International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Attacks and Remedies of Authentication Techniques : A Review

Hiral Patil[1], Chandresh D Parekh[2]

[1]M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India
[2]Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

Most people now access all the important areas of their life banking, shopping, insurance, medical records, and so on-normally by typing a username and password into a website. A password based mechanism is the mostly used method of authentication in distributed environments. Text based passwords are not so secure enough for real-time applications. Authentication plays a major role in protecting resources against unauthorized users. But now-a-days many user authentication systems suffer from limitations and security threats. Graphical passwords use images as passwords. Human brain is good in remembering picture than text. There are various graphical password techniques or graphical password software in the market The main goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

Keywords : Password, Password attacks, countermeasures, Authentication methods, Conclusion.

I. INTRODUCTION

Because of increasing threats to networked computer systems, there is great need for security revolutions. Today there is an increasing recognition that security issues are also fundamentally human computer intercommunication. Authentication is the process of finding whether a user should be allowed access to a particular setup. It is a demanding area of security research and practice. Alphanumeric passwords are used universally for authentication, but other methods are also available now-a-days, with biometrics and smart cards. Shortage of awareness About how attackers influence to attacks. unsuccessfully, these passwords are broken unkindly by intruders by any simple means such as masquerading, Eaves dropping and other attacks like dictionary attacks, shoulder surfing attacks, social engineering attacks. To reduce the problems with traditional methods, advanced methods have been proposed using graphics as passwords. There is a fast and growing interest in graphical passwords for they are more or infinite in numbers thus providing more support. Authentication of humans is based on some merge of what you are (biometric), what you have (token), and what you know (password). In this paper, we give the overview of authentication techniques, the attacks on text based password, and also give analysis on importance of graphical passwords and their techniques.[1]

II. DIFFERENT TECHNIQUES INVOLVED IN AUTHENTICATION

Present authentication methods can be classified as follows:

- **Token based authentication:** Token based tactics, such as key cards, bank cards and smart cards are widely used. Many token based authentication systems also use knowledge based techniques to upgrade security. For example, ATM cards are generally used with a PIN number.
- **Biometric based authentication:** Biometric based authentication tactics, such as fingerprints, iris scan and facial recognition are not still widely accepted. The major fault of this approach is that such systems can be expensive, and the identification process can be slow and often unstable. However,

this type of technique provides the maximum level of security.

- **Knowledge based authentication:** Knowledge based tactics are the most widely used authentication techniques and combine both text-based and picture-based password.

The picture-based techniques can be further split into two categories:

- **Recognition-based:** Using recognition based techniques, a user is presented with a set of images and the user is authenticated by observing and identifying the images he or she selected during the registration stage.
- **Recall-based:** a user is asked to recreate something that he or she created or selected earlier during the registration stage.[2]

III. TYPES OF ATTACKS ON TEXT BASED PASSWORDS

- **Dictionary attacks:** A dictionary attack is a method of breaking into a password secured computer or server by systematically entering every word in a dictionary as a password. Many users generally write passwords similar to the names of birds, familiar places, famous actor's names etc. These passwords can be broken by the dictionary attack. A dictionary attack can also be used in an attempt to find the key need to decrypt an encrypted message or document.
- **Guessing attacks:** Depending upon our brain's emotional connections we sometime gives password to the things that we likes, so the chances are that there may be random passwords based upon our interest, hobbies, pets, family, activity& so on. Actually password are based upon the things that we like to chat on social networks and even we involve in our profile, so the attacker can look very accurately at these information for guessing the password.
- **Key Logger Attacks:** A hacker or attacker uses a program to track all of the user's keystroke so that at last everything that the user has typed along with his login IDs and password have been recorded. A key logger or screen scraper program which are the malware virus or full blasted virus programs that can be installed by malware which records everything user typed on his/her screen. These programs can be installed directly by the hacker or they invent the trick to install this program by user through email by clicking or downloading the link so these programs must be first make on the user's device. Some malaria will look for the existence of a web browser client password file and copy this which, unless properly encrypted, will contain easily got saved passwords from the user's browsing history. Even though stronger passwords don't give much higher security against the key logger attacks.
- **Shoulder Surfing:** The most confident of hackers will take the appearance of a parcel courier, aircon service technician or anything else that gets them access to an office building. Once they are in, they will notice the staff members how they are entering the passwords, the attacker scheme out the user to install that file into his name of spying in which attacker spies the user's system then the key logger makes the log file of his login actions & then sends it to the attacker's file. The attacker monitors the user how he/she enter the password, in how much time, what keys of the keyboard the user has pressed & hence attacker get the password & then he can access the target system. The attacker can use the binocular to see the video recording of the user that how he/she enter the password all these recording can be seen from remote place with the help of mobile camera or any other such devices, use the hidden close circuit TV camera to monitor the camera, inspects the recorded video of user's password entering from a remote location. The attacker can listen the password entered by the user in it user's password that how many keys the user has pressed and actions are recorded once or twice then the attacker uses all the possibilities related to the password length to crack it.
- **Rainbow table attack:** A rainbow table is a list of pre-computed hashes i.e. of an encrypted password used by most of the systems used now-a-days. Hashes mean the numerical value of an encrypted password, and that is the hashes of all possible password combinations for any given hashing algorithm. The time it takes to break a password using a rainbow table is decrease the time it takes to look it up in the list. However, the table itself will be huge and needs some serious computing horse power to run, and it is waste if the hash it is trying to find has been 'salted' by adding random characters to the password before applying the hashing algorithm. It is said that salted rainbow

tables are exist, but these would be so vast as to be difficult to use in practice.

- **Offline cracking:** Passwords are secure in blocking automated guessing applications because after entering incorrect password it will automatically block the system .but in real password cracking can takes place offline outside the system using a set of hashes in a password file that has been 'achieved' from a compromised system. In this method hacker can take a captured password hash & turning it to its original plaintext. To crack a password, an attacker requires tools such as extractors for hash guessing, rainbow tables for studying the plaintext passwords, and password sniffers to extract authentication information.
- **Sql injection attack:** The imperfectly designed websites are the victim of this type of attacks. In this attack the attacker can inject the SQL commands & gain access to derive the data from database. It is a code injection technique used to attack on websites & login with administrator advantage.
- **Social engineering:** The practice of fooling the user into giving or giving access to sensitive information, thereby avoiding the most or all protection. Social engineering takes the entire 'ask the user' concept outside of the inbox that phishing tends to stick with and into the real world. EX. Suppose after hacking attempts failed a hacker attempted as social engineer by walking into the building or offices and claiming that he/she had to do some important work in the server room.
- **Password Resetting:** Attackers repeatedly find it much easier to reset passwords than to guess them. More password cracking programs are actually password resetters. In most cases, the attacker boots from a floppy disk or CD-ROM to get about the typical Windows protections. Most password resetters carry a bootable version of Linux that can mount NTFS volumes and can help to find and reset the Administrator's password.[4]
- **Video Recording Attack**: In such type of attack the attackers with the help of camera equipped mobile phone, observes the recorded video of users which enters password. In it user's password entry operations are recorded once or twice.[5]
- **Replay Attacks**: The replay attacks [5] are also familiar as the reflection attacks. It is a way to attack challenge response user authentication system. The method for this type of attack is that the attacker first enters his/her name in basic login connection. To authenticate the user, the receiving device sends the test to the sender (in this case attacker). The attacker opens another login at the same time with its own authoritative user name and replies the receiving device as challenge of previous connection. The receiving system accepts the challenge and responds to it. The attacker then sends back that response through the account to be hacked and therefore it gets authenticated. Then the attacker gain access to that account.

IV. SOLUTION OF THIS PROBLEMS

To solve the problems associated with text password based authentication systems, the researchers have suggested the concept of graphical passwords and developed the alternative authentication systems. Graphical passwords systems are the most. good alternative to conventional password based authentication systems. Graphical passwords use images instead of textual passwords and are relatively motivated by the reality that humans can remember images more easily than a string of characters. The proposal of graphical passwords was originally described by Greg Blonder in 1996. An essential advantage of GP is that they are easier to remember than textual passwords. Human beings have the potential to remember faces of people, places they visit and things they have seen for a longer duration. Hence, graphical passwords provide a means for making more user friendly passwords while increasing the level of security.

V. IMAGE BASED PASSWORD TECHNIQUES

Different Graphical Password tactics are
1. Pass-point Scheme,
2. Cued-click point Scheme,
3. Persuasive Cued-Click Point Scheme.

1. Pass-point Scheme: In this scheme a series of 5 dissimilar click points are consisted by a given image. For generating a password user select any sequence of 5pixels in the image as a cloud click point on same image and for login the user has to enter the same series of clicks in an accurate sequence on the image, then get further access to the system. The main disadvantage with this scheme is the HOTSPOTS because it is very easy for attackers to imagine the pixel points selected as password as user forms specific patterns to remember the secret code which result the pattern generation make easy for attackers to guess.

2. Cued-Click Points: Cued Click Point scheme was designed to reduce patterns and the use of hotspots for attackers. Inspire of selected 5click-points on single image, CCP technique uses one click -point on 5 different images. The next image in series is based on the location of the last entered click-point; it creates a sequence through an image series. One of the best points of Cued-Click Point is that it shows authentication failure only after clicking final click-point, to protect from guessing attacks. Drawback of these techniques are like false accept and false reject.[3]

3. Persuasive Cued Click Points: Persuasive Cued click points is technique in which convicing feature is included into cued click point for selecting less predictable password. PCCP uses viewport and shuffle for password generation. While creating password images are gently highlighted exclude for viewport which are randomly positioned to avoid known hotspots. The advantage of PCCP is password theft have to improve their guesses where user shave to choice a click points within the selected viewports and after clicking on shuffle button click outside of the viewport for randomly positioned the view port. PCCP technique is suffered from security drawback at some level.[6]

VI. Existing Image Authentication Techniques

The important techniques for authenticating an image are as follows,

- Watermarking based authentication technique
- Cryptography based authentication technique
- Robust image hashing authentication technique

1) Watermarking based authentication

Digital watermarking is the art and science of embedding copyright data in the files; the data which is embedded in files is called watermarks. Digital watermark is one of the signals which are attached to a document to authenticate it and to prove the ownership. Two methods for watermarking data authentication are fragile watermarking and robust watermarking.

Benefits of watermarking

- Uniquely identify the writer of copyright work.
- Implementation on private computer platform is possible.
- Embedding watermarks is so easy.
- Image altering detection.

Drawback of watermarking

- Doesn't prevent image duplication.
- Watermark disappears if someone manipulates the image.
- Resizing, compressing images from one file type to another may decrease the watermark and it becomes unreadable.

2) Cryptographic–based authentication

Cryptography is the science of changing the documents or images. It contains two functions encryption and decryption. Algorithms based on conventional cryptography show valuable results for image authentication with high tamper detection. Localization performances are not better but may be acceptable for some applications. The image is classified as manipulated, when just only one bit of this image is altered; this is very critical formost of applications.

Benefits

Conventional cryptography show valuable results for image authentication with high tamper detection.

Drawbacks

- Localization performances are not so good.
- Hash functions are more sensitive.
- Understanding of private key.
- Identical to distinguish between malicious and innocuous modification.
- Delay in communication.

3) Robust image hashing –based authentication: Perceptual hash function (PHF) extract a set of features from the image to form a solid representation which can be used for authentication. Robustness, fragility and security are the three key problems of image hashing. Robustness needs that image hashing should be invariant to minor modifications, such as JPEG compression, blur, noise, enhancement and some other constantly similar operation. Fragility means that the image hashing should have the potential to distinguish the visually distinct images. Security is the degree to prevent the attacker from tricking the authentication system with a maliciously altered image. A tough and secure image hashes using Zernike moments, is based on rotation invariance of magnitudes. In image processing, orthogonal rotation invariant moments (ORIMs) can effectively catch essential information in an image.

Benefits

- Hashes produced are robust against usual image processing operations including brightness adjustment, scaling, small angle rotation, JPEG coding and noise contamination.
- Collision probability between hashes of dissimilar images is very low.
- Reasonably short hash length and best ROC performance.

Drawbacks

- Large part cropping[7]

VII. CONCLUSION

Authentication is an important part of a network's security scheme, as it is the system for ensuring that the identity of a user, computer, or service is valid. There are a number of different ways that authentication can be accomplished, depending on network operating system and connection type. In this Daily Drill Down, I have provided an overview of some of the most common authentication methods, under what situations each is used, and how they work. In this review paper, a survey over existing graphical password protection techniques has been presented. A review over the benefits and drawbacks of the password protection techniques is also presented. This survey will help us in developing more secure and efficient graphical password based authentication schemes to provide the better security to the user data.

VIII. ACKNOWLEDGEMENT

I would like to thank my guide prof. Chandresh D Parekh for this help and guidance throughout this project. Thanks to all my family members for their affection, care and encouragement. Special thanks to my college for giving me the valuable knowledge.

IX. REFERENCES

[1]. Neha Vishwakarma, Kopal Gangrade, "Secure Image Based One Time Password", International Journal of Science and Research(IJSR), ISSN(Online): 2319-7064,Index Copernicus Value(2013):6.14|Impact Factor(2015):6.391

[2]. R.V.Sudhakar1, A. Mruthyunjayam2, D. SugunaKuamari, M. Ravi Kumar,B.V.S. Ramesh Babu5," Improving Login Authorization by Providing Graphical Password (Security)", R.V.Sudhakar et al Int. Journal of Engineering Research and Applications, ISSN : 2248-9622, Vol. 3, Issue 6, Nov-Dec 2013, pp.484-489

[3]. SurajHande, Nitin Dighade ,RuchalBhusari, MrunaliShende,Prof. Heena Agrawal "Image Based Authentication for Folder Security using Persuasive Cued Click-Points and SHA" IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. IX (Mar-Apr. 2014), PP 124-128

[4]. Savita Kamalakarrao Kulkarni" A Survey of Password Attacks, Countermeasures and Comparative Analysis of Secure Authentication Methods" International Journal on Advance Research in Computer Science and Management Studies, Volume 3,Issue 11, November 2015.(attack types)

[5]. Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider"A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication "World Applied Sciences Journal 19 (4): 439-444, 2012.(video recording attack,replay)

[6]. Ms. Jyoti Madhukar Shinde," Prevention Against Online Password Guessing Attacks Using Image Based Authentication Technique PCCP", Open Access International Journal of Science &Engineering, Volume 1, Issue 1 ,July 2016 .(Image Based Password Techniques:)

[7]. S.Jothimani, P.Betty," A Survey on Image Authentication Techniques" ,International Journal of Engineering Trends and Technology (IJETT) , Volume 7 ,Number 4,Jan 2014(Existing Image Authentication Techniques watermark)