Implementation of a New Secured Mail Server Application that Overcomes the Hazardous Loopholes of Existing Mail Server

[1]Arunadevi M, [2]Mohanapriya S
Assistant Professor, Assistant Professor
Department of Computer Science and Information Technology,
Nadar Saraswathi College of Arts and Science,
Theni, Tamilnadu India.

***Abstract* — Evolution of the Internet has introduced many features such as Assortment of Information, Communication, Transaction, Shopping, Social Networks, Chats, Advertisements, Online Education, Encyclopedia etc. The basic requirement for each user to manage E-mail is to have a separate ID known as Mail Identity. But most of the Mail ID's are not really safe and are easily accessible by Black hat Hacker. Email hacking is one of the most common attacks on the Internet. We analyzed some well secured mail servers regarding their security, based on some unchancy hacking techniques. From the analysis, we found some of the loopholes in existing mail servers, which are allowing the hackers, to hack the victim's account. In this project, we describe some dangerous techniques that are considered as loopholes in the existing mail servers, and also some vulnerability from existing mail servers. To fadeout the loopholes and vulnerabilities, we found some compromising methods. Finally, we have created a new Email server named as IMail, which adhere those compromising methods with some intelligent security measures.**

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

I. Introduction

Email 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. 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 is the process to allow users to confirm his or her identity to a Web application. The password is kept secret from those not allowed access. 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. A typical computer user may require passwords for many purposes: logging into Computer accounts, retrieving email from servers, accessing files, databases, networks, and websites and even reading the newspaper online. Possessive young lovers would do anything to be able to get a glance of their partner's email account contents. Thus the way, there are some loopholes in existing mail servers. It allows hackers to hack the victim' account with some hacker's technical knowledge. The success and speed of this technique largely depends upon the strength of the victim's password. Simply, I described the access level of passwords in mathematical form as,

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

Techniques Involved in Password Hacking

There are some unchancy methods to access the passwords. Some methods use intellect coding to break strong passwords and steal the victim's information. We analyzed all the techniques by Level of Execution and Threat Level. From the analysis, we selected some hazardous methods of E-mail hacking after filtered out the Low-level hazardous techniques.

- Password guessing
- Brute Force attack
- Forgot password attacks

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. 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.
- Victim's own name + Birthday/Phone number. For example abdulrahim3328.

The time to crack a password is related to bit strength, which is a measure of the password's information entropy. One example is brute-force cracking, in which a computer tries every possible key or password until it succeeds. More common methods of password cracking such as dictionary attacks, pattern checking, word list substitution, etc., attempt to reduce the number of trials required and will usually be attempted before brute force. Higher password bit strength increases exponentially the number of candidate passwords that must be checked, on average, to recover the password and reduces the likelihood that the password will be found in any cracking dictionary. A password that is easy to remember is generally also easy for an attacker to guess. Similarly, the more stringent requirements for password strength, e.g. "have a mix of uppercase and lowercase letters and digits" or "change it monthly", the greater the degree to which users will subvert the system. However, asking users to remember a password consisting of a "mix of uppercase and lowercase characters" is similar to asking them to remember a sequence of bits: hard to remember, and only a little bit harder to crack (e.g. only 128 times harder to crack for 7-letter passwords, less if the user simply capitalizes one of the letters). Asking users to use "both letters and digits" will often lead to easy-to-guess substitutions such as 'E' → '3' and 'I' → '1', substitutions which are well known to attackers. Similarly typing the password one keyboard row higher is a common trick known to attackers.

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,

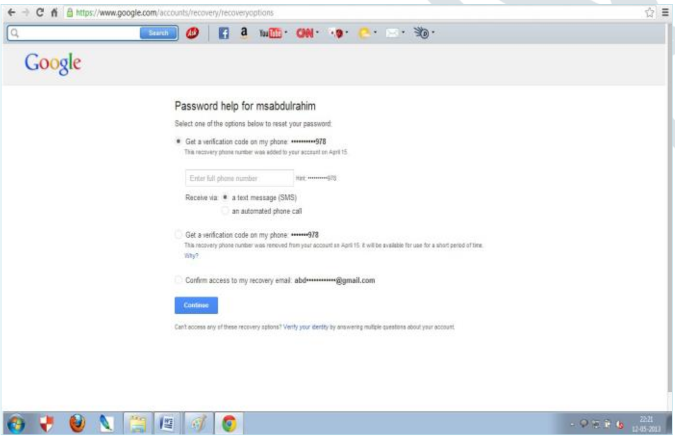
- Complexity of the password, and
- How well the attacker knows about the victim.

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.

C. Forget password attacks

The forget 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. 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. 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 forget 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.



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

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.

Text-based passwords remain the dominant authentication method in computer systems, despite significant advancement in attackers' capabilities to perform password cracking [1].

TABLE I. ANALYSIS OF HACKING TECHNIQUES

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.

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.	**

II. LOOPHOLES & VULNERABILITIES OF AN EXISTING MAIL SERVERS

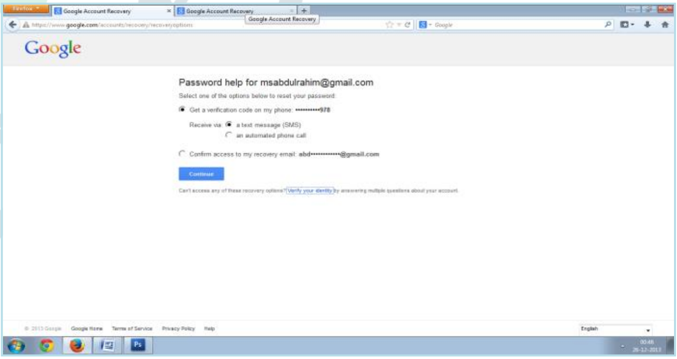
Here, we discussed with the problems of Existing mail servers that are considered as loopholes, based on above specified hacking techniques that permit the Hackers to crack the account. Beyond the loopholes, we defined the vulnerabilities too.

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.

B. Loopholes under Forgot password attack

- There is an option is there in Forget password attack is, "Verify your Identity". By clicking this option, Hacker can change the password, by answering some simple predefined questions. This option is available in all mail servers.



Password help for msabdulrahim@gmail.com

Select one of the options below to reset your password:

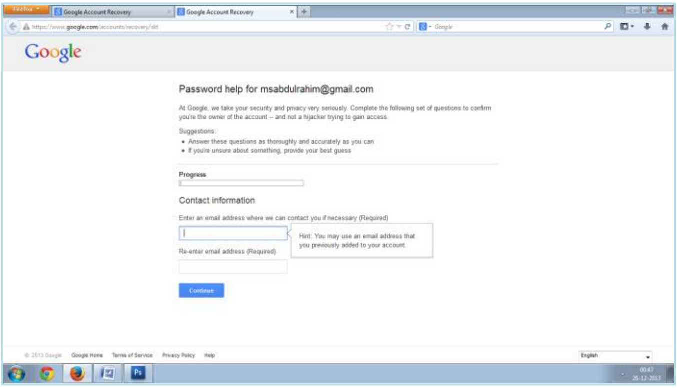
● Get a verification code on my phone: ••••••••••978

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

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

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

Fig.2. Diagram of Gmail's Verify your Identity option



Password help for msabdulrahim@gmail.com

At Google, we take your security and privacy very seriously. Complete the following set of questions to confirm you're the owner of the account – and not a hijacker trying to gain access.

Suggestions:

- Answer these questions as thoroughly and accurately as you can
- If you're unsure about something, provide your best guess

Progress

Contact information

Enter an email address where we can contact you if necessary (Required)

Hint: You may use an email address that you previously added to your account.

Re-enter email address (Required)

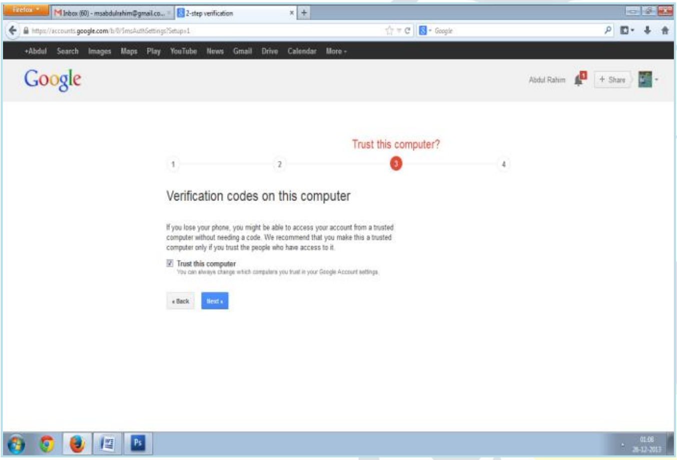
Fig.3. Diagram of answering Predefined questions for Verify your Identity option of Gmail.

- 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 ******." At the same time, 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.

C. Loopholes under Two-step verification

Gmail only provides a high security measure i.e. Two-step Verification. This measure also becomes a bug in the following ways.

- If user activates two-step verification method, he needs to enter Google verification code for every time. Because of this reason, even if a user activates 2step verification initially, he will deactivate later.
- If user assign a particular system (in which he works usually) as a specific trusted system, G-mail never apply Two-step verification method for that system.



Trust this computer?

Verification codes on this computer

If you lose your phone, you might be able to access your account from a trusted computer without needing a code. We recommend that you make this a trusted computer only if you trust the people who have access to it.

☑ Trust this computer
You can always change which computers you trust in your Google Account settings.

Fig.4. Diagram of Trusted system option in Gmail.

- If hacker wants to hack his friend's/relative's/colleague's id means, simply he can hack from Victim's trusted system even if the victim activated 2step verification method.

D. Remaining 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.
- Most of the mail servers provide the security questions relevant to our personal. By this option, hacker can hack victim's account and steal his/her information.
- Beyond the security measures of mail systems, if a hacker entered into that account, there are no options obtained to save the label which contains our bank transactions, personal chats & confidential in a label with proper security measures.

III. Implementation of New Mail Server with the Compromising Methods to the Loopholes & Vulnerabilities

We developed a new mail server, named IMail, as a proposed system to compromise the lore techniques of E-Mail Hacking and bugs of existing mail server. In IMail server, we added the above specified compromising measures to tight the security.

A. Compromise to the Brute-Force attack

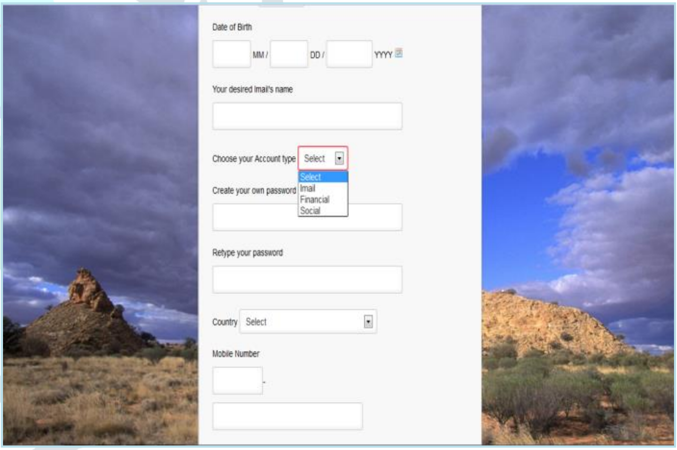
- To avoid Brute-force attack, IMail alerts the user / victim by SMS Alert if the hacker completed his third trial. The alert message will be "Hello user, someone is trying to access your account. Make change your password soon". Even the user type his password as wrong at thrice, he too will get the above SMS Alert. By this solution, we can totally avoid Brute-force password attack.

B. Compromise to the Forgot password attack & Two step verification

- If a hacker tries to hack a password by Forgot-password attacks, IMail sends the alert message, "Hello username, Someone is trying to change your Imail password via Forget password method. Please safe your account., to the victim's mobile phone. By this detailed alert message, Non-technical user also can know why these alert messages have come.
- By the above (A) and (B) solutions, the two-step verification method of Gmail will fade out. There is no use of two-step verification method when we use those options.

C. Compromise to the Vulnerabilities

- To avoid maintaining a same password for personal, financial and also for social networking websites, IMail server provides three options when the user creates a new account.



Date of Birth

Your desired Imail's name

Choose your Account type: Select

Create your own password

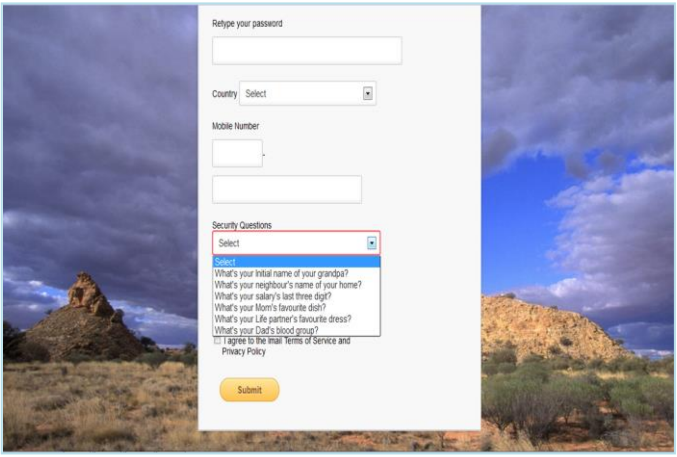
Retype your password

Country: Select

Mobile Number

Fig.5.Diagram of asking three different types of account in the Signup page of IMail Server.

- Most of the security questions in existing Mail servers are relevant to the user's personal. We planned to set Security questions that are irrelevant to the user. The questions are,
  a. What's your Initial name of your grandpa?
  b. What's your neighbour's name of your home?
  c. What are your salary's last three digits?
  d. What's your Mom's favourite dish?
  e. What's your Life partner's favourite dress?
  f. What's your Dad's blood group?



Retype your password

Country Select

Mobile Number

Security Questions

Select

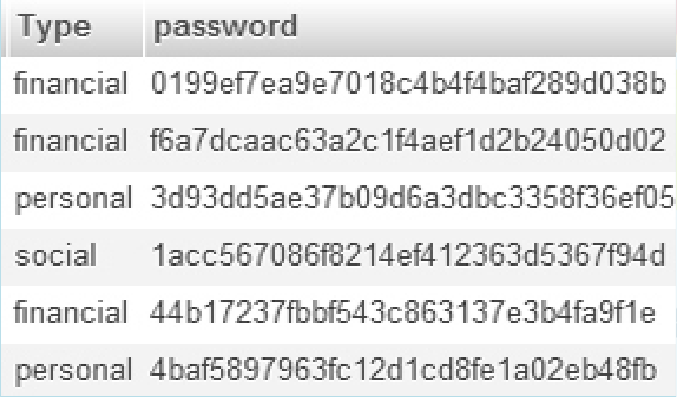
Select
What's your Initial name of your grandpa?
What's your neighbour's name of your home?
What's your salary's last three digit?
What's your Mom's favourite dish?
What's your Life partner's favourite dress?
What's your Dad's blood group?

□ I agree to the Imail Terms of Service and Privacy Policy

Submit

Fig.6. Diagram of asking Security questions as irrelevant to the user in IMail's Signup Page.

- Store the passwords of IMail users in the database as MD5 Format [6]. By this feature, hacker can't decrypt the passwords. MD5 algorithm takes as input a message of length 512-bit blocks which are further divided into 16, 32-bit sub blocks. The output of the algorithm is a set of four, 32-bit blocks i.e., 128-bit message digest.
- MD5 has so much of complexity and randomness. So that no two message digests produced by MD5 on any two different messages are equal. MD5 has a property that every bit of the message digest is some function of every bit in the input [6, 9].
- The possibility that two messages produce the same message digest using MD5 is in the order of 2^{64} operations.



Type	password
financial	0199ef7ea9e7018c4b4f4baf289d038b
financial	f6a7dcaac63a2c1f4aef1d2b24050d02
personal	3d93dd5ae37b09d6a3dbc3358f36ef05
social	1acc567086f8214ef412363d5367f94d
financial	44b17237fbbf543c863137e3b4fa9f1e
personal	4baf5897963fc12d1cd8fe1a02eb48fb

Fig.7. Diagram of store the Account type & Passwords as MD-5 format in IMail database

- IMail provides the option to user that he/she can set the password option to the Label, which the user wants to be more confidential. The benefit of this option is, even if a hacker has hacked the victim's account he can't steal the victim's confidential information.

IV. Architecture Design of IMail Server

There are two architecture designs are drawn below. One is Architecture design of IMail validation and another one is Architecture design of Retrieve the password when the user lost his password.

A. Architecture design of IMail validation & verification

The Architecture design of the IMail server validation defined the Authentication process of IMail server. After victim enters his username and password, the IMail server verifies the given details with the database of IMail server. The passwords are stored in the database as MD-5 format. If the given username and password is matched means, he can enter into his account and get his privileges of IMail server.

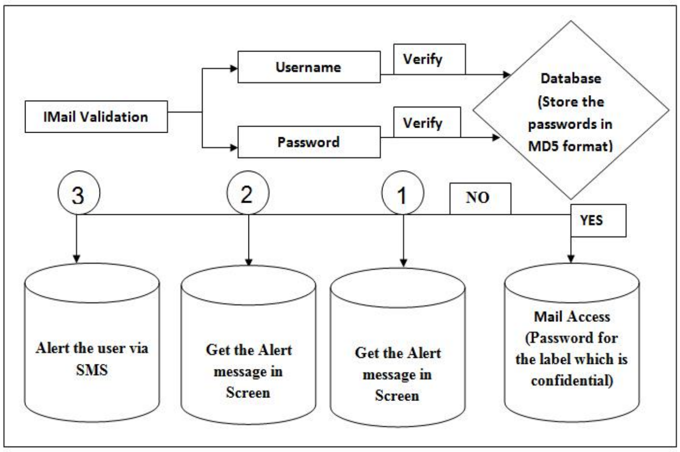

IMail Validation
Username
Password
Verify
Verify
Database (Store the passwords in MD5 format)
NO
YES
3
2
1
Alert the user via SMS
Get the Alert message in Screen
Get the Alert message in Screen
Mail Access (Password for the label which is confidential)

Fig.8. Architecture diagram of IMail validation & verification

At first and second time of false authentication, he gets the alert message in the screen. At the third time of false authentication, he gets the alert via SMS to the registered mobile number. After he entered into his account, he can lock the label, which he wants to be more confidential.

B. Architecture design o f Forget Password Method

The Architecture design of Forget password method is slightly designed from the other mail servers with new intelligent security measures. When the user are requested the IMail user to retrieve his hacked/forgot password, he needs to click the 'Forget your Password' in the Homepage of the IMail server. After he clicked, IMail server asks to enter his corresponding IMail id, which he lost. After he entered his Mail id, IMail server will confirm whether the entered ID is of him or not, by asking to the enter type of account. This option is already given in the Signup form, when the user creates a new account. If the entered account option is right, it will ask the next option, which asks to enter the answer for security question.

IMail server will confirm, whether the entered answer of the corresponding security question is right or not. This option too is already given in the Signup form, when the user creates a new account. If the given answer is right, he can reset the new password with confirm password. Else, IMail server will alert the user via SMS or Automated call option.

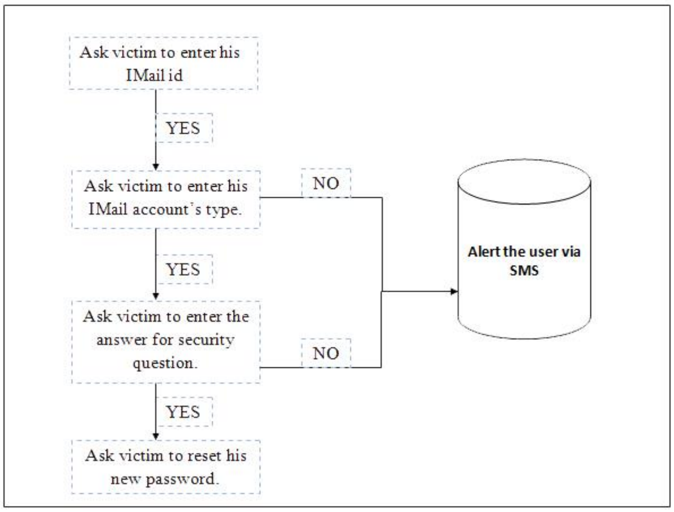

Ask victim to enter his IMail id
YES
Ask victim to enter his IMail account's type.
NO
YES
Ask victim to enter the answer for security question.
NO
YES
Ask victim to reset his new password.
Alert the user via SMS

Fig.9. Architecture diagram of Forget password Method

V. Implementation of Proposed System

To create IMail server, I used the two types of requirements that are Hardware and Software. Hardware requirements are used to establish and host the IMail server and also to connect IMail server with the SMS server. After getting the Domain Name from the private host, I hosted the IMail server, from the advanced processor that is Intel Xeon Quad Core, 2.5GHz processor. Due to this processor's speed, user can use the IMail server with the guaranteed QOS. This will decrease the delay and improve the server's performance. And also I can store and maintain the database of the IMail's users / victims, up to the 4GB memory level. If the number of users exceeds than 4GB, I'll add the additional space later. The software requirements of an IMail server used to design and develop the webpages of an IMail server and also used to configure the server with the database.

To establish the IMail server, I divided the tasks into three levels such as Design Develop, and Configure

A. Design

In the designing task of IMail server, I designed the overall layout of IMail webpages by using the web programming languages like HTML and Ajax. Here, I defined that how I'm created the webpages. I designed the background designs, foreground designs and other formatted sizes, alignments of forms; buttons are coded by using Cascading style sheets (CSS). Here, I set the margin, border, background, default font size and other attributes for an IMail server and also I designed the layout for Sign Up and Sign In pages, by using CSS only. I saved the file as 'theme.css', and I annexed the 'theme.css' file, in the Main pages, when I needed.

B. Develop

In the developing task of IMail server, I enhanced the programming level for an IMail server, by providing the Authentication, Level of Authentication, Get the multiple types of input from a user and providing an error messages for wrong inputs. And also, I connect the server with the database by providing the code is, *include ('dbconnect.php');* By this code, we can fetch the data from the database. In *dbconnect.php* file, I have given the local host, username as local host and root. The password option is optional.

The corresponding coding is,

```
<? php
 $link = mysql_connect ("localhost","root","");
if (!$link)
    {
   die (‘could not connect: ' . mysql_error());
    }
  //else echo 'Connected successfully';
if (!mysql_select_db('imail', $link))
   {
   echo 'Could not select database';
      exit;
   }
?>
```

If the database is not connected, it shows the error message as 'could not connect'. After I connected with the database, I selected the corresponding table from the database. The table name given here is 'imail'. The entered username and password by the victim are validating by checking the details with the stored values of the database. MySQL query is used to create, connect, modify and truncate the database. To check and validate the authentication process, the following coding is used.

```
$name = mysql_real_escape_string ($_POST ['username']);
$pwd = mysql_real_escape_string ($_POST ['password']);
$sql=“SELECT * FROM imail_users WHERE
     imail_username='“. $name. "'" AND
     imail_password='“. $pwd. "'";
```

After validated, the results are stored in the variable $result1, and fetch the result from the corresponding row of $result1.

```
$result1 = mysql_query ($sql, $link) or die ('Error updating
     database: ‘. mysql_error ());
$row = mysql_fetch_row ($result1);
```

If the result is not null, the validation process for the given inputs of the victim have started. If it's not matched with the database values, the session will destroy and the current page is repeated. If it's matched means, it will switch to the main page of the user, by using the '*header'.*

```
     if (!$row)
      {
      $msg='<span
       style="color:#fd1000;float:left;margin:0px 0px 5px
30px;">Username and Password is incorrect</span>';
     session_destroy ();
     unset ($_SESSION ["username"])
     header ("location: index.php");
       }
    else
      {
        $_SESSION ['username'] = $row [1];
        //echo $_SESSION ['username'];
        header ("location: hmpg.php? usrnm=".
$_SESSION ['username']);
      }
```

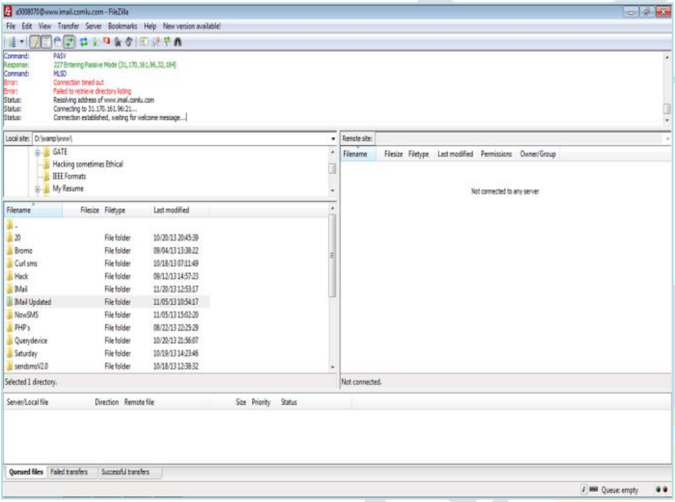
If the false authentication process exceeds thrice, the IMail server will send the alert to the victim through his/her registered mobile number. The mobile number is already stored in the database with the values First name, Last name, User name, Password, Gender, Account type, Password and Answer for the security question are stored. So, if the victim / hacker entered the wrong password at thrice, it will automatically fetch to the database, pick the mobile number from the database and send the alert message to the corresponding mobile number of that Mail id.

```
     $sql = "SELECT mobileno FROM imail_users
WHERE imail_username='".$name."'";
     $result = mysql_query ($sql, $link) or die ('Error
updating database: ' . mysql_error());
    $row = mysql_fetch_row ($result);
     $mobile = $row [0];
    $message="Hello ". $name.” someone is trying to
access your imail account. Make change your password soon
as irrelevant to you";
```

The message which the IMail server sends to the victim's mobile number, is manually assigned in the variable $message. In that variable, $name indicates the username is already assigned and fetched from the database. The message received to the victim's mobile number is “Hello Rahim, someone is trying to access your email account. Make change your password soon as irrelevant to you. I got some access to send sms from the private gateway. Through that gateway, IMail server will send the message. To access the gateway, I have to give the gateway id and the parameters. But both are confidential. But the syntax is used to access the gateway is '*fopen'*. To send the sms through the gateway, the code '*fpassthru'* is used, and '*fclose'* is used to close the gateway.

C. Configure

To configure the IMail server, I got the Domain Name from the private gateway, under the Commercial of Generic domain name (.com) is "isolmail.com". And also, I have got the userid and password, to manage the gateway. By having that userid and password, I can upload and also modify the uploaded data of IMail server, in that gateway. The IMail server has been designed under MVC Framework. Model View Controller has been widely adopted as architecture for World Wide Web applications in all major programming languages. Several commercial and non-commercial application frameworks have been created that enforce the pattern. These frameworks vary in their interpretations, mainly in the way that the MVC responsibilities are divided between the client and server In this approach, the client sends either hyperlink requests or form input to the controller and then receives a complete and updated web page (or other document) from the view; the model exists entirely on the server. As client technologies have matured, frameworks such as JavaScriptMVC and Backbone have been created that allow the MVC components to execute partly on the client.



a5008070@www.imail.comlu.com - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!

```
Command:   PASV
Response:  227 Entering Passive Mode (31,170,161,96,32,184)
Command:   MLSD
Error:     Connection timed out
Error:     Failed to retrieve directory listing
Status:    Resolving address of www.imail.comlu.com
Status:    Connecting to 31.170.161.96:21...
Status:    Connection established, waiting for welcome message...
```

Local site: D:\wamp\www\

GATE
Hacking sometimes Ethical
IEEE Formats
My Resume

Filename	Filesize	Filetype	Last modified
..			
20		File folder	10/20/13 20:45:39
Bromo		File folder	09/04/13 13:38:22
Curl sms		File folder	10/18/13 07:11:49
Hack		File folder	09/12/13 14:57:23
IMail		File folder	11/20/13 12:53:17
IMail Updated		File folder	11/05/13 10:54:17
NowSMS		File folder	11/05/13 15:02:20
PHP's		File folder	08/22/13 22:25:29
Querydevice		File folder	10/20/13 21:56:07
Saturday		File folder	10/19/13 14:23:46
sendsmsV2.0		File folder	10/18/13 12:38:32

Selected 1 directory.

Remote site:

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group

Not connected to any server

Not connected.

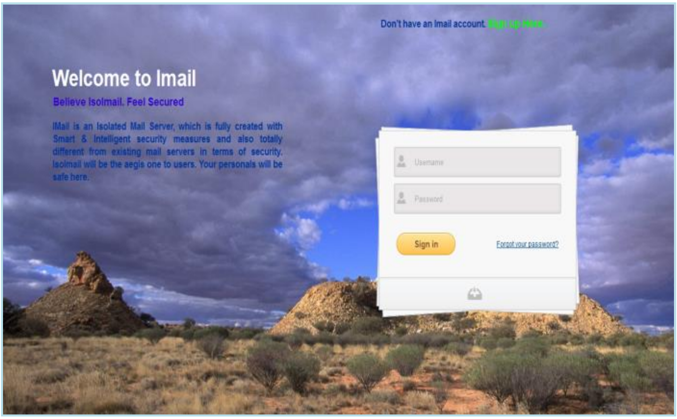
Server/Local file	Direction	Remote file	Size	Priority	Status

Fig 10: Upload IMail server files in Filezilla.

To upload and modify the data, I use the Filezilla as an interface. Filezilla is free and cross-platform FTP software, consisting of Filezilla client and Filezilla server. Telecom Regulatory Authority of India (TRAI) limits the number of messages for a person is 100 msgs/day. It doesn't affect the victims of IMail server, because the corresponding gateway of IMail server, already have got the specialized permission for unlimited Short Message Service.

VI. Results and Discussions

The results of this project are given many solutions to the above specified loopholes. Here, I start the discussions about IMail from the overall design layout of an IMail server. The design of the IMail server has been designed as a user-attractive one with the cool backgrounds.



Don't have an Imail account. Sign Up Here.

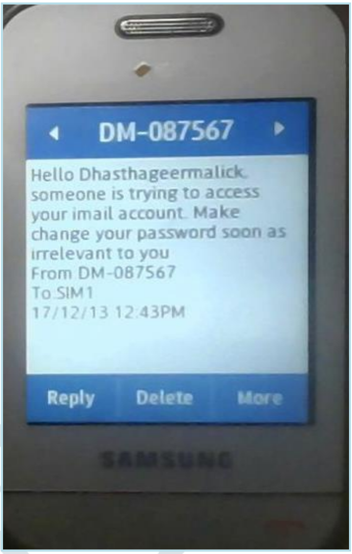
Welcome to Imail

Believe Isolmail. Feel Secured

IMail is an Isolated Mail Server, which is fully created with Smart & Intelligent security measures and also totally different from existing mail servers in terms of security. Isolmail will be the aegis one to users. Your personals will be safe here.

Fig 11: Homepage of an IMail server

In the homepage of IMail server, I have given the links to create an account and the main page to get the privileges of the users. If the hacker try to get the victim's password by infinite trials means (Brute force attack), IMail server will alert the victim to the victim through his registered mobile number from the IMail database. Existing mail servers doesn't have this option.

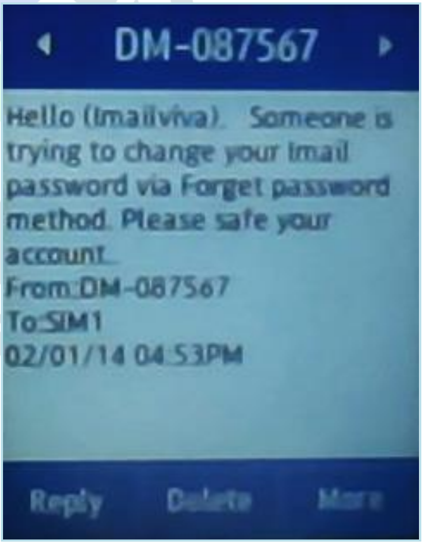


DM-087567

Hello Dhasthageermalick. someone is trying to access your imail account. Make change your password soon as irrelevant to you
From DM-087567
To SIM1
17/12/13 12:43PM

Fig 12: Alert message to prevent Brute-force Attack

And also, I give the link is 'Forget your password', to retrieve the user's password when he forget his password or someone stolen his password. This technique used in IMail server is totally different from other's mail server, and also implemented with the intelligent security measures.

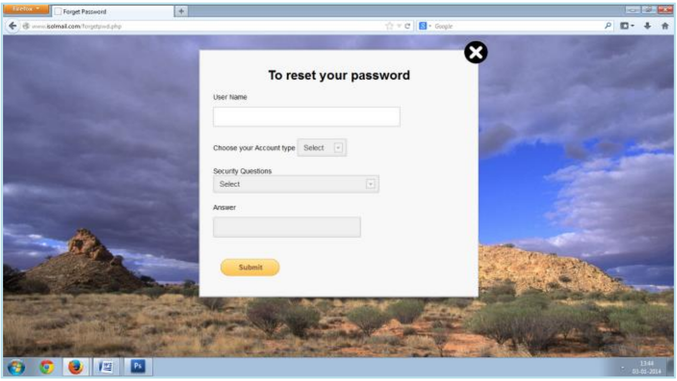


DM-087567

Hello (Imailviva). Someone is trying to change your Imail password via Forget password method. Please safe your account.
From DM-087567
To SIM1
02/01/14 04:53PM

Fig 13: Alert message to fade out the Forget password Attack

The basic criterion of the retrieve password is One-time password technique. But to retrieve the password, user should know and give the right answer for his type of account and the answer for his secondary questions.



To reset your password

User Name

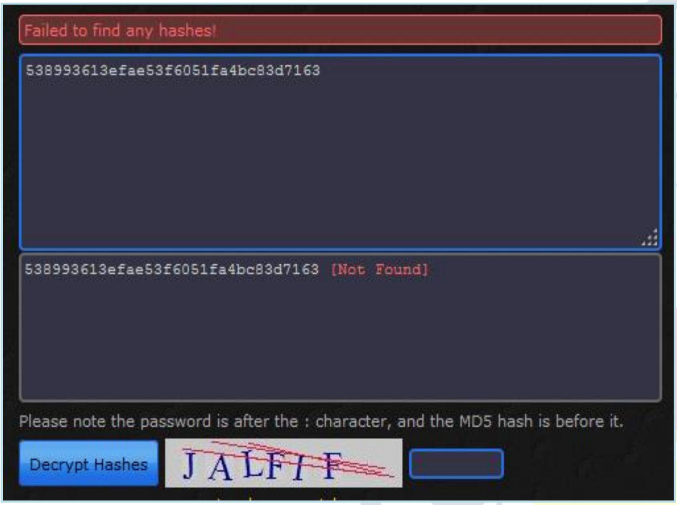
Choose your Account type: Select

Security Questions: Select

Answer

Fig 14: Forget password option in IMail with proposed security measure

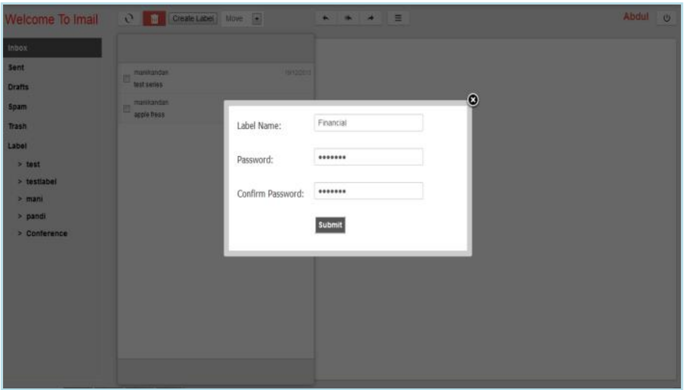
Behind the screen, the passwords of victim's are stored as MD-5 format in the IMail's database. The code is used to convert the text based passwords in MD5 form is, *$pass = md5 ($password)*. I checked the 99% of the passwords are not decrypted, in the topmost sites of MD-5 decryption.



```
Failed to find any hashes!

538993613efae53f6051fa4bc83d7163

538993613efae53f6051fa4bc83d7163 [Not Found]

Please note the password is after the : character, and the MD5 hash is before it.
```

Fig 15: MD5 passwords are not decrypted in the topmost sites.

In the signup page, I have added two security measures are, Types of account and asking security questions which are indirect to the user. By providing the types of account option, user can avoid the use of same ID to all purposes such as Transactions, Personals and Social Networking websites. By providing security questions, Hacker can't ask these questions directly to the victim; in the case of Hacker is the friend/relative to the victim. Next to the Sign-up page, In the Sign-in page, user can get the privileges of his account such as managing the mail. In the main page, user can lock the label by a separate key, which the user wants to be more confidential. After the user gets authenticated, he can access the rights to enter into his account and manage the mail transactions.



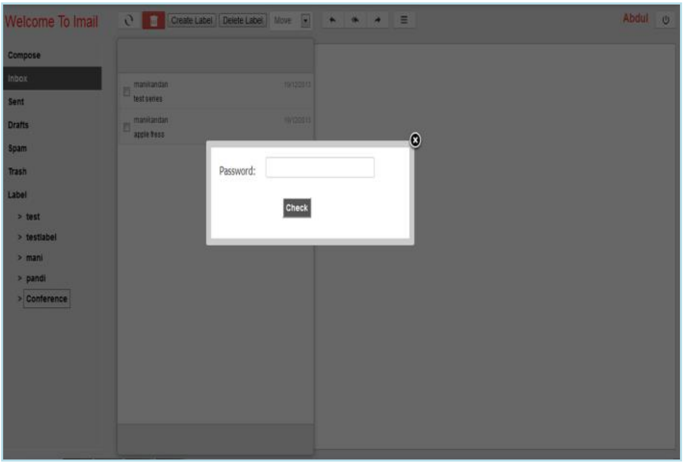
Label Name: Financial

Password: •••••••

Confirm Password: •••••••

the password for the corresponding label and access it.

Fig 16: Diagram of set the password to the Label in IMail.



Password:

Fig 17: Diagram of asking the password to access the label.

VII. Conclusion

This project 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. It's not used by the hackers' only, also ethical hackers. As with most technological advances, there is also a dark side: criminal hackers. 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 Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. 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. 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.

So, I created a new mail server, named IMail server to compromise the loopholes as a proposed system. In IMail server, I completed the specified compromising methods. Now, 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. 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.

In Phase-II, I have planned to tight the security bound on Mail transferring by implementing Cryptographic algorithms and techniques like Pretty Good Privacy. PGP is one such cryptography system that uses the public-private key pair to encrypt and decrypt data securely. It's not only used to encrypt local files on your system but can also be used to securely transfer encrypted e-mails over the Internet. The PGP cryptography system is not only very safe, but is also very easy to implement and use. The working of the PGP system can be explained in the following manner.

- In the encryption, PGP compresses the plaintext data that has to be encrypted using a predefined compression algorithm. PGP compresses the plaintext data not only to save bandwidth and hard disk space, but also to make it more difficult for an attacker to crack the encryption algorithm.
- PGP creates a random single-use encryption key known as the session key. This is normally randomly generated using totally random data (like mouse movements, prime number multiplication, RAM contents etc.) and is used to encrypt the plain text data into ciphertext data. Normally a very fast and strong encryption algorithm is used with the session key to encrypt the plaintext data.
- Finally, the session key generated in step (ii) is generated using the recipient's public key. Once this is done, PGP then sends this encrypted session key and the cipher text data to the recipient.
- In decryption, PGP at the receiver's end uses the private key of the recipient to retrieve the encrypted session key. It is important to note here that the receiver is asked to enter the passphrase to decrypt and use the private key.
- This retrieved session key is then used to decrypt the encrypted cipher text data sent by the source.
- Finally, this retrieved compressed plaintext data is uncompressed and the original plaintext data is obtained.

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 Ethical Hacking by their encouragement.

REFERENCES

[1] Komanduri, S., Mazurek, M.L., Shay, R and 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] Palmer, C.C., "Ethical Hacking," IBM Systems Journal Vol.40 , Issue.3

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

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

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

[6] Putri Ratna., Anak Agung Dewi., Purnamasari., Prima., Shaugi., Ahmad., Salman and 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

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

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

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

[10] Steve Suehring, Tim Converse, Joyce Park, *PHP and MySQL*, Wiley India Publications, 2012, pp. 1-712.

[11] Ryan Russell, *Hack Proofing: Your Network*, Syngress Publications, 2008, pp. 11-37

[12] Seema Khanna., Harish Chaudhry., "Anatomy of compromising E-mail accounts", IEEE International Conference on Information and Automation Shenyang, 2012.

Mohammed Serrhini., Abdelmajid Dargham., Abdel Aziz Ait-Moussa., "Improve Security of Web Browser with Stand-Alone-E Learning Awareness Application", 2012.