www.ijiarec.com

DEC 2013

International Journal of Intellectual Advancements and Research in Engineering Computations

USER AUTHENTICATION DEFENSE AGAINST ONLINE DICTIONARY ATTACKS

[*1]Mr. A.Ganesan, [2]Mrs.D.Bhuwaneshwari,M.E.,

ABSTRACT

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate 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, the inadequacy 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). 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, 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 with an ATT. Finally, the performance of PGRP with two real-world datasets and find it more promising than existing proposals.

Index terms: Sensitive-attributes, Quasive-identifiers, Generalization, Bucketization, Multiset generalization .

I INTRODUCTION

Online 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 a top cyber security risk. As an example of SSH passwordguessing attacks, one experimental Linux honeypot setup has been reported to suffer on average 2,805 SSH malicious login attempts per computer per day (see also. 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 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 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 failed attempts occur from a given machine;

Author for Correspondence:
[*1]Mr.A.Ganesan, PG Scholar, Department of CSE, Sri Krishna Engineering College Panapakam, Chennai-301, India.
E-mail: ganeshraja944@gmail.com
[2]Mrs.D.Bhuwaneshwari, M.E., Asst.Professor, Dept. of CSE, Sri Krishna Engineering College, Panapakam, Chennai-301, India.

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 for most people. However, users increasingly dislike ATTs as these are perceived as an (unnecessary) extra step; see Yan and Ahmad for usability issues related to commonly used CAPTCHAs. Due to successful attacks which break ATTs without human solvers, 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 users, 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 Pinkas and Sander (herein denoted PS), and van Oorschot and Stubblebine (herein denoted VS). For convenience, a review of these protocols. 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. The VS profe reduces this but at a significant cost to usability; for example, VS may require all users to answer ATTs in certain circumstances. The proposal in the present paper, called Password Guessing Resistant Protocol (PGRP), significantly improves the security-usability trade-off, and can be more generally deployed beyond browser-based authentication. PGRP builds on these two previous proposals. In particular, to limit attackers in control of a large botnet (e.g., comprising hundreds of thousands of bots), PGRP enforces ATTs after a few (e.g., three) failed login attempts are made from unknown machines. On the other hand, PGRP allows a high number (e.g., 30) of failed attempts from known machines without answering any ATTs. We define known machines as those from which a successful login has occurred within a fixed period of time. 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 expire after a certain time. PGRP accommodates both graphical user interfaces (e.g., browser-based logins) and character-based interfaces (e.g., SSH logins), while the previous protocols deal 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. 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 (i.e., a simple NAT 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.

II PROBLEM AND ANALYSIS

Computers and Humans Apart (CAPTCHAs) are widely used by websites to distinguish abusive programs from real human users. Captchas typically present a user with a simple test like reading digits or listening to speech and E. Bursztein, S. Bethard, J. C. Mitchell, D. Jurafsky, and C. Fabry presented a completely Automated Public Turing tests to tell then ask the user to type in what they saw or heard. The image or sound is usually distorted in various ways to make it difficult for a machine to perform the test. When successful, captchas can prevent a wide variety of abuses, such as invalid account creation and spam comments on blogs and forums. Captchas are intended to be easy for humans to perform, and difficult for machines to perform. While there has been much discussion of making captchas difficult for machines, to the best of our knowledge there has been no large scale study assessing how well captchas achieve the former goal: making it easy for humans to pass the test. We address this problem by collecting captcha samples from each of the 13 most used image schemes and 8 most used audio schemes, for a total of over 318,000 captchas. D. Ramsbrock, R. Berthier, and M. Cukier practical experience report presents the results of an experiment aimed at building a profile of attacker behavior following a remote compromise. For this experiment, we utilized four Linux honeypot computers running SSH with easily guessable passwords. During

the course of our research, we also determined the most commonly attempted usernames and passwords, the average number of attempted logins per day, and the ratio of failed to successful attempts. To build a profile of attacker behavior, we looked for specific actions taken by the attacker and the order in which they occurred. These actions were: checking the configuration, changing the password, downloading a file, installing/running rogue code, and changing the system configuration. Shiying Hu, Eric A. Hoffmanand Joseph M. Reinhardt says that "Throughout the developed world, governments, defense industries, and companies in finance, power, and telecommunications" are increasingly targeted by overlapping surges of cyber attacks from criminals and nation-states seeking economic or military advantage. The number of attacks is now so large and their sophistication so great, that many organizations are having trouble determining which new threats and vulnerabilities pose the greatest risk and how resources should be allocated to ensure that the most probable and damaging attacks are dealt with first. Exacerbating the problem is that most organizations do not have an Internet-wide view of the attacks. This report uses current data - covering March 2009 to August 2009 - from appliances and software in thousands of targeted organizations to provide a reliable portrait of the attacks being launched and the vulnerabilities they exploit. The report's purpose is to document existing and emerging threats that pose significant risk to networks and the critical information that is generated, processed, transmitted, and stored on those networks. This report summarizes vulnerability and attack trends, focusing on those threats that have the greatest potential to negatively impact your network and your business. It identifies key elements that enable these threats and associates these key elements with security controls that can mitigate your risk.

III SOLUTION AND MECHANISM

Online guessing attacks on password-based systems are inevitable and commonly observed against web applications identified password guessing attacks on websites as a top cyber security risk. 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. 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. 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 timeout 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 for most people. However, users increasingly dislike ATTs as these are perceived as an (unnecessary) extra step; see Yan and Ahmad for usability issues related to commonly used CAPTCHAs. Due to successful attacks which break ATTs without human solvers. The PS proposal reduces the number of ATTs sent to legitimate users, but at some meaningful loss of security; incorrect login attempts requiring an ATT) PS allows attackers to eliminate 95% of the password space without answering any ATTs. The VS proposal reduces this but at a significant cost to usability; for example, VS may require all users to answer ATTs in certain circumstances. The proposal in the present paper, called Password Guessing Resistant Protocol (PGRP), significantly improves the security-usability trade-off, and can be more generally deployed beyond browser-based authentication. PGRP builds on these two previous proposals. In particular, to limit attackers in control of a large botnet (e.g., comprising hundreds of thousands of bots).

SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual design that defines the structure and/or 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 fundamental organization of a

system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution. The composite of the design architectures for products and their life cycle processes. A Rep 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.

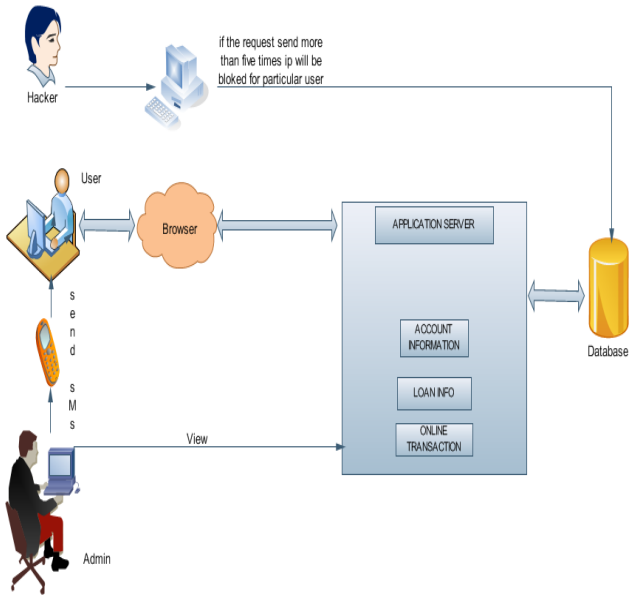

Fig System Architecture.

METHODOLOGY

Registration

This module allows the user to login and use their account. The login program invokes the user shell and enables command execution. Login is the very first step for the user to use their account. The usage of login form is to give security to the user. If the user doesn't have the account then the user should create the account.

Creating New Accounts

This module allows the user to create the new account. If the user doesn't have account then he can create the account online. Customer who creates account online he/she must have to submit the essential documents for proof of address, Identification at the nearest branch or they can send documents through postal. Creation allows the user to get all the facilities offered by the online Banking.

Tracking hackers: Invalid username when a user tries login with a non-existent username (e.g., typing errors), an ATT challenge is given. Irrespective of the password or ATT answer, the login fails. This feature restricts attackers from learning valid usernames (except the usernames obtained via brute force attacks as explained in and improves protocol performance in terms of memory usage (i.e., no entries in protocol data structures. However, from a usability point of view, this is not ideal. We expect that this type of error would be limited in practice (in part because usernames, in contrast to passwords, are echoed on a display).

Send password

Send password perform password generation, it belongs to special user, it will be often change for each transaction, 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 send random generator password to belong user, otherwise Logging is not valid then send information such as "unauthorized users are accessing your account ".

Block source 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.

IV CONCLUSION

In this project, novel robust active shape method for the fully automated segmentation of lung cancer region was presented. The robustness and effectiveness was demonstrated, where conventional segmentation methods frequently fail to deliver usable result. Low segmentation error was achieved in cases with and without high-density pathology, compared to two clinically utilized methods. This approach not only allows coping with disturbances (e.g. outliers), but it also well suitable for large shape models and parallel implementation, allowing low computation times. Though it present a fully automated segmentation of lungs, it is not optimized for segmentation of small lung nodules and lung lobes. To overcome this issue, local shape analysis approach is used, which focus on handling small lung nodules. It is based on correction procedure of a preliminary initial segmentation. The correction method has the advantage that it locally refines the nodule segmentation along recognized vessel attachments only, without modifying the nodule boundary elsewhere. The proposed correction method, improve the segmentation quality of lung nodules.

REFERENCE

[1]. [1] T. Kohno, A. Broido, and K.C. Claffy, “Remote Physical Device Fingerprinting,” Proc. IEEE Symp. Security and Privacy, pp. 211-225.

[2]. [2] M. Motoyama, K. Levchenko, C. Kanich, D. Mccoy, G.M. Voelker, and S. Savage, “Re: CAPTCHAs Understanding CAPTCHASolving

[3]. Services in an Economic Context,” Proc. USENIX Security Symp., Aug. 2010.

[4]. [3] C. Nampempre and M.N. Dailey, “Mitigating Dictionary Attacks with Text-Graphics Character Captchas,” IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, vol. E90-A, no. 1, pp. 179-186, 2007.

[5]. [4] A. Narayanan and V. Shmatikov, “Fast Dictionary Attacks on Human-Memorable Passwords Using Time-Space Tradeoff,” Proc.

[6]. ACM Computer and Comm. Security (CCS ’05), pp. 364-372, Nov. 2005.

[7]. [5] Nat’l Inst. of Standards and Technology (NIST), Hashbelt. http:// www.itl.nist.gov/div897/sqg/dads/HTML/hashbelt. html, Sept. 2010.

[8]. [6] “The Biggest Cloud on the Planet Is Owned by ... the Crooks,” NetworkWorld.com., http://www.networkworld.com/ community/node/58829, Mar. 2010.

[9]. [7] J. Nielsen, “Stop Password Masking,” http://www.useit.com/ alertbox/passwords.html, June 2009.