ARTICLE:

PINs, PASSWORDS AND HUMAN MEMORY[1]

By **Wendy Moncur**
and **Dr Grégory Leplâtre**

Introduction

Automated Teller Machines (ATMs) provide access to cash, confidential information and services for service users of all types, cultures and abilities, across the globe. The standard authentication mechanism by which these users gain access to ATMs consists of use of a token (in the form of a bank card) combined with a password known as a personal identity number (PIN), that can be between 4 and 12 digits (for instance, 4 digits are used in the UK, 5 digits are used in South Africa and 6 in France). Yet this mechanism, which is based on knowledge retained by the person, is unsatisfactory. Passwords are easily forgotten. Users deal with this problem by behaving in a manner that reduces the security: by writing down their PIN, or making them all the same, or disclosing them to friends and family.[2] Whilst security administrators may blame the user for the failure in securing their PIN, in reality the method of authentication chosen by banks as a means of authentication at the ATM disregards users' innate cognitive abilities and limitations. Awareness is emerging of the need to design authentication with these abilities and limitations in mind, with researchers at IBM describing this as 'a critical area for research'.[3] NCR, a leading ATM manufacturer, employs experts to address these issues specifically.

This article explores the literature in respect of current Western authentication systems, together with an overview of some of the main authentication alternatives. In considering current and proposed authentication mechanisms, information is drawn from a range of sources, including journal articles, conference proceedings, company reports and sales literature for security products designed for use on mobile telephones and the internet. These mechanisms are examined under the following headings: authentication; pervasive mechanisms and known user behaviours; usability and universal design at the ATM; how we remember, and a taxonomy of alternative authentication methods.

Throughout this article, reference will be made to the term 'usability'. 'Usability' is a quality that can be measured in relation to the ease of use of a computer application. The elements that make up usability comprise the following:

a. Learnability: this tests the ease with which users can complete basic tasks the first time they encounter the computer system.

b. Efficiency: this measures how quickly users can perform tasks once they are familiar with the system.

c. Memorability: this tests how easily users can re-establish competence after a period of not using the system.

d. The number of times users make mistakes are measured, as is the extent of the errors that are made by users.

e. Measures of satisfaction establish if users find the system enjoyable to use, and utility measures whether the system does what the user needs it to do.

Authentication: pervasive mechanisms and known user behaviours

In this section, how people use authentication

[1] *This article is taken from 'Exploring the usability of multiple graphic passwords', a dissertation written by Wendy Moncur and submitted in partial fulfilment of the requirements of Napier University for the degree of Master of Science in Multimedia and Digital Technology (School of Computing, May 2006), which was awarded a Distinction. Wendy Moncur acknowledges the advice and guidance of Dr. Grégory Leplâtre and Dr.Lynne Coventry in exploring the area of password security and usability. A useful text on this topic is Lorrie Faith Cranor and Simson Garfinkel, Security and Usability: Designing secure systems that people can use (2005, O' Reilly Media, Inc.).*

[2] *Anne Adams and Martina Angela Sasse, 'Users are not the enemy', Communications of the ACM, Volume 42, Issue 12, July 1999, 41-46.*

[3] *Clare-Marie Karat, John Karat, Carolyn Brodie, 'Why HCI research in privacy and security is critical now', International Journal of Human-Computer Studies, Volume 63, Issue 1-2, July 2005, 41-46.*

mechanisms and their known behaviours are reviewed across the broad range of prevailing mechanisms, rather than limiting the review to ATMs. Whilst ATMs have very specific requirements for speed, security and usability in a small space, knowledge-based authentication mechanisms in general share common issues, regardless of which form of device the person is required to interact with. It is pertinent that an account can be viewed through an ATM, the internet, the counter at a bank, and from point of sale machines in retail outlets. A different authentication mechanism might be required for each avenue by which a person can obtain access to their account. This can cause problems for the person, such as *memory interference*, which in turn causes *memory confusion*, which in turn leads to insecure behaviour towards ATM security.[4] By understanding the broader picture, it is possible to more fully understand the behaviour of users when interacting with authentication mechanisms, which in turn helps to formulate future research.

Context

ATMs provide access to cash, confidential information and services to consumers across the globe. Machines may be located indoors or outdoors, in a wide range of climates, but are usually in a public place. The banks authenticate a customer with the use of a token, in the form of a bank card, and a PIN.

Mechanism

Current user authentication systems are based on the knowledge of the user, yet this approach is known to be error-prone.[5] Knowledge-based authentication systems require selection of a strong password to resist attack. Ideally, a password should consist of a set of eight or more randomly allocated characters, incorporating upper and lower case characters, digits and special characters.[6] Yet this is extremely difficult for users to remember. Similarly, a numeric password – or PIN number – made up of a series of digits appears challenging for users to remember, and can be easily changed to a code that is easy to crack. In addition, up to 50 per cent of users write down their PIN number and store it in close proximity to the matching bank card.[7]

An extra layer of complexity is introduced by the variety of mechanisms applied to a single account, depending on how the customer is required to obtain access to the account. For example, one leading UK bank requires customers to use four different mechanisms to obtain access to the same account:

At the bank: presentation of the bank card, plus a manuscript signature, is considered adequate.

ATM: presentation of the bank card and entry of the correct PIN number.

Internet: a combination of customer number, a random selection of digits from the user identification code (this is different to the PIN number or the account number) plus 'secret' personal information.

Making a payment via the internet: in addition to the above, the customer must insert their bank card into a separate card reader supplied by the bank, enter their PIN, then enter the random number displayed on the card reader into their internet banking session.

From the bank's perspective, this may be simple to administer, but from a usability perspective, it is doubtful that it provides user satisfaction. For instance, in a study of Canadian banks, on-line banking customers reported that they found documented security practices confusing and extremely difficult to comply with.[8]

People

People involved in the use of authentication systems can be divided into three groups: administrators, legitimate users and unauthorized users.

Administrators understandably want to protect 'their' systems from attack by unauthorized users. It is common for security departments in organisations not to have any contact with their legitimate users, and to fail to communicate with them. Such detachment can lead to a failure to understand users' needs and

[4] *Anne Adams and Martina Angela Sasse, 'Users are not the enemy', Communications of the ACM.*

[5] *Rachna Dhamija and Adrian Perrig, 'Deja vu: A user study using images for authentication', Proceedings of the 9th conference on USENIX Security Symposium, Volume 9 (Denver, Colorado, 2000).*

[6] *Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, 'Authentication using graphical passwords: effects of tolerance and image choice', Proceedings of the 2005 symposium on usable privacy and security, (Pittsburgh, Pennsylvania) (ACM International Conference Proceeding Series, Volume 93, 2005), 1-12.*

[7] *Anne Adams and Martina Angela Sasse, 'Users are not the enemy', Communications of the ACM, cited by Karen Renaud and Antonella De Angeli, 'My password is here! An investigation into visuo-spatial authentication mechanisms', Interacting with Computers, Volume 16, Issue 6, December 2004, 1017-1041.*

[8] *Mohammad Mannan and P. C. van Oorschot, 'Security and Usability: The Gap in Real-World. Online Banking', Proceedings of the 2007 New Security Paradigms Workshop, September 2007, available from http://www.scs.carleton.ca/~paulv/papers/pubs.html.*

objectives, resulting in the creation of unusable security systems. It may seem reasonable to an administrator to create a system that enforces regular password changes, because users are unlikely to change them otherwise. Yet the same system may be perceived as a hindrance by users, because frequent password changes add to the burden placed on human memory, known as 'memory burden'. Similarly, administrators may assign individual passwords when it may be more appropriate to share a common password across an organisational unit. A parallel may be found in joint bank accounts, where each card holder is given a different PIN or password to the same account.

As a result of security being forced upon them by the organisation rather than tailored to their needs, users do not consider themselves to be accountable for security as much as the bank might wish them to be. When the purpose of the security mechanism is unclear or inappropriate, the motivation to comply is weakened, thus eroding the culture that ought to accompany security. The system may be perceived as an obstacle to 'real' work, which therefore must be circumvented.[9] The failure is compounded when security administrators advise users to write down their passwords: this is a clear indication that the authentication mechanism is not viable.

The error rate, a measure of usability, may be high because legitimate users have difficulty remembering passwords that are less vulnerable to cracking – known as 'strong' passwords. While 94 per cent of users can remember semantic passwords, they can remember syntactic passwords only 35 per cent of the time.[10] The 'Power Law of Forgetting' explains that not only do individuals forget a great deal quickly, but their memory is further eroded over time.[11] For a password to be remembered without resort to an insecure aide-memoir of some form (usually by writing it down), it must be encoded within long term memory. To achieve this, the password must be meaningful or easy to work out, practiced, based on information that is personal to the user that is already familiar, and incorporated into a special memory scheme. It is difficult to apply these criteria to strong passwords.

Given that most people in the twenty-first century are required to remember a number of passwords for different purposes, users may mix up which password applies to which authentication mechanism. This phenomenon is known as 'interference'. At one industry site, where users had 16 different passwords for use within the organisation, it was extremely common to forget passwords, or mix up which password was used for which system, because of intra-password interference.[12] An added layer of confusion is also generated when different rules for the creation of passwords are enforced in different systems.

Standing at an ATM in a public place and observed by others, users may feel pressurised when trying to recall their password. This pressure can itself adversely affect recall. Failure to recall their password can generate embarrassment in the user when they are observed by others, but it may also generate a suspicion of wrong-doing amongst observers.[13] Further pressure may be added if a user is aware of the risks of being observed either directly or by a hidden camera when entering their password: a phenomenon known as 'shoulder-surfing'.

The card holder may give another person authority to use their card and PIN. The authority may be given expressly or by implication, such as how they deal with their card within the family, for example. A person that has authority to use the card and PIN is not expected to use the card beyond the authority given to them by the card holder. When a user shares their password with a colleague, friend or family member, they are in effect sharing the method by which they are authenticated and, by extension, authorisation to use the facilities that may be afforded to the user when using an ATM, for instance. Depending on the terms and conditions of use, the organisation operating the authentication mechanism may consider this practice to be insecure. However, it may be reasonable from the perspective of the user to share their authentication details with others. It is certainly extremely common – 36 per cent of users admit to sharing their PIN with someone,

[9] *Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, 'PassPoints: Design and longitudinal evaluation of a graphical password system', International Journal of Human-Computer Studies, Volume 63, Issue 1-2, (July 2005), 102-127.*

[10] *Moshe Zviran and William J. Haga, Cognitive passwords: The key to easy access control, Computers & Security (1990) 9(8), 723-736, cited by Karen Renaud and Antonella De Angeli, 'My password is here! An investigation into visuo-spatial authentication mechanisms', Interacting with Computers, Volume 16, Issue 6, December 2004, 1017-1041.*

[11] *Harry P. Bahrick, Semantic memory content in permastore: Fifty years of memory for Spanish learned in school, Journal of Experimental Psychology: General, Volume 113(1), March 1984, 1-29 cited by Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, 'Authentication using graphical passwords: effects of tolerance and image choice', Proceedings of the 2005 symposium on usable privacy and security.*

[12] *Anne Adams and Martina Angela Sasse, 'Users are not the enemy', Communications of the ACM.*

[13] *Martina Angela Sasse, Sacha Brostoff and Dirk Weirich, 'Transforming the weakest link - a human/computer interaction approach to usable and effective security', BT Technology Journal, Volume 19, Issue 3, 2001, 122-131.*

although the real percentage is likely to be higher. Some users even view it as desirable that they share their authentication details.[14] The card holder authorises the other person to act within the scope of the authority grated by the person whose password is used. For instance, the woman manages the finances in 70 per cent of households, thus it may not be acceptable for her to refuse to tell her partner the PIN for the family bank account. Disabled users may be unable to obtain access to the ATM because of cognitive or physical limitations. By necessity, they may need to divulge their PIN to enable a helper to obtain access to the ATM with their authority. Using knowledge-based authentication mechanisms that are easily communicated verbally or in writing means it is difficult to prevent passwords from being shared.

People posing as legitimate users can exploit poor usability. When organisations routinely ask users for their password in order to resolve usability difficulties with the security mechanism, they open the way for malign users to trick legitimate users into divulging their passwords. The poor design of a security system often requires users to share their passwords with an administrator. This in turn enables an attacker to use various social engineering techniques to trick legitimate users into divulging their passwords. An ATM with a mouse or clearly displayed fixed position keys, facilitates shoulder-surfing, sometimes known as 'observer attack'.[15] Software applications that help thieves are common, but the threat is poorly understood by legitimate users. Multilingual dictionary attack software can break 85 per cent of passwords through a simple exhaustive search. Rule-based attacks extend this capability further, altering known words according to a number of rules, for example searching on words written backwards.[16]

Design for ATM users

Characteristics of ATM users

There is no such thing as a 'typical' user at the ATM. Young, old, able-bodied and disabled may all wish to use ATMs. Yet ability and disability are not distinct categories. A wide range of physical, cognitive and sensory abilities may be displayed by users. Abilities may fluctuate, affected by circumstance at any given point in time. This makes it difficult to provide a universal design. For example, consider an elderly person who is holding a number of bags of shopping. Without the bags of shopping, they are normally able-bodied and alert, yet when carrying the bags of shopping, they are temporarily 'disabled'. Their physical function is hampered by tangible external constraints, as they juggle shopping bags whilst entering their PIN. Furthermore, older adults generally find it more difficult to use computer software than younger people.[17]

Usability of current mechanisms

As previously discussed, the prevailing knowledge-based authentication mechanisms are not very good. Users are generally not very satisfied with them, and there are high error rates. Further problems include difficulty in memorising passwords and learning how to use authentication systems.

Knowledge-based authentication mechanisms place a requirement on people that passwords be recalled correctly, otherwise the user will fail to obtain access to the service or system. People find it difficult to remember passwords, because not enough consideration is given to the difficulty that people experience in recalling passwords that are not frequently used. The cognitive ability to remember imprecisely is not taken into account. The policy of many knowledge-based mechanisms is that if the user fails to key in the correct password on the third attempt, they are denied access to the service or system, regardless of a realistic security appraisal of security requirements.[18] When an account holder wants to check the balance on a seldom-used account without withdrawing cash, for instance, it is a matter of debate as to whether their bank card should be revoked if they get one digit wrong on the PIN number.

When a user chooses a new password, they find it very difficult to learn the new password if it is created in the random way that is usually required. The lack of understanding of what constitutes a strong password can lead to the creation of weak passwords that are vulnerable to attack. It is rare for training to be provided on how to create a secure password. Without

[14] *Rachna Dhamija and Adrian Perrig, 'Deja vu: A user study using images for authentication', Proceedings of the 9th conference on USENIX Security Symposium.*

[15] *Volker Roth, Kai Richter and Rene Freidinger, 'A PIN-entry method resilient against shoulder surfing', Proceedings of the 11th ACM conference on Computer and communications security, (Washington DC, USA) (ACM, 2004), 236-245.*

[16] *Rachna Dhamija and Adrian Perrig, 'Deja vu: A user study using images for authentication', Proceedings of the 9th conference on USENIX Security Symposium.*

[17] *Ann Chadwick-Dias, Michelle McNulty and Tom Tullis, 'Web usability and age: how design changes can improve performance', Proceedings of the 2003 Conference on Universal Usability, (ACM Conference on Universal Usability, 2003), 30-37.*

[18] *Sacha Brostoff and Angela Sasse, '"Ten strikes and you're out": Increasing the number of login attempts can improve password usability', Workshop on Human-Computer Interaction and Security Systems part of Conference on Human Factors in Computing Systems 2003, 5-10 April 2003, Fort Lauderdale, Florida.*

appropriate help and advice when a weak password is selected, the user's inaccurate understanding of security remains uncorrected, and security is undermined. This means that the utility of the mechanism that is designed to help provide for security is poor. This in turn reflects on the inability of those people responsible for security to understand that the very measures they have implemented are not secure, and illustrates their failure to design truly secure systems.

Conflict between security and usability

The need to provide for security whilst also providing a system that is relatively easy to use can be in conflict. For an authentication mechanism to be secure, it must use passwords that are secret, and there must be a very wide range of possible passwords available for users to use. For example, if a password can only be two characters in length, it will be far easier to guess than one that is six characters long. Further, the security of a password should be rated for the ability of a potentially malign user to observe the code, guess the code and record the code. Users can be perceived by administrators as undesirable, because they undermine secure systems. They allow their passwords to be observed. They create weak, guessable passwords. They record them in obvious places. Users feel justified in adopting such insecure, apparently careless, behaviour by systems that are poor to use, and that seem inadequately matched to user needs. In contrast, part of the success of hackers can be attributed to the attention that they pay to users and their behaviour.[19]

Users do have a shared purpose with the system and its administrators, but a perceptual divide exists. It is in the interests of both administrators and users to protect data. Unfortunately, there is little dialogue or shared understanding between the two groups regarding what security needs really exist. System designers follow a simplistic approach to security. Users are thus subjected to an impossible burden to memorise complex passwords, forced to remember multiple passwords, and often given no guidance on what makes a password secure.[20]

Reducing conflict

If authentication mechanisms are to become more usable, they must incorporate usability considerations from the start. Knowledge-based systems could use a single sign-on for a whole system and also reduce forced changes, thus reducing the burden on memory. Alternative approaches to authentication, such as graphical or biometric authentication, are also possible.

A shift of emphasis needs to occur. Rather than users and security designers being in conflict, a partnership might be promoted, with an emphasis on shared aims. Communication is essential. By involving users from the start, security system designers can understand users' needs and develop systems that are compatible with their requirements. The degree of security can be appropriate to the risk. Systems can be evaluated for usability with users before being implemented. Cost savings can be made by paying attention to the needs and abilities of users. As passwords are forgotten less, there is less need to spend corporate time and effort resetting them. Moreover, satisfied users are more likely to abide by the security rules.

The value of training users to create strong passwords is disputed: Sasse and her colleagues found that user training increased usability of security systems,[21] yet Yan and others found that this did not significantly improve the strength of the passwords that were created.[22] Online guidance during the process of creating a password may be a better approach. This method is now used by some online service providers. For example, GoogleMail provides real-time feedback to show if a password is weak, fair or strong. The use of colour coding and a bar chart helps to reinforce the comments offered in respect to a password used by a customer. The security software reviews the proposed password as the user types it in. For example, in the process of typing the password 'secret12', the following comments are provided:

'secret1' is reported as 'too short'

'secret12' is reported as 'fair'

'Secret12' is reported as 'strong', because of to the inclusion of an upper case letter

Further advice is given to users on creating a strong password if the user clicks on a link on the same web page, entitled 'Password strength'. Whilst such online guidance forces users to choose a strong password, it

[19] *Anne Adams and Martina Angela Sasse, 'Users are not the enemy', Communications of the ACM.*

[20] *Martina Angela Sasse, Sacha Brostoff and Dirk Weirich, 'Transforming the weakest link - a human/computer interaction approach to usable and effective security', BT Technology Journal.*

[21] *Anne Adams and Martina Angela Sasse, 'Users are not the enemy', Communications of the ACM; Martina Angela Sasse, Sacha Brostoff and Dirk Weirich, 'Transforming the weakest link - a human/computer interaction approach to usable and effective security', BT Technology Journal.*

[22] *Jianxin Yan, Alan Blackwell, Ross Anderson and Alan Grant, 'The Memorability and Security of Passwords – Some Empirical Results', Technical report No. 500 (Cambridge University Computer Laboratory, 2000).*

can also be used to provide the rationale for security, and enable the user to understand what makes up a strong password.

How we remember

Limitations in the way people remember make it difficult to recall alphanumeric passwords. The 'Power Law of Forgetting'[23] describes how an individual may experience rapid forgetting immediately after learning, followed by a further gradual decay. Over time, recall becomes progressively more inaccurate. This inaccuracy is a particular problem when password authentication demands total accuracy. Retroactive interference, where new additions to memory disrupt existing memories, adds to the problem. It may be inferred that multiple passwords are particularly prone to retroactive interference.

Recall is easier when distinct items are familiar, and when they are associated with each other. Mnemonics are useful in exploiting this feature of memory. Amongst the mnemonic systems of memorization, two commonly used techniques are loci and PegWords. Using the loci technique, locations serve as retrieval cues for the information being recalled. PegWords entail learning a series of words that serve as 'pegs' on which memories can be hung. Both techniques have been used in trials of authentication mechanisms.[24]

In contrast to their imperfect ability to recall, 'humans have a vast, almost limitless memory for pictures' – an ability known as the 'Picture Superiority Effect'.[25] Unlike recall, picture recognition appears to be relatively unaffected by the process of ageing. There remains some debate as to why pictures are significantly easier to remember than words. The Dual-code theory suggests that the advantage springs from the brain remembering pictures simultaneously in two different ways, using an image code and a semantic code. Another possibility is that pictures generate a more detailed memory, and are thus easier to extract from long term memory.[26] Regardless of this debate, the brain has a proven greater capacity to store and recognise pictures over letters and numbers. This makes images an excellent candidate for authentication mechanisms, especially given the acknowledged failings of current knowledge based authentication mechanisms.

Alternative authentication mechanisms

Despite the prevalence of knowledge-based authentication at the ATM and online, research continues into alternatives, such as graphical authentication and mechanisms that monitor an individual's behaviour and include additional security checks when their behaviour deviates from its normal pattern. The use of biometric measurements is a further option, but is outside of the scope of this article. Further details on biometric measurements can be found in the dissertation from which this paper is drawn.[27] No mechanism is perfect: all have limitations. The ideal password should be easy to remember but hard to guess. As Renaud comments, 'any authentication mechanism teeters between memorability and predictability requirements'.[28]

Personalisation and behaviour

An emergent trend in security mechanisms is the tracking of patterns of user behaviour. If a user who travels relatively little takes a holiday abroad, they may be surprised and inconvenienced to find their card disabled, when security software notices an abnormal transaction. Conversely, the same user may be relieved when the system prevents their account from being used by a thief. Sasse highlights the desirability of determining the method of authentication after taking into account the nature of the task.[29] For instance, a user could be asked for less stringent authentication if they are performing a task that fits their normal behaviour pattern, and a more stringent method of authentication if their behaviour is unusual. For example, a customer consistently withdraws £20 from her local ATM. If she tries to take out £200 from a different ATM, she will be prompted for extra authentication. This approach is consistent with current societal trends that demand speed and an individual approach from technology services. They may provide increased customer loyalty as a result. The approach does not provide

[23] *A term first used by J. R. Anderson and L. J. Schooler, 'Reflections of the environment in memory', Psychological Science, 2, 1991, 396-408.*

[24] *Jianxin Yan, Alan Blackwell, Ross Anderson and Alan Grant, 'The Memorability and Security of Passwords – Some Empirical Results'.*

[25] *Antonella De Angeli, 'Pictorial security at the ATM: the visual identification protocol', Advances 2002: annual research report for NCR Self-service strategic solutions, Volume 1, 2002, 161-169.*

[26] *Antonella De Angeli, Lynne Coventry, Graham Johnson and Karen Renaud, 'Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems', International Journal of Human-Computer Studies, Volume 63, Issue 1-2, (July 2005), 128-152.*

[27] *Wendy Moncur, 'Exploring the usability of multiple graphic passwords', MSc Dissertation, retrieved from http://www.csd.abdn.ac.uk/~wmoncur/publications/Exploring%20the%20usability%20of%20multiple%20graphical%20passwords.doc, 2006.*

[28] *Karen Renaud and Antonella De Angeli, 'My password is here! An investigation into visuo-spatial authentication mechanisms', Interacting with Computers, Volume 16, Issue 6, December 2004, 1039.*

[29] *Martina Angela Sasse, Sacha Brostoff and Dirk Weirich, 'Transforming the weakest link - a human/computer interaction approach to usable and effective security', BT Technology Journal.*

The effects of interference on memorability when a user has many separate graphical passwords are small in comparison to that exhibited when a user has multiple knowledge-based passwords.

authentication in itself. It must be combined with other approaches, such as knowledge-based or graphical authentication before it can be assessed for memorability and predictability.

Graphical authentication mechanisms

Graphical authentication mechanisms use picture recognition to authenticate the user. This is based on the understanding that people remember images far better than words.[30] They can remember more images, more accurately, and with less adverse effects from the process of aging. An attractive feature of graphical authentication mechanisms is that they are harder to disclose than PINs and semantic or syntactic passwords. Research into the potential of graphical authentication continues.

Graphical authentication systems have their own requirements relating to usability. It is recognised that images used must be concrete, nameable and distinct.[31] Each image displayed must be visually dissimilar, and from a separate semantic category. For example, if a user is shown ten images, ideally they should each be from a separate category such as transport, mammals, faces, architecture, to prevent the user from mixing images of a similar nature. Conceivably, they should not be shown two pictures of the same item, such as flowers on the same screen, because this can cause confusion. The effects of interference on memorability when a user has many separate graphical passwords are small in comparison to that exhibited when a user has multiple knowledge-based passwords.[32]

Immaturity of authentication systems

Successful authentication mechanisms should provide a balance between security and usability. Yet no current authentication mechanism fits all the requirements: every mechanism has its failings. Providers of secure systems must look to their users, and to understand and accept their innate cognitive and physical limitations, if they are to create authentication mechanisms that are usable, and thus less flawed. In the meantime, users will continue to exhibit insecure behaviours, circumventing the best intentions of secure systems.

Wendy Moncur is a PhD candidate, working between the Universities of Aberdeen and Dundee. She was awarded an MSc with Distinction in Multimedia and Interactive Systems in 2006. She has seventeen years experience of Information Technology in industry, including ten years working as a database design specialist for a leading UK bank and European financial services institutions.

Dr Grégory Leplâtre is a lecturer at Edinburgh Napier University. His research interests lie in interface design and human-computer interaction, and include collaborative work with NCR, a global manufacturer of ATMs and point-of-sale systems.

[30] *Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter and Aviel D. Rubin, 'The Design and Analysis of Graphical Passwords', Proceedings of the 8th USENIX Security Symposium, 1999, available at http://www.usenix.org/events/sec99/full_papers/jermyn/jermyn_html/.*

[31] *Antonella De Angeli, Lynne Coventry, Graham Johnson and Karen Renaud, 'Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems', International Journal of Human-Computer Studies.*

[32] *Wendy Moncur and Grégory Leplâtre, 'Pictures at the ATM', Proceedings of the SIGCHI conference on Human factors in computing systems, 2007, 887-894.*

