SOME REMARKS CONCERNING THE SECURITY OF ONLINE TRANSACTIONS BASED ON NETBILL E-COMMERCE PROTOCOL

A. M. SPIRIDONICĂ[1],**A. G. FERARU**[1], **N. MANOLICĂ**[1]

[1] „Gheorghe Asachi" Technical University, Iasi
e-mail: aspiridonica@ee.tuiasi.ro

The development of the Internet has a great impact on the promoting and selling of the ordinary or digital goods. It allows the creation of new on-line commercial schemes, which are characterized by a very fast access to economical information. All of these require exchanges of documents in digital form between several firms, organizations and/or physical persons. Besides its advantages, the transactions on the Internet leads to major security problems because the information may be available to unauthorized parties. It is necessary to develop, maintain and analyze specific security solutions dedicated to digital transactions. Thus, several e-commerce, e-payment, e-auction protocols have been proposed in order to assure proper and secure transactions. The main dificulty is that the information flow on the Internet is free, without any control or censorship. Moreover, the identity of the involved partners is not always known. This implies that the information can be intercepted, modified or even deleted by dishonest users. In this paper we analyze a very important e-commerce protocol, namely NetBill, in the context of on-line transactions.

Key words: *on-line transactions, security protocols, e-commerce, e-payment*

NetBill is a set of rules, protocols and software, designed for delivering of the text and images over the Internet. It has been developed at Carnegie Mellon University, in collaboration with Visa and Mellon Bank, in order to make micropayments (payments of 1 U.S cent). The main characteristic of this protocol is that the client is billed only after he has received the encrypted desired information; the decryption key, that permits to obtain the real information, is delivered to the client only after he makes the payment. This approach is useful especially for the repeated delivering of a small amount of information, e.g., in the case of e-news, software updates or purchase of ring-tones. Besides its function as payment intermediary, the NetBill server has also the role of certification authority. Moreover, it supervises the distribution of public/private RSA keys and the session keys, that are used for encrypting the messages between the client and the vendor, and the messages with the NetBill server. In this paper we review the NetBill protocol and we make some very interesting remarks on its security.

MATERIAL AND METHOD

As method we have used the algorithms of NetBill e-commerce protocol through a presentation in own way of his mode of operation, which may seem very difficult at a first glance and which addressed to readers which have a average experience in e-commerce domain and also in on-line security assurance of such transactions. The methodology used in this protocol have six stages, which will be presented below.

The first stage is *the registration*. Customers are recorded giving the informations of their credit cards or the coordinates of a encrypted payment instrument using a downloaded security modul (e.g., using *Money Tool*). Instead, the customer received from NetBill server an ID and a pair of public and private keys *RSA*, namely KP_c and KS_c. Similarly, after the registration, the vendor received the *Product server* program and also a pair of public and private keys RSA, namely KP_v and KS_v [2]. The accounts of those enrolled at NetBill are prepaid and fueled from banking accounts, preferably through NetBill bank. The software display the available sum on the screen. In a next phase, the NetBill will consider the post-payment authorization.

The second stage is the acquisition. The basic acquisition protocol used 8 *HTTP* mesages in order to cover the four main phases of commercial and financial transaction: negotiation, order, supply and payment. These operations implies three parts: customer, vendor and payment intermediary (the NetBill server). The payment intermediary plays the role of a notary and communicate directly with the merchant. Though the vendor, he communicates directly and with the customer.

Before the establishment of communication channels, there is a phase of mutual recognition to enable partners to identify and authenticate (using, e.g., the *Kerberos system*). Thus, the vendor server authenticates the client using a session ticket and a certificate signed by the certification authority. The ticket is signed using the customer's private key and the is encrypted with the public key of the vendor's server. Through the ticket, the customer and the vendor will be able to encrypted the messages, using a symmetric encryption method. This ticket also offer a strong resistance against any attack on the Kerberos server. The customer build a symmetric key K_1 and send this key to vendor, which is included in the following message:

$$e_K(\text{customer name, vendor name, time parameter, } K_1),\ e_{KP_v}\ (K, \text{Sig}_c)$$

The vendor's server verify the signature using the public key of the customer, which is extracted from the certificate. Next, the vendor produces the symmetric session key K_{CV} and build the *session ticket* τ_{cv}.

The ticket contains two parts:

- the vendor name;
- the customer name and also the customer address, the expired date of the ticket, the symmetric session key K_{CV}, all of these encrypted with the vendor private key; the expired date can be set later.

The vendor's server encrypted the session ticket τ_{cv} and the symmetric session key thorugh a symmetric key K_1 and then connects this and also send to the customer in the following form:

$$e_{K_1}(\tau_{cv}, K_{cv})$$

Only the customer and the vendor know the K_1 key – thus, the customer is sure that this key comes only from the vendor. The vendor decrypted this key in order to obtain the session ticket τ_{cv} and also the symmetric key K_{CV}. Next, using the public key of the vendor, the customer verifies if the session key is identical with the key which the session ticket contain.

The third stage is the negotiation. In the negotiation phase, the customer request the price of an article and the vendor responds with a personalized question. This phase starts with the customer identification so that the vendor will customize the offer depending on the customer profile.

After the negotiation phase follows the phase command, in which the customer will agree on the transaction:

$$\tau_{cv}, e_{K_{cv}}(\text{transaction identifier})$$

The next phase is the delivery phase in which the file encryption products is stored on the customer's hard disk, but the products cannot be accesed yet because the customer not holds the decryption key; the customer will received this key after the payment quittance.

The last phase is the payment phase in which the objective is to complete the transaction, through the payment to vendor and by providing the decryption key to customer. In this phase, the application used by the client builds an electronic payment order.

RESULTS AND DISCUSSIONS

Regarding the financial status, the funds credited to the merchant are accumulated and next these funds are periodically stored through VisaNet in the bank accounts of the various merchant. NetBill take a commission which varies between 2,5 cents for a 10 cents transaction and 7 cents for a 1 dollar transaction. NetBill ensure the main security services (confidentiality and security messages, identification and authentication of participants and acceptance). More, the NetBill transactions satisfy the following requirements of monetary transactions :

- *the atomicity*, which means that the transaction must take place as a whole of all effects that occur. The customer is billed only after he receives the goods and the payment leads to acces to goods delivered;
- *the consistence*, because many transactions are made in all respects purchase;
- *the separability*, which is given that the transactions are independent of each other;
- *the durability*, because each part has a record of the transaction

NetBill server behave as a third trusted part and also as an a arbitrator in resolving conflicts. Although the informations about the identity of the customer

are dissociated from the exchange of goods, the electronic payment order reveal to the vendor which is the identity of the vendor, and transactions can be viewed. Because the NetBill server intervenes in each exchange, this thing can be used to protect the customer identity. NetBill server intercept all of the customer messages to hide them before sending them to the merchant. The server can ensure the vendor's anonymity exactly in the same way.

CONCLUSIONS

In conclusion, NetBill presents interesting ideas (e.g., the electronic command or distinction between information delivery and acces to information), but the frequent use of digital signatures, especially public key signatures, tends to reduce performance commercial applications to a reasonable scale. Particularly, since the intervention of intermediaries (NetBill server) is required in each transaction, the number of transaction may be limited by the computational power available on the NetBill server.

Information security within an organization is extremely important for the good running of the company and therefore this domain of protection and security of data gains a major importance. More and more companies, even small and medium enterprises have started to implement a compartiment dedicated to information security. Even companies that are considered or were considered invulnerable in terms of a data security had big problems related to this issue, reach in the end to widely-accepted conclusion that no system is invulnerable.

BIBLIOGRAPHY

1. Bellare, M., et.all – *iKP Family of Secure Electronic Payment Protocols.*
2. Cox, B., 1994 – *Maintaining Privacy in Electronic Transactions*. Information Networking Institute Technical Report TR 1994-8.
3. Hashem Sherif, M. , 2000 – *Protocols for Secure Electronic Commerce*, CRC Press.
4. Cox, B., Tygar, J.D., Sirbu, M.,1998– *NetBill Security and Transaction Protocol*, Carnegie Mellon University.
5. Sirbu, M., Tygar, J.D., 1995 – *NetBill: An Internet Commerce System Optimized for Network Delivered Services*. IEEE Personal Communications, pages 6-11.