Anonymous and Confidential Communications from an IP Addressless Computer

Carlos Molina–Jiménez* and Lindsay Marshall

Department of Computing Science, The University of Newcastle upon Tyne, U.K.
{Carlos.Molina, Lindsay.Marshall}@newcastle.ac.uk

Abstract. Anonymizers based on a mediating computer interposed between the sender and the receiver of an e–mail message have been used for several years by senders of e–mail messages who do not wish to disclose their identity to the receivers. In this model, the strength of the system to protect the identity of the sender depends on the ability and willingness of the mediator to keep the secret. In this paper, we propose a novel approach for sending truly anonymous messages over the Internet which does not depend on a third party. Our idea departs from the traditional approach by sending the anonymous messages from an Internet wireless and addressless computer, such as a Personal Digital Assistant (PDA) bridged to the Internet by a Mobile Support Station (MSS).

1 Introduction

The degree of anonymity offered by anonymizers based on mediating computers is limited since there is no way the sender can hide its IP address from the mediator. Trying to send an anonymous message from an IP addressed computer is analogous to trying to make an anonymous call from a home telephone line. To make a truly anonymous call, the caller must find a public telephone box and operate it by coins. Complete anonymity is guaranteed here by the use of a non–personal terminal (the public telephone box) and by the anonymous method of payment (the coins). With this in mind, we have developed a model to send truly anonymous messages based on the functionality of the public telephone box.

2 Addressless Connection with Anonymous Payment

A well–known approach to connecting wireless computers to the Internet is the model presented in Ioannidis et. al. [1], where an MSS identifies each wireless computer by its permanent IP address. In our approach, a non–personal, temporary, random identifier (TempId) is used instead. The TempId is assigned by the MSS on a per–communication session basis. The caller pays for the call by anonymous electronic cash (e–cash) [2, 3]. Confidential communication is ensured by the use of the public key (Kpu) of the MSS and a session key (Ks) belonging to the caller.

* PhD student supported by The National Autonomous University of Mexico

3 The Algorithm

In our system shown in Fig. 1, Bob is the anonymous sender, Alice is the recipient of the anonymous message on her work station (WS), and Doug is the owner of the MSS and offers communication services on a pay–for–time–used basis. Claudia is a bank owner and offers support for anonymous e–cash payments to her account holders (Bob and Doug). Finally, Ebe is another PDA user. The algorithm works as follows:

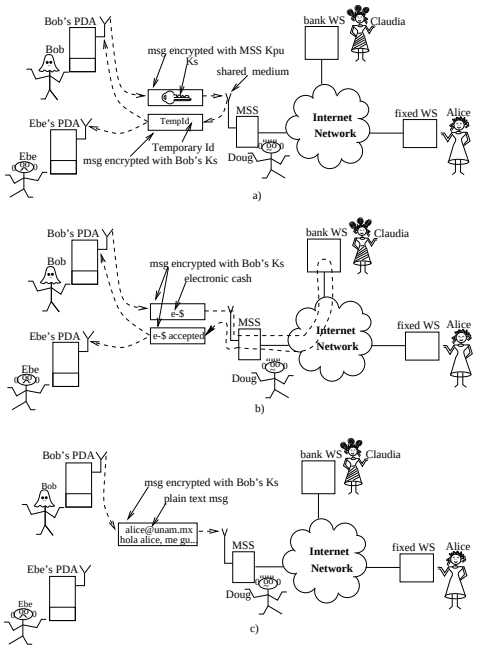

Fig. 1. Anonymous and confidential call from a PDA

1. Bob turns on his PDA and learns the Kpu of the MSS by listening to its advertisement
2. The PDA creates a Ks, encrypts it using the Kpu, and sends it to the MSS for approval, waiting t units of time for a reply
3. The MSS checks that the Ks suggested by Bob is correct and not in use. If so, it creates a TempId for Bob, encrypts it using the Ks, and sends it to the PDA as a reply. If the Ks suggested by Bob is incorrect, the MSS does not reply. If it is correct but has been assigned to an existing user, the MSS does not reply to Bob and additionally asks the user of the existing Ks to renew his Ks. After t units of silence, Bob can try again. The approved Ks is used then to encrypt and decrypt messages between the PDA and the MSS

until either the end of the session or until it has to be renewed. Messages encrypted with Bob's Ks can be overheard by Ebe but they will be ignored
4. Bob sends an anonymous e–coin to Doug to pay for the communication session. Doug consults Claudia about the authenticity of the coin before accepting or refusing it
5. If Bob wishes to anonymously e–mail Alice, he appends the message body to Alice's address, encrypts the result with Ks, and sends it to the MSS
6. The MSS decrypts the message, encrypts the enclosed message body together with Bob's TempId using Alice's Kpu, and forwards it to her
7. Alice has no means to discover the identity of the TempId holder. Yet, she can reply to Bob by addressing her response to the MSS and including Bob's TempId
8. Bob's session ends when he turns off his PDA, leaves his current MSS, or his MSS times-out his session

To stop the MSS from reading the message addressed to Alice, Bob can encrypt the message body with Alice's Kpu. Likewise, if he does not want the MSS to read Alice's reply, he can create and append a Ks to Alice's message body and ask Alice to encrypt the message body of her reply.

4 Conclusions

Aside from its obvious advantages, anonymity has several serious and negative side effects that make its deployment in the Internet a controversial issue. There are strong arguments for and against it. We believe that before saying that anonymity is good or bad, legal or illegal, we have to bring it into practice and test it rather than blindly approve or banish it.

In this work, we presented a system for sending truly anonymous and confidential messages from a PDA served by an MSS. The system imitates a public telephone box by identifying the PDA not with an IP address but with a random, temporary, non–personal identifier and by paying the MSS by anonymous e–cash for the service. An implementation model for the algorithm has been written in PROMELA code and its correctness is currently being tested using SPIN [4].

References

[1] John Ioannidis, Dan Duchamp, and Jr. Gerald Q. Maguire. IP-based protocols for mobile internetworking. In *SIGCOM'91 Conference. Communications Architecture and Protocols*, Zurich, Swizerland, September 3-6 1991. ACM.

[2] N. Asokan, Phillipe A. Janson, Michael Steiner, and Michael Waidner. The state of the art in electronic payment systems. *Computer*, 30(9), September 1997.

[3] Bruce Schneier. *Applied Cryptography.* John Wiley & Sons, Inc., second edition, 1996.

[4] Gerard J. Holzmann. *Design and Validation of Computer Protocols.* Prentice Hall, 1991.