Asian Journal of Management Sciences

ISSN: 2348-0351

Published on: 29-03-2014

Dr. Nishikant C Dhande
Assistant Professor,
School of Commerce &
Management Science,
S.R.T.Marathwada University,
Nanded, Maharashtra India

QR Code for Mobile users

Conflict of Interest: None Declared !

Secure Human Computer Interface: An Approach to Intrusion Detection.

Dr. Nishikant C Dhande
Assistant Professor, School of Commerce & Management Science, S.R.T.Marathwada University, Nanded, Maharashtra India.

ABSTRACT

A tremendous amount of information and data is shared by the World Wide Web users all over the world. On an average there are 20 to 40 new vulnerabilities are discovered every month in commonly used networking and computer products. Such wide-spread vulnerabilities in software add to today's insecure computing/networking environment. This insecure environment has given rise to the ever evolving field of intrusion detection and prevention. If a password is weak and is compromised, user authentication cannot prevent unauthorized use; firewalls are vulnerable to errors in configuration and suspect to ambiguous or undefined security policies. They are generally unable to protect against malicious activities. Hence a new approach based on the 'Apriory approach of intrusion detection' has been suggested to enhance the log in security to make the user more secure while using the computers.

Keywords: Human Computer Interface, Login Security, Algorithm, User Behaviour.

Cite this article as:
Dr. Nishikant C Dhande,
Secure Human Computer Interface: An Approach to Intrusion Detection.
Asian Journal of Management Sciences.
02 (03 Special Issue); 2014; 176-179.

Introduction

Since millions of transactions taking place on the Internet everyday, network security plays a major role in creating and advancing new business opportunities. A tremendous amount of information and data is shared by the World Wide Web users all over the world [1]. Similarly as per the findings of VanDyke Software in 2003 that some "66 percent of the companies stated that they perceived system penetration to be the largest threat to their enterprises. Although 86 percent of the respondents used firewalls, their consensus was that firewalls by themselves are not sufficient to provide adequate protection" [3,4,6]. On an average there are 20 to 40 new vulnerabilities are discovered every month in commonly used networking and computer products. Such wide-spread vulnerabilities in software add to today's insecure computing/networking environment. This insecure environment has given rise to the ever evolving field of intrusion detection and prevention [5].

The conventional or traditional protection techniques such as user authentication, data encryption, avoiding programming errors and firewalls are used as the first line of defense for computer security. If a password is weak and is compromised, user authentication cannot prevent unauthorized use; firewalls are vulnerable to errors in configuration and suspect to ambiguous or undefined security policies. They are generally unable to protect against malicious activities [2].

Security at Logon Time

The present security available at logon time is insufficient and hence should be refining due to vulnerable of intrusions. Therefore, a new approach is needed with respect to adding steadiness and robustness to security system. Security is the art of restricting access to certain entities. One of the fundamental aspects of all security systems is accessor identification which is also called as logon security. Of course, no additional layers of security can help if the logon security system is inadequate. It will surely make the system vulnerable & wide open to any potential computer criminals.

It is expected that, a good logon security system must ensure user ID integrity, and, if a violation is detected, it must take proper measures to inform appropriate user (e.g. the system manager and the console operator) of the violation. Furthermore, it must protect against internal tampering with the security system by maintaining a clear audit trail of all security modifications. And, it may also be of benefit for it to prevent user access at times and from places in which it is easiest to go through system security (e.g. on weekends, after hours, over telephone lines, etc.) [11,12]

In order to ensure user ID integrity, conventional logon security system uses passwords. However, these passwords provide only false impression of security, because:

- There is only one password for each level (user, account, or group) of security. Thus, knowing this one password guarantees that you can break through that level of security.
- Ignorant people treat passwords as a non essential, and may make it public even to unauthorized person.
- Passwords are stored in the system in clear text or may be in encrypted format. Thus, they may be readily found in job streams, discarded LISTDIR2 listings, on SYSDUMP tapes, etc.

Thus an approach is taken here regarding the behavioural aspects of human being while using the computer systems at the time of the login process.

Human behavioral factors:

Every human being has got some typical habits related to the nature of individual and the way of doing the work. These behavioural habits may become characteristics of individual as a practice of doing the things in his or her own way. These styles of functioning and doing a work in a very specific and typical manner can be treated as a measure of performance one displays through personality.

These can be like-

1. Time taken to login
2. Time of login
3. Particular way of login
4. Specific keys that are habitually used in for login
5. Specific behavioral habits of handling the gadgets and tools
6. Typical actions one always perform as a reflex action or habit

Keeping a track of these and analyzing these with the standard data base of the behavioral record of each individual will certainly help identification of the authentic user from the intruder. To achieve the same experiments were carried out and the relevant data has been recorded with following aspects.

Design of the experiment:

In an experiment designed an attempt is made to record the behavioural factors of the user. Any deviation from the regular habits will be treated as a 'mis match' and the logger is treated as an intruder for the system as the behavioural aspects are not matching. The activity carried out by each individual at the time of the logging in process is treated as an event specific to each individual. Each event further kept a track of, and recorded accordingly as an individual characteristic identifier. The entries made at each login were recorded and compared to the standard record of the habits displayd through one's personality out come as a habit. On comparison based on the data mining support, the intruder action can be singled out and isolated to add to security to the system from un authorized user. The algorithm in support is as follows.

Algorithm – Event Generation:

The proposed method detains the normal user's behavior along with username and password at logon process. The proposed method consist of following steps –

Input :

U - user_name // string used for user's name at logon time.

P- password // key (complex string) used to gain access to user account.

Events : Generates intentionally/unintentionally by the user at logon time.

- Events generates while accessing username textbox with -
  E1 - varE1UsrTxtMousClk // Mouse Click
  E4 – varE4UsrTxtAltU // Alt+U Key
- Events generates while accessing password textbox with -
  E2 – varE2UsrTxtEntrKey // Enter Key
  E5 – varE5PassTxtMousClk // Mouse Click
  E7- varE7UsrTxtAltP // Alt+P Key
  E11– varE11PassTxtTab // Tab Key
- Events generates while accessing command button with -
  E3 – varE3OkCmdClck // Mouse Click
  E6 – varE6OkCmdAltO // Alt+O
- Events generates with Malicious Activity -
  E8 – varE8ImgMousMov // Image Mouse Move
  E9 – varE9UsrTxtAltU // Form Click
  E10 – varE10UsrTxtAltU // Backspace Key

Output :

ES – eventsequence // Generate event sequence [Used as an input to Apriori Algorithm to find the strongest Association Rules between most frequently occurring events.]

The Proposed Method-Algorithm:

Step - 1 : Start the process

Step - 2 : Declare and initialize local variables and start the timer. [Local variables are used to trap the events/actions generated when logon process is going on.]

Step - 3 : Allow user to enter for Username and Password.

Step - 4 : Detaining all the specified events/activities [Performed by user intentionally or unintentionally]

Step - 5 : Generate the **eventsequence** from trapped events and process on the session time and logon time.

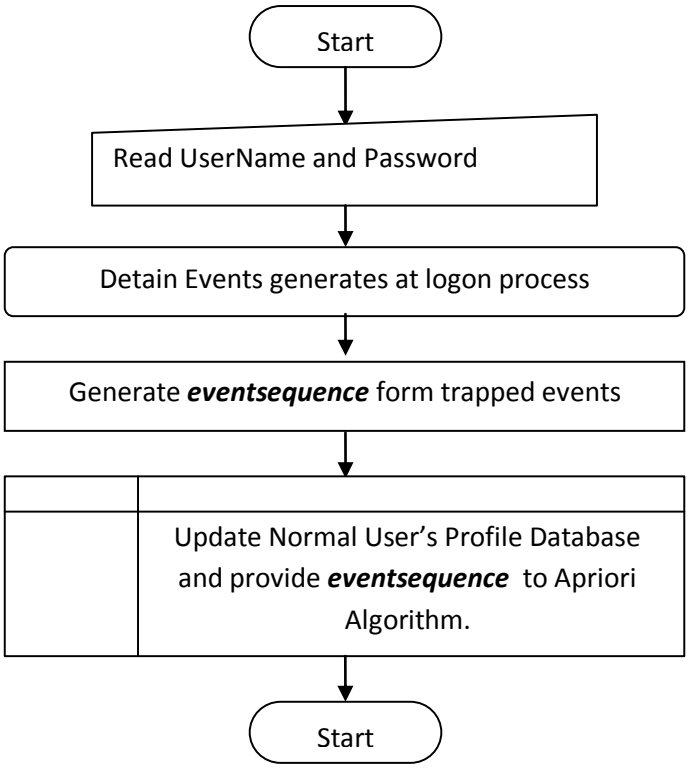
Step - 6 : Update the normal user's behavioral profile.

Step - 7 : Provide generated **eventsequence** as an input to Apriori algorithm.

Step - 8 : Stop the process.

From this **eventsequence**, by applying Apriori algorithm the strongest association rule(s) will be produced between most frequently occurred events as an output.

Flow Chart of the Proposed Method –



Apriori Algorithm

The Apriori Algorithm is powerful algorithm for mining frequent itemsets for Boolean Association Rules. The Apriori algorithm is the most well known association rule algorithm and is used in most commercial products. It uses the following property, which will be termed as large **itemset property.**

"Any subset of a large itemset must be large".

The large itemsets are also said to be downward closed because if an itemset satisfies the minimum support requirements, so do all of its subset. Looking at the contra positive of this, if we know that an itemset is small, we need not generate any supersets of it as candidates because they also must be small.[1,2]

Definitions :

- **Frequent Itemsets:** The sets of item which has minimum support (denoted by L_i for i^{th}-Itemset).
- **Apriori Property:** Any subset of frequent itemset must be frequent.
- **Join Operation:** To find L_k, a set of candidate k-itemsets is generated by joining L_{k-1} with itself.

The Apriori Algorithm

- Find the frequent itemsets: the sets of items that have minimum support
  – A subset of a frequent itemset must also be a frequent itemset
- i.e., if {AB} is a frequent itemset, both {A} and {B} should be a frequent itemset

– Iteratively find frequent itemsets with cardinality from 1 to k (k-itemset)
- Use the frequent itemsets to generate association rules.

The Apriori Algorithm : Pseudo code

- Join Step: C_k is generated by joining L_k-1with itself
- Prune Step: Any (k-1)-itemset that is not frequent cannot be a subset of a frequent k-itemset
- **Pseudo-code:**

C_k: Candidate itemset of size k
L_k : frequent itemset of size k
L_1 = {frequent items};
for (k = 1; L_k !=.; k++) **do begin**
C_{k+1} = candidates generated from L_k;
for each transaction t in database do incr. the count of all candidates in C_{k+1} that are contained in t
L_{k+1} = candidates in C_{k+1} with min support
End return $\mathbf{U}_k$ L_k;

Conclusion:

Hence it is clear that the human behavior can be tracked for the authentication of the user at the time of the login process. The concept of the apriory assumptions based of the strongest association rules of the human computer interface can be used with the designed algorithm to enhance the security to the user be distinguishing the user from the intruder.

References:

1. Intrusion Detection Subgroup, available on http://www.ntsac.org as FIDSGREP.PDF
2. Intrusion Detection Systems as Evidence Peter Sommer Computer Security Research Centre, London School of Economics & Political Science P.M.Sommer@lse.ac.uk
3. E. Millard, “Internet attacks increase in number, severity,” In CIO Today at http://www.cio-today.com/story.xhtml?story id=003000002F13, August 2005.
4. J. Phillips, “Hackers’ invasion of ou data raises blizzard of questions,” In The Athens News at http://www.athensnews.com/issue/article.php3?story id=24611, May 2005.
5. C. staff, “Hackers: companies encounter rise of cyber extortion,” In ComputerCrime Research Center Website http://www.crime-research.org/news/24.05.2005/Hackers-companies-encounter-rise-cyber-extortion/, 2005.
6. C. Warrender, S. Forrest, and B. Pearlmutter, “Detecting intrusions using system calls: Alternative data models,” in IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE Press, 1999, pp. 133–145.
7. Jones, Anita K., Sielken, Robert S., “Computer system intrusion detection: A survey”,Technical Report, Computer Science Dept., University of Virginia, 1999.
8. Koziol, Jack, “Intrusion detection with Snort”, Sams Publishing, 2003.
9. Bace, Rebecca Gurley, Intrusion detection”, Macmillan Technical Publishing, 2000.
10. Crothers, Tim, “Implementing intrusion detection systems”, Wiley Publishing, Inc., 2003.
11. Mohammadian, M., “Intelligent Agents for Data Mining and Information Retrieval,”Hershey, PA Idea Group Publishing, 2004
12. Wang, J., “Data mining: Opportunities and challenges,” Idea Group Publishing, September, 2003.