Securing online transactions with biometric methods

James A. Pope*

College of Business Administration,
University of Toledo,
2801 Bancroft St. Toledo, Ohio 43606 USA
Fax +1 419-530-2380
E-mail: jpope@utoledo.edu
*Corresponding author

Dieter Bartmann

Information Systems II,
Universität Regensburg,
93040 Regensburg, Germany
Fax:+49 941-943-1881
E-mail: dieter.bartmann@wiwi.uni-regensburg.de

Abstract: As more and more marketing and retailing is done electronically, the security of online transactions becomes a growing problem. The public media almost daily carry stories of security breaches in firms of all types and sizes, from banks to retailers. If the electronic retail supply chain cannot assure its customers that their transactions will be secure, the growth of this sector will be limited. Traditionally, the primary method of securing access to an online transaction system and its databases has been passwords. Passwords have been widely used because of their simplicity of implementation and use, but are now regarded as providing minimal security. More sophisticated methods based on biometric attributes have been developed. Among them are voice recognition, fingerprint identification and typing recognition methods. We shall describe and discuss the traditional methods, and then biometric methods and their relative advantages and disadvantages in securing online transactions.

Keywords: online transactions; security; biometric; voice recognition; fingerprint systems; typing authentication systems; passwords; security tokens; retina scans; PIN; electronic marketing.

Reference to this paper should be made as follows: Pope, J.A. and D. Bartmann (2010) 'Securing online transactions with biometric methods, *Int. J. Electronic Marketing and Retailing*, Vol. 3, No. 2, pp.132–144.

Biographical notes: James A. Pope is a Professor in the Department of Information, Operations and Technology Management at the University of Toledo, Toledo, Ohio, USA. He has taught and conducted research at universities in the USA, the Netherlands, Germany and India.

Dieter Bartmann holds the Chair in Information Systems at the University of Regensburg, Germany. He is also the Director of the Institute for Bank Innovation at the University of Regensburg. In addition to Regensburg, he has held chairs at several European universities including Nuremburg and Bamberg in Germany and St. Gallen in Switzerland.

1 Introduction

With stories of data theft appearing almost daily in the press (e.g., Pereira, 2008), the issue of keeping online transactions secure has become a critical issue with most organisations. In a 2007 survey, half the bank customers surveyed said that security features were extremely important when deciding whether to go online. (*Economist*, 2008) Organisations engaging in online transactions such as retailers and banks are constantly at risk from breaches in security in online transactions and the subsequent damage to their reputations. A prime example is the US retailer Target. Thousands of records of customers and transactions were compromised and the incident was widely publicised (Banks, 2007). In addition to the actual financial loss and subsequent liability sustained in these data breaches, the businesses and organisations suffer reputation damage. In the Target case, for example, although the data breach took place in 2006, they are still negotiating settlements with those who were damaged (in particular, the credit card companies) in 2009 and having these settlements continue to be reported in the media (Kingsbury, 2009).

Traditionally, the primary method of securing access to an online information system and its data bases has been passwords. Passwords have been used widely because they are easy to implement and use. For reasons we will discuss below, passwords have become increasingly deficient as a primary protection scheme. More sophisticated knowledge based methods as well as token based and biometric methods have been developed: among the latter is voice recognition, fingerprint identification and typing recognition methods. In this paper, we shall describe and discuss several of these methods and their relative advantages and disadvantages in securing online transactions and then focus on biometric methods.

Without more sophisticated methods of providing security, the electronic retailing supply chain faces significant limits on its growth. Users want security and protection from schemes such as financial loss and identity theft, but they also resist complex methods such as long passwords or involved token-based methods. Trying to find this balance between security and simplicity has been the bottleneck in securing online transactions. Finding the balance will reassure the customers in the electronic retailing supply chain and protect the firms involved from financial and reputational loss.

2 Security of online transactions

In addition to the security breaches reported in the popular media, various academic and industry surveys report the same problems. A ten-year-old survey of Australian companies reported that 37% of the respondents had experienced some form of intrusion or other unauthorised use of their computer systems in the previous twelve months (Thompson, 1998). Two years later, the Canadian Government reported in a survey that 32% of respondents had experienced someone hacking into their e-mail accounts or computer files while 11% reported that their personal information had been made public (Borchers et al., 2008)

In 2007, the Computer Security Institute (CSI) reported that 46% of the respondents to their annual survey had suffered a security incident. Interestingly, 10% reported that they did not know if they had had a security breach. In the same survey, 18% of the

respondents reported that biometrics was one of the security technologies they used (Richardson, 2007). In their 2008 survey, 43% reported experiencing a security incident, down three percentage points from the year before. On the other hand, the percent not knowing went up three percentage points to 13%. The percent using biometrics went up to 23% (Richardson, 2008). The fluctuations can be explained by the non-random nature of their surveys.

The Deloitte Touche Tohmatsu 2009 Global Security Survey reported that 50% of their respondents had experienced an external security breach in the previous 12 months. Of those reporting a breach, 52% reported repeated attacks. Significantly, almost 60% could not answer the question asking the financial loss they had suffered from the security breaches (Brightman and Buith, 2009).

Although some of these surveys are a bit old, their age emphasises that the problem of the security of online transactions is not new, and the subsequent reports tell us that the problem is getting worse and will not go away by itself. Let us now look at some of the methods that can be used to protect against these security breaches and the resulting financial and reputational loss.

2.1 Knowledge based methods

2.1.1 Passwords and PINs

Knowledge based methods rely on something you know, sometimes referred to as 'shared secrets' (FFIEC, 2006; Maus, 2008). Because of this, they authenticate the knowledge rather than the authorised user (Matyáš and Riha, 2002). These methods include passwords and personal identification numbers (PINs). For a number of reasons, protection with passwords and PINs is no longer sufficient in modern information systems. 'Passwords are now a larger security risk than ever before' [Reid, (2004), p.22]. Password secrecy cannot be guaranteed. With the increasing number of passwords the user has to remember, people resort to increasingly insecure methods of remembering them. Some people keep a written list of their passwords, often in plain view in their work areas. In addition, users may use the same password or close variations for all applications. Or, users may choose a password which is easy to guess, such as names of children or birthdates. There is no way to prevent the unauthorised passing on of passwords. In a downtown San Francisco poll, two-thirds of the workers asked exchanged their passwords for a $3 coffee coupon. In another poll, 80% of workers said they would disclose their passwords to someone in the company if asked. (Bjorn, 2007) Often these shared passwords are kept in lists since the secondary user does not use them often enough to commit them to memory. St. Clair et al. (2006) conclude that the low entropy (unpredictability) of passwords in use and the increasing sophistication of password cracking methods make passwords obsolete as a data security method.

This is especially critical against the background of constantly increasing damage potentials and stricter requirements in controlling risk. Intrusive methods such as key logging, shoulder surfing, phishing, social engineering, man-in-the-middle and password ruses can be used to record the key strokes for passwords or PINs or to lure the user into revealing the password or PIN (Maus, 2008). Besides the risk factor, passwords are costly to companies in other ways. Many employees forget their passwords. The reset is costly. For example, 40% of all calls to help desks are for forgotten passwords. Each year, companies spend up to $150 per user trying to maintain secure passwords (Bjorn, 2007).

Passwords are scaleable (referring to the ability to increase the level of security). A longer or more complex or random password increases the security level. The change in scalability, however, must be done consciously at a point in time and is not done easily by the system 'on the fly.' This scalability is limited by the ability of humans to remember passwords. We can typically at most remember a maximum of seven random characters, so longer passwords do not necessarily increase their unpredictability (St. Clair et al., 2006).

2.1.2 Transaction numbers and other methods

A form of passwords used in German banks is the transaction number or TAN. All online transactions must be accompanied by a TAN. The bank periodically sends the user a computer generated list of 120 or so TANs. One method is to ask the user to type in any TAN from the list (each one may be used only once). The computer authenticates it and allows the transaction if there is a match. This means the user needs only a sample of the TAN list available at any given time and the rest of the list may be kept secure. This makes it easier, however, for an unauthorised user use a number he previously obtained, e.g. by 'phishing'. Another method is for the application to specify the sequence number of the TAN and then authenticate it. This makes it harder for attackers by reducing the probability of a guess, but means the user must have the entire TAN list available anytime there is a transaction (which makes it subject to compromise or loss). Neither method is particularly secure from a skilled and determined attacker, especially one using phishing. In addition, German banks report that the TAN list method costs approximately €3 per year per customer.

An alternative method used in the UK is to ask the user for characters in specified positions in the password. Passwords can also be used in combination with social knowledge, such as the maiden name of one's mother. Although these social knowledge items are routinely known only to the user, they are generally public knowledge and could be learned by someone determined to compromise the system.

A colleague in India reports the use of virtual credit cards for online transactions. Before conducting the transaction, the customer receives a one-time credit card number from his or her bank. The one-time number is connected to the actual credit card at the bank, but can be used only once and for only the amount specified by the customer. The system does involve multiple additional steps (i.e., increased complexity) and could be subject to a phishing attack.

2.2 Token based methods

Token based methods involve something you have (FFIEC, 2006). They include smart cards and other devices such as universal serial bus (USB) identifiers. Although the user cannot transmit the security code as with a password, the token can be loaned, lost or stolen. As with knowledge based methods, they authenticate the holder of the token, not the authorised user (Matyáš and Riha, 2002). In addition, if the user does not have the token at the moment, online transactions cannot be conducted until the token is retrieved. Tokens can also be expensive. Smart cards, for example, must be manufactured, personalised, and delivered to the customer. The German banking industry has estimated that smart cards will cost €50 per customer. This includes the three items we mentioned

plus the security infrastructure and the cost of the misdelivered or misdirected cards. Tokens with imbedded RFID chips can be read without the owner's knowledge. For example, a cyber-intruder could sit in a busy shopping mall with a reader in a briefcase and read the cards of people walking past him. This has even spawned a secondary industry of protective shielding for personal cards (Shepard Envelope Company, 2008).

The biggest advantage of knowledge and token based methods is that they can be changed easily. If there is a system compromise, the user need only be issued a new PIN or token. As we shall see, biometric methods are much more permanent. There are additional methods such as the mobile TAN, digital signatures with smartcards, smartcards with flicker codes, and so on, but all have the same drawbacks of being expensive to implement and complex to use.

3 Biometric methods

Biometric methods are those which use a distinguishable physiological or behavioural attribute of the user for authentication, in other words, who you are (Matyas and Stapleton, 2000; Zivran and Erlich, 2006). The three most common are voice recognition, fingerprinting and typing recognition (Welcome to Biometrics Australia, 2008). A fourth which has received notice in the press, but which has limited usefulness is eye (retina/iris) identification. Each has its advantages and disadvantages, but, as we shall see, all are not equal either in their range of applications or in their usefulness or security levels.

Biometric methods have become a key technology for person authentication. A project survey (Graevenitz, 2007) yielded the following results:

The vast majority of those responding think that biometrics will be successful in the future, 40% predicted strong growth rates ranging up to over 60% per year. The International Biometric Group estimates that the yearly revenues of biometrics will increase from €3 billion in 2007 up to almost €6 billion in 2010. Experts such as Reid (2004) think that *in the future, biometric methods will dominate the security market and replace passwords*. Nevertheless, important issues of practicability remain.

In Germany, the industry association Bitkom has estimated that the turnover revenue of biometrics will grow from €120 million in 2006 to €300 million in 2010. Government demand is very important here, up to 45% according to Soreon Research.

3.1 Success factors and problems

From the point of view of the user, for a biometric method to be successful it must be acceptable, easy to use and non-invasive. From the point of view of the organisation providing the security, it must be economical, deployable, mature and have a short habituation time [Reid, (2004), p.56]. A part of maturity is the error rate. With large numbers of users and transactions, the error rates can yield intolerable numbers of errors. For example, a system which is 99.9% accurate will still yield 100 errors per million transactions. This is in contrast to Six Sigma which specifies 3.4 errors per million as a maximum. Two key measures of quality in any system are:

1 the false rejection rate (FRR) or false non-match rate (FNMR) or more generically, false negatives

2 the false accept rate (FAR) or false match rate (FMR), or, more generically, false positives (Basics of Biometrics, 2008).

An additional measure is the cross over error rate (CER) or equal error rate (EER). It measures the sensitivity of the biometric method in '…balancing ease of use for the authentic user while at the same time reducing the impostor rate access' (Revett et al., 2007)

3.2 Eye identification

This method involves scanning either the retina or the iris of the eye of the user and either comparing it to a pattern in the user's files or to a pattern on an ID carried by the user. The iris is preferred since it is possible to damage the retina by scanning it with a laser beam. The method is highly accurate since each individual's iris pattern seems to be unique.

The primary drawbacks are size and cost. This method requires expensive, bulky equipment, so is useful only when the user comes to the system. Examples are security checkpoints (such as at airports) or fixed terminals (such as cash machines) (Lichanska, 2008). A user may also be forced to verify his or her identification by intruders. In the case of large scale operations such as airport security, it is unlikely that all passengers will have their patterns on file, so they must carry special cards. Unless the identity pattern is encrypted in a highly secure manner, the system can be easily fooled. Age and disease (cataracts, for example) can also alter the eye patterns, so the file pattern would have to be updated periodically.

A final problem is scalability. A given system, under ideal circumstances, will yield a fixed level of security. The system cannot be changed easily to adapt to the required security need of the application. On the other hand, the system cannot be fooled with a representation of the retina or iris (Lichanska, 2008).

3.3 Voice recognition

One of the largest companies providing voice recognition technology for security purposes is Voice.Trust, AG in Germany, their system is used primarily to reset forgotten passwords. Founded in 2000, they have approximately 250,000 licenses installed.

The principle advantage of voice recognition is simplicity and ease of use. Within an enterprise with an internal phone system, minimal additional equipment is needed. The user is prompted to speak a phrase and the system matches the speech pattern to a file on that individual. (Biometrics – Voice Verification, n.d.) It does require the individual to 'train' the system.

There are a number of problems with a voice recognition system. The system can be fooled if the user's voice is recorded and played back by an intruder. (Biometric Authentication, 2008) The user can be forced to use the system, although stress may alter the speech patterns to the point where they do not match the file. A user may also 'give away' sample recordings of their speech patterns in collaboration with an outside intruder. Even in normal use, the password is given to the user in a non-encrypted manner which may be intercepted. Furthermore, employees have shown a reluctance to use the system knowing that their voices are recorded. At one large German bank, 80% of the employees still preferred using the help desk for password reset rather than the voice

recognition system. Voices may change with age or illness, but the system may be 'retrained' to adapt to these changes.

More serious is the limitation on accessing the system from outside the enterprise. Although voice systems are available through the internet, the quality of the system and thus, transmission can vary widely. This may make it difficult for off-site users to access the home system. Because of the low level or lack of encryption, the system is more susceptible to interception or attack when used remotely for online transactions.

Voice recognition is scalable. To increase security at any given time, the user can be asked to speak longer sentences.

3.4 Fingerprint recognition

Fingerprint recognition has been used for over 100 years (Kleinst, 2007). Fingerprint recognition is similar to eye recognition in terms of advantages, disadvantages and scalability. The required equipment tends to be smaller and less expensive. A fingerprint scanner imbedded in a mouse, for example, can be purchased for as little as $50 (APC APC Biometric Mouse, 2008). This makes it possible for a user to carry the equipment while travelling, but, on the other hand, requires the user to carry special equipment. This means the user must have his or her own computer or the computer being used must be equipped with the hardware and software interface to use the equipment. A common use is to use a fingerprint scanner to protect a file containing the user's passwords (Groom, 2007; Harris, 2008) Fingerprints are easier to gather on a large scale (and are often done so as with people in the military), so loading the database of patterns would be less onerous than with eye scanning when they are used for identification. A drawback, however, is that some types of scanner can be fooled by pictures or moulds of fingerprints. (Harris 2008) In addition, preliminary studies have shown that people, in general, are not comfortable with having their fingerprints on file in a central database (Schmidt et al., 2008). In other words, it fails the invasiveness test.

3.5 Typing recognition

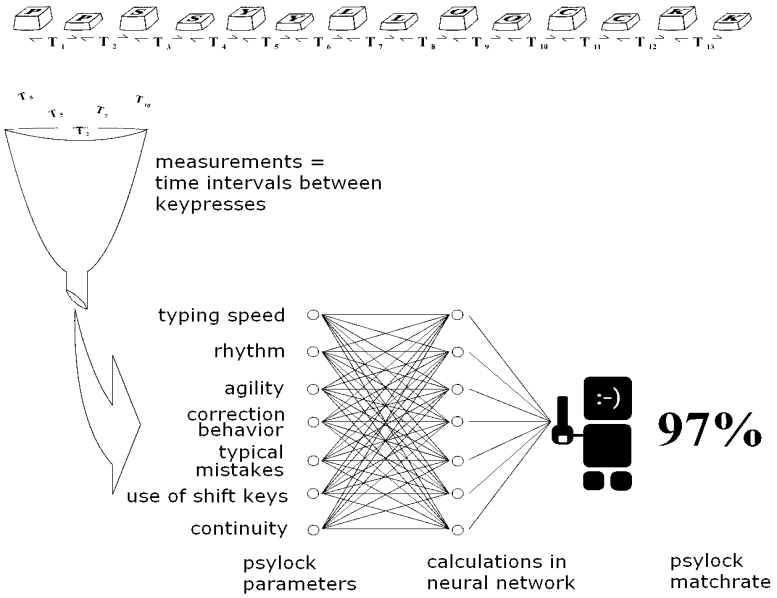
Typing recognition analyses the pattern of a user's typing and grants or denies access bases upon a match on file (Guven and Sogukpinar, 2003). Early methods, such as BioPassword, are similar to the eye, voice and fingerprint systems. A sample is on file, and the system directly compares the way the user types the sequence with the file sample using features such as speed and rhythm.

The other approach, used by a system called Psylock (Bartmann et al., 2007a, 2007b), analyses the user's typing with a statistical model which measures seventeen characteristics of a person's typing such as right- and left-handedness, general features of typing (ten-finger system, typing with two fingers, ...) and the precision of typing (overlaps: a second key is pressed while the first key was not yet released, and so on). The process records the basic observation data 'key holding time' and 'time of transition' and fifteen others. The program then generates and calculates the parameters for a complex stochastic model. The various features are individually weighted using a simulated neural network.

In other words, the user may type any sequence, using a different one each time, and the system analyses the typing characteristics and either grants or denies access. In practice, the system gives the user a sentence to type when prompted.

Typing recognition, in general, has the advantage that no additional equipment is necessary. The system in the home server analyses what is typed from any keyboard. Systems such as BioPassword are more sensitive to different keyboards since they must match a given pattern. Since Psylock uses a statistical model, it is nearly keyboard independent. Both require the user to 'train' the system to recognise their typing patterns. No additional equipment means there is no cost for equipment, distribution, installation, maintenance or replacement. The system is 'nearly' keyboard independent because keyboards for different languages differ and may affect one's typing parameters.

Figure 1 Illustration of the Psylock methodology



An additional advantage of Psylock is scalability. Since it does not try to match a pattern, the system can generate a sentence of any length or complexity 'on the fly' depending upon the desired level of security. The longer and more complex the sentence, the more secure the system. The system can automatically determine the required security level and give the user a longer or shorter sentence to type.

Finally, the user cannot share the Psylock 'key' as one can a password or PIN. Even if one knew all the parameters used in the statistical model, one could not describe his or her typing technique in a manner which could be used to gain unauthorised access. The user generally could not be forced to enter the system since the stress would cause the typing characteristics to change. There is no secrecy in Psylock. Anyone can see the sentence the user is asked to type; only the correct user can type it correctly.

All biometric methods suffer from first time enrolment (FTE) problems. Individuals who do not have the biometric characteristic cannot enrol. For example, someone who is paralysed and types with a stick held in his or her mouth could not use a typing or fingerprint system (Matyáš and Riha, 2002). In addition, something could happen to the 'biology.' A broken or sprained finger, for example, would change the typing characteristics, although it would affect the early systems more than Psylock. In the case

of a permanent change (arthritis, missing digit, etc.) the system could be 'retrained.' Likewise, an illness which affected the voice would render a voice system useless.

Something that the other methods do not have that Psylock does is the ability to run in the background. Without the user's explicit knowledge, the system could determine if given users are who they say they are. In e-mail applications, the system could determine if the person typing the message is the one identified as the sender. Or, it could sound an alarm in a security area if an unauthorised user is typing on a terminal. Or, in distance learning, it could determine if the person taking the exam is the one who signed up for the course (but, alas, it cannot tell if someone else is sitting there giving the answers, or if someone is a surrogate course taker).

3.5.1 Areas of application for keyboard systems

Since it is a pure software solution based on a stochastic model, Psylock has a great deal of flexibility compared to the other methods. The most interesting application is for web access. All web applications that have been using passwords so far (eBay, PayPal, Amazon, online banking, etc.) can be secured with Psylock. Worldwide remote access to the company network through the internet is possible as well. With Psylock, age recognition for the legal protection of children and youth is possible. Registration has to be done only once to be used as a secure gate to gain access to the internet. The application which should find the most popularity among consumers is the authentication of individuals in Web 2.0. The security and comfort of online banking applications can be significantly increased. Typing behaviour shown while filling out a transfer form is analysed and the result added to the transfer as a fraud resistant signature. This makes TANs (transaction numbers) obsolete and prevents phishing. It is possible to offer a virtual USB stick secured with Psylock as a web service.

Psylock can be used for login at a computer workstation instead of or, if necessary, in addition to a password. If the customer definitely wants to keep the password, he can at least simplify the reset procedure with Psylock. This saves time and costs. Psylock can be used as a digital signature on a typed document or as a proof of authorship, e.g., in secure emailing. This use would be appropriate for government sectors. It can be used to improve the security of access to common databases in supply chains involving firms in several countries.

3.5.2 Comparative analysis (conducted by Wincor Nixdorf AG)

The Wincor Nixdorf AG in October 2006 conducted a comparison of its own product Pro Tect/Work Enterprise (fingerprint), the voice recognition software VoiceTrust and Psyock (typing). It was not made available publicly, but they provided a copy to one of the authors.

The limitations it found were: special hardware requirements for fingerprint, quality of the speech channel for voice and possibly wireless keyboards for typing. Of the three main uses they tested initially, login to PC, activations/password reset and legitimation processes, only Psylock was found to be applicable in all three uses. In further tests involving individual use cases, accessing systems, e-mail/document signatures, legitimations such as online banking and online authentication service, only Psylock was found to work in all cases. Pro Tect/Work Enterprise (fingerprint) systems were limited

in signatures and legitimations and not useable for online authentication. Voice trust was limited in signatures and online authentication.

As a result of the test, Wincor Nixdorf AG decided to become a distributor for Psylock.

4 Summary and conclusions

4.1 Summary

In discussing methods of providing online security, we have covered a number of features of each of the methods. In Table 1, we summarise these features. The seven features are:

a Ease of use. This includes aspects such as the ease of remembering a password, the number of steps in using the method and the complexity of the steps.

b Ease of change. If the method is compromised, how easy is it to change it?

c Ease of Transferability. The difficulty in voluntarily allowing someone else to use the method.

d Scalability. The ability to increase the level of security, ranging from requiring a conscious deliberate effort to the system being able to change 'on the fly.'

e Special hardware. Whether or not special hardware is required to use the method.

f Attack vulnerability. The ability of someone other than the authorised user to obtain access to the system without permission.

g Ease of First Time Enrolment (FTE). The difficulty or even possibility of enrolling a user in the method.

Table 1 Features of security methods

Feature	*Method*				
	Passwords	*Tokens*	*Fingerprint*	*Voice*	*Typing*
Ease of use	High	Medium	Medium	Medium	High
Change	Medium	Medium	N/A	N/A	N/A
Transfer	High	High	Low	Low	N/A
Scalable	Medium	Low	Medium	Medium	High
Hardware	No	Yes	Yes	Yes	No
Attack	High	Medium	Medium	Medium	Low
FTE	High	High	Medium	Medium	Medium

From the table, we can see that the most significant advantages of biometric methods are the difficulty or inability to transfer them to an unauthorised user, their safety from attack (especially typing), ease of use and their scalability. They are weakest in ability to change and first time enrolment. Special hardware feature is a mix with passwords and typing the best options. Of the biometric methods, typing has the best features, especially if the method is based on a stochastic model such as Psylock rather than the traditional pattern

matching. Passwords continue to be used widely because of their ease of use and, probably, because of familiarity. Unfortunately, they provide the weakest security. 'Passwords in the best of times are weak and in general, easy to guess… a biometric is a stronger means of authentication than a password' [Reid, (2004), pp.15, 18].

4.2 Conclusions

Security of online transactions is an important problem now, and will continue to increase in importance. Failure to provide online security will hamstring the further development of retail based electronic commerce. Consumers are increasingly fearful of financial fraud and identity theft. A broad range of applications require online transaction security from online retailers, banks, corporate data bases to the military. The US Air Force has (April, 2008) run recruiting commercials on TV showing airmen whose sole job is defending the US Department of Defense computers against intruders. Apparently, the task is more difficult than they anticipated (Gorman and Ramstad, 2009). Given the significant weaknesses of knowledge and token based security methods, biometric methods will become ever more important. They authenticate the user and are difficult to obtain by fraud. They must overcome unease with intrusiveness and deployability. Unfortunately, this is happening slowly. Shin et al. (2008), acting as customers, visited the websites of nine financial institutions in the USA. They included five banks (two national, one online and two local), two credit card companies, an online stockbroker and an online payment processing company. None of the nine used any biometric methods for authentication of the users.

Attempts to make knowledge and token based methods more secure have increased their level of complexity to the point where the ease of use may become a dominant factor in swinging the pendulum of acceptability to biometric methods. It cannot happen too soon; the security is necessary and needed.

As with many applications in the information technology area, the crux of the matter may hinge upon whether the protectors or the hackers advance most rapidly technologically. In fact, the technology of being connected is also a factor. Personal data assistants (PDAs) are becoming more powerful and more widely used in place of laptops or terminals (Wingfield, 2008). None of the biometric methods have been adapted for use with PDAs. And, PDAs are being replaced by smart phones, many without physical keyboards. Whether or not biometric methods can be adapted to this new technology easily is a matter for further research and will become a matter of critical importance for online transaction security.

References

APC Biometric Mouse (2008) Available at http://www.cnet/review/mice/APCBiometricMouse.htm, (accessed on June).

Banks OK Visa, TJX Deal (2007) *The Boston Globe*, 21 December.

Bartmann, D. and Wimmer, M. (2007a) 'Kein problem mehr mit vergessenen passwörtern (No more problems with forgotten passwords)', *Datenschutz und Datenversicherheit*, Vol. 3, pp.1–5.

Bartmann, D., Bakdi, I. and Achatz, M. (2007b) 'On the design of an authentication system based on keystroke dynamics using a predefined input text', *International Journal of Information Security and Privacy*, April/June, Vol. 1, No. 2, pp.1–12.

Basics of Biometrics (2008) Available at http://www.biometricinnovations.com/BiometricTechnology_Overview.html, (30 May).

Biometric Authentication: Which Method Works Best?' (2008) Available at http://www.technovelgy.com, (accessed on 2 April).

Biometrics – Voice Verification – Homeland Security (n.d.) Available at http://globalsecurity.org/security/systems/biometrics-voice.htm, (accessed at 29 December).

Bjorn, V. (2007) *Solving the Weakest Link in Network Security: Passwords*, available at http:///www.digitalpersona.com, (accessed on 2 June 2008).

Borchers, A., Park, S-H. and Smith, J. (2008) 'Business value of IS security quality: the effect of data breaches on the market value of firms', *Proceedings of the 2008 DSI Meeting*, pp.4761–4766.

Brightman, I. and Buith, J. (2009*) Losing Ground: 2009 TMT Global Services Security Survey*, Deloitte Touche Tohmatsu DTT Technology, Media and Telecommunications Industry Group.

Economist (2008) 'Bodily functions: can biometrics make banking more secure?', 12 July, p.85.

FFIEC (2006) *Authentication in an Internet Banking Environment*, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf, (accessed on 29 December 2008).

Gorman, S. and Ramstad, E. (2009) 'Cyber blitz hits US, Korea', *Wall Street Journal*, 9 July, p.A1.

Graevenitz, G. (2007) *Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren (Success Factors and Sales Opportunities for Biometric Identification Solutions)*, Münster – Hamburg.

Groom, R. (2007) *Fingerprint Scanner: Help Remembering Passwords with Your Finger*, available at www.espionageinfo.com, (accessed on 2 April 2008).

Guven, A. and Sogukpinar, I. (2003) 'Understanding users' keystroke patterns for computer access security', *Computers and Security*, Vol. 22, No. 8, pp.695–706.

Harris, T. (2008) *How Fingerprint Scanners Work*, available at http://www.about.com, (17 May).

Kingsbury, K. (2009) 'TJX to pay $9.8 million to settle data-breach probe by states', *The Wall Street Journal*, 23 June.

Kleinst, V.F. (2007) 'Building technologically based online trust: can the biometrics industry deliver the online trust silver bullet?', *Information Systems Management*, Vol. 24, No. 4, pp.319–329.

Lichanska, A. (2008) *Retina and Iris Scans*, available at http://www.espionageinfo.com, (accessed 2 April).

Matyas, S. and Stapleton, J. (2000) 'A biometric standard for information management and security', *Computers and Security*, Vol. 19, pp.428–441.

Matyáš, V. and Riha, Z. (2002) 'Biometric identification – security and usability', in Jerman-Blazic, Borka and Tomaz Klobucar (Eds.): *Advanced Communications and Multimedia Security (IFIP Advances in Information and Communication Technology)*. Norwell/Dordrecht, p.227–239.

Maus, T. (2008) 'Das Passwort ist tot – lang lebe das passwort (The password is dead; long live the password)', *Datenschutz und Datensicherheit*, Vol. 8, pp.537–542.

Pereira, J. (2008) 'Chains report stolen card data', *Wall Street Journal*, 18 March, p.B4.

Reid, P. (2004) *Biometrics for Network Security*. Prentice-Hall, Upper Saddle River, NJ.

Revett, K., Tenreiro de Magalhães, S. and Santos, H.M.C. (2007) 'On the use of rough sets for user authentication via keystroke dynamics', in Neves, J., Santos, M. and Machado, J. (Eds): *EPIA 2007*, LNAI4874, Springer Verlag, Heidelburg, pp.145–159.

Richardson, R. (2007) *CSI Computer Crime and Security Survey*, Computer Security Institute.

Richardson, R. (2008) *CSI Computer Crime and Security Survey*, Computer Security Institute.

Schmidt, M.B., Das, D., Kumar, V. and Bekkering, E. (2008) 'A proposed study and analysis of user perceptions of biometric acceptance,' *Proceedings of the Decision Sciences Institute*, November, pp.3961–3966.

Shepard Envelope Company (2008) Auburn, MA, available at www.shepardenvelope.com.

Shin, S., Cunningham, J. and Tucci, J. (2008) 'A study of two-factor authentication against online identity theft', *Proceedings of the Decision Sciences Institute*, November, pp.11001–11006.

St. Clair, L., Johansen, L., Enck, W., Pirretti, M., Traynor, P., McDaniel, P. and Jaeger, T. (2006) 'Password exhaustion: predicting the end of password usefulness' in Bagchi, A. and Atluri, V. (Eds): *ICISS 2006*, LNCS 432, Springer Verlag, Heidelburg, pp.37–55.

Thompson, D. (1998) 'Computer crime and security survey', *Information Management & Computer Security*, Vol. 6, No.2, pp.78–101.

Welcome to Biometrics Australia (2008) Available at http://www.biometricsaustralia.com/, (accessed 30 May).

Wingfield, N. (2008) 'Time to leave the laptop behind', *Wall Street Journal*, 27 October, p.D1.

Zivran, M. and Erlich, Z. (2006) 'Identification and authentication: technology and implementation issues', *Communications of the AIS*, Vol. 17, No. 4, pp.2–30.