IS Security: User Identification and Authentication with reference to South African Financial Services Case Studies

Subtitle

J.D. Rollason, K.I. Munro and T.M. Addison
University of the Witwatersrand

Key words: identification, authentication, biometrics

Abstract:

The Internet has brought many advantages to everyday and business life. Among the advantages is that an individual can now perform several financial transactions such as the transferring of funds and payments to creditors, from home or office (or even from overseas) 24 hours a day, seven days a week. However, the advantage of easy access also brings certain disadvantages. Recent television publicity highlighted how a technical expert could breach the security of several institutions' on-line systems with relative ease.

Information and security are paradoxical. There is a desire to maximise the openness of the Internet and to make transacting as simple as possible, yet too much ease of use can cause security problems. Access control, which includes user identification and authentication, is a vital pre-requisite to information security. This paper examines user identification and authentication in the context of a five-pillar framework for information security, as described by respected authorities.

Identification can be equated to a username and is used to authorise access to a system. As usernames can be lost or stolen, it is necessary

to validate that the intended user is really the person he orshe claims to be – the authentication process. The three main authentication measures of passwords, access tokens and biometrics are described, and the advantages and disadvantages are reviewed.

Authentication measures are also paradoxical. Users prefer easy-to-remember passwords, but these can be discovered by dictionary attacks. If complex passwords are used, they are difficult to memorise and a hard copy can be stolen. Access tokens may be a more reliable form of authentication, but are also subject to loss or other abuse. Biometrics is probably the most tamper-proof form of authentication, but more expensive equipment is required to handle them.

Security is also a trade-off between the cost of its implementation and the value that can be lost if security is breached. The only way to guarantee 100 percent security is to incur infinite expenditure. The objective is always to implement all reasonable, cost-effective security measures, but more importantly is the assurance of a climate of security among the users involved with the system.

The user identification and authentication protocols describing the passwords of selected South African online financial services are reviewed.

1. Introduction

Schneier (2000, p.6) deems that 'the Internet has intertwined itself with almost every major system in our society'. This development has generated both advantages and disadvantages for online financial consumers. One advantage is that an individual can undertake financial transactions on a 24/7 remote basis, i.e. a consumer could transfer funds, pay creditors, buy and sell shares from his home or office (or even from overseas) 24 hours a day, seven days a week, without going anywhere near his bank branch or stockbroker's office.

However, the advantage of easy access has also generated certain disadvantages. As noted by Schneier (2000, pp.18-22), the Internet has three characteristics which made attacks against digital systems more devastating:

1. *Automation* – computers excel at dull repetitive tasks. Fast automation make attacks with a minimal rate of return profitable.

2. *Action at a distance* – the Internet has no borders. Internet attackers do not need to be anywhere near their prey.
3. *Technique propagation* – the ease with which successful techniques can be propagated: in cyberspace damage can grow exponentially; the Internet is a perfect medium for propagating successful attack tools; hackers can download computer viruses from web sites.

`The number one rated concern for both business and consumers in ...participating in e-commerce is the potential for loss of assets and privacy due to breaches in the security of commercial transactions.' Ghosh ((1998, p.9)

The fundamental dilemma of computer security and the Web is that, whilst the Internet has opened up a whole new online world to users, `security-unaware users have specific security requirements but usually no security expertise' (Gollman 1999, p.10). The key point made by Schneier (2000) in his seminal work, `Secrets and Lies', was that there was no such thing as *outright* information security, but steps could be taken to maximise protection and minimise risk of attack or loss. Schneier would undoubtedly have disagreed with the statement by Bothma (2000, p.124) that `online banking can be compared to using an ATM without fear of muggers!'

A framework was therefore developed for information security based upon five different services (von Solms, Eloff, Eloff and Smith, 2002, pp.1-3), which these authors called the five pillars or principles of information security. They are:

1. Identification and authentication
2. Confidentiality
3. Authorisation
4. Integrity
5. Non-repudiation

This paper examines the first service, identification and authentication in more detail and is restricted to the situation where a user is known to the system, for example, an existing client or a user who has pre-registered. Theory is also related to practice in some online South African financial service providers, such as Tradek.com, Mercantile Lisbon Bank, Standard Bank and Nedbank.

2.1. The Five Information Security Services

Schneier defined computer security as the `prevention and/or detection of unauthorised actions by users of a computer system' (2000, p.120). This section lists the five information security services and sets out how each can help achieve this objective.

2.1.1 Identification and Authentication

Before users access a system, it is necessary for them to be identified (the system must establish *who* they are) and authenticated (the system must receive *proof* of identity). This procedure is designed to allow valid users in and prevent access by hackers or other unauthorised users.

Identification and authentication measures are based on one of three things, something the user:

- knows (passwords)
- is (biometrics)
- has (access tokens) (Schneier 2000, p.136), (Liu and Silverman 2001, p.27).

These will be examined in more detail in sections 2.2.1 to 2.2.3 below.

2.1.2 Confidentiality

Confidentiality is akin to privacy and the objective of this service is to ensure that the contents of data, be they in a database or in transit between user and system, are protected against unauthorised reading (von Solms et al, 2002, p.10).

2.1.3 Authorisation

This process, also known as logical access control, determines either

- what different users *are allowed* to do, or
- what *can be done* to different objects in the system.

Whilst a user may have been validly identified and authenticated, he may only be permitted restricted access, for example, `read-only'.

2.1.4 Integrity

Every piece of data in the system should be as the last authorised modifier left it. Integrity applies to computer security (the security of writing data), data (ensuring data are not deleted or altered by unauthorised users) and software (ensuring programs are not altered, whether by error, malicious user or virus) (Schneier 2000, p.122).

2.1.5 Non-repudiation

This service (also known as `non-denial') means that the system has sufficient proof such that a user cannot later deny that a function had been undertaken or repudiate responsibility for a particular transaction.

Incorporation in, and enforcement by, a computer system of the five services listed above will help protect the system against unauthorised and fraudulent use (van Solms et al 2002, p.10), although, as consistently pointed out by Schneier (2000), no system is totally secure from attack. The following section will examine aspects of identification and authentication in more detail

2.2 Identification and Authentication Defined

`Authentication refers to the authentication or verification of a claimed identity' (Ashbourn 2000 p.1). Thus, for example, when a customer logs on to a Web site in order to undertake a financial transaction and claims to be an account holder, the authentication process verifies this claim via the customer providing a password and/or PIN linked in the bank's database to the customer's identity. A one-to-one matching process is undertaken, as the password and/or PIN is matched against the data held for the claimed identity.

The aim of identification, on the other hand, is to establish the identity of a single customer from within a database of possible customers, according to one specific or multiple characteristics which can be reliably linked to a particular user, without an identity being explicitly claimed by the customer. In this case there is a one-to-many matching process undertaken against a database of relevant data (Ashbourn 2000 p.1)..

The following sections will examine aspects of the application in practice of the three identification and authentication measures listed above.

2.2.1 Passwords

The traditional approach has been to allocate (or allow users to select) usernames for identification and passwords for authentication. The system has a list of usernames and passwords and compares those entered by users with entries stored in the database.

There are problems with passwords. Schneier (2000) considered that passwords were based on an oxymoron in that the concept was to have a *random string* that was *easy* to remember! Users opted for the latter and, thus, dictionary attacks against passwords were remarkably effective. (L0phtcrack was an example of a password recovery hacker tool optimised for Windows NT passwords).

Another problem is that e-mail messages and other items sent over the Internet travel as short data packets, (computers divide large files into packets for easier transmission). These packets are sent over the network by routers and, as packets pass from router to router, the data contained therein are open to anyone who wants to read them. An attacker can install a `packet sniffer' designed to steal usernames and passwords (Schneier 2000, pp.177-179).

Microsoft (2002) advises that `the key to strong passwords lies in their length and unfamiliarity' and provides the following tips for creating strong passwords:

- Do not use a common word with which the user can be identified
- Use both upper and lower case if the system can distinguish between them
- Use a minimum of six characters (but eight is preferable) including both letters and symbols
- Use a unique, long, strong password for each web site visited or service used.

Microsoft's browser, Internet Explorer, can also keep track of usernames and passwords, but this is a serious security risk, as such information could be obtained by a hacker or used by another person on the same computer. It is obviously also a high security risk simply to have a list of passwords written down next to a user's PC. However, as it is difficult to remember multiple, strong passwords, both Microsoft (2000) and Schneier (2000, p.147) acknowledge that it is necessary to have a list kept in a secure place and Schneier makes the additional suggestion that there should be two parts to the password, one memorised and the other written down.

Assuming that passwords are kept secret by their users, there are still the problems of communicating them in secret to the host and the host storing them securely (von Solms 2002, p.26). There are different ways of protecting passwords:

- Restrict access to the password database in the system
- Scramble the password prior to storing in the database

- Scramble the password on the user's PC prior to transmission

Most online systems make use of cryptography (`the science of secret writing' and seen by many `as the miraculous cure that will solve all computer security problems' according to Gollman 1999 p.200).

Cryptographic algorithms use keys to protect data through encryption, but cryptography today relies not on the secrecy of the algorithm, but that of the cryptographic key. As cited in both Gollman (1999 p.203) and Schneier (2000 p.91), Auguste Kerckhoffs first stated this thesis in 1883: `there is no secrecy in the algorithm, it is all in the key'. A short key is bad, but a long key is not automatically good. A cryptographic key is a secret value that makes a cryptographic algorithm unique for those sharing the key. If an eavesdropper does not know the key, the only option is to try to break the algorithm. In a `brute-force' attack, a hacker will try every possible key (Schneier 2000, p.99), (Gollmann 1999, p.203).

Space does not allow a full discussion of cryptographic keys, but two points should be noted:

1. The level of security will be determined by the level of encryption available. Originally, only US e-commerce web sites were allowed to support 128-bit encryption, as this was considered by the US Government to be of strategic importance and therefore not available for export. So the rest of the world had to make do with 40-bit encryption (Jarvis 1999). However, this restriction has since been relaxed.
2. Keys can be private and known only to the owner or public, details of which are freely available. Use of these two keys can be combined to exchange encrypted data between parties who have not met or do not know each other.

Thus, passwords are something the user knows (and should store in memory), which can be communicated in the open but should rather be sent encrypted.

2.2.2 Biometrics

`Biometrics are the oldest form of identification' (Schneier 2000, p.141). They are best defined as unique, measurable *physiological* and/or *behavioural* characteristics which can be digitised and stored with the user's id in the system database and thereby utilised to verify the identity of an individual (Ashbourn 1999, von Solms et al 2002, p.30). Liu and Silverman

(2001, p.27) wrote that a biometric was `the most secure and convenient authentication tool'. Physical examples are: fingerprints, palm prints, hand geometry, facial recognition, retina and iris characteristics. Behavioural examples include: signature verification, voice patterns, key stroke analysis. There is an eight-step process involved in the operation of a biometric system:

1. Capture the biometric
2. Process the biometric, extract and enrol the biometric template
3. Store the template in either a fixed or mobile repository (e.g. smart card)
4. Live-scan the biometric
5. Process the biometric and extract the biometric template
6. Match scanned and stored biometric templates
7. Provide a matching score to business applications
8. Record secure audit trail with respect to system use.

Liu and Silverman (2001, p.30) noted that, although there were many hardware and software vendors, standards were emerging. In terms of e-commerce applications, developers were looking at using biometrics and smart cards to verify user identity.

Marshall (2000, p.5) reported that a provider of biometric identification solutions could provide smart card users with a `method of securing access to multiple forms of information at a level much higher than that of a simple PIN code. By providing a combination of a PIN code and voice, face and/or fingerprints users would be protected from unauthorised individuals and personal data on the card would be secure'.

The following year it was reported that biometrics were being used to keep track of criminals out on parole, who were authenticated by the telephone number from which they called in and identified by their voice, a sample of which was kept on file. The technology involved used `algorithms to filter out noise and could be used via a mobile handset or on a PC'. The supplier deemed that `voice verification technology was the natural thing to use in M-commerce' (Computer Fraud and Security, July 2001, p.4).

Schneier (2000, pp.144-145) was of the opinion that biometrics worked well only if the verifier could confirm two items: first, that the biometric came from the user at the *time* of verification and, secondly, that the biometric supplied *matched* the record held on file. If the system could not achieve both, then it was insecure.

2.2.3 Access Tokens

`A physical token serves to authenticate the holder of it', but the most serious problem with such an item is the risk of theft as the system authenticates the token (by retrieving the username from it) rather than the holder. As a result, it is common practice for the system to require a password or PIN (personal identification number) in addition to the token, the PIN being memorised by the user (Schneier 2000, pp.145-147).

Examples of access tokens are magnetic cards, memory cards, smart cards and hand-held password generators (von Solms et al 2002, p.28). Smart cards can be secure and in such cases it is possible to store both the user id and the password on the card, but many access tokens are insecure and in that situation it is necessary for the user to keep the password elsewhere.

3. Identification and Authentication in Practice

Baker (1999) notes that `when our personal financial information is available on a network, we certainly want that information to be protected by strong authentication so that only we – and authorized bank officials – can access it.' This section therefore takes the first authentication measure, passwords, and looks at how these are applied in practice by some South African online financial services.

3.1 Mercantile Bank

Access to Mercantile's online banking service (Bankability) requires a profile number, user name and password. The system is *atypical* in that it is not browser-based. All information communicated between the user's PC and Mercantile's system is both encrypted and authenticated. An advanced password system, based upon a patented technique, is used to ensure that only the client can access his accounts. This technique ensures that the password is never communicated across the network, never stored in the user's PC and never known or stored at Mercantile Bank.

The client chooses his own password and can change it at his discretion. As long as the client keeps his password secret, only he can authorise access to, and perform transactions against, his accounts via Bankability. The system provides users with an option to input the password with the mouse rather than the keyboard. When using the mouse the keyboard is displayed on screen and the characters can be selected from the screen. Mercantile

recommends that its customers use the mouse option for entering their passwords for greater security.

Following a television expose of poor security in browser-based electronic banking applications, Mercantile tightened the log-on procedure for Bankability.Lite (a restricted, browser-based service, available to customers wishing to access their accounts from an Internet Café or from overseas) by incorporating a security step from its telephone banking system, Telability. To log on to Bankability.Lite a client must now not only enter his profile number, user name and password, but also his Telability card number together with one of 60 six-digit log-on codes provided on the Telability card. The system will request a different log-on code each time the system is accessed. Mercantile claims this makes Bankability.Lite more secure than other South African online banking systems (Botha, 2002).

3.2 Nedbank

Nedbank originally required online users to log on with a profile number allocated by the bank and a 4-digit PIN selected by the customer. When the service was re-launched in 2001 the system also required the user to create a third item, a password composed by the user. Further security measures adopted by Nedbank are the termination of an online banking session after a user's PC is left unattended for more than eight minutes and cancellation of a PIN or password if either is repeatedly entered incorrectly three times (Nedbank, 2002b).

3.3 Standard Bank

Standard Bank (2002) recently e-mailed its online clients advising the incorporation of a new feature, which increases the security of the Internet login. Since 5 February 2002 users were asked to create a case-sensitive password within the following parameters: any letter or number or combination thereof, subject to a maximum of 16 characters and a minimum of 6. The e-mail gave the following password example: `Stev493Safe'.

3.4 Tradek.com

Tradek.com is an online stockbroker also offering limited banking facilities. Although clients can issue high value stockbroking orders online and transfer funds between Tradek-linked accounts, funds will only be transferred by Tradek externally into a client pre-designated bank account. As a result, Tradek considers that it does not require as high a level of security as that used by online banks (Theron and Naryshkine, 2002). To gain access to a Tradek account a client need only enter a user id (allocated

by Tradek) and a password. The default password issued by Tradek is the client's e-mail address, but the client can change this to one of his own choosing.

Tradek previously allowed clients to access multiple, linked stockbroking accounts in one session, using the same user id and password. However, following its launch of online banking services, security was tightened in October 2001 and clients had to log on separately to each stockbroking account using the latter's unique user id and password (Naryshkine, 2001).

4. Conclusion

Information, computer and Internet security are paradoxical. There is a desire to maximise the openness of the Internet and to make transacting as simple as possible, yet too much ease of use can cause security problems. Access control, which includes user identification and authentication, is a vital pre-requisite to information security.

Identification can be equated to a username and is used by a system to ensure that the user is allowed access. As usernames can be lost or stolen, it is necessary to validate that the intended user is really the person he claims to be – the authentication process. There are three main authentication measures: passwords (something known by the user), access tokens (an item in the user's possession) and biometrics (biological data pertaining to the user, such as a fingerprint, which can be digitally captured).

Authentication measures are also paradoxical. Users prefer easy-to-remember passwords, but these can be discovered by dictionary attacks by unauthorised users. If complex passwords are used, they are difficult to memorise and a hard copy can be stolen. Access tokens may be a more secure user id and can contain a secure password or PIN, but are also subject to loss or other abuse. Biometrics are probably the most tamper-proof form of authentication, but more expensive equipment is required to handle them.

Security is a trade-off, first, between the ease of use of a system and the need to protect the data it contains and, secondly, between the cost of its implementation and the value of what can be lost if security is

breached. No system is ever 100 percent secure. The objective is always to implement all reasonable, cost-effective security measures, but more important is to inculcate a strong security ethos in the *people* involved with the system, both externally and internally (Schneier, 2000).

In practice, this means (a) educating clients in the use of strong, more secure passwords and the need both to keep them secret and to change them from time to time and (b) either storing usernames and passwords (or other authentication measures) in an *encrypted* form in the system database or severely restricting staff access to the system database if identification and authentication data are stored in clear text.

Although the South African companies identified in this study are not currently using biometrics for applications such as ATM, the literature suggests that, overseas at least, the use of biometrics as authentication measures is increasing in scope, encouraged by the development of new technologies and less costly equipment. Some financial institutions have been experimenting with biometrics for several years. Standard Bank was using fingerprint verification on DieBold ATMs, but as reliability was an issue, it was terminated. They are currently researching other biometric solutions. The interim results of this work will not be declared unless an institution is poised to use a biometric technique. Kausch (2001) reports that companies such as Aplitec are making significant use of smart card payment systems in southern Africa and this could form the basis of further study as to their effectiveness in the field of user identification and authentication.

References

Ashbourn, J. (1999) `The Biometric White Paper', available at http://homepage.ntlworld.com/avanti/whitepaper.htm accessed 22 January 2002

Ashbourn, J. (2000) `The Distinction Between Authentication and Identification', available at http://homepage.ntlworld.com/avanti/authenticate.htm accessed 22 January 2002

Baker, S.A. (1999) `Privacy, Anonymity and the Attack on Authentication Technologies' available at http://www.itsecurity.com/papers/baker.htm accessed 20 January 2002

Botha, D. (2002) Personal Interview with Devilliers Botha, Technical Business Development Officer of Mercantile Bank's Electronic Banking Division, held in Johannesburg on 22 January 2002

Bothma, C.H. (2000) *`E-Commerce for South African Managers',* Interactive Reality, Irene

Computer Fraud and Security (2001) `Biometrics used as correction tool', July, p.4

Ghosh, A. K. (1998) *`E-Commerce Security –Weak Links, Best Defenses',* John Wiley & Sons, New York

Gollmann, D. (1999) *`Computer Security',* John Wiley & Sons, Chichester

Kausch, B. (2001) `Malawi uses fingerprint ID for new national card' available at www.aplitec.co.za/aplitec/releases/ITWEB_22_11_01.htm accessed 20 January 2002

Jarvis, N. (1999) `E-commerce and Encryption: Barriers to Growth' available at http://www.itsecurity.com/papers/p36.htm accessed 20 January 2002

Liu, S. and Silverman, M. (2001) `A Practical Guide to Biometric Security Technology', *IT Pro,* January/February, pp.27-32

Marshall, E. (2000) `Biometrics secures Sun's Java Card', *Computer Fraud and Security.* June, p.5

Mason, S. (1999) `Electronic Signatures in the EU and world e-commerce: technical and legal ramifications' available at http://www.itsecurity.com/papers/digsig.htm accessed 20 January 2002

Microsoft (2002) `Safe Internet: Microsoft Privacy and Security Fundamentals – Best Practices Checklist', available at *www.microsoft.com/privacy/safeinternet/security/best_practices/passwords.htm* accessed 21 January 2002

Naryshkine, A. (2001) `Linked Accounts' e-mail to clients from Tradek.com Webmaster, 17 October

Nedbank (2002a) `Encryption', available at *www.nedbank.co.za/content/youtheindividual/electronic/internet/Encryption.asp* accessed 20 January 2002

Nedbank (2002b) `User Authentication', available at *www.nedbank.co.za/content/youtheindividual/electronic/internet/User.asp* accessed 20 January 2002

Netbank (2002) `Change PIN', available at *https://netbank.nedsecure.co.za/CustPswdMod.asp* accessed 20 January 2002

Schneier, B (2000) *`Secrets and Lies: Digital Security in a Networked World',* John Wiley & Sons, New York.

Standard Bank (2002) `Introducing additional security features for your peace of mind', e-mail sent to Standard Bank clients in January 2002; further information is stated to be available at *https://www.encrypt.standardbank.co.za/jb2/* but author unable to access

Theron, P.R. and Naryshkine, A. (2002) Personal Interview with Paul Theron, Chief Executive, and Sasha Naryshkine, Webmaster, of Tradek.com, held in Johannesburg on 22 January 2002

von Solms, S.H., Eloff, J.H.P., Eloff, M. and Smith, E. (2002) *`Information Security',* Draft book to be published