Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

Web Guard: Web Intrusion Detection and Prevention

Ms. J. Cynthia
Department of Computer science
Coimbatore, Tamilnadu,

***Abstract*— Internet service and applications have become an inextricable part of daily life, enabling communication and the management of personal information from anywhere. To accommodate this increase in application and data complexity, web services have moved to a multitier design wherein the webserver runs in application front-end logic and data are outsourced to a database or file server. Daily tasks, such as banking, travel and social networking, all are done via the web with this multitier design. Such services typically employ a webserver front end that runs the application user interface logic, as well as a back-end server that consists of a database or file server. This is the part that covers the server architecture. Text password is the most popular form of user authentication on websites due to its convenience and simplicity. Providing passwords for accessing a particular account is for end users security. However user's password is easily stolen and compromised under different treats and vulnerabilities. Firstly user often select weak password and reuse same password across different websites that cause domino effect that is compromised by using one-time password. Secondly typing password into untrusted computers suffer password theft treat. Several password stealing attacks like phishing, key loggers and malware. These problems can overcome by monitoring both web application and database. In existing system only precautions are handled for this type of attacks. In proposed system not only handles precautions but also counter measures. A user authentication protocol is designed to avoid end user attacks and monitoring process is designed for Denial of Service (DoS) and SQL Injection attack.**

Keywords- Domino effect, Phishing, Key loggers, Denial of Service attack, SQL Injection attack.

I. INTRODUCTION

Internet usage is widely spread all over the word for all type of usages like social network, banking etc. For user's authentication purpose we make use of text password. When people enter inside any of the websites they make use of this user name and password for registration. Password based user authentication can resist brute force attacks. The main problem with this password is user may not be able to remember the password so they use ease-to-remember password that is hazardous. So people reuse the password for different website [1]. Password reuse may cause domino effect [2]. Due to this password reuse the user may lose some of the sensitive information and if the hacker finds out the password of one then he can find out all other sites too [3].

In spite of password reuse attacks we must know the effects of password stealing effect. If the hacker hacks the password that may lead to malicious attacks, collect sensitive information and perform unauthorized payment actions [4]-[7]. Phishing is one of the most common passwords stealing attack. According to the report of phishing, the number of unique phishing websites detected at the second 6 months of 2010 is 97, 388. In the first 6 months of 2011 is 1, 22,472 [8]. Many previous studies have proposed systems to defend against the password stealing attacks. As a result the number of successful phishing attacks has been continuously increasing and many anti-phishing techniques have been proposed. Over the period of three weeks, we automatically test the effectiveness of blacklists maintained by Google and Microsoft with 10,000 phishing URLs. By analyzing a large number of phishing pages we explore the existence of page properties that can be used to identify phishing pages.

Phishing is considered as one of the serious threats for the internet and e-commerce. They abuse trust with the help of malwares, deceptive e-mails and fraudulent websites. To overcome this type of phishing attack we make use of one-time password.

Three-factor authentication is based on password, number of tokens sent and biometrics. To overcome this type of authentication the user must input the password and provide the pass code generated by the tokens. This type of authentication is relatively high cost [9]. So we make use of two-factor authentication.

Two-factor authentication is more attractive and practical. So many banks support this authentication. Even in two-factor authentication, it suffers from negative influence of human factor such as password reuse attack. In banks user have to remember only four-digit pin number. In this paper, we propose leverage with user's cellphone and short message service (SMS) to avoid password stealing and password reuse attack.

Key Logger is another type of web attack, direct client attack. When user enters in any untrusted computer the hacker can gather the sensitive information from the user. In the proposed system, when user able to log into web services without password so the hacker can't find the user's password [20].

Another type of web services attack is database server attack also called as SQL Injection attack [10]. Hacker tries to corrupt the back-end database system. This type of multi-tier web services can be determined by Intrusion Detection System (IDS). In multi-tier architecture, the back-end database server is protected behind the firewall while the webservers are remotely accessible over the internet.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

II. RELATED WORKS

The work described in this paper is related to different previous research results in the intrusion detection field. First of all, there is a corpus of work on detecting intrusions using anomaly detection techniques However, there are several proposed anomaly detection approaches that are more closely related to the solution proposed here. First of all, there is the previous work from our group on performing anomaly detection of web-based attacks by analysing the requests and replies exchanged between clients and servers [13, 14]. This previous work introduced the idea of using statistical models to characterize the normal values of the parameters of web requests

More precisely, the analysis of requests and replies does not allow for the identification of attacks that subvert the intended, normal workflow of a web application. Another set of results that this work is related to is in the contextualization of intrusion detection, that is, the use of detection models that take into account the different phases in which an application might be when an attack is executed.

A number of previous researchers have proposed to protect user credentials from phishing attacks in user authentication. The proposed systems leverage variable technologies, for example, mobile devices, trusted platform module (TPM), or public key infrastructure (PKI). However, these solutions were short of considering the negative influence of human factors, such as password reuse and weak password problems. To prevent compromising user credentials, [18] proposed an authentication protocol depending on a trusted proxy and user mobile devices. Secure login is authenticated by a token on untrusted computers, to thwart phishing sites, a random session name is sent by SMS from the proxy to the mobile device.

The attackers can bypass the webserver to directly attack the database server. We assume that the attacks can neither be detected nor prevented by the current webserver IDS, that attacker may take over the webserver after the attack, and that afterward they can obtain full control of the webserver to launch subsequent attacks. For example, the attackers could modify the application logic of the web applications, eavesdrop or hijack other users' web requests, or intercept and modify the database queries to steal sensitive data beyond their privileges.

On the other hand, at the database end, we assume that the database server will not be completely taken over by the attackers. Attackers may strike the database server through the webserver or, more directly, by submitting SQL queries, they may obtain and pollute sensitive data within the database. These assumptions are reasonable since, in most cases, the database server is not exposed to the public and is therefore difficult for attackers to completely take over. We assume no prior knowledge of the source code or the application logic of web services deployed on the webserver. In addition, we are analysing only network traffic that reaches the webserver and database. We assume that no attack would occur during the training phase and model building.

CLAMP [16] is an architecture for preventing data leaks even in the presence of attacks. By isolating code at the webserver layer and data at the database layer by users, CLAMP guarantees that a user's sensitive data can only be accessed by code running on behalf of different users. In contrast, Web Guard focuses on modelling the mapping patterns between HTTP requests and DB queries to detect malicious user sessions. There are additional differences between these two in terms of requirements and focus. CLAMP requires modification to the existing application code, and the Query Restrictor works as a proxy to mediate all database access requests. Moreover, resource requirements and overhead differ in order of magnitude: Web Guard uses process isolation whereas CLAMP requires platform virtualization, and CLAMP provides more coarse-grained isolation than Web Guard. However, Web Guard would be ineffective at detecting attacks if it were to use the coarse-grained isolation as used in CLAMP. Building the mapping model in WebGuard would require a large number of isolated web stack instances so that mapping patterns would appear across different session instances.

III. WEB ATTACKS AND ARCHITECTURE

We initially set up threat models to include our assumptions and type of attacks that we are aiming to protect. In this section we consider various methods of password stealing. We introduce oPass system and Double Guard system and make some assumptions.

A. Problem Definition

People trust heavily on the internet to work with all the network related activities. It has increased in both popularity and complexity over the past few years. A web service facilitates and enriches several applications like banking, social network etc. Such services employ a webserver front-end that runs the application and back-end server that consists of database or file-server. Text password is one of the user authentication used for website registration everywhere. But text password creates several critical disadvantages.

Many problems occur in web application one of the critical problem we face is password stealing and password reuse. The attackers are network abided and come from the web clients. The attackers can bypass the webserver to directly attack the database server. First, user creates their password for ease-of-use that leads to password stealing and password reuse. Second, humans can't memorize complex or long password. To overcome this type of problems we propose user authentication called oPass to protect from password stealing. In oPass leverage we make use of one-time password that s sent as an short message service to user's mobile phone. Once the user finishes the current session one-time password expires.

On the other side at the database end, we assume that the database server will not be completely taken over by the attackers. Attackers may strike the database server by submitting SQL queries and affect the sensitive data in the database. We analyze the network traffic that reaches the webserver and the database through the Double Guard system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

B. *Phishing and Keylogger attack*

Phishing is an electronic online identity theft in which the attackers use the combination of social engineering and spoofing techniques to trick a user into revealing confidential information. This information is typically used to make an illegal economic profit. So phishing attacks are remarkably effective for attackers. As a result, the numbers

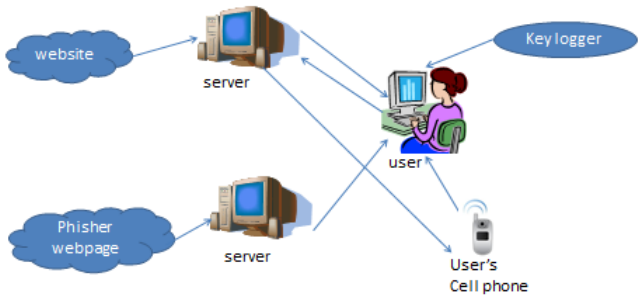

Figure 1. Architecture of phishing and Keylogger attack

of successful phishing attacks have been continuously increasing and many anti-phishing solutions have been proposed. Keylogger and phishing attacks can extract user identity and sensitive information for unauthorized access. To overcome this type of problem we propose security issue called oPass leverage. The main goal of this oPass leverage is to send the one-time password as short message service to user's mobile to avoid password stealing. This one-time password expires after the user completes his work. The long-term password is used to protect the information in user's mobile.

C. *SQL Injection Attack*

An SQL Injection attack consists of insertion or injection of SQL query through the input data from the client into the application. A successful SQL injection exploit can read sensitive data from the database, modify the database data, execute administration operation and recover the content.

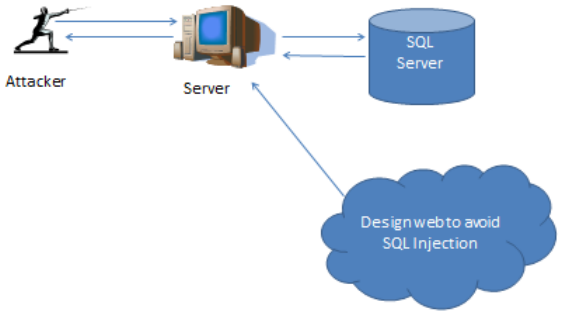

Figure 2. Architecture of SQL Injection attack

D. *Dos Attack*

In the Denial of Service (Dos) attack the numbers of users are accessing, the server slows down the rate of processing. When the number of packets is received from a particular IP address exceeds the limit then the packets are terminating the client. An attacker usually takes over the webserver and therefore hijacks all subsequent legitimate user sessions to launch attacks. For instance, by hijacking other user sessions, the attacker can eavesdrop, send spoofed replies, and/or drop user requests.

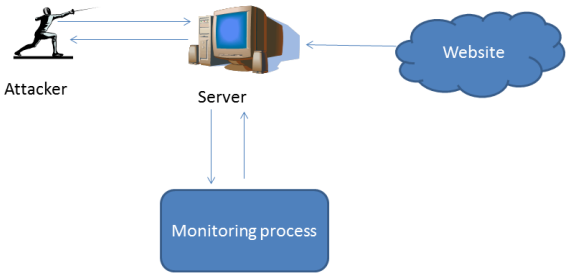

Figure 3. Architecture of DoS Attack

IV. SECURITY ANALYSIS

Although web application attacks have existed over past 10 years like simple coding error, failed input validation and output sanitization continue to exist in web application. Most prevalent web application attacks like SQL injection attack, Dos attack, phishing, key logger attack and so on.

There are multiple ways to detect and prevent these vulnerabilities from being exploited. Some of the prevention measures are analyzed and described.

A. *Phishing and Keylogger Attack Security*

Phishing attack is done by creating fake website and stealing the password and attacking the end user. First, user creates password by them and uses the same password for different websites that causes domino effect.

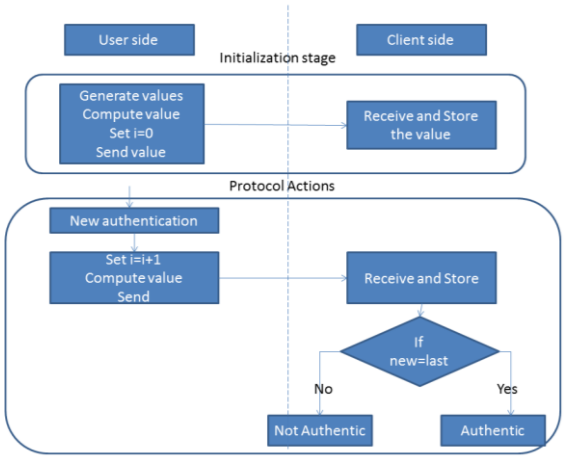

Figure 4: One- Time password Generation

Secondly, humans have difficulty in remembering the complex password more than 3% yahoo users forget their password based on the study [11].

To overcome this type of problems, we propose a technique called one-time password. In this technique password information is no longer important it expires when the user completes the current session. We use the short message service and users mobile phone to avoid password stealing attacks. Based on the user's identity this one-time password is generated. If there is any request from the fake website one-time password is not generated,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

password is generated only for the request from the original website. The user's mobile is protected using security lock. But if the user loses the mobile phone it can be notified to telecommunication service provider (TSP) to disable the lost SIM and apply for the new SIM with the same mobile number. Then the user can perform the recovery phase using a new mobile phone.

One-Time password consists of registration phase, login phase and recovery phase. In the existing system SHA-256 algorithm is used, since it has many web vulnerabilities in the proposed system we make use of MD5 algorithm to avoid these vulnerabilities.

B. SQL Injection Attack security

The SQL Injection attack consists of insertion of SQL queries through the input data from the client to the application. SQL Injection exploit can read sensitive data from the database, modify database data execute administration operations on the database recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

SQL Injection attacks are a type of injection attack, in which SQL commands are injected into data input in order to effect the execution of predefined SQL commands. SQL Injections to work, the attacker has to jump out of the original SQL statement. This is usually done by the single quote (') or the double dash (--). The single quote acts as a delimiter for an SQL query; the double dash is the comment character in Oracle and MS SQL.

SQL injection is possible even without the singlequote [12]. Let us take thisexample SQL statement:

select value1, numeric_value2 from table1 where numeric_value2=**user_input**

Here, an attacker may execute an additional SQL query, by supplying an input like:

7; select * from users

A SQL injection attack can allow a malicious user to execute arbitrary queries on the database server. As a result, the attacker can steal sensitive information and/or modify the information stored in the database tables.For example, a typical web application where the authentication module compares the user provided credentials with the known accounts contained in the database. The username provided by the user is used to compose the query, without any checks on its contents:

"SELECT * FROM users WHERE name = '" + userName + "';"

Since the username is not sanitized, it can be crafted by the attacker so that arbitrary SQL code is injected into the query.

So to make the back-end database more secured, we have proposed a solution to the problem to overcome the attackers. If any attacker tries to inject SQL queries and hack the server an alert is generated for illegal queries.

C. Denial of Service Attack Security

Denial of Service (DoS) attack not only diminishes the network capacity but also affects the reliability of information being transmitted. Denial of Service attack where, attacker tries to disrupt, denies, degrade or destroy information resident in nodes memory. There are various kinds of denial of service attacks which are planned in different manner and decreases network lifetime in different ways.

In this scheme power of hash functions is used to secure the communication link between the chaining nodes for communication purpose. The technique works well when number of nodes is less but performance of techniques degrades as number of nodes increases. With increase in number of nodes memory required to store hash value corresponding to each node also increases. Another setback of this technique is that it cannot handle wide range of DoS attacks.

To overcome this type of attack first we check for the format of the IP address and then the length if it matches then we processes the steps. When the number of packets is received from the particular address more than the maximum limit then that particular IP address is terminated. This type of attack is also called as the counter attack.

V CONCLUSION

Web applications have become a common way to access information and services. These applications are vulnerable to a number of attacks that cannot always be detected by observing the application from the outside. This paper presented Web Guard an approach to the detection of attacks against web applications, based on the analysis of the internal application state. The approach is the first that models the values of session variables in association with critical execution points in a web application. In addition, we introduced a novel detection model that relies on multi-variable invariants to detect web-based attacks. We presented an intrusion detection system that builds models of normal behaviour for multitier web applications from both front-end web (HTTP) requests and back-end database (SQL) queries. Unlike previous approaches that correlated or summarized alerts generated by independent IDSs, Web Guard forms container-based IDS with multiple input streams to produce alerts. We have shown that such correlation of input streams provides a better characterization of the system for anomaly detection because the intrusion sensor has a more precise normality model that detects a wider range of threats. When we deployed our prototype on a system that employed dot net as web application, and a MySQL back end, Web Guard was able to identify a wide range of attacks with minimal false positives. As expected, the number of false positives depended on the size and coverage of the training sessions we used. Finally, for dynamic web applications, we reduced the false positives to 2percent.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 04, April-2016

VI REFERENCE

[1] B. Ives, K. R. Walsh and H. Schneider, "The Domino effect of password reuse," ACM , vol. 47, no. 4, pp. 75 -78, 2004.

[2] S. Gaw and E. W. Felten, " Password management strategies for online accounts," in SOUPS '06: Proc. 2nd Symp. Security, New York, 2006, pp. 44-55, ACM.

[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM.

[4] R. Dhamija, J. D. Tygar, andM. Hearst, "Why phishing works," in *CHI'06: Proc. SIGCHI Conf. Human Factors Computing Systems*, NewYork, 2006, pp. 581–590, ACM.

[5] C.Karlof,U. Shankar, J. D.Tygar, andD.Wagner, "Dynamic pharmingattacks and locked same-origin policies for web browsers," in *CCS '07:Proc. 14th ACMConf. computer Communications Security*, NewYork,2007, pp. 58–71, ACM.

[6] T. Holz, M. Engelberth, and F. Freiling, "Learning more about the undergroundeconomy:Acase-study of keyloggers and dropzones," *Proc.Computer Security ESORICS 2009*, pp. 1–18, 2010.

[7] N. Provos, D. Mcnamee, P. Mavrommatis, K. Wang, and N.Modadugu, "The ghost in the browser: Analysis of web-basedmalware," in *Proc. 1st Conf. Workshop Hot Topics in UnderstandingBotnets*, Berkeley, CA, 2007.

[8] Phishing Activity Trends Rep.,2nd Quarter/2010 Anti-PhishingWorking Group [Online]. Available: http://www.antiphishing.org/

[9] L. O'Gorman, "Comparing passwords, tokens, and biometrics for userauthentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[10] C. Anley, "Advanced Sql Injection in Sql Server Applications,"technical report, Next Generation Security Software,Ltd., 2002.

[11] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell,"Stronger password authentication using browser xtensions," in *SSYM'05: Proc. 14th Conf. USENIX security Symp.*, Berkeley, CA, 2005, pp. 2–2, USENIX Association.

[12] Anley, C. (2002). Advanced SQL Injection In SQL Server Applications.http://www.nextgenss.com/papers/advanced_sql_injection.pdf

[13] Kruegel, C., Vigna, G.: Anomaly Detection of Web-based Attacks. In: Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS '03),Washington, DC, ACM Press (October 2003) 251–261

[14] Kruegel, C., Vigna, G., Robertson, W.: A Multi-model Approach to the Detection of Web-based Attacks. Computer Networks 48(5) (August 2005) 717–738

[15] M.Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in *DIMACS Workshop Usable Privacy Security Software*, Citeseer, 2004.

[16] B. Parno, J.M. McCune, D. Wendlandt, D.G. Andersen, and A.Perrig, "CLAMP: Practical Prevention of Large-Scale Data Leaks,"Proc. IEEE Symp. Security and Privacy, 2009.

[17] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for securely managing passwords," in *WWW '05: Proc. 14th Int. Conf. World Wide Web*, New York, 2005, pp. 471–479, ACM.

[18] K.-P. Yee and K. Sitaker, "Passpet: Convenient password management and phishing protection," in *SOUPS '06: Proc. 2nd Symp. Usable Privacy Security*, New York, 2006, pp. 32–43, ACM.

[19] T. Verwoerd and R. Hunt, "Intrusion Detection Techniques and Approaches," Computer Comm., vol. 25, no. 15, pp. 1356-1365, 2002.

[20] G. Vigna, W.K. Robertson, V. Kher, and R.A. Kemmerer, "A Stateful Intrusion Detection System for World-Wide Web Servers," Proc. Ann. Computer Security Applications Conf. (ACSAC '03), 2003.

[21] G. Vigna, F. Valeur, D. Balzarotti, W.K. Robertson, C. Kruegel, andE. Kirda, "Reducing Errors in the Anomaly-Based Detection ofWeb-Based Attacks through the Combined Analysis of WebRequests and SQL Queries," J. Computer Security, vol. 17, no. 3,pp. 305-329, 2009.

[22] Mutz, D., Valeur, F., Kruegel, C., Vigna, G.: Anomalous System Call Detection. ACM Transactions on Information and System Security 9(1) (February 2006) 61–93