International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Revisiting Defenses against Large-Scale Online Password Guessing Attacks

Ravi Kumar Yalagandala[1], Dr. N. Chandra Sekhar Reddy[2]

[1]Student, M.Tech CSE Department, Institute of Aeronautical Engineering, Hyderabad-500043, Andhra Pradesh, India

[2]Professor, CSE Department, Institute of Aeronautical Engineering, Hyderabad -500043, Andhra Pradesh, India

Abstract: ***Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing rapidly in Day to day life. Enabling users convenient login for legitimate users while preventing such attacks is a difficult problem and not Much convenient Automated Turing Tests (ATTs) are effective and easy to implement but cause reasonable amount of inconvenience to the user.We discuss the existing and proposed login protocols designed to prevent large scale online dictionary attacks. We propose Password Guessing Resistant Protocol (PGRP), which is derived upon revisiting prior proposals designed to restrict such attacks. PGRP reduces the total number of login attempts from unknown remote host while trusted or legitimate users can make several failed login attempts before being challenged by ATT***

Keywords: c,java, online password, failed trials, CAPTCHA

1. Introduction

With increasing number of online users in the real world, maintaining privacy details and protecting them with a password also becomes difficult. Here we involve developing a secure application to prevent our privacy information by using Password Guessing Resistant Protocol (PGRP) guessing attacks on password-based systems are inevitable and commonly observed against web applications and SSH logins. In a recent report, SANS identified password guessing attacks on websites as atop cyber security risk. As an example of SSH password guessing attacks, one experimental Linux honeypot setup has been reported to suffer on average 2,805 SSH malicious login attempts per computer per day. Interestingly, SSH servers that disallow standard password authentication may also suffer guessing attacks, e.g., through the exploitation of a lesser known/used SSH server configuration called keyboard interactive authentication. However, online attacks have some inherent disadvantages compared to offline attacks: attacking machines must engage in an interactive protocol, thus all wing easier detection and in most cases attackers can try only limited number of guesses from a single machine before being locked out, delayed, or challenged to answer Automated Turing Tests (ATTs, e.g., CAPTCHAs Consequently, attackers often must employ a large number of machines to avoid detection or lock-out. On the other hand, as users generally choose common and relatively weak passwords (thus allowing effective password dictionaries and attackers currently control large botnets online attacks are much easier than before

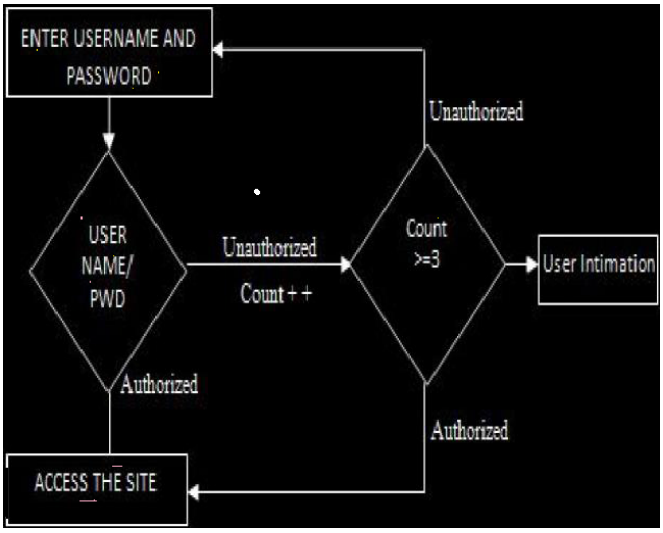
One effective defense against automated online password guessing attacks is to restrict the number of failed trials without ATTs to a very small number (e.g., three),limiting automated programs (or bots) as used by attackers to three free password guesses for a targeted account, even if different machines from a botnet are used. However, this inconveniences the legitimate user who then must answer an ATT on the next login attempt

Several other techniques are deployed in practice, including: allowing login attempts without ATTs from a different machine, when a certain number of faile Several other techniques are deployed in practice, including: allowing login attempts without ATTs from a different machine, when a certain number of failed attempts occur from a given machine allowing more attempts without ATTs after a time-out period; and time-limited account locking. Many existing techniques and proposals involve ATTs, with the underlying assumption that these challenges are sufficiently difficult for bots and easy formost people.

However, users increasingly dislike ATTs as these are perceived as an (unnecessary) extra step; see Yanand Ahmad for usability issues related to commonly used CAPTCHAs. Due to successful attacks which break ATTs without human, ATTs perceived to be more difficult for bots are being deployed. As a consequence of this arms-race, present-day ATTs are becoming increasingly difficult for human use fueling a growing tension between security and usability of ATTs.

Therefore, we focus on reducing user annoyance by challenging users with fewer ATTs, while at the same time subjecting bot logins to more ATTs, to drive up the economic cost to attackers .Two well-known proposals for limiting online guessing attacks using ATTs are Pink as and Sander (herein denoted PS), and van Oorschot and Stubblebine (herein denoted VS). For convenience, a review of these protocols is given in Section 6. The PS proposal reduces the number of ATTs sent to legitimate users, but at some meaningful loss of security; for example, in an example setup (with p ¼ 0:05, the fraction of incorrect login attempts requiring an ATT) PS allows attackers to eliminate 95 percent of the password space without answering any ATTs.

2. System Design



Exisisting system: The use of passwords is a necessity in computer security but passwords are often easy to guess by automated programs or tools running dictionary attacks. In the existing system, an automated test is implemented that humans can pass, but current computer programs can't pass. Any program that has high success over these tests can be used to guess passwords cause security risks. An example of such a test is a 'captcha'. A captcha is a test used in computing which ensures that the response is generated by a person and not by a tool. The process usually involves a computer asking a user to complete a simple test which can ensure a successful login. These tests are designed to be easy for a computer to generate, but difficult for a computer to solve, so that if a correct solution is received, it can be presumed to have been entered by a human.

Proposed system: The is much more convenient than the existing system and consists of minimal steps for legitimate user to login. Two processes involved in this:

1) If a trusted system fails the first login attempt then it is given two more chances (totally three chances). If the user fails in the third attempt to login then the intimation will be given.
2) If an unknown system fails in the first login attempt then it will not be given any more chances and intimation .
3) 3)if the third attempt fails the user cannot login with the same user name. there is a change if it .

3. Motivations

Now a days lot of hacking of pass words has been done in different applications . the users has to select a pass word in a manner that it is so secure in different alphabetical or number order.this is so secure to the user.by this the user may lost his secured information or data. The capcha is also help full to the user in a secure manner to enter the digital code present in the box present in capcha.

Objectives

To detect the pass word gussing attaks against the hackers of data broadcast from server to client via various routers. Identifying the guilty router and also avoiding the security guessing attacks in this systems that could been avoided by all the pass word guessing forms.

Analysis

In the system design there are three modules as :
1.pass point module
2. cued click point module
3.recursive cued click point module

Pass point module: This is a form of click point graphical pass word system and contains a sequence in it and places a pixel image process 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 by this all the given point sequences that has shown in it

a. The number of successful login attempts. The larger the ratio of successful login attempts without answering ATTs to total successful login attempts, the more convenient the login experience for the user.

b. The number of unique usernames in successful logins. For PGRP default parameters, the number of unique usernames in successful logins that involved answering Thus, the majority of valid users were not challenged with any ATT. For the other data set, 11 valid usernames faced an ATT challenge. Cued click point module: This is a form in this as the same sequence that point of equation the next image that can bee diaplayed but current computer programs can't pass. Any program that has high success over these tests can be used to guess passwords

c. The number of failed login attempts with valid usernames. Failed login attempts with valid usernames could be from either malicious or benign sources. In the firstexperiment on PGRP there are 315 failed attemptsnot involving ATTs in the SSH data set and 1,199 in the email data set. Given that the source IP addresses of all theseattempts are in W, these failed attempts are considered benign.

d. The number of unique valid usernames in failed login attempts. In both data sets, setting k2 _ 1 in PGRP causes a significant decrease in the number of unique valid usernames that face ATT challenges in failed login attempts. Other parameters have no significant effect in this manner recursive cued click point module: In this system the recursive form that can been shown as the same form that can been placed as a Due to successful attacks which breakATTs without human , ATTs perceived to be more difficult for bots are being deployed.As a consequence of this arms-race

e. The number of failed login attempts with invalid usernames. Any login attempt with invalid username triggers an ATT in PGRP no failed login attempt with invalid usernames avoids an ATT Indeed, all attempts with invalid usernames trigger ATTs in both data sets.

Algorithm:
begin if Att challenges()=pass then
read credential(un,pw)
if login correct(un.pw)then
accessm is granted to the accoumt

```
else
message('the username and password is correct')
else
message('Att answer is incorect')
end
```

4. Conclusion

Password guessing attacks have been increasing rapidly. To put an end to this we use PGRP. PGRP will restrict the number of attempt made by a system or a machine and allow the legitimate user to have a full secured access over their account. PGRP appears suitable for organizations of both small and large number of user accounts. PGRP can restrict brute force attack and dictionary attack, so it enhances the security of user's account.

5. Future Scope

The developer of an application can never be carried out to the fullest extend in a stipulated time, the main reason why revisions of the secure systems the hacking has done as a greate applicable in it application are always introduced in course of time. This application being restricted to one time development will have no revision done.

6. Acknowledgement

We thank our H.O.D Prof. Dr.N. Chandrashekar Reddy for giving us the eminent facilities to perform my Project work. I am obliged to of CSE department, IARE for their timely help and support.

References

[1] Amazon Mechanical Turk. https://www.mturk.com/mturk/,June 2010.
[2] S.M. Bellovin, "A Technique for Counting Natted Hosts," Proc. ACM SIGCOMM Workshop Internet Measurement, pp. 267-272, 2002.
[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] M. Casado and M.J. Freedman, "Peering through the Shroud: The Effect of Edge Opacity on Ip-Based Client Identification," Proc. Fourth USENIX Symp. 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," Proc. USENIX Security Symp., pp. 1-16, 2006.
[6] D. Florencio, C. Herley, and B. Coskun, "Do Strong Web Passwords Accomplish Anything?," Proc. USENIX Workshop Hot Topics in Security (HotSec '07), pp. 1-6, 2007.
[7] K. Fu, E. Sit, K. Smith, and N. Feamster, "Dos and Don'ts of Client Authentication on the Web," Proc. USENIX Security Symp., pp. 251-268, 2001.
[8] P. Hansteen, "Rickrolled? Get Ready for the Hail Mary Cloud!," http://bsdly.blogspot.com/2009/11/rickrolled-get-ready-forhail- mary.html, Feb. 2010.
[9] 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.
[10] T. Kohno, A. Broido, and K.C. Claffy, "Remote Physical Device Fingerprinting," Proc. IEEE Symp. Security and Privacy, pp. 211-225, 2005.
[11] M. Motoyama, K. Levchenko, C. Kanich, D. Mccoy, G.M. Voelker, and S. Savage, "Re: CAPTCHAs Understanding CAPTCHASolving Services in an Economic Context," Proc. USENIX Security Symp., Aug. 2010.
[12] C. Namprempre and M.N. Dailey, "Mitigating Dictionary Attacks with Text-Graphics Character Captchas," IEICE Trans. Fundamentalsof Electronics, Comm. and Computer Sciences, vol. E90-A, no. 1, pp. 179-186, 2007.
[13] A. Narayanan and V. Shmatikov, "Fast Dictionary Attacks on Human-Memorable Passwords Using Time-Space Tradeoff," Proc. ACM Computer and Comm. Security (CCS '05), pp. 364-372, Nov. 2005.
[14] Nat'l Inst. of Standards and Technology (NIST), Hashbelt. http:// ww.itl.nist.gov/div897/sqg/dads/HTML/hashbelt.html, Sept.2010.
[15] "The Biggest Cloud on the Planet Is Owned by ... the Crooks," NetworkWorld.com., http://www.networkworld.com/community/node/58829, Mar. 2010.
[16] J. Nielsen, "Stop Password Masking," http://www.useit.com/alertbox/passwords.html, June 2009.
[17] B. Pinkas and T. Sander, "Securing Passwords against Dictionary Attacks," Proc. ACM Conf. Computer and Comm. Security (CCS '02), pp. 161-170, Nov. 2002.
[18] D. Ramsbrock, R. Berthier, and M. Cukier, "Profiling Attacker Behavior following SSH Compromises," Proc. 37th Ann. IEEE/IFIP Int'l Conf. Dependable Systems and Networks (DSN '07), pp. 119-124, June 2007