IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 9, July 2010
ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

Implementation of 'Habit sensitive login system' An approach to strengthen the login security

Nishikant C Dhande
School of Commerce and Management Sciences,
Swami Ramanand Teerth Marathwada University, Nanded
Maharashtra India

Abstract

Providing reliable security to the computer user without overstepping any of the privacy related issues is the biggest challenge faced by the computer technologists now a day. An attempt is made herein to tailor a solution based on the personality features of an individual as a factor of identification and authentication. The traditional approach based on verification of the username and the password is insufficient. Hence, a new approach is needed to be introduced so as to make the existing login process more secure. To achieve the goal one can use the advantages of data mining techniques as well as the algorithms similar to the apriori algorithm. The suggested method is based on detection of intrusions at the time of logon. The system so designed; not only by verifies the username and password but also verifies the user's behavior in comparison with the 'recorded normal behavior' of the user. The experiments carried herein are fruitful in recognizing the user by their 'habits as behavior'. And hence the system based on the approach is practicable in real sense.

Keywords: *security, user behavior, habit, apriori algorithm, data mining, intrusion detection.*

1. Introduction

Providing good security to the user without overstepping any of privacy related issues is the biggest challenge faced by the computer technologists now a day. Although there are many options available, the objections and the controversy follow with the invention hand in hand. A very recent issue is of the security system introduced and implemented by 'Google' based on 'Face Identification' technique. This technology is hot debated and strongly argued world wide as a move against the privacy of the user.

An attempt is made herein to tailor a solution based on the personality features of individual as a factor of identification and authentication.

1.1 Problem Definition

The present available security methods are based on the traditional login system that allows 'authentic' (normal) user to gain access to his/her account after providing the 'username' and 'password'. The traditional approach is insufficient with reference to the security provisions. Hence, a new approach is needed to be introduced so as to make the existing login process; more secure. To achieve the goal one can use the advantages of data mining techniques as well as the algorithms similar to the apriori algorithm[2].

Research Objectives and Hypothesis

To perform the research on the issue, following objectives are decided

1) To study the present Intrusion Detection Systems (IDS).
2) Identify limitations of IDS.
3) Design and develop new logon system.
4) To test and evaluate the performance of newly designed IDS.

To implement the system following assumptions are made-

1) Hypothesis 1 H_0 – User's behavior can be detected in the forms of 'events' as a series of the activities carried by the user as a habit.

2) Hypothesis 2 H_0 – Anomaly if any, can be detected by studying the behavior of the user with the help of the Data Mining Techniques.

3) Hypothesis 3 H_0 –The system based on the new approach helps to solve problem of intrusion at

logging in process by providing more security to the authentic user.

1.3 Research Strategy-Design and Creation

According to the research methodology [1] "*Design and Creation*" is carried out in this research attempt. It focuses on developing new IT product which is also called as "*artifacts*". Types of IT artifacts such as [March & Smith, 1995] *Constructs, Models, Methods* such as Soft Systems Methodology (Checkland & Scholes, 1990) or Information Engineering (Martin, 1989), *Instantiations.*

In general, the research for the IT application focuses mainly on-

1. IT application that uses IT in a new domain, which has not previously been automated.
2. IT applications that incorporate a new theory, which may be drown from other discipline.
3. IT application that expresses or explores novel artistic ideas.

While searching for exploration of new ideas, an approach is accepted by combining various data mining techniques. For tailoring the solution to the problem of security regarding authentication and prevention from any unauthorized access techniques such as association, clustering in the Intrusion Detection System at login time are prefered.
The tools used here are the Visual Basic and the data base for the verification of the idea and to find out the feasibility of the implementation of the idea.

This activity focuses on designing of an improved Information System (IS). This kind of approach was not been taken earlier for detecting the anomaly using data mining. It is an attempt towards design and creation of new IS product to give good security to the user at the time of the user login for any system[3].

1.4 The Method suggested for the implementation of the idea:

The suggested method is based on detection of intrusions at the time of logon. To achieve this, the system designed not only verifies the username and password but also verifies the user's behavior in comparison with the recorded normal behavior of the user (or profile). The behavioral practices and the habits displayed by the user are to be recorded and stored into the database. The database is updated time to time. The behavior refers to **"the sequence of events/actions that are performed intentionally and/or unintentionally by the user at the time logon process"**. From this, the behavioral profile, event sequence set that contains one or more of such events is obtained for the normal user.

The output of the proposed system is the sequence of events; termed as *eventsequence* detained from user at logon time. On this *eventsequence,* Apriori Algorithm is applied so as to obtain the **"strongest association rule(s) between most frequently occurring events"**. The system so designed thus makes it possible for leading to the decision **'whether or not to allow access permission to user'** for the session further. The decision is taken by comparing current user's events/actions that are generated at the time of each logon with the strongest rules produced from profile database by the algorithm. In this way, the proposed system becomes capable to detect intruder before logon into the system.

1.5 Normal User's Profile Database

Of course, to achieve the goal in this regard, one has to have proper record of the normal user's behavior. This record is treated as the profile of the user constructed using database software MS-Access. This profile of the user contains the attributes such as – **UserID**, **Username**, **Password**, **Event sequence string**, **Session time**. The very first table created for the purpose is-

Table Name: tlbUserMaster which is used **to store the information of the user** like User ID, User Name and Password. The primary on attribute UserID is applied to uniquely identify user. Following table shows the structure of *tlbUserMaster* table

Table-1: User Master Table Structure

Attribute Name	Data Type	Size/ Format	Description
UserID (Primary Key)	Number	Integer	User ID to identify each user distinctly or uniquely.
UserName	Text	15	Name of the user that has to provide at Logon Time.
UserPassword	Text	10	Key (Complex String) in encrypted format used to gain access into the system.

(Source: System design suggested by Dr. N.C.Dhande)

Table Name: tlbNormalUserProfile : This table is used **to store the behavior of the normal user at logon time** for example, events/actions generated by the user (normal/anomaly) at the logon time. This table is referred by the table *tlbNormalUserProfile*

Table-2: Normal User's Behavioral Profile Structure

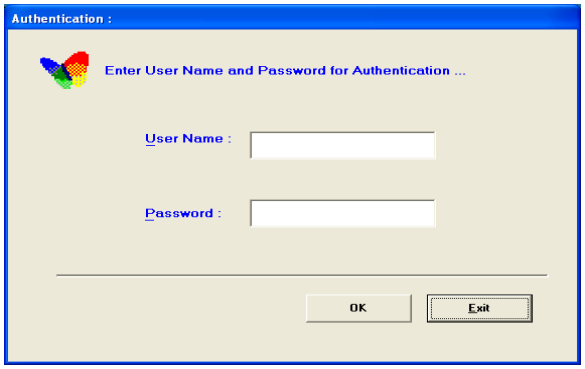
SN	Attribute Name	Data Type	Size/ Format	Description
1	UserID (Foreign Key)	Number	Integer	This field is refers the field UserID from the table **tlbUserMaster.**
2	EventSequence	Text	50	Used to store the events generated intentionally or unintentionally at logon time.
3	LogonTime	Date/ Time	Medium Time	Used to store login time of user.
4	SessionTime	Number	Integer	Used to store time (in Seconds) spend by the user at the time of logon process.

(Source: System design suggested by Dr. N.C.Dhande)

1.6 Proposed Method - Design and layout

While implementing the idea of detecting the unauthorized user, the suggested system is designed with the VB and Access combination. The prepared logon form using VB accepts the username and password inputted by the logger, the **system also simultaneously records the actions/events those are generated at logon time by the current user who may be a normal user or an anomaly**. Also it calculate the time used up by the current user in logon process.

Figure-1: Proposed Logon Form that record Normal User's Behavior



(Source: System design suggested by Dr. N.C.Dhande)

The designed logon form is provided to the user to record his/her behavior at the time of logon process. As stated in the suggested method – the behavior means, "set of events that generated purposely or accidentally when user trying to logon". While doing it, the user has to enter username and password. The application for proposed method records the events performed by the user and also calculates the time taken by the normal user to logon as a normal process.

In this way the sequential set of events is now made available in ***EventSequence*** field that is obtained from the application of the designed system. The application of the Association Rules of the Apriori Algorithm[4] on these set of events gives the output so as to establish an association.

1.7 Verification of the facts on implementation:

Description: The username, password and behavior detained by the application and are then transferred in to table. The normal user's sample behavior recorded by application is given in the following table.

Table-3: Normal User's Recorded Behavior at Logon

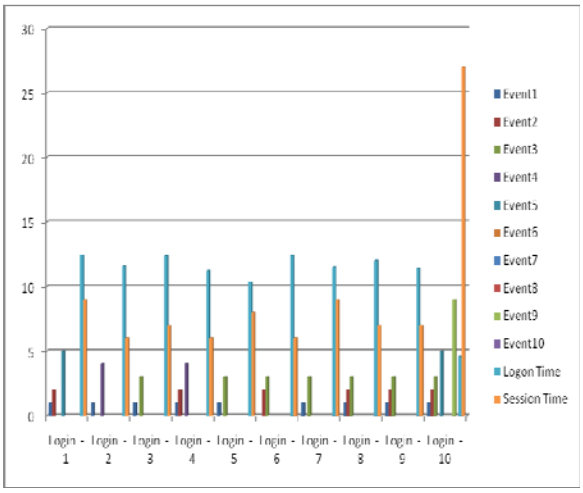
User ID	User Name	User Password	Event Sequence	Logon Time	Session Time
101	Nishikant	Nishi#123	E1,E2,E5	12:45 PM	9
101	Nishikant	Nishi#123	E2,E4	11:57 AM	6
101	Nishikant	Nishi#123	E2,E3	12:35 PM	7
101	Nishikant	Nishi#123	E1,E2,E4	12:05 PM	6
101	Nishikant	Nishi#123	E1,E3	10:11 AM	8
101	Nishikant	Nishi#123	E2,E3	12:40 PM	6
101	Nishikant	Nishi#123	E1,E3	11:50 AM	9
101	Nishikant	Nishi#123	E1,E2,E3,E5	12:03 PM	7
101	Nishikant	Nishi#123	E1,E2,E3	11:42 AM	7
101	Nishikant	Nishi#123	E1,E2,E3,E10	03:00 PM	27

(Source: System design sugggested by Dr. N.C.Dhande)

To illustrate it more the graph of the events recorded is shown in the figure given ahead. On each of the event of the logging in session, the session time is

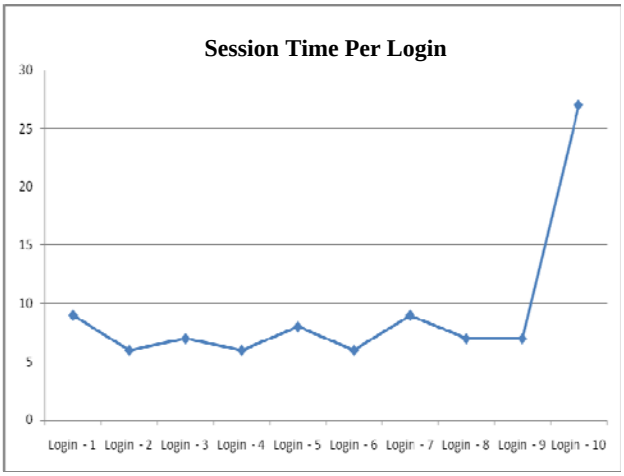
recorded and the same is further used to interpret the behavioral pattern of the user at the time of the login.

Graph 1: Graphical Representation of Normal User's behavior Recorded by the Application



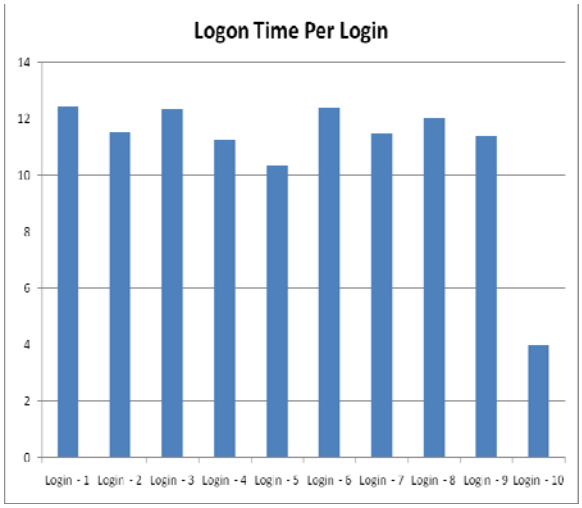
(Source: System design suggested by Dr. N.C.Dhande)

Graph 2: Graphical Representation of Normal User's SessionTime/Login



(Source: System design suggested by Dr. N.C.Dhande)

Graph 3 : Graphical Representation of Normal User's LogonTime/Login



(Source: System design suggested by Dr. N.C.Dhande)

The Graph 1 shows the Normal User's behavior at logon time with respect to session time that means time (in second) spent by the user at each logon process. From this it clears that for the first nine logon processes time taken by the user is in between 6-9 seconds hence average value for session time will be 7.22 and normal deviation ranging from -1.77778 to +1.22222. While in the last logon process user takes 27 seconds to log-on. Similarly, Figure-10 shows average logon time for first nine logon processes is 12:21 PM. While in the last logon process time will be 3:00 PM. Also **occurrences of backspace key ensure that E10 user trying to logon in the last logon process may be anomaly** up to some extent hence deviation occurred at three levels and **hence denied** current user at first level to gain access to the system. And once again has to verify the current user with some other parameters.

1.8 Conclusion:

Though it is difficult to give a total secure login procedure using traditional methods, a new approach based on identification of the user beyond the user name and password is a successful attempt towards achieving the design of a total secure logging process (TSLP). The experiments made herein are fruitful in recognizing the user on their habits as behavior. Hence it is clear that, user behavior can be detected in the forms of 'events', 'Anomaly' can be detected by on behavior using Data Mining Techniques and a system based on the new approach can provide more security to the authentic user. The system based on the approach is practicable in real sense and can be attached as a middleware with the 'key operated interface system' like internet, ATM, etc .

References:

1] "Research Methodology", SAGE publications India Pvt.Ltd., London/Thousand Oaks/New Delhi

2] 1. T. Gilb, *Principles of Software Engineering Management*, Addison Wesley Publishing Company, 1988.

3] D. E. Denning, "An intrusion-detection model," *IEEE Transactions in Software Engineering*, vol. 13, no. 2, pp. 222–232, 1987.

4] Lam, K.-Y., Hui, L., and Chung, S.-L. (1996). Journal of Systems and Software, 33:101{108}.

Dr. Nishikant C Dhande: Diploma in Industrial Electronics 1988, M.Sc. Computer Science 1991, M.B.A. 2002, B.Tech Electronics 2008, Ph.D. System Management 2007. Former Lecturer in Electronics Technology, S.B.E.S. College of Science, Aurangabad. Faculty for M.C.A. and M.Sc. Computer Science, presently working as Assistant Professor, School of Management Science, S.R.T.M University, Nanded, Maharashtra India. **Ten** Books and course material published. Current research interests are in Systems and Management along with computer application. Founder member of Computer Society of India Aurangabad Chapter. Experience of More than 22 years in teaching, industrial consultancy besides the R & D.