Two Dimensional Passwords

Alochukwu Vincent Animalu & Mamilus A. Ahaneku*
Department of Electronic Engineering, University of Nigeria, Nsukka.
alochukwu.animalu@unn.edu.ng; mamilus.ahaneku@unn.edu.ng
*Corresponding author

Abstract- Password has become a vital area in computer/mobile phone security. Cryptography, which involves encryption and decryption, has to deal with the secrecy of its password (pass-code, or key or passphrase). Information transmitted over the network is not secure and can be observed and recorded by eavesdroppers. This information can be replayed in attempts to access the server. Again, imposters can attempt to gain unauthorized access to a server, for example, a bank account or a database of personal records. The need to ensure a secure password cannot be overemphasized. In this paper, we have presented two systems using two-dimensional passwords. First system will comprise the arrangement of the letters in which the password is made to appear in a tabular format (matrix). The second system will authenticate an action when all participants in a transaction enter their passwords in a two dimensional format. An example of the second system is where a treasury of bank account of an organization is to be enabled by more than one person in an e-banking. The system ensures that all the clients involved in the authentication are pre-informed as they are also involved in the transaction thereby improving the overall security of cryptography. Furthermore, we depicted an improvement over existing two-dimensional passwords.

Keywords*: Cryptography, encryption, decryption, password, key, passphrase*

1. Introduction

Password or passphrase or passcode or simply key is defined as a string of characters used for authenticating a user on a computer system [1]. For example, you may have an account on your computer that requires you to log in. In order to successfully access your account, you must provide a valid username and password. This combination is often referred to as a login. It should be noted that usernames are generally public information, while passwords are private to each user.

2. Literature Review

In this section, some of the works done in the area of password are reviewed. Timothy S. Dare, et al patented a work in which they presented a method for authenticating an authorized user to multiple computer servers within a distributed computing environment after a single network sign-on is disclosed. In accordance with the method and system of their invention, an authentication broker is provided within the distributed computing network. The authentication broker first receives an authentication request from a workstation. After a determination that the authentication request is valid, the authentication broker then issues a Kerberos Ticket Granting Ticket to the workstation [2].

Jakob Nielsen invented and patented a work on password helper using "A Client-Side Master Password" which automatically presents the appropriate server-side password to a particular remote server. He explained further that a user operating a client System may access a plurality of remote Servers requiring passwords for access by employing a master password. The master password is used to decrypt a stored password for a particular remote Server to which the client desires access. The client System maintains a database of encrypted passwords and user IDs for remote Servers to which the user is registered. Although each remote Server is accessed using a different password, the user need only remember one master password [3]. In such system only the master password needs to be remembered by the client.

Greg E. Blonder also invented and patented a work on graphical password, A graphical password arrangement displays a predetermined graphical image and requires a user to "touch' predetermined areas of the image in a predetermined sequence, as a means of entering a password. The password is set by allowing the arrangement to display the predetermined areas, or "tap regions', to a user, and requiring the user to position these tap regions in a location and sequence within the graphical image, with which the user desires the password to be set at [4]. This invention is illustrated using the Figure 1(a) and (b).

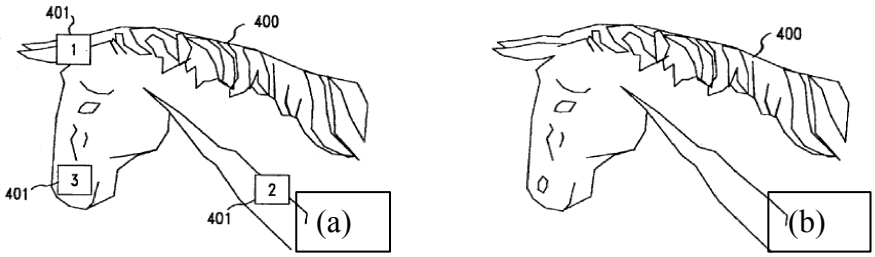

Figure 1: (a) Graphical image used for pass-wording (b) Graphical image to be clicked or touched [4]

It is important to mention that before the diagram appears on a screen for the right portion to be clicked or touched, there is no indication to show where the client is going to be clicked or touched. Figure 1(a) shows the graphical image used for passwording, while Figure 1(b) shows how it looks like at the beginning.

Finding from our literature review revealed that, although graphical password invented by Greg E. Blonder could be seen as a two dimensional password in a graphical format, for every client to have his or her own image for pass-wording, will occupy a lot of memory space since we know that images occupy thousands or sometimes millions of bytes for storage. We believe that our two dimensional password, which is, in form of matrix occupies less storage space.

3. Network Attacks On Computers/Mobile Phones

In this section, different ways in which attack is made on a computer/mobile phones and different types of attack on a network are depicted. It is important to note that some of these could expose a password if not encrypted. But with the techniques we are elaborating in this paper, it becomes certain that passwords security can be enhanced. Public communication networks traditionally have not been secured in the sense of providing high levels of security for the information that is transmitted. As these networks are increasingly used for commercial transactions, the need to provide security becomes critical. As we know many transactions take the form of a client/server interaction (that is distributed computing). Figure 2 shows several threats that can arise in a network setting [5]:

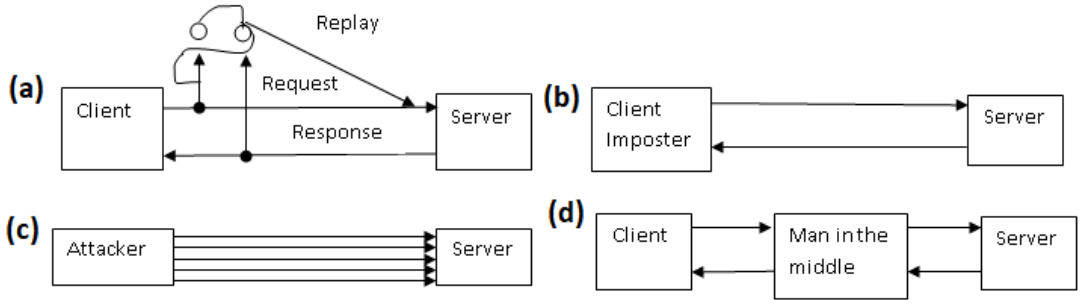

Figure 2: Network Security Threats [5]

- Information transmitted over the network is not secure and can be observed and recorded by eavesdroppers. This information can be replayed in attempts to access the server.
- Imposters can attempt to gain unauthorized access to a server, for example, a bank account or a database of personal records.
- An attacker can also flood a server with requests, overloading the server resources and resulting in a denial of service to legitimate clients.
- An imposter can impersonate a legitimate server and gain sensitive information from a client, for example, a bank account number and associated user password.
- An imposter manages to place itself as the man in the middle, convincing the server that it is the legitimate client and the legitimate client that it is the legitimate server.

These threats give rise to one or more of the following security requirements for information that is transmitted over a network [6]-[9].

In a paper, "Overview of the Candidates for the Password Hashing Competition And Their Resistance Against Garbage-Collector Attacks," Christian Forler, et al provided a work on an overview (functionality, security, general properties) of the candidates of the Password Hashing Competition, which are not yet withdrawn. Further, they analyzed each algorithm regarding to its vulnerability against garbage-collector and weak garbage-collector attacks – two attack types were introduced in their work. For more information on this see reference [10].

In the above, some attacks are mentioned, other forms of attacks are that done software wise or through calls are given below [11]:

- Phishing [12] /spear phishing, in which unsolicited emails tricks you to open an attachment.
- Spoofing/spoofed websites, in which you are directed to a fake website that tricks you into giving away your login details.
- Unsolicited calls, in which you are cajoled or threatened into doing something, usually involving money.
- Confidence scams, in which your confidence is built up until you comply with some demand.
- Hijackscams (viruses, Trojan horses, ransomware), in which malicious software is installed on your computer, tablet, or phone.

With suitable secure protocol and passwords and being meticulous, all of these attacks can be minimized. Also, Michelle Mazurek and Blase Ur in their book [13] suggested using one way hash function as one of the best practices in storing password. Although, this paper is not on cryptography [14], in general, it is important to note that encrypting a password before

transmitting it on a network will further facilitate its security. For more on cryptography, see reference [15]-[25]

4. Contribution

In this section, a showcase of the two systems which we developed was presented. They are:

i) Two Dimensional Password with Different Forms of Entry, and

ii) Multiple Passwords for Single Authentication System

4.1 Two Dimensional Passwords with Different Forms of Entry

The best way to illustrate this system is by using examples shown in Figure 3 (top and bottom), respectively. In this example, a matrix is displayed for the user to enter his/her password.

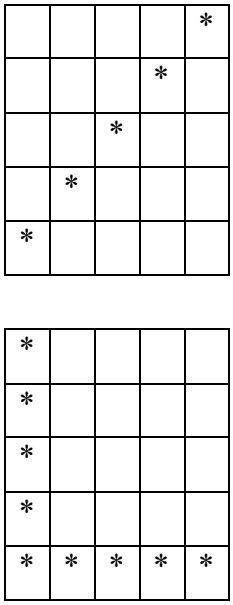

Figure 3: Two Dimensional Password with Diagonal Entry (top) and with L-Shaped Entry (bottom)

The user determines how and in what order to place the letters, vertical, horizontal, diagonal, etc. The order can also be random, provided the client remembers the letters and the order it is keyed in and this is an improvement to exiting system.

4.2 Multiple Passwords for Single Authentication System

Two-dimensional passwords can enable more than one person to authenticate an action.

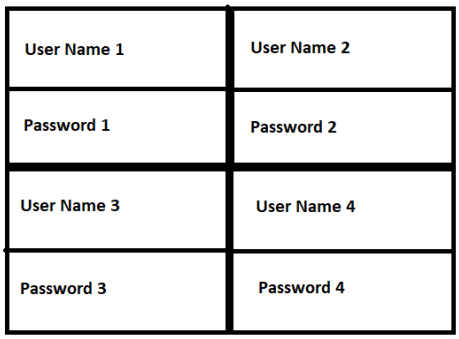

Figure 4: Multiple Passwords for Single Authentication System

In Figure 4, once all the individuals involved put their user names and passwords within a specific time meant for signing in, then the action needed takes place. In the system, the

authentication is designed for four persons, in real world; the number of user names and corresponding passwords could be less or more.

4.3 Applications

1. Banking systems: In a banking system where more than one person possesses the same account in the bank. To make a transfer, all the individuals who have to authenticate the move with their passwords must have presented their passwords within a specific time for the transaction to take place. It is possible that the treasurer may not have password to enable withdrawal or transfer of money but may have to call the attention of the chairman, secretary, financial secretary, etc. of the group or organization before such transaction could take place.
2. Accessing Information belonging to a group: For example, e-mail belonging to an organization could be accessed by the secretary or public relation officer only when it is authenticated by the group of people responsible for it.
3. Opening an electronic door or pass-worded security door can only be enabled when the owners or authorizers enter their passwords. Examples of such security rooms are where money, golden jewelries, golden ornaments, etc., are kept.

5. Conclusion

To conclude this paper, we presented some literature on password, discussed different forms of attacks on a system, which could be a networked or stand-alone system. We finally presented our own systems which are; (1) Two Dimensional Password with Different Forms of Entry and (2) Multiple Passwords for Single Authentication System. We believe these systems when integrated into existing ones will help to increase the strength of a cryptography with regards to password or passcode secret since it requires both the correct spelling of the password and how it is arranged in the two dimensional matrix. In the case of Multiple Passwords for Single Authentication System, it ensures that all the clients involved in the authentication are informed and are also involved in the transaction.

References

[1] https://techterms.com/definition/password, June 2020

[2] Timothy S. D., et al, (1997) Method And System For Authentcating Users To Multiple Computer Servers Via A Single Sign-On, United States Patent. Patent Number: 5,684.950, November 4, p.1.

[3] Jakob N. (1999), Password Helper Using A Client-Side Master Password Which Automatically Presents The Appropriate Server-Side Password To A Particular Remote Server, United States Patent, Patent Number: 6,006,333, December 21.

[4] Greg E. Blonder, Graphical Password, United States Patent, Patent Number: 5,559,961, September 24, 1996.

[5] Animalu A. V.(2015) , Improving Computer/Network Security Using File Encryption And Decryption, Master of Science Thesis, University of Nigeria Nsukka. p. 33.

[6] [Minoru E. (Editor) (2005), Next Generation Mobile Systems 3G and Beyond, John Wiley and Sons Ltd; England, p. 285.

[7] Savo G. and Beatriz L. (2009), Advanced Wireless Networks Cognitive Cooperative and Opportunistic 4G Technology, 2nd Edition, John Wiley and Sons Ltd; United Kingdom. p. 632

[8]Frank O. (2004) Voice over 802.11, Arthech House, Inc, Norwood, pp.100-101.

[9] William S. (2003), Data and Computer Communications, 5th Edition, p. 623.

[10] Christian F. et al (2015) Overview of the Candidates for the Password Hashing Competition And Their Resistance Against Garbage-Collector Attacks, Technology and Practice of Passwords International Conference on Passwords, PASSWORDS'14 Trondheim, Norway, December 8–10, 2014 Revised Selected Papers, Published by Springer, New York, p. 16.

[11] Jason M. (2018), The Password Book: Internet Security & Passwords Made Easy, Published by Excerpti Communications, Inc. p. 19.

[12] James G. R. and Howard R, O, (Editors) (2011), CYBER SECURITY ESSENTIALS, Published by Taylor and Francis Group, LLC, U.S.A., pp. 87-89.

[13] Michelle M. and Blase U. Introduction to Password Cracking & Research on Passwords, University of Maryland, p.21.

[14] Al S.(2018), Cracking Codes with Python An Introduction to Building and Breaking Ciphers, Published by William Pollock, U.S.A. p.2.

[15] Neal K. (1994) A Course in Number Theory and Cryptography, 2nd Edition, Published by Springer-Verlag New York.

[16] Richard A. M. (2007), An Introduction to Cryptography, 2nd Edition, Published by Taylor & Francis Group, U.S.A.

[17] Bruce Schneier, Applied Cryptography, Protocol, Algorithm and Source Code in C, 2nd Edition.

[18] Michael W. (2005), Cryptography in C and C++, Published by Apress, U.S.A.

[19] Atul K. (2008), Cryptography and Network Security, 2nd Edition, Published by Tata McGraw- Hill, New Delhi.

[20] Jonathan K. and Yehuda L. (2008) Introduction to Modern Cryptography, Published by Chapman & Hall/CRC, U.S.A.

[21] Jean-Philippe A. (2018), Serious Cryptography: A Practical Introduction to Modern Encryption, Published by No Starch Press, Inc, San Francisco.

[22]Christof P. and Jan P. (2010), Understanding Cryptography: A Textbook for Students and Practitioners, Published by Springer, New York.

[23] Samuel B. (2018) Hands-On Cryptography with Python: Leverage the power of Python to encrypt and decryp data, Published by Packt, Mumbai.

[24] Hans D. and Helmut K. (2007), Introduction to Cryptography: Principles and Applications, 2nd Edition, Published by Springer, India.