Dynamic Grid Based Authentication With Improved Security

Anjali Somwanshi[1], Devika Karmalkar[2], Sachi Agrawal[3], Poonam Nanaware[4],

Mrs. Geetanjali Sharma[5]

Department of Information Technology

D. Y. Patil College of Engineering

Pune, Maharashtra

India.

ABSTRACT:

Today IT infrastructure is one of the important parts of everyone's life. Various applications are used for string managing and transferring data from one place to another. We have various techniques to secure these applications. Textual password is most commonly used authentication technique for securing these applications. Authentication schemes are vulnerable to various types of attacks. The proposed system provides solution to the attacks namely, 'Keystroke Logging', 'Shoulder Surfing' and 'Duplicate Login Pages'. The system improves login security mechanism.

Key Words: P*assword, Authentication, Security.*

I. INTRODUCTION

Today computer and internet has become one of the key necessities of human being. There are many applications for real world problems. These applications are used to store different types of data and manipulate it. To secure all these application various authentication techniques are being used. Banking, defense, e-commerce, business uses number of applications. Security techniques have a paramount importance in any system where user's identity is a matter of concern [1].

Authentication is the process to verify user's identity i.e. username and password and accordingly avail the resources. Knowledge based authentication mechanism that provides the text passwords are used in many of the web applications today. Many times the username is so common that the attacker can easily guess it. Once the attacker is aware of the username, now he can easily get the password by various techniques like permutation-combination, trial and error, etc. Many techniques are used to provide the authentication to the system. Passwords are the strongest strength of authentication. These are simple alpha-numeric arrangement of strings shared between user and the server [5].

The system becomes secured by random and lengthy passwords. But these lengthy passwords are difficult to remember. Research tells that users tend to pick short passwords that are easy to remember. Unfortunately, these passwords are easily cracked by attacker. The vulnerabilities for textual passwords are shoulder surfing, key stroke logging, social engineering, dictionary attack, etc. [1] [2].

II. RELATED WORK

Authentication is responsible to verify the identity of the user. There are various authentication techniques available like textual passwords, graphical passwords and biometrics. As compared to others, textual password is most popular technique. It is a combination of alphabets and special characters. Generally the user tends to have short and simple password i.e. spouse's name, pets name, favorite dish name etc. To avoid attacks from attacker's user can choose any random or lengthy password. But they are not easy to remember. Various attacks possible on the textual passwords are Shoulder Surfing, Dictionary attack, Social Engineering, Key Stroke Logging, Brute Force attack, Eavesdropping etc. [3].

III. ATTACKS ON AUTHENTICATION TECHNIQUE

1. Shoulder Surfing

Shoulder surfing is a type of social engineering technique used to obtain information of the user like username, password and other confidential information by looking over the victim's shoulder. This attack can be done by either of the two cases like the attacker is at a close distance and he is directly looking into the victims computer or if he is at a longer distance he can use a pair of binoculars. Technical skills are not required to perform this type of attack, in depth observation and typing pattern is sufficient. Places which are heavily crowded are susceptible to this type of attack.

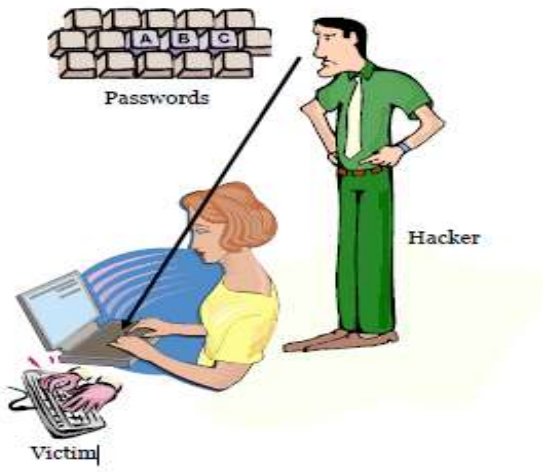

Figure1. Shoulder Surfing

2. Keystroke Logging

Keystroke logging also known as key logging or key loggers is the way of tracking the keys pressed on a keyboard, in such a way that the user is unaware of being monitored by the attacker [4].

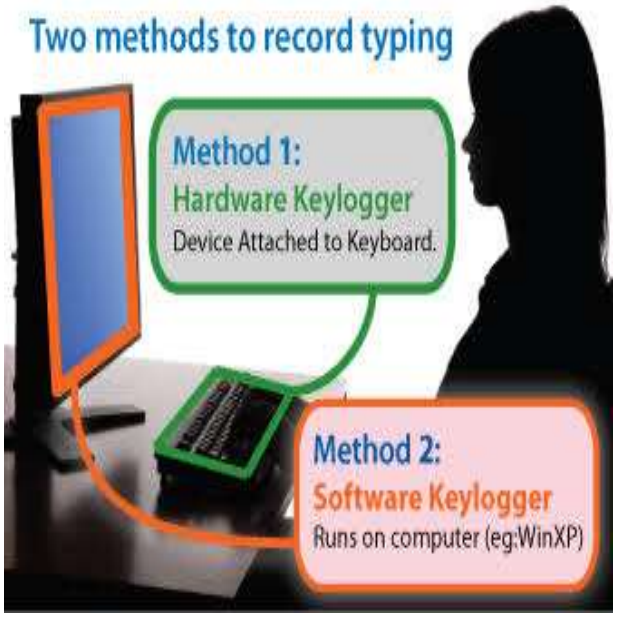

Figure2 Keystroke Logging

There are various key stroke logging methods, like hardware and software based approaches.

2.1 Software based Keystroke Logging

Key loggers are used in IT firms to handle technical problems with computer systems and business networks; it is also designed to execute on the operating system of target computer. To monitor the network usage people use these key loggers without user's direct knowledge. However, unknown and unauthorized individuals can use key loggers on public computers to get passwords or credit card information. HTTPS encryption is incapable of stopping most key loggers because it only secures data in transit between computers, thus the threat is being transferred from the user's computer.

2.2 Hardware Keystroke Logging

Hardware key loggers are used for keystroke logging. It is a method of monitoring, capturing and recording key stroke of the users system, including sensitive passwords. They can be implemented either via BIOS-level firmware, or via a device introduced in between a computer and a keyboard. All the keyboard activities are logged by the internal memory.

IV. Authentication Schemes

Following are the authentication schemes:

1. Textual Password
2. Graphical Password
3. Biometric
4. Dynamic Grid based Password

Following table shows the attacks possible on the above scheme.

Table 1. Comparison of Authentication technique [3].

Authentication Schemes	Cost	Protection Level	Processing Time	Additional Hardware Required
1)Textual Password	Low	Medium	Low	No
2)Graphical Password	High	Medium	High	Yes
3)Biometric	High	High	High	Yes
4)Dynamic Grid Based	Low	High	Low	No

Table 2.Attacks on the Authentication technique [3].

Authentication Schemes	Attacks	Resistant to Attacks	Cost
1)Textual Password	Eves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Eves Drooping, Guessing	--	Low

2)Graphical Password	--	Eves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Eves Drooping	High
3)Biometric	--	Eves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Eves Drooping	High
4)Pair Based Dynamic Grid	--	Eves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Eves Drooping	Low

From the above table we can see that except textual password all other schemes resist various attacks but their implementation cost is high.

V. DYNAMIC GRID BASED PASSWORD AUTHENTICATION SYSTEM

The system consists of 6X6 matrix of 26 alphabets and 10 digits to enter the password. While registering in the system the user need to give his private key which will be used while entering the password into the grid. The private key of the user will never be used anywhere hence there are no chances of getting the password cracked [4].

A lot of research is been done on the grid based authentication system. The advanced thing we are doing here is securing the private key. Suppose the user decides that the private key is ABC i.e. ABC would be half part of private key and remaining half of it would be sent to the user's registered mobile number or email-id which is implemented using OTP example DE, therefore while entering the password to grid, it would be the combination of the private key selected by user and the one which is generated by OTP i.e. ABCDE, hence the system becomes more secured.

While entering the password into the grid, firstly divide the private keyword into the pair of two letters in a single pair, and then find the intersection of that two letters. The intersection letter will be the row of first alphabet and column of second alphabet. Similar steps followed for the next pair of the private keyword. If the length of the private keyword is odd then the last letter should be taken as it is from the grid.

VI. EXAMPLE

Suppose the private keyword is "ABCDE" then the password will be "9NE".

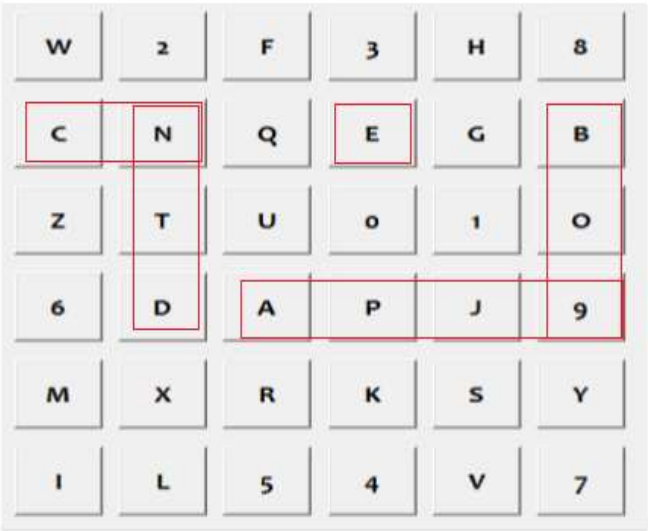

Fig 3. Intersection Letters for Keyword "ABCDE"

Next time during password input he will get different grid. So the keyword will be same but password will be different. Now for the same keyword "ABCDE" password will be "TWE"

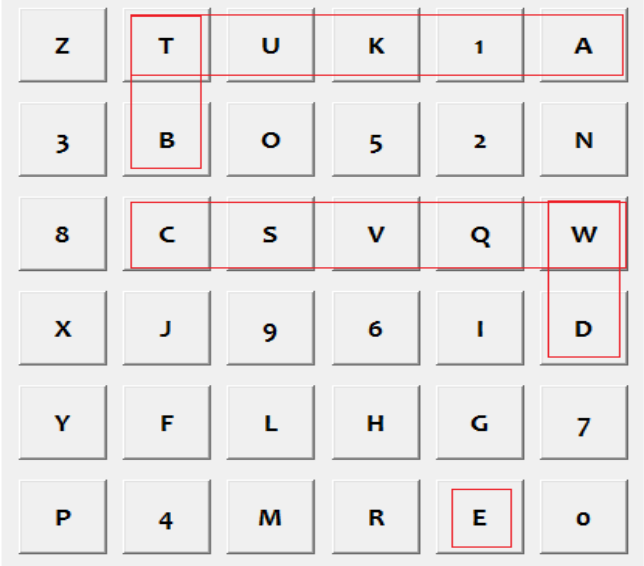

Fig 4.Intersection Letters for Keyword "ABCDE"

CONCLUSION

In this paper we have discussed various attacks and authentication schemes and have also compared all of the techniques used for authentication. The proposed work i.e. Grid based authentication system is more powerful and

secured as compared to the other authentication techniques as it provides security and protection from attacks such as "Shoulder Surfing", "Keystroke logging" & "Duplicate login pages". Therefore the vulnerabilities are also reduced to an extent. Many websites should adopt this technique to enhance the security level of their system.

REFERENCES

[1] Vijayshri D. Vaidya, Imaran R. Shaikh, "*Authentication Using Grid-Based Authentication Scheme and Graphical Password"*, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015

[2] Harsh Desai, Ninaad Suvarna, Dipen Desai and Simranjeet Singh Chawla, Prof. Sowmyashree, *"Grid Based Authentication Password Using Hash Technique",* International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 4, Issue 5(2), September - October 2015

[3] Janhavi Thakur, Sheetal Rathi, *"Pair Based Authentication using Dynamic Grid",* International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3, Issue: 8, August 2015

[4] Yogesh Mali, Viresh Chapte, *"Grid Based Authentication System",* International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 10, October 2014

[5] Shivani Agrawal, Adil Zafar Ansari, M. Sarosh Umar, *"Multimedia Graphical Grid Based Text Password Authentication",* IEEE, 2016

[6] Mun-Kyu Lee *"Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry"*,IEEE Transaction 2014.

[7] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao *"A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme"*, IEEE Conference 2014

[8] D.Aarthi, Dr.K.Elangovan *"A Survey on Recall-Based Graphical User Authentications Algorithms"*, IJCSMA Feb 2014

[9] Dr Harsh Kumar Sarohi, Farhat Ullah Khan*,"Graphical Password Authentication Schemes: Current Status and Key Issues"*, IJCSI March 2013.

[10] Devika S, Backiyalakshmi R*,"Design and Analysis of User Identification for Graphical Password System"*, IJCSIT March 2014.

[11] A.R.Johnson Durai, V .Vinayan, *"A Novel Crave-Char Based Password Entry System Resistant to Shoulder-Surfing"*, IMECS May 2014.

[12] William Stallings and Lawrie Brown, "*Computer Security: Principles and Practice",*Pearson Education, 2010.

[13] J. Goldberg, J. Hagman, and V. Sazawal, "*Doodling our way to better authentication*", in Proc. of CHI '02 extended abstracts on Human factors in computing systems, 2002, pp. 868–869.