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

SECURE USER AUTHENTICATION TO THE INFORMATION SYSTEM USING THE METHODS OF FRACTAL GEOMETRY

MOTYL, I[vo]; JASEK, R[oman] & PALKA, J[iri]

Abstract: *This article is focused on authentication of users inside and outside the information systems. For this purpose is widely used hash function. The proposed process is based on the elements of the fractal geometry. The algorithm here uses a wide range of the fractal sets and the speed of its generation. The system is based on polynomial fractal sets, specifically on the Mandelbrot set. The system meets all the conditions for the construction of hash functions.*

Key words: *HASH, fractal geometry, information system, authentication, fractal set*

1. INTRODUCTION

Hash functions have in the world of information technology an important role. They are represented in many areas of the information system. (Piller, 2009) Hash functions can be used for example in password section of information system (Champlain, 2003), data identification, integrity control, database comparing and many others solutions (Harper et al., 2008).

The aim of this study was describe how to using fractal geometry (Zelinka et al. 2006) generates hash function for secure authentication inside of the information system.

2. PROBLEM FORMULATION

Using of fractal geometry for the authentication process is an alternative to authentication process using the hash function. For proper function of the process is necessary to ensure the following parameters:

- One-way function – For a given message *M* is very simple compute *h* = *H(M)*, but the *h* is computationally impossible to calculate *M*.
- Non-collision function – impossibility to find a variety of *M* and *M '*, then the *M≠ M '* so that *h(M)= h (M ')*. Two input strings are not allowed to apply the same hash.
- Random oracle – Output of the hash function must be random.

2.1 Principle of the classical HASH function in the authentication process

In the modern information systems are items for more sophisticated solutions. (OracleThinQuest, 2011) One of them is for example Salting process. This is one of many possibilities how to increase the password security. The password processing in this case is very simple. The password is extended by the several random characters. All string is converted by the hash function to HASH. This HASH string is stored to database.

Fig. 1 shows the login process with the hashed password. The information system contain database with users password. In the first step user enter his secret password into the login form. The entered password is converted by the hash process to hash string. This string is compared with the record in database. If the entered password is correct, the user is successfully logged. (Piller, 2009)

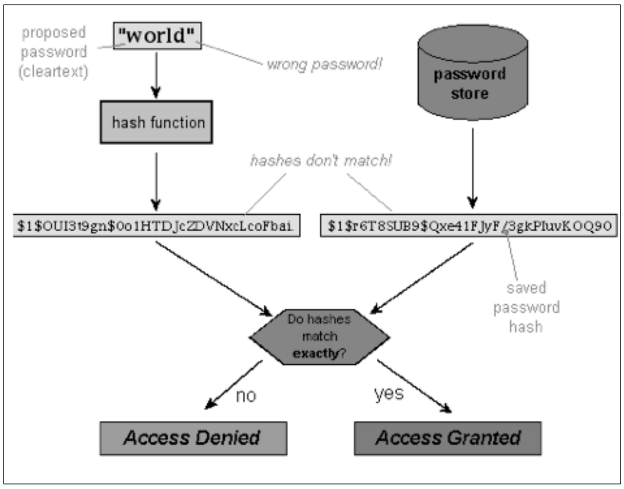

Fig. 1. Login process (Harper et al., 2008)

3. PROBLEM SOLUTION

Polynomial fractals are between the most popular. Their design takes advantage of the attractiveness of areas for various solutions of nonlinear systems. The coordinate system is tested at points belonging to it, whether the rule meet the specified condition. Evaluation of equations, which are based on polynomial fractals, happens iteratively. Iterative cycle can be terminated either after a specified number of iterations, or after the evaluation of test conditions.

3.1 Parameters for fractal construction

For the construction of fractal hash is necessary to set the initial conditions. Parameters X1, X2, Y1 and Y2 specify the coordinates of fractal field. Parameters were found by experimental process. The experimentally determined parameters are used as the basis for creating new parameters for the user password. User password is converted to ASCII characters arranged in a row and increment to rest of the value on the fifth place behind the decimal point. This border is optimal for the purpose of this process. In the case that the value of place was less could to be stuck in a place where he reached the full number of iterations in the creation of fractal.

X1- real part of the operating quadrant	*0,371447488729618*
Y1- imaginary part of the operating quadrant	*0,37149495542098*
X2 - real part of the operating quadrant	*0,585327310008748*
Y2 - imaginary part of the operating	*0,58537477670011*

quadrant	
Number of iterations	*640*

Tab. 1. Fractal parameters

Fig. 2 shows the output of the fractal structure used in the algorithm for advanced user authentication. It is part of the Mandelbrot set. The coordinates for generating this picture was used from Tab. 1.

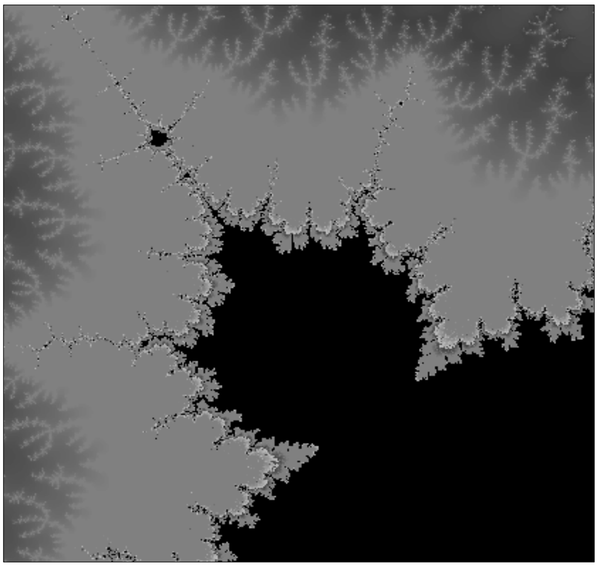

Fig. 2. fractal structure for advanced user authentication

3.2 Fractal HASH functions in the authentication process

Fig. 3 shows the login process with the fractal hashed password. The information system contain database with users password in the form of fractal. In the first step user enter his secret password into the login form. The entered password is converted to parameters for fractal algorithm. The fractal algorithm produces fractal images in agreement by the initial conditions. This image is compared with the record in database. If the entered password is correct, the user is logged.

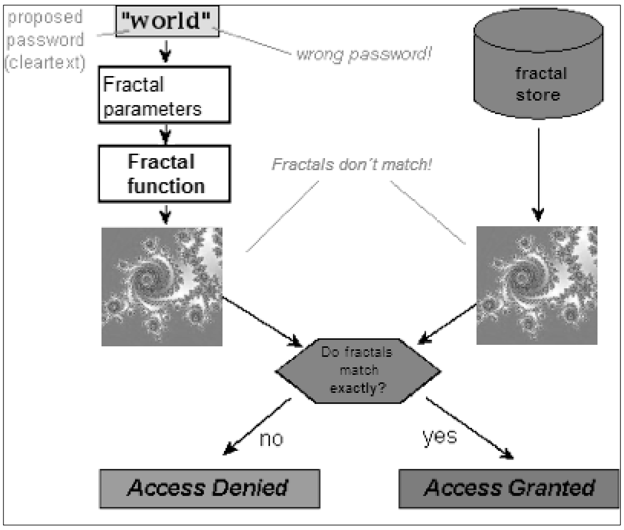

Fig. 3. Fractal authentication process

4. CONCLUSION

This article was focused on the possible use of fractal geometry for secure authentication of users. This process is an alternative for the now widely used hash function. The process of authentication and its principles are described in chapter three. If we compare the authentication process using hash function and fractal geometry, we find that in many ways are similar. The size of fractal object can be selected by modifying the function generating the initial conditions for the creation of fractals. The system uses the advantages of fractal geometry, in particular the wide range of fractal sets and the speed of its generation. At present most frequently were subjected to analysis of two-dimensional polynomial fractals, especially Mandelbrot set, made partial research and testing in this area. In another part of the planned line of research focused mainly on fractals located in multiple dimensions, and examined the applicability of the topic. Research will continue to become increasingly important to use the existing solution, which will be linked new knowledge to create an output unit for possible use in engineering practice. Future research will become increasingly important for multi-dimensional fractal structures, in particular, variations and Julio Mandelbrot sets. Another part will be to test the possibility of using IFS fractals for secure authentication of users within the information system. A prerequisite for use of the IFS algorithm will be their determinism. This is a basic requirement for obtaining identical output parameters from a user password into the information system.

5. ACKNOWLEDGEMENTS

This article was supported by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089 and Internal grant agency (IGA/29/FAI/11/D).

6. REFERENCES

Brodtkorb, A. R. & Hagen, T. R. (2008), *A Comparison of free commodity – level parallel architectures: Multi-core CPU, cell BE and GPU.* 7th International Conference MMCS, ISBN 10-3-642-11619-1 Tonsberg, Norway

Champlain, J. J. (2003) *Auditing information systems.* ISBN 0-471-28117-4, John Wiley and sons, 2003, New York

Harper, A., Harris, S. & Eagle, Ch. (2008) *Hacking – manuál hackera.* ISBN 8024713462, Grada Publishing, Praha

Lofstedt, T. (2008).*Fractal Geometry, Graph and Tree Constructions*, Umea University, Sweden.

Mandelbrot, B. B. (2004), *Fractals nad chaos: the Mandelbrot set and beyond.* Springer, ISBN 0-387-20158-0, New York

Motyl, I.; Palka, J. & Palka, J. (2010). *Advanced Methods for Securing the Information Systems*, Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, 20-23rd October 2010, Zadar, Croatia, ISSN 1726-9679, ISBN 978-3-901509-73-5, Katalinic, B. (Ed.), pp. 1207-1208, Published by DAAAM International Vienna, Vienna

OracleThinQuest (2011), *Hash Codes and Hashing,* Oracle, *available from*: http://library.thinkquest.org/07aug/01676 /relevance_cryptographictechxnologies_authentication_hashcodes.html *Accessed:* 2011-06-07

Piller, I. (2009), *Hashovací funkce a jejich využití při autentizaci*, Vysoké učení technické v Brně

The Mandelbrot set (2011), *available from:* http://warp.povusers.org/Mandelbrot Accessed: 2011-05-13

Tříska, D. (2009), *Kryptografická ochrana*, Univerzita Tomáše Bati ve Zlíně

Zelinka, I., Včelař, F. & Čandík, M. (2006). *Fraktální geometrie principy a aplikace*, BEN, ISBN 80-7300-191-8, Praha