PREVENTNG DEFENSES AGAINST ONLINE PASSWORD GUESSING ATTACKS

[1]C.P Dhanakarna, [2]S.Jayalakshmi

[1]Research Scholar, Department of Computer Science, [2]Asst. Prof, Department of IT,
VELS University, Pallavaram, Chennai – 117, Tamil Nadu, (India)

ABSTRACT

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for licensed users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users. In this paper we discuss the deficiency of existing and proposed login protocols designed 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), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, licensed users in most cases (e.g., When attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT. We analyze the performance of PGRP with two real-world datasets and find it more promising than existing proposals.

I INTRODUCTION

Online guessing attacks on password-based systems are unavoidable and commonly observed against web applications and SSH logins. However, online attacks have some inherent disadvantages compared to offline attacks: attacking machines must engage 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, 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 (e.g., Conficker), online attacks are much easier than before.

II PASSWORD GUESSING RESISTANT PROTOCOL (PGRP)

Goals, Operational Assumptions

2.1 Protocol goals

Our objectives for PGRP include the Following:

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

2.2 Assumptions

We assume that rival can solve a small percentage of ATTs, e.g., through automated programs, brute force mechanisms, and low paid workers (e.g., Amazon Mechanical Turk . Incidents of attackers using IP addresses of known machines and cookie theft for targeted password guessing are also assumed to be minimum. Traditional password-based authentication is not suitable for any untrusted environment (e.g., a key logger may record all keystrokes, including passwords in a system, and forward those to a remote attacker). We do not prevent existing such attacks in untrusted environments, and thus essentially assume any chiness that licensed users use for login are trustworthy. The data integrity of cookies must be protected (e.g., by a MAC using a key known only to the login server).
Our method of protection against online password-guessing attacks and related denial-of-service attacks, the owner and the users granted administrative privileges are referred to administrators. Only the owner registers with the application provider other user accounts are created by admin using a Web interface. Each user logs in with three credentials rather than the usual two: The application instance name, which is considered a secret shared by the users of the application instance. The instance name can be changed by the owner. A user ID, which is known only to the user and the administrators.
The user ID is chosen by the admin who creates the user account, and can be changed by an admin (by any administrator if the user has no administrative privileges, by the owner if the user is herself an admin). A password, known only to the user. After a certain number of consecutive bad guesses against a password, the user is locked out. Bad guesses are considered to be consecutive if there is no intervening successfully completed login to the user's account. All the consecutive bad guesses must be against the same password; counting starts over if the password is changed. A user who has been locked out was allowed to log in again once her password has been reset.

When the user changes her password, she is not allowed to select as the new password a password that has previously been used as a permanent or temporary password on her user account. This method provides protection against online guessing attacks and related denial-of-service attacks, including attacks by ex-users, and other security benefits.

III THE REMOTE NETWORK MONITORING (RMON)

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. An RMON implementation typically operates in a client/server model. Monitoring devices (commonly called "probes" in this context) contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients.

In our research work the Remote Monitoring is achieved by the use of Android Mobile device . Android Mobile device acts as remote. Others are clients.

Advantages:

- The user ID is chosen by the admin who creates the user account, and can be changed by an admin.
- Hackers trying to attempt more time to lock the particular account.

3.1 Data Structure and Function Description

PGRP maintains three data structures:

1) W: A list of fsource IP address, usernameg pairs such that for each pair, a successful login from the source IP address has been initiated for the username previously.

2) FT: Each entry in this table represents the number of failed login attempts for a valid username, UN. A maximum of failed login attempts are recorded. Accessing a non-existing index returns 0.

3) FS: 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. An entry is set to 0 after a successful login attempt. Accessing a non-existing index returns 0. Each entry in W, FT, and FS has a “write-expiry” interval such that the entry is deleted when the given Period of time has lapsed since the last time the entry was inserted or modified. There are different ways to implement write-expiry intervals (e.g., hash belt. A simple approach is to store a timestamp of the insertion time with each entry such that the timestamp is updated whenever the entry is modified. At anytime the entry is accessed, if the delta between the access time and the entry timestamp is greater than the data structure write-expiry interval, the entry is deleted.

IV CONCLUDING

Online password guessing attacks on password-only systems have been observed for decades. Present-day attackers targeting such systems were empowered by having control of thousand to million node botnets. PGRP appears suitable for organizations of both small and large number of user accounts.

The required system resources (e.g., memory space) 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 (e.g., SSH and FTP).

REFERENCES

[1] Amazon Mechanical Turk. Accessed: June 2010. https://www. mturk.com/mturk/.

[2] S. M. Bellovin. A technique for counting natted hosts. In ACM SIGCOMM Workshop on Internet measurement, pages 267–272, New York, NY, USA, 2002. ACM.

[3] E. Bursztein, S. Bethard, J. C. Mitchell, D. Jurafsky, and C. Fabry. How good are humans at solving CAPTCHAs? A large scale evaluation. In IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 2010.

[4] M. Casado and M. J. Freedman. Peering through the shroud: The effect of edge opacity on ip-based client identification. In 4th USENIX Symposium on Networked Systems Design and Implementation (NDSS'07), 2007.

[5] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability studyand critique of two password managers. In USENIX Security Symposium, pages 1–16, Vancouver, B.C., Canada, 2006.

[6] D. Florˆencio, C. Herley, and B. Coskun. Do strong web passwords accomplish anything? In USENIX workshop on Hot topics in security (HotSec'07), pages 1–6, Berkeley, CA, USA, 2007.

[7] K. Fu, E. Sit, K. Smith, and N. Feamster. Dos and don'ts of client authentication on the web. In USENIX Security Symposium, pages 251–268, Washington, DC, USA, 2001.

[8] P. Hansteen. Rickrolled? Get Ready for the Hail Mary Cloud! http://bsdly.blogspot.com/2009/11/ rickrolled-get-ready-for-hail-mary.html. Accessed: Feb. 2010.

[9] Y. He and Z. Han. User authentication with provable security against online dictionary attacks. Journal of Networks (JNW), 4(3):200–207, May 2009.

[10] 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.

[11] M. Motoyama, K. Levchenko, C. Kanich, D. Mccoy, G. M. Voelker, and S. Savage. Re: CAPTCHAs understanding CAPTCHAsolving services in an economic context. In USENIX Security Symposium, Washingtion, DC, USA, Aug. 2010.