Asian Journal of Information Technology 6 (2): 207-208, 2007

A Proposed Theory of Using Biometrical User Authentication Via Smart Cards in an OLTP System under Heterogeneous Environment

[1]Vidyaathulasiraman and [2]S.P. Rajagopalan
[1]HOD/MCA, Priyadarshini Engineering College, Vaniyambadi-635 751, India
[2]Advisor-Md. Satak Group of institutions and (Former) Dean, College Development Council, University of Madras, Chennai-600 005, India

Abstract: This study proposes a technique of using biometrical user authentication in a simple ECMA authentication model proposed for a heterogeneous environment in an Online Database Transaction Processing (OLTP) system. An elaborated view of the ECMA authentication model is discussed. Significance of using biometrical authentication is brought about. An algorithm is also proposed in this study, which is expected to assure security to high level of resources, where there is no much physical security. Thus we conclude that the proposed technique would be a challenge to the hackers.

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

INTRODUCTION

Distributed systems have gained more importance in the recent years, with the advent of internet and e-commerce, security is a major threat in a distributed computing environment. 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). 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 protocols (Bellare and Goldreich, 1993; Brickell, 1993; Feigenbaum, 1992; Guillou *et al*., 1992; Imai and Rivest, 1993; Mitchell *et al*., 1992; Preneel and Govaerts, 1993; Seberry and Zheng, 1993; Simmons, 1992; Waleffe and Quisquater, 1993). It is shown (Rodnicky, 1993) that the biometrical modes of impact is gaining importance in the present day scenario, where everyone moving towards the age of sophistication. Smart cards which allows to store more than one property/attribute (such as speech, handwriting and finger prints) of a specific person, is gaining more importance in the area of authentication.

On the other hand ECMA is currently working on a draft proposal for authentication (Rank Xerox Contribution, 1984) based largely on the earlier papers by Needham and Schroeder (1978), Israel and Linden (1983). Two forms of authentication are proposed in the ECMA document, Strong and Simple. "Strong" form resists attacks, but introduces computational delays at execution time, whereas "Simple" is fast.

EXISTING MODEL

According to Murthy and Krishnamurthy (1994) the ECMA simple authentication model is

A → B:A,Ksa
B → Au:A,Ksa
Au → B:b
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, 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.

PROPOSED MODEL

The proposed model is a modification brought over the "Simple" ECMA model. In the proposed model we replace Ksa as the biometrical characteristic of authentication and Au as the biometrical way of authentication scheme over the "Simple" ECMA model.

Corresponding Author: Vidyaathulasiraman, HOD/MCA, Priyadarshini Engineering College, Vaniyambadi-635 751, India

ASSUMPTION

The biometrical characteristics of the user is stored in a Smart Card. A reliable interface unit for Smart card is made available in the system. The server B contains an Authentication service Au, which contains a user's biometrical character database, which is used during authentication process, to compare with the characters stored in the smart card.

Algorithm

Step 1 : B → S, Ci,Cv
Step 2 : B → Au : Ci,Cv
Step 3 : Au → B : b
Step 4 : B → U : Rst

Where S-Smart Card, B-Processor/Server/recipient, Ci/Cv- is the ith biometrical character/value of the user, which is stored in the smart card, U-User, Rst-Result [a user's process request is accepted/rejected], b - a Boolean variable Accepted-T, or Rejected-F, Au-Authentication Service.

ALGORITHM DESCRIPTION

- For each transaction the server B selects a random word from the smart card, which is actually a representation of one of its user's characteristic and its associated value.
- B then submits the results of step 1 to the authentication service Au, which.checks for the particular biometrical characteristic match with its users biometrical character database.
- The authentication service declares whether the match performed in step 2 was a success/failure (i.e., the database entry and the smart card entry for a particular user, for a particular character, matches/ does not match).
- Based on the b value (success/failure) from step 3, the user's request is accepted/rejected for processing.

Note: The above specified process is repeated at the start of every new process/transaction in an Online-transaction processing system under heterogeneous systems.

CONCLUSION

Thus the proposed method is expected to ensure greater level of security for an OLTP system under heterogeneous environment. It is applicable to secure high level of resources, where there is no much physical security. So we conclude that the proposed technique would be challenge to the hackers.

REFERENCES

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

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

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

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

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

Israel, J.E. and T.A. Linden, 1983. Authentication in office system Internetworks, ACM. Trans. Office Inform. Sys., 1: 193-210.

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

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

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

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

Needham, R.M. and M.D. Schroeder, 1978. Using Encryption for Authentication in large Network of Computers, CACM 21, 12: 993-999.

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

Rank Xerox Contribution, 1984. ECMA Authentication Service Standard-Draft proposal.

Rodnicky, A.I., 1993. Mode preference in a simple data retrieval task, in Proc. 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.

Waleffe, D. and J. Quisquater, 1993. Better login protocols for computer networks, In: Computer Security and Industrial Cryptolography, LNCS 741, (Ed.), B. Preneel *et al*., Springer-Verlag, pp: 50-70.