Journal of Engineering and Applied Sciences 2 (5): 846-848, 2007

A Proposed Theory of Using Finger Print as the Primary Tool of Biometrical User Authentication in an OLTP System under Heterogeneous Environment

[1]Vidyaathulasiraman and [2]S.P. Rajagopalan
[1]HOD/MCA, Priyadarshini Engineering College, Vaniyambadi-635751, India
[2]Satak Group of Institutions Chennai, University of Madras, Chennai-600005, India

Abstract: This study proposes the use of finger print as the only biometrical user authentication in a simple ECMA authentication model proposed for a heterogeneous environment in an Online Database Transaction Processing (OLTP) system. An algorithm is proposed in this study which uses finger print scanning as the primary tool for biometrical user authentication and is expected to assure security to high level resources, where there is no much physical security. The study presents the existing authentication models and an analysis is made to justify finger print as the best suitable model among them, for OLTP systems under heterogeneous environment.

Key words: Authentication, distributed systems, internet, e-commerce, security control, biometrics, smart cards, finger print

INTRODUCTION

Network Security has gained a great importance in the recent years. In olden days only the academics and other research-oriented people used internet for e-mail or file access/exchange. So the need for building a secured network was not of high priority. But with the application of internet in almost all the fields, especially when highly confidential matters and financial matters are dealt, the need for network security is recognized.

Layering of the security devices go on, depending on the information being protected and the degree of determination of the attacker (Patrick and Bulent, 1999). A goal of a security system is to increase the cost an attacker must pay in terms of financial or technical effort, in attacking a system to the point where it is no longer cost effective. Careful measurement and planning in the software security development process is needed to assure adequate integrity and reliability (Kenneth, 1986). Computer security solutions must be tailored to the specific needs of a particular installation (Jack, 1986). Justification is made on the use of hardware-based equipment in security would be much advantageous, as unauthorized modifications will be practically more difficult and support automatic monitoring (Charles and Howard, 1986). For keyboard model input from the user, the authentication schemes described in the literature use exact arithmetic based on finite fields for designing cryptographic algorithms and protocol (Bellare and Goldreich, 1993; Brickell, 1993; Feigenbaum, 1992; Guilou *et al*., 1992; Imai and Rivest, 1993; Mitchell *et al*., 1992; Landwehr and Jajodia, 1992; Preneel and Govaerts, 1993; Seberry and Zheng, 1993; Simmons, 1992; Waleffe and Quisquater, 1993). It is shown (Rodnicky, 1993; Murthy and Krishnamurthy, 1994; Vidyaathulasiraman and Rajagopalan, 2005, 2007) that the biometrical modes of impact is gaining importance in the present day scenario. Designing user authentication schemes to provide security control for an OLTP system has become one of the major research area (Landwehr and Jajodia, 1992; Murthy and Krishnamurthy, 1994, 1993).

Many online transaction processing systems in a distributed environment such as E-Marketing, Banking, Stock-Broking, etc., had been developing, where a high level of security is expected. The proposed algorithm uses an interface device (hardware) for finger print scanning which is used in the authentication process in an OLTP system.

A REVIEW ON AUTHENTICATION MODELS

The ECMA simple authentication model (Murthy and Krishnamurthy, 1994), is:

Step 1: A → B: A, Ksa
Step 2: B → Au: A, Ksa
Step 3: Au → B: b
Step 4: B → A: Ksa

Where A is the name of the initiating client, B is the name of the recipient or server Au is the authentication service,

Corresponding Author: Vidyaathulasiraman, HOD/MCA, Priyadarshini Engineering College, Vaniyambadi-635751, India

Ksa is A's simple key and b is a Boolean variable which indicates whether or not Ksa is A's simple key.

The restriction here is there needs to be a per transaction or session an authentication performed, which is of the form

A → Au: Pwd
Au → A: Ksa

Where Pwd is some token for authenticating A. Since both Ksa and Pwd are plain text, intruders can easily read the information.

An enhancement over (Murthy and Krishnamurthy, 1994) is (Vidyaathulasiraman and Rajagopalan, 2007) in which the Ksa is replaced as the biometrical characteristic of authentication and Au as the biometrical way of authentication scheme. And it is represented as follows:

Step 1: S → B : b
Step 2: B → Au: U, Res
Step 3: Au → B: Req S,b
Step 4: B → U: Rst

Where S-Smart Card, B-Processor/Server/recipient, U-User, Res-Response, Rst-Result (a Boolean variable Accepted-T, or Rejected-F), Au-Authentication Service and B-the random characteristics of the user selected for authentication proposed by the smart card.

Note : The above specified process is repeated at the start of every new process/transaction.

PROPOSED MODEL

The proposed model throws light on the flaws that may crop-up in (Vidyaathulasiraman and Rajagopalan, 2007) in which the smart card usage is stressed. Of-course the usage of smart cards do offer certain advantage, such as even if the card falls in the hands of an imposter/intruder, he/she has to prove their identity for using the card (as the contents in the smart card and self should match). But the constraint in this method is smart card has to be carried physically along with the client. Also in this method the processor just acts as an interface between the client and the smart card. Also the system had to be equipped with more than a single interface device. So a need for enhancement is recognized.

Assumption: The biometrical authentication scheme proposed here is finger print. The details of the finger print of all the authorized users are stored in the server. A special component is attached to all the systems, which is used to scan the finger print, during authentication.

Algorithm:

Step 1: A → B: A, RRT
Step 2: B → A: Req
Step 3: A → B: A, Ksa
Step 4: B → Au: A, Ksa
Step 5: Au → B: b
Step 6: If (b) Then B → A: RRT
Else B → A: DEM.

Where A is the name of the initiating client, B is the name of the recipient or server, RRT is the requested resource/transaction, Req is the Request for finger print of A, Au is the authentication service, Ksa is A's finger print and b is a Boolean variable which indicates (yes/no, that is whether Ksa is A's finger print or not)and DEM is Displaying an Error Message.

The restriction here is there needs to be a per transaction or session an authentication performed, which is of the form

Algorithm description:

- A initiates a request to B, asking for a resource or for the execution of a transaction.
- For which, B challenges A to provide the finger print through the special equipment provided.
- A then responds with appropriate action, so that Ksa- can proceed to certify whether the user is genuine.
- B then executes the authentication sevice (Au), which compares A's finger print with the finger prints that are stored in the system database.
- Au submits the result of the matching process to B in b.
- If b is true, B proceeds to supply the requested resource/transaction to A. If b is false the system produces an error message to A.

Note: The above specified process is repeated at the start of every new process/transaction initiated by any client(A).

CONCLUSION

The greatest advantage here is practically the people need not carry any card nor had to remember their password, as it is in-born with them. The time taken for processing a finger print is less than a minute. So this is highly advantageous for automated environment and in which the authentication process had to be performed often. Thus the proposed method is expected to ensure

greater level of security for an OLTP system under heterogeneous environment, where it involves securing high level resources, where there is no much physical security.

REFERENCES

Bellare, M. and O. Goldreich, 1993. On Defining Proofs of Knowledge in Advances in Cryptology, LNCS 740, Brickell, E.F. (Ed.), Springer-Verlag, pp: 390-420.

Brickell, E.F., 1993. Advances in Cryptology- CRYPTO'92, LNCS 740, Springer-Verlag.

Charles, C.W. and H.M. Zeidler, 1986. Security modules: Potent Information Security System Components, Computer Security. Elsevier Sci. Pub. B.V., 5:114-121.

Feigenbaum, J., 1992. Overview of Interactive Proof Systems and Zero-Knowledge, In: Contemporary Cryptology. Simmons, G.J. (Ed.), IEEE. Press, pp: 423-439.

Guillou, L.C., M. Ugon and J.Quisquater, 1992. The Smart Card, in Contemporary Cryptology. Simmons, G.J. (Ed.), IEEE. Press, pp: 561-613.

Imai, H. and R.L. Rivest 1993. Advances in Cryptology-ASIACRYPT'91 LNCS 739, G Springer-Verlag.

Jack, G.J., 1986. Random Bits and Bytes: A plea for professional responsibility, Computer Security. Elsevier Sci. Pub. B.V., 5: 383-384.

Kennneth O., 1986. Computer Security: IFIP Addresses Practical Issues, Computer Security. Elsevier Sci. Pub. B.V., 5: 68-73.

Landwehr, C.E. and S. Jajodia, 1992. Database Security, IFIP Processing, Elsevier, New York.

Mitchell, C.J., F. Piper and P. Wild, 1992. Digital Signatures, in Contemporary Cryptology. Simmons, G.J. (Ed.), IEEE. Press, pp: 325-378.

Murthy, V.K. and E.V. Krishnamurthy, 1993. Knowledge-Based Key-Hole Monitoring of Users for Security Control in Transaction Processing Systems, Proceedng SICON Conference, Singapore.

Murthy, V.K. and E.V. Krishnamurthy, 1994. Knowledge-Based Security Control for On-line Database Transaction Processing Systems, ACM SIGSAC Review.

Patrick, W.D. and Y. Bulent, 1999. Network Security, IEEE. Network, pp 10-12.

Preneel, B. and R. Govaerts, 1993. Computer Security and Industrial Cryptography, LNCS 741, Springer-Verlag.

Rodnicky, A.I., 1993. Mode preference in a simple data retrieval task. In: Proceeding of the Arpa Workshop on Human Language Technology, Morgan Kaufmann, CA.

Seberry, J. and Y. Zheng, 1993. Advances in Cryptology-AUSCRYPT'92, LNCS 718, Springer-Verlag.

Simmons, G.J., 1992. Contemporary Cryptology, IEEE. Press.

Vidyaathulasiraman and S.P. Rajagopalan, 2005. A proposed theory of using Biometrical User Authentication in an OLTP system under Heterogeneous environment, in National-Workshop on Cryptography, organized by CSI and JNNCE, during the year 2005 at Shimoga.

Vidyaathulasiraman and S.P. Rajagopalan, 2007. A proposed theory of using Biometrical User Authentication via Smart Cards in an OLTP system under Heterogeneous environment. Asian Journal of Information Technology.

Waleffe, D. and J. Quisquater, 1993. Better Login Protocols for Computer Networks, in Computer Security and Industrial Cryptolography, LNCS 741. Preneel, B. *et al.*, (Eds.), Springer-Verlag, pp: 50-70.