Journal of Web Engineering, Vol. 3, No. 2 (2004) 095–123

QUANTIFYING THE QUALITY OF WEB AUTHENTICATION MECHANISMS A USABILITY PERSPECTIVE

Karen Renaud[a]
Department of Computing Science, University Of Glasgow

karen@dcs.gla.ac.uk

Received June 3, 2004
Revised September 29, 2004

Users wishing to use secure computer systems or web sites are required to authenticate themselves. Users are usually required to supply a user identification and to authenticate themselves to prove that they are indeed the person they claim to be. The authenticator of choice in the web environment is the simple password. Since the advent of the web the proliferation of secure systems has placed an unacceptable burden on users to recall increasing numbers of passwords that are often infrequently used. This paper will review the research into different types of authentication mechanisms, including simple passwords, and propose a mechanism for quantifying the quality of different authentication mechanisms to support an informed choice for web site administrators.

Keywords: Authentication, metric, memorability, accessibility, security, vulnerability

Communicated by: B White & C Watters

1 Introduction

Digital security is achievable — theoretically — but in practice the human factor plays a major role in subverting the best-laid plans of system administrators and security experts. The user is often referred to as the "weak link" in computer security. As Bruce Schneier [61] points out, people generally don't understand risks, and they sometimes don't understand computers. The Internet has exposed millions of computer-illiterate people to substantial risks they are completely unaware of. Email-attachment viruses prove this admirably: even though users know they ought not to open unexpected attachments they still do; and viruses spread because of a lack of security consciousness.

Users' naïvety with respect to security issues is exacerbated by a mismatch of goals. The goal of the authentication mechanism is to ensure that the current user is not masquerading as another user, whilst the goal of the user is to gain access to the web site to carry out a task. Unfortunately, the stronger the authentication mechanism, the more time-consuming and potentially difficult it may be for the legitimate user to gain access to the system to achieve his/her goals. If the system makes authentication onerous or time-consuming the user will probably find a way around it — especially in an uncontrolled environment such as the Web.

This paper is specifically concerned with the problem of Web authentication; one of the primary examples of the difficulties caused by the effects of "human" factor related to authentication in an uncontrolled environment. A study by Friedman *et al.* [30] found that very few users were concerned about online identity or online interactions. It is interesting to note that this concern was higher in more technologically-aware users, suggesting that increased

[a]Department of Computing Science, University Of Glasgow, 17 Lilybank Gardens, Glasgow, G12 8RZ

exposure had sensitised them to security risks. However, even amongst the high-technology group surveyed, only 14% were concerned about online identity.

Hence even extended exposure to the online world will probably not change the trusting nature of the web user significantly. Thus it is even more important that the security mechanisms are designed with due care and consideration towards the user.

Web developers are often faced with a range of authentication mechanisms which could be used to control access to the system. It is difficult to take all the relevant factors and environmental characteristics of the system into account when choosing a mechanism for a particular system. It would be useful, therefore, to have some sort of method for quantifying the quality of different web authentication mechanisms, from a usability perspective, and not purely from a security perspective. The security of the mechanism is also important and will thus also be included in the quantification scheme, and, together with usability issues, will be used to derive a value that reflects the usability of the specific mechanism. A scheme based on the literature and security practitioners' experience [48, 63] will be proposed in this paper.

2 Quantifying Quality

Quantification is the process by which a particular aspect of an artifact is measured or expressed in terms of a quantity. The quantification process applies a set of applicable metrics in order to assign a particular value, often to support a ranking process. Sometimes the quantification process is done in order to improve the quality of something, such as, for example, software [19, 70, 38]. The ISO 9126 standard defines the characteristics of software quality as functionality, maintainability, usability, efficiency, reliability and portability.

These metrics facilitate measurement of internal qualities of the software components. The pertinent quality of software for this paper is the external quality: the quality of a software component in terms of its *suitability* within a particular environment. In this case we require a context-specific or usage-specific quality measurement process. This paper will introduce a quantification scheme which, unlike most software quality measurement schemes, will not use the above-mentioned quality metrics. This scheme will concentrate solely on the quality of the software in terms of its suitability for the task in a particular domain — the web.

Gilb [33] proposes the following steps for formulating quantitative specifications:

- Identification of the *quality concerns.*
- Assignment of *scales of measure* to these quality concerns.
- Identification of *required quality levels.*

Gilb argues that in order to measure quality it is necessary to break the process down into several measures of goodness, but that the number of facets should not attempt to be exhaustive, rather using only as many facets as are relevant. Ward [70] points out that the metrics have to be viewed in an integrated context to come up with a measure for the total quality.

Following these guidelines, Section 3 discusses authentication in general in order to identify the quality concerns. Section 4 proposes an authentication mechanism quality quantification scheme to identify the measures of goodness which define these quality concerns and to assign the scales of measure to these measures in an integrated fashion. Section 5 further refines the proposal given in Section 4 to take contextual and environmental factors into account. Section 6 discusses the particular characteristics of web authentication in order to identify the quality levels in this environment. Section 7 gives a short synopsis of current web authentication mechanisms and applies the quantification scheme to each to assign a quality coefficient to each one in the context of web authentication. Section 8 discusses the application of the quantification scheme in choosing a particular authentication scheme to suit system requirements. Section 9 concludes.

3 Authentication

Security systems are designed to let authorised people in (the *permission* problem), and to keep unauthorised people out (the *prevention* problem). Furthermore, they need to ensure that people only carry out actions they are authorised to carry out. To this end, all security systems will ask a person to identify him or herself. Once the identification has been accepted,

the person will have to *prove* that identity — which is where authentication comes in [63]. Once the person is authenticated the security system will have to ensure that users can only access what they are authorised to access.

In real-world security systems identification, authentication and authorisation are often merged. For example, a security officer controlling access to a building recognises the people who work in the building (identification and authentication) and they are permitted to enter (authorisation) simply because the officer has recognised their faces. In the digital world the three steps have be distinct to make them tenable. Without this separation each step becomes too difficult. This paper considers one of the most challenging steps — authentication. As Schneier points out [63], authentication does not have to be able to identify a random person as person X, but rather only to prove that person X is who she says she is during the identification step.

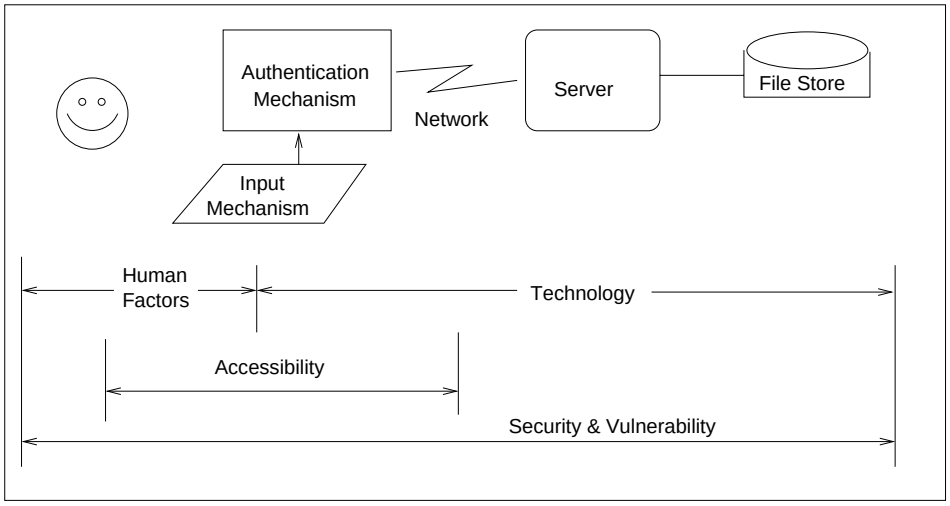

Fig. 1. *Areas of Concern*

Figure 1 depicts the authentication process and identifies the major areas of concern. There are several weak points from a security perspective, with only the first two being considered to have an impact on the usability of an authentication mechanism:

- *User*: vulnerable to breaking by: research-based attack; social engineering attack (such as phishing [62]); or unsecured recording of authentication keys.
- *Point of entry*: vulnerable to shoulder surfing, keyboard tapping, spoofing and trojan horses.
- *Transmission*: vulnerable to sniffers and cracking.
- *Server*: authentication key storage vulnerable to dictionary and brute force attacks.

Users of digital systems *identify* themselves either by means of a token or by means of an identification string such as an email address or account number. They authenticate by what they *know*, what they *have* or by what they *are*. Each authentication option has its own particular problems. Biometric hardware is still relatively expensive and users can be excluded from using it due to amputations or other disabilities. Biometrics have a perceptible failure rate with respect to permission, with false negatives sometimes being experienced more often than is acceptable [17]. They also fail with respect to prevention because biometric digital signatures can be stolen and will let a person pretend to be another.

Authenticating by what a user knows is far more widespread, especially in a web environment, and also has significant problems relating to permission and prevention. Users who

forget their knowledge-based item will not be permitted access and a person who gains access to another user's knowledge-based authentication key will easily be able to masquerade as another user in an uncontrolled environment since identification keys are easily obtained and authentication is the step that really controls access to the system.

Maintaining the secrecy of authentication keys is a particular problem because humans are (in)famously the weak link in information security [48, 61]. People trust each other and will sometimes disclose classified information upon request [48]. Even when people are security-conscious enough not to disclose their authentication key, they will often write down codes they should be memorising. They will do this in self-defence if the codes change too often or if they have too many. These weaknesses are caused by the human factor in security, and no authentication mechanism can succeed in meeting its dual roles of permission and prevention until the human factors are taken into account.

There is an increasing understanding of the user's role in the security of any system, as just one of many links of a chain which can be considered to surround and secure the system. One way to make the user link stronger is to consider essential factors such as the user's needs, abilities, inclinations and skills in formulating security mechanisms and policies. The following sections will consider the areas which pertain to a user-centred approach — accessibility, human factors and security & vulnerability — in turn.

3.1 Accessibility

The general trend today is towards inclusivity. Technology is no longer an optional item but something which everyone needs to be able to use. Hence the issue of accessibility is also important when one considers security.

Accessibility ensures that everyone, regardless of cognitive, mobility and sensory skills, can use an authentication mechanism [50]. This includes disabilities such as hearing, sight, mobility, learning and colour, which are pertinent in an authentication context. In Europe, website designers have a legal obligation to ensure that disabled users receive the same information.[b] In one of the first cases based on the new laws, Barry Maguire successfully sued the Sydney Olympics Organising Committee for having an inaccessible web site [29]. Since 8.5 million people in the UK alone have some form of disability this is a very important issue.

Accommodating learning disabilities such as dyslexia[c](15% of the population) is a challenge because the disability has so many different forms. For most dyslexics though, words are a problem, and text is a primitive on the web and the memory of text is relied on by many authentication mechanisms. Dyspraxic users[d](10% of the population) have difficulty remembering sequences, which impacts on any mechanism that relies on memory of a sequence. Prosopagnosic users[e](prevalence unknown) cannot easily recognise faces which affects their usage of face-recognition authentication mechanisms. Colour-blind users (8% of males) have difficulty distinguishing colours, which will affect any image-based authentication mechanism.

Some disabilities are permanent — such as blindness — but some are caused by advancing age or accidents. Colour blindness can be a late-onset problem, and it has been shown that older users identify faces with less accuracy than younger users [72]. Thus the authentication mechanism should be able to accommodate changes in user abilities over time as well.

The difficulty of accommodating users of all types can be illustrated by an example. Blind users tend to use screen readers and web developers are thus instructed to add a textual pop-up to each image so that the screen reader can describe the image to the user and not to use image gratuitously. For dyslexic users, on the other hand, the advice is that basic concepts should be demonstrated by means of an image rather than a textual description [15]. True universal accessibility is a complex issue — there is no "one best way" that will accommodate everyone, and this will be demonstrated in Section 7 when different authentication mechanisms are evaluated.

Accessibility also applies to levels of technical skills and literacy as well as the quality of the user's equipment [50]. Thus authentication systems that require special hardware, software

[b] www.rnib.org.uk
[c] www.interdys.org
[d] www.dyspraxiafoundation.org.uk
[e] www.faceblind.org/research

or technical expertise may also exclude users and violate the general principle of accessibility in an uncontrolled environment.

Finally, the convenience of the authentication mechanism is a very important factor in the usability thereof. Users can be overly sensitive to systems that waste their time [27] — especially when they consider the system's contents to be less than essential. They tend to accede to security requests only up to a point and become annoyed if these are too time-consuming. This also becomes an accessibility issue, especially for users accessing a system via a modem. There are basically three stages in authentication that should be considered from the convenience perspective:

- *enrolment*: first use of the system, when the authentication key is assigned. The time spent here is usually one-off and a comprehensive enrolment process is likely to pay dividends later. For example, information provided at this stage can be used effectively at the key replacement stage.
- *authentication*: subsequent usage of the system, when the user is authenticated prior to entry. The price paid at authentication time will be paid repeatedly and is thus the most important stage convenience-wise. Brentano and Wiseth [11] cite Bellcore as stating that time spent logging in can take as much as 44 hours a year for a user with four applications.
- *replacement*: this step is necessary when the user's key is no longer valid. It can prove very expensive for an organisation if it is not automated — Murrer reports that half of all help desk calls are related to passwords [51]. There are a number of techniques for replacing an authentication key [47]:
  - *In-Person Identification* — In a controlled environment this option is the best since it is legally defensible. It is very time-consuming and inconvenient though.
  - *Faxed Documentation* — This provides a tangible record of the replacement but is not necessarily very secure and requires users to have access to a fax machine.
  - *Email Recovery* — this is probably the most convenient mechanism but also the least secure since emails are often sent in the clear and if an attacker is able to intercept the email he or she will be able to access the account easily.
  - *Encrypted Email Recovery* — encryption prevents interception but only works if the user is able to provide a public key.
  - *Question and Answer* — the user provides answers to a set of questions at enrolment time, and these questions are then used to prove identity when the user needs to replace the authentication key [31]. This mechanism will probably foil the opportunistic attacker but not a targeted attack where the attacker has done research on the user.

  The convenience of this step is not as critical as the authentication stage, but system administrators have walk a fine line between ensuring identity of the person requesting the key and making the legitimate user feel like a criminal because he or she has lost or forgotten an authentication key.

3.2 Human Factors

Humans receive information from their senses. The human information processing process is depicted in Figure 2. The information received by these senses is interpreted in terms of previous experience. The information passes from the sensory short-term storage to short-term memory — also referred to as *primary memory* (PM). The information in the primary memory will be encoded within the *long-term memory* (LTM) only by further processing [52]. This processing usually entails the organisation of the new information in terms of previously encoded information, or the categorisation or other encoding of the new material. Hence the information is only stored in the LTM once it has been understood and interpreted.

Items can be encoded by linking a new item to previously learnt items — making it meaningful, which eases recall. Deducible items are even easier to retrieve, since the person

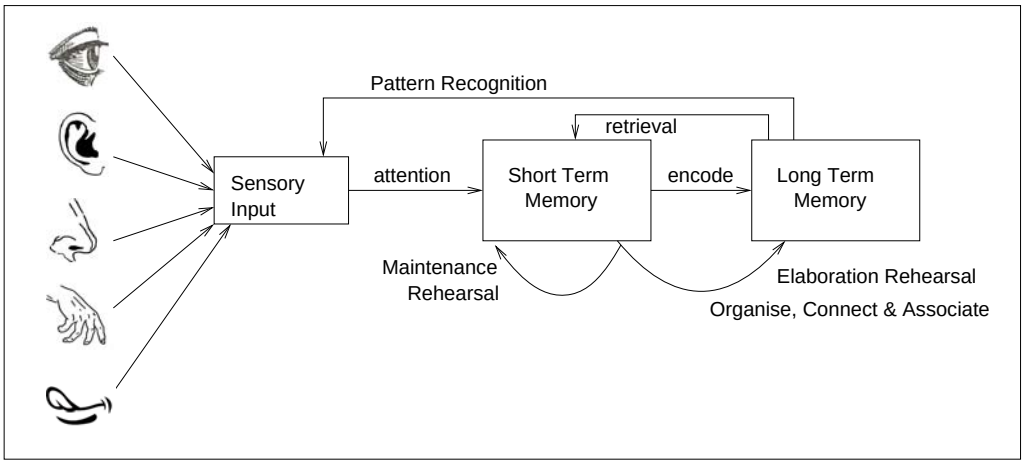

Fig. 2. *Memory and Information Processing*

can reconstruct what he/she did at encoding time, and retrieve the item that way [18]. A non-meaningful item can be learnt effectively if the person puts some effort into learning it, but it will probably decay within approximately 30 days [24].

The encoding process is relevant insofar as we need to understand the circumstances which will support long-term recording and retrieval of knowledge-based authenticator keys. An authentication key can only be retrieved after a delay if it is stored in LTM — any information stored in primary memory will dissipate as soon as new information is presented to the senses. Information *can* be maintained in PM for a period if the person engages in specific activity to keep it there. For example, the verbal repetition of a particular number will keep the number in the PM store, but will not send it to the LTM store unless some meaning is attached to the number. Verbal repetition is referred to as *maintenance rehearsal*, and is essentially a cursory and superficial processing of the information. If the authentication key is to be retrieved later some specific effort must be made to encode it — an activity which is called *elaboration rehearsal*.

Retention is a direct function of the depth of processing at encoding time, which is determined by the amount of attention paid to the activity, and the processing time available. Hence cursory processing of a knowledge-based item almost guarantees that it will decay within minutes or hours. If an effort is made to learn the non-meaningful item it will be encoded in memory and will be lost in a matter of days or months at best. If the item is meaningful to the person, he or she will be able to encode it in relation to previously-learnt or known items. If the item is not meaningful, but the user is able to come up with some scheme to derive it, this is even more helpful in supporting retrieval [18]. A previously-recorded item will be forgotten due to one of the following reasons:

- *Decay or fading.* This can happen if the item was not encoded specifically enough and the person cannot retrieve it.
- *Interference.* This happens when an item in memory interferes with another item. When an older item interferes with a newly-learnt item it is called *proactive* interference and when a new item interferes with a previously-learnt item it is called *retroactive* interference. Items that are similar are most likely to interfere with one another [28]. Hence a weakly encoded list of knowledge-based items will be subject to interference from one another.
- *Retrieval failure.* Items are retrieved from memory by a process called recall, which requires the person to reproduce the item from memory. Retrieval is facilitated by means of established connections with previous structures in LTM. The more connections that

are established the easier retrieval will be later. Uncued recall is the most fallible type of retrieval mechanism, and becomes far more difficult as people age [56].

Sometimes people can be assisted by providing them with *cues* to support recall [68]. For example, people can often recall better if it is possible to re-create the context within which the original item was encoded in memory. An example of this is seen when we are used to seeing a person in a particular setting. If we see that person in an unexpected setting we sometimes have difficulty placing them. The best possible cued-recall situation is constructed when the user is presented with the target amongst a number of distractors and is asked to *recognise* it. Finally, people tend to recognise and identify previous seen images with greater accuracy than words [54], although this effect has not been proved for older users [72].

Recognition can ease retrieval in certain situations, but has its own problems too. If one uses recognition in an authentication situation the target items need to be displayed along with a number of distractors. In terms of making recognition easier the distractors should be semantically different from the target items. In terms of unpredictability one has to ensure that this semantic difference does not make it easier for an intruder to easily identify the target items. Visual PIN (VIP) [4], for example, may have a visual PIN composed of a lemon, an oak leaf, a chair and a rabbit. They would not use a distractor such as an orange or a fig leaf since that might cause confusion in the user's mind. They would perhaps use a fish, a clock, a precious stone, an olive, an egg and a camel. These are semantically different but do not necessarily make it easier for an intruder to identify the correct pictures.

3.3 Security

Identification, authentication and authorisation are steps that secure access and information. Information security ensures that confidentiality of data is protected, that integrity of data is ensured and that non-repudiation is supported [69]. On the other hand, security mechanisms should also ensure that the mechanism being used to authenticate users is commensurate with the access being provided. Thus critical access which can cause loss of life requires a much stronger authenticator than non-critical access to a shared resource.

The technical approach to information security typically works on encryption of passwords during transit and storage, auditing of user accounts and monitoring of log files to detect illegal activities. The human aspects of information security require that attention is paid to other aspects of the process too.

A provably infallible authentication mechanism is a necessary requirement for non-repudiation. Unfortunately none of the current mechanisms can make this claim. Infallible identification is made even more difficult if users disclose their authentication key, or if they record it and it is stolen. Some authentication mechanisms make it easy for users to do this, and some are inherently weak and make it easy for other users to observe authentication keys during key entry.

If a computer user is allowed to self-select an authentication key it is necessary for the authentication mechanism to provide a wide enough choice of keys to ensure unpredictability. Often users simply make weak choices but sometimes the authentication mechanism offers an insufficient range of possible authenticators and the user cannot choose a key which meets security requirements such as unpredictability. Unfortunately key choices which make the key memorable for users, such as meaningful keys, also make them predictable or guessable.

There are three levels of attackers that security systems try to guard against: external to the organisation, internal to the organisation and close family and friends. In terms of predictability the latter is the biggest threat.

There are some specific characteristics of different authentication mechanisms that can be used to evaluate their vulnerability:

- *Breakability & Crackability* — how easy is it to work around the mechanism; to gain access to the system or algorithm that generates the authenticator in some other way. This can happen for one of the following reasons: the software can be incorrectly configured, the remote authoring and administration tools open holes, insider threats are overlooked, and the organisation sometimes doesn't have a security policy [67]. Finally,

how much computing or research time is needed to work out what the authentication key is?

- *Change regime* — does the authenticator age and is there a specific enforced expiration time, or are users permitted to use the same authentication key as long as they wish to?
- *Restricted login attempts* — many systems only allow three attempts before the user is required to renew the authentication key. This helps to prevent attackers getting into a system using guesswork. Brostoff and Sasse [13] argue that this should be extended to 10 attempts, and further aver that this will not make the system any more vulnerable to threats from outside the organisation. Whatever the actual number, attempts are usually restricted and thus this factor will not be included in the metric.

The authentication mechanism will either make or break the security system and it should be chosen with due afore-thought to support the kind of security required by the data being protected or the access being provided.

3.4 Context & Environment

Each of the preceding sections has discussed issues which are important to the authentication process in terms of the factors that affect the process in general. However, one also has to consider the effects of the context within which the user makes use of the authentication mechanism. For example, sometimes the organisation will have security policies which require regular renewal of authentication keys. This impacts on the users because they have to repeatedly learn a new key. Another important factor is how often the user will make use of the system. If the system is used infrequently it is even more important for the key to be memorable. One also has to take users' security motivation into account. Organisations can attempt to enforce good security practices, which should raise security awareness, but sometimes this can be counter-productive. If users are forced to renew their authentication key regularly they will do so, but they will probably choose predictable keys, or use the same key with a different appendage, in order to make it easier for them to remember the frequently-changing key.

Auditability entails real-time archival and retrieval of events and audit trails in order to identify suspicious events. The system is only really secure if someone is regularly auditing it and trying to spot suspicious events. Otherwise attackers will gain access and use this access to possibly do real damage before their presence is noticed.

When choosing a usable and suitable authentication mechanism it is important to consider both human, security and environmental factors. Having a suitable quantification mechanism is one way of discriminating between different authentication mechanisms. The following section will explore the relative merits of quantification for this purpose. The following section will propose a quantification scheme to support system designers in choosing the best authentication mechanism for their particular system.

4 The Quality Coefficient

An authentication mechanism should be totally accessible, totally memorable and secure the system completely. However, the reality of the situation is that authentication mechanisms often have deficiencies in one or more of these areas. Four fundamental authentication mechanism deficiency dimensions can be identified from the discussion in the previous section: *accessibility*, *memorability*, *security* and *vulnerability*. A *deficiency value* can be calculated for each of the dimensions and these values used to derive a quality coefficient for an authentication mechanism.

Each deficiency dimension is composed of three distinct *aspects* which will be used to derive a value for the deficiency dimension. The variations in the dimensions are not necessarily absolute but should be viewed as a continuum where some quality can be sacrificed rather than an all or nothing situation. The *deficiency* with respect to each of these dimension aspects will be determined so that this can be used to determine the quality of the mechanism. To this end, each deficiency dimension aspect is assigned a value ranging from 0 to 1 — as described below — and then a method is outlined for using these values to arrive at a single value indicating the deficiency of a particular authentication mechanism for each dimension.

The final generic quality coefficient can be calculated once all deficiency values have been derived. The mechanism outlined below proposes one possible way of quantifying the quality of authentication mechanisms to support measured comparison.

The axis representing each dimension aspect has an equal weight; all axes have the same length. This means that each dimension aspect used to quantify the deficiency dimension is equally important in the calculation of a deficiency value. When no significant problem occurs in the particular dimension aspect, the value zero is assigned to the axis, while a maximal deficiency will be assigned a value of 1.

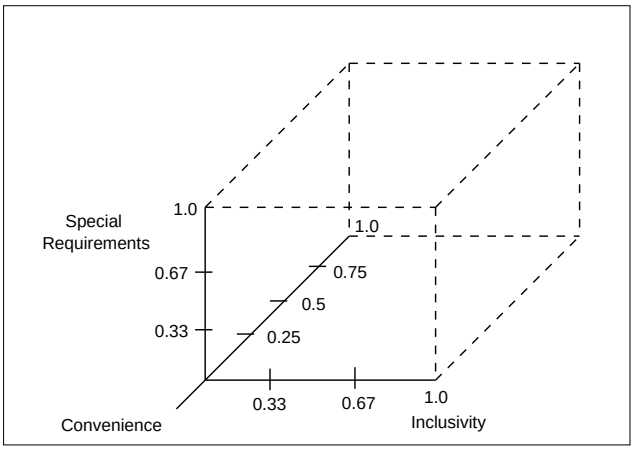

Fig. 3. *Accessibility*

1. **Accessibility:** Figure 3 depicts the various aspects of this dimension, which reflects how easy it is for users to use a system with a particular authentication mechanism. Each dimension reflects a different aspect of the accessibility of the mechanism. The first measure reflects the expectations of the mechanism in terms of extra software, hardware or technical expertise. Since time to authenticate is a strong predicator in determining whether a mechanism is acceptable to users or not the second measure reflects this. The third measure reflects accessibility with respect to users with disabilities. The axes are:

   - *Special Requirements* — This addresses the minimum system configuration (hardware or software) and technical expertise required to support the authentication mechanism. If only one of these is required at the user's machine a value of 0.33 is assigned. If two are required a value of 0.67 is assigned and if all are required a value of 1 is assigned.
   - *Convenience* — There are three aspects of convenience: enrolment time, authentication time and key replacement time. Authentication time is the most important so a deficiency of 0.5 is assigned to time-consuming authentication. A value of 0.25 is assigned the mechanism is time-consuming at either enrolment or replacement. A value of 1 results if all stages are time-consuming.
   - *Inclusivity* — This addresses the issue of the exclusion of users. Since disabilities could be cognitive, mobility or sensory we will assign a value of 0.33 to each category of disability. Hence if a mechanism excludes only users with cognitive disabilities only 0.33 is assigned. If users with both cognitive and sensory disabilities are excluded a value of 0.67 is assigned and if users in all categories are excluded a value of 1 is assigned. It may be impossible to find a mechanism that does not exclude users with at least one type of disability, thus a small deficiency is assigned to only one kind of exclusion.

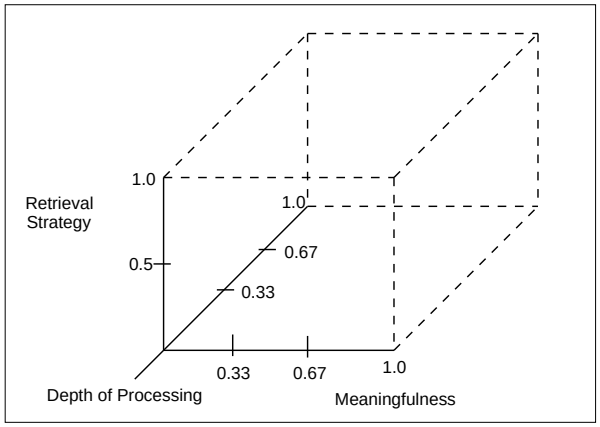

Fig. 4. *Memorability*

2. **Memorability**: Figure 4 depicts the various aspects of this dimension, which reflects the importance of the memorability of authentication mechanisms. Most authentication mechanisms are knowledge-based so this dimension is important. Each aspect reflects different characteristics of the ease with which users will be able to memorise and retrieve the authenticator.

   - *Retrieval Strategy* — Users find it easier to recognise than to recall, especially with advancing age. Hence a value of 0 is assigned to recognition and a value of 1 to recall. A value of 0.5 will be assigned to a mechanism that relies on recall, but provides cues to support the recall process, since cued recall and recall within context make it more likely that the user will remember their authenticator than in an uncued recall situation, as discussed in Section 2. These values are assigned because of the way that users will typically deal with authentication as a necessary evil. Self-assigned authentication keys will often be assigned with the goal of getting into the system as quickly as possible and users will seldom not make an effort to "learn" the key. In this kind of situation recognition is superior to recall [23].
   - *Meaningfulness* — Humans remember things better if they are meaningful. Hence if the authenticator is self-assigned and deducible by means of a special scheme a value of 0 is assigned. If it is self-assigned and meaningful to the user, a value of 0.33 is assigned. If it is self-assigned but not necessary meaningful or deducible a value of 0.67 is assigned. If it is assigned arbitrarily by the system a value of 1 is assigned.
   - *Depth of Processing* — Humans remember things better if, at the encoding stage, there is some cognitive activity associated with the process [35]. The cognitive activity involved in the encoding of an authenticator based on something the user knows will determine how well the user can retrieve the authenticator later. A value of 0 is assigned to an authentication system does not require effort to remember (such as biometrics).

     A value of 0.33 if the user is required to use a particular level of processing at enrolment time — this increases the likelihood of the authenticator being remembered later. A value of 0.67 is assigned if a visual mechanism is used rather than a text-based mechanism, since humans remember visual images better than words. A value of 1 is assigned if only cursory and shallow cognitive activity, such as maintenance rehearsal, is involved at enrolment.

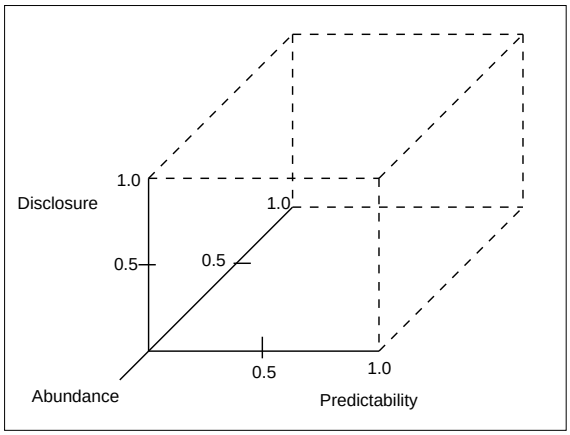

Fig. 5. *Security*

3. **Security**: Figure 5 depicts the various aspects of this dimension, which reflects the different security aspects of the authentication mechanism.

   - *Predictability* — Predictability of an authentication key is a big issue: the plethora of password choice recommendations on the web is a testimony to the tendency of people to choose weak authentication keys. A value of 0 will be assigned if the authentication key is completely unpredictable, as is the case for a public encryption key. A value of 0.5 is assigned if the key is predictable only to friends and family and a value of 1 is assigned if the key is predictable to a wider audience of attackers.
   - *Abundance* — The user should be able to either choose from, or be assigned, one of a wide number of possible authenticators. Abundance has a direct effect on the breakability of the authentication key — hence the more keys there are in the dictionary space, the longer it will take to break the key. A value of 1 will be assigned if the key is unique and irreplaceable, such as biometric keys, or if fewer than 2^{40} keys are available since that can be broken in less than a day. A value of 0.5 will be assigned if there are more or less 2^{50} keys available since that can be broken in less than a month. A value of 0 will be assigned if the range of keys is greater than or equal to 2^{64}
   - *Disclosure* — An authenticator should not be disclosed to another user, otherwise authentication fails. Hence a value of 1 will be assigned if a user can easily record his authenticator and it can be either purposely disclosed, or stolen by, another user. A value of 0 will be assigned if it is impossible for the user to do this, and a value of 0.5 is assigned if it is possible for another user to observe a user's authentication key.

4. **Vulnerability**: Figure 6 depicts the various aspects of this dimension, which reflects the different vulnerability aspects of the authentication mechanism.

   - *Confidentiality* — Authentication requires a user and the system to share a secret. If the user has to supply the full secret at authentication then it is possible for a transmission sniffer to observe the secret, or some other person to observe it, and reuse it. If there is another way for the user to demonstrate knowledge of the secret without revealing the secret that makes the authentication mechanism

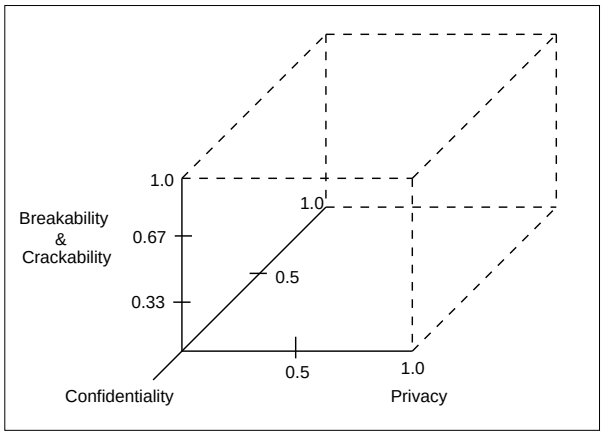

Fig. 6. *Vulnerability*

less vulnerable. Hence an authenticator that relies on the full authentication key being revealed is more vulnerable and a deficiency value of 1 will be assigned. A value of 0.5 is assigned if only part of the key needs to be revealed. An example of this is when a system asks for a full password at enrolment and thereafter only asks for specific letters of the password — this is often used by telephone banking operators. It prevents the operator from gaining knowledge of the full password and makes the system stronger. A value of 0 is assigned if the key does not have to be revealed or if the exposed key cannot be reused.

- *Privacy* — An authenticator may record many details about the user to support authentication or key replacement, which. if not stored securely, could compromise other systems for which the person is required to use the same details, since a key reused is a key weakened [60, 40]. It can also violate the person's privacy [8, 9]. If an authenticator requires the user to reveal personal details a value of 1 is assigned. If the authentication mechanism allows the user to choose the specific details to be revealed a value of 0.5 will be assigned. This option should be used with caution though, because users may choose bad questions in the same way as they choose bad passwords, and because it is difficult for people to formulate good questions [25]. A value of 0 will be assigned if no personal details are required.
- *Breakability & Crackability* — The values will be assigned depending on the time an attacker would have to spend to attack the authenticator. The higher the price an attacker must pay in terms of time and effort, the less vulnerable an authentication mechanism. A research-based attack is inevitably time-consuming for anyone other than close friends and family. Thus if the authentication mechanism is vulnerable to a research-based attack a value of 0.33 is assigned. If the authentication key is vulnerable to dictionary or brute force attacks, a value of 0.67 is assigned. If the authenticator is vulnerable to a keyboard tapper a value of 1 is assigned. Many users do not have virus software or firewalls running on their home computers and thus this mechanism is particularly cheap from an attacker's point of view. A value of 0 will be assigned if this category does not apply.

The axes of different dimensions can be interdependent — such as, for example, meaningfulness and predictability. This is because there is a close relationship between the various deficiency dimensions as described above and this should be considered beneficial in measuring deficiency because a small deficiency in one area may impact on other dimensions. When

we have values for the three axes of the individual dimension aspects, namely x, y and z, we can work out the final overall deficiency value for that dimension by using the following formula:

$$\bar{n} = \sqrt{x^2 + y^2 + z^2}$$

The maximum value for $\bar{n}$ is $\sqrt{3} =\sim 1.73$. A maximal deficiency of any single axis is significant because if it is maximally violated, it represents 57.7% of the maximum. A maximal deficiency along two axes is 81.6%. This reflects the characteristic of this quantification method which reflects maximal deficiencies far more seriously than multiple minor deficiencies. This is important because a number of small deficiencies are less of an issue than a large deficiency. So, for example, if a mechanism excludes dyspraxic users and is inconvenient only at enrolment time it is not nearly as big a deal as a mechanism that is inconvenient at enrolment, authentication and key replacement time.

After quantifying these four dimensions, we can work out a total quality deficiency taking the four dimensions: *ad: accessibility deficiency*, *md: memorability deficiency*, *sd: security deficiency* and *vd: vulnerability deficiency* into account. Now finally we can work out the deficiency value, $\overline{d}$, for the authentication mechanism as follows:

$$\overline{d} = ad + md + sd + vd$$

The maximum length of each dimension (ad, md, sd, vd) is 1.73 so that the maximum value of $\overline{d}$ will be $1.73 * 4 =\sim 6.92$. A single value can therefore represent a measure of the deficiency of a particular authentication mechanism. The final quality coefficient for any authentication mechanism is then $\bar{q} = 7 - \overline{d}$. A quality coefficient of 7 will imply a high quality authentication mechanism and as the coefficient nears 0 the quality of the mechanism declines.

The identified dimensions are not necessarily equally applicable or relevant for authentication mechanisms used in differing environments. A proposal for tailoring the coefficient to reflect the quality of authentication mechanisms used in particular environments will be presented in the next section.

5 Environmental Factoring of the Coefficient

Environmental factors were not considered when the quality coefficient was calculated in the previous section, and this weakens the measure as a determinant of its efficacy within the particular environment and in relation to other authentication mechanisms being used in similar environments. The former will be referred to as *usage* factors and the latter as *association* factors. To accommodate these factors, particular characteristics of the environment, as they apply to the different deficiency dimensions identified in the previous section, are quantified in terms of both usage and association environmental factors. We will use these usage factors to modify the deficiencies for each dimension by applying one of the following modifier values: 0.5 (reduced), 1.0 (nominal) or 1.5 (increased). The usage factors in each dimension are:

Accessibility:

- *Control of Environment* — this refers to the extent to which the environment can be controlled. So, for example, a web environment is potentially completely uncontrolled; whereas an ATM is an example of a controlled environment because the network used to communicate with the server is not public and it is a relatively easy matter to control extra hardware and software that is required by the mechanism.

  This factor determines how important the accessibility dimension will be in the calculation of the final quality coefficient since accessibility factors can be easily alleviated in a controlled environment. We thus define a factor, called *control* to represent this. If the environment is uncontrolled a value of 1.5 is assigned and if the environment is controlled a value of 1 is assigned.

Memorability:

- *Frequency of use* — this refers to the frequency of use of the particular authenticator. Usage can be categorised as low (less often than once a month), medium (once a week) or high (daily). More frequently used items will be remembered more easily [43] so a daily usage will seldom cause memorability problems and since people remember items with comparative ease for a month medium usage should cause only minor memorability problems. Requiring a user to remember at longer time spans will inevitably fail.

  A factor called *use* is used to quantify this. A value of 0.5 is assigned to *use* if the system is used daily, 1 if usage is weekly and 1.5 if usage is monthly or less.
- *Forced renewal* — this refers to the organisational rules which force the users to change authentication keys. Adams *et al.* [2] have shown that restrictive policies like this will actually reduce the security of the system since the more restrictive the security mechanisms, the more likely users are to subvert them. A factor called *renewal* is defined and 1 is assigned if the organisation does not enforce regular changes or 1.5 if they do.

Security:

- *Risk* — this refers to the information being protected or the kind of access being granted. If the access being provided is not critical then the security deficiency becomes less important; but if the data being protected or the access being provided is critical then the security deficiency becomes more important.

  To capture this factor we define *risk* and assign a value of 0.5 if it will not be damaging to the user if another user gains access, 1 if wrongful access can affect only the user him or herself. If wrongful access can affect more than one user a value of 1.5 is assigned.
- *Security Motivation* — this refers to the degree to which the environment can impose sanctions to force the user to act in a secure and responsible way [1]. We define *motive* to capture this factor: if some sanction can be applied to the user who behaves irresponsibly a value of 1 is assigned; whereas a value of 1.5 is assigned in a situation where the user is uninformed about security issues and cannot be forced to take them into account.

  For example, in a controlled environment one can come up with schemes which allow legitimate users to gain emergency access to unauthorised data if they consider such access to be critical at a particular point in time [58]. The system must have built-in logging processes and the organisation must have particular procedures for observing, approving and reversing any changes made during such accesses.

Vulnerability:

- *Auditing* — a system that actively audits in real-time can be less vulnerable to attacks. Such auditing procedures can activate some other security measure if something suspicious is detected. We define a *audit* to capture this: a value of 1.5 is assigned if no auditing is done and a value of 1 if auditing is carried out.

The *association* factors are (a) how widely the mechanism is used in the environment and (b) the design difficulty associated with the mechanism. These factors will tend to cancel each other out. A ubiquitous mechanism is probably well understood and has fewer design difficulties whereas a novel mechanism often presents unexpected design challenges when it is first used. Hence these factors will not be used directly in the calculation of the environmental quality coefficient.

One way of including all the environmental factors in the deficiency calculation is the following, with the deficiency value $\overline{d_{env}}$, for the authentication within the particular environment as reflected by the above-mentioned factors being calculated as follows:

$$\overline{d_{env}} = ad * control + md * freq * renewal + sd * access * motive + vd * audit$$

The maximum length of each dimension (ad, md, sd, vd) is 1.73 so that the maximum possible value of $\overline{d_{env}}$ using these environmental factors will be $2*(1.5*1.73)+2*(1.73*1.5*1.5) =\sim 12.98$. A single value therefore represents a measure of the deficiency of a particular authentication mechanism in a particular environment. The final environmental quality coefficient for any authentication mechanism is then $\overline{eq_{env}} = 13 - \overline{d_{env}}$.

However, there may be certain situations where a deficiency of a particular aspect or dimension can completely disqualify the authentication mechanism for a particular system. For example, the developer may decide that the system controls access to such critical data that only a completely non-predictable mechanism will suffice. Thus another step is required. After the environmental quality has been determined, certain *critical aspects* will be examined for each mechanism and mechanisms which do not meet the minimal quality in this aspect or dimension will be eliminated from consideration. The following section will consider the particular environment of interest for this paper — the web.

6 Web Authentication

Web authentication adds a new dimension to the difficulty of maintaining security. Authenticating web users is far more difficult than authentication in other, more controlled, settings such as office environments, intranets or ATMs.

The web environment impacts on the three deficiency dimensions as follows:

- *Range of Users*: Making the web accessible to a wider range of users has become an important issue.[f] The ubiquitous use of passwords affects those users with impaired memory skills, such as elderly users and people who have experienced a stroke. So ageing or illness could make a web site inaccessible to a user who was previously quite happy with a knowledge-based authentication mechanism.

- *Web Users are Customers*: Web site administrators have a fine line to maintain between authenticating people properly and not annoying them. People easily abandon websites that are onerous to use. The most important factor here is that it should not be too time-consuming [44] emphasising convenience rather than technical brilliance.

- *Technical Expertise*: Whereas in an organisation one can send employees on courses and ensure that they have all attained a minimum level of competence, in a web situation the range of technical competence will be vast. To make the web site accessible to all users the authentication mechanism is going to have to take this into account.

- *Equipment*: Few assumptions can be made about the hardware and software available to the web user. Design should therefore be based on the principle of lowest common denominator in all areas, to ensure universal accessibility.

These factors are captured to a certain extent by the generic *convenience* and *special requirements* aspects of the accessibility dimension. However, the *control of environment* factor best represents the difficulties encountered by the uncontrolled nature of the web environment.

- *Multitudinous Websites*: The information on the web is increasing by the day. Many organisations now retail on the web too. Many of these sites require users to identify and authenticate themselves. This increases the number of authentication keys users have to remember.

[f] http://www.w3.org/WAI/

- *Infrequent Use*: The nature of the web is such that users will use a website infrequently — since many of the sites are not work-related. Hence any authentication key is unlikely to be remembered after perhaps only one use, and then a delay of months.

The former issue is an association factor and, as such, will not be quantified. The latter is captured by the *frequency of use* memorability dimension factor.

- *Risk*: Web sites are an open invitation to any passing hacker because they have to allow access to all legitimate users. Inside an organisation, on the other hand, protection is maintained by means of firewalls and other sophisticated mechanisms. Thus, a web authentication mechanism should provide keys that are unpredictable and multifarious.

- *Gratuitous Authentication*: Web sites appear to authenticate far more than is required, without much thought given to the information that is being protected by the authentication. Many websites use authentication to collect user data when a far more lightweight approach, such as cookies, could be used. This kind of attitude devalues authentication and makes users careless of their authentication keys.

- *Security Motivation*: Whereas in an organisation one can require and enforce certain levels of security, in a web situation one cannot rely on any level of compliance.

Risk can be factored in using the *risk* factor. The security motivation, which reflects both the second and third issues, is captured by the *motive* factor.

When calculating the quality coefficient of web authentication mechanisms in the following section we will assign the usage environmental factors as follows:

- *Frequency of use (use), forced renewal (renewal), auditing (audit) and type of access (risk)* — site dependent therefore a value of 1 is allocated.

- *Control of Environment (control)* — no control is possible, therefore a value of 1.5 is assigned.

- *Security Motivation (motive)* — We cannot assume any degree of security motivation and indeed the evidence points towards very little awareness [30] therefore a value of 1.5 will be assigned.

Hence the deficiency for each of the mechanisms reviewed in this section will be calculated as follows:

$$\overline{d_{web}} = ad * 1.5 + md + sd * 1.5 + vd$$

and the quality of web mechanisms will be calculated as $\overline{eq_{web}} = 13 - \overline{d_{web}}$.

The critical aspect is the "Special Requirements" aspect, since the authentication mechanism cannot require the use of extra hardware, which would make it completely unsuitable in the current web environment. We can now consider various categories of authentication mechanisms in terms of this general framework. The next section will consider the range of possible authentication mechanisms in terms of this quantification scheme.

7 Authentication Mechanisms & Web Quality

The quality of each mechanism will be calculated based on the deficiency allocated to each dimension, with environmental factors as identified in the previous section. Users are generally authenticated in one of three ways: by what they *are or do*, by what they *know* or by what they *have*. The following sections will discuss each of these categories of authentication mechanisms individually.

7.1 What the User Is or Does

Biometrics mechanisms fall into two distinct categories:

- *Physiological* characteristics which can be based on fingerprints [39], voice [6], iris or retina [16], vein pattern [41], face [75], hand or finger geometry or ear shape [14].
- *Behavioural* biometrics, which can be based on mouse usage patterns [37], key-stroke latencies or dynamics [20, 21, 49, 53, 7]; or signature dynamics.

Biometric systems are not perfect: one will either get false positives, or false negatives, depending on how the system is tuned. Neither of these is particularly desirable, and the direction to which the system errs depends on the criticality of the type of access. So, for example, if the system gives an authenticated user access to a large amount of money the authentication should rather err on the side of false negatives, whereas a system which issues something fairly cheap, such as, perhaps, postage stamps, should rather err on the false positive side.

Biometrics, while appearing infallible, actually suffer from some potentially insuperable flaws. In the first place, they are easy to forge. If a hacker steals the digital image of a user's iris signature, it is easy for him/her to masquerade as the user. It is also impossible for the user to get a replacement iris. Once it is stolen, another biometric has to be used for that user [61]. There is also some difficulty in using biometrics over a wide-area network, since the biometric signature has to be transferred to some central site holding the identity of each user, and this creates yet another security problem.

Furthermore, biometrics are not suitable for use in an uncontrolled environment firstly in terms of convenience because the user's biometric has to be captured securely at enrolment, and this would probably require the user to present him/herself somewhere with a recognised form of identity such as a passport. This authentication mechanism is also susceptible to attack in an uncontrolled environment. For example, a voice authentication mechanism which authenticates over a telephone could be fooled by a tape recording.

Furthermore, every biometric device has its own set of usability issues and more work is required to understand the nature of permanent and transient exclusions to any biometric technology as well as how to guarantee universal usability [16].

The web-deficiency and environmental quality coefficient of biometric mechanisms can be calculated as follows:

```
Accessibility Dimension (ad = 1.56)
    Special Requirements 1     All required [Fails Critical Access Requirement]
    Convenience          1     Significant time at all stages
    Inclusivity          0.67  Visually Impaired, Amputees and Elderly

Memorability Dimension (md = 0)
    Retrieval            0     Neither
    Meaningfulness       0     Competely
    Depth of Processing  0     Not Required

Security Dimension (sd = 1)
    Predictability       0     Unpredictable
    Abundance            1     Once lost or stolen cannot be replaced
    Disclosure           0     Not possible to observe

Vulnerability Dimension (vd = 1.56)
    Confidentiality      1     Full
    Privacy              1     Very private
    Breakability         0.67  Replay attack, reverse engineering, fake finger tests
```

The overall web environmental deficiency is $\overline{d_{web}} = 5.41$. Hence the web environmental quality of biometric mechanisms is $\overline{eq_{web}} = 7.59$

7.2 What the User Knows — Text-Based

The preferred, and almost ubiquitous, Web authentication mechanism is the password. Schneier points out that passwords are an oxymoron — if it is hard for another person to guess, the user will probably either forget it, or record it manually (or on a post-it attached to the monitor) [61]. If it is easy for the user to remember, then someone else will probably either be able to guess it or to break it using a brute-force dictionary attack [73].

Users choose easy (bad) passwords. Password cracking programs regularly break 90% of passwords in any system within the first hour. If the system forces the user to choose a strong password, he or she will probably write it down so that it will not be forgotten. If users are forced to change passwords regularly they will come up with various ways to make it easier for themselves. They may, for example, use two passwords in relay, or use the same password with a concatenated number which is incremented each month.

Many security professionals have little sympathy for the user. Mitnick [48], a reformed social engineer, recommends various policies which will make people more aware of typical attacks and make people resistant to them. These policies address a wide spectrum of security issues. Even though his book deals with user issues his recommendations with respect to passwords are disappointing. He recommends that passwords be changed every 60 days, and that passwords should be 12 characters long, not a word found in the dictionary, be mixed upper- and lower-case, with one numeral and one special character, and not be related to the company or individual in any way. These recommendations are unrealistic because of memory limitations, and demonstrate wide-spread ignorance of human factors in authentication. IT departments need to understand that this kind of advice can make security designs that look good on paper fail [1].

There are three types of passwords: the *syntactic*, *semantic* and *one-time*. The syntactic approach uses a remembered sequence of letters and digits, and is called a password, or a passphrase if it consists of more than one word. The semantic approach relies on the memory of a concept, or a phrase: often called a cognitive password. One-time passwords are in a class of their own since they deal with many of the predictability issues of other passwords but their implementation causes other difficulties.

7.2.1 Syntactical Passwords

There are two approaches to assigning a password; either the user chooses the password or the system assigns one. There is evidence that users remember passwords better if they choose them [76], but the system-assigned password will probably be stronger. Some innovative schemes attempt to assist users in choosing stronger passwords. One example is the Diceware Passphrase[9] They propose a mechanism whereby a hard-to-guess phrase is generated by a sequence of dice throws.

Despite such widespread use passwords have a number of well-known drawbacks regarding security and memorability. This is a problem particularly in the light of an ageing population [45]. Ageing affects memory, and despite a few areas of relative preservation (such as basic short-term memory span, some aspects of meta-memory and visual memory) the general trend is that of deterioration [36].

The 21st century user has to remember increasing numbers of passwords. Maintaining these passwords becomes arduous in time (changing them regularly, choosing strong passwords every time, and remembering them).

Figure 7(a) shows the way passwords are often held — in an ever expanding list — and this explains why many of the passwords seem to go missing. A new password is defined and rapidly appended to the list, without it having any particular meaning or connections to other memory structures and thus the person has very few ways of retrieving the information. People tend to use the same authentication key for different systems, as shown in Figure 7(b), if they are allowed to self-define their keys. This minimises cognitive activity, but weakens the security of the system because one leaked or stolen password compromises a number of systems. One password definition scheme is the use of mnemonics, as shown in Figure 7(c). This will increase the likelihood of retrieval at a later stage, since it is meaningful and deducible, but a number of such passwords may still cause interference in the user's mind.

[9] http://world.std.com/ reinhold/diceware.html

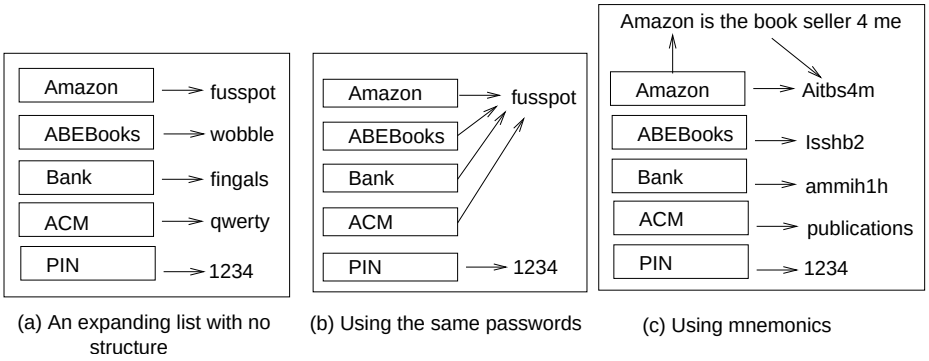

Fig. 7. *Storing Authentication Keys*

Users often deal with this unacceptable memory load by creating a physical record of difficult passwords [3]. Adams and Sasse [1] report that as many as 50% of users do this, which defeats any of the excellent mechanisms which have been implemented in order to maintain security. In terms of abundance, a 6 character password can have $102^6 =\sim 10^{12}$ possible values. Realistically, one can assume that most users will use only lowercase alphabet letters and perhaps the digit '1', hence the realistic number of passwords is $27^6 =\sim 3 * 10^8$.

In terms of predictability, when users choose their own authentication keys they tend to choose badly [65]. Since most web-passwords are either self-defined or changeable after login, this is a large deficit for syntactical passwords.

The web-deficiency and environmental quality coefficient of syntactical passwords can be calculated as follows:

```
Accessibility Dimension (ad = 0.47)
    Special Requirements 0     None
    Convenience          0.33  Potentially time-consuming at replacement
    Inclusivity          0.33  Cognitive

Memorability Dimension (md = 1.45)
    Retrieval            1     Recall
    Meaningfulness       0.33  Usually meaningful
    Depth of Processing  1     Cursory

Security Dimension (sd = 1.5)
    Predictability       1     Usually self-assigned
    Abundance            0.5
    Disclosure           1     Passwords are easy to record

Vulnerability Dimension (vd = 1.41)
    Confidentiality      1     Full
    Privacy              0     Not necessarily private
    Breakability         1     Vulnerable to keyboard tapper & Dictionary attack
```

The overall deficiency is $\overline{d_{web}} = 5.82$. Hence the quality of a self-assigned syntactic password mechanisms is $\overline{eq_{web}} = 7.18$. If the user is assigned a non-meaningful password then the meaningfulness dimension scores 1 and the predictability score goes down to 0. The final web-environmental quality coefficient in this case will be 7.48, increasing the overall quality slightly.

7.2.2 Semantic/Cognitive Passwords

Cognitive passwords rely on a cognitive process to produce the required password. This contrasts with semantic passwords, where any word will do; it is up to the user to relate it to the system in some way. Cognitive passwords will typically ask the user a question, and obtain an answer which requires some thought. The theory is that the user will have less problems recalling these passwords because the cognitive password requires recall of an established fact or opinion. It has been recognised since 500BC that well-organised information is remembered more easily than unordered information [74].

Spector and Ginzberg [66] propose a pass-sentence approach. Their approach is based on semantics, rather than the more syntactical password approach. The user using their scheme may not remember the sentence perfectly, but should remember the semantics thereof. So, for example, the user may choose the sentence, "We had a picnic with rolls, apples and cola". When the user has to reproduce the sentence, she may respond: "We had a picnic with rolls, fruit and cola". The software would detect that the semantics of the sentence is the same, and question the user, perhaps as follows: "What kind of fruit did you have?". If the user is able to correctly enter the answer, "apples", she is authenticated.

Smith proposed a word association approach [64]. Zviran and Haga [76] extended Smith's ideas by developing a set of questionnaires which asked users to answer some fact-based and some opinion-based questions. Two control groups were used; one with self-defined passwords and another with system-provided passwords. Only 23% of users remembered the system-provided passwords and 35 % remembered the passwords they defined themselves three months later. The recall rate for cognitive passwords was 94%. Since there was a concern that someone who knew the respondent well could predict their answers to the questions, a test was done to determine correct guessing by significant-others. The average correct guessing was 27%. In order to use this kind of mechanism to authenticate users enough questions must be asked, and answered, to ensure that user is correctly authenticated.

Most cognitive passwords ask a user to answer a specific challenge question, based on the assumption that the system and the user will share this secret and that it will be difficult for an attacker to find out the secret. Since one secret is perhaps known to an attacker, a cognitive authentication mechanism will tend to ask a number of questions, the answers to all of which are unlikely to be known to an attacker. These passwords suffer from the same problems as biometric authentication mechanisms since many of these 'secrets' cannot be changed once they are known to an attacker.

Mechanisms based on cognitive passwords appear to address the two of the provisos of good authentication mechanisms: memorability and relative unpredictability. However, they are weak in the time dimension. We recall that users see authentication as a necessary evil, and are prepared to put up with it only if it does not cause them too much pain. The snag with this mechanism is the time it takes the user to answer the minimum number of questions required to satisfy security requirements. Users will become annoyed with this type of mechanism and annoyance always leads to subversion if the user is forced to use the system; or abandonment if alternatives are available. Since people have difficulties setting questions [26] abundance is limited. The web-deficiency and environmental quality coefficient of semantic passwords can be calculated as follows:

```
Accessibility Dimension (ad = 1)
    Special Requirements 0     None
    Convenience          1     Time consuming at all stages
    Inclusivity          0     None

Memorability Dimension (md = 0.6)
    Retrieval            0.5   Recall with cues
    Meaningfulness       0     Deducible from personal history
    Depth of Processing  0.33  Links to previously stored knowledge

Security Dimension (sd = 1.22)
    Predictability       0.5   Predictable to close friends and family
    Abundance            1
```

```
    Disclosure           0.5   Question responses can be recorded

Vulnerability Dimension (vd = 1.17)
    Confidentiality      0.5   Only questions asked
    Privacy              1     Private Questions
    Breakability         0.33  Research Based Attack
```

The overall web environmental deficiency is $\overline{d_{web}}$= 5.1. Hence the web environmental quality of cognitive password mechanisms is $\overline{eq_{web}} = 7.9$

7.2.3 One-Time Passwords

One way of dealing with the user tendency to choose poor passwords is by using one-time passwords. There are two ways of implementing this: using hardware tokens such as SecurID[h] or using codebooks [32]. The former displays a new PIN or password for each login, or presents the user with a challenge which requires the users to enter their PIN and to calculate the password to be used. The latter list valid passwords. Users use a new one at each login attempt. These passwords alleviate the problems experienced with poor choice of passwords, but rely on extra hardware or special software, which is not always available. It is also possible for the client and server machine to get out of synch, which requires intervention to re-synchronise.

Some of these mechanisms use random number generation. However, random number generators are notoriously flawed [60]. For example, some generators rely on a particular time and state, and this can be predicted. There are also no standards for these generators. So even though a transmission sniffer will not be able to use a particular one-time password again, it is possible to determine what the next password will be based on a predictable pattern. The web-deficiency and environmental quality coefficient of one-time passwords can be calculated as follows:

```
Accessibility Dimension (ad = 0.72)
    Special Requirements 0.67   Hardware or Software [Fails Critical Aspect Requirement]
    Convenience          0.25   Time consuming at authentication
    Inclusivity          0      None excluded

Memorability Dimension (md = 1)
    Retrieval            1      Hardware version requires recall
    Meaningfulness       0      Not applicable
    Depth of Processing  0      Not applicable

Security Dimension (sd = 1)
    Predictability       0      Unpredictable
    Abundance            0      Large number available
    Disclosure           1      Code Book can be stolen

Vulnerability Dimension (vd = 0.67)
    Confidentiality      0     Cannot be reused
    Privacy              0     Not Applicable
    Breakability         0.67  Algorithm can be broken
```

The overall web environmental deficiency is $\overline{d_{web}}$= 4.24 Hence the web environmental quality of one-time password mechanisms is $\overline{eq_{web}} = 8.76$

7.3 What the User Knows — Graphically-Based

The idea of graphical authentication relies on the knowledge that visual memory is extremely powerful. Classic cognitive scientific studies have shown that humans have a vast, almost limitless memory for pictures in particular. Pictures are usually remembered far better than

[h] www.peapod.co.uk/signify-problems-of-passwords.htm

words [46], and visual memory does not seem to be significantly affected by the general decline of cognitive capabilities associated with ageing which occurs with other types of memory [55].

Graphical codes are becoming increasingly popular in personal technology. Two main approaches can be identified, involving different types of skills: (a) recognition-based; and (b) position-based. Recognition-based systems require the user to select target pictures among a set of distractors. This approach relies on pure visual memory, and exploits the ability to recognise previously seen visual objects among others. Position-based systems require the user to identify target objects within an individual picture. This approach relies on both the visual and the spatial aspects of the visuo-spatial memory and on precise movements.

7.3.1 Recognition-based system

Example recognition-based systems are Passfaces [12], Déjà Vu [22]and the Visual Identification Protocol or VIP. They all follow the same paradigm - identify target images among distractors — but use very different visual stimuli. Passfaces by Real User Corp is based on face recognition, a skill at which humans are remarkably proficient. Users are given 'five faces', which represent their visual code. Each 'face' is displayed on a separate screen amongst different distractors. A longitudinal field evaluation of this scheme revealed controversial results which did not fully support the expected superiority of faces against passwords [12]. Furthermore, this scheme disadvantages people with prosopagnosia (face blindness).

Déjà Vu is based on random art images generated by Andreij Bauer's random art program available on the Internet. These types of visual stimuli are considered particularly secure since they cannot be easily communicated to others. Using Déjà Vu, people have to create an image portfolio of 5 pictures and then select their images from a challenge set of 25 pictures. A user evaluation of this scheme has investigated the memorability of different type of visual stimuli (abstract vs. photographic) against passwords and Personal Identification Numbers (PINs). Results showed that creating passwords and PINs is much faster than selecting image portfolios, with photographic pictures requiring the longest time. Pictures in general were found to be less error prone than passwords and PINs after a week interval. Users preferred photographic pictures [22].

VIP has been designed to improve user authentication in self-service technology, supporting easy, fast and secure interaction [4, 5]. VIP consists of a self-enrolment and an authentication phase. At enrolment, the user is given an image portfolio, which represents their password. To authenticate, the user must correctly identify the images that are part of their portfolio inside a wider challenge set randomly selected from a visual database. As part of the VIP project, different visual authentication prototypes were designed and compared against the traditional PIN approach. The visual prototypes displayed detailed, colourful and meaningful photos of objects on a touch screen interface. VIP was found to provide a promising and easy-to-use alternative to the PIN approach. Pictures were found to be slightly less error prone than numbers after a week interval, without compromising the speed of the transaction. The users' reaction to the VIP concept was also very promising. Despite these encouraging results this evaluation and associated design explorations demonstrated that graphical passwords are not a simple panacea to user authentication. Indeed, it has been demonstrated that the advantages of visual memory can be easily disrupted if one does not take into consideration specific constraints of visual memory, such as its susceptibility to interference.

The web-deficiency and environmental quality coefficient of recognition-based graphical mechanisms can be calculated as follows:

```
Accessibility Dimension (ad = 1.41)
    Special Requirements 0     None
    Convenience          1     Time-consuming at all stages
    Inclusivity          1     Visual Impairment, Colour Blindness, Face Blindness,
                               Dyspraxia, Pointing Precision

Memorability Dimension (md = 1.2)
    Retrieval            0     Recognition
    Meaningfulness       1     Not meaningful - mostly system-assigned
```

```
    Depth of Processing  0.67  Visual Mechanism

Security Dimension (sd = 0.5)
    Predictability       0     Not applicable - usually system assigned
    Abundance            0     Potentially unlimited
    Disclosure           0.5   Difficult to record, but possible to observe

Vulnerability Dimension (vd = 1.2)
    Confidentiality      1     Full
    Privacy              0     Not Applicable
    Breakability         0.67  Brute force attack
```

The overall deficiency is $\overline{d_{web}} = 5.28$. Hence the quality of recognition-based mechanisms is $\overline{eq_{web}} = 7.72$

7.3.2 Position-based systems

The original approach to graphical authentication relied on different types of location-based systems. In 1996 Blonder patented a graphical password which required the user to touch predetermined areas of an image in a fixed sequence for authentication [10]. Jermyn and colleagues then implemented the concept on a PDA, thus exploiting the input capabilities of graphical devices. The password consisted of a simple picture drawn on a screen [42]. An evaluation of this form of "pass-doodle" has revealed discouraging results [34]. People remembered pass-doodles with stroke order as a match determinant less accurately than alphanumerical passwords.

V-go Password windows is a commercial example of a position-based system developed by Passlogix. V-go requires the user to simulate familiar actions on a graphical interface. Thus, people can mix a cocktail, cook a meal or hide valuables, by clicking on and dragging objects of a graphical window. The authentication code corresponds to the sequence of mouse movements. To the best of our knowledge, no usability evaluation of this scheme is currently available.

Two proposals combine memory of an authentication key with a location-based key-entry scheme. These are not true location-based graphical authentication mechanisms, but rather use a location-based PIN entry to prevent shoulder-surfing. The first, authentigraph, is proposed by Pierce *et al.* [57]. This scheme augments the traditional password with a display of images on the screen — either alphanumeric characters or shapes and colours — some of which the users have to click on in order to authenticate themselves. Users do not use the keyboard to enter the password, but rather click on the display to make up their authentication key. Two different schemes are incorporated to accommodate visually impaired users.

The second is proposed by Swivel Technologies[i]. The user has to provide a 4-digit authentication key, but the user does not enter it using the numeric keyboard. The digits are displayed on the screen and and digits are highlighted in turn. The user chooses the number by hitting any key, which prevents a keyboard tapper from recording the password.

These mechanisms are valuable in terms of preventing network-based and shoulder surfing attacks but in fact have two requirements that are particularly problematical for users. In the first place, they still have to memorise an authentication key, which relies on unimpaired recall — an unrealistic expectation. Furthermore, authentigraph requires users to be able to click on the key with a level of precision, and Swivel's mechanism requires them to hit a key on the keyboard when the number is highlighted in the second proposal. Authentigraph's required level of precision is not always possible and the Swivel system relies on a reaction speed that will challenge older users.

Despite the growing interest generated by different approaches to visual authentication systems, we are still far away from robust solutions. Most of current proposals concentrate on maximising security and may overestimate visual-memory potentialities. More work is needed to understand limits and potentials of graphical approaches to user authentication, especially

[i] www.swivelsecure.com

as regards position-based systems which requires the ability to recognise visual targets and the ability to indicate these targets.

One evaluation has identified severe flaws in the location-based paradigm, at least for the particular implementation of the loci-mechanism called Jiminy, which was evaluated in the study [59]. The main problems with the mechanism appear to relate to the predictability of choices which in turn is caused by the severely limited number of possible positions the user can choose in authenticating him or herself.

The web-deficiency and environmental quality coefficient of location-based graphical mechanisms can be calculated as follows:

```
Accessibility Dimension (ad = 1.2)
    Special Requirements 0     None
    Convenience          1     Time consuming at all stages
    Inclusivity          0.67  Visual Impairment, Colour Blindnss, Pointing Precision

Memorability Dimension (md = 0.47)
    Retrieval            0     Recognition
    Meaningfulness       0.33  Possibly meaningful
    Depth of Processing  0.33  Some cognitive effort involved

Security Dimension (sd = 1.5)
    Predictability       1     Choose own position and possibly image
    Abundance            1     Few positions
    Disclosure           0.5   Difficult to record, but possible to observe

Vulnerability Dimension (vd = 1.2)
    Confidentiality      1     Reveals position on screen
    Privacy              0     Not Applicable
    Breakabilit          0.67  Can be brute force attacked
```

The overall deficiency is $\overline{d_{web}} = 5.73$. Hence the quality of position-based mechanisms is $\overline{eq_{web}} = 7.27$

7.4 What the User Owns

Users can also be authenticated by means of public key cryptography. The user is authenticated when the server decrypts information information sent by the user. If the key is going to be used for authentication purposes it will have to be stored on the user's machine so that when the site receives subsequent information with that particular key it automatically authenticates the user.

Whilst this mechanism would deal with the memorability and predictability problems admirably it does not guarantee that the person interacting with the site is actually the person who initially enrolled and collected the key. Another user could easily be masquerading since no knowledge-based authenticator is required. Furthermore, the public key has to be stored securely on either the user's machine or on a smart card because if another user gains access to it, it would be a simple matter to impersonate the user. Secure storage on the user's computer requires either another key for encryption or a password mechanism to protect it — reverting once again to "something the user knows" or "something the user has and can lose" in the case of the smart card.

Public key authentication's use in web authentication is currently not tenable — public key systems are often poorly implemented [40] and people find them difficult to use [71]. The web-deficiency and environmental quality quotient of token-based mechanisms can be calculated as follows:

```
Accessibility Dimension (ad = 1.12)
    Special Requirements 1    Key & Technical Expertise [Fails Critical Access Requirement]
    Convenience          0.5  Enrolment and replacement
    Inclusivity          0    All
```

```
Memorability Dimension (md = 1.73)
    Retrieval            1    Recall for accompanying PIN
    Meaningfulness       1    Not meaningful
    Depth of Processing  1    No processing

Security Dimension (sd = 1)
    Predictability       0    Unpredictable
    Abundance            0    Maximum
    Disclosure           1    Public key may be stolen

Vulnerability Dimension (vd = 0.67)
    Confidentiality      0     Private Key Not Revealed
    Privacy              0     Not Applicable
    Breakability         0.67  Can be cracked if too small
```

The overall web environmental deficiency is $\overline{d_{web}} = 5.58$. Hence the quality of card-based mechanisms is $\overline{eq_{web}} = 7.42$

8 Choosing a Mechanism

Table 1 summarises the web environmental quality coefficients for each of the categories of web authentication mechanisms. Biometrics, one-time passwords and public-key based authentication will not be considered since they fail with respect to the special requirements critical aspect.

Type	$\overline{eq_{web}}$
Semantic Password	7.9
Recognition-Based Graphical	7.72
Location-Based Graphical	7.27
Syntactic Password	7.18

Table 1. Summary of Quality Coefficients

These findings emphasize the fact that the web developer should at least consider alternative mechanisms before automatically reaching for the ubiquitous syntactic password. According to this quantification scheme recognition-based graphical mechanisms have a hitherto untapped potential in a web environment. Semantic passwords are also a good alternative, but most developers use this only to request the mother's maiden name, which, because of widespread misuse, is almost worthless.

9 Conclusion

Most, if not all, Web authentication mechanisms will authenticate by what the user knows. In a few years card or biometric scanning devices may become as ubiquitous as mouse devices are today, but currently extra equipment is seldom available to the web-user and thus cannot be used in universally accessible sites.

Syntactic passwords are currently the most popular web-user authentication mechanism. Passwords are inherently weak and in the current atmosphere of increasing web fraud it is becoming necessary for web developers to consider other authentication mechanisms. However, it is difficult for a web developer to make an informed decision about the quality of these mechanisms and this paper therefore proposed a quantification scheme for authentication mechanisms. This quantification scheme takes the particular characteristics of the mechanism into account, as well as the environment within which the mechanism will be used.

Work into alternative authentication mechanisms is ongoing and this quantification scheme will offer a way of making informed decisions and judgements about these mechanisms. An-

other way of strengthening these mechanisms is to use two in tandem. Work on the tailoring of this scheme to capture the strengths of such an approach is being considered.

Acknowledgements

I acknowledge the contributions of Antonella De Angeli, without whom this work could not have been carried out.

References

1. A Adams and M A Sasse. Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12):40–46, December 1999.
2. A. Adams, M. A. Sasse, and P. Lunt. Making passwords secure and usable. In H. Thimbleby, B. O'Conaill, and P. Thomas, editors, *People & Computers XII,Proceedings of HCI'97*, pages 1–19, Bristol, August 12-15 1997. Springer. http://www.getrealsecurity.com/publications.htm.
3. A M De Alvare and E E Schultz Jr. A framework for password selection. In *Proceedings of USENIX Unix security Workshop*, pages 29–30, aug 1988.
4. A De Angeli, M Coutts, L Coventry, and G I Johnson. VIP: a visual approach to user authentication. In *Proceedings of the Working Conference on Advanced Visual Interfaces AVI. 2002*, pages 316–323. ACM Press, 2002.
5. A De Angeli, L Coventry, G I Johnson, and M Coutts. Usability and user authentication: Pictorial passwords vs. PIN. In P.T.McCabe, editor, *Contemporary Ergonomics 2003*, pages 253–258. Taylor & Francis, London, 2003.
6. L Bahler, J Porter, and A Higgins. Improved voice identification using a nearest neighbour distance measure. In *Proceedings Proc. International Conference of Acoustics, Speech and Signal Processing*, pages 321–324, Adelaide., April 19-22 1994.
7. F Bergadano, D Gunetti, and C Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):367 – 397, 2002.
8. Hal Berghel. Identity theft, social security numbers, and the web. *CACM*, 43(2):17–21, 2000.
9. D Besnard and B Arief. Computer security impaired by legitimate users. *Computers and Security*, 23(3):253–264, may 2004.
10. G E Blonder. Graphical password, 1996. United States Patent 5559961.
11. J Brentano and K Wiseth. Enterprise-wide security: Authentication and single sign-on. In *Network Applications Consortium*, San Francisco, 1996. position paper. http://www.alameda-tech-lab.com/portfolio/samples/Old_Papers/NACSEC02.pdf.
12. S Brostoff and A Sasse. Are passfaces more usable than passwords? a field trial investigation. In S. McDonald, editor, *People and Computers XIV - Usability or Else! Proceedings of HCI 2000*, pages 405–424. Springer, 2000.
13. S Brostoff and A Sasse. Ten strikes and you're out: Incresing the number of login attempts can improve password usability. In *Workshop on Human-Computer Interaction and Security Systems*, Fort Lauderdale, Florida, April 2003. ACM.
14. M Burge and W Burger. Using ear biometrics for passive identification. In G Papp and R Posch, editors, *Proceedings of the IFIP TC11 14th international conference on information security, SEC'98*, pages 139–148, Wien, 1998.
15. J Clark. *Building Accessible Websites*. New Riders, 2002.
16. L Coventry, A De Angeli, and G I Johnson. Usability and biometric verification at the atm interface. In *CHI 2003 Proceedings*. ACM Press, 2003.
17. Lynne Coventry, Antonella De Angeli, and Graham Johnson. Honest, it's me! Self service verification. In *Workshop on Human-Computer Interaction and Security Systems*, Fort Lauderdale, Florida, April 2003. ACM.
18. F I M Craik and E Tulving. Depth of processing and word retention. *Journal of Experimental Psychology*, 104(3):268–294, 1975.
19. R Crutchfield and D A Workman. Quality guidelines = designer metrics. In *Annual International*

Conference on ADA, pages 29–40, Baltimore, Maryland. US, 1994.
20. W G de Ru and J H P Eloff. Reinforcing password authentication with typing biometrics. In *Proceedings of the IFIP TC11 eleventh international conference on information security, IFIP/SEC'95*, pages 562–574, London, UK, 1995. Chapman and Hall.
21. W G de Ru and J H P Eloff. Enhanced password authentication through fuzzy logic. *IEEE Intelligent Systems & their applications*, 12(6), Nov/Dec 1997.
22. R Dhamija and A Perrig. Déjà vu: A user study using images for authentication. In *Proceedings of USENIX Security Symposium*, August 2000.
23. M Eagle and E Leiter. Recall and recognition in intentional and incidental learning. *Journal of Experimental Psychology*, 68:58 – 63, 1964.
24. H Ebbinghaus. *Memory: A contribution to experimental psychology.* Dover Publications, Inc, New York, 1964. Translated by H A Ruger and C E Bussenius. Originally published, 1885.
25. C. Ellison, C. Hall, R. Milbert, , and B. Schneier. Protecting secret keys with personal entropy. *Future Generation Computer Systems*, 16:311–318, 2000.
26. C Ellison, C Hall, R Milbert, and B Schneier. Protecting secret keys with personal entropy. *Future Generation Computer Systems*, 16:311–318, 2000.
27. Y Endo, Z Wang, J B Chen, and Margo I. Seltzer. Using latency to evaluate interactive system performance. In *Proceedings of the 2nd USENIX Symposium on Operating Systems Design and Implementation*, pages 185–200, Berkeley, October 28–31 1996. USENIX Association.
28. K A Ericsson and W Kintsch. Long-term working memory. *Psychological Review*, 102:211–245, 1995.
29. Foolproof. Accessibility online briefing, April 2004. http://www.foolproofservices.co.uk/accessibility/.
30. B Friedman, H Nissenbaum, D Hurley, D C Howe, and E Felten. User's conceptions of risks and harms on the web: A comparative study. In *Proceedings of CHI 2002.*, Minneapolis, Minnesota, April 20-25 2002. ACM.
31. N Frykholm and A Juels. Error-tolerant password recovery. In *Proceedings of the 8th ACM conference on Computer and Communications Security*, pages 1–9. ACM Press, 2001.
32. S Garfinkel, G Spafford, and A Schwartz. *Practical UNIX and Internet Security.* O'Reilly, Cambridge, 3rd edition, 2003.
33. T Gilb. Advanced requirements specification: Quantifying the qualitative. In *PSQT Conference St Paul MN*, oct 1999. http://citeseer.ist.psu.edu/332850.html; http://www.pimsl.com/TomGilb/Quantify_Quality_paper_PSQT.pdf.
34. J Goldberg, J Hangman, and V Sazawal. Doodling our way to better authentication. In *Poster presented at CHI 2002*, Minneapolis, April 2002.
35. V H Gregg. *Introduction to Human Memory.* Routledge & Kegan Paul, 1986.
36. I S Hamilton. *The Psychology of Ageing.* Jessica Kingsley Publishers, 3 edition, 2000.
37. K Hayashi, E Okamoto, and M Mambo. Proposal of user identification scheme using mouse. In T Okamoto Y Han and S Qing, editors, *Proceedings of the 1st International Information and Communications Security Conference*, pages 144–148, 1997.
38. K S Hendis. Quantifying software quality. In *Proceedings of the ACM '81 conference*, pages 268–273. ACM Press, 1981.
39. L. Hong and A Jain. Integrating faces and fingerprints for personal identification. *Lecture Notes in Computer Science*, 1351, 1997.
40. B Ives, K R Walsh, and H Schneider. The domino effect of password reuse. *Commun. ACM*, 47(4):75–78, 2004.
41. A Jain, L Hong, and S Pankanti. Biometric identification. *Commun. ACM*, 43(2):90–98, 2000.
42. I Jermyn, A Mayer, F Monrose, M K Reoter, and A D Rubin. The design and analysis of graphical passwords. In *Proceedings of the 9th USENIX Security Symposium*, August 2000.
43. M Kinsbourne and J George. The mechanisme of the word-frequency effect on recognition memory. *Journal of Verbal Learning and Verbal Behavior*, 13:63 – 69, 1974.
44. J Liddell, K V Renaud, and A De Angeli. Authenticating users using a combination of sound and images. In *HCI 2003*, Bath, UK, September 2003. Short Paper.

45. A Lusher. Keypad pensions cause problems. Sunday Telegraph, 18 May 2003.
46. S Madigan. Picture memory. In J.C. Yuille, editor, *Imagery, memory, and cognition: essays in honor of Allan Paivio*. Lawrence Erlbaum Associates, Hillsdale, NJ, 1983.
47. C Miller. Password recovery. Web Document, 2004. http://fishbowl.pastiche.org/archives/docs/PasswordRecovery.pdf.
48. K D Mitnick and W L Simon. *The Art of Deception*. Wiley, Indianapolis, 2002.
49. F Monrose and M K Reiter. Password hardening based on keystroke dynamics. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 73–82, 1999.
50. T Moss. Web accessibility and uk law: Telling it like it is, July 2004. http://www.alistapart.com/articles/accessuk.
51. E Murrer. Fingerprint authentication. *Secure Computing*, pages 26–30, March 1999.
52. D A Norman. *Memory and Attention. An introduction to human information processing*. John Wiley & Sons, 1969.
53. M S Obiadat and B Sadoun. Verification of computer users using keystroke dynamics. *IEEE Transactions on Systems, Man and Cybernetics - Part B: Cybernetics*, 27(2):261–269, April 1997.
54. A Paivio. *Mental representations: A dual coding approach*. Oxford University Press, Oxford, UK, 1986.
55. D C Park. Ageing and memory: Mechanisms underlying age differences in performances. In *Proceedings of the 1997 World Congress of Gerontology*, 1997.
56. A J Parkin. *Memory: Phenomena, Experiment and Theory*. Blackwell, 1993.
57. J D Pierce, J G Wells, M J Warren, and D R Mackay. A conceptual model for graphical authentication. In *1st Australian Information Security Management Conference*, Perth, Western Australia, 24 November 2003.
58. D Povey. Optimistic security: a new access control paradigm. In *Proceedings of the 1999 workshop on New security paradigms*, pages 40–45. ACM Press, 2000.
59. K V Renaud and A De Angeli. My password is here! Investigating authentication schemes based on visuo-spatial memory. *Interacting with Computers*, 204. To Appear.
60. B. Schneier. Security in the real world: How to evaluate security. *Computer Security Journal*, 15(4):1–14, 1999.
61. B Schneier. *Secrets and Lies*. Wiley, 2000.
62. B Schneier. Customers, passwords, and web sites. *IEEE Security & Privacy Columns*, 2004.
63. B Schneier. Sensible authentication. *ACM Queue*, 1(10), February 2004.
64. S L Smith. Authenticating users by word association. In G Papp and R Posch, editors, *Proceedings of the Human Factors Society 31st Annual Meeting*, pages 135–138, Wien, 1987.
65. E. H. Spafford. Preventing weak password choices. In *Proc. 14th NIST-NCSC National Computer Security Conference*, pages 446–455, 1991.
66. Y Spector and J Ginzberg. Pass-sentence - a new approach to computer code. *Computers and Security*, 13:145–160, 1994.
67. L Stein. *Web Security*. Addison Wesley, 1998.
68. E Tulving and S Osler. Effectiveness of retrieval cues in memory for words. *Journal of Experimental Psychology*, 77:593–601, 1968.
69. H van Solms, J H P Eloff, M Eloff, and E Smith. *Information Security*. B & D Printers, 2003.
70. W A Ward and B Venkataraman. Some observations on software quality. In *ACM Southeast Regional COnference. Proceedings 37th Annual southeast regional conference.*, 1999.
71. Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, Washington, D.C., USA, August 1999. USENIX.
72. E Winograd and E W Simon. Visual memory and imagery in the aged. In *New Directions in Memory and Aging. Proceedings of the George A Talland Memorial Conference*, chapter 27, pages 485–506. Lawrence Erlbaum, 1980.
73. T Wu. A real-world analysis of kerberos password security. In *Proceedings of the 1999 Network and Distributed System Security Symposium*, February 3-5 1999.

74. F Yates. *The Art of Memory*. Pimlico, London, 1966.
75. W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld. Face recognition: A literature survey. *ACM Comput. Surv.*, 35(4):399–458, 2003.
76. M Zviran and W J Haga. Cognitive passwords: The key to easy access control. *Computers and Security*, 9:723–736, 1990.