www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11349-11351

Organizational Mail Tracking With Security Using 3d Password And Database Encryption

Megha Sunil, Navami M Chandrabose, Neethu Pious
Department of Computer Science
Vidya Academy of Science and Technology
Thrissur, Kerala, India
Sunilmegha19@gmail.com

Department of Computer Science
Vidya Academy of Science and Technology
Thrissur, Kerala, India
navamimenilakath@gmail.com

Department of Computer Science
Vidya Academy of Science and Technology
Thrissur, Kerala, India
piuskallery@gmail.com

Abstract—**This paper proposes to design an organizational mail server which has the property of tracking unauthorized mails send between employees of different scales in an organization for reducing security issues. It is a direct intruding into each employee's mail in an organization, tracking and monitoring the mail, which is done in a secret format. In Mail Compose web page, an additional function which does not allow employees to send invalid mail and send a report to the administrator about this attempt. Administrator stores these reports in a separate database in an encrypted format. For secure operations, 3D Password is used as the protection tool for administrator login.**

Keywords— Email Network Analysis,3D password, Enhanced Affine Block Cipher,Cued Click Points

I. INTRODUCTION

This paper proposes to design an organizational mail server which has the property of tracking unauthorized mails send between employees of different scales in an organization for reducing security issues. Email has widely become the means of communication in an organization. Therefore email has been established as an indicator of collaboration and knowledge exchange. Email network analysis helps management systematically view its organization as a whole.
As the theme of the project, it is a direct intruding into each employee's mail in an organization, tracking and monitoring the mail, which is done in a secret format. In Mail Compose web page, an additional function which does not allow employees to send invalid mail and send a report to the administrator about this attempt. Administrator stores these reports in a separate database in an encrypted format. For secure operations, 3D Password is used as the protection tool for administrator login. Enhanced Affine Block Cipher technique is proposed for database encryption, which improves the weakness of the original affine cipher and have modification on Cipher Block Chaining (CBC) mode of operation for block cipher. The 3D password is multi-password authentication system which uses a textual password, Graphical password and some movements in a 3D virtual environment.

II. EMAIL NETWORK ANALYSIS

Email has widely become the means of communication in an organization. Therefore email has been established as an indicator of collaboration and knowledge exchange. For each email there is a sender and receiver, which are nodes in the network and there is edge between them. As a sum of the nodes and edges, we obtain the email network. Email network analysis helps management systematically view its organization as a whole [1].An email network was derived from an email log file from the email server. In the email network, each node represents an email address and each edge between two nodes represents an email exchange between these two email addresses. Analysis of email networks used to identify the informal communication structure within an organization and to discover the shared interests between people. Visualization of email networks has been applied to assist the users to understand email data and also to analyze the social network [9].

Email network are useful information resources to find informal communities and providing structure and communication pattern within an organization. We use the

clustering method that can rapidly detect dense communities within an email network. The result of the clustering process reveals informal communities and hierarchical structures within an organization. To characterize people in the informal communities, we calculate several network centralities of a person using the structure of an email network [1].

Email network analysis consists of:

1. Construct email network
2. Identify communities in network by topological clustering
3. Calculate network centralities
4. Analyze the results

To identify the communities in the email network we perform topological clustering of networks. This algorithm was based on the concept of modularity. We divide networks into clusters and then repeatedly join clusters together in pairs, choosing the join which results in the greatest increase in modularity in each step. A node in a cluster is characterized with its network centralities [21]. We calculate centralities as follows.

1. Degree centrality: The number of links of a node.
2. Betweenness centrality: The number of node pairs that pass through a node.
3. Closeness centrality: Average shortest path to other nodes.
4. Pagerank centrality: The stationary distribution of the Markov chain corresponding to the stochastic transition matrix of a network.

III. 3D PASSWORD

There are many authentication techniques such as textual password, graphical password, etc. but each of this individually having some limitations and drawbacks. To overcome the drawbacks of previously existing authentication technique, a new improved authentication technique called as 3D password. The 3D password is multi-password and multi-factor authentication system as it uses a textual password, Graphical password etc in a 3D virtual environment [2]. The working of the 3D password is as follows:

1. Fill User name.
2. Enter into 3D environment.
3. Enter textual password.
4. Enter graphical password.
5. Move objects in the environment.
6. Create a password which is a combination of these three.

The 3D password authentication scheme has some advantages:

- 3D Password scheme is combination of re-call based, recognized based, etc into single authentication technique.
- Due to use of multiple schemes into one scheme, password space is increased to great extend.
- More secure authentication scheme over currently available schemes.

The 3D password authentication scheme has some disadvantages:

- Time and memory requirement is large.
- Shoulder-suffering attack is still can affect the schema.
- More expensive

A. Graphical Passwords

Cued Click Points is a graphical password technique used in this project. It is a combination of Pass Points and Pass Faces. A password consists of one click point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in.CCP provides better security because the number of images increases the workload of attackers [4,7].

There is a new and more secure graphical password system, called Pass Points. Our scheme: (1) allows any image to be used and (2) does not need artificial predefined click regions with well-marked boundaries a password can be any arbitrarily chosen sequence of points in the image .Complex images can have hundreds of memorable points. In order to log in, the user has to click close to the chosen click points, within some set tolerance distance. Password space is larger than text based password [8].

Usability Features in Graphical Password Scheme are:

- Memorability: User capability to memorize the created graphical password.
- Efficiency: How quick users can create the password and how fast a user can login using the graphical password.
- Input Reliability and Accuracy: Pointing to the right spot is basically depending on the input devices.
- Easy and Fun to Use: System should provide a good platform in creating the password.
- Grid based: Clickable area are arranged inform of grid based technique.
- Freedom of Choice: User can click anywhere within the selected picture thus providing the freedom to choose the password location [5].

IV. DATABASE ENCRYPTION

Information inside the database is shared by multiple parties and sensitive data stored in database could be a target to attackers (external /within the organization).Adding the database encryption, valuable information in database becomes more secure since the encrypted data ensure the confidentiality of the data. A new affine block cipher named Enhanced Affine Block Cipher technique is proposed for database encryption, which improves the weakness of the original affine cipher and have modification on Cipher Block Chaining (CBC) mode of operation for block cipher [3].To enhance database security, we can use the combination of substitution and transposition ciphers. When affine cipher or keyed transposition cipher techniques are used individually, cipher text obtained is easy to crack. Therefore combination of both produces a cipher text that is hard to crack [6].

A. Enhanced Affine Block Cipher

There are two main approaches for database encryption which is whether performing encryption and decryption inside the database or performing encryption and decryption outside the database. The best ways to secure the information stored in database is database encryption and apply it at outside the database i.e. at application level encryption. This approach was selected because it provides good end-to-end data protection. Cipher Block Chaining (CBC) mode adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the previous cipher text block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same cipher text. The affine block cipher [11] is one of the symmetric key cryptography that was known as classical cryptography and it is easier to break by cipher text-only cryptanalysis. This approach applied end-to-end encryption between client and

applications server. For encryption process, the data is encrypted at application server and then inserted into the appropriate fields or columns in the database. For decryption process, the encrypted information is retrieved from the database and then decrypts it at application server so that only authorized user can see the information. The keys used to encrypt and decrypt the data in this approach is stored in file storage at application server not in the database. Hence, this approach will add one security layer in securing the data stored in the database. The keys must be found before the attacker can see and know the contents of data.

Acknowledgment

The authors wish to thank Nitha K P, as well as the members of the Department of Computer Science of our college for useful discussions and comments on this research.

References

[1] Tashiro, H.; Lau, A.; Mori, J.; Fujii, N.; Kajikawa, Y. "Email network analysis for leadership", Industrial Engineering and Engineering Management(IEEM), 2011 IEEE International Conference on, On page(s):1456-1460

[2] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod Secure Authentication with 3D Password ,International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.

[3] Noor Habibah Arshad, Saharbudin Naim Tahir Shah, Azlinah Mohamed,Abdul Manaf Mamat, "The Design and Implementation of Database Encryption",International Journal of Applied Mathematics and Informatics, issue 3,Volume 1, 2007.

[4] Sonia Chiasson, P.C. van Oorschot, Robert Biddle, Graphical Password Authentication Using Cued Click Points

[5] Muhammad Daniel Hafiz, Norafida Ithnin, Abdul Hanan Abdullah, Hazinah Kutty Mammi, "Usability Features of Graphical Password in Knowledge Based Authentication Technique"..

[6] Shishir Shukla, Prabhat Kumar Verma, " Implementation of Affine Substitution Cipher with Keyed Transposition Cipher for Enhancing Data Security",International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1, January 2014 ISSN: 2277 128X.

[7] Lavanya Reddy L,K.Alluraiah,"ECCP: Enhanced Cued Click Point Method for Graphical Password Authentication",International Journal of Advanced Research in Computer Science and Software Engineering, Volume3,Issue8,August2013ISSN:2277128X.

[8] Susan Wiedenbeck,Jim Waters, Jean-Camille Birge,Alex Brodskiy,Nasir Memon , " Authentication Using Graphical Passwords: Basic Results".

[9] Xiaoyan Fu, Seok-Hee Hong, Nikola S. Nikolov, Xiaobin Shen,"Visualization and Analysis of Email Networks".

[10] Ralf Holzer,Bradley Malin,Latanya Sweeney,"Email Alias Detection Using Social Network Analysis"

[11] Jure Leskovec,Kevin J. Lang, Michael W. Mahoney,"Empirical Comparison of Algorithms for Network Community Detection".

[12] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi , " Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique", Second Asia International Conference on Modelling and Simulation.

[13] Elmasri and Navathe,"Fundamentals of database systems",pearson Education,2004.

[14] Silverschatz A,Korth H.F, Sudharshan S,"Database System Concepts",Tata McGraw Hill.

[15] Ullman J.D,"Principles of Database Systems",Galgotia Publications.