Intelligent Password File Protection By Dynamic Honeywords

M.Aishwarya, S.Kiruthika, R.Ramya, M.Gayathri and P.Manikandaprabu.

Anjalai Ammal Mahalingam Engineering College,Kovilvenni.

ABSTRACT*-System security admin and black hat attackers are the evergreen rivals from long time by the introduction on computing and security. There are several methodologies and algorithms to protect a system and also there are several tools and back-door process to break the security credentials of a PC or a Server. Brute force attacking and DDOS tools has the capability to break the passwords stored in the password hash. The tools like ophcrack and rainbowcrack has the ability to effectively crack the password hash from the password database. Most of the non computer students are using the same password for all of their online accounts. If any one of the weakly secured password database is attacked by any hackers then he/she can also try that account details to access your other domain accounts. To prevent this process this project work proposes a novel method named PasswordProxy. PasswordProxy is the fake authentication server implemented in low cost to spoof the attackers. Unlike existing system the proposed methodology doesn't allow the hacker in the real domain rather in fake PasswordProxy. The system will be implemented and tested to ensure security, preserve domain privacy policy, provides low cost implementation with less effort.*

Keywords: PasswordProxy, Honeywords, Password protection

I. INTRODUCTION

Password Security

Password managers are critical pieces of software relied upon by users to securely store valuable and sensitive information, from online banking passwords and login credentials to passport- and social security numbers. Surprisingly, there has been very little academic research on the security these applications provide. This paper presents the first rigorous analysis of storage formats used by popular password managers. We define two realistic security models, designed to represent the capabilities of real-world adversaries. We then show how specific vulnerabilities in our models allow an adversary to implement practical attacks. Our analysis shows that most password manager database formats are broken even against weak adversaries.

Problems with Password Databases

Users typically solve this problem in one of the two ways. A common solution is to reuse the same password on many different websites. This approach increases the potential damage if a password is stolen, cracked, or if a service that has access to it is compromised, since the attacker will be able to reuse it on all online services that share the password. Another approach is to use a "password manager" to store strong (random) passwords for each site. A password manager is a piece of software that requires a user to remember a single strong master password, used to decrypt the password manager's database. Remembering a single master password is much more feasible for users, who still get the security benefits of using a different password for each online service

Password Storage methods

For password authentication systems, users often are the enemy. Schneier writes, [1] "the problem is that the average user can't and won't even try to remember complex enough passwords to prevent dictionary attacks. As bad as passwords are, users will go out of the way to make it worse. If you ask them to choose a password, they'll choose a lousy one. If you force them to choose a good one, they'll write it on a Post-it and change it back to the password they changed it from the last month. And they'll choose the same password for multiple applications." In short, poor password practices undermine the system. Many projects focus on developing new technology around these poor practices without studying them. In contrast, this paper broadly looks at password practices, quantifying password reuse and also surveying the contributing factors to this reuse. We not only consider how users justify their poor practices but also study what encourages them to do better. We link these practices password management tools and discuss ways current technology supports poor practices. We also demonstrate users are ill-informed about dictionary attacks from responses to a survey of what constitutes strong passwords and who could compromise passwords.

Previous methodology

Recently, Juels and Rivest proposed honeywords (decoy passwords) [2] to detect attacks against hashed password databases. For each user account, the legitimate password is stored with several honeywords in order to sense impersonation. If honeywords are selected properly, a cyber-attacker who steals a file of hashed passwords cannot be sure if it is the real password or a honeyword for any account. Moreover, entering with a honeyword to login will trigger an alarm notifying the administrator about a password file breach. At the expense of increasing the storage requirement by 20 times, the authors introduce a simple and effective solution to the detection of password file disclosure events. In this study, we scrutinize the honeyword system and present some remarks to highlight possible weak points. Also, we suggest an alternative approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords – a perfectly flat honeyword generation method – and also to reduce storage cost of the honeyword scheme.

Our approach

The proposed method introduces PasswordProxy for faking the security weaknesses of the server. PasswordProxy is the fake authentication server implemented to handle password attacks against the domain like DOS and Bruteforce. The idea is instead of fighting against the attacks lets fake the attacker by providing less secure user account details to be vulnerable. The proposed model uses the Request Repentance Detection mechanism to identify the attack and switching the attacker session to the fake PasswordProxy. PasswordProxy collects the attacker's location information, IP, MAC and application details which is send to the real authentication server. Using the attacker’s information the real authentication server may block the attacker from the real domain environment. PasswordProxy is the low cast server with lesser resources to fake the attacker. So the cost of implementation is low compared to the existing Honeyword. PasswordProxy manages its own fake password database account, webserver to allow attacker to get fake details of the user. Privacy policy of the domain is preserved by the proposed PasswordProxy. The attack is detected before every the attacker gets into the password database.

II. RELATED WORK

This paper proposed a two-factor lightweight privacy preserving authentication scheme which employs two core methods: decentralization of CA and biological password based 2FA [3]. Based on the decentralization of CA, the proposed scheme requires only several extreme lightweight hashing process and a fast MAC generation is needed for message signing, a hash function along with one fast MAC re-generation for verification, which increases efficiency of computation and communication. To the best of our knowledge, 2FLIP [4] is the first authentication scheme that achieves both strong privacy preservation and DoS resilience for secure VANET communication with the benefits of combining the two core methods. It also provides a feasible feature of offline biological password update to support driving right transferring from one to the other of a vehicle.

The machine-to-machine (M2M) communication [5], which plays a vital role in the Internet of Things (IoT), allows wireless and wired systems to monitor environments and exchange the information among various machines automatically without human interventions. In order to promote the development of the IoT and exploit the M2M applications, the Internet Engineering Task Force (IETF) [6] has been developing a standard named Internet Protocol version 6 (IPv6) over Low Power Wireless Personal Area Networks (6LoWPAN) [7] to enable IP-based M2M devices to connect to the open Internet. The formal verification and the simulation show that the proposed scheme in 6LoWPAN could not only enhance the security functionality with the ability to prevent various malicious attacks but also incur less computational and transmission overhead.

Mobile user authentication is an essential topic to consider in the current communications technology due to greater deployment of handheld devices and advanced technologies. Memon et al. recently proposed an efficient and secure two-factor authentication protocol for location based services using asymmetric key cryptography. Unlike their claims, the vigilant analysis of this paper substantiates that Memon et al.’s protocol has quite a few limitations such as vulnerability to key compromised impersonation attack, insecure password changing phase, imperfect mutual authentication and vulnerability to insider attack.

A Universal Serial Bus (USB) Mass Storage Device (MSD) [8], often termed a USB flash drive, is ubiquitously used to store important information in unencrypted binary format. This low cost consumer device is incredibly popular due to its size, large storage capacity and relatively high transfer speed. However, if the device is lost or stolen an unauthorized person can easily retrieve all the information. Therefore, it is advantageous in many applications to provide security protection so that only authorized users can access the stored information. This paper analyses the security of the proposed protocol through a formal analysis which proves that the information is stored confidentially and is protected offering strong resilience to relevant security attacks. The computational cost and communication cost of the proposed scheme is analyzed and compared to related work to show that the proposed scheme has an improved tradeoff for computational cost, communication cost and security.

Spectrum sensing and spectrum sharing are two fundamental issues in a cognitive radio network (CRN). The spectrum sensing data falsification (SSDF) attack imposes bad effect on both spectrum sensing process and spectrum sharing process. In order to deal with the SSDF attack and incent secondary users (SUs) to behave well, a joint spectrum sensing and resource allocation (JSSRA) [9] scheme in a CRN is proposed in this paper. The JSSRA problem is formulated as a weighted-proportional-fairness-based resource allocation optimization problem under the constraint that the primary user network is sufficiently protected. Comprehensive performance evaluation is conducted by computer simulation. It is shown that the proposed JSSRA scheme deals with the SSDF attack well in cooperative sensing process to improve the system robustness, and achieves a significant system utility gain in resource allocation.

We propose two algorithms to counteract the above mentioned attack, DRM and SecureVF. DRM is a light-weight algorithm which randomly repositions sensors from overcrowded areas. SecureVF requires a more complex coordination among sensors but, unlike DRM, it enables detection and identification of malicious sensors. We investigate the performance of DRM and SecureVF [10] through simulations. We show that DRM can significantly reduce the effects of the attack, at the expense of an increase in the energy consumption due to additional movements. By contrast, SecureVF completely neutralizes the attack and allows the achievement of the coverage goals of the network even in the presence of localization inaccuracies.

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, we discuss the inadequacy of existing and proposed login protocols designed to address large scale online dictionary attacks.

In this paper we demonstrate a novel and complementary approach to exploiting physical layer differences among wireless devices that is more energy efficient and invariant with respect to the environment. Specifically, we exploit subtle design differences among transceiver hardware types. Transceivers fulfill the physical-layer aspects of wireless networking protocols, yet specific hardware implementations vary among manufacturers and device types. In this paper we demonstrate that precise manipulation of the physical layer header prevents a subset of transceiver types from receiving the manipulated packet.

III. Methodology

The proposed system model is developed with the following given methodologies and procedures,

Web Server

A web server is a computer system that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web. The term can refer to the entire system, or specifically to the software that accepts and supervises the HTTP requests. The primary function of a web server is to store, process and deliver web pages to clients. The communication between client and server takes place using the Hypertext Transfer Protocol (HTTP). Pages delivered are most frequently HTML documents, which may include images, style sheets and scripts in addition to text content. A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP and the server responds with the content of that resource or an error message if unable to do so.

Authentication Server

An authentication server provides a network service that applications use to authenticate the credentials, usually account names and passwords, of their users. When a client submits a valid set of credentials, it receives a cryptographic ticket that it can subsequently use to access various services. Authentication is used as the basis for authorization, which is the determination whether a privilege may be granted to a particular user or process, privacy, which keeps information from becoming known to non- participants, and non-repudiation, which is the inability to deny having done something that was authorized to be done based on the authentication. Authentication Server also implemented with the Request Repentance Detection to detected the security attacks on the server. If any attacks detected it redirects the session to the Password Proxy.

Account Server

A user account is a location on a network server used to store a computer username, password, and other information. A user account allows or does not allow a user to connect to a network, another computer, or other share. Any network that has multiple users requires user accounts. A user often has a user account and is identified to the system by a username. A user is a person who uses a computer or network service. Users generally use a system or a software product without the technical expertise required to fully understand it. Power users use advanced features of programs, though they are not necessarily capable of computer programming and system administration.

PasswordProxy

PasswordProxy is web server which acts as the victim for the security attacks. When the security attack is detected by the authentication server it redirects the session to the PasswordProxy. Then the responsibility of the PasswordProxy is to provide the fake honey account to the user attack. And then it detects the attacker location, username which is used to attack the server and honeyword used as credential. These are used to improve the server security in future. These information are sent to authentication server to make aware of the attacker.

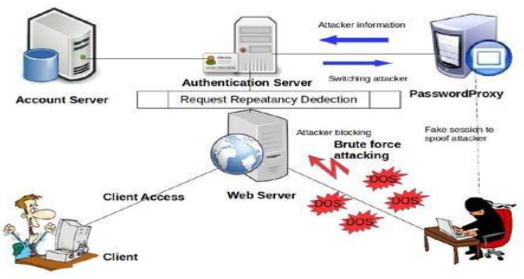
Honeyword database

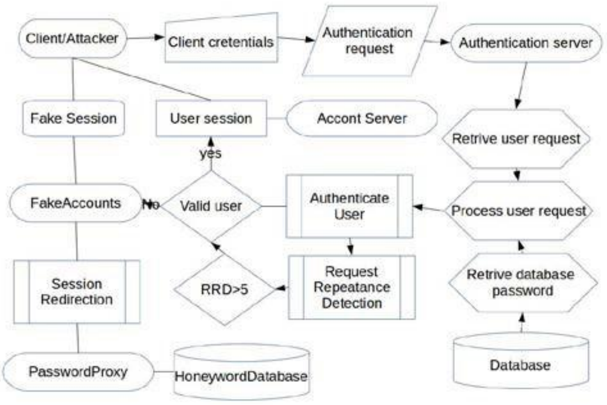
Honeyword database is held by the PasswordProxy with given number of fake honey accounts in it. After the attack is detected on the authentication server the attacker session is transmitted to the PasswordProxy. Unlike other systems the attackers not blocked on the server they are given access for the fake honey account by not disturbing the main webserver. The honeyword database has the fake accounts exactly like the real accounts. This may fake the attackers to feel that they attacked a real accounts on the web server.

Request Repentance Detection

Request Repentance Detection (RRD) algorithm is implemented on the Authentication Server. While on user authentication the RRD gather user-agent information like client browser, client os, client IP, client Host along with username and password. If the request is received from the same host more than the acceptable count then the client host detect as the attacker. And the signal is triggered to the authentication server.

Architecture Diagram





IV. Experimental Evaluation

The number of accounts in the first pass is the number of successful login attempts, a conservative measure of the number of online accounts. The reported statistics from the second pass incorporate the information from the first pass; it was not an independent measure. There were fewer participants in the first pass than in the second pass due to noise introduced by requesting self-reported statistics. One participant was confused between the goals of the first and second passes; his observations were inconsistent and, therefore, dropped. One participant entered nonsense values for the first pass and these observations were dropped.

V. CONCLUSION

This project work has presented a novel PasswordProxy supported with the Request Repentance Detection algorithm to fake the attacker for the password attacks. This project proves that the proposed PasswordProxy is effective to work against the password attacks on the hashed password. The implementation and testing showed that the proposed method is the cost effective one and intellectual in protecting passwords and preventing server privacy policies. The system is tested in the simulated environment and it shows the acceptable performance.

Reference

[1] 2FLIP: A Two-Factor Lightweight Privacy Preserving Authentication Scheme for VANET, Fei Wang, Student Member, IEEE, Yongjun Xu, Hanwen Zhang, Yujun Zhang and Liehuang Zhu, Member, IEEE, 2015

[2] A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks, IEEE Transactions On Industrial Informatics, 2016

[3] A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography, Alavalapati Goutham Reddy, Ashok Kumar Das, Eun-Jun Yoon, and Kee-Young Yoo, 2016

[4] Deceptive Deletion Triggers Under Coercion, Lianying Zhao and Mohammad Mannan, IEEE Transactions On Information Forensics And Security, Vol. 11, No. 12, December 2016

[5] Efficient Biometric and Password Based Mutual Authentication for Consumer USB Mass Storage Devices, Debasis Giri, R. Simon Sherratt, Fellow, IEEE, Tanmoy Maitra, and Ruhul Amin, 2015

[6] Joint Spectrum Sensing and Resource Allocation Scheme in Cognitive Radio Networks with Spectrum Sensing Data Falsification Attack, Huifang Chen, Member, IEEE, Ming Zhou, Lei Xie, Member, IEEE, Kuang Wang, and Jie Li, Senior, IEEE, 2016

[7] On the vulnerabilities of the virtual force approach to mobile sensor deployment, N. Bartolini, Member, IEEE, G. Bongiovanni, T. La Porta, Fellow, IEEE and S. Silvestri, Member, IEEE, 2014

[8] Revisiting Defenses against Large-Scale Online Password Guessing Attacks, Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, Member, IEEE, IEEE Transactions On Dependable And Secure Computing, 2012

[9] Security Considerations in Minutiae-based Fuzzy Vaults, Benjamin Tams, Preda Mihăilescu and Axel Munk, IEEE Transactions on Information Forensics and Security, 2015

[10] Wireless Intrusion Detection and Device Fingerprinting through Preamble Manipulation Benjamin W. Ramsey, Member, IEEE, Barry E. Mullins, Senior Member, IEEE, Michael A. Temple, Senior Member, IEEE, and Michael R. Grimaila, Senior Member, IEEE, IEEE Transactions On Dependable And Secure Computing, 2014.