Influence of Payment Protocol in e-Negotiations

Abstract. There are several ways to perform an electronic payment corresponding to the existing types of transactions. Their characteristics and intention may be quite different. One of them should be chosen. Although participants (buyer and seller) seldom do not question this decision, the selection of an electronic payment system has quite a lot importance in the purchase. The influence of this decision on the amount to be paid, the computational resources required, anonymity, trust set in participants, etc. is usually ignored. However most of these terms are often under discussion in the negotiation of commercial agreements. In this paper, we analyse the characteristics of some of the most relevant electronic payment systems and their influence in the agreement terms under discussion.

1 Introduction

The easy access to a wide range of information has leaded to an exponential growth of the interest in Internet. Since many costly services and products can be provided through electronic means, commercial interactions soon played a central role in electronic communities. Commercial interactions has been studied from different points of view: game theory, sociology, artificial intelligence, etc [1].

Despite of the very remarkable advantages of electronic shopping (a high number of available offerings and timesaving) its level of success is far away from the expectations. One of the most argued reasons is the suspicious attitude from the potential buyers due to a lack of security in electronic payment.

Although the application of cryptographic mechanisms to electronic transactions provides quite enough level of security, many potential buyers still have reticences in electronic payments. Many factors may cause the perception of insecurity: negative references from the newspapers, inadequate distribution channels, personal habits, lack of well-formed specialists, etc. But another remarkable aspect is that potential buyers have difficulty understanding the sound mathematical foundations of cryptographic mechanisms, and therefore, the details and specific features of each electronic payment system are ignored. Due to this problem, electronic payment is executed in a way transparent to buyers. They do not realise what electronic payment is using and why. This blind execution of the electronic payment does not allow a suitable selection depending on the concrete circumstances of the situation faced, in order to argue it as a subject under discussion in agreement negotiations.

Security protocols often define handshake communications where a limited negotiation of cryptographic parameters takes place [2]. This handshake process follows prefixed rules of dialogue choosing encryption and key-exchange algorithms, random seeds, compression methods, etc. The selection agreed would allow both parts to perform identical computations, and therefore to communicate successfully the information. The dialogue consists of a pair of request/response messages where the respond message picked the desired parameter from the options sent in the request.

This so-called negotiation involves neither discussion nor bargaining. A more complex dialogue with several speech-act-typed messages was applied in [3] to reflect a real negotiation of security policy criteria. But the little number of options, and their limited (and difficult to estimate) relevance make the associated complexity senseless.

But we take the stance that when the electronic payment system was subject to negotiation, some level of discussion about them would be useful [4]. Such discussions consist of exchanging rational arguments to persuade the other part to improve its offering. These human-like automated negotiations may contribute to reduce the level of suspicious in potential buyers.

Although negotiation and payment are autonomous processes, we will show how arguing about electronic payments makes automated negotiation richer, and it would possibly improve the corresponding agreements. We will give a brief description of the characteristics of the most remarkable electronic payment systems. Next we will link some of these characteristics with commonly used negotiation criteria.

2 Some Electronic Payment Protocols

2.1 Classification of payments

Money is typically transferred in three major communications: withdrawal, payment and deposit. Entities may play four essential roles in these communications: payer, payee, acquirer and issuer of payment means. Figure 1 shows a model of a generic transaction.

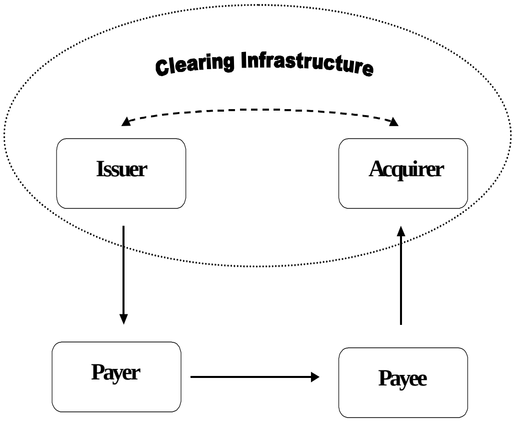

Fig. 1. Abstract model of typical transactions

Computer Security copes with the protection of communications. This research area has defined the cryptographic mechanisms, the content and sequence of the messages involved in the protocol used in the communication. Each of these protocols provides several security services: authentication, confidentiality, integrity and non-repudiation [5]. The security services provided by a protocol depend on the intention of the communications. So protocols are often denoted by the pursued intention: authentication, key distribution, electronic payment, etc.

Electronic payment systems may be classified according to several criteria:

a) Payment mode: prepayment, instant payment and credit payment.

b) Payment scope: available payees, application domains.

c) Payment means: cards, cheques and cash.

The last attribute is the most commonly used, and we have adopted it in order to describe some remarkable electronic payment systems in next subsections.

2.2 Credit Card based Payments

The use of credit card in payments is broadly extended in real life. Payment mean consists of the identification number of a credit card. Payment requires an additional communication between the payee and the issuer of the card in order to verify online the validity of the card number together with the amount to be credited. This type of credit payment is not anonymous, and it is especially advisable when a great amount of money is involved. Both protocols authenticate the participants, and protect the secret of the number of credit card using public-key cryptography.

Secure Socket Layer [6] protocol (so called SSL) ensures communications through sockets. It intends to create a secure communication channel, providing confidentiality, integrity and authentication. However it does not provide non-repudiation, and therefore, it is not a suitable payment protocol, although most commercial sites uses it because it is relatively easy and cheap to implement.

Secure Electronic Transaction protocol [7] provides non-repudiation and it protects the knowledge of the number of the card from the payee, and the details of the product bought from the issuer and the acquirer. Dual signatures to ensure the link between both secrets. So the payee and the bank may verify online such link, while they only know the information relevant to the role they played. The use of SET protocol is not widely extended yet because of the computational and economic costs required.

2.3 Micropayments

These electronic payments are called Micropayments because they are suitable for transferring frequent transactions of small value. Furthermore, in micropayments payee does not require online verification with any third party. Micropayments require significant less computational times and storage than other payment systems, because they use one-way hash functions rather than public key cryptography. However micropayments sacrificed security for this reason and therefore, they are not suitable for large amount transactions. At least security is enough for small payments because the cost of counterfeiting is supposed to be higher than its value.

Payword [8] is based in a chain of hash values, each of them represents a denomination of a unit of economical value. In payword, chains are created by payers from a random seed and a strong one function. No broker or intermediary is needed to create/withdraw money. The payment mode is credit-based because the money is not debited from payer until the payee makes redemption of several micropayments corresponding to a complete hash chain.

Public key cryptography is used to show the initial commitment of a payer with a given chain of hashes. Commitment also links a hash chain with a given payee, so hashes from this chain can be used only with that payee. The detection of double spending and depositing requires from payees and payers the storage of all the valid sent and received commitments. The main undesirable feature of payword is that payers and payees have to maintain long term commercial relationships in order to be efficient. Hash chains should be disjoints, and each of them is useful just for a payee.

In Micromint [8], money is issued by a broker or intermediary who certifies the validity of the money. A high number of hashes is required to generate a valid unit of economical value. It is a debit-based approach because payer has to buy from the broker a certain number of micropayments in advance through an alternative form of payment.

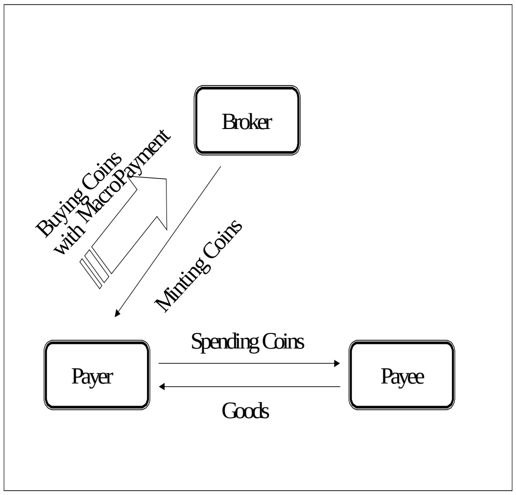

Fig. 2. Role of brokers in Micromint

This scheme requires a return policy in order to recover the money involved in unused micropayments. Money can be generic, user-specific, and even user-vendor specific. Generic coins can be easily stolen and replaced and double spending is more difficult to detect. On the other hand, user-vendor specific coins are more secure and reduce the chance of fraud, although minting them is more complicate process. Using a broker as an intermediary provides no additional security, but the relationship of a payee with a broker may last longer than with a payer. Therefore, micropayments for different. The unique identity of the coin is used to detect double spending. Payees keep a blacklist of already spent user-vendor specific coins.

2.4 Electronic checks

In check-like payment system, funds are transferred at the time the transaction takes place. Online verification of funds availability takes place at that instant. They are obviously not anonymous.

Financial Services Technology Consortium [9] is concerned in defining en electronic check intended to make maximal use of the existing interbank clearing infrastructure. It uses the public key cryptography let payers to sign checks. Applying the digital signature of issuer, will yield a certified check. It requires a tamper resistant hardware device to keep securely store secret key and certification information. The security level implicit is very high, but quite a lot computational time is required, and this problem prevents a generalised use of this payment scheme.

NetBill [10] uses a unique intermediary to manage all communications of payers and payees with acquirers and issuers. It guarantees that payee receives the corresponding amount of money, and that payer successfully receives the bought goods. The protocol used is a modified version of Kerberos [11], so called public-key kerberos, which make efficient use of symmetric encryption, but it still requires some public key cryptography. The existence of this central entity is an obvious bottleneck, making it inherently not scalable.

NetCheque [12] uses pure Kerberos ticket-based authentication model. It avoids the use public key encryption and thus is more efficient than netbill and ntfs. Payers and payees just deal directly with their preferred bank in order to write and endorse checks respectively. It consists of a hierarchy of banks that allows the scalability of the system. Communication costs depend on the length of the path from the acquirer to the issuer in that hierarchy. It may become unobtrusive in small transactions.

2.5 Electronic cash

David Chaum proposed an electronic payment system called ecash [13] in order to emulate the performance of electronic cash. The main property of electronic cash is anonymity in transactions. Blind signatures uses public key cryptography in order to hidden the identity of payer. Issuer does not know the identification number of the electronic coins withdrawn and therefore issuer can not link the identity of the entity who withdrew coins with such coins. Even when the issuer colludes with the payee, the identity of the payer can not be revealed.

One disadvantage of ecash is the low level of scalability provided since banks have to keep a blacklist of the coins already used. So payee should verify online the validity of coins with issuer. Other relevant problem of ecash is possible abuse of blind signatures when there is no redundancy in blinded text [14]. This is one of the main critics and limit to the application of such mechanism because they might be used to forge coins [15]. These limitations have prevented ecash from an extensive acceptance.

3 Negotiation issues involved in the selection of electronic payment

Many criterions may influence over commercial negotiations, some of the most important are time required, money involved and risks assumed.

Time may play a fundamental role in negotiations, when the product/service has an expiration time, or when one of the parts is hurried up due to any external reason. In those cases, it is not an easy task to estimate the time required to complete the purchase. Different electronic payment systems require different number of messages, and they also involve different computation processes. We can therefore, assume that offline payments last less time than online payments because they involve additional communications. In an analogous way, we can expect payments based on public-key encryption to take more computational time than others. Finally we can also suppose that centralised systems have worse latency time than distributed ones.

Money involved is usually a critical factor in negotiations. Since the use of some electronic payments may be taxed (SET protocol, for instance), merchants have room for rewarding the use of alternative electronic payments. Payment mode has also a strong influence in this factor. For example, credit payments allow buyers a greater flexibility in the management of their income than prepayments. Furthermore, computational costs may have serious economical consequences due to the potential buyers lost while the computational resources of the merchant are busy. Finally, merchants may increase the prices in order to recoup the implementation costs of an electronic payment system.

The risk assumed in the selection of an electronic payment system is very difficult to guess. Although there are certain guidelines to consider:

- The amount of money involved in the payment increase the risk assumed. Eavesdropping a credit card number may also involve additional costs of future forgery of false payments.
- Merchants would be able to misuse the credit card number too if they knew it (SSL protocol, for instance). Then, trust set in the other part (the seller) should be considered before accepting SSL protocol.
- The level of security of certain cryptographic mechanisms (one-way functions, blind signatures) is supposed to be relatively fewer then others (encryption).

Other factors may be also considered since seller-specific money limit the future use of such amount to a given seller or group of sellers and anonymity may be desirable under certain circumstances.

Therefore the seller might reward the use of certain payment systems through improvements in other issues under discussion. For instance, we can guess that merchants would prefer electronic payments with some of desirable attributes:

- Computational time required. Fast operations may allow seller to deal with more potential buyers.
- Vendor-specific payments. This kind of money links the buyer with the seller, and it influences the buyer in favour of future purchases with the seller.
- Taxes levied on the use of some electronic payment systems: the seller earns money by using not taxed electronic payments.

On the other hand, buyers might consider the disadvantages of certain characteristics of electronic payments in order to reject offerings from sellers. For example, some features to avoid in electronic payments are:

- The high implementation costs of any service often has repercussions on the price of providing such service. So this consideration may apply to electronic payments too.
- Centralised approach lead to bottleneck problems, and therefore response time is usually greater than with distributed alternatives.
- Online electronic payments involve an additional communication, so these payments last more than offline ones.
- The delicate matter of certain purchases suggests the use of anonymous payments. Buyers may desire that anypart would not be able to trace their identity.

Credit card payments, specially if sellers were not enough trusted to let the merchant know credit card number.

4 Conclusions and Future Work

We have showed how electronic payments may play a relevant role in automated negotiations through a brief overview of the main characteristics of some remarkable electronic payment systems. The different features of them introduced the necessity of a deliberation about electronic payments in e-negotiations.

Electronic payments may be selected according to the different situations possibly faced. We have considered the influence of this selection over major decision criteria of commercial negotiations as price, time, trust, risks, etc. The agreements coming from those negotiations could possibly use a more suitable electronic payment, or they could provide more profit because of using an electronic payment more suitable for the other part.

The issues that are relevant for the negotiation of a deal are intended to be formally specified in ontologies. Since the characteristics of electronic payments are important for the negotiation of a purchase, an ontology of universally accepted differences among electronic payment systems would be useful to avoid misunderstandings. In future, we will define such ontology, probably using the methodology described in [16].

Furthermore, future works will involve the formalisation of arguments related to electronic payments in order to increase the expressiveness of the framework of persuasive negotiation defined previously in [17].

References

1. Rosenchein, J. Zlotkin G., Rules of Encounter: Designing conventions for automated negotiation among computers. MIT Press (1994).
2. Schneider, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley and Sons, (1996).
3. Hu Y.J., Negotiating Compatible Crypto Protocols in behalf of the End-User. RSA Data Security Conference (1998).

4. Mackie-Mason J.K., White K., Evaluating and Selecting Digital Payment Mechanisms. In G. Rosston and D. Waterman, editors, Interconnection and the Internet, pages 113--134. Lawrence Erlbaum, (1997).
5. National Institute of Standards and Technology. Agency Use of Public Key Technology for Digital Signatures and Authentication, National Institute of Standards and Technology Special Publication 800-25, (2000).
6. Freier A., Karlton P., Kocher P.., The SSL Protocol version 3.0 Internet Draft, Netscape Communications Corporation, http://home.netscape.com/eng/ssl3/ (1996).
7. VISA & MASTERCARD Corporation. Secure Electronic Transaction Specifications. http://www.setco.org/set_specifications.html (1997).
8. Rivest R., Shamir A., Payword and Micromint: Two Simple Micropayment Schemes. CryptoBytes, volume 2, number 1, 7--11. (1996)
9. Andreson M., Financial Services Technology Consortium Electronic Check Project Architecture, http://echeck.commerce.net/library/ (1995).
10. Steiner J.G., B.C. Neumann, J.I. Schiller, "Kerberos: an Authentication Service for Open Networks Systems" Proceedings of the USENIX UNIX Security Symposium, (1998).
11. Sirbu M., J. Chuang, NetBill: an Electronic Commerce System Optimized for Network Delivered Information and Services. Proceedings IEEE Compcon (1995).
12. B. Clifford Neuman and Gennady Medvinsky. Requirements for Network Payment: The NetCheque Perspective In Proceedings of IEEE Compcon (1995).
13. Chaum D., Blind Signatures for Untraceable Payments. Advances in Cryptology: Proceedings of CRYPTO (1983).
14. Stadler M., J.M. Piveteau, J. Camenisch, Fair blind signatures. Lecture Notes on Computer Science 921, pp. 209-219, (1995).
15. von Solms S., D. Naccache, On blind signatures and perfect crime. Computer and Security 11, pp 581-583, (1992).
16. Fernández, M. ; Gómez Pérez, A. ; Juristo, N. METHONTOLOGY : From ontological art towards Ontological Engineering. Symposium on Ontological Engineering. American Association for Artificial Intelligence (AAAI), (1997).
17. Carbo, J., J.M. Molina, J. Davila, Augmenting users' confidence in agent-mediated commerce negotiations. Proceedings of the IASTED International Conference on Artificial Intelligence and Applications, pp. 388-392, (2001).

Appendix: Springer-Author Discount

The appendix should appear directly after the references, and not on a new page

All authors or editors of Springer books, in particular authors contributing to any LNCS or LNAI proceedings volume, are entitled to buy any book published by Springer-Verlag for personal use at the "Springer-author" discount of one third off the list price. Such preferential orders can only be processed through Springer directly (and not through bookstores); reference to a Springer publication has to be given with such orders. Any Springer office may be contacted, particularly those in Heidelberg and New York:

Springer Auslieferungsgesellschaft
Haberstrasse 7
69126 Heidelberg
Germany
Fax: +49 6221 345-229
Phone: +49 6221 345-0

Springer-Verlag New York Inc.
P.O. Box 2485
Secaucus, NJ 07096-2485
USA
Fax: +1 201 348 4505
Phone: +1-800-SPRINGER
(+1 800 777 4643), toll-free in USA

Preferential orders can also be placed by sending an email to
orders@springer.de or orders@springer-ny.com.

For information about shipping, please contact one of the above mentioned orders departments. Sales tax is required for residents of: CA, IL, MA, MO, NJ, NY, PA, TX, VA, and VT. Canadian residents please add 7% GST. Payment for the book(s) plus shipping charges can be made by giving a credit card number together with the expiration date (American Express, Eurocard/Mastercard, Discover, and Visa are accepted) or by enclosing a check (mail orders only).