Implementation of Secured Mail Server for Group Communication

Arunadevi M
Nadar Saraswathi College of Arts and Science, Theni, India

Abstract

Electronic communication is an emerging technique where we send information from sender to receiver in the form of E- Mail. To send and receive an Email, each user should have an ID. That ID must be locked with the unique password. The password is in the form of text. It may be alphabetical, numbers, alphanumerical and etc. Email servers provide the constraints to set the passwords, for the users. Even most of the servers secured, Black hat hackers hack the account and access the information. A graphical password is an authentication system that works by having the user select from images in a specific order, presented in a Graphical User Interface (GUI). The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, user tends to pick a passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember.

Keywords

Mail Identity, Threat Level, Level of Execution, Message Digest-5 Algorithm, Pretty Good Privacy.

I. Introduction

E-mail hacking is one of the most common attacks on the Internet. Almost all computer security enthusiasts – irrespective of their expertise level – are sure to have indulged in email account cracking at same point of time or the other. Most companies would find it difficult to survive even a single day without using the e-mail system. As more and more people start depending upon emails for both official and personal subsistence, the threat of e-mail account cracking is only going to increase.

The hugely critical role played by e-mail in today's world makes e-mail cracking all the more attractive from a criminal's point of view. Authentication plays a crucial role in protecting resources against unauthorized and illegal use [4]. A number of computer crime investigations also require police and forensic agencies to covertly break into the suspects email accounts to gather evidence. Possessive young lovers would do anything to be able to get a glance of their partner's email account contents.Friends acrosseducational institutions and organizations would love to break into each other's e-mail accounts simply as practical jokes. In this age of corporate espionage, many organizations strive to break into their competitors email accounts to gather as much as business intelligence as possible.

II. Techniques Involved in E-mail Hacking

E-mail account cracking is indeed one of the most exciting and sought after attacks through the Internet, though many industry veterans consider such attacks merely lame. Although there is no particular guaranteed method of breaking into a victim's e-mail account, there are definitely a few different techniques that are commonly used by attackers, namely:

- Password guessing
- Brute Force attack
- Forgot password attacks

E-mail systems are only as secure as the people using it. Unless all e-mail users are made aware of the security risks involved, it will be very difficult to successfully prevent any kind of e-mail fraud.

A. Password Guessing

Password guessing is probably one of the most commonly used password cracking techniques prevalent on the Internet, even though the success rate of such attacks is very low. In this attack, the hacker first gather as much personal information about the victim's like phone number, birthday, parents names, girlfriend's names, pet's names etc. and then simply tries his luck by entering different combinations of different names and numbers at the password prompt [7]. If the hacker is lucky then one such random combination might actually work. Some of the most common passwords that an attacker usually guesses are:

- Loved one's name + Birthday/Phone number, Vechile's+ Name/Number. For example Discover3328.
- Victims own name + Birthday/Phone number. For example abdulrahim3328.

B. Brute-Force Attacks

Brute force is probably one of the oldest techniques of password cracking known to the underground community. For most attackers, brute force password cracking remains the ultimate fallback attack if all other techniques fail. In this attack, an automatic tool or script tries all possible combinations of the available keyboard keys as the victim's password [7-8]. The amount of time it takes to complete these attacks is dependent on the criteria such as,

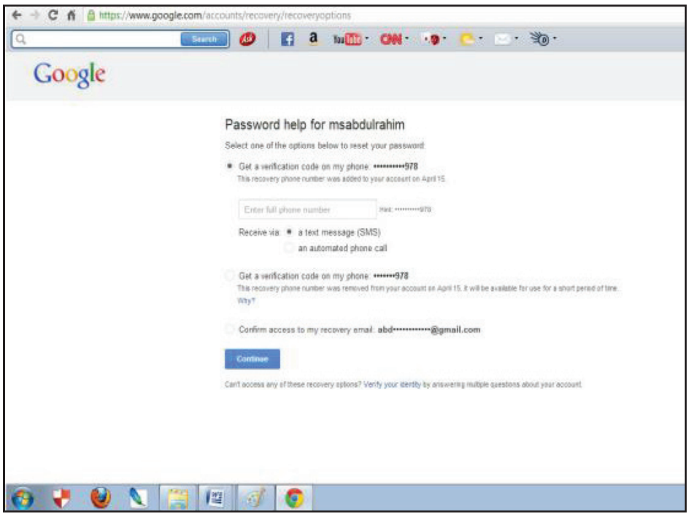
- Complexity of the password, and
- How well the attacker knows about the victim.

Such a hit and trial method of trying out all available permutations and combinations means that irrespective of the victim's password, it will sooner or later definitely be cracked. As soon as the correct password is found, it is immediately displayed on the screen. Obviously, due to the extremely high number of possible combinations of keystrokes, Brute Forcing can sometimes take an extremely long time to reach the correct password. However, if an attacker is lucky, then this technique will reveal the correct password within a matter of seconds. The success and speed of this technique largely depends upon the strength of the victim's password. From these attacks we can say,

Hacker's success rate 1/∞ Victim's password strength

C. Forgot Password Attacks

The forgot password attack can definitely be labeled as an extension to the password guessing attack. All e-mail service providers have an option that allows users to reset or retrieve their e-mail account password by simply answering a few pre-defined questions [7-8]. Ideally, e-mail service providers should ask users to enter only personal information that other people don't know to retrieve or reset the forgotten password.



Password help for msabdulrahim

Select one of the options below to reset your password

● Get a verification code on my phone: ••••••••••978
This recovery phone number was added to your account on April 15

Enter full phone number Hint: ••••••••••978

Receive via: ● a text message (SMS)
○ an automated phone call

○ Get a verification code on my phone: •••••••978
This recovery phone number was removed from your account on April 15. It will be available for use for a short period of time. Why?

○ Confirm access to my recovery email: abd•••••••••••••@gmail.com

Continue

Can't access any of these recovery options? Verify your identity by answering multiple questions about your account.

Fig. 1: Diagram of Retrieve a Password using Forgot Password Options of G-mail.

Unfortunately in reality, most e-mail service providers ask users, to enter publicly accessible information like country, ZIP postal code, birth date, city etc. An attacker can easily find out such information without much trouble, retrieve/reset the victim's password using the forgot password option and then gain access to the victim's e-mail account [7]. Some people like to enter false contact information may be a friend's contact details while registering a new e-mail account. Such a practice can sometimes prevent an attacker from cracking an e-mail account using this technique. Text-based passwords remain the dominant authentication method in computer systems, despite significant advancement in attackers' capabilities to perform password cracking [1]. By some general methods, we can protect our passwords.

Table 1. Analysis of Hacking Techniques

Methods	Threat Level	Level of Execution	Result Analysis	Rating
Password Guessing	Low	Easy	Very common & not effective.	*
Forgot password attacks	Mid	Easy	Very Effective	***
Brute-Force Attacks	High	Tedious & slow.	Effective.	**

We analyzed the above hacking methods based on two criteria's such as Threat level and Level of Execution (LOE). By the result analysis, we give rating to the methods.

III. Attacks Become Holes & Vulnerabilities of an Existing Mail Servers

A. Loophole under Brute-Force Attack & Password Guessing

- Existing mail servers allows hackers, to proceed Brute-force attack. (i.e.) If you want to hack someone's Email Id by Brute-Force attack means, you can try by typing an infinite number of wrong passwords for corresponding username. By this method, Hacker can identify the right password after some trials.

1. Loopholes under Forgot Password Attack

- If the hacker tries to get a password via Forgot password Attack, Mail servers provides an option "Get a verification code on my phone: **.......78**. By clicking that option, the corresponding user receives a message "Your Mail server's Verification code is ******." If the User doesn't have technical knowledge, he/she wouldn't know why such type of messages has come.
- Even while user set a code for Two-step verification method in Gmail, it sends a message "Your Google verification code is ******". There is no difference between in the messages of Retrieve the password and set the Two-step verification.

B. Vulnerabilities

- Mail servers allow users to maintain a same password for personal, financial and also for social networking websites. It's a major bug in Mail servers. Because of this, if a hacker hijacks victim's mail account means, he can hack corresponding mail's social networking account and also access the financial transactions.

IV. Proposed System

This unique and user-friendly 3-Level Security System is involving three levels of security, where the preceding level must be passed in order to proceed to next level. Text based passwords are not enough to compromise the above specified attacks. We concluded to implement some additional security system to ensure the account's security. So, we decided to install three level security measures.

A. Level 1

Security at this level has been imposed by using Text based password (with special characters), which is a usual and now an anachronistic approach.

B. Level 2

At this level the security has been imposed using Image Based Authentication (IBA), where the user will be asked to select from the two grids. Both the grids will be having 100 unique Image grids, from where the user has to select two, one from each grid.

C. Level 3

After the successful clearance of the above two levels, the 3-Level Security System will then generate a one- time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his signed up email-id. Any hacker if in the extreme case, suppose (although difficult) will cross through the above two mentioned security levels, will definitely not be able to cross the third security level, unless he has access to the original user's email-id. The user will be authenticated as an authentic user, and will be awarded access to the stored information, only after crossing the three security levels (Security level1-Text password, Security level2-Image Based password, and Security level3- One-Time Automated password).

V. Implementation of Imail Server with the Image Based Authentication

We created a new mail server, named IMail, as a proposed system to compromise the hazardous techniques of E-Mail Hacking and bugs of existing mail server. In IMail server, we planned to add the new enhanced technique to overcome the limitations of text based passwords. We came to the decision that we use Image based authentication to tight the security of Mail server. Now, it's active under http://www.isolmail.com URL.

In IMail server, we have implemented the image based authentication as a primary authentication for the user's account.

A. Create an account in IMail by selecting the Images

To use IMail, user should create an individual account. We implemented the Image based authentication from here itself. Before create an account, user instructed to follow some constraints. The constraints are listed below.

1. Here we give a set of Image grids. In Grid1, 100 images are given and also, In Grid 2, 100 images are given.
2. You should select two images from two grids. Images what you select from two grids are may be same or unique.
3. Keep the pictures; what you select in your mind is necessary.
4. User shouldn't select the both images from same grid itself.

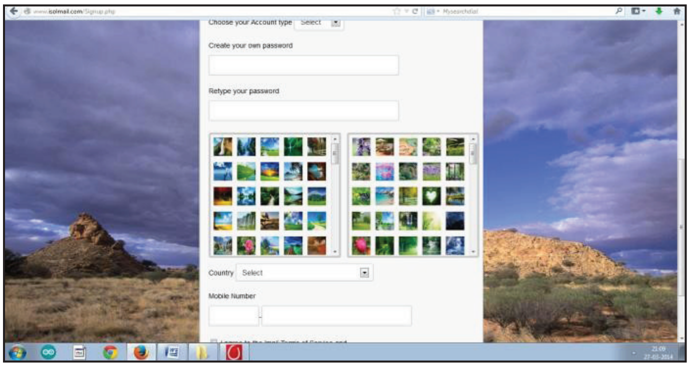


Fig. 2: Diagram of Select the Images from Two Grids at the Session of Create an Account.

5. Additions to set the text based password, selection of images are taking as a must one, to secure the account.

B. Signin to the IMail by using the Selected Images

In the case of existing mail servers, this is the process which the user wants to access their account, by entering the text based passwords what they have selected. But in Imail, user should click the correct images from two grids, what he has selected in the sign up process, addition to the text based password authentication.

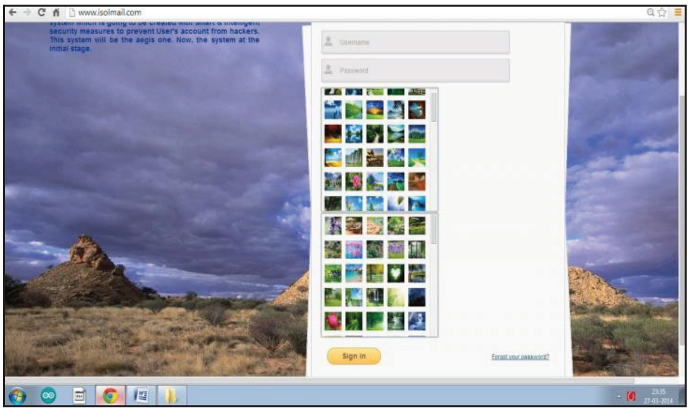
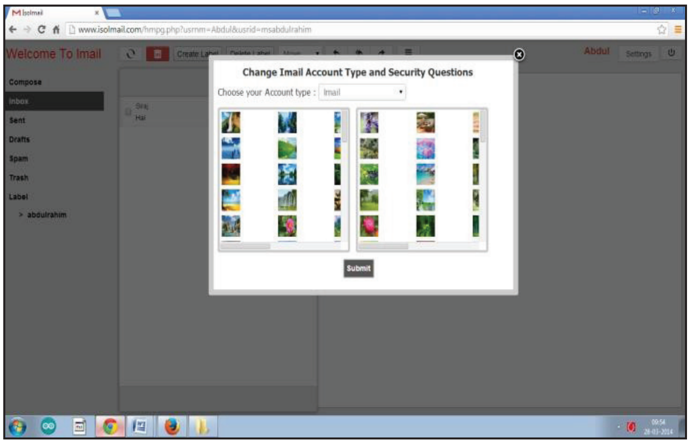

system which is going to be created with smart & intelligent security measures to prevent User's account from hackers. This system will be the aegis one. Now, the system at the initial stage.

Fig. 3: Diagram of Select the Images from Two Grids in the Signin Process.

C. Change the Image Sets Option to Ensure the Security

There is a fact that, user should change the passwords for every month. Like that, we set the option to change the image sets for every month to ensure the security of an account. To change the image set, user should login into his account and select the correct account type.



Choose your Account type : Imail

Fig. 5: Diagram of Change the Images from Two Grids when the User Wants

VI. Features of Image Based Over Text Based Authentication in Imail

Graphical passwords may offer better security than text based password because many people in attempt to memorize text based passwords, use plain words (rather than recommended jumble of characters). A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But in Imail, a set of selectable images from two grid are used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random. If there are 100 images on each of the 2 grids in a 100-image password, there are 100^2 or Ten thousand (10,000), possible combinations that could form the graphical password. If the system has the built-in delay of only 0.1 second following the selection of each image until the selection of the next grid, it would take millions of years to break into the system by hitting it with random image sequences. Therefore hacking by random combination is impossible. If the hacker tries to access victim's account, by selecting the images as wrong more than three times means, Imail server will alert the victim by SMS alert.

VII. Conclusion

This paper presents what are the techniques are involved in hacking and also performed by a hacker. Security attacks can come from both viruses and hacking programs [5]. It's not used by the hackers' only, also ethical hackers. E-mail communication is nowhere close to being safe on the Internet. Hence it is always a good idea to use secure e-mail systems like Pretty Good Privacy (PGP) and digital signatures. Such a strategy will prevent an attacker from being able to intercept an e-mail and read its contents [8]. Encrypted e-mail systems also make it all the harder for attackers to be able to perform forged e-mail attacks. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Mail Id and steal their personals. Most of the people think that, the programming skill is needed to hack. But, it's not needed to become a hacker. The terms "Hacking" and "Password" are dependent and inversely proportional. Such a strategy will prevent an attacker from being able to intercept an e-mail and read its contents. Encrypted e-mail systems also make it all the harder for attacker to be able to perform forged e-mail attacks.

Some mail servers are spending huge amount to secure their system. Beyond that, Black hat hackers hack the victim's account by using his/her technical knowledge. Now, we have started to create a new mail server, named IMail server to compromise the loopholes as a proposed system. In IMail server, we completed some of the compromising methods and still we are creating rest of the compromising methods. After finished all of the modules, it will be surely secured and effective mail server that surely fadeout the loopholes of existing mail servers and some dangerous techniques of Email hacking. Apart from the compromising methods, we stored the passwords as MD5 format, in the IMail database. Because of this option, even if the hacker hacked the IMail database, he can't access the user's passwords. In future, we have planned to store the passwords in the formats of SHA-1(Secure Hash Algorithm), RIPEMD-160 (RACE Integrity Primitives Message Digest algorithm-160) and implement PGP algorithms with Digital signatures [9].

I conclude that, by creating a new mail server (i.e.) IMail server with Intelligent security measures, we can totally block the given loopholes of existing mail servers and some lore techniques of Email hacking.

VIII. Acknowledgement

We would like to express our thanks to all the authors who submitted papers related to prevent hacking and also special thanks to all of my valuable professors who made us to involve in Network Security & Neural Networks by their encouragement.

References

[1] Komanduri, S., Mazurek, M.L., Shay, R, Kelley, P.G., "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms", Security and Privacy (SP), IEEE Symposium, 2012.

[2] Arunprakash, M., Gokul, T.R,"Network Security – Overcome Password Hacking Through Graphical Password Authentication", National Conference on Innovations in Emerging Technology 2011.

[3] Palmer, C.C.,"Ethical Hacking", IBM Systems Journal Vol. 40, Issue 3.

[4] Smith, B., Yurcik, W, Doss, D.,"Ethical Hacking: The security Justification Redux", Technology and Society, (ISTAS'02), International Symposium 2012.

[5] Surabhi Anand, Priya Jain, Nitin, Ravi Rastogi,"Security, Analysis and Implementation of 3-Level Security System using Image Based Authentication", 4th International Conference on Modeling and Simulation", 2012.

[6] Zuo, Y, Panda, B.,"Network viruses: Their working principles and marriages with hacking programs", Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, 2013.

[7] Putri Ratna, Anak Agung Dewi, Purnamasari, Prima, Shaugi, Ahmad, Salman, Muhammad,"Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system", QiR (Quality in Research) International Conference on 2013.

[8] Sai Sathish, Srinivasa Rao K., Aditya Gupta, Hacking Secrets, pp. 8-26, 2012.

[9] Ankit Fadia, Email Hacking: Even You can Hack, Vikas Publishers, pp.77-89, 2012.

[10] William Stallings,"Cryptography and Network Security", Pearson Prentice Hall, pp. 317-346, 2009.

M.Arunadevi received his B.C.A degree in from Nadar Saraswathi College of Arts and Science,Theni India in 2009, the M.C.A degree in Fatima College, Madurai in 2012 and M.Phil (Computer Application) in Madurai Kamaraj University in 2016. She is a Assistant Professor in Nadar Saraswathi College of Arts and Science,Theni. Her Research Interest include Network and Big Data.