available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Electronic signatures and security issues: An empirical study

A. Srivastava

Department of Business Law and Taxation, Faculty of Business & Economics, Monash University, Australia

Keywords:
Electronic signatures
Digital signatures
Biometrics
Electronic signature security
Password security
Hard disk security
Smart cards
Portable information storage devices

ABSTRACT

Security concerns with regard to the use of electronic signatures in the electronic environment seem to represent a potential barrier to their usage. This paper presents an empirical study that examines businesses' perceived security concerns with the use of the electronic signature technology for executing contracts and commercial transactions and whether such issues represent a disincentive for their usage. The findings of the study reveal that there are significant security concerns in the business community with regard to the use of electronic signatures. However, such perceptions seem to be primarily driven by a lack of awareness and understanding. Advising prospective users of electronic signatures about the kind of safeguards that could be put in place to minimise risks associated with their usage can be a useful step towards overcoming their fears and hesitance.

1. Introduction

Merriam-Webster online dictionary defines security as the quality or state of being secure; freedom from danger; and freedom from fear or anxiety.[1] In the context of electronic signatures,[2] there is always a danger, fear or anxiety regarding their unauthorised or malicious use. The protection from such unauthorised and malicious usage requires some process, device or mechanism that ensures the confidentiality of electronic signatures. In particular, electronic signatures are secured in these three basic ways: through the use of passwords where an electronic signature is stored on the hard disk of a computer; using portable information storage devices (PISDs); and using biometric devices. The underlying theoretical underpinning for these three methods of securing electronic signatures relates to the three ways of authenticating a user: by something he knows, by something he has, and by something he is.[3] Furthermore, since the Internet is an essential tool for the transmission of electronic signatures, a secure transmission process where a document signed through an electronic signature is not tampered with by a third person and reaches the recipient in the form in which it left the signatory, is also required.

However, the above security measures present certain challenges. In particular, security issues with the private key of a digital signature[4] – the most well-known form of

[1] *Merriam-Webster's Online Dictionary* (2008) Merriam-Webster <http://www.merriamwebster.com/dictionary/security>; at 2 June 2008.

[2] '"Electronic signature" is defined as data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message'. See UNCITRAL *Model Law on Electronic Signatures 2001* art 2(a).

[3] Steven Furnell. An Assessment of Website Password Practices. *Computers & Security* 2007;26(7):445, 445; Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (2003) 186.

[4] Digital signature is a type of electronic signature which is 'created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form'. See UNCITRAL, *Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures* (2001) [36] <http://www.uncitral.org/pdf/english/texts/electcom/mlelecsig-e.pdf>; at 5 August 2007.

0267-3649/$ – see front matter © 2009 A. Srivastava. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2009.05.007

electronic signature[5] – have been widely debated in the literature. Scholars argue that passwords or pass phrases are not an adequate method of protecting a private key.[6] People often choose passwords that are easy to guess,[7] or omit to change password at regular intervals unless forced to do so, making a private key secured behind such passwords prone to attack.[8]

A few studies have also explored the use of smart cards for storing a private key. However, there has been mixed opinions in favour of smart card usage. Many scholars believe that the use of portable information storage devices (PISDs) such as smart card is a secure option for the storage of a private key.[9] Myers notes that with the usage of smart cards or cryptographic tokens the private key never resides in the computer's memory and therefore an unauthorised user will not be able to retrieve it even if he or she gains access to the subscriber's computer.[10] On the other hand, some scholars argue that storing a private key on a smart card is insecure because the latter can easily be stolen.[11]

In contrast, biometrics is considered as the most favourable option for securing a private key.[12] Bharvada argues that although smart cards can be lost or stolen, and passwords and PINs can be forgotten or tampered with, biometrics is not susceptible to such concerns.[13] She remarks that as biometrics becomes cheaper, powerful and more convenient to use, the way ahead could be a combination of biometrics and private key.[14] Julia-Barceló and Vinje consider smart cards enhanced with biometrics as a more desirable option for reducing risk associated with the loss and theft of key pairs.[15] However, Biddle remarks that the usage of smart cards particularly those further secured with biometrics to protect a private key, is only a wishful thinking as these technologies are neither commercially deployed currently nor will they be in the foreseeable future.[16]

Conversely, some studies have pointed out that none of the above-mentioned methods used to protect a private key – password, smart card or biometrics – could be secure enough. Bohm, Brown and Gladman argue that 'neither PCs [personal computers], nor smart cards, biometrics nor any methods currently available or likely to be available in the near future can enable a user to keep his signature key secure'.[17] A few studies have discussed the human and institutional risks associated with the use of digital signatures.[18] Technologies such as digital signature can only provide computer to computer security but 'there will still be human security problems of people using someone else's computer or computer account improperly'.[19] There is also human frailty involved in the sense that many people know how to avoid losing credit cards and door keys but they still lose them.[20]

Against the above background this empirical study uses a qualitative methodology to examine businesses' perceived security concerns with regard to the use of electronic signatures, in particular digital signatures for contracts and commercial transactions and whether such issues represent a disincentive for their usage.[21]

The study is based on a sample comprising 17 large public-listed Australian companies. Participants entailed elite staff from legal department, information technology (IT) department and Senior Management (SM). Semi-structured

[5] Note that worldwide many governments have promoted the use of digital signatures. Yet, PIN and name typed at the bottom of the e-mail are the more widely used forms of electronic signature. See Stephen Mason, Electronic Signatures in Law (2nd ed, 2007) 1.

[6] See Stephen G Myers, 'Potential Liability under the Illinois Electronic Commerce Security Act: Is it a Risk Worth Taking?' (1999) 17(3) *The John Marshall Journal of Computer & Information Law* 909, 941; Don Davis, 'Compliance Defects in Public-key Cryptography' (Paper presented at the 6th Conference on USENIX Security Symposium, Focusing on Applications of Cryptography, San Jose, California, 22–25 July 1996) 17.

[7] Stephen Mason and Nicholas Bohm, 'The Signature in Electronic Conveyancing: An Unresolved Issue?' (2003) *The Conveyancer and Property Lawyer* 460, 465; Davis, above n 6.

[8] Mason and Bohm, above n 7, 465–466.

[9] Julia-Barceló R, Vinje T. Towards a European Framework for Digital Signatures and Encryption. *Computer Law & Security Report* 1998;14(2):79, 82; William Kuechler, Fritz H Grupe. Digital signatures: a business view. *Information Systems Management* 2003;20(1):19, 28; Myers, above n above n 6, 941.

[10] Myers, above n 6, 941.

[11] Jueneman RR, Robertson Jr. RJ. Biometrics and Digital Signatures in Electronic Commerce. *Jurimetrics* 1998;38(3):427, 428; Davis, above n 6.

[12] Kamini Bharvada. Electronic Signatures, Biometrics and PKI in the UK. *International Review of Law, Computers & Technology* 2002;16(3):265; R Julia-Barceló, T Vinje. Towards a European Framework for Digital Signatures and Encryption. *Computer Law & Security Report* 1998;14(2):79, 8282; Myers, above n 6, 941.

[13] Bharvada, above n 12, 269.

[14] Bharvada, above n 12, 274.

[15] Julia-Barceló and Vinje, above n 12, 82.

[16] Bradford C Biddle, 'Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Market Place' (1997) 34 *San Diego Law Review* 1225, 1235.

[17] Nicholas Bohm, Ian Brown and Brian Gladman, 'Electronic Commerce: Who Carries the Risk of Fraud' (2000) 3 *Journal of Information, Law and Technology* [13] <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm>; at 29 January 2006.

[18] See William A Hodkowski, 'The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law' (1997) 13(1) *Computer and High Technology Law Journal* 217; Bohm, Brown and Gladman, above n 17, Jueneman and Robertson Jr., above n 11.

[19] Hodkowski, above n, 273.

[20] Bohm, Brown and Gladman, above n 17, 465.

[21] Note that this article is part of a comprehensive research project that investigated the various factors impeding the use of electronic signature amongst large Australian businesses. Security issues with the use of the electronic signature technology were identified as one of the major factors. Other concerns raised were legal understanding and issues with the use of the technology; the cost of using the technology; the complexity associated with its setting up and usage; the prevailing culture and customs associated with manuscript signatures; and ignorance about the technology.