A Certified E-Mail Protocol

Bruce Schneier
Counterpane Systems
schneier@counterpane.com

James Riordan
IBM Zurich Research Laboratory
rij@zurich.ibm.com

Abstract

Protocols to facilitate secure electronic delivery are necessary if the Internet is to achieve its true potential as a business communications tool. We present a protocol for secure e-mail that protects both the sender and the receiver, and can be implemented using current e-mail products and existing Internet infrastructure.

1 Introduction

Electronic mail, or e-mail, has become an essential communication tool for business. The ease of communicating over e-mail, as opposed to traditional tools such as physical mail, fax, or telephone, makes it the communications medium of choice for many people. As more people and businesses move on-line, and Internet access becomes more commonplace, e-mail will be used for even more communications.

In order for e-mail to be used for important communications, some notion of certified delivery must be provided for users. Not all e-mail needs to be certified. Just as in the physical world, conventional mail is sufficient for most communications, but some important communications needs to be sent via certified mail.

A certified e-mail protocol must have the following security properties:

1. Alice (the sender) must have some way of proving that Bob (the receiver) received the mail, should Bob later try to deny it.

2. Bob must have some way of proving that Alice did not send the mail, should Alice later try to claim that she did.

Certified paper mail uses the notion of a signed receipt. When Alice sends Bob certified mail, the Post Office will not release the mail to Bob unless he signs a receipt. This signed receipt is returned to Alice, and acts as a proof of delivery. If Alice does not have this receipt, Bob can claim that the certified mail was never sent. Here the Post Office is acting as a Trusted Third Party. Of course, this protocol only certifies that Alice sent Bob *some piece of mail* and not a particular piece of mail. This weak binding between the certification and the contents being certified is pervasive through all paper authentication protocols, and a problem that digital signature protocols solve easily.

In this paper we present a certified e-mail protocol that both satisfies all the security requirements of a protocol of this type, and is simple to implement and requires no specialized infrastructure. The rest of the paper is organized as follows. In Section 2 we describe previous work on certified delivery and related cryptographic problems. In Section 3 we describe our protocol and the message exchanges involved. In Section 4 we present a security analysis, and in Section 5 we describe the protocol's security properties. Section 6 discusses implementation details, in in Section 7 we offer some conclusions.

2 Previous Work

Several protocols for certifying electronic delivery have been proposed in the literature. The earliest

[Blu81, EGL85] use the notion of oblivious transfer [Kil90]: sending someone a message, with only a probabilistic guarantee of receipt. These protocols, while they have nice provable properties, are extremely computationally intensive and require many communications exchanges between the sender and receiver.

Many protocols, especially those implemented by companies attempting to make a business out of certified delivery, rely on trusted software to provide the security. Alice sends Bob an encrypted message via a certified-delivery software program, which will not allow Bob to read it until he sends Alice back a receipt. These protocols are susceptible to reverse-engineering and hacking, and cannot provide any real assurance of delivery.

Some protocols require a Trusted Third Party. The protocol in [BT94], for example, uses a trusted "Postmaster" to mediate between Alice and Bob. Aside from the logistical (and liability) problems of setting this Postmaster, the Postmaster needs to know the message Alice is sending to Bob. Alice cannot send a certified message to Bob without the Postmaster being able to read it. (Alice could always encrypt the message outside this protocol, but then all the Postmaster could certify is that Bob received an unintelligible bucket of bits.) Similar protocols appear in [Mic96, Mic97a, Mic97b].

Protocols requiring a Trusted Third Party are said to be optimistic [ASW97, ASW98] if the third party is only required in the exceptional case (e.g. one of the parties cannot or will not follow the protocol to its normal conclusion).

In all cases requiring a Trusted Third Party, it is highly desirable to minimize trust and complexity requirements on that third party.

Still other protocols ignore the problem of non-repudiation. The above protocol ends with the Postmaster sending Alice a certified receipt at the same time it sends Bob a key so that he can read the message, but no provisions are made for network transmission errors.

Another similar protocol [ZG96a, ZG96b], specifically does not try to solve the non-repudiation problem. ((more about this))

The system in [PA96] is similar in design.

3 The Protocol

Alice wishes to send Bob a certified message. Bob wants to receive a certified message. We need to build a protocol to facilitate this exchange. That is, we want to build a protocol to allow Alice to be able to prove to an arbiter that Bob has received her message if and only if he did receive it.

We assume that Bob has a public key [RSA78, ElG85] in some commonly recognized format (e.g. X.509 [CCITT89]), that there exists some public-key infrastructure (e.g. PKIX [**?**]) that Alice can use to verify the public key, that an arbiter can verify the key was valid at the time of the transaction using the public key infrastructure, and that there exists some timed stamped public forum whose contents are publically available (e.g. *The New York Times*, a World Wide Web kiosk service, or a Usenet newsgroup).

Let M be the message, K a key, E_K an encryption method using K and some standard symmetric cipher [NBS77, LMM91, Sch94], and H a message digest, or hash, function [NIST93, Riv95].[1]

1. Alice chooses a random key, K, and sends Bob the encrypted message $E_K(M)$.

2. Bob returns to Alice a digitally signed message with the form:

   I would like Alice to publish the key for the E_K- encrypted message, whose digest is $H(E_K(M))$, by date T at location X. — /s/ Bob

3. Alice publishes the pair $H(E_K(M)), K$ in X on or before date T.

4. Bob retrieves the key and decrypts the message.

If Alice is called upon to prove that Bob received the e-mail, she presents her copies of M, K, $E_K(M)$, and Bob's signed message from Step (2), along with the public record of her publishing them in Step (3) in accordance with Bob's request. The arbiter confirms that $E_K(M)$ is correct and conforms to what was

[1] Details on the cryptographic primitives used in this protocol, including symmetric cryptography, public-key cryptography, message digest functions, and public-key infrastructures, can be found in [Sti95, Sch96, MOV97].

published in Step (3), and also that the publication was in accordance to Bob's request in Step (2).

If Bob is called upon to prove that Alice did not send him the e-mail, he challenges Alice to present the body of evidence listed above. If she cannot, or if any of the evidence does not conform to the rules of the protocol (e.g. the pair $H(E_K(M)), K$ published in X in Step (3) does not match the $H(E_K(M))$ of the message Alice claims to have sent Bob), the arbiter has no choice but to believe Bob.

4 Analysis

The protocol is secure against cheating attempts by either Alice or Bob:

- If Bob refuses to comply in Step (2) or gives an unreasonable date or location, then he does not receive the key for the encrypted message and hence does not receive the message. This is conceptually equivalent of Bob's refusing certified mail at his doorstep.
- If Alice refuses to comply in Step (3) and claims that Bob has received the message when he has not, then Bob can show that Alice did not publish the key by calling upon the public records of location X. This is conceptually equivalent to Alice not sending the message but then claiming she had.
- If Bob refuses to comply with Step (4), then he loses because has claimed that he will comply in Step (2). This is conceptually equivalent of Bob's accepting and signing for the certified mail but refusing to open it.

5 Security Properties

The protocol has a few properties which are worth explicitly noting.

- The signed message of Step (2) must make clear how and when to retrieve the key and how to use it to decrypt the message. This prevents Bob from claiming that Alice has waited unduly in publishing the key while preventing Alice from publishing the key several months late in the East Podunk Quarterly for the message which was encrypted using AC5 (Alice's Code 5).
- Bob may wish to include with his message of Step (2) a description of what he expects from the contents of decrypted message. Doing so greatly reduces Alice's ability to deliver bogus information.
- So long as neither Alice nor Bob attempt to cheat, their identities need never be revealed to a third party. That is, this whole protocol could be conducted anonymously, through anonymous remailers [Sch95, TG96].
- This method does not offer privacy in that an eavesdropper has access to both $E_K(M)$ and K. If privacy is required, the exchanges at Steps (1) and (2) should be conducted using a method providing adequate privacy. There are several e-mail security protocols that could suffice: e.g., PGP [Zim95, Sch95, Gar95, Sch96], PEM [Lin93, Ken93, Bal93, Kal93, Sch95, Sch96], S/MIME [RSA96, Dus96], and others [SH97].
- Alice must retain a copy of T, K, and Bob's key request message for as long as she wishes to be able to prove receipt. This is conceptually equivalent to Alice keeping a copy of the certified-mail receipt.

6 Implementation

Unlike other certified-delivery protocols, the one presented in the paper can be implemented using the current Internet infrastructure. Any of the e-mail security programs mentioned above could be used to provide certified e-mail in this manner. While the integration of this protocol into secure e-mail clients would make it easier to use, it is not required.

A commercial certified-delivery service would necessarily have to combine the delivery protocol with some sort of payment protocol. The NetBill protocol [CTS95], for example, includes a certified- delivery mechanism as part of the protocol. The protocol presented in this paper could easily be augmented with a payment mechanism: a commercial entity could accept payment from Alice is exchange for providing a common public forum for Alice to use in Step (3).

The public kiosks of such commercial certified-delivery services are easily distributable; this stands in sharp contrast to several other schemes involving a third party which require Byzantine agreement [LSP82]. Different kiosks could included time stamped hashes of one anothers contents to improve security. An anonymous access method could be used to minimize trust requires placed upon the service.

Alternately, the protocol could be used in the absence of any commercial provider, simply by using the already-public Usenet newsgroups and a public archiving mechanism such as DejaNews.com.

Similarly, this protocol could be easily used within fair-exchange protocols [Blu81, Ket95, KG95, ASW97, ASW98] to certify delivery of information.

Finally, we note that if Alice has a reliable connection to the public channel, we can render the protocol optimistic [ASW97] by adding steps between 2 and 3:

- Alice gives Bob K directly
- Bob gives Alice a receipt for k

If Bob gives Alice the receipt for K, she need not publish as required by step 3 (thus reducing network traffic). If Bob fails to give Alice the receipt, Alice may continue with step 3.

7 Conclusions

We have presented a protocol allowing certified mail and an optimistic variation on that protocol. These protocols have the features of minimizing trust and complexity requirements on parties external to the two players. The minimization of trust results in greater security. The minimization of complexity results in resilience, ease of deployment, and the possibility of distributing the external party without difficulty.

8 Acknowledgments

References

[ASW97] N. Asokan , Matthias Schunter , and Michael Waidner, "Optimistic protocols for fair exchange", *ACM Computer and communications security*, 1997, pp. 7.

[ASW98] N. Asokan , Victor Shoup , and Michael Waidner, "Optimistic fair exchange of Digital Signatures", *Proceedings of Research in Security and Privacy, Oakland, CA*, May 1998, IEEE Computer Society Press.

[BT94] A. Bahreman and J.D. Tygar, "Certified Electronic Mail," *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, Internet Society, 1994, pp. 3–19.

[Bal93] D. Balenson, "Privacy Enhancement for Internet Electronic Mail: Part III—Algorithms, Modes, and Identifiers," RFC 1423, Feb 1993.

[Blu81] M. Blum, "Three applications of the oblivious transfer: Part I: Coin flipping by telephone; Part II: How to exchange secrets; Part III: How to send certified electronic mail," Department of EECS, University of California, Berkeley, CA, 1981.

[CCITT89] CCITT, Recommendation X.509, "The Directory–Authentication Framework," Consultation Committee, International Telephone and Telegraph, International Telecommunications Union, Geneva, 1989.

[CTS95] B. Cox, J.D. Tygar, and M. Sirbu, "NetBill Security and Transaction Protocol," *The First USENIX Workshop on Electronic Commerce*, USENIX Association, 1995, pp. 77–88.

[DGLW96] R.H. Deng, L. Gong, A.A. Lazar, and W. Wong, "Practical Protocols for Certified Electronic Mail," *Journal of Network and Systems Management*, v. 4 n. 3, 1996.

[Dus96] S. Dusse, "S/MIME Message Specification: PKCS Security Services for MIME," IETF Networking Group Internet Draft, Sep 1996.

[ElG85] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory,* V. IT-31, n. 4, 1985, pp. 469–472.

[EGL85] S. Even, O. Goldreich, and A. Lempel, "A Randomized Protocol for Signing Contracts," *Communications of the ACM*, v. 28, n. 6, Jun 1985, pp. 637–647.

[Gar95] S. Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly & Associates, 1995.

[Kal93] B.S. Kaliski, "Privacy Enhancement for Internet Electronic Mail: Part IV—Key Certificates and Related Services," RFC 1424, Feb 1993.

[Ken93] S.T Kent, "Privacy Enhancement for Internet Electronic Mail: Part II—Certificate Based Key Management," RFC 1422, Feb 1993.

[Ket95] S. Ketchpel, "Transaction Protection for Information Buyers and Sellers," in Proceedings of the Dartmouth Institute for Advanced Graduate Studies '95, 1995.

[KG95] S. Ketchpel and H. Garcia-Molina, "Making Trust Explicit in Distributed Commerce Transactions," Stanford Digital Library Project Working Paper SIDL-WP-1995-0018, October 12, 1995.

[Kil90] J. Kilian *Uses of Randomness in Algorithms and Protocols*, MIT Press, 1990.

[LMM91] X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," *Advances in Cryptology—CRYPTO '91*, Springer-Verlag, 1991, pp. 17–38.

[Lin93] J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I—Message Encipherment and Authentication Procedures," RFC 1421, Feb 1993.

[LSP82] L. Lamport, R. Shostak, and M. Pease "The Byzantine Generals Problem" *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, July 1982, pp. 382-401.

[Mic96] S. Micali, "Simultaneous electronic transactions with visible trusted parties," U.S. Patent 5,553,145, 3 Sep 1996.

[Mic97a] S. Micali, "Simultaneous electronic transactions with visible trusted parties," U.S. Patent 5,629,982, 13 May 1997.

[Mic97b] S. Micali, "Simultaneous electronic transactions," U.S. Patent 5,666,420, 9 Sep 1996.

[MOV97] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[Mue84] C Mueller-Scholer, "Method and apparatus providing registered mail features in an electronic communication system," U.S. Patent 4,458,109, 3 Jul 1984.

[NBS77] National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard," National Bureau of Standards, U.S. Department of Commerce, Jan 1977.

[NIST93] National Institute of Standards and Technology, NIST FIPS PUB 180, "Secure Hash Standard," U.S. Department of Commerce, May 1993.

[PA96] C.J. Petrie Jr. and W.P. Allen, "Electronic Proof of Receipt," U.S. Patent 5,509,071, 16 Apr 1996.

[PC93] D. Pinkas and P. Caille, "Method for obtaining a securitized cleartext attestation in a distributed data processing system environment," U.S Patent 5,214,700, 25 May 1993.

[Riv95] R.L. Rivest, "The RC5 Encryption Algorithm," *Fast Software Encryption, 2nd International Workshop Proceedings*, Springer-Verlag, 1995, pp. 86–96.

[RSA78] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, v. 21, n. 2, Feb 1978, pp. 120–126.

[RSA96] RSA Data Security, Inc., "S/MIME Implementation Guide Interoperability Profiles, Version 2," S/MIME Editor, Draft, Oct 1996.

[Sch94] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," *Fast Software Encryption, Cambridge Security Workshop Proceedings*, Springer-Verlag, 1994, pp. 191-204.

[Sch95] B. Schneier, *E-Mail Security,* John Wiley & Sons, 1995.

[Sch96] B. Schneier, *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996.

[SH97] B. Schneier and C. Hall "An Improved E-Mail Security Protocol," *Thirteenth Annual Computer Security Applications Conference*, IEEE Computer Society, 1997, pp. 227–230.

[Sti95] D. Stinson, *Cryptography Theory and Practice*, CRC Press, 1995, pp. 138–145.

[TG96] G. Tsudik and C. Gulcu, "Mixing E-Mail with BABEL," *ISOC Symposium on Network and Distributed System Security*, IEEE Computer Society Press, 1996, p. 2–16.

[ZG96a] J. Zhou and D. Gollman, "A Fair Non-Repudiation Protocol," *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, IEEE Press, 1996, pp. 55–61.

[ZG96b] J. Zhou and D. Gollmann "Certified Electronic Mail," *Computer Security — ESORICS '96 Proceedings*, Springer-Verlag, 1996, pp. 160–171.

[Zim95] P. Zimmermann, *The Official PGP User's Guide*, MIT Press, 1995.