Intelligent Circumstance Aware Mechanism: A New Approach toward Secure Online Transactions

Arash Salehpour and Mohammad Ali Sharifloo

***Abstract*—In the world of online payments, preservation of accounts vital information in the state of interaction between server side and client side is one of the major issues, for both purchasers and global payment companies. This paper present an intelligent Mechanism, which have a device that owned by customers to have a safer transacts with the banking systems. A unique finger print recognition unit and a built in hashed serial number is used instead of The card serial numbers, The process of authorization is done by a questioner unite that asks randomly questions related to customers private data in the bank database to admit he/she to access to the system, and these sections combined with an intelligent software that exists in the payment gateway to detect the suspiciousness and inform the server to abort the connection. During the process, server and device communicate each other in a fully secured cryptographic manner's and protected real-time protocols. With these systems we sight to solve the linear ways that all users in all situations are equal for the payment gateways, and conduct with end users with an attended of a real time circumstance.**

***Index Terms*—Credit card transaction, payment system, security, internet shopping, security, mutt factor authentication.**

I. Introduction

Online transactions are an inseparable process in people's life within the information technology age. Traditional shopping swiftly supplants by online interaction methods in most of populations all over the universe. Preservation of accounts critical information, authentication and authorization are the major issues that service provider companies confront it, since the time that these technologies take place in people's life. Most banking systems act in traditional and linear ways that request some codes which is placed on the card and the password. This method have low security in authentication, the man who have the password, is the man who is account owner- with the sight of the security server-. To solve this problem some researchers use biometric authentication systems. user who attempt to Data theft, the user who steal the card and obtained password, the user who want trans act 1 dollar, the user who want trans act 10 thousand dollar, and so on are same for the gate ways and no increasing security policy appear, and the security walls can go harder and harder in threat situations. In order to protecting the customers bank accounts, within our method ICAM (Intelligent circumstance aware Mechanism), we introduce two major components. The device that we must deliver to the customer which we introduce it in section 3, and the intelligent circumstance aware software in transaction doorway for observing and informing the server for decision making , in order to update the security policies. It can be an intelligent security agent that the bank delivers to customer's computer. The Composition of the built in real time genera table code that we placed in the device (in production process), and the hashed code that we generate from the finger print recognition, is used instead of the credit card numbers.

Manuscript received June 16, 2012; revised July 1, 2012.

The authors are with the Dept of Computer, Faculty of Engineering University College of Nabi Akram,Tabriz, Iran.

A. Focus

Under the heading of intelligent circumstance aware mechanism, our main focus is on intelligent methods that can prevent attacks against banking accounts vital information such as Eavesdropping, Data theft, Illegal Use of another peoples account. The Remainder of this paper is organized as follows. Section II introduces common related works approaches including virtual credit card number, master card secure code. The purposed method is presented in Section III; and conclusion will follow in Section IV.

II. Related Works

We briefly introduce some popular secure mechanisms that now used all over the world. For this section we introduce the Virtual Credit card number and master card secure code and due to the popularity of them in the real world

Fig. 1. A usual authorization cycle.

A. Virtual credit Card Number

In this approach, a credit card holder is assigned a virtual credit card that shares the same account as the card holder's physical credit card. It can be used in online transactions as a traditional credit card until its expiry date.

The virtual card has a card number, a CVC number, an expiry date and a flexible monetary limit that can be redefined by the user prior to a transaction and reset periodically. The advantage offered by a virtual credit card is that, even if the credit card number is stolen together with other details, it cannot be used until the user redefines a new temporary limit for a new transaction. [1].

B. Master Card Secure Code

The approach is based on the protocol called 3D secure `verified by visa' and `master card secure code' In its initial form, 3DS would pop up a password entry form to a bank customer who attempted an online card payment; he/ she would enter a password and, if it was correct, would be returned to the merchant website to complete the transaction. Difficulties arose with pop-up blockers and now the recommended mode of operation uses inline-frames (`iframe'). The merchant passes the card number to [2].Visa or MasterCard, and gets back a URL to embed in an iframe to display to the customer. If the customer executes the protocol successfully, the merchant gets an authorization code to submit to his bank. [2].

III. Proposed Mechanism

The main focus here is on the intelligent behavior of this mechanism. The ICAM (Intelligent circumstance aware mechanism) consist of three major components that working together:

1) A device which it has a special program that fully matched with the bank web server.
2) An intelligent software which is placed on the Trans action doorway for observe the user environment.
3) An expert system that placed on server side for making the decisions and send it to ICAM's Device and Doorway software.

With the help of this method, we are planning to detect the suspicious conditions that appear in the users host machine, and update the security policies, in order the behavior of the user. For example a user run a hacking program in his environment and wants to attack the system.

The program which installed in payment door way with the help of OS observer mechanism can detect and feed it back to server, for rupture the connection.

We can Solve the linear ways that is usual in most of banking systems-which seen the all users in all situations in a same vision-with the help of ICAM's Device, The device conation's a screen for both I/O operations. And we can update the security policies with the wide range of flexibility.

According to the user specifications and transaction characteristics, (In custom range of user) The banks system, give it's users the device, and when ever the user want to trans act, his/her finger print is his/her identification for authentication.

Here we are proposing a usual Trans act scenario with the help of The ICAM

1) The ICAMS Device connect within the usb port to the portable software that placed in the use computer or in P.O.S operating system, the portable software starts automatically detecting the trans action doorway and connect to it.
2) With the help of doorway program, and device built in program, the two component start handshaking, and the device date and time matched with the server's date and time. -in a special format and encrypted format that the human cant read it – this date and time is one of our important keys that will being mixed with a unique function with the fingerprints output serial.
3) Encrypted code will be sending in this section, the encryption key definite in handshaking level and every time when the Trans act done, the key will be change.
4) IF the encrypted serial is true and the software that place on doorway don't report any malicious situations the trans act will be complete successfully.
5) IF any dangerous situation reported by the doorway software or the device. the security policy updates and go to next level that the questioner screen ask about one of the private data's of the user likes passport ID and this process continue with 3 level of security. If all of the questions have wrong answers the device destroyed itself, and reports the bank for the fault.
6) For the security levels we have wide range of actions like send a sms to user for give permission and so on.

The above process is an ordinary process; all the process can be flexibly change with the user's specification, transaction amounts, and so on.

A. Questioner Screen

A screen that placed in front of the ICAM's device is an touch screen LCD monitor that the bank web server can communicate with its users, in a creatively way, all the inputs from user can taken by the virtual keypad that appear on the screen The existence of screen is necessary, we sight to design the doorways which have no computer aided systems like the P.O.S and they have only usb or phone line ports and don't aim of the computer screen in the shopping centers this work will place on our future works.

B. Cient/Server Comunication

The Connection between ICAM's Device and the web server of the banks server possible trough fully encrypted secured cryptographic layers, with the technologies of the secure socket layer .Each device have a different certification built in on it, and can be updated with the bank in fault situations or within a specific periods.

C. Desicion Making Policy

The major section of decision making is about the security policy updates. Trans action health is done by server side application .the decisions made by the Expert system is based on the information's which sent by the door way software, and ICAM's Device We want to use an expert system in our server side for decision making process. The primary goal of expert systems research is to make expertise available to decision makers and technicians who need answers quickly. One of the most key factors in human intelligence is the capacity of evolution and adaption in different and changing environments [3]. The focus here is on Fuzzy Rule-Based Systems using a predefined database [4].the survey on DB (Data Base) take place in our future works.

D. Security Policy

With this work the banking systems have a wide range of different security manners to provide to there users, the users who wants to trans act 1 dollar through the users that wants trans act 100.000 dollar daily, policies can go harder and harder through the situation occurred in users environment. The decisions made by server side expert systems which order the ICAM's to do the updated rules.

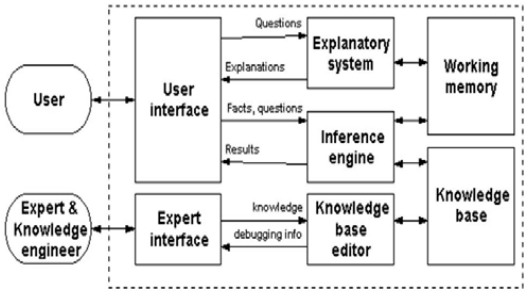

Fig. 2. Expert systems mechanism.

E. Observing the Enviroment

The observer asks OS to provide it with the events occurring in the environment. It then classifies those deleting unrelated and unimportant ones.

F. Door Way Software Specifications

Doorway software is a connection bridge between the server side and the client side computer and ICAM's device, the observer section of ICAMS device repeatedly observe and search the host environment and inform the server about the status.

G. Intelligent Decision Making

The focus here is on Fuzzy Rule-Based Systems using a predefined database [5]-[8]. In these systems, database has a significant influence on decision making process. The learning method will automatically fill the knowledge base, (by finding an appropriate database by means of a genetic algorithm). While using a simple generation method to derive the rule base [9]. The capability of observing the user environment to detect the malicious behavior is a powerful component of system for gathering information and modification the database and knowledge base. A rule means a structure which has an "if" component and a "then" component. The knowledge base contains all the rules and critical conditions that we make it, and send it to the user's machine. This knowledge base is known as our primary knowledge base. The rules must update themselves in the conditions of the host machine, by our observing technology, which generates an adopted knowledge for our decision making system. Decision makers combine different types of data (i.e. internal and external data) and knowledge (i.e. tacit and explicit knowledge) available in various forms in its external environment. However this task is made extremely difficult by the uncertainty affecting decision-making processes [10]. We use fuzzy logic in our work, for the vital decisions making through the continuous execution of transaction. Fuzzy logic is a superset of conventional (Boolean) logic that has been extended to handle the concept of partial truth ± truth values between "completely true'' and "completely false'' [10].

IV. Conclusion and Future Work

The usual systems and mechanisms that now popular in the world in most cases behave as a linear and barren way, the behavior of the users and all the situations that can occur through the trans actions, is a significant matter in security polices real-time update and adoption, they must effect the trans action health automatically. Design of the expert system for decision making, and generate rules for it. Door way software challenges and the ICAM's Device electronically sides are all the challenges that we face on in our future work.

Fig. 3. Card codes.

References

[1] M. Umamaheswari, S. Sivasubramanian, and B. Harish Kumar, "Online Credit Card Transaction Using Finger Print Recognition," *International Journal of Engineering and Technology* vol. 2, no. 5, pp. 320-322, 2010.

[2] S. J. Murdoch and R. Anderson, *Verified by Visa and master Card Secure Code: or, How not to Designauthentication Financial Cryptography and Data Security '10*, Tenerife. vol. 25, no. 28, January 2010.

[3] R. R. Yager "Learning methods for evolving intelligent systems," *Evolving Intelligent Systems: Methodology and Applications*, Edited by IEEE 2010.

[4] J. A. Bardossy and L. Duckstein, "Fuzzy Rule-Based Modeling with Application to Geophysical, Biological and Engineering Systems," Boca Raton, FL: CRC, 1995, R. Nicole, J. Name Stand. Abbrev. in press.

[5] Y. Jing, "On-line Payment and Security of E-commerce," in *Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang*, P. R. China, May 22-24, 2009, pp. 046-050.

[6] A. Hiltgen, T. Kramp, and A. Weigold, "Secure internet banking authentication," *Published by the IEE Computer Society*, 1540-7993/05/$20.00 © 2005 IEEE

[7] O. Cordón, F. Herrera, and P. Villar, "Generating the Knowledge Base of a Fuzzy Rule-Based System by the Genetic Learning of the Data Base," *IEEE Transactions On Fuzzy Systems*, vol. 9, no. 4, August 2001

[8] A. Bardossy and L. Duckstein, *Fuzzy Rule-Based Modeling With Application to Geophysical, Biological and Engineering Systems*, Boca Raton, FL:CRC,1995.

[9] M. N. Gagnon, S. Taylor, and A. K. Ghosh, "Software protection through anti-debugging," *IEEE Computer Society*, 1540-7993/07© 2007 IEEE.

[10] K. Metaxiotis, J. Psarras, and E. Samouilidis, *Integrating Fuzzy Logic into Decision Support Systems: Current Research and Future Prospects*, Decision Support Systems Laboratory.

Arash Slehpour is B.Sc. (computer science –software engineering- junior student in University College of Nabi akram ,Tabriz Iran, He has worked as Program Committees, reviewer at numerous international conferences such as : The International Conference on Informatics Engineering and Information Science (ICIEIS2011), University Technology Malaysia, Malaysia, The World Congress on E-Commerce and Business on the Web (WCEBW2012), United Kingdom and …, The areas of his Research and Interests include: Examines both automatic systems and collaborative systems as well as computational models of human software Engineering activities, Presents knowledge representations and artificial intelligence techniques as well as, he is already acts as member in numerous international organizations such as: The Society of Digital Information and Wireless Communications (SDIWC).

Mr. Mohammad ali Sharifloo received his B.Sc. from Azad University of Ghazvin and his M.Sc. from Azad University of Tehran. Currently he is master at University College of Nabi Akram. His main research interests are IT, Distributed Systems, Real-time Systems and Formal Verification.