Security For Password Based Systems Using PGR Protocol

[1]K. S. Shashikala, [2]Mrs. Manjula. G
[1]M.Tech, Department of ISE, East West Institute of Technology, Karnataka, India
[2]Assistant Professor, Department of ISE, East West of Technology, Karnataka, India

Abstract

Dictionary and brute force attacks on password based systems are now widespread and increasing along with cyber security attacks like bots. An effective approach to identify automated malicious login attempts with reasonable cost to users is the Automated Turing Tests (ATTs). The inadequacy of existing and proposed login protocols designed to address password guessing attacks is discussed here. Two well-known existing proposals for limiting online guessing attacks using ATTs are Pinkas and Sander (PS) and Van Oorschot and Stubblebine (VS). We propose a new Password Guessing Resistant (PGR) protocol derived upon revisiting prior proposals. PGR protocol uses either cookies or IP addresses or both for tracking users. PGR protocol limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username.

1. Introduction

Web applications and Secure Shell (SSH) logins are observed against password based systems. Password guessing attacks on websites is a top cyber security risk commonly observed these days. Online attacks have some disadvantages compared to offline attacks. Attacking machines must engage in an interactive protocol and the attacker can guess a limited number of attempts before being locked out. Attackers often must employ a large number of machines to avoid detection or lock-out. Dictionary and brute force attacks on password-only remote login services are now widespread and increasing. Cyber security attacks like bots are also increasing on the password based systems. Enabling convenient login for users and preventing such attacks is a difficult problem. An effective approach to identify automated malicious login attempts with reasonable cost to users is the Automated Turing Tests (ATTs).

The inadequacy of existing and proposed login protocols designed to address large scale password guessing attacks is discussed here. Two well-known proposals for limiting online guessing attacks using ATTs are Pinkas and Sander (PS) and van Oorschot and Stubblebine (VS). We propose a new Password Guessing Resistant Protocol, derived upon revisiting prior proposals. These proposals were designed to restrict the password guessing attacks.

The PGR protocol allows a high number of failed attempts from known machines without answering any ATTs. Tracking users through their IP addresses also allows PGR protocol to increase the number of ATTs for password guessing attacks and meanwhile to decrease the number of ATTs for legitimate login attempts. This is the strict and user friendly ATT based scheme applicable to both web based and text based logins. The whitelist table and failed login table is maintained to keep track of the legitimate users and there threshold value is checked. The protocol is easy to deploy and scalable requiring minimum resources. We analyze the protocol by comparing it with other ATT based protocols.

2. Existing system

Strawman protocol causes the Automated Turing Tests to be generated for each and every login. PS allows attackers to eliminate 95% of the password space without answering any ATTs. The VS proposal reduces attack at a significant cost to usability and requires all users to answer ATTs in certain circumstance username and possibly an expiration data. The users are traced using the cookies, a name value pair which is a temporary one generated for each and every session. Strawman login protocol is another password protection protocol it requires answering an ATT challenge first before entering the user name and password. If the user fails to answer the ATT correctly it prevents the user from proceeding further. So this is a secure but inconvenient login protocol. This protocol is said to be secure and effective against online dictionary attacks because the adversary requires passing an ATT challenge for each password guessing attempt. But legitimate users must also pass an ATT challenge for every login attempt. The main disadvantage of this protocol is that it affects user convenience substantially. It requires the login server to generate an ATT challenge for every login attempt.

PS protocol referred to as Pinkas and Sander protocol that requires answering an ATT challenge first before entering the username, password pair. Failing to answer the ATT correctly prevents the user from proceeding further. This protocol requires the adversary to pass an ATT challenge for each password guessing attempt, in order to gain information about correctness of the guess. VS protocol referred to as Van Oorschot and Stubblebine protocol proposed modifications to the previous protocol which track failed logins per username to impose ATT challenges after exceeding a configurable threshold of failures. In addition, upon entering correct credentials in the absence of a valid cookie, the user is asked whether the machine in use is trustworthy and if the user uses it regularly. The cookie is stored in the user's machine only if the user responds yes to the question.

3. Proposed system

Password Guessing Resistant protocol, derived upon revisiting prior proposals designed to restrict such attacks. While PGR protocol limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, legitimate users in most cases can make several failed login attempts before being challenged with an ATT. The PGR protocol is strict but user-friendly ATT-based scheme. The proposed PGR protocol scheme is more restrictive against attackers than commonly used counter measures. PGR protocol is applicable for both web based logins and SSH logins.

The objectives for PGR protocol include the following.

- The login protocol should make brute force and dictionary attacks ineffective against online guessing attacks.
- The protocol should not have any significant impact on usability issues.
- The protocol should scalable and easily deployable requiring minimum resources.

3.1. Data structures

PGR protocol maintains three data structures. The white list (W) table is maintained for the source IP address, username pairs such that for each pair, a successful login from the source IP address has been initiated for the username previously.The failed login table (FT) is maintained and each entry in the table represents the number of failed login attempts for a valid username. A maximum of k2 failed login attempts are recorded. The failed login table (FS) is maintained and each entry in this table represents the number of failed login attempts for each pair of IP address and username. Here, a maximum of k1 failed login attempts are recorded and crossing this threshold may mandate passing an ATT.

3.2. Different ATT Decision Functions

The decision to challenge the user with an ATT depends on two factors first is whether the user has authenticated successfully from the same machine previously and the second is the total number of failed login attempts for a specific user account. The IP address and the threshold values k1 and k2 are checked here in the below criteria.

3.2.1. ATT challenge will not be asked for valid username and password

The ATT challenge will not be asked for a valid user name and password in the following cases.

- If a valid cookie is received from user machine and if the number of failed login attempts from the user machine's IP address for that username is less than k1 over a time period determined by t3.
- If the user machine's IP address is in the white list W and if the number of failed login attempts from this IP address for that username is less than k1 over a time period determined by t3.
- If the number of failed login attempts from any machine for that username is below a threshold k2 over a time period determined by t2.

3.2.2. ATT challenge will not be asked for invalid username and password

The ATT challenge will not be asked for invalid user name and password in the following cases.

- If a valid cookie is received from user machine and if the number of failed login attempts from the user machine's IP address for that username is less than k1 determined by t3.
- If the user machine's IP address is in the whitelist W and if the no. of failed login attempts from this IP address for that username is less than k1determined by t3.
- If the username is valid and if the number of failed login attempts from any machine for that username is below k2.

3.2.3. ATT challenge for invalid user name and password

The ATT challenge will be asked for invalid user name and password in the following cases.

- If invalid cookie or no cookie is received and if the no. of failed login attempts from any machine for that username is more than k3.
- If the user machine's IP address is not in whitelist W and if the no. of failed login attempts from that IP address for that username is more than k3.

4. System architecture

The system has two users one is “Admin” user who is a super user, who is able to create the user accounts and maintain the captcha images. Another user is “End User” who is able to login into his account and send a mail to other users. The constrain in this system is ATT has to invoke only if the end user did mistake in login details from new IP client systems, ATT should not invoke if the end user did mistake in his regular IP client system.

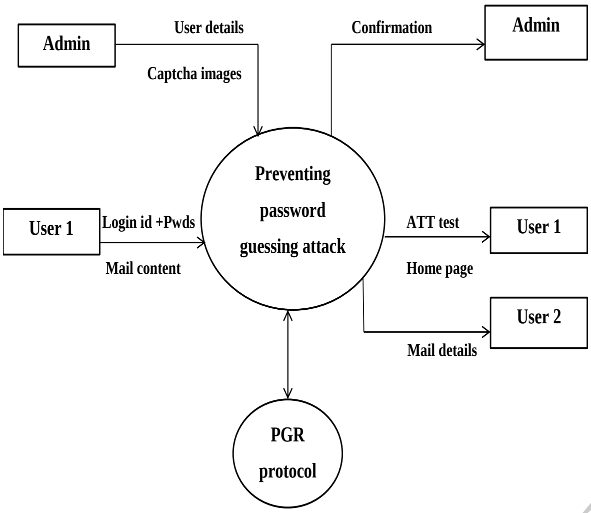

Figure 1.High level design of system working.

When user tries to login to the system if the user enters the correct username and password then the IP address table will be checked. The failed login table for username and password (Pwds) is checked if details are correct then the user is allowed into the home page. The whitelist table will be updated for every successful login. If only valid username is received then the failed login table for username is checked and the table is incremented for valid username.

The user can check the mail inbox in which the user will have sent mails and received mails list. The user can compose mails and send it to the other users. All these transaction details can be seen by the administrator. The user can change the password if needed for the security reasons. The messages will be displayed if the user fails to answer any login condition. The ATT test is the Automatic Turing Test which will be asked for the security reasons. ATT test can be either text or audio which the user has to answer. The different conditions can be checked by connecting two or more systems. First time login from the user and subsequent login from the user are the different conditions that are checked. The client has to open the browser enter the uniform resource locator address, if the client logins correctly then the client can access the service available. The two or more systems can be connected through the local area network connection.

5. Comparison with other ATT based protocols

Strawman protocol is effective against online dictionary attacks assuming that the used ATTs are secure. But this protocol affects user convenience substantially as legitimate users must also pass an ATT challenge for every login attempt.

Table 1.Comparison of Protocol Limitations

parameters	PS	VS	PGR protocol
Ask ATT function required	yes	yes	No
User friendly for legitimate users	No	No	yes
security	Less	Less	High
Cookies drawback	Yes	Yes	No
Suitable for browsers only	Yes	Yes	No
Protocol state grows linearly for failed attempts	No	Yes	No

The PS proposal stores a valid cookie on the browser machine from which user had previously logged in successfully. This protocol is almost similar to Strawman protocol except in the case of successful logins with valid cookies where no ATT is required. The VS proposal decreases the number of incorrect attempts that an adversary can go through without passing any ATT challenge. While this VS protocol overcomes the security drawback of the PS proposal, the legitimate user always faces an ATT challenge once the threshold value is exceeded. The PGR protocol reduces the number of ATTs asked for legitimate users and thus reduces the inconvenience. It provides more number of ATTs for adversaries when they are identified as bot logins.

6. Conclusion

The login protocols which use cookies have a security usability trade-off because of cookie theft and other issues. The proposals like Strawman, Pinkas and Sander, Van Oorschot and Stubblebin had the problems related to security. The Password Guessing Resistant protocol increases the number of ATTs for password guessing attacks and meanwhile decreases the number of ATTs for legitimate login attempts. The problems related to security and usability can be solved using the existing protocol. Existing protocol is more user friendly compared to other ATT based protocols.

7. References

[1] S. M. Bellovin. A technique for counting natted hosts. In ACMSIGCOMM Workshop on Internet measurment, pages 267–272, NewYork, NY, USA, 2002. ACM.
[2] T. Kohno, A. Broido, and K. C.Claffy.Remote physical device fingerprinting. In IEEE Symposium on Security and Privacy, pages 211–225, Washington, DC, USA, 2005. IEEE Computer Society.
[3] B. Pinkas and T. Sander.Securing passwords against dictionary attacks. In ACM conference on Computer and communications security (CCS'02), pages 161 - 170,Washington, DC, USA, Nov. 2002.
[4] M. Casado and M. J. Freedman.Peering through the shroud: The effect of edge opacity on ip-based client identification.In 4thUSENIX Symposium on Networked Systems Design and Implementation (NDSS'07), 2007.
[5] S. Chiasson, P. C. van Oorschot, and R. Biddle.A usability study and critique of two password managers. In USENIX Security Symposium, pages 1–16, Vancouver, B.C., Canada, 2006.
[5] D. Ramsbrock, R. Berthier, and M. Cukier. Profiling attacker behavior following SSH compromises. In IEEE/IFIP Dependable Systems and Networks (DSN'07), pages 119–124, Edinburgh, UK, June 2007.
[6] S. Chiasson, P. C. Van Oorschot, and R. Biddle.A usability study and critique of two password managers. In USENIX Security Symposium, pages 1–16, Vancouver, B.C., Canada, 2006.
[7] J. Yan and A. S. E. Ahmad. A low-cost attack on a Microsoft CAPTCHA. In ACM Computer and Communications Security (CCS'08), pages 543–554, Alexandria, VA, USA, Oct. 2008.