fitted with smartcard readers, the trial issued digital certificates for users who needed them. The initial phase has seen a high number of calls to the helpdesk, the majority of which (83) were due to problems with using these digital certificates. The second most frequent problem was that personal details registered about the owners of the cards were incorrect.[8] These insights offer some pointers as to logistical aspects and the costs that are likely to be associated with issuing such tokens to a large number of citizens. At the same time, small businesses, single traders and professionals report significant time savings and benefits from online access and payments compared to paper-based system and access restricted to office hours.

Smartcards can offer additional usability benefits: once the login procedure is completed, the token can be used to carry sessions from one machine to another, thus removing the need to log out or lock the screen when leaving the machine unattended for brief periods. They can also offer additional security features for applications such as credit cards.

One usability concern arising from the increasing popularity of tokens is that users may end up being ‘weighed down’ by a collection of tokens that they find hard to manage. There are two possible ways in which this might be prevented:

1. Single tokens carrying multiple credentials. A single token, such as a smartcard, could be used to store users’ credentials for multiple systems. The single token could either store data for multiple identification and verification mechanisms operated by different organizations (providing the user with a personal ‘credential/password manager’), or have a single strong verification (providing the user with a ‘magic key’). Both approaches would require an open standard for credentials, and the second would also require agreement on a single form of authentication and a high degree of trust between participating organizations. The ‘magic key’ model would create least work for the user, but also create a single point of attack.
2. Miniaturization of tokens. Organizations continue to issue their own tokens and decide their own access control mechanisms, but the tokens are so small (for example, RFID chips) that users can keep all of their tokens on them at all times, for example, in a smartcard-type device to which individual chips can be added.

2.1.3 Biometric authentication

Biometric authentication uses a physical characteristic (the most commonly used ones being a fingerprint, iris recognition, hand geometry and face recognition) to identify or verify individuals. Since biometrics use physical characteristics, they are generally perceived to provide a strong form of identification or authentication. However, many usability experts (for example, Schneier (2000)) dismiss biometrics as an ineffective security mechanism because, unlike knowledge-based items, biometrics are not secret: systems can be attacked by harvesting characteristics from legitimate users (for example, ‘lifting’ a fingerprint from a surface or taking a picture of the eye). As a heuristic, the better that systems protect against such attacks, the more expensive they are.

Most biometric solutions are designed to operate in the traditional two-step mode: the user identifies herself with using a token or user_id, and then presents her biometric characteristic, which is compared to a previously stored template: access to cash dispensers, for instance, could be secured with a card and fingerprint. Templates are reduced versions of the biometric characteristic, mapping a certain number of key data points. As a rule of thumb, the more data points a template has, the more accurate the recognition, and the more expensive the application is to procure and run. Accuracy of identification has implications for both usability and security: lack of accuracy leads to false rejection (keeping legitimate users out, which reduces usability) or false acceptance (letting in an unauthorized user, or mistaking one user for another), which reduces security. For any particular application with given levels of accuracy, the operators have to make a trade-off: minimizing the number of false acceptances made by the application will lead to a higher number of false rejections. Effectively, operators have to make a trade-off between usability and security. Schneier (2003) cites a study that estimates that even a false rejection rate of one per cent could increase the average throughput time for each passenger through airport security by 45 minutes.

An assumed usability advantage of biometrics is that, since individuals always carry their characteristics with them, there is no token that users can forget, lose or have stolen and this therefore minimizes the memory load on the user and supports the usability principle of universal access (Fairhurst et al. 2002). The reality is that biometric security solutions raise a raft of usability issues, for individuals and organizations alike. A significant number of users are temporarily or permanently unable to register a particular biometric. For instance, five per cent of people are estimated not to have readable fingerprints,[10] and blind users cannot register iris images. Temporary inability to register or use a biometric can result from cuts or burns on fingers for fingerprints, or pregnancy or certain types of medication for iris recognition. While temporary inability to use a biometric application might lead to mere delays (decrease in task performance) or annoyance (decrease in user satisfaction), permanent inability to use the system would violate the principle of universal access. Since exclusion of certain user groups is not feasible or acceptable for a wide range of applications, operators have to provide a contingency authentication system (for example, a PIN, though this is likely to cause problems, or staff checking written credentials). The cost of operating a contingency authentication system can increase the cost of the biometric application significantly.

More than any other security mechanism, biometric authentication raises the question of acceptability. For certain reasons, some user groups are not comfortable with the use of biometrics, or with the use of biometric authentication in general, for example:

1. *Religious reasons*. Some religions prevent their members from having their face or eyes photographed, others prohibit touching of artifacts that have been touched by a member of the opposite gender.
2. *Safety concerns*. Some people fear they might be maimed or killed by criminals trying to obtain their biometric. This seems to be particularly prevalent in individuals who have had no personal experience with biometrics (BIOVISION 2003), since for these individuals, the perception of biometrics is fed by depictions in films (for example, of removing eyeballs or hands to overcome biometric access control systems in *Minority Report* or *Die Another Day*).
3. *Privacy concerns*. Some biometrics, such as face recognition, can also be used in a one-step identification process. An issue here is that they can be used covertly (without the individual being aware that she is being identified), for example, in combination with security cameras, to detect known shoplifters, football hooligans, etc. A key concern for many users is whether their biometric data are 'safe'. This concern can be de-composed into two questions:
   (i) How safe is my biometric data? The concern is whether data can be copied or changed.
   (ii) How is my biometric data used? The concern is whether the operator, or anyone else, can use the data for purposes other than those advertized, for example, for tracking users' movements.

   Users weigh these concerns against benefits to themselves and others.
4. *Labour relations*. In corporate environments, biometric authentication is often used as a means of exerting control over employee behaviour – for example, biometrics on a time and attendance monitoring system prevent 'buddy-punching'. Employees have fewer issues with the system provided it works well enough, and they trust the operator of the system (usually their employer) (BIOVISION 2003). However, most people dislike the idea of being constantly monitored and tightly controlled, which is a particular concern with fine-grained monitoring of behavioural biometrics (for example, monitoring keystrokes on a keyboard) (Henderson et al. 1998). Constant worry about not performing, or how behaviour is being interpreted by the 'watchers', can be a significant source of stress.

These concerns will need to be balanced by significant real and perceived benefits to make the technology useful and acceptable. Data from surveys and interviews with individuals and organizations reviewed in the EU Roadmap Project on Biometrics (BIOVISION 2003), indicate that this balance will be hard to achieve for large-scale public security deployments of biometrics. The performance that can be achieved with current systems is not sufficient, the cost of deployment and operation is high and most users currently have no security needs that are addressed by these systems. The perceived benefits are seen as being for 'government', with the 'citizen user' shouldering the cost in terms of use and increased cost of identification documents.

In marked contrast, acceptability of biometric solutions was high for applications in areas with a perceived security need (such as access control for neo-natal wards in hospitals) or if users experienced a reduction in physical or mental workload (such as fingerprint logins replacing multiple passwords and PINs). In general, acceptability of biometric solutions is higher amongst those with first-hand experience of biometric applications or those that have a relative or friend who has such experience.

BIOVISION (2003) identified many commercial applications of biometrics that are likely to succeed. Some of these applications will be in areas with high security needs, where performance with a limited number of registered users can be achieved at acceptable cost. Most manufacturers focus on the financial sector and fraud reduction as the most likely application areas (Coventry et al. 2003). The Director of US National Biometric Test Center, James Wayman, suggested as early as 1998 that "The technology now exists to replace pass codes [PINs] with biometric measures without a substantive decrease in security protection" (Wayman 1998).

However, many banks have ruled out use of biometrics on cash dispensers in the foreseeable future, partly because of concerns about how customers will respond to false rejection,[11] and partly because the cost of the technology is too high. In the UK, the Nationwide Building Society has investigated the potential costs and benefits of biometric applications over a number of years. Trials with fingerprints and iris recognition showed good usability[12] and user acceptance, but the increased cost of cash dispensers (25 per cent) does not make the widespread introduction of such systems viable (McClue 2003). A German study also raised the additional cost of the secure registration process (which has to be performed by trained and trustworthy staff), and the technical and organizational measures required to safeguard customers' biometric templates as key reasons against use of biometric authentication. The same study also concluded that reliability of biometrics was such that customers would have to be issued with a PIN as a backup (Thiel 2001), which is likely to lead to significant usability problems. The entertainment industry employs biometrics for convenient verification (as opposed to strong identification): Disney registers hand geometry with season tickets to stop travel agents misusing season tickets for tour groups, and lap dancing clubs register fingerprints with credit cards on entry and request that customers confirm each order (which will appear on their bill) with a fingerprint.

These developments indicate that, even though biometrics is generally perceived as a security technology, it may be more likely to succeed in areas where it enables business process improvement, leading to improved productivity of services or cost reduction. An example is the use of dynamic signature recognition (DSR), which authenticates users based on the shape of their signature and characteristics of their signing pattern. In contrast to most other biometrics, providing a dynamic signature is also a declaration of will in the legal sense (BIOVISON 2003). DSR means contracts can be kept in electronic form, thus allowing companies to finally enter the long-promised age of the paperless office. The Nationwide Building Society, for instance, is deploying DSR in its branches and aims to store all mortgage agreements in electronic form only, and forecasts significant cost savings (BBC 2002).

2.2 Summary: Authentication Mechanisms

Passwords and PINs were first introduced when computers were expensive and scarce, and anyone attempting unauthorized access had to have physical access to a machine. With the exception of a few professionals, such as systems administrators, each user only had a few items to recall. The arrival of networking technology has increased the number of attacks and attackers that each system faces, and the proliferation of devices that have to be protected means that each user has to manage a multitude of knowledge-based items. In this context, knowledge-based authentication in the form of passwords and PINs as the general authentication mechanism has become unusable, both from an individual user's and an organization's point of view.

At the same time, as this paper points out, there are a number of usability issues with other authentication mechanisms, and – given that most of these are relatively new and largely untried – further issues are bound to emerge with more extensive use. To anticipate usability issues, we have to consider not only the immediate task of using the security mechanism, but also the question of universal access. Knowledge-based authentication inconveniences many users, but presents an insurmountable access hurdle for only a relatively small number of elderly users and some users with learning difficulties. These user groups would have even bigger problems with token-based authentication, which requires them to look after the token, plus usually to have more technical skills. Biometric identification has potentially the lowest mental workload, but any specific biometric technique bars some users because they cannot register the biometrics – in the case of fingerprint, favoured by many politicians because of its success in the context of law enforcement, the number is around five per cent. Authentication of multiple characteristics would solve this problem, but is currently prohibitively expensive; the development of smart cameras, which can capture and process a range of biometric characteristics, would make it feasible.

To conclude that because fingerprint matching works in a law enforcement context it will work for biometric authentication, is misguided: the techniques employed and context of operation are very different.[13] The general public is as unaware of these subtle differences as are many politicians – many find fingerprinting unacceptable precisely because 'it is something you do to criminals'. More than any other mechanism, biometrics face acceptability issues, not only because of such misconceptions and Hollywood depictions, but also because individuals have to place a great deal of trust in the operator of the technology to safeguard their biometric templates and their privacy. If biometric templates are compromised, the consequences for individuals can be severe, particular if one characteristic is used in a variety of applications. Biometric authentication can afford invasions of privacy if technology is set up to collect data beyond the immediate purpose of authentication – for example, to determine who goes where, when, and in the company of whom. BIOVISION (2003) reports that (particularly young and technically knowledgeable) users oppose the use of biometric characteristics on id_cards and passports because they perceive governments would most likely succumb to the temptation of 'function creep'.

Any of the alternative mechanisms will increase the cost of authentication, in some cases substantially, and the question is who will bear the cost. Individual customers are usually not inclined to pay more for better security. In corporate environments, the cost will be weighed against the losses (in tangible financial terms, and/or intangibles, such as reputation). This section has pointed out that application of biometrics, for instance, can be used for business process improvements that reduce cost. For a pure security application, a good cost-benefit ratio will be much harder to achieve.

The answer to the question of which is the most usable authentication mechanism is that 'it depends' – on the characteristics of the user group, and the task, and the physical and social context in which users and the security mechanism interact.

2.3 Security and Tasks

The notion of task is key to considerations of usability in general, and performance in particular. Human behaviour is largely goal-driven, so the effective and efficient execution of tasks that help us attain goals is important. The discussion so far has shown that usability of knowledge-based authentication differs for frequently and infrequently performed tasks. In addition to minimizing the physical and mental workload for users, a well-designed mechanism needs to maximize effectiveness and efficiency of task execution. A mechanism must support the desired outcome, and it must be configured for efficient task execution. An example would be providing a hands-free access control mechanism on a door when there is a need to carry things, or the use of speaker recognition as a means of authentication in a system accessed by telephone.

A further notion of key importance is the distinction between production tasks and supporting tasks. Security – like safety – is a supporting task, for instance, it is not on the critical path to attaining the goal. This means that performance in terms of efficiency is even more critical than for the production task, on which users are focused. If a supporting task conflicts with a production task, users will attempt to work around it or cut it out altogether. If a supporting task requires significant extra effort, and/or interferes with the production tasks (and this is often the case with security and safety measures), users need to understand the reason for this, and be motivated to comply. Failure to provide users with the necessary understanding, training and motivation will result in human error (Reason 1990). The current reality is that security is badly integrated with production tasks, and individual users are often left to make a choice between complying with security regulations or getting their job done – with predictable results. The conclusion is that the selection of a security mechanism and how it is configured cannot be left to security experts; rather, such decisions need to be made in the context of business processes and workflow (Brostoff and Sasse 2001).

2.3.1 User motivation

Many users are not motivated to comply with security regulations. Beyond the conflicts with production tasks, Weirich and Sasse (2001) identified the following key factors in a survey on user motivation and security.

1. Users do not believe they are personally at risk.
2. Users do not believe they will be held accountable for not following security regulations.
3. The behaviour required by security mechanisms conflicts with social norms.[14]
4. The behaviour required by security mechanisms conflicts with users' self image. The perception is that only 'nerds' and 'paranoid' people follow security regulations.

There can be no doubt that security in general, and ICT security in particular, currently suffer from an image problem. Education campaigns (similar to those employed in health education) can be effective, provided they make users believe that they are at risk,[15] but good security behaviour also needs to be re-enforced on a regular basis. The recent notion of persuasive design of technologies

(Fogg 2003) offers techniques for designing systems that intrigue, persuade and reward users for good security behaviour.

2.3.2 Security policies and security culture

At an organizational level, a key change that companies need to undertake is to integrate security into their business processes. This means that the habit of copying ‘standard’ security policies and mandating ‘maximum strength’ security irrespective of security needs, should be replaced by risk and threat analysis appropriate to the business. Many companies already do this, but as Schneier (2003) points out, the interests and needs of all stakeholders are rarely considered, and the economics of security are generally not well understood.

Once security aims appropriate to the organization have been established, role models are essential to change behaviour and rebuild the security culture. This will require buy-in from the top (senior management often exhibit the worst security behaviour because they believe they are too important to bother with ‘petty’ security regulations), and making secure behaviour a desirable trait, for example, by making it part of professional and ethical norms (Sasse et al. 2001).

Brostoff and Sasse (2001) point out that in many western countries, health and safety regulations have led to significant changes in organizational culture with respect to employee safety, and that Reason’s (1990) approach for designing safety as a socio-technical system offers a blueprint for a similar approach in the security domain.

2.3.3 User interfaces to security tools and user-centred design

Many security researchers and practitioners see usability of security as a user interface problem. The most widely known and cited paper on usability and security – ‘Why Johnny Can’t Encrypt’ (Whitten and Tygar 1999) – reports that a sample of users with a good level of technical knowledge failed to encrypt and decrypt their mail using PGP 5.0, even after receiving instruction and after practice. Whitten and Tygar attribute the problems they observed to a mismatch between users’ perception of the task of encrypting email, and the way that the pretty good privacy (PGP) interface presents those tasks to users. There can be no doubt that the security community has not paid much attention to usability until recently and, consequently, few tools have interfaces that fulfil usability criteria. Well-designed user interfaces can reduce users’ workload significantly: the AT&T Privacy Bird,[16] for example, alerts users when a site does not match their specified P3P (Platform for Privacy) preferences, which relieves users from inspecting the privacy policy of each site they interact with.

User-centred design of security mechanisms, however, is more than user interface design. The case of PGP (Zimmermann 1995) presents a good example. The problem lies less with the interface to PGP than with the underlying concept of encryption (which pre-dates PGP), and how it functions. The concept of encryption is complex, and the terminology employed is fundamentally at odds with the everyday meaning of the terms: a cryptographic key does not function like a key in the physical world, and people’s understanding of ‘public’ and ‘private’ is different from how these terms are applied to public and private keys. While some security experts advocate educating all users on how encryption works so they can use it properly, this author argues that security systems should be designed to make it easy for users to do the right thing, with a minimum amount of effort and knowledge.

There are examples showing that this is possible: statistics suggest that only 10 per cent of installed burglar alarms are armed when they should be, because they are too difficult to use. In the Channel 4 TV series, *Better by Design*, designers Richard Seymour and Dick Powell addressed the problem by applying the successful and well-understood car central locking mechanism to the house burglar alarm. The resulting alarm is extremely easy to operate (the system is armed and de-armed with a single key-press), and the device is light and visually appealing, so users can carry it on a keyring (Seymour Powell 2000). Another example of a step in the right direction is Friedman and Felten’s (2002) application of the user-centred approach for their Cookie-Watcher, which was designed to match users’ actual needs and values for privacy (as opposed to security experts’ prescriptions of how users should manage cookies). While users of the AT&T Privacy Bird still have to understand P3P in all its complexity to use it effectively, the Cookie-Watcher only presents users with the information they want, when they want it, and allows them to make decisions about whether to accept cookies. Given that most users’ perception of threats and risks is not accurate, user needs and preferences will need to be complemented by, and reconciled with, output from an expert risk analysis.

2.4 Trust

In the past, interactions between strangers who never met face-to-face used to be rare events. Today, new technologies support an ever-increasing number of interactions between strangers: People who have never met ‘in real life’ buy and sell goods from each other on eBay, spend hours playing against each other on Xbox-live and date via instant messaging. These interactions involve different types and levels of risk and they are only possible if actors have trust in each other and in the systems they use to meet, communicate and transact. Yet, in many recent applications, this essential ingredient has proved difficult to attain: lack of trust in e-commerce applications, for instance, causes many people to stay away from these systems (Consumer WebWatch 2002).

Since trust is a critical factor for user acceptance of cyber-systems and their long-term success, it has prompted a spate of research on human-computer interaction (HCI) and computer-meditated communications (CMC). Most of this research aims to help those designing or deploying such systems: the focus is on increasing users’ trust perceptions, rather than allowing users to make correct trust decisions. The recent surge of empirical studies on trust has also produced a large number of definitions and operationalizations of trust. Given that trust is an everyday term that applies in many different situations, this is not surprising. Several researchers have recognized the need for a trust framework and presented candidates. However, these models address only one type of trust-requiring on-line interaction (for example, e-commerce (Corritore et al. 2003; Egger 2001; Riegelsberger and Sasse 2001)) or focus on trust as a psychological construct (McKnight and Chervany 2000). There is a need to unify these different perspectives on trust and – more importantly – to link them to structural dimensions that differentiate situations that require trust. The following provides a summary overview and discussion of the factors that have been identified.

Trust is only required in situations characterized by risk and uncertainty. Only if something is at stake, and only if the outcome is uncertain, do we need to trust to engage in the situation. The simplest possible trust exchange involves only two actors – the trustor (the trusting actor) and the trustee (the trusted actor). Normally, both have something to gain by conducting the exchange – this might involve money, but also information, time or other goods that have value to the actors. Prior to the exchange, trustor and trustee have information about each other before they engage in the exchange. In interactions in cyberspace, many of these interactions are dis-embedded (Giddens 1990), since the actors are not in the same physical or time context. In e-commerce, for instance, the trustor may have to wait for days or week to take possession of the goods and check that they are to her satisfaction. Because of dis-embedding, interactions in cyberspace are riskier and require more trust than similar interactions in a physical context. In addition to having to trust the trustee, users have also to be prepared to trust the technology that mediates interaction (for example, the Internet) and their own ability to use both the underlying technology, and the specific application (for example, the e-commerce website) correctly. For the last two factors, usability is a key prerequisite.

Whether users are prepared to trust and engage in an exchange, additionally depends on a number of other factors that characterize the interaction. Factors that have been identified include:[17]

1. the number of actors involved in the exchange (ranging from dyads to potentially millions in public good dilemmas);
2. the actor type (individuals, organizations, technology such as an e-commerce web site);
3. whether there is synchronous or asynchronous trust exchange (asynchronous exchanges create higher strategic insecurity);
4. whether the user can identify trust-warranting properties;
5. the type of signals employed to communicate trustworthiness (symbols and symptoms of trustworthiness, identity and property signals);
6. the trustor’s propensity to trust;
7. the trustor’s knowledge of the situation;
8. the trustor’s prior experience;
9. the potential benefits expected by the trustor; and
10. the risk to the trustor’s risks (enacted as ‘trusting action’).

This summary illustrates how pervasive the need is for trust in technology-mediated interactions.

Since the technology that mediates interactions in cyberspace is novel and complex for most users, their willingness to trust will be mostly influenced by previous experience with a particular trustee and situation (factors 2, 7, and 8) and assessment of the trust-warranting properties (factors 4 and 5). For interactions with low numbers of actors (for example, e-commerce transactions), it will, therefore, be important that users can reliably (i) identify the actors, for example, that it is easy to determine whether an email purporting to be from my bank is really from my bank, and (ii) identify and interpret the trust-warranting properties in an interaction: for example, are the hundreds of positive votes or reviews I see honest reviews from real customers. Currently, the technology makes it easy to fake identities and trust-warranting properties in cyberspace; consequently, the trust basis for interactions in cyberspace is rather fragile.

2.5 Privacy

Safeguarding privacy is a key concern for many users in cyberspace. On the one hand, security mechanisms can be an essential tool for protecting privacy, for example, because they prevent unauthorized access to data. On the other hand, a security technology can enable invasions of privacy, for example, because it becomes possible to monitor an individual's behaviour closely, or track her movements.

Much of the published literature on privacy concentrates on protecting certain types of data without establishing what people regard as private information (Davies 1997). Expert opinion on what is invasive is a necessary, but not sufficient basis for designing technology that is acceptable in use. Adams and Sasse (2001) found that users' perceptions and values differ from the legal perspective in that:

1. People do not classify data as 'private' or 'not private' – rather, they rate the sensitivity of their information on a continuum.
2. The sensitivity of a particular data item will vary over time and in response to events.
3. The sensitivity of a particular data item will vary depending on who is using the information that can be derived from the data, and for what purpose.
4. Users are less concerned about securing access to data, and more concerned about protecting themselves from the adverse effects that may result from having the information that can be derived from the data used against them.[18]
5. Data do not have to identify an individual to be perceived as private: individuals regard some usage of information about a family unit, a geographic area, or demographic, racial, social or interest group as an invasion of privacy.

Essentially, most peoples' attitude to privacy is pragmatic rather than dogmatic. Rather than treating privacy as an absolute value to be protected, people weigh the risks to their privacy (see point 4 above) against potential benefits that might be derived by providing the data. For instance, in the presence of a perceived safety need (for themselves or significant others), privacy usually becomes a secondary concern. People's decisions to disclose information are mediated by the degree of trust they have in the receiver of the data.

However, this 'pragmatic' attitude should not be confused with privacy not being important. Firstly, the ability to disclose information selectively, depending on perceived risks and benefits and the degree of trust in the receiver, is key to users 'feeling in control' in cyberspace. Secondly, there are many legitimate and beneficial interactions (such as self-help groups, role-playing and games), where anonymity or the ability to adopt multiple personae is seen as essential or important.

3 CONCLUSION

This paper has revealed the range of usability issues that current security mechanisms raise. It has also shown that usable security is not simply an issue of 'fixing' user interfaces to current mechanisms; rather, a change in how individuals, organizations and governments think about security is required. Usable security means appropriate security, and effective security is an integral part of the socio-technical system it is supposed to protect. Effective security has to take into account the needs of all stakeholders, acknowledge that their needs sometimes conflict and find a solution that is acceptable for all stakeholders in ongoing use.

The review has highlighted issues affecting individual users and organizations. There are other stakeholders in the design and operation of security whose needs have not been explicitly discussed. System developers and system administrators are critical of effective security, but currently often make mistakes because of the number and complexity of security issues they have to consider (Zurko and Simon 1996; Flechais et al. 2003). The needs of administrators could be addressed by reducing the amount and complexity of data they have to contend with. Machine learning and agent technologies could be used to summarize and filter information, and data visualization can be employed to help them interpret data and identify critical events.

To address the problems of developers, security needs to be integrated into current development approaches (for example, it should be part of the software engineering documentation developers work with, rather than in a separate document). Design decisions must consider the mental and physical workload mechanisms impose on system administrators as well as end users, and provide them with tools that support their decision-making. The safety community has devised methods for developing systems that do exactly that, and security developers could harness and adapt their approaches.

While the review emphasizes the urgent need to put users' needs and values at the centre of security design, one caveat must be added: most users are not knowledgeable about security, nor do they want to be. Motivational approaches can be employed to change underlying perceptions about security and a limited set of key behaviours, but they will not motivate the majority of users to become security experts. Most users' perceptions of security threats and risks to their assets are highly inaccurate and input from security experts is required to make sure they protect their assets effectively. Security experts, in turn, need to be prepared to design security that is appropriate for, and can work in, a particular social and organizational context, and incorporate basic ergonomic and economic principles in their considerations.

Only systems that support the exchange of reliable trust cues – and thus allow for correct trust attribution – will be viable in the long run. If users find that they cannot rely on their trust perceptions when ordering goods or taking advice via videoconferencing, trust in the technologies and application domains may be lost, or result in a system burdened with costly regulation and control structures. What is sometimes described as a 'lack of trust' in e-commerce or free-riding in peer-to-peer systems is not an unavoidable consequence of technology-mediated exchanges; rather, it is a symptom of difficulties in adapting traditional ways of trustworthiness signalling and trust formation to new structural conditions. This should, however, not be interpreted as 'in time, the trust problem will disappear because people will learn' – negative trust experiences can cause long-term damage to the technologies and/or application domains involved. The damage will not only be to commercial companies – technology providers and organizations offering innovative services – but may also deprive individuals and society of the benefits the technology or service could offer. Such developments would disenfranchise those who can least afford to take financial risk, and/or lack in-depth knowledge and technical savvy to distinguish trustworthy actors from untrustworthy ones.

Safeguarding privacy is a key concern for many users in cyberspace. On the one hand, security mechanisms can be essential tools for protecting privacy, for example, because they prevent unauthorized access to data. On the other, a security technology can enable invasions of privacy, for example, because it becomes possible to monitor an individual's behaviour closely, or track her movements. Biometric technologies, seen by many governments and some security experts as the solution to providing 'strong' authentication, raise particular concerns in this respect. To make biometric applications acceptable, these applications will need to address a perceived security need, or offer other tangible benefits to users.

NOTES

[1] In a cracking attack, the attacker downloads the encrypted password file and tries all possible 'key combinations' to reveal the password. Such 'brute force' attacks take a lot of computing power, or a very long time. Attackers can improve their chances by trying more 'likely' combinations (such as common words) first. Many users do not understand how cracking works, and assume passwords are 'cracked' by an individual trying to 'guess' their password (Adams and Sasse 1999).

[2] The reasons for lack of compliance are discussed later.

[3] Human memory performance for human faces is even better than for other images.

[4] An additional issue is that, since credential recovery occurs infrequently, the clues used would have to be extremely memorable and, at the same time, what Zviran and Haga (1990) call spouse-proof, i.e. not guessable by someone who knows the user well.

[5] Even though writing down passwords is forbidden in most security policies, the security research community is divided on this issue. Schneier (2000) endorses 'secure writing down' (in his case, in a file protected with a long passphrase) as the only way of managing a plethora of passwords, and makes fun of the 'kneejerk' reaction that

traditional security has against it. However, writing the password down violates the cardinal assumption of knowledge-based authentication (that the password should never be externalized in plain text). There are plenty of anecdotal reports and observations that users do externalize passwords and PINs for their own benefit in a way that significantly assists attackers (see section on PINs). Also, since writing down is a form of disclosure, permitting some form of disclosure whilst punishing others makes it harder for users to distinguish between bad and good security behaviour.

[6] This issues also reiterates the need for spouse-proof authentication, see fn. 4.

[7] The use of credentials which are not secrets is becoming increasingly untenable in cyber-society. Users with some technical savvy recognize that such credentials could be used for identity theft, and use fake answers in an attempt to protect themselves. Unless this is done with careful planning (and possibly writing the credentials down); however, fake credentials are extremely vulnerable to being forgotten.

[8] Based on statistics compiled by researchers at the University of Bologna accompanying the trial.

[9] A key usability principle championed, amongst others, by the EU's Information Society Technologies (IST) programme.

[10] Because some people do not have hands, or because their fingerprints are genetically indistinct or have been worn down by manual labour or exposure to chemical (The Economist 2003).

[11] Most users are more likely to blame themselves for failure to memorize a PIN, whereas failure to authenticate on a biometric system is perceived as a failing of the technology.

[12] A caveat that has to be added here is that the users were Nationwide employees, and the machines were situated indoors.

[13] Fingerprinting usually matches 'found' fingerprints against scanned full images of rolled fingerprints (usually taken of all 10 fingers, with expert handlers checking the prints on registration, and no time limits during registration or retrieval), as opposed to matching a template of a partial fingerprint against a registered template. A key usability issue is that the right part of the user has to present the same part of the registered finger that matches the stored template and that many authentication systems have to work very fast to be effective.

[14] Trust is a particularly interesting and relevant example of such a social norm. A user may not want to upset a colleague by locking their screen when they leave the office, because this may be interpreted as a lack of trust. Mitnick (2002) points out that social engineering attacks often exploit the users' reluctance to declare or signal that they do not trust the attacker.

[15] In a context of high security awareness and shared security goals (for example, during the second world war), campaigns with simple reminders of how an individual's behaviour puts them and others at risk may suffice. If people do not believe they are at risk, campaigns need to make the risks and consequences tangible – see, for instance, the current anti-smoking advertisements using real people, dying as a result of smoking, and other graphic imagery illustrating the consequences. Social marketing can have some effect, but changes in behaviour come about mostly when undesirable behaviour is confronted directly by other people.

[16] http://www.privacybird.com/ accessed 17 Apr. 04.

[17] These factors interact with each other, for example, a user's previous experience can raise or lower her general propensity to trust.

[18] An example would be that an organization obtains data about a person from several sources by legal means, and then uses the information that can be derived from the data to classify the person without their knowledge.

REFERENCES

Adams, A. and Sasse, M.A. (1999, 'Users Are Not The Enemy', *Communications of the ACM*, 42(12): 49-64.

Adams, A. and. Sasse M.A. (2001), 'Privacy in Multimedia Communications: Protecting Users, Not Just Data', in A. Blandford, J. Vanderdonkt and P. Gray (eds) *People and Computers XV - Interaction without frontiers. Joint Proceedings of HCI2001 and ICM2001*, Lille, Sept., Berlin: Springer, pp. 49-64.

Anderson, R. (2001), *Security Engineering*, Hoboken NJ: John Wiley & Sons.

Axelrod, R. (1980), 'More Effective Choice in the Prisoner's Dilemma', *Journal of Conflict Resolution* 24(3): 379-403.

BBC (2002) http://news.bbc.co.uk/1/hi/technology/2420143.stm accessed 17 Apr. 04.

BIOVISION (2003) – *Final Report*.,

http://www.eubiometricforum.com/biovision/index.htm accessed 17 Apr. 04.

Brostoff, S. and Sasse, M.A. (2000), 'Are Passfaces More Usable than Passwords? A Field Trial Investigation', in S. McDonald, Y. Waern and G. Cockton (eds) *People and Computers XIV - Usability or Else! Proceedings of HCI 2000*, Berlin: Springer, pp. 405-24.

Brostoff, S. and Sasse, M.A. (2001), 'Safe and Sound: A Safety-critical Design Approach to Security', in *Proceedings of the New Security Paradigms Workshop 2001l*, 10-13 September, Cloudcroft NM, New York: ACM Press, pp. 41-50.

Brostoff S. and Sasse M.A. (2003), '"Ten Strikes and You're Out": Increasing the Number of Login Attempts can Improve Password Usability', paper presented at the CHI Workshop on Human-Computer Interaction and security systems, Ft Lauderdale, April 1-6, http://www.andrewpatrick.ca/CHI2003/HCISEC-papers.html accessed 17 Apr. 04.

Checkland, P. (1999), *Soft Systems Methodology. A 30-year Retrospective*, Chichester: John Wiley.

Consumer WebWatch (2002), 'A Matter of Trust: What Users Want From Web Sites', Consumer WebWatch, Yonkers, NY,

http://www.consumerwebwatch.org/news/report1.pdf accessed 17 Apr. 04.

Corritore, C.L., Kracher, B., and Wiedenbeck, S. (2003), 'On-line Trust: Concepts, Evolving Themes, A Model', *International Journal of Human Computer Studies* 58(6): 737-58.

Coventry, L., De Angeli, A. and Johnson, G. (2003), 'Honest it's Me – Self-Service Verification', paper presented at the CHI Workshop on Human-Computer Interaction and security systems, Ft Lauderdale, 1-6 April, http://www.andrewpatrick.ca/CHI2003/HCISEC-papers.html accessed 17 Apr. 04.

Davies, S. (1997, 'Re-engineering the Right to Privacy, in P.E. Agre and M. Rotenberg (eds) *Technology and Privacy - The New Landscape*, Cambridge MA: MIT Press, pp.143-66.

Dhamija, R. and Perrig, A. (2000), '*Deja Vu*: A User Study. Using Images for Authentication', in *Proceedings of the 9th USENIX Security Symposium*, Aug. 2000, Denver, Colorado, pp. 45-48,

http:/www.usenix.org/events/sec2000/dhamija.html accessed 17 Apr. 04.

Economist (2003), 'Prepare to be Scanned – Will Biometric Passports Improve Security?' *The Economist Technology Quarterly* 6 Dec.: 20-22.

Egger, F.N. (2001), 'Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness', in M. Helander, H.M. Khalid and Tham, (eds) *Proceedings of CAHD 2001: Conference on Affective Human Factors Design*, Singapore, 27-29 June, London: ASEAN Press, pp. 317-24.

Ellison, C., Hall, C., Milbert, R. and Schneier, B. (2000), 'Protecting Secret Keys with Personal Entropy', *Future Generation Computer Systems* 16: 311-18.

Fairhurst, M.C., Guest, R.M., Deravi, F. and George, J. (2002), 'Using Biometrics as an Enabling Technology in Balancing Universality and Selectivity for Management of Information Access', in N. Carbonelle and C. Stephanidis (eds) *Universal Access: Lecture Notes in Computer Science 2615*, Berlin: Springer, pp. 249-59.

Flechais, I. Sasse, M.A. and Hailes, S.M.V.H. (2003), 'Bringing Security Home: A Process for Developing Secure and Usable Systems', paper presented at the ACM/ACSAC New Security Paradigms Workshop, Switzerland, August,

http://www.cs.ucl.ac.uk/staff/I.Flechais/downloads/nspw2003.pdf accessed 17 Apr. 04.

FIPS (1985), 'Announcing the Standard for PASSWORD USAGE', Federal Information Processing Standards Publication, 112, US Department of Commerce, National Bureau of Standards,

http://csrc.nist.gov/publications/fips/fips112/fip112-1.pdf accessed 17 Apr. 04.

Fogg, B. J. (2003), *Persuasive Technology. Using Computers to Change What We Think and Do?* San Francisco CA: Morgan Kaufmann.

Friedman, B. and Felten, E. (2002). 'Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design', *Proceedings of the Thirty-Fifth Annual Hawaii International Conference on System Sciences*, Abstract, p. 247,

http://www.ischool.washington.edu/networksecurity/outcomes.html accessed 17 Apr. 04.

Giddens, A. (1990), *The Consequences of Modernity*, Stanford CA: Stanford University Press.

Henderson, R., Mahar, D., Saliba, A., Deane, F. and Napier, R. (1998), 'Electronic Monitoring Systems: An Examination of Physiological Activity and Task Performance within a Simulated Keystroke Security and Electronic Performance Monitoring System', *International Journal of Human-Computer Studies* 48(2): 143-57.

Just, M. (2003), 'Designing Secure Yet Usable Credential Recovery Systems with Challenge Questions', paper presented at the CHI Workshop on Human-Computer Interaction and security systems, Ft Lauderdale, 1-6 April, http://www.andrewpatrick.ca/CHI2003/HCISEC-papers.html

McClue, A. (2003), 'Nationwide Ditches Iris and Fingerprint Biometrics', 23 September,

http://www.silicon.com/software/security/0,39024655,10006129,00.htm accessed 17 Apr. 04.

McKnight, D.H. and Chervany, N.L. (2001-2002), 'What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology', *International Journal of Electronic Commerce* 6(2): 35-59.

Mitnick, K. (2002), *The Art of Deception*, Hoboken NJ: John Wiley & Sons.

PassfacesTM for Windows (2003), http://www.realuser.com/cgi-bin/ru.exe/_/homepages/index.htm accessed 17 Apr. 04.

Petrie, H. (2002), 'Password Clues, CentralNic',

http://www.centralnic.com/page.php?cid=77 accessed 17 Apr. 04.

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

Riegelsberger, J. and Sasse, M.A. (2001), 'Trustbuilders and Trustbusters: The Role of Trust Cues in Interfaces to e-Commerce Applications', in B. Schmid, K. Stanoevska-Slabeva, and V. Tschammer (eds) *Towards the E-Society. Proceedings of I3E 2001*, Zurich, 3-5 October, Norwell MA: Kluwer, pp, 17-30.

Sasse, M.A., Brostoff, S. and Weirich, D. (2001), 'Transforming the "Weakest link": A Human-computer Interaction Approach to Usable and Effective Security', *BT Technology Journal* 19(3): 122-31.

Schacter, D.L. (2002), *The Seven Sins of Memory: How the Mind Forgets and Remembers*, Boston MA: Mariner Books.

Schelling, T.C. (1960), *The Strategy of Conflict*, Oxford: Oxford University Press.

Schneier, B. (2000), *Secrets and Lies: Digital Security in a Networked World*, Hoboken NJ: John Wiley & Sons.

Schneier, B. (2003), *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York: Copernicus Books.

Seymour, R. and Powell, D. (2000), 'Better by Design – The Burglar Alarm',

http://www.designcouncil.org.uk/betterbydesign/security/challenge.html accessed 17 Apr. 04.

Shackel, B. (1975), *Applied Ergonomics Handbook*, Guildford: IPC Science and Technology Press.

Thiel, C. (2001), 'Voraussetzungen für den Ersatz der PIN bei Geldausgabeautomaten: bankfachliche Anforderungen', paper presented at BIOTRUST Workshop June 5, University of Giessen-Friedberg.

TORINAFACILE (2003), available at: http://www.torinofacile.it/ accessed 17 Apr. 04.

Tucker, A. (1995), *A Two-person Dilemma*, Stanford CA: Stanford University Press.

V-GO SINGLE SIGN-On (2003), at http://www.passlogix.com/ accessed 17 Apr. 04.

Valentine, T. (1999a), 'An Evaluation of the Passfaces Personal Authentication System', Technical Report, Department of Psychology Goldsmiths College, University of London.

Valentine, T. (1999b), 'Memory for Passfaces after a Long Delay', Technical Report, Department of Psychology Goldsmiths College, University of London.

Wayman, J. (1998), 'Biometric Identification and the Financial Services Industry', http://financialservices.house.gov/banking/52098jlw.htm accessed 17 Apr. 04.

Weirich, D. and. Sasse, M.A. (2001), 'Pretty Good Persuasion: A First Step Towards Effective Password Security for the Real World' in *Proceedings of the New Security Paradigms Workshop 2000*, Cloudcroft NM, 10-13 September, New York: ACM Press, pp. 137-43.

Whitten, A. and Tygar, D. (1999), 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0' in Proceedings of the 8th USENIX Security Symposium, Washington DC, 23-26 August, http://www.usenix.org/publications/library/proceedings/sec99/whitten.html accessed 17 Apr. 04.

Yan, J., Clackwell, A., Anderson, R. and Grant, A. (2000), 'The Memorability and Security of Passwords - Some Empirical Results', Technical Report No. 500, Computer Laboratory, University of Cambridge,

http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf accessed 17 Apr. 04.

Yan, J.J. (2001), 'A Note on Proactive Password Checking' in Proceedings of the New Security Paradigms Workshop, 2001, Cloudcroft NM, 10-13 September, New York: ACM Press, pp. 127-36.

Zimmermann P.R. (1995), *The Official PGP User's Guide*, Cambridge MA: MIT Press..

Zurko, M.E., and Simon, D. (1996), 'User-Centered Security' in *Proceedings of the 1996 Workshop on New Security Paradigms Workshop*, Lake Arrowhead CA, New York: ACM Press, pp. 27-33.

Zviran, M. and Haga, W.J. (1993), 'A Comparison of Password Techniques for Multilevel Authentication Mechanisms', *The Computer Journal* 36(3): 227-37.

Zviran, M. and Haga, W.J. (1990), 'Cognitive Passwords: The Key to Easy Access Control', *Computer and Security* 9(8): 723-36.