Fifth Int. Workshop on GNs, Sofia, 10 Nov. 2004, 41-47

MODELING OF E-TRADE WITH MOBILE COMMUNICATIONS BY THE APPARATUS OF GENERALIZED NET

E. Sotirova[1], H. Panayotov[1], M. Krawczak[2], P. Melo-Pinto[3]
[1] "Prof. Asen Zlatarov" University, Bourgas-8000, Bulgaria,
e-mails: {esotirova, itko}@btu.bg

[2] Systems Research Institute – Polish
Academy of Sciences, Wyzsza Szkola Informatyki Stosowanej i
Zarzadzania, Warsaw, Poland, e-mail: krawczak@ibspan.waw.pl

[3] CETAV – University of Tras-os-Montes e Alto Douro,
Ap. 1014, 5001-911 Villa Real, Portugal,
e-mail: pmelo@utad.pl

Abstract
It is introduced a generalized net model of WEB system for e-trade. By this model can be trace out and test different real systems basing on information transfer associated with the bank sector.

Keywords: Generalized nets, Mobile communication, E-commerce

Introduction

The term "e-trade" can be define like a turn to financial transactions in electronic way by using of the global network Internet by the help of WEB software, specially worked out for the purpose or from the other hand like direct purchase from online Web based shops, giving delivery of the goods or some virtual service [2, 4, 5, 8].

In the last years the number of these electronic shops grows up with fast speed. Meanwhile in a front position appears the security problem and transaction protection and the relationships realized in electronic way. More and more frequently in the world means of mass communications are published data for serious "out flows" of confidential information given from the client to the dealer. The affair in question is for personal data which is necessary to be bring in by the consumer while purchase – name, number of the credit/debit card, password, "expire date" /validity of the pay document/ and others. The vulnerability of this information continues to be one of the major problems impeding the normal development of this kind trade [6]. Of course question arises where the weak places of the security are and at what directions can be seek the new ways of its increasing.

The examinations indicate like most vulnerable transmission "client-WEB site". All measures for protection, no matter how tested are, do not give one hundred-required result. Incessantly are searched new way for increasing the security in data transportation not only in this area but in many other too, using the world network.

The expansion of the Network and growth of the number of users go in parallel with another phenomenon of the time we live – the mobile communication. The last years are characterized with real leap in this area. Gradually from a normal means for human communication they turn to a serious competitor of the Network integrating more and more the possibilities of the wireless communication with Internet technologies.

This in high degree is valid for the mobile communication means from third and four generation [7]. At the same time their possibilities regarding to the e-trade still can not approach to these of the standard personal computers like an element of the Internet and especially of the e-trade.

But they could be turn in an invaluable assistant for increasing the security in transportation of confidential data of the same type like in e-trade. Two are the factors determining this possibility. At the first place these are the security and coding of the transported information in GSM standard /voice, SMS, and et./ established in the developed countries. And second, this is extremely increasing of the users of this kind communication. The statistic data show that the number of GSM users exceeds already the number of the people using the Internet services, so the conclusion is that at least every client of e-shop has and GSM communication, the exceptions incline to zero.

This possibility could be used in "the narrow" regarding to the security places in the circuit client-dealer-Third Party Provider (TPP) and especially in the first transmission. In request or purchase of goods the client has to enter information for the way of paying /credit or debit card and its details/ (Fig. 1).

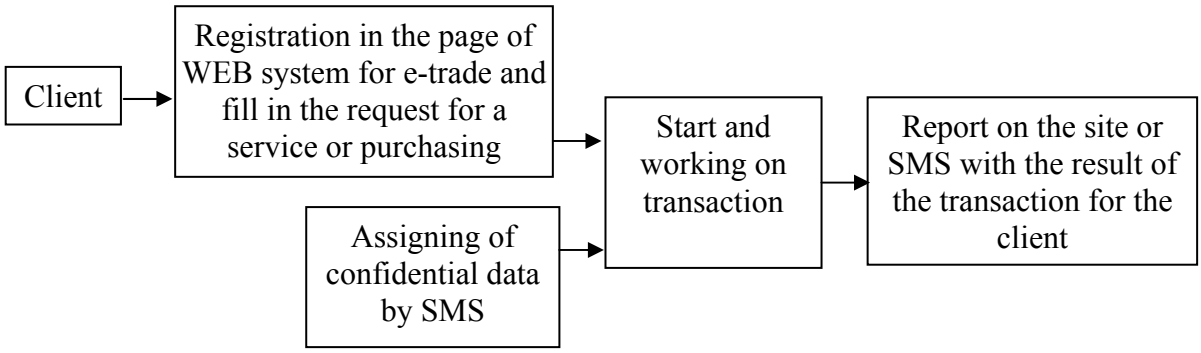

Fig. 1 Scheme of the e-payment by mobile communications

Exactly this process, the most vulnerable from the point of the security, could be turned into discreet by the help of the GSM communication. Instead of entering online whole the information about the purchase, the client can do a request for the desired goods followed of the address and name of the applicant, if it is necessary. The rest confidential data could just be "delivered" to the WEB site by the help of GSM. The realization of this scheme is not very complicated from hardware and software point of view. It is necessary the server of the WEB shop to be supplied with one GSM terminal and its respective program module in the WEB software for attendance of the arriving SMS from the clients.

So, in its registration in the e-shop the client has to enter only non confidential data like a kind of the chosen goods or service for purchasing, followed by name and address for delivery and obligatory a number of mobile telephone which CLIP /Calling Line Identification Presentation/ must be bound by the data for the request. WEB software has to do "invitation" to the user for sending the rest part /confidential/ from the information for realizing the transaction by TPP. It is enough by template at the screen to be given directions for the form and the contents of SMS expected by the WEB server, for example a number of the request /generalized by the site/, number of the paying means, validity, bank issued the card, password and et. and also the relevant dividers. Of course must be predicted a limit of time in which to be received the information and after transferring in it the transaction to be nullified. The receiving of that information from GSM terminal and its supplying with the others data starts the transaction to TPP. Depending on the result of the bank transaction – successful, card with expired time limit, different type REFFERAL /rejection because of shortage of resources or other reason/ the user is informed by a message on the site or SMS sent from GSM terminal of the server. For the permanent clients can be planned together with non confidential information in the base to appear a number of the telephone expected to start the transaction.

A GN-model

For modeling the described processes for e-pay by mobile communication, is used the apparatus of the generalized net (GN) [1]. The model is introduced at fig.2.

GN is the of transitions

$$A = \langle Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7 \rangle,$$

where the transitions describe the next processes:

- Registration of a client in the page of the WEB system for e-trade – transition Z_1;
- Filling the request for a service or buying goods - transition Z_2;
- Loading of the page with message about the form and the content of SMS – transition Z_3;
- Accepting of SMS from GSM terminal – transition Z_4;
- Checking the time for client's answer – transition Z_5;
- Starting and processing the transaction - transition Z_6;
- Deducing of a message with the result of the transaction – transition Z_7.

In [3] is developed GN model for e-payments. The transition Z_6 in GN model from the current development (Fig. 2) can be replaced by GN model [3] by applying of hierarchical operator H_3 from the theory of GNs [1].

Initially there is in one β-token that is located in place S_3 with initial and current characteristic

$$x_0^{\beta} = \text{"GSM terminal"}.$$

The clients of the WEB system for e-trade (interpret by α_i-tokens, $i = 1, 2, \ldots, n$), enter in the net through place N_1. They have the initial characteristic

$x_0^{\alpha_i}$ = “client i”.

The SMS from the clients of the WEB system for e-trade (interpret by β_i-tokens, i = 1, 2,…, n), enter in the net through place S_1. They have the initial characteristic

$x_0^{\beta_i}$ = “client i: SMS”.

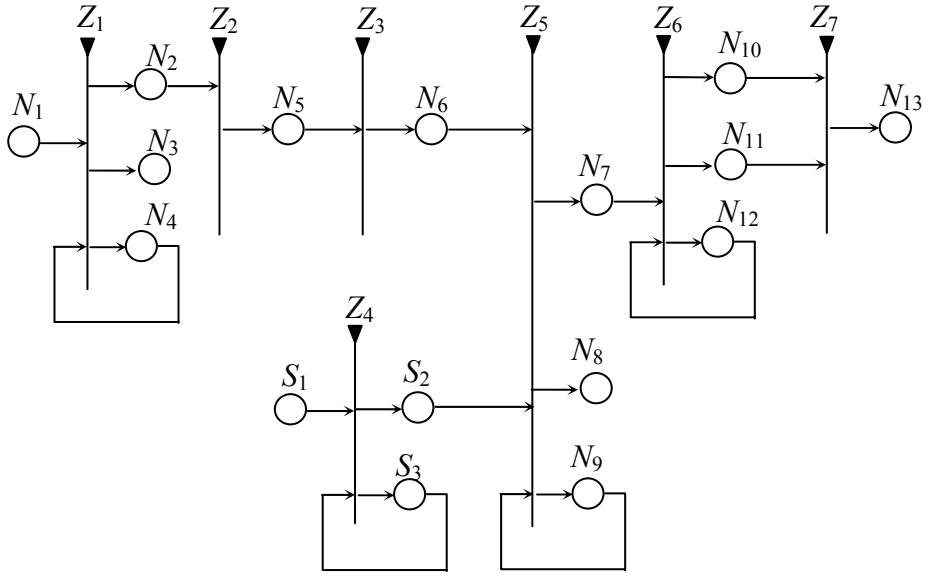

Fig.2 GN model of e-pay by mobile communications

The GN transitions have the following form. Everywhere i is the number of the clients of the WEB system for e-trade (for i = 1, 2,…n).

$$Z_1 = <\{N_1, N_4\},\ \{N_2, N_3, N_4\},\ \begin{array}{c|ccc} & N_2 & N_3 & N_4 \\ \hline N_1 & false & false & W_{1,4} \\ N_4 & W_{4,2} & W_{4,3} & true \end{array},\ \vee (N_1, N_4)> ,$$

where:

$W_{1,4}$ = “There is a new client for registration”,
$W_{4,2}$ = “A new client is registered”,
$W_{4,3}$ = “The registration of a client is reject”.

The tokens entering in place N_4 (from place N_1) not obtain new characteristics.
The tokens entering places N_2 and N_3 obtain characteristics respectively:

“client i”
and “client i: the registration is reject”.

$$Z_2 = <\{N_2\},\ \{N_5\},\ \begin{array}{c|c} & N_5 \\ \hline N_2 & W_{2,5} \end{array},\ \wedge (N_2)> ,$$

where:
$W_{2,5}$ = “There is filled request for buying goods or service”.

The tokens entering place N_5 obtains characteristic:

$$x_{cu}^{\alpha_i} = \text{“client } i\text{: request”}.$$

$$Z_3 = <\{N_5\},\ \{N_6\},\ \begin{array}{c|c} & N_6 \\ \hline N_5 & W_{5,6} \end{array},\ \wedge (N_2)> ,$$

where:
$W_{5,6}$ = “It is bring out a message about the content and form of the required SMS”.

The token entering place N_6 do not obtains new characteristic.

$$Z_4 = <\{S_1, S_3\},\ \{S_2, S_3\},\ \begin{array}{c|cc} & S_2 & S_3 \\ \hline S_1 & false & W_{1,3} \\ S_3 & W_{3,2} & true \end{array},\ \vee (S_1, S_3)> ,$$

where:
$W_{1,3}$ = “SMS is sent from a client to the SMS terminal”,
$W_{3,2}$ = “SMS is processed from the terminal”.

The tokens entering in place S_3 (from place S_1) not obtain new characteristics.

The tokens entering places S_2 obtain characteristic

$$x_{cu}^{\beta_i} = \text{“client } i\text{: confidential data”}.$$

$$Z_5 = <\{N_6, S_2, N_9\},\ \{N_7, N_8, N_9\},\ \begin{array}{c|ccc} & N_7 & N_8 & N_9 \\ \hline N_6 & false & false & W_{6,9} \\ S_2 & false & false & W_{2,9} \\ N_9 & W_{9,7} & W_{7,8} & true \end{array},\ \vee (\ \wedge(\ N_6, S_2), N_9)> ,$$

where:
$W_{6,9}$ = “There is prepared request”,
$W_{2,9}$ = “The data for a client from SMS terminal are processed”,
$W_{9,7}$ = “The request with the data of SMS are supplied for a client”,
$W_{7,8}$ = “The request for a client is nullified”.

The α- and β-tokens entering in place N_9 (from places N_6 and S_2) merge in γ-token with characteristic

$$x_{cu}^{\gamma} = \text{"} x_{cu}^{\alpha_i} \cup x_{cu}^{\beta_i} \text{"}.$$

The tokens entering in place N_7 not obtain new characteristic.

The tokens entering in place N_8 obtain characteristic
"client *i*: nullified request".

$$Z_6 = <\{N_7, N_{12}\}, \{N_{10}, N_{11}, N_{12}\}, \begin{array}{c|ccc} & N_{10} & N_{11} & N_{12} \\ \hline N_7 & false & false & W_{7,12} \\ N_{12} & W_{12,10} & W_{12,11} & true \end{array}, \vee (N_7, N_{12})> ,$$

where:
$W_{7,12}$ = "The transaction for a client's request is started",
$W_{12,10}$ = "The successful transaction for a client's request is done",
$W_{12,11}$ = "The transaction for a client's request is unsuccessful".

The tokens entering at places N_{10}, N_{11} and N_{12} obtain characteristics respectively:
"client *i*: request, successful transaction",
"client *i*: request, unsuccessful transaction"
and "client *i*: request".

$$Z_7 = <\{N_{10}, N_{11}\}, \{N_{13}\}, \begin{array}{c|c} & N_{13} \\ \hline N_{10} & W_{10,13} \\ N_{11} & W_{11,13} \end{array}, \vee (N_{10}, N_{11})> ,$$

where:
$W_{10,13} = W_{12,10}$,
$W_{11,13} = W_{12,11}$.

The tokens entering at place N_{13} receive characteristic
"client *i*: result of the transaction".

Conclusion

The developed GN model gives a possibility to be traced and tested different real systems based on information transfer in relation with the bank sector.

References

1. Atanassov, K. Generalized Nets, World Scientific. Singapore, New Jersey, London, 1991
2. Nenov, A., S. Sotirov, Protocols and standards for E-commerce, International Conference Computer Systems and Technologies, Sofia, Bulgaria, 2000, 4071 - 4075, ISBN:954-9641-17-1

3. Kodogiannis, V., S. Sotirov, A. Nenov, Modelling of Electronic Payment by Generalized Net, 10th ISPE Int. Conf. on concurrent engineering: research and applications, Madeira Island - Portugal, 26 - 30 JULY, 2003, pp. 1043-1046, ISBN 905809622X.
4. Lelieveldt, S. Research study on the integration of e-payments into the online transaction process, http://www.simonl.org/index.html/epsosum.htm
5. eServices, eComPay – Authenticated ePayments, http://ecompany.ae/eco/isp/english/services/e-payment/ecompay/payments.html
6. Ghosh, A., "E-Commerce Security:Weak Links, Best Defenses", Published by John Wiley & Sons ISBN 0-471-19223-6, 1998
7. Renfoe, D. "Mobile Messaging Gateways" – Review, 2005
8. Fingar, P., H. Kumar, T. Sharma, "Enterprise E-Commerce"