ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

Intelligent and Robust Authentication Management Framework to Resist Password Attacks

B.Sunil Kumar, P.Jayasankar, T.P Sarachandrika, D. Kiran Kumar

Abstract: ***Majority of internet based applications were using the most popular password based authentication mechanism to allow the valid users to access the confidential data. Password based authentication became insecure because of various types of attacks like phishing, eavesdrop and dictionary attacks were introduced by adversaries to compromise the system. Automated Turing Tests (ATTs) were designed to resist the online dictionary attacks earlier, but they become too hard to identify by legitimate human-users, because to secure them from attacks.In this paper we introduced the Intelligent and Robust Authentication Management Framework to resist password attacks. This Intelligence of this work identifies the legitimate user to allow them to login without the ATT test by increasing the limit of failed login attempts to them and robustness of this framework forces more complex ATTs to improve the hardness of cracking passwords. To identify the legitimate users of an account this framework internally uses the valid user IP addresses and HTTP cookies stored at client machine. Experiment results shows that this framework is scalable for reducing the burden on legitimate users without compromising the security levels.***

Keywords: **Security, password authentication, online dictionary attacks, ATTs.**

I. INTRODUCTION

Passwords based authentication is most common mechanism for online or offline applications. Although various authentication techniques like bio-metrics, face recognitions and PKI based authentications [2] were introduced, majority of applications are still depending on password based authentication because of they are user friendly and easy to maintain. Passwords become most popular technology for authenticating the users trying to access confidential data stored in computers. Majority of online application like Social Networks, Bank Applications, Shopping cart apps and Online secure Transactions completely relied on password based authentication.

It is a well-known issue that protecting the password authenticating system from adversaries becomes more complex today, due the updated attacking techniques like dictionary attacks, eaves dropping, phishing mails and man-in-the-middle attack etc. Although there are many attacking models to compromise systems, the most prominent ones are online dictionary attacks and eaves dropping techniques. Eavesdropping attacks can be prevented by encrypting the communication between the user and the server, for example using SSL implementation [4, 5]. Resisting the online dictionary attacks became harder against the password based authentication mechanism due to their complexity.Successful dictionary attacks have, e.g., been recently reported against WordPress user accounts, where attackers broke into accounts of customers with default admin user account [8].

In order to prevent from online dictionary attacks, recent research techniques were introduced Automated Turing Test's (ATT) stands for CAPTCHA. After the limited number of login attempts systemwill generate the image CAPTCHA and forces the users to enter the valid value for ATT. Breaking the ATT with correct username and password become more complex to adversaries earlier. Due to successful automatic attacks on ATT's to break, they were become more difficult for bots being deployed[3]. As a consequence of the leading race between adversaries and ATT creators CAPTCHAs become more difficult even for human-users also. Complex ATT[5]s Implementation will improve the security against dictionary attacks but unnecessarily legitimate users also suffering from the hardness of ATT while they are trying to login after limited failed attempts.

In this paper we introduced the Intelligent and Robust Authentication Management Framework to resist password attacks. This Intelligence of this work identifies the legitimate user toallow them to login without the ATT test [9] by increasing the limit of failed login attempts to them and robustness of this framework forces more complex ATTs to improve the hardness of cracking passwords. To identify the legitimate users of an account this framework internally uses the valid user IP addresses and HTTP cookies stored at client machine. This framework mainly reduces the legitimate users burden while false attempts without compromising the security. This framework mainly concerned on internet based CUI & GUI applications.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

II. RELATED WORK

There have been several previous attempts to measure password security by analyzing real life passwords. To make them secure it must be complex with case sensitiveness, numeric and special characters. But complex passwords are hard to remember by users for several of their accounts. Henceforth people were interested to go for easiest passwords which can be crack by the attackers easily with different attacking techniques. In this section we explained those password cracking attack techniques [1, 2].

Dictionary Attacks: The challenge-response protocol is vulnerable to a password-guessing attack. In this kind of attack, we assume that an adversary has already built a database of possible passwords, called a dictionary. The adversary eavesdrops on the channel and records the transcript of a successful run of the protocol to learn the random challenge and response. Then the adversary selects passwords from the dictionary and tries to generate a response that matches the recorded one. If there's a match, the adversary has successfully guessed A's password. After every failed matching attempt, the adversary picks a different password from the dictionary [8] and repeats the process. This non-interactive form of attack is known as the offline dictionary attack. Sometimes an adversary might try different user IDs and passwords to log in to a system. For popular Internet services like Yahoo!, the adversary can trivially choose any reasonable user ID due to the large number of registered users. An adversary may also find user IDs within interactive Web communities such as auction sites. If the system rejects the password as being incorrect for that particular user, the adversary picks a different password from the dictionary and repeats the process. This interactive form of attack is called the online dictionary attack.
CAPTCHA: The term "CAPTCHA" was first introduced in 2000 by von Ahn et al. [6], describing a test that can differentiate humans from computers. Under common definitions [4], the test must be easily solved by humans, easily generated and evaluated but not easily solved by computer. Over the past decade, a number of different techniques for generating CAPTCHAs have been developed, each satisfying the properties described above to varying degrees. The most commonly found CAPTCHAs are visual challenges that require the user to identify alphanumeric characters present in an image obfuscated by some combination of noise and distortion.The basic challenge in designing these obfuscations is to make them easy enough that users are not dissuaded from attempting a solution, yet still too difficult to solve using available computer vision algorithms.

III. INTELLIGENT AND ROBUST AUTHENTICATION MANAGEMENT FRAMEWORK

This section describes the implementation of Intelligent and Robust Authentication Management(IRAM) framework to resist password attacks. This framework contains the below modules.

1. White list creation from server logs: There are a number of practical benefits to using IP addresses as the basis for enforcing access controls in today's Internet. IP-based filtering, ACLs [8], and rate-limits are all standard on firewalls and routers. In this paper to reduce the ATTs burden on legitimate users we are also using the IP addresses of users. Every user maximum access their online accounts from a standard set of devices in general. Our framework will record the successful login attempts of every user from various IP addresses and stores that data on server logs. For every given periodic interval time it will update the unstructured data from server logs to the respective structure format i.e. to XML or RDBMS. In this case, this structured data always contains the list various IP's of valid users is treated as white List.

2. Identifying the legitimate users from whitelist and browser cookies Recently Attackers were tried to compromise the online accounts by using online dictionary attacks. Due these attempts are limited (i.e. for Google maximum 3 attempts) and later attacks had to identify the ATTs (CAPTCHA [9]) along with username and password information. With the help ofupdated attacking systems models [8] some adversaries succeeded to crack ATTs, henceforth ATTs become more rigid to protect against attacks. These complex ATTs also became more difficult to identify by legitimate users also. Under these circumstances our framework provides the comfortable access to the legitimate users and rigid access to adversaries with the help of whitelist. Because of the limited normal attempts for authentication from each IP address, adversaries are using various systems with different IP address.

In order to differentiate the legitimate users from attackers our research assuming the whitelist users are legitimate to authenticate. Once any request came to server for authentication after the limited attempts server checks weather the user IP address is available from white list or not. If it is then framework will feel the user is

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

legitimate and challenges only username and password without any ATT for maximum number of attempts. To give the more support to whitelist data [1] this research also considering the cookies information from the request except some exceptional cases. When attackers are trying to compromise the system after limited attempts with DHCP [6], our system will increase to send complex ATTs to user calculated based on number of false attempts. This will work as an interception mechanism for the implemented framework. In order to implement this process we implemented the given below algorithm.

3. Robust authentication algorithm:

Input

WL - whitelist : IP - IP address : UN - Username : PWD - password

NBA - Number of Attempt : MNBA - Maximum Number of Attempts : LNA - limited number of attacks

Begin

ValidateUser(UN,PWD,IP,NBA**)**

If ((NBA <= LNA**) && LoginCheck(**UN,PWD**))**

than allowAccess(un) and **addToWhitelist**(IP)

Else If ((NBA <= MNBA**) && getFromWhiteList(**IP**) || LoginCheck(**UN,PWD**))**

than Message ('Invalid username or password')

displayLogin(un,pwd)

Else If ((NBA <= MNBA**) || getFromWhiteList(**IP**) || LoginCheck(**UN,PWD**))**

than Message ('Invalid username or password')

displayLogin(un,pwd,ATT)

else Message ('Account has been locked for max attempts ')

End

The above algorithm will validate the users from whitelist and increases the complexity for attacks and comforts the accessibility for legitimate users by intelligence [2]. Implementation and results of the framework are explained in the below section.

IV. EXPERIMENTS

In this section we describe the experiments on framework and obtained result information. To test the above approach we are extended the functionality of open source web server apache tomcat of version 6.x. we build a java project to implement the above contributions and attached to java web server tomcat [10]. This java project will create the whitelist with apache server log and identifies the legitimate users in an intelligent manner with the aid of whitelist and cookies information. One of deployed tomcat web applications we chosen with 20 user accounts for attacking with the help of online dictionary manner.

In order to continuously attack on our framework we chosen the popular open source Nessus vulnerability discovery software [6,7]. This software has its own database and several test cases to identify the vulnerabilities on applied server mechanism. Randomly we initiated the attacking from 12 machines with installed software Nessus 4.5 version and tracked the result information for scalability forecasting. In this comparison our framework results we compared with normal Systems with only ATTs. Experimental results are showing in the below table Tab.1.,that our system is providing the comfortable access to legitimate users and becomes very rigid for attackers after limited number of normal attempts. In this case our framework proven that it is legitimate user friendly as well as robust challenge to attack by adversaries.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

Number of:	SSH log	Email log
a) Login events	90,190	48,375
i) with valid usernames	5%	99%
ii) with invalid usernames	95%	1%
b) Valid usernames entered	26	147
c) Invalid usernames entered	13,654	130

Table.1. Attacks Success ratio from SSH Log and Email Log.

V. CONCLUSION

Password based authentication is suffering from various attacking methodologies through online or offline. This authentication became insecure because of various types of attacks like phishing, eavesdrop and dictionary attacks were introduced by adversaries to compromise the system. We covered different types of attacks on password management system and their prominent solutions also. But the solutions against the attacks also become difficult to the legitimate users. In this paper we introduced a new Intelligent and Robust Authentication Management Framework to secure password based authentication as well to make comfortable accessibility to legitimate users. This framework will greatly reduce the ATTs burden on legitimate users and dramatically improves the complexity for compromising the authentication with the aid of user IP address and cookies information by maintaining at server logs.

REFERENCES

[1] Y. He and Z. Han, "User Authentication with Provable Security against Online Dictionary Attacks," J. Networks, vol. 4, no. 3, pp. 200-207, May 2009.

[2] "Fast Dictionary Attacks on Human-Memorable Passwords Using Time-Space Tradeoff," by A. Narayanan and V. Shmatikov, Proc. ACM Computer and Comm. Security, pp. 364-372, Nov. 2005.

[3] E. Bursztein, S. Bethard, J.C. Mitchell, D. Jurafsky, and C. Fabry, "How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation," Proc. IEEE Symp. Security and Privacy May 2010.

[4] Shai Halevi and Hugo Krawczyk, Public-key cryptography and password protocols, ACM Transactions on In-formation and System Security, Vol 2, No. 3, Pages 230-268, August 1999.

[5] P. MacKenzie, More Efficient Password-Authenticated Key Exchange, Topics in Cryptology – CT-RSA 2001,pp. 361-377, 2001.

[6] Carey, Mark; Russ Rogers, Paul Criscuolo, Mike Petruzzi. Nessus Network Auditing. O'reilly. ISBN 978-1-59749-208-

[7] http://www.tenable.com/blog/nessus-521-is-available

[8] http://www.intego.com/mac-security-blog/wordpress-sites-hit-by-dictionary-attack/

[9] Jeffrey P. Bigham and Anna C. Cavender. Evaluating existing audio captchas and an interface optimized for non-visual use. In ACM Conference on Human Factors in Computing Systems, 2009.

[10] tomcat.apache.org/download-70.cgi

AUTHOR BIOGRAPHY

Mr. B. Sunil Kumar working as Assistant Professor in Department of Computer Science & Engineering in Jawaharlal Nehru Institute of Technology, I am having 4 years of Teaching Experience. My interested subjects are Web Technologies, Web services, Mobile computing, cloud computing, Computer Networks, Operating System, Computer Organisation, Java, C, and C++.

Mr. P.Jayasankar, M.Tech (CSE) from Acharya Nagarjuna University. I am presently working as Associate Test Architect in Alliance Global Services in Hyderabad. I am having 8 years of experience as a Test Lead. My interested subjects are Embedded Systems, Computer Networks, Network Security, Operating Systems and Computer Organization.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 2, March 2014

Mrs. T.P.Sarachandrika, M.Tech (CSE) from Acharya Nagarjuna University. I am presently working as Assistant Professor in Department of Computer Science & Engineering in Sri Venkateswara College of Engineering - Tirupathi. I am having 6 years of teaching experience. My interested subjects are Operating Systems, Computer Organization, Software Engineering and Data Base Management Systems.

Dasari.Kiran Kumar M.Tech from ANU Guntur, completed M.C.A from KU, Warangal,. I am presently working as Assistant Professor in Department of Computer Science Engineering in Vignana Bharathi Institute of Technology, Ghatkesar, Aushapur, Hyderabad. I am having 6 years of Teaching Experience. My interested subjects are Software Engineering, Data mining, Web services, Web Technologies, Java, C, and C++.