ABSTRACT

Computer security has become a very important part of human life. Adding to the race authentication counts as an important issue among many access control mechanisms.

Secure networks allows only intended recipient to intercept and read a message addressed to him. Thus protection of information is required against possible violations than to compromise its secrecy. Secrecy is compromised if information is disclosed to users not authorized to access it. Password authentication is one of the mechanisms that are widely used to authenticate an authorized user. Normally we assign usernames and passwords to each and every authorized user. In order to check whether a user is authorized or not each server stores all these usernames and passwords in a table. Whenever a user want to avail a service from the server he then uses enters his username and password, then the server uses its inbuilt information stored in the password table and checks whether the user is authorized or not.

The main limitation with traditional password authentication method is that server has to store password table which occupies memory space. As the number of users increases the (user id, password) combinations increases and memory requirement increases. Another limitation in using the traditional password authentication method is that a server must maintain a password table that stores each user’s ID and password. Therefore, the server requires extra memory space to store the password table. When a user logs into a computer, he types in the ID and password. The server searches the password table and checks if the password is legal. However, this method is dangerous. The password information table could be read or altered by an intruder. An intruder can also append a new ID and password into the table.
In earlier methods the password table was protected using hash functions, but it was not safe. Later instead of password table verification table containing hashed password (encrypted) was used to store password table in the server. Even though password is encrypted still there is a chance of modification of the verification table since it is open access environment. There are so many disadvantages in the traditional password authentication schemes. New techniques for password authentication were introduced in this work. Before observing the drawbacks in traditional password authentication schemes (PAS) or to see how the proposed method can overcome the pitfalls of PAS, traditional password authentication scheme discussed.

Neural networks have been used recently for password authentication in order to overcome pitfall of traditional password authentication methods. We used Associative memories algorithm for both alphanumeric (Text) and graphical password by which the level of security can be enhanced. This work along with test results shows that converting user password in to Probabilistic values enhances the security of the system. The advantage of using neural networks over statistics is its ease in expressing and learning nonlinear relationships between variables. Experiments using neural networks resulted that the behavior of super user (roots) are predictable. The number of neurons in the input layer depends on the number of possible inputs we have, while the number of neurons in the output layer depends on the number of desired outputs. The number of hidden layers and how many neurons in each hidden layer cannot be well defined in advance, and could change per network configuration and type of data.
To overcome the disadvantages of traditional password authentication schemes, novel techniques for password authentication were introduced. In these techniques server need not store usernames and passwords, instead this work uses a feed forward neural network and train the server using usernames as input and password as output. When a particular user submits his login credentials, his user name and password were given as input for the algorithm and check whether user is authenticated or not. When the training is completed the weight values will be stored in the weight table, in the server. Therefore when a user submits his/her login credentials network uses this weight values to produce output.

The proposed method of password authentication uses two types of passwords - Textual password and Graphical password. Whenever new users are creating accounts, network has to adjust weights to recognize all the users who are registered. This process of changing weights is called learning. Here in order to do learning we used any one of the Associative memories. The proposed method can use any one of the passwords to train the network in order to authenticate the users. This method is very difficult to attack (Provides More Security). To decrypt cipher text attacker has to identify weight matrix (Even one element of matrix changes attacker can’t decrypt), No. of Hidden layers, Output function, Character set (Including order of Characters in Character set), Minimum and Maximum values used in character set. Even though we use existing character set we can improve security by changing order of characters or minimum value to change unique number and probabilistic values associated to each character so that attacker may confuse in guessing the unique numbers or probabilistic values. This method can provide more security by increasing number of Hidden layers. The users (Organization) of this algorithm can define their own character set, by doing so users can add new characters into their character set.
The system users can freely choose their password and the servers are required to retain only the pair user ID and password. The password authentication scheme can prevent the replay attack; the intruder cannot obtain a login password through the open network and replay the password to login to a server. Server only stores the weights of the network. Our method prevents Replay attack.

o0o