On Shopping *Incognito*

Ralf Hauser*
McKinsey Consulting
Zürich, Switzerland
hauser@acm.org

Gene Tsudik†
University of Southern California
Information Sciences Institute
Marina Del Rey, CA
gts@isi.edu

Abstract

The increasing popularity and importance of electronic commerce makes very apparent the issue of privacy and anonymity for electronic consumers. Technologies are already in existence that offer some degree of electronic privacy, e.g., electronic/digital cash. However, the mere fact that electronic commerce is conducted over existing network infrastructure (such as the global Internet) runs counter to the privacy of the consumer. This is due mainly to the end-to-end nature of application protocols that are used as vehicles for electronic commerce – World-Wide Web (WWW), Electronic Mail, File Transfer Protocols and others.

In this paper we discuss the issue of consumer anonymity and propose some solutions for the activities that typically "surround" electronic payment: pre-purchase browsing and merchandise delivery.

1 Introduction

The state of the Internet today demonstrates the importance and the proliferation of electronic commerce. In this type of an environment – just as in the traditional "non-electronic" commerce – consumer privacy is becoming a major concern. The mere fact that electronic commerce is conducted over an existing open network infrastructure such as the Internet runs counter to the privacy of the consumer. Often, there are legitimate reasons for a party to remain anonymous at least during an initial stage of developing a business relationship with another party. But it becomes very difficult or even impossible for a party to safeguard its identity when addressing another party over an open network. Of course, this issue becomes even more complex when both communicating parties want to stay anonymous.

The problem is essentially due to the end-to-end nature of communication protocols used as a vehicle for electronic commerce. From the outset, the nature of current network protocols and applications runs counter to privacy. The vast majority have one thing in common: they faithfully communicate end-point identification information. "End-point" in this context can denote a user (with a unique ID), a network address, or an organization name. For example, electronic mail routinely communicates sender's address in the header. File transfer (e.g., FTP), remote login (e.g., TELNET), and hypertext browsers (e.g., WWW) expose addresses, host names and IDs of their users.

*This work was performed in part while both authors were at the IBM Zürich Research Laboratory, Rüschlikon, Switzerland

†This work was supported in part by the Defense Adavanced Research Project Agency (DARPA), Computer Sytems Technology Office, under contract DASG60-95-1-002.

Given the inadequacies of current communication protocols, our main goal is to provide a solution enabling anonymous data exchange, i.e, a method that would allow a prospective consumer to obtain bids or offers from prospective merchants without disclosing his identity. A closely related scenario is that of a consumer who, having already paid, takes delivery of the (electronic) merchandise while still remaining anonymous with respect to the merchant. Such methods must be resistant to false representations from both sides: the consumer's as well as the merchant's. Another goal is to exploit existing services already available in open networks and thus minimize deployment costs.

It is **NOT** the purpose of this paper to obtain a method for anonymous electronic **payment**. This topic has been addressed elsewehere, e.g., [3, 5]. More concretely, the two aspects of electronic commerce that are of particular interest:

- Pre-purchase Browsing (PPB) and
- Electronic Merchandise Delivery (EMD)

PPB refers to the electronic equivalent of *browsing*[1] or *window-shopping* in real life. During this stage a consumer typically compares various merchandise and advertized prices; at times a consumer even gets a written and signed estimate (or cost-breakdown) for services or goods. Following the analogy with physical commerce, a prospective consumer should not have to reveal his identity in order to partake in PPB.

EMD is the ultimate stage of an electronic commerce transaction. It involves the actual delivery (communication) of the electronic goods or services such as digital video, audio or text. Once again, provided that the interaction preceding EMD preserves the anonymity of the consumer, there is no reason for it to be sacrificed during EMD.

2 Required Infrastructure

Both PPB and EMD are not self-contained, independent mechanisms; they require certain basic security services for proper operation. We identify two main requirements:

1. Public-key certification infrastructure
2. Anonymous message-based communication

They are briefly described below.

[1] Not to be confused with WWW browsing.

2.1 Public Key Certification

Public key certification (PKC) serves a multitude of purposes. Currently, its most prominent use is in the area of secure electronic mail. Two of the best known examples are Privacy-Enhanced Mail (PEM) and Pretty Good Privacy (PGP) [7, 10]. The latter and its derivatives is, without a doubt, the most widely used. PEM includes a PKC hierarchy and functions. PGP's certification is somewhat *ad hoc*, although it does allow for informal certification hierarchies.

In the discussions below it is assumed that all relevant parties: merchants and consumers, are equipped with individual public key certificates. At the very minimum, a certificate is assumed to contain the party's name, public key, validity time, and the name of issuing authority. (The issuing authority is often referred to as the "Certification Authority" or CA.)

2.2 General-Purpose Anonymous Communication

Anonymous communication is necessary in order to preserve anonymity of the sender, i.e., the consumer in this context. It can also be used to hide the location of the sender. We note that sender's identity and location are often (but not always) tightly coupled.

Anonymous shopping requires some form of anonymous message-based communication. This communication can be synchronous (real-time, e.g., via WWW) or asynchronous (store-and-forward, e.g., via email.) In case of synchronous communication we assume the existence of a protocol-specific anonymizer or a mix [15]. An anonymizer is essentially a program that functions as a conduit between the real sender and receiver and hides the identity of the sender, e.g., by using a random alias. In case of asynchronous communication, we assume the existence of an anonymizing relay service. One example is the anonymous remailer (AR) – an anonymizing relay for electronic mail. There are at least a dozen Internet ARs offering varying degrees of anonymity and inter-operability [11, 6, 13].

Anonymizers for synchronous communication are not yet widely used[2] The only currently available tool is the WWW Anonymizer [19] which provides (weakly) anonymous Web access. (It is a single-site service which implies a central point of trust as well as a central point of failure. This is far less secure than the Chaum's Mix approach used by some of the current anonymous remailers.)

Anonymous shopping should place no restrictions on the type of the anonymizing tools. The only exception is the requirement for two-way communication: it should be possible for a consumer to send an anonymous request to the merchant and for the merchant to reply to the consumer. This can be done in a number of ways. One method used by simple (existing) ARs is to set-up a table that maps real email addresses into aliases; this way, a merchant can reply to the alias that is subsequently translated into a real email address by the AR.[3] There are certainly more secure and sophisticated methods such as having the sender (consumer) pre-compute a secret return path which is then "blindly" used by the receiver/merchant. Suffice it to say that, as long as it is available, the exact nature of the two-way anonymous communication is not germane to the discussion at hand.

2.3 Notation

The table below illustrates the notation used throughout this paper.

C,M	Protocol participants; consumer and merchant
H()	Strong one-way hash function, e.g., SHA or MD5.
CA	Certification Authority
PK_x	Public key of X
SK_x	Private (secret) key of X
$K(text)$	Encryption of "text" under key K
$Cert_X$	Public key certificate of X; includes PK_x
$S_x[text]$	Signature computed with SK_x, $S_x[text] = SK_x[H(text)]$
{text}	Optional text
R_x	Random number (nonce) generated by party X

3 Anonymous Pre-Purchase Browsing

3.1 Consumer Request

A prospective consumer (C) who wishes to obtain a bid/offer from a merchant (M) for certain merchandise composes the following message:

OFFER_REQ =DESCR,SIG_c

where:

- DESCR is the textual description of the desired merchandise including, e.g., quantity, color/size, delivery dates, etc.[4]
- $SIG_c = S_c[\text{DESCR}, R_c]$

In other words, SIG_c is the consumer's signature computed over the hash digest of DESCR together with a randomly-generated, used-only-once quantity R_c.

A crucial detail is that, even though R_c is used in computation of SIG_c, R_c is NOT included as part of OFFER_REQ message.

After composing OFFER_REQ the consumer uses the anonymous communication service to send the message to the merchant.

3.2 Merchant Reply

Upon receiving OFFER_REQ the merchant is not required to perform any security-related activity. Instead, the merchant examines DESCR and determines whether or not he can make a corresponding offer or bid. This process depends both on the merchant and on the type of merchandise specified in the incoming request. If and when the merchant is ready to make an offer, he composes the following message:

[2] It appears that anonymizing synchronous communication has been largely the province of military communications. However, solutions for anonymizing real-time traffic in certain restricted environments (e.g., Ethernet, ISDN) have been proposed [9].

[3] This is, in fact, the exact *modus operandi* of Penet – the first Internet remailer service located in Finland.[13]

[4] We assume that the consumer already obtained DESCR by either contacting the merchant beforehand (perhaps, via an anonymizer) or pulling it out of a catalog.

OFFER_REP= $\{SIG_c\}, \{Cert_m\}$,OFFER_DESCR,SIG_{offer}
where:

- SIG_c is the same as in OFFER_REQ message
- $Cert_m$ is the public key certificate of M
- OFFER_DESCR is the textual description of the offer including, e.g., current date/time, price, currency type, accepted payment type, delivery schedule, etc.
- $SIG_{offer} = S_m[SIG_c$,DESCR, OFFER_DESCR]

The merchant's public key certificate – $Cert_m$ – is optional in OFFER_REP since it is possible that the consumer already has it in his possession.

The hash function digest of DESCR and SIG_c is also optional since its only purpose is to help the consumer match the outstanding OFFER_REQ with the incoming OFFER_REP. This is only necessary in the asynchronous communication model.

3.3 Subsequent Actions by Consumer

When OFFER_REP is received, the consumer performs the following actions:

1. Using SIG_c identifies the outstanding OFFER_REQ.
2. If applicable, verifies the validity, authenticity and data integrity of the merchant's certificate – $Cert_m$. (Techniques for doing this are well-known.)
3. Examines OFFER_DESCR for consistency with the corresponding DESCR and determines whether to accept the offer.
4. If the offer is not accepted, no further actions are taken.
5. If the offer is of interest, the consumer computes:
   $PK_m(SIG_{offer})$ where PK_m is the merchant's public key extracted from $Cert_m$.
   and
   $H(SIG_c$,DESCR,OFFER_DESCR)
6. If the two values match the consumer is assured that the offer is genuine.

Given that the offer is acceptable and genuine, the consumer – if he so wishes – can approach the merchant directly, i.e., without going through the anonymizing process. (The consumer may decide to act upon the merchant's offer some time after the initial exchange, e.g., the next day.) Of course, this is not a requirement, i.e., if the merchandise is digital it can be delivered on-line. In that case, it may be possible and desirable for the consumer to remain anonymous.[5]

[5] Of course, in some cases the consumer will resort to conventional methods of payment (e.g., a credit card) thus sacrificing his anonymity.

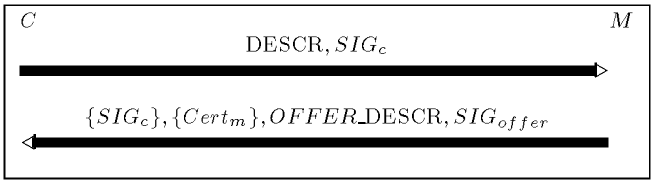

Figure 1: Anonymous Pre-Purchase Browsing Protocol

3.4 Subsequent Actions by Merchant

If and when the consumer decides to accept the offer, the merchant needs to establish that the offer is both genuine and still valid. Regardless of how the consumer goes about it, the following information must be communicated to the merchant:

- DESCR
- SIG_c
- OFFER_DESCR
- SIG_{offer}
- $Cert_c$
- R_c

The first four are taken directly from the aforementioned OFFER_REQ and OFFER_REP messages. $Cert_c$ is the public key certificate of the consumer and R_c is the hereto secret quantity that was used to compute SIG_c (see above.)

In order to establish the validity of the bid, the merchant does the following:

1. Verifies the validity, authenticity and data integrity of the consumer's certificate – $Cert_c$.
2. Extracts PK_c from $Cert_c$.
3. Computes $PK_c(SIG_c)$ and H(DESCR, R_c)
4. If the two values match the merchant is satisfied that SIG_c is the genuine signature of the consumer C.
5. Finally, M computes:
   $S_m[H(SIG_c$,DESCR,OFFER_DESCR)]
6. If this value matches SIG_{offer}, M is satisfied that the signature (and, hence, the corresponding offer) is genuine.

3.5 Maintaining Consumer Privacy

In the event that the consumer objects to revealing his identity to the merchant (even after deciding to go ahead with the payment), a mutually-trusted third party can be employed to verify the validity of the offer instead of the merchant. An obvious choice of such a third party is an *Acquiring Gateway* or simply *Acquirer* – an entity that in any case gets involved in the payment process. In this case, R_c and $Cert_c$ must be communicated to the third party bypassing the merchant (either physically or by means of encryption.) This is almost exactly the procedure in the *iKP* electronic payment protocol [3, 4].[6]

A much simpler way of maintaining consumer anonymity is to forgo consumer certification (at least in the context of the current discussion.) Then, the protocol has to be revised to replace SIG_c with H_c (see Figure 2) where $H_c = H(\mathrm{DESCR}, R_c)$. The main consequence is that the merchant's offer becomes *transferable*, i.e., the merchant can no longer establish that the consumer who reveals R_c and desires to pay for the merchandise is the same one who originally generated OFFER_REQ (and received the corresponding OFFER_REP.)

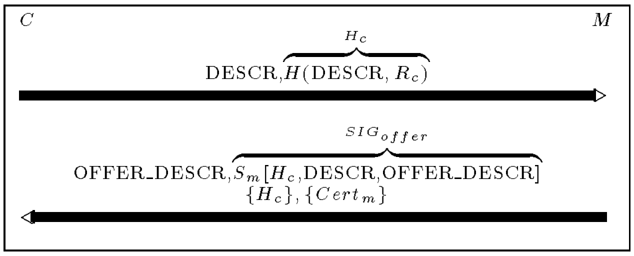

Figure 2: Anonymous PPB protocol without consumer certification

3.6 Minor Variations

The PPB method outlined this far can be amended as follows:

1. In the event that the user already has a copy of the merchant's certificate – $Cert_m$ – OFFER_REQ can be enciphered under the merchant's public key, PK_m. The resulting secrecy of the message offers protection against snoopers and eavesdroppers.
2. Furthermore, secrecy of the merchant's reply can be obtained if the consumer encloses a secret key (say, K_s) in the encrypted OFFER_REQ thus allowing the merchant to use this key for encrypting OFFER_REP.

3.7 Security Properties

In summary, the anonymous PPB method has the following security properties:

1. Anonymity of the consumer (while browsing before purchase) with respect to both outsiders and merchants.
2. Authenticity, data integrity and non-repudiation of the offer by the merchant.
3. Unlinkability of multiple requests by the same consumer. This is a particularly important feature which essentially prevents the merchant from *recognizing* a browsing consumer as someone who has previously made purchases (even if the merchant possesses that consumer's certificate.)
4. Authenticity and non-repudiation of offer request by the consumer (this only becomes apparent when the consumer decides to act upon the offer.)
5. Optionally, privacy from eavesdroppers of merchant-consumer communication.

[6] However, $Cert_c$ is not encrypted or otherwise treated in iKP.

3.8 Practical Considerations

The anonymous PPB method can be applied in both asynchronous (e.g., email-based) and synchronous (e.g., http-based) electronic commerce. In case of the former, the necessary infrastructure already exists, i.e., there are a number of functioning anonymous remailers and several public key certification schemes (even an informal one like PGP's can be used.) Electronic commerce via synchronous communication is currently gathering momentum and is widely believed to be the way of the future. The increasing popularity of WWW-based commerce is a case in point. The only missing ingredient is an http anonymizer – a relay that takes incoming http requests and, acting as a proxy, connects them to desired points of interest while preserving the anonymity of the actual incoming end-points. (Of course, the replies must be mapped back.) We observe that much of this functionality is already provided by firewalls.

4 Delivery of Electronic Merchandise

We now consider the issue of consumer anonymity *after* the payment is already made. If the purchased merchandise is of electronic nature and the consumer has remained anonymous with respect to the merchant during PPB and subsequent payment, there is no reason to give up on anonymity during merchandise delivery stage.

However, the anonymous PPB method as described in Section 3 terminates with the consumer revealing his identity upon initiating the payment. This obviously contradicts our goal. For this reason we assume that the PPB method is amended in either of the two ways described in Section 3.5. (In other words, either consumer certificates are not used at all or a trusted third party takes care of asserting the consumer's identity.)

4.1 Assumptions and Preliminaries

Prerequisites are almost identical to those for anonymous PPB, i.e., public key infrastructure (for merchants only) and a facility for general-purpose anonymous communication.

The present method commences when the consumer decides to purchase the merchandise based on a previous bid/offer obtained from a run of the PPB protocol. Although it can, in principle, take place concurrently, we assume that payment takes place before the delivery of goods. The particulars of the payment process are out of the scope of this paper. (See [4] or [14] for examples of secure electronic payment protocols and scenarios.)

4.1.1 Step 1

The protocol begins whenever the consumer is ready to take delivery of the merchandise:[7]

- Consumer generates another random number R_d and computes $H(R_d)$.
- Consumer sends to the merchant a COMMIT_REQ message containing:
$$H(R_c), H(R_d)$$

4.1.2 Step 2

- Merchant extracts both $H(R_c)$ and $H(R_d)$; the latter is stored for future reference.
- Using $H(R_c)$ merchant locates the corresponding offer in his records. If the offer is no longer valid (e.g., it has been already processed), merchant notifies the consumer accordingly and terminates processing.
- If the offer is still valid, merchant composes and sends to consumer a COMMIT message containing:
$$\underbrace{S_m[\text{COMMIT\_REQ}]}_{SIG_{commit}}$$

4.1.3 Step 3

- Consumer receives the COMMIT message and verifies SIG_{commit}. If the signature is invalid, an error message to that effect is sent to merchant.
- If signature is valid, consumer generates and sends to merchant a DELIVERY_REQ message containing: R_c.

4.1.4 Step 4

- Merchant receives DELIVERY_REQ and extracts R_c.
- Merchant computes $H(R_c)$ and compares to $H(R_c)$ stored in the appropriate transaction record. If there is a mismatch, an error message to that effect is sent to consumer.
- If $H(R_c)$ values match, merchant composes and sends to consumer a DELIVERY message containing:
$$\text{GOODS}, \underbrace{S_m[SIG_{commit}, \text{GOODS}]}_{SIG_{deliver}}$$

4.1.5 Step 5

- Consumer receives DELIVERY and obtains GOODS
- Using PK_m and SIG_{commit} (received in Step 3) consumer verifies $SIG_{deliver}$. If $SIG_{deliver}$ is invalid an error message to that effect is sent to merchant.
- Otherwise, consumer sends to merchant a TERMINATE message containing: R_d.

4.1.6 Step 6

- Finally, merchant receives TERMINATE, extracts R_d, computes $H(R_d)$ and compares it with $H(R_d)$ received in COMMIT_REQ (see step 2.) If they match, the transaction is terminated. Otherwise, an error message is sent to consumer (along with the re-transmission of DELIVERY.)

Figure 3: Anonymous EMD protocol

4.2 Dispute Resolution

The anonymous EMD method provides protection against dishonest behavior by either merchants or consumers involved. Potential cases of cheating and disputes are addressed below. All cases require intervention of a mutually trusted off-line authority that we refer to as COURT.

(Some forms of disputes are not addressable in a protocol format. For example, any dispute over the nature and content of GOODS is most likely to be handled on a case-by-case basis.)

While dispute resolution is likely to take place off-line, it is expected that consumer will remain anonymous with respect to merchant. However, consumer may be required to reveal his identity to COURT.

At the end of a successful transaction both consumer and merchant must have the following in their possession:
$$R_c, R_d, SIG_{commit}, SIG_{offer}, H(R_c), H(R_d)$$
In case of a dispute, the following procedure takes place:

1. Consumer is asked to produce a valid SIG_{offer}
   (a) No valid SIG_{offer}; merchant prevails.
   (b) Valid SIG_{offer}; continue with (2).

[7] Note that the consumer is assumed to retain R_c and SIG_{offer} from PPB above.

2. Merchant is asked to provide R_c.
   (a) Merchant can not produce the correct R_c; continue with (3).
   (b) Correct R_c; continue with (4)
3. Consumer is asked to produce R_c.
   (a) Correct R_c; consumer prevails (protocol can be re-run.)
   (b) Incorrect R_c; merchant prevails.
4. Consumer is asked to produce R_c.
   (a) Correct R_c; continue with (5).
   (b) Incorrect R_c; merchant prevails.
5. Consumer is asked to produce a valid SIG_{commit}.
   (a) No valid SIG_{commit}; merchant prevails.
   (b) Valid SIG_{commit}; continue with (6).
6. Merchant is asked to produce R_d.
   (a) Correct R_d; merchant prevails.
   (b) Incorrect R_d; consumer prevails (merchant is ordered to send a DELIVERY message to consumer and consumer is ordered to reply with a TERMINATE message; the latter containing a valid R_d.)

Unlike merchant's other signatures, $SIG_{deliver}$ is not used in dispute resolution. This is because consumer can always deny having received it. The purpose of $SIG_{deliver}$ is to provide both origin authentication and non-repudiation of GOODS in the DELIVERY message. Moreover, $SIG_{deliver}$ can prove very useful in the event of a product misrepresentation dispute (which is out of scope of this paper.)

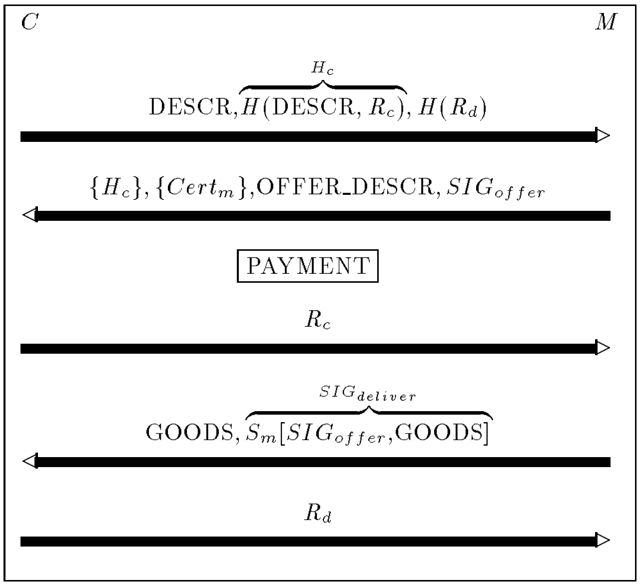

Figure 4: Combined protocol

5 Streamlining Anonymous PPB and EMD

The two methods described above are presented independently in order to emphasize their different goals. However, it is certainly possible (and desirable) to combine the two into a unified protocol (as depicted in Figure 4.) The present protocol combines OFFER_REQ and COMMIT_REQ messages.

The OFFER_REP and COMMIT_REP are similarly collapsed into a single message flow. This saves one signature operation for the merchant.

5.1 Related Work

There has been a lot of research activity in anonymity in the context of electronic cash and other forms of payments. Anonymity, as considered in this paper, has received far less attention. A notable exception is the NetBill project at CMU [16, 17, 18].

NetBill is an all-around electronic commerce system. It bundles browsing, bidding, payment, delivery and other services. It also includes some provisions for anonymity. This paper, in contrast, considered consumer anonymity as a separate feature, indepedent of (or orthogonal to) the particular payment mechanism (NetBill, iKP, Ecash, SET, etc.) and payment type (cash, credit, check, etc.)

Furthermore, since NetBill is built on top of Kerberos, it inherently requires a trusted thrid party, something we consider only in case of disputes.

NetBill provides two forms of customer anonymity: one-time (per transaction) or multiple use (per merchant). In either case, the customer is not free to choose his own aliases; every single alias must be obtained from a *Pseudonym-Granting Server* (PGS). This requires the disclosure (to the PGS) of the customer's true identity. Consequently, the level of anonymity in NetBill is weaker than that decribed in this paper.

6 Future Work

This paper concentrated on the motivating factors and mechanisms for maintaining consumer anonymity with respect to merchants. While the motivation for the opposite is less apparent, some forms of commerce (auctioning, open bidding) call for merchant anonymity.

A simple (but not always practical) approach is for the consumer to post OFFER_REQ on an anonymous bulletin board, e.g. a USENET newsgroup and solicit bids. If the consumer trusts COURT or another trusted third party to properly certify the merchants' public keys in an anonymous way (see [2]), the protocols can be run almost exactly as described above, but without the consumer knowing the merchant's identity.

If mutual anonymity is to be attained without the involvement of a trusted third party, we need to look into protocols for anonymous fair exchange [1].

7 Conclusions

In this paper we discussed the issue of consumer anonymity in the setting of secure electronic commerce. More specifically, we concentrated on consumer anonymity during *Pre-Purchase Browsing* (PPB) and *Electronic Merchandise Delivery* (EMD). We argued that anonymity does not imply lack of recourse in cases of dishonest merchants. Simple, yet secure, methods for anonymous pre-purchase browsing and anonymous electronic merchandise delivery have been developed. Both methods provide mechanisms for disambiguating inconsistencies and arbitrating disputes.

We have also shown that consumer anonymity in activities surrounding electronic payment (PPB, EMD) does not require any more security infrastructure to be in place than that already necessitated by the state-of-the-art electronic payment systems.

8 Acknowledgements

The authors would like to thank Michael Waidner, Michael Steiner, Ari Medvinsky, Cliff Neuman and the anonymous referees for their helpful comments.

References

[1] Holger Buerk, Andreas Pfitzmann, *"Digital Payment Systems Enabling Security and Unobservability,* Computers & Security 8/5 (1989) pp. 399-416.

[2] Ralf Hauser, *"Using the Internet to decrease Software Piracy - on Anonymous Receipts, Anonymous ID Cards and Anonymous Vouchers,"* INET'95, Annual Conference of the Internet Society, Honolulu, HI, June 1995.

[3] M. Bellare, J. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik and M. Waidner, *"iKP - A Family of Secure Electronic Payment Protocols",* Usenix Electronic Commerce Workshop, July 1995.

[4] M. Linehan and G. Tsudik, *"Internet Keyed Payments Protocol (iKP)",* Internet Draft, "draft-tsudik-ikp-00.txt", June 1995.

[5] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *Journal of Cryptology*, 1/1, 1988, pp. 65–75.

[6] L. Cottrell, "Mixmaster and Remailer Attacks," http://obscura.com/~loki/remailer-essay.html.

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

[8] T. May, "Crypto Anarchy and Virtual communities," *Internet Security Journal*, April 1995.

[9] A. Pfitzmann and M. Waidner, "Networks Without User Observability—design options," *Computers & Security*, 6/2 1987, pp. 158–166.

[10] P. Zimmerman, "PGP User's Guide", included in PGP distribution 2.6i, October 1994.

[11] C. Gulcu and G. Tsudik, "Mixing E-mail with BABEL", *1996 Symposium on Network and Distributed System Security*, February 1996.

[12] D. Chaum, A. Fiat and M. Naor, "Untraceable Electronic Cash", *Proceedings of Crypto'88*, August 1988.

[13] J. Helsingius, "Penet Anonymous Remailing Service", Information available from *anon@penet.fi*; (set subject field to HELP.)

[14] MasterCard International, "SET: Secure Electronic Transactions", see: http://www.mastercard.com/.

[15] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, vol. 24, no. 2, February 1981.

[16] M. Sirbu and D. Tygar, "NetBill: An Internet Commerce System Optimized for Network Delivered Services," *IEEE CompCon Conference,* March 1995.

[17] B. Cox, D. Tygar and M. Sirbu, "NetBill Security and Transaction Protocol", *Usenix Electronic Commerce Workshop,* July 1995.

[18] B. Cox, "NetBill Security and Transaction Protocol", *CMU TR-1994-8 (MSc Thesis)*, August 1994. (http://www.ini.cmu.edu/NETBILL/pubs.html.)

[19] Community ConneXion, "The Anonymizer", (http://www.anonymizer.com/.)