ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 3, Issue 12, December 2016

Advance Security System Using Encrypted Password

[1] Prof. Jyoti Khurpade [2] Paras Patil [3] Aditya Kharde [4] Digvijay Desai [5] Ashutosh Kamat
[1][2][3][4][5] Computer Engineering,
MAEER'S MIT Polytechnic, Pune

***Abstract:*-- With increasing demand of security. Now a day's it is very critical issue, there for user authentication is one of the important topics in information security to protect user's privacy. So we have to develop an application for the peoples who want to secure their system from unauthenticated users. If somebody have hacked or find password of our computer by any mean and trying to access our system, then this application will not allow him to do that. When any unauthenticated user will enter password and clicks on login button the application will change password of system and restart the system. Before restarting the system application will capture snap of user and send it on the email id of administrator with new password. Actually we will provide a dummy login screen to the users after he enters in operating system. If admin wants to login in system he have to use keystrokes for actual login screen. If admin enter login credentials in this screen application will allow him to access the system. Admin can change the keystrokes of dummy login screen any time.**

***Keywords:*— Authentication, Security, Capture Snap, Password, Login Screen, Keystrokes.**

I. INTRODUCTION

Password is the most common method for users to authenticate themselves when entering computer systems or websites. It acts as the first line of defense against unauthorized access, and it is therefore critical to maintain the effectiveness of this line of defense by rigorously practicing a good password management policy.

With the ever-increasing use of information technology in our daily lives, there are also an ever-increasing number of user accounts and passwords we have to remember and manage. The choice of passwords used for different information systems presents a dilemma. On one hand, an intruder could gain access to ALL the systems if the same password used for accessing these systems is compromised. On the other hand, when different passwords are used for different systems, users may have the tendency to choose easy-to-remember or weak passwords, or even write them down, which would again jeopardize the security of the systems concerned. There is also a higher chance of users forgetting their passwords, increasing the associated user support and operation overheads for password resets.

II. THE SECURITY THREATS TO PASSWORDS

A password is a convenient and easy method of authentication for users entering a computer system. The system simply requires the user to present something he knows as a proof that he is actually who he claims to be. This is easily implemented, but at the same time the password approach is subject to a number of security threats. The following are common security risks where a legitimate user may lose his or her password: 1. Over the shoulder attack: when a person types in his or her password, someone might be able to observe what is typed and hence steal the password by looking over the person's shoulder, or by indirect monitoring using a camera. 2. Brute-force attack: because a password has a finite length, usually 8 alphanumeric characters, an attacker can use programs that automatically Password Management Page 4 of 18 generates passwords, trying all possible combinations until a valid password is found. With recent advances in computing power, the time needed to execute a successful brute force attack has dropped considerably. 3. Sniffing attack: when a password is sent over a network, it could be captured by network sniffing tools if the network channel is not properly encrypted. In addition, certain malicious tools (such as a key logger) might be able to capture a user's password when the password is typed in during the authentication process. 4. Login spoofing attack: this is where an attacker sets up a fake login screen that is similar in look-and-feel to the real login screen. When a user logins to the fake screen, his password will be recorded or transmitted to the attacker. All these attacks, if successful, can help unauthorized users harvest the passwords of legitimate users. Systems using passwords as the only authentication method will be unable to differentiate whether the holder of the password is a valid user or not.

To avoid above problems we have proposed a secured scheme in which, if attacker hacked or find password of our computer by any mean and trying to access our system, then this application will make his effort useless and the access will be denied.

III. LITERATURE SURVEY

In 1961 First computer password was developed by MIT's CTSS (Compatible Time-Sharing System), when computer time was scarce, extremely expensive and limited to research institutions. CTSS employed the first password and username method of user authentication - and may have been the first system to experience a password breach. In 1966, a software bug jumbled up the system's welcome message and its master password file, so that anyone who logged in was presented with the entire list of CTSS passwords.

In 1995 "Hackers" the cult classic introduces the mainstream to Phreaking, computer viruses, and general hacking culture, just as the consumer web starts heating up - and data encryption becomes ever-more relevant.

In 1997 AES was developed .The National Institute of Standards and Technology developed AES (Advanced Encryption Standard), which is still used today. 128-bit encryption takes 2 to the 55th power (or 2*55 years) to crack. A device that could check a billion (1018) AES keys per second (if such a device could ever be made) would in theory require about 3x10*51 to exhaust the 256-bit key space. (That's 74,449,211,009,120,120,166,087,753,728 years.)

In 1997 CAPTCHA as online spam grew, AltaVista chief scientist Andrei Broder and his colleagues developed a filter that generates an image of random text that machine vision systems cannot read, though humans can. In 2009, Luis van Ahn at Carnegie Mellon updated the concept with extra layers of security that measured up to more evolved spam and hacking practices. With ReCAPTCHA, words became even harder for machines to read, thanks to increase waviness and features like lines running through the text.

In 2006 hacking and identity theft became big business as more and more people join the Internet, adding increasingly large amount of personal data to the web. One of the largest data thefts in recent times took place on networks belonging to the T.J. Maxx and Marshall's department stores: as many as 45 million credit and debit card numbers were stolen between 2005 and 2007, highlighting how hackers can breach decrypted data networks.

In 2011 Advanced Persistent Threats (APTs) emerged: well-funded, coordinated groups of hackers pursuing specific agendas. 70 million Sony PlayStation users were hacked; so were 200,00 Citibank customers. Facebook revealed that 600,000 of its accounts were being compromised each day. And 2012 promises to be more of the same. This January, Zappos was hacked in a big way: 24 million customers' names, e-mails, phone numbers, addresses, and partial credit card numbers were exposed.

In 2012 Personal data lockers have emerged as a way to make the most of the Internet while remaining safe. By centralizing storage of personal data -- from payment information and passwords to ID numbers and receipts – in one locally-encrypted place that only the user can access, the data is as secure as possible, while remaining conveniently under his or her control. No one else can decrypt the data -- not even purveyors of the technology or the government can get to it. In a sense, personal data can now go wherever a user wants it to go.

In our project, we are making the system hack proof by providing more security. The login screen prevents the system from access by unauthorized user. But some professional attacker can login the system successfully by implementing some attacking techniques like shoulder surfing. One way to avoid this attack is by using encryption technique. By encrypting the password, it becomes unreadable and more complex. In this way we can make the job of attacker more difficult.

IV. PROPOSED PROJECT

For our project we are using JAVA platform, because Java is more beneficial to our project. Java provides many features those are required for implementation of our project.

A. In this project there are three different modules

1. First comes, the registration screen. In which the user has to enter his/her username, password, hotkeys and email. After registration, password will be sent to the user's mail.
2. Next comes, the fake screen. This screen looks similar to the login screen of Windows OS. The hot key

provided by the user is required to escape from fake screen.

3. After fake screen comes the original login screen in which the user has to enter his/her credentials i.e. username and password to access the system.

In this login process, the fake screen plays the important role in security. For legitimate user it functions as provided above. But for the attacker who wants to penetrate through the user's system, he/she must face this screen.

B. The security provided for fake screen

1. As the fake screen requires the hot keys which are unknown to attacker, the attacker will enter the normal credentials which he/she knows. But the system will display message "incorrect username or password".
2. The system will give him/her three chances to try. But if attacker fails to escape the screen, then the system will take snapshot of attacker, change the password, encrypt it and then mail it to legitimate user. The system will reboot later.
3. The encryption technique provided here is "bcrypt algorithm". The bcrypt function is the default password hash algorithm for BSD and other systems including some Linux distributions such as SUSE Linux.[2]

For encryption we are using bcrypt algorithm. The bcrypt function is the default password hash algorithm for BSD and other systems including some Linux distributions such as SUSE Linux.[2] The prefix "$2a$" or "$2b$" (or "$2y$") in a hash string in a shadow password file indicates that hash string is a bcrypt hash in modular crypt format.[3] The rest of the hash string includes the cost parameter, a 128-bit salt (base-64 encoded as 22 characters), and 184 bits of the resulting hash value (base-64 encoded as 31 characters).[4] The cost parameter specifies a key expansion iteration count as a power of two, which is an input to the crypt algorithm.

The prefix "$2a$" or "$2b$" (or "$2y$") in a hash string in a shadow password file indicates that hash string is a bcrypt hash in modular crypt format.[3] The rest of the hash string includes the cost parameter, a 128-bit salt (base-64 encoded as 22 characters), and 184 bits of the resulting hash value (base-64 encoded as 31 characters).[4] The cost parameter specifies a key expansion iteration count as a power of two, which is an input to the crypt algorithm.

In this way we are providing the security to the operating system.

C. Hardware Description

1. Webcam with installed drivers.
2. Internet connection.
3. Windows OS (above Windows XP)

D. Features

1. Provides more security for Windows OS.
2. Easier to track attacker by taking his/her snapshot through mail.
3. If the mail is hacked then also the attacker will not be able to guess the password because it is in the encrypted form.
4. It is the best software to prevent our system from hacking.

REFERENCES

1. /https://www.npmjs.com/package/bcrypt Algorithms and other resources.

2.http://www.java2s.com/Code/Java/Security/GeneratearandomStringsuitableforuseasatemporarypassword.htm-automatic -Generation of random password.

3. http://www.bmscentral.com/learn-employee-scheduling/setting-up-snap-schedule-to-e-mail-schedules/ - Sending mail.