Middle-East Journal of Scientific Research 20 (1): 29-33, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.20.01.11267

The Large-Scale Online Password Guessing Attacks Against with Revisiting Defenses

K. Rajakumari

Department of Computer Science & Engineering,
Bharath University, Tamilnadu, India

Abstract: The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by online attacks such as dictionary and brute force attacks. These attacks are increasing widely during remote login-services. Preventing authorized users from such attacks is a difficult problem. Automated Turing Tests (ATT) is one of the approaches to identify automated malicious login attempts with low cost. Due to inadequacy of existing, we designed a login protocol to address large-scale online dictionary attacks (e.g., from a botnet of hundreds of thousands of nodes). We propose a new Password Guessing Resistant Protocol (PGRP), to restrict such attacks. PGRP limits the total number of login attempts from unknown remote hosts to low as a single attempt per username, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged within ATT.

Key words: Online password guessing attacks · Brute force attacks · Dictionary attacks · ATTs

INTRODUCTION

Online guessing attacks on password-based systems are inevitable and commonly observed against web applications. In a recent report, identified password guessing attacks on websites as a top cyber security risk. online attacks have some inherent disadvantages, attacking machine must engages in an interactive protocol, thus allowing 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, eg., CAPTCHAs). Consequently attackers often must employ a large number of machines to avoid detection or lock-out.

These are identified by their IP addresses saved on the login server as a white-list, or (as in PS) cookies stored on client machines. A white-listed IP address and/or client cookie expires after a certain time. PGEP accomadates both graphical user interface (e.g., browser-based logins) and character-based interfaces (e.g., SSH logins), while the previous protocols seals exclusively with the former, requiring the use of browser cookies. PGRP uses either cookies or IP addresses, or both for tracking legitimate users. Tracking users through their IP addresses also allows PGRP to increase the number of ATTs for password guessing attacks and meanwhile to decrease the number of ATTs for legitimate login attempts. Although NATs and web proxies may (slightly) reduce the utility of IP address information, in practice, the use of IP addresses for client identification appears feasible [1]. In recent years, the trend of logging in to online accounts through multiple personal devices (e.g., PCs, laptops, smart-phones) is growing. When used from a home environment, these devices often share a single public IP address.

Related Works: Existing techniques and proposals involve ATTs, with the underlying assumption that these challenges are sufficiently difficult for bots (automated machines) and easy for humans. 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). Traditional password-based authentication is not suitable for any un trusted environment. He and Han pointed out that a poor design of this function may make the login protocol vulnerable to attacks such as “known function attack"," changed password attack”. Pinkas and Sander presented a login protocol (PS protocol) based on the

Corresponding Author: K. Rajakumari, Department of Computer Science & Engineering,
Bharath University, Tamilnadu, India.

ATT to prevent from brute force and dictionary attacks. To improve the security of PS protocol, Van Oorschot and Stubblebine suggested a modified protocol (VS protocol). In which ATTs are always required once the number of failed login attempts for a particular username exceeds a threshold. For both protocols requires, AskATT () function.

Disadvantages: Protocol is suitable for browsers only. Neither the PS nor VS protocol uses IP addresses. Attackers use different botnets to gain the password for particular user account. So there are more chances to attack the user account from various botnets. The PS proposal reduces the number of ATTs sent to legitimate users, but at some meaningful loss of security. The VS proposal reduces this but at a significant cost to usability.

Proposed System

Password Guessing Resistant Protocol (PGRP): Password Guessing Resistant Protocol (PGRP), significantly improves the security-usability trade-off and can be more generally deployed beyond browser-based authentication. This protocol should make brute force and dictionary attacks ineffective even for adversaries with access to large botnets. PGRP enforces ATTs after a few (eg. 3) failed login attempts are made from unknown machines. PGRP allows a high number (eg. 30) of failed attempts from known machines without answering any ATTs. These are identified by their IP addresses saved on the login server as a white-list, or cookies stored on client machines. A white-listed IP address and/or client cookie expire after a certain time. In recent years, the trend of logging in to online accounts through multiple personal devices (e.g., PCs, laptops, smart-phones) is growing. When used from a home environment, these devices often share a single public IP address which makes IP-based history tracking more user-friendly than cookies. For example, cookies must be stored, albeit transparently to the user, in all devices used for login [2].

Protocol Goals: Our objectives for PGRP include the following:

- The login protocol should make brute-force and dictionary attacks ineffective even for adversaries with access to large botnets (i.e., capable of launching the attack from many remote hosts).
- The protocol should not have any significant impact on usability (user convenience). For example: for legitimate users, any additional steps besides entering login credentials should be minimal. Increasing the security of the protocol must have minimal effect in decreasing the login usability.
- The protocol should be easy to deploy and scalable, requiring minimum computational resources in terms of memory, processing time and disk space.

Modules:

- ATT based protocols
- PGRP protocol
- Block IP
- Send password

Module Description

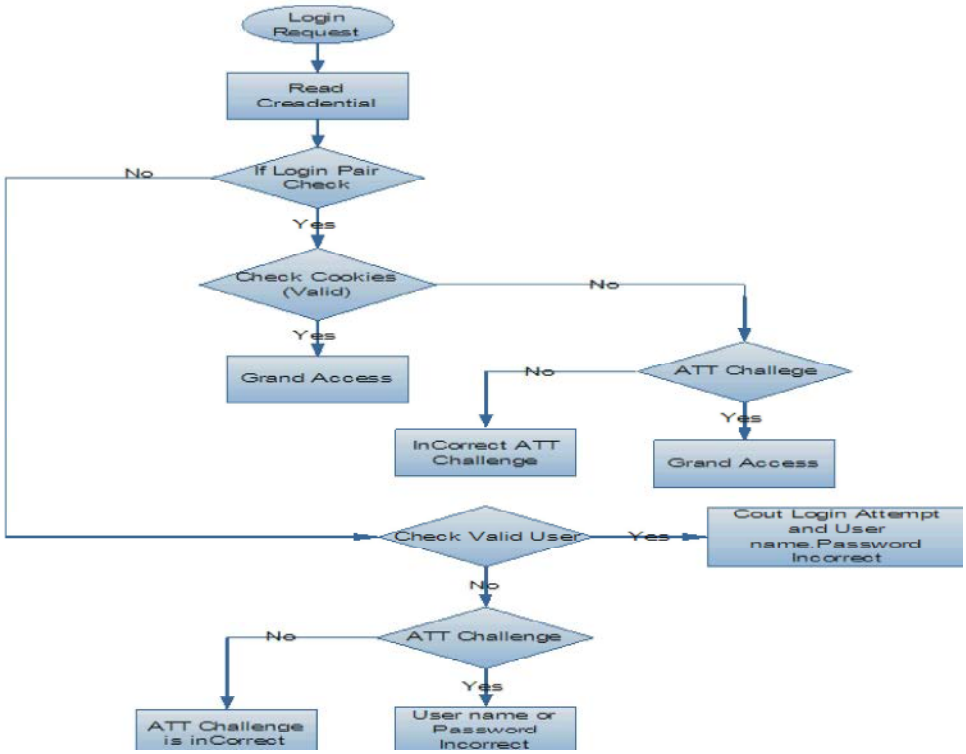
ATT Based Protocols: The user request to enter a *{*username, password*}* pair (Fig. 1). If the pair is correct and a valid cookie (i.e., an unexpired cookie indicating that a successful login for the username was made from the same browser) is received from the browser then the user is granted access. If the pair is correct but no valid cookie is received, then an ATT challenge must be answered before account access is granted. Otherwise, if the {username, password*}* pair is incorrect then according to a function *AskATT* (*username, password*), an ATT challenge might be required before informing the user that the {username, password*}* pair is incorrect [3].

```
1  begin
2      ReadCredential(un, pw, cookie)                  // login prompt to enter username/password pair
3      if LoginCorrect(un, pw) then                    // username/password pair is correct
4              if Valid(cookie, un) then               // cookie unexpired and matches username
5                      GrantAccess(un)                  // access is granted to the account
6              else                                    // no cookie or the cookie is invalid
7                      if ATTChallenge() = Pass then
                               GrantAccess(un)         // access is granted to the account
8                      else Message('login fails')
9      else                                            // username/password pair is incorrect
10             if AskATT(un, pw) = True then
11                     if ATTChallenge() = Pass then Message('login fails')
12                     else Message('login fails')
13             else
14                     Message('login fails')
15 end
```

Algorithm : PS protocol, adapted from Pinkas and Sander

Fig. 1: ATT BASED PROTOCOL

PGRP Protocol:



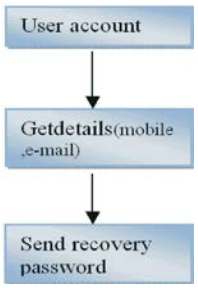
PGRP Protocol:

First the user sent the login request and then reads the credentials. Here the credential means valid username and password pair. Then the username password pair is checked whether it is valid or not. If it is Valid then check for the valid cookies and IP address. If the Cookies and IP address also valid then grant access to the user. Otherwise give ATT challenge to the user. If the ATT challenge is correct then grant access. If the user credential is invalid [4].

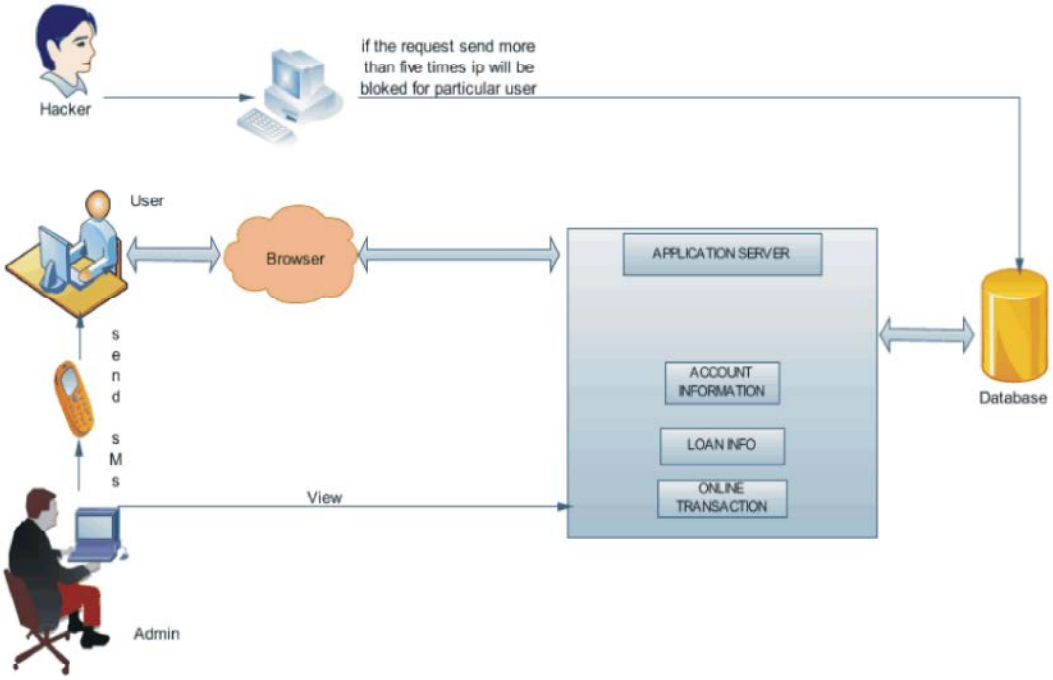
BLOCK IP:

User machine can be identified by the source IP address. Relying on source IP addresses to trace users may result in inaccurate identification for various reasons, including: (i) the same machine might be assigned different IP addresses over time (e.g., through the network DHCP server and dial-up Internet); and (ii) a group of machines might be represented by a smaller number or even a single Internet-addressable IP address. Each entry in this table represents the number of failed login attempts for each pair of (srcIP, un). Here, srcIP is the IP address for a host in W or a host with a valid cookie and un is a valid username attempted from srcIP. A maximum of k1 failed login attempts are recorded; crossing this threshold may mandate passing an ATT (e.g., depending on an entry is set to 0 after a successful login attempt. Accessing a non-existing index returns 0. It prevents the connection between server and particular IP. It limits the number of failed login attempts [5].

Send Password: Perform password generation, it belongs to legitimate user, it will be often change for each login attempts, so, this account password won't be trace out as everyone i.e. unauthorized person. This operation comes after the checking the login count. If verification success then user get grand access, otherwise Logging is not valid then send information such as "unauthorized users are accessing your account " and also generate a onetime password to reopen legitimate user account.



System Architecture: System architecture is the conceptual design that defines the structure and behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured and systems developed, that will work together to implement the overall system. This may enable one to manage investment in a way that meets business needs.



The composite of the design architectures for products and their life cycle processes. A representation of a system in which there is a mapping of functionality onto hardware and software components, a mapping of the software architecture onto the hardware architecture and human interaction with these components. An allocated arrangement of physical elements which provides the design solution for a consumer product or life-cycle process intended to satisfy the requirements of the functional architecture and the requirements baseline. Architecture is the most important, pervasive, top-level, strategic inventions, decisions and their associated rationales about the overall structure (i.e., essential elements and their relationships) and associated characteristics and behavior.

CONCLUSION

Online password guessing attacks on password-only systems have been observed for decades. Present-day attackers targeting such systems are empowered by having control of thousand to million-node botnets. In previous ATT-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts versus user login convenience. In contrast, PGRP is more restrictive against brute force and dictionary attack, while safely allowing a large number of free failed attempts for legitimate users. our empirical experiments show that PGRP is apparently more effective in preventing password guessing attacks [6-15].

PGRP appears suitable fo organizations of both small and large number of user accounts. The required system resources are linearly proportional to the number of users in a system.PGRP can also be used with remote login services where cookies are not applicable [16-20].

REFERENCES

1. Bursztein, E., S. Bethard, J.C. Mitchell, D. Jurafsky and C. Fabry, 2010. How good are humans at solving CAPTCHAs?A large scale evaluation.In IEEE symposium on security and privacy. USA.
2. Kerana Hanirex, D. and K.P. Kaliyamurthie, 2013. Multi-classification approach for detecting thyroid attacks, International Journal of Pharma and Bio Sciences, 4(3): B1246-B1251.
3. Khanaa, V., K. Mohanta and T. Saravanan, 2013. Comparative study of uwb communications over fiber using direct and external modulations, Indian Journal of Science and Technology, 6(6): 4845- 4847.
4. Kumar, Giri, R. Saikia and M. Multipath, 2013. Routing for admission control and load balancing in wireless mesh networks, International Review on Computers and Software, 8(3): 779-785.
5. Kumarave, A. and K. Rangarajan, 2013. Routing alogrithm over semi-regular tessellations IEEE Conference on Information and Communication Technologies, ICT.
6. Kumarave, A. and K. Rangarajan, 2013. Algorithm for automaton specification for exploring dynamic labyrinths, Indian Journal of Science and Technology, 6(6).
7. Pinkas, B. and T. Sander, 2002. Securing password against dicionary attacks. In ACM conference on computer and communications security. USA.
8. Motoyama, M., K. Levchenko, C. Kanich, D. Mccoy, G.M. Voelker and S. Savage, 2010. Re: CAPTCHA's understanding CAPTCHA-solving services in an economic context in USENAX security symposium. USA.
9. Chiasson, S., P.C. van Oorschot and R. Biddle, 2006. Usuability study and critique of two password managers in USENAX security symposium. CANADA.
10. Bellovin, S.M., 2002. A technique for counting natted hosts. In ACM SIGCOMM workshop on internet measurement, USA.
11. Van Oorschot, P.C. and S. Stubblebine, 2006. On countering online dictionary attacks with login histories and humans-in-the-loop.ACM transactions on information and systems security (TISSEC).
12. Von Ahn, L., M. Blum, N. Hopper and J. Langford, 2003. CAPTCHA: Using hard AI problems for security. In Eurocrypt, Poland.
13. Weir, M., S. Aggarwal, M. Collins and H. Stern, 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM conference on computer and communications security, ACM.
14. Xie, Y., F. Yu, K. Achan, E. Gillum, M. Goldszmidt and T. Wobber, 2007. How dynamic are IP addresses? SIGCOMM comput. Commun.
15. Yan, J. and A.S.E. 2008. Ahmad. A low-cost attack on a Microsoft CAPTCHA. In ACM computer and communications security, USA.
16. Shafaq Sherazi and Habib Ahmad, 2014. Volatility of Stock Market and Capital Flow Middle-East Journal of Scientific Research, 19(5): 688-692.
17. Kishwar Sultana, Najm ul Hassan Khan and Khadija Shahid, 2013. Efficient Solvent Free Synthesis and X Ray Crystal Structure of Some Cyclic Moieties Containing N-Aryl Imide and Amide, Middle-East Journal of Scientific Research, 18(4): 438-443.
18. Pattanayak, Monalisa and P.L. Nayak, 2013. Green Synthesis of Gold Nanoparticles Using Elettaria cardamomum (ELAICHI) Aqueous Extract World Journal of Nano Science & Technology, 2(1): 01-05.
19. Chahataray, Rajashree and P.L. Nayak, 2013. Synthesis and Characterization of Conducting Polymers Multi Walled Carbon Nanotube-Chitosan Composites Coupled with Poly (P-Aminophenol) World Journal of Nano Science and Technology, 2(1): 18-25.
20. Parida, Umesh Kumar, S.K. Biswal, P.L. Nayak and B.K. Bindhani, 2013. Gold Nano Particles for Biomedical Applications World Journal of Nano Science & Technology, 2(1): 47-57.