first monday
PEER-REVIEWED JOURNAL ON THE INTERNET

Non-Repudiation in the Digital Environment

by Adrian McCullagh and William Caelli

Contents

Introduction

> "The times they are a changin'
> Bob Dylan

The investment community in many instances has traditionally relied heavily on face-to-face communications. With the advent of new digital signature technology, face-to-face communication as a manner of doing business will, in the not too distant future, become the exception rather than the norm. The tyranny of distance will be overcome, enhancing the efficiencies of business.

Electronic commerce is affecting all industries. The investment and finance communities have increasingly become dependent on technology for their survival, thanks to a variety of cost savings. Therefore it is not surprising that the banking, securities, and insurance industries have each in recent times taken specific interest in electronic commerce and the benefits that may be available to them individually and cross sectionally.

Fundamentally, electronic commerce involves the use of remote communications and therefore necessitates all parties involved to authenticate one another [1]. One of the primary technologies proposed for authentication is digital signature technology, which some commentators have noted will provide the investment and finance communities with substantial cost efficiencies [2]. A further claimed advantage of digital signature technology concerns the issue of "non-repudiation" claimed by the relying party against the alleged signer of an electronic document [3].

What does the term "non-repudiation" really mean? This paper will deal with inconsistencies that have arisen between legal and crypto meanings of "non-repudiation". In so doing this paper addresses the following issues:

- the legal meaning of "non-repudiation";
- the crypto meaning of "non-repudiation";
- the UNCITRAL Model Law and the onus of proof issue under Article 13;
- the technical vulnerabilities in adopting Article 13; and,
- Trusted systems as a basis to support the Common Law position.

This paper will show that lawmakers around the world are confused by these definitions and are in turn creating fundamental and major problems by not addressing the issue of "trust" at the signer's end of electronic communication within the electronic commerce environment.

Traditional Legal Meaning of "Non-Repudiation"

There is a definitional distinction between the legal use of the term "non-repudiation" and its crypto-technical use. In the legal sense an alleged signatory to a document is always able to repudiate a signature that has been attributed to him or her [4]. The basis for a repudiation of a traditional signature may include:

- The signature is a forgery;
- The signature is not a forgery, but was obtained via:
    - Unconscionable conduct by a party to a transaction [5];
    - Fraud instigated by a third party [6];
    - Undue influence exerted by a third party [7].

There appears to be a movement within the electronic commerce environment to take away these fundamental rights that exist within common law jurisdictions [8]. The general rule of evidence is that if a person denies a particular signature then it falls upon the relying party to prove that the signature is truly that of the person denying it [9]. It should be understood that the term "deny" and the term "repudiate" are synonymous and this position is supported by standard dictionary definitions [10].

Furthermore, the common law trust mechanism established to overcome a false claim of non-repudiation is witnessing [11]. Witnessing simply occurs at the time the signature is being affixed. That is, by having an independent adult witness the signing of a document reduces the ability of the signatory to successfully deny the signature as a forgery at a later date. It is always open for the signatory to deny the signature on other grounds such as those enumerated above.

The issue that arises is whether a digital signature should be treated differently to that of a traditional signature. It is submitted that the law should not in the electronic commerce environment alter this position as regards to the legal rights of parties to repudiate a digital signature [12]. Governments' worldwide have consistently espoused this position [13]. The electronic commerce environment should not have different rules from those developed over many centuries in the paper-based environment. These rules have been developed and judicially tested so as not to disadvantage any party in a transaction.

Should a digital signature
should be treated differently
from a traditional signature?

There is a clear contradictory position between the technical meaning and the legal meaning of the term "non-repudiation" where there is a clear case of forgery as regards to an alleged digital signature.

In the traditional legal sense, the onus of proof in a case involving a forged paper-based signature lies upon the party wishing to rely upon the signature. The relying party in relation to an alleged forged signature is required to establish:

- In a civil action, on the balance of probabilities; and,
- In a criminal action, beyond reasonable doubt,

that the signature is not a forgery.

If the alleged signatory disputes the signature as belonging to him or her then the onus falls upon the relying party to prove that the signature is in fact that of the alleged signatory.

Crypto-Technical Meaning of "Non-Repudiation"

In general terms, the term "non-repudiation" crypto-technically means:

- In authentication, a service that *provides proof of the integrity and origin of data*, both in an *unforgeable relationship*, which can be verified by any third party at any time; or,
- In authentication, an authentication that with high assurance can be asserted to be genuine, and *that can not subsequently be refuted*. (Emphasis added) [14]

The term "refuted" according to the *Shorter Oxford Dictionary* also means among other things "deny". In 1998, the Australian Federal Government's Electronic Commerce Expert Group adopted a technical meaning in its report to the Australian Federal Attorney General, by defining "Non-repudiation" as follows:

> Non-repudiation is a property achieved through cryptographic methods *which prevents an individual or entity from denying having performed a particular action related to data* (such as mechanisms for non-rejection or authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).(Emphasis added) [15]

It is this denial of the right of being able to repudiate [16] a digital signature that causes great concern and is resulting in a misinterpretation of its use within digital signature regimes. Additionally, the draft standard for *Guidelines for the Use and Management of Trusted Third Party Services* that has been promulgated by the International Organisation for Standardisation (ISO) as regards to non-repudiation services [17] provides that:

> TTPs may be involved in the provision of non-repudiation services, depending on the mechanisms used and the non-repudiation policy in force. The purpose of non-repudiation, in conformance with ISO/IEC 13888-1, -2 and -3, is to provide verifiable proof or evidence recording of data, based on cryptographic check values generated by using symmetric or asymmetric cryptographic techniques, of:
>
> - *Approval*
>   Non-repudiation of approval service provides proof of whom is

responsible for approval of the content of a message;
- *Sending*
  Non-repudiation of sending service provides proof of who sent a message;
- *Origin*
  Non-repudiation of origin service is a combination of approval and sending services;
- *Submission*
  Non-repudiation of submission service provides proof that a delivery authority has accepted a message for transmission;
- *Transport*
  Non-repudiation of transport service provides proof for the message originator that a delivery authority has given the message to the intended recipient;
- *Receipt*
  Non-repudiation of receipt service provides proof that the recipient received a message;
- *Knowledge*
  Non-repudiation of knowledge service provides proof that the recipient recognised the content of a received message; and,
- *Delivery*
  Non-repudiation of delivery service is a combination of receipt and knowledge services as it provides proof that the recipient received and recognised the content of a message.

In the electronic commerce environment, the technical meaning of the term "non-repudiation" either shifts the onus of proof from the recipient to the alleged signatory or entirely denies the signatory the right to repudiate a digital signature. That is, if a digital signature is verified so as to identify the owner of the private key that was used to create the digital signature in question then it is that person who has the onus of proving that it is not their digital signature. Hence, there is a shift in the burden of proof. This crypto-technical position does not correspond with what occurs in the paper-based environment.

Some commentators have gone so far as to advocate that if the digital signature is verified then the owner of the private key is prevented from repudiating the digital signature. This is clearly the position taken in the second meaning above of the term.

This technical meaning of non-repudiation is wrong as it does not take account the possibility of private key theft or illicit usage, essentially a form of identity theft. Furthermore, the technical meaning relates to post-signature events and not to the actual signing mechanism. That is, the traditional concept of witnessing the affixation of a traditional signature reduces the incidence of forged signatures. One of the primary roles of the TTP is to establish a repository of digital certificates that embody the public keys that corresponds to private keys used for digital signatures. These certificates are used to verify that the digital signatures - effected using private keys - correspond to the public keys embodied in the digital certificates. Its usage does not relate to the signing process in any way.

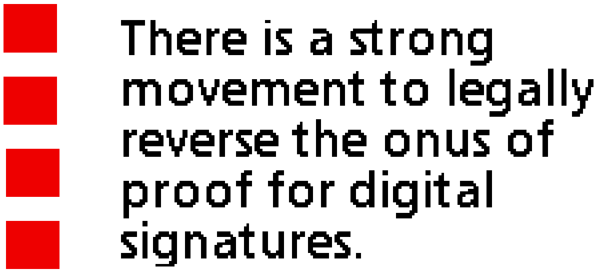
A further complicating factor is that RFC 2459 [1] specifies a bit within the KeyUsage extension called the Nonrepudiation bit. This bit is "asserted when the subject public key is used to verify digital signatures used to provide a non-repudiation service which protects against the signing entity falsely denying some action, excluding certificate or CRL signing". It is difficult to accept that the use of a single bit within an extension of a digital certificate can sufficiently attribute non-repudiation. The verification of a digital signature does not logically prove that the alleged signatory actually affixed the digital signature. The verification process only establishes that the private key of the person whose public key is specified in the digital certificate [18] was used to affix the digital signature. This verification process is a post-signing mechanism and does not correspond to the trusted witnessing mechanism established within the traditional signature environment [19].

This confusion in the technical community of the term non-repudiation is in turn confusing policy makers. This confusion extends to the role and use of the entity known as a "Trusted Third Party" as this party does not participate in the signing process. This confusion is best illustrated by the position taken by the drafters of the UNCITRAL Model Law.

UNCITRAL Model Law: Article 13

There is a strong movement to legally reverse the onus of proof for digital signatures [20]. The position being promoted is for the alleged signatory to have the onus of proof in establishing that he or she did not digitally sign a given document.

Legally there are only a few examples where a defendant has, from the commencement of an action, the onus of proof. In taxation cases, it is common for the onus of proof to lie with the taxpayer. After all, it is the taxpayer who is claiming a particular position and, as such, is in a better position to disprove the revenue collecting body's case.



There is a strong movement to legally reverse the onus of proof for digital signatures.

Another example occurs when the plaintiff in a negligence action relies upon the legal maxim *res ipsa loquitur* [21].

In a negligence action, the plaintiff generally has the onus of proof in establishing that the defendant failed to meet the standard of care required by law. This onus of proof is in effect shifted in cases where the plaintiff is able to establish that the event would not have occurred but for the negligence on the part of the defendant.

In such cases, it is for the defendant to tender such evidence as to disprove negligence. Hence, there is a shifting of burden of proof.

It has been proposed for the electronic commerce environment in the UNCITRAL Electronic Commerce Model Law, Article 13 that the onus of proof should lie upon the alleged signatory to show that the digital signature is a forgery. This is contrary to the position in the paper-based world.

In summary, the three positions are:

- Electronic Commerce Environment (Article 13 Model Law)
  Onus of proof is upon the signatory to prove that the digital signature is a forgery.

- Electronic Commerce Environment (Section 15 of the Electronic Transactions Act (CWTH) 1999) [22]

  The ECEG in its 1998 report specifically rejected Article 13, as the electronic commerce environment should not be different from the paper-based environment. Section 15 provides that a person purporting to be the originator of an electronic communication will only be bound by the electronic communication if in fact the electronic communication was sent by that person with their authority. This position corresponds to the common law position and as such the onus of proof will lie with the relying party.

- Paper-Based Environment
  Onus of proof is upon the relying party to prove that the signature is not a forgery.

In the paper-based environment there exists an absolute trusted system because the signatory is placed in the position of total control over the signing mechanism and the signatory does not have to rely on any external information or belief in order to affix his or her signature. The same is not true in the electronic commerce environment because the signatory has to rely on the signing mechanism to affix a digital signature only on the intended document.

Technical Vulnerabilities of Article 13 and the Common Law Position

Both the Common Law position and the Article 13 position are not sustainable unless the signing mechanism is effected in a trusted environment. In 1984, Thompson showed that mobile code was a major problem and that it was relatively easy to develop [23].

Concern about mobile code is increasing and will become an even greater problem with the increased deployment of ADSL cable modem technologies [24]. With ADSL, the general public can be permanently connected to the Internet. This will result in:

- computers will have a permanent IP address instead of being allocated a dynamic IP address each time a connection to the Internet is made. Having a permanent IP address increases the vulnerability to attacks by hackers because it increases the opportunities for a hacker to attack. A dynamic IP address reduces this window of opportunity; and,
- computers that are not located behind firewalls are exposed [25].

Unfortunately, there does not appear to be any trustworthy filtering technology commercially available that can reside on personal computers. One of the more prevalent attacks in recent years has been the use of mobile code, such as trojan horses, to operate covertly on computer systems.

It is not difficult to imagine a virus or trojan horse that is designed to steal private keys. This is particularly easy if the private key is stored in a commonly known file, such as "PGPPrivateKeyRing". The virus could be a Visual Basic macro that is attached to Microsoft Word documents. Its function could be to search storage devices for the PGP secret key ring. Once located, the program could then FTP the private key to a remote locality [26]. This program could perform its functions without the knowledge of the computer's owner; it could turn off certain display functions so that no dialogue boxes would be displayed. On completion of the transfer the rogue program could check the address book on the target computer and send a Word document with itself attached to five other unsuspecting victims. Finally the program could destroy itself and in the process delete any relevant entries in the sent mail folder. Such a program obviously would be a clear violation of a properly formulated security policy. For example, if object/activity labeling security mechanism paradigm was implemented then the program would not be capable of performing its functions since the intruding program would not be recognised by the security kernel as a valid subject, a valid object, or a valid activity [27].

Shamir and Van Someren [28] have proposed a mobile code attack that is known as the lunchtime attack. This strategy involves the efficient searching for RSA cryptographic keys in large amounts of data that may be stored on the hard drives of personal computers. The private key and the public key in the RSA crypto-system comprises:

Private key: e and n

Public key: d and n.

The modulus n forms vital part of the private key and the public key. Thus, if a hard-drive was searched for randomness and within any random section located a search was undertaken for a bit string that corresponds to n, then the private key may have been located. The efficiency of this attack is that the amount of data to be searched is greatly reduced.

It is not difficult to see that these attacks greatly hamper an alleged signatory where the Model Law is implemented within a legislative mechanism. How can an alleged signatory ever successfully deny that it was not him or her who signed the document? Under the Model Law position, the alleged signatory has the onus of proof in demonstrating that it was not him or her who signed the document.

In these sorts of attacks, how can a relying party - under the common law position - ever produce sufficient evidence to establish the identity of the alleged signatory who signed the document? Under common law, the relying party has the onus of proof in establishing that the alleged signatory did in fact affix that signature. The common law position was developed in a paper-based environment where witnessing was the trusted mechanism to prevent non-repudiation of a signature. With this trusted mechanism it was reasonable for the onus of proof to lie upon the relying party to show that the alleged signatory did in fact sign the document.

Without the implementation of trusted signing mechanisms it does not matter which position is adopted. Neither position (model law or common Law) adequately provides a solution.

Trusted Computing Systems

A trusted computing system performs in accordance with its documented specification and will prevent any unauthorised activity. Specifically a trusted computing system can be relied upon to enforce a documented security policy. Such systems are usually classified as providing either discretionary or mandatory security enforcement policies and functionality.

The role of trusted systems has for more than 30 years been identified as a proper mechanism to protect the correct functioning of a computer system.

Computer systems are continually under threat of attack not only by ackers but especially through the use of "mobile code". These attacks since the development and continued advancement of the Internet have substantially increased.

The origin of network security was first approached in the defence environment by the development of the U.S. "Rainbow Series" in the 1980's which advanced the proposition of computer system protection through the construction of a "Trusted Computing Base". The classification of trusted systems has recently been standardised internationally under the general term "Common Criteria" (ISO 15408).

In the U.S., it is now recognised that the National Information Infrastructure is critical to the entire social fabric of the U.S. economy. Such a realisation should not be U.S.-centric but rather be viewed from a global perspective. The development of the Global Information Infrastructure and its move from a purely defence and academic environment to a commercial one has been a primary impetus for the development of the "Common Criteria" as an international standard. But the "Common Criteria" only address the security of systems that have been designed and manufactured against known security risks.

The problem lies in the connection of many untrusted systems by what ever means the parties so select. COTS products have proliferated on the computing landscape and the pervasiveness of untrusted operating systems and allied software subsystems has virtually made it impossible for trust to be allocated to any transaction. In order to overcome this security flaw it is possible to implement highly trusted subsystems which may be reasonably and cost effectively incorporated in untrusted systems. An example of this is the untrusted cash register and the incorporation of a separate "pin pad" that is an integral part of the highly trusted EFTPOS system in Australia.

The only available legal position is for the digital signature mechanism to be affected via a trusted computing system. Such a base should be at least Bl (TCSEC)/E3(ITSEC)/ or even possibly B2(TCSEC)/E4(ITSEC) or their equivalent in the "Common Criteria".

While security functions and their reliability assessment are a basic requirement for ITSEC/TCSEC evaluation there is an even more fundamental need in relation to overall system reliability and thus trust. The original TCSEC described six fundamental requirements of any computer system that aims for a level of trustworthiness. These were:

a. *Security Policy:*
   There must be an explicit and well-defined security policy enforced by the system;
b. *Marking:*
   Access control labels must be associated with objects;
c. *Identification:*
   Individual subjects (users) must be identified;
d. *Accountability:*
   Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party;
e. *Assurance:*
   Computer system must contain hardware and software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces the security requirements; and,
f. *Continuous Protection:*
   The trusted mechanism enforcing these basic requirements must be continuously protected against tampering and unauthorised changes.

With these fundamental requirements in mind, ITSEC went further than TCSEC and separated security functions from their reliability and assessment. It defined seven evaluation levels to form a "trust hierarchy" in the reliable operation of the security features of an information system. Security functions were to be assessed or evaluated by human "evaluators" and as a result of that evaluation a simple measurement or tag was to be associated with the functions. The words used are important since they emphasize this building of trust by human users in overall information systems. The assurance levels are as follows:

E0
Inadequate assurance

E1
Informal description of architectural design of product/system exists:

- Functional testing used to confirm target is met.

E2, or E1 plus:

- Informal description of detailed design exists:
    - Evidence of functional testing to be evaluated
    - Configuration control system exists
    - Approved distribution process exists

E3, or E2 plus:

- Source code and/or schematics for hardware to be evaluated
- Evidence of testing of these must be evaluated

E4, or E3 plus:

- Underlying formal model of security policy supporting the security target exists; and,
- Security enforcing functions, architectural design, detailed design specified in semi-formal style

E5, or E4 plus:

- Close correspondence between detailed design and software source code/ engineering hardware design drawings.

E6, or E5 plus:

- Security enforcing functions and architectural design must be specified formally - consistent with formal model of security policy.

The use of a trusted system will solve the problem identified above as regards to mobile code and the theft of cryptographic keys. If the signing mechanism works with a trusted system at the level of at least E3 (which proves the functionality of the signing mechanism thus preventing unauthorised access to the private key), then the common law position can be maintained in the electronic commerce environment. E3 also provides that the source code is evaluated and thus it is possible to show that the signing mechanism will only perform the desired function - and no other. The implementation of these security features can be adequately assessed, ensuring that the private key has not been stolen. With these features it is reasonable for the common law position to be implemented and thus have a balance between the electronic commerce and paper-based environments.

Conclusion

This paper demonstrates that the deployment of a trusted computing system for digital signatures is the only secure option, resulting in a legal position where the onus of proof for the electronic environment is equivalent to the paper-based environment. If a trusted computing system is used to affect a digital signature, then and only then can the onus of proof lie with the recipient in the same manner that exits in the paper-based world. Without a trusted computing system, neither party - the signer or the recipient - is in a position to produce the necessary evidence to prove their respective case.

Hence the implementation of a trusted computing system will allow for a balance between the two environments. Therefore, no party will enjoy an advantage over another.

The issues raised in this paper are highly important to the investment and finance communities because they will provide the necessary confidence to encourage global trading opportunities. The issues raised in this paper need to be understood by the relevant policymakers in order to create the necessary balance between the traditional paper-based environment and the emerging global electronic commerce environment.

About the Authors

Adrian McCullagh, B.App.Sc (Computing) (Q.I.T), L.L.B.(Hons) (Q.I.T.), is National Director for Electronic Commerce, Gadens Lawyers, Brisbane, Australia and a Ph. D. Candidate at the Queensland University of Technology (QUT).
E-mail: AMcCullagh@exchange.gadens.com.au

Professor William Caelli, B.Sc.(Hons) (Newcastle), Ph.D. (ANU), is Head of the School of Data Communications at Queensland University of Technology (QUT) and formerly Director of the Information Security Research Center, QUT.

Notes

1. That is the parties will not at the time of transacting have face to face dialogue.

2. Bank for International Settlements, Report No. 35, "Risk Management for Electronic Banking and Electronic Money Activities" (March 1998); at http://www.bis.org/publ/index.htm, accessed on 15 December 1999.

See also "Communication from the Commission to the European Parliament - the Council, the Economic and Social Committee and the Committee of the Regions - 'Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures'" COM(1998)297final, 13.05.98.

3. "American Bar Association Guidelines for Digital Signatures," at http://www.abanet.org/scitech/ec/isc/dsgfree.html, accessed on 15 December 1999.

4. *L'Estrange v. Graucob* [1934] 2 K.B. 394. See also A. McCullagh, W. Caelli, and P. Little, "Electronic Signatures - Understand the Past to Develop the Future," 1998 UNSWLJ, accessed on 15 December 1999 at http://www.law.unsw.edu.au/unswlj/ecommerce/mccullagh.html

5. Unconscionable conduct rests upon the concept of inequality of bargaining power. The characteristics of the concept are:

(a) Unconscionable involves the obtaining, by one party to a transaction, of an unfair advantage against the better judgement of the other weaker party to the transaction;

(b) The dominant party knowing either actually or by imputation of the disadvantage;

(c) In many cases there is a striking disparity in the value of the consideration passing between the parties.

See M.L. Cope, "The Review of Unconscionable Bargains in Equity," (1983) 57 A.L.J. 279; *Commercial Bank of Australia v. Amadio* (1982-83) 151 C.L.R. 447.

6. Fraud involves any intentional conduct that has the purpose not necessarily the sole or dominant purpose of obtaining some gain from the party who is the subject of the fraudulent conduct. See *Earl of Aylesford v. Morris* (1873) 8 L.R. Ch. App. 484.

7. Undue influence involves a situation where a person has the ability to take control over another's independent will power so that the innocent person is not able to resist the actions of the first person. Such cases usually involve some disability as in *Blomley v Ryan* (1956) 99 C.L.R. 362. Mr. Ryan was a severe alcoholic and was never in a position to resist the actions of Mr. Bromley.

8. "UNCITRAL Model Law on Electronic Commerce with Guide to Enactment" Article 13, at http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm, accessed on 15 December 1999.

9. A. McCullagh, W. Caelli, and P. Little, "Electronic Signatures - Understand the Past to Develop the Future," 1998 UNSWLJ. Thematic Issue, at http://www.law.unsw.edu.au/unswlj/ecommerce/mccullagh.html, accessed on 15 December 1999.

10. Shorter Oxford Dictionary, D. Thompson, (Ed) 19th Edition, Clarendon Press, "Repudiate" 1 (a) disown, disavow, reject, (b) refuse dealings with, (c) *deny*.

11. *Ibid.*

12. The above position is the same in many jurisdictions.

13. Report of the Electronic Commerce Expert Group to the Attorney General, "Electronic Commerce: Building the Legal Framework - 31 March 1998", at http://law.gov.au/aghome/advisory/eceg/eceg.htm, accessed on 15 December 1999.

14. W. Caelli, D. Longley, and M. Shain, 1991. *Information Security Handbook.* London: Macmillan.

15. *Ibid.*

16. B. Schneier, 1996. *Applied cryptography: Protocols, algorithms and source code in C.* Second edition. New York: Wiley, p. 2.

17. R. Granito and A. Hovstø (editors). "Guidelines for the use and management of trusted third party services", JTC 1.27.19 (Working Draft).

18. One of the primary roles of a TTP is too reliably authenticate the identity of the holder of the key pair, of which the public key is embodied in the digital certificate.

19. The issue of witnessing the affixing of digital signatures is more fully explained in McCullagh et al., *ibid.*, note 9.

20. *Article 13. Attribution of data messages*

(1) A data message is that of the originator if it was sent by the originator itself.
(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:
(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or
(b) by an information system programmed by, or on behalf of, the originator to operate automatically.
(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:
(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.
(4) Paragraph (3) does not apply:
(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or
(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.
(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.
(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

21. *Lambos v. Commonwealth of Australia* (1967-68) 41 A.L.R. 180.

22.This position has also been accepted by the UK Government as promoted in the draft "Electronic Communications Act".

23. K. Thompson, 1990. "Reflections on Trusting Trust," In: P. Denning (editor). *Computers Under Attack: Intruders, Worms and Viruses.* Reading, Mass.: Addison-Wesley.

24. C. Serban, "Security Issues for 'Always on' Devices: ADSL and Cable Modem Access" AT&T 1999, unpublished copy of this paper was given to the authors and is in their possession.

25. *Ibid.*

26. The secret key ring in PGP is usually encrypted with a much simpler crypto-system. Also the key ring is subject to a pass phrase but this can usually be broken using one of the hacker programs available on the Internet such as cracker, Satan, or cops.

27. D.E. Bell and L.J. La Padula, 1976. "Secure Computer System: Unified Exposition

and Multics Interpretation," ESD-TR-75-306 (March), Mitre Corporation.

28. A. Shamir and N. Van Someren. "Playing hide and seek with stored keys," accessed on 15 December 1999, at at http://www.ncipher.com/products/files/papers/anguilla/keyhide2.pdf

Editorial history

Paper received 11 July 2000; accepted 19 July 2000.

Contents Index

Non-Repudiation in the Digital Environment by Adrian McCullagh and William Caelli
First Monday, volume 5, number 8 (August 2000),
URL: http://firstmonday.org/issues/issue5_8/mccullagh/index.html