Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679
ISBN 978-3-901509-83-4, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2011
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2011

MULTIDIMENSIONAL USER AUTHENTICATION

MALANIK, D[avid] & JASEK, R[oman]

Abstract: *The commonly used methods for the authentization of people occasionally use only the one method for user verification. This paper deals with the more complex method for successfully authentization of people inside the area with hardly restricted access. The multidimensional user authentication is based on multiplication of used methods with diferent principles. The result is the n-dimansional deformed function with only one correct positive identification. This method might represented the best practices of future security system.*

Key words: *user autentification, security, n-dimension functions*

1. INTRODUCTION

There are many methods for the user authentication. Every method is built on the small group of cryptographic models. The most commonly using method for user password verification is hash verification. The password is as a hash code of the password string. The authentication routine just compares the stored hash code and the hashed password which user type to the authentication window (Delfs & Knebl, 2010). But after this verification is the user verified or not. This action is only once. This is only at the beginning of work. There were some other methods to prevent a user changing without de-authorization and other user authentication. The common rule is: if you leave your computer, you must log out or lock your account. But this is not real in many organisations. For example: if user goes to the toilet, the user doesn’t log out his account with some processing work. In many cases, the user just goes. In minority cases, the user locks his account.

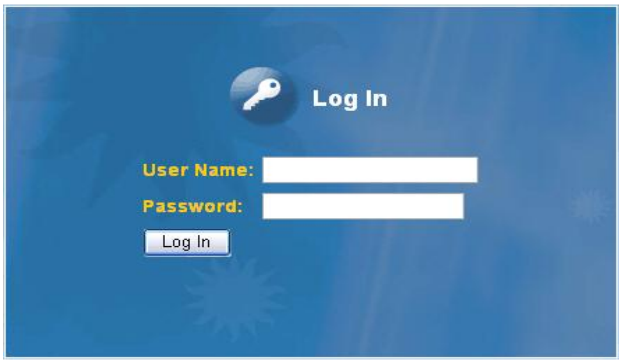

Fig. 1. Login scree

2. PROBLEM FORMULATION

2.1 Authentication continuum

The problem of commonly using authentication methods is, that the user was verified only once (Fig.1.); at the beginning of work. Next, the user is verified until he stop his work and “touch logout button”. During his work, the authentication environment doesn’t check if the working user is the authentication user. The system just trusts him and does not repeating the verification procedure anymore. The system is open and user does not provide valid username and password until he does not finish his work.

2.2 Security issue

The possible security misuses of this commonly using solution flowing from the one-time verification procedure. If there is some break during the logout procedure, the system stay inside the successfully login state. The attacker might misus it with the current verified procedure and user profile.

3. SOLUTION

3.1 Repeating of verification procedure

The first possible solution of previously described problem is flowing from the autentization continuum. But logging to the system with username and password every 15 or 5 minutes is quite problematic. Biometrical identification based on fingerprint is not applicable, because the principle is physically same. This methods need user physical interaction. The solution flowing from the methods which does not require user contact, it must be based on the behavior of verified people.

3.2 Multidimension/multifactor user verification

The multidimensional user verification is based on the n-dimensional testing function with the one global extreme point. The special functions is using as a carrier basemap. The usable functions are Ackley, the De Jong, or the Rana (Bucki, 2009). The factor might be some oh user behavior or biometric characteristic. For example: user face captured by camera, frequency of typing, acceleration of mouse movement in each axis, and many more users originally characteristics.

3.3 Examples of n-dimension functions

The example of carrier function is shown on Fig. 2.

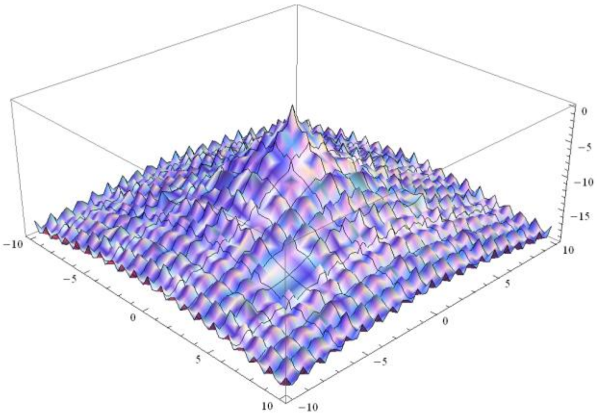

Fig. 2. Ackley carrier function (Bucki, 2009)

This function is the base for the autentization procedure. For the procedure is usable function with more dimensions. Each dimension upper the three represents one of the autentization factors. The identification factors are responsible for the deformation of n-D space of carrier function. The first of the deformations might by represented by the hash code of username and the second one by the password. Each other factor is affecting different dimension (different cut in specific dimension). These deformations produce the deformation of the global extreme position. The position is moving in n dimensions and the value of this extreme point was changed.

There are two diferent methods for the user verification. The first and less precision is based on the value of the extreme point. This might be used for the periodically checking of user identification. The second one is based on the position of extreme point. This position originally identifies the each user. Position of extreme point might fluctulate, because the user's behaviors are not totally stable, but the fluctulation is minimal inside the n-dimension space. The basic carrier function has the extreme point on coordinates {1.53291; 2.2993} with the value 3.70948. This is the carrier extreme point, with the small deformation of function in x and y axis (hashcode of username and password) produce the different extreme coordinates and value.

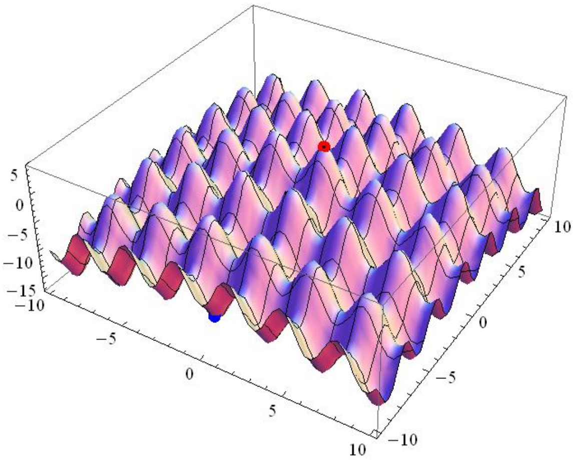

Fig. 3. Deformed verification function

The Fig. 3 shows the carrier function after deformation. The new position of extreme value is on coordinates {1.54678; 2.28796} with the value 3.73596. This diferece marks the verified people. The 3D space is using only for the demonstration. The practical using calculates with more than 10D spaces.

3.4 Authentication system

The system calculates the position of extreme and its value. This procedure collects the user specifications without username and password. These two values are provided by user only once at the beginning of login procedure. There is the internal database with user identities, the identification informations are hidden inside the coordinate and value of extreme point the username, and the next information is the type of carrier function. Login process contains procedure for building temporally autentization function for loging user. The building needs all verification factors; this mean: username, password, biometric autentization data (fingerprint, faceprint, etc…).

Afther this procedure, the user is basically checked and verified. But the system continues with collecting of user characteristics and compares the new position of extreme value with the database. If there are some marginal changes, system safety disconnects the current session. This is the prevention for user switching without logout and login procedure.

4. CONCLUSION

Computer security is one of the most discutable thema of the present Wordl. There are many systems with limited access, which contains confidential data, and company or government must protect it. But this is not only the problem of companies and goverments, every people around this world nned some level of privacy. There are many methods for securing this data and limited access to it. But mayority piece of these systems does not deal with one possibility such is the user switching without logout and login (Huang; Maccallum & Dingzhu, 2010).

Many companies use the security policies, which requires the user logouting inside any work breaks during the day, some of these companies using electronic cards and biometric scaners. Thus this policies, many users does not logout his session when they go out only for some minutes (for example: go to the toilet). Autentization continuum is really common thing. It is well known fact, but there are not available any suitable solution for solving this problem. There are partiullary solution based on the timers, whitch automatically disconnection current session after some minutes without activities, but this is quite impractical. If the interval is to short, users must provide theirs credential repeatly during day. If it is longer, the rule does not affect.

Continuosly verification procedure might help with the user switching, system recognize the abnormal user behavior and characteristics and close the session. The user profile was disconnected and incidend was written to log file. System administrator is contacted by the system.

The autentization system migh be developed as a selflearning system with the dynamically selfteaching function, which might dynamically modify the verification function by the evolution of user characteristics.

The next possible future steps are improvement of the neural network for the "undeforming" of image source. This will be represented as the algorithm for the templationg of source picures, this algorithm might transform the captured picture to some template style with specific size and rotation of verified faces.

5. ACKNOWLEDGEMENTS

The research work was performed to financial support of grant reg. No. IGA/57/FAI/10/D and by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

6. REFERENCES

Bucki R., Modelling Flexible Production Systems, Artificial Intelligence, No. 4, Doneck, 2009, pp. 113-118, ISSN 1561-5359

Delfs, Hans; Knebl, Helmut. Introduction to cryptography : principles and applications [online]. 2nd ed. Berlin : Springer, 367 s. Available from WWW: < http://www.springerlink.com/content/gm2886/?p=7d653593e3e247faa59f202fe838cf57&pi=1332 >. ISBN 978-3-540-49243-6

Huang, Scott Ch; Maccallum, David; DU, Dingzhu. Network security [online]. New York : Springer, 280 s. Available from:http://www.springerlink.com/content/t8p22v/?p=3f1b9f4e5c354281985379f8818765b9&pi=141 >. ISBN 978-0-387-73821-5

Tipton, Harold F; Krause, Micki. Information security management handbook. 6th ed. Boca Raton : Auerbach, 2007. 3231 s. ISBN 0-8493-7495-2

Zelinka, Ivan; Oplatková, Zuzana; Šenkeřík, Roman. Aplikace umělé inteligence. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 151 s. ISBN 978-80-7318-898-6

Zelinka, Ivan. Umělá inteligence : hrozba nebo naděje?. 1. vyd. Praha : BEN - technická literatura, 2003. 142 s. ISBN 8073000687