Research Journal of Applied Sciences, Engineering and Technology 4(18): 3209-3214, 2012
ISSN: 2040-7467

Submitted: December 23, 2011 Accepted: January 21, 2012 Published: September 15, 2012

Web Prior Architecture to Avoid Threats and Enhance Intrusion Response System

K.S. Ravichandran, R. Baby Akila and T. Durga Laxmi
School of Computing, SASTRA University, Thanjavur-613401, India

Abstract: Web is hierarchically composed of entities such as domains, Web sites and documents distributed over Web sites and linked together by hyperlinks. The response component of the intrusion detection system issues the response to the jarring requests. In this paper, the intension is to allow the legitimate user to access the target website and perform the selective operations on the database to avoid threats and protect the database from unauthorized users. The designed Web Prior Architecture (WPA) permits the legal client to obtain the privilege license by clicking on an authority link provided by the referrer. Using this license, the client can get the liberty to perform the operations on the target website. In that website, database can be accessed by the client with the selective permissions. These can be performed by the two methods, namely strategy toning and strategy management. By this way, the database is accessed in a highly securable manner. The massive scale of this study specifies the method to avoid the threats from the unauthorized users and augment the intrusion response system. This will protect the target website and its database from the unconstitutional users. Our pragmatic study demonstrates that Web Prior Architecture enables the legitimate user to connect to the target website and perform selective database operations.

Keywords: Database, intrusion detection, privilege license, strategies, web prior architecture

INTRODUCTION

In recent days, most of the users are familiar with online networking and perform all their day to day activities (Online shopping, Bank transactions, Ticket booking etc.,) via internet. The Internet owes much of its historic success and growth to its openness to new applications. A key design feature of the Internet is that any application can send anything to anyone at any time, without needing to obtain advance permission from network administrators. New applications can be designed, implemented and come into widespread use much more quickly. Usage of internet has both merits and demerits. Users can perform activities in the website with authority provided by that website. Some unauthorized users may behave like authorized users and try to attack the website and its database. This leads to a problem of creating threats and make the web sites in securable. To avoid this problem, permit the users with some license. First the users send the request to the referrer like negotiator. Then the negotiator generates authority link to the user and then it is able to access the target website.

Most often Database accumulates information and data about the organizational systems. In this study, database is used to store the user details, log files and website details. After getting license to access the target website, users can also access its database. All operations like creation, insertion, modification, selection etc can be achieved in the database. While performing these operations, it may be a chance for the database to get corruption. Database administrator validates the users by generating DBID for every user and assigns the role for them. Then the user is able to perform the assigned operations with restrictions. Various nations of world follow regulations concerning data management such as SOX, PCI, GLBA, HIPAA and so forth.

Threats may come from many different sources such as e-mail, web sites and programs. In fact, most on-line activities and some offline ones expose computer to the threat of virus infection. There are, however, some basic precautions that can be taken to protect the computer. The first rule of internet safety is to trust the source. Files, documents, web sites or any other link should only be clicked, when the person is trusted who has given a request. Another way to keep safe is to avoid downloading files that do not come from a well-known company. In this study, we certify both the website and database to circumvent the threats and augment the intrusion response system. It makes the system more authenticated with high performance. For the past days, only either on the database or on the website is concentrated.

The proposed pragmatic study shows that Web Prior Architecture (WPA) enables the users to thwart very intensive flooding threats against a website and protect the database from anomalous requests in reasonable

Corresponding Author: K.S. Ravichandran, School of Computing, SASTRA University, Thanjavur-613401, India, Tel.: +91-4362-264105 Ext.175; Fax: +91-4362-264120

behavior. The main objective is to protect website by generating authority link and privileged license. Anomalous requests may distort database. To avoid these requests, various types of schemes such as strategy toning and strategy management are used. These schemes will protect the database from prohibited operations. Efficient defense against threats and intrusion is well known to be a challenging task because of the difficulty in eliminating the vulnerabilities introduced during the design and implementation of different network components and database which can be probably utilized by the opponent.

LITERATURE REVIEW

Last decade, in order to avoid threats, various actions have been anticipated. In particular, the three approaches such as overlay based approaches, capability based approaches and WRAPS are considered. Overlay networks have been applied to proactively defend against Denial of Service (DoS) attacks. Keromytis *et al.* (2002) propose a "Secure overlay Services" (SoS) architecture, which has been generalized (Anderson *et al*., 2003) to take into account different filtering techniques and overlay routing mechanisms.

A different style of approach to combating Threats focuses on trying to detect a threat in progress and then respond to the specific attack. Threats have been a real problem for less than three years and not much published work exists on the subject. Identification of different abstractions for the Web graph depends on the granularity (Wu *et al*., 2004). The feasibility of deploying explicit authorization in the Internet cleanly addresses DoS. It is more broadly an attempt to define the structures needed for any large network to be DoS-resistant (Anderson *et al*., 2003). Recently researchers have studied capability-based approaches that authorize a legitimate client to establish a privileged communication channel with a server using a secret token (capability). An approach utilizes a client's secret path ID as its capability for establishing a privileged channel with a receiver (Yaar *et al*., 2004). DoS-limiting Internet architecture improves SIFF (Yang *et al*., 2005). Implementation of end-to-end user agreement (Gligor, 2004) to protect connections against flooding attacks on the TCP layer. A system engineered to address the various security and performance considerations (Xu and Lee, 2003).

Similar to these approaches, WRAPS uses capability tokens to identify good traffic (Xiao and Michael, 2010). However, WPA focuses on important challenges that have not been addressed previously. In the intrusion response system, equality predicates have been used for policy matching algorithm in the previous study. The policy matching algorithms take into account arbitrary predicates while the scheme in (Kamra *et al*., 2008) only considers equality predicates. The concepts of fine-grained response actions such as suspend and taint has been introduced (Kamra and Bertino, 2009). The design and implementation of an access control model that is capable of supporting such fine-grained response actions (Kamra and Bertino, 2009). Some strategies thus forced organizations to reevaluate security for their internal databases (Natan, 2005). Matching algorithms apply a global optimization strategy to exploit predicate redundancy and predicate dependencies among subscriptions to reduce the number of predicate evaluations (Pereira *et al*., 2000).

Another approach toward addressing the problem of insider threats from malicious DBAs is to apply the principle of least privilege. Such approach is followed by (Oracle Database, 2009) using the concept of a protected schema for the administration of the database vault policies. Many algorithms for content-based event matching are described (Pereira *et al*., 2000). Database response policies to support intrusion response system (Ashish and Elisa, 2011). In this study, the proposed system addresses both website and database to make a system more reliable. The main goal is evade threats, guard database and improve intrusion response system. WPA provides greater advantages compared to previous methods and schemes. It is helpful for the server by generating license and DBID for every user. Log files, Blacklist and whitelist are also maintained that reduce the time for validating clients.

FRAMEWORK

Internet is accessed through URL (uniform resource locator). A URL is a string of characters that indicate the address of a specific website or file on the internet. URL contains http path, application and parameters. Like this URL, in a Web Prior Architecture (WPA) privileged license has been generated for the users to access the target website. Privileged license [pl] is embedded with token that contains IP [IP], name [N], class [CL] and referrer ID. Referrer ID [RID] indicates which users are permitted by which referrer.

Intrusion is an illegal entry upon or appropriation of the property of another. It includes anomaly detection and anomaly response. To prevent this intrusion various strategies stored in the system catalogue are used. Strategies are used for governing database in a secure aspect. Strategy toning and strategy management are two main strategies to protect the database. Strategy toning detects the outlier requests by matching complete requests with role consigned with it. Similarly, Strategy management is accountable for taking trials once a deviation is detected. The technique is also illustrated in Fig. 1:

In Web Prior Architecture (WPA), the website allows the client by assigning a secret license with

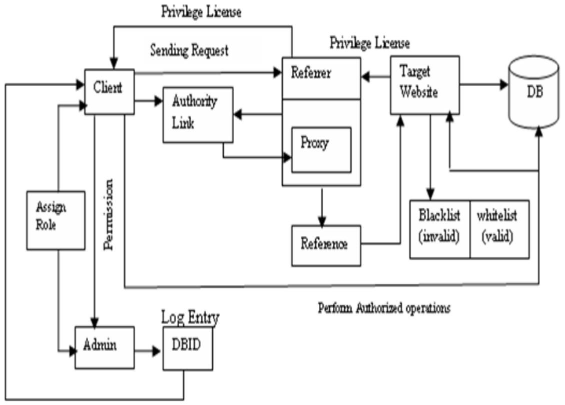

Fig. 1: Web prior architecture

some token. The token includes key bit, priority field and authentication code. Using that license, client establishes the authenticated route with target website even in the presence of threats. Client can access the target website either directly or indirectly through the privilege license. Digital signature format is described as follows:

$C \rightarrow R : M[IP_k||N_k||CL_k]$
$R \rightarrow C : E_{kc}[al_k||RID_k]$
$T \rightarrow R : E_{kr}[pl_k||DID_k]$
$R \rightarrow C : E_{kr}[M]$

The website [T] offers a privilege license to clients [C] trusted by the referrer [R] or is otherwise qualified by the site policies. The qualified client will be able to access target website. This protection scheme protects the website from unauthorized clients and differentiates the privileged and unprivileged clients. The privileged client can also be able to access its target website database with restrictions. The privileged client obtains DBID [DID] from the database administrator and it assigns role to every client. DBIDs are updated in log entry maintained by the administrator. The client is only able to perform the selective operations assigned by administrator. If it tries to misuse, then the administrator generates alert to client by sending the warning message. The client may be blocked by administrator if it abuses the database continuously.

METHODOLOGY

The Internet is an extremely complex system and it is able to make accurate measurements in order to understand its underlying behavior or to detect improper behavior (e.g., attacks). Threats work by flooding some limited resource on the Internet, thereby preventing legitimate users from accessing that resource. Targets include the bandwidth of access links and other network bottlenecks and also the computing and memory resources on servers, clients, routers and firewalls.

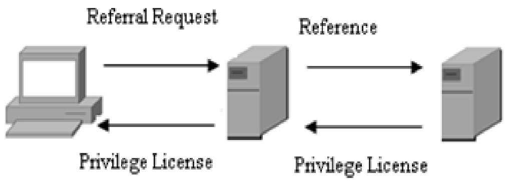

Fig. 2: Accessing target website

Generating authority link: The clients want to access the target website to satisfy their needs by utilizing the services of website. To provide security for website, client must be authenticated. Therefore, Client does not directly access the target website. This concept is described in Fig. 2 First it sends the request to the referrer; the request includes the details of client and its characteristics. Referrer acts like a mediator to validate the client and helps to access the target website. After receiving a request from a client, the referrer verifies all the details. If referrer confirmed that particular client as a qualified client, it generates the authority link [al]. Otherwise, client is deemed to be an unqualified client and its request is aborted. Authority link is unique and fictitious because it does not directly deal with web services.

Establishing authenticated route: Whenever a client wants to access target website, first it gets the permission from referrer by applying a request. The client can be able to send the request to only one referrer. If it tries to send the same request to another referrer, that client's request will not be validated.. This is also one type of threat induced by the adversaries. Referrer accepts client by generating Referrer ID for qualified clients. If the client request is accepted by anyone referrer, the referrers will not validate the same client. Therefore client will be referred by only one referrer. The referrers list is already available in the target website. A client attempts to send request to the referrer and that referrer is not present in the target website list and then the client will be blocked by the target website. In Web Prior Architecture (WPA), the authenticated route will be established between one client and one referrer. No one too many routing path is present between client and referrer. The referrer has all the autonomy to accept or reject clients request according to the client reference. Digital signature format for establishing route is described as follows:

$C_i \rightarrow R_i: M[IP_k||N_k||CL_k]$
$R_i \rightarrow C_i : E_{kci}[al_k||RID_k]$
$C_i \rightarrow R_j: M[IP_k||N_k||CL_k]$
$R_j \rightarrow C_i : M[D_i]$

The client may send more than one request to the same referrer. Referrer processes the request and makes a decision whether accept or reject the client. If it accept means first request only will be accepted and other same requests gets cancelled. This procedure is also same for rejection process. Once the client is accepted, the referrer generates an authority link. It is not a real target website address and it is an imaginary one. The proxy script in the referrer site is running by the client clicking on authority link. This will send complete reference of the client to the target website. The indication for the acceptance of client is authority link provided by referrer.

Creating blacklist and whitelist: In Web Prior Architecture (WPA), every client is validated to reach the target website with the help of referrer. Once the client is validated, again it must be verified by the target website to perform operations on it. Before allowing the client to do the operation, its details (IP, class name) must be updated in the whitelist. It is possible that the privileged client may misbehave in target website. At that time the privileged client license is blocked and reference details are updated in the blacklist. The misbehaving privileged client may attempt recurrently to access the target website. The target website checks its blacklist and whitelist, whether the client details are in which list. In case of whitelist, client is permitted to perform the operations on the website. Otherwise it is completely blocked.

The user those who entered into the target website is validated through their provided details such as IP, class name and so on. Only the valid client enters into the site. Also, the log entry is maintained by the website for future use. The log entry contains the details about the entered client with the corresponding date and time. Blacklist and whitelist are used to control the traffic congestion problem by partitioning the traffic in to privileged and unprivileged flows. Through the privileged flow, authenticated legitimate client approach the target website. Unauthorized clients are prevented by passing them in the unprivileged path. These lists are very advantageous because of misbehaving privileged clients are blocked to avoid the insecure operations in the website.

Strategy toning: To evaluate the performance of database, allocate the role for every user. It is done by constructing the database access profiles of roles for users and such profiles are used for Anomaly Detection task. A client whose request does not match with DBID is qualified as anomalous. User profile can record information of different levels of details such as roles, users, time, source and so on. Thus, the role is assigned for each of the client which defines the access privileges on the database. This phenomenon is depicted in Fig. 3.

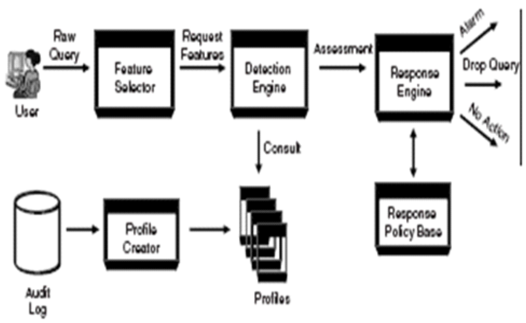

Fig. 3: Performing database operations

Web Prior Architecture (WPA) allows client to access the target website's database. The database contains all the information regarding clients, website and administrator. Database administrator generates the DBID for every client those who wants to access the database with this DBID selective operations specified. This will protect the database from the unauthorized user. The client will only do these specified operations. Any attempt except these selective operations leads a problem of intrusion.

The anomalous detection is done by monitoring each client request. Upon received the request from the client, the target website matches the strategy allocated for it. If the strategy matches client request, the request is transferred to the target website normally. Otherwise, it is treated as an Anomalous Request and it is handled by Intrusion Response System. The strategy toning is the process of detecting the anomalous request by matching each and every request with the stratagem assigned with it.

Strategy management: The Strategy management is responsible for taking some actions, once an anomaly is detected. Database contains plenty of profitable data about the target website. The anomalous request along with its type and the action taken to handle the anomalous requests are stored in the database for future reference. Database administrator has the liability to protect the database from the unauthorized user's activities. For every user, some set of Strategies and policies are assigned. Users may abuse the database by performing the unselective operation. To prevent this, administrator delivers the notification like alert message. Policy is described as:

$$A \rightarrow C : E_k[M[RA_k||DID_k||T]]$$
$$A \rightarrow C_m : M[ALM_k]$$
$$A \rightarrow C_{rm} : M[TRN_k]$$

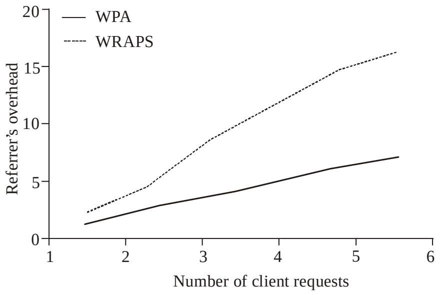

Fig. 4: Number of client requests versus refferr's overhead

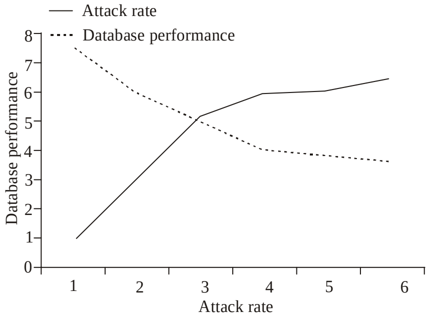

Fig. 5: Analysis of database performance

The unauthorized clients violate this notification and make an attempt repeatedly overwhelm database meanwhile administrator block that client by eliminating the entire license assigned to it. Using WPA, the client can ingress the website as well as it is database with this selective strategy enumerated by the administrator. While accessing the database again unauthorized client may acquire the authorization from the administrator by sending request and accomplish the scrupulous operations. This is the recovery procedure for unauthorized client to attain the authentication.

PERFORMANCE ANALYSIS

In this section, the empirical evaluation of WPA is proposed in a given experimental network by using simulation. The goal of the experimental evaluation is to measure the overhead incurred by clients' requests to referrer and accessing database.

Most important websites are interrelated by hyperlinks. We evaluate the performance of a referrer website when it is making referrals to a website under flooding attacks. In this study, we analyze the overhead of referrer due to repetition of client requests. If client continuously sends the request to the referrer, it will be overhead for the referrer. This overhead is present in all methods. In WRAPS, overhead is very high and it leads to a problem of congestion. But in WPA, this much overhead is reduced by generating Referrer ID. Compared to WRAPS, Overhead is very less in WPA. This is shown in Fig. 4.

Clients access the database with restrictions identified by the administrator. Client violates restrictions indicates that the database is hacked by intruder. In Fig. 5, we evaluate this as if intruder seems to access database; it reduces the performance of database. Incremental attack rate signifies poor performance of database.

The designed WPA architecture secures the website and database constructed with 5 nodes, out of which one acts as a server. We tested the actual data with the designed WPA architecture and also the simulated data sets. It is found that both the experimental and simulated results are almost the same with respect to prevention and response rate.

CONCLUSION

The vulnerability of public services to flooding attacks in the Internet will continue to grow as the gap between network line rates and server rates continues to increase. Whether this vulnerability materializes as a significant service threat depends on whether new Internet services (e.g., voice over IP) will provide sufficiently attractive economic targets for attacks. Threats yield a major problem in today's internet world. Analysis shows that such threats could be diminished and database is protected from intruder. To alleviate these threats, we propose architecture called Web Prior Architecture (WPA). WPA has been constructed upon the existing web sitegraph and WRAPS, elevating existing hyperlinks to privilege license and authenticated route. Users can access the database reliably by applying the schemes strategy toning and management. In this paper, target website and its database are maintained securable to avoid threats and improve intrusion response system.

REFERENCES

Anderson, T., T. Roscoe and D. Wetherall, 2003. Preventing Internet Denial-of-Service with Capabilities, Proceeding of Second Workshop Hot Topics in Networks (HotNets '03).

Ashish, K. and B. Elisa, 2011. Design and implementation of an intrusion response system for relational databases, 23(6): 875-888.

Gligor, V ., 2004. Guaranteeing Access in Spite of Service-Flooding Attack, Proceeding of Security Protocols Workshop (SPW '04), R. Hirschfeld, (Ed)., SpringerVerlag.

Kamra, A., E. Bertino and R.V. Nehme, 2008. Responding to Anomalous Database Requests. Secure Data Management, Springer, pp: 50-66.

Kamra, A. and E. Bertino, 2009 . Design and Implementation of SAACS: A State-Aware Access Control System. Proceeding of Ann. Computer Security Applications Conference (ACSAC).

Keromytis, A., V. Misra and D. Rubenstein, 2002. SOS: Secure Overlay Services, Proceeding of ACM SIGCOMM ’02.

Natan, R.B., 2005. Implementing Database Security and Auditing. Digital Press.

Oracle Database, 2009. Vault Administrator’s Guide 11g Release 1 (11.1). Reterived from: http://download.oracle.com/docs/cd/B28359-01/server.111/b31222/toc.htm, (Accessed on: Jan, 2009).

Pereira, J.A., F. Fabret, F. Llirbat and D. Shasha, 2000. efficient matching for web-based publish/subscribe systems, Proceeding of Int’l Conf. Cooperative Information Systems (CooplS). 162-173.

Wu, J. and K. Aberer, 2004. Using Siterank for p2p Web Retrieval. Technical Report IC/2004/31, Swiss Fed. Inst. Technology.

Xiao, F.W. and K.R. Michael, 2010. Using web-referral architectures to mitigate denial-of-service threats. IEEE T. Depend. Secure, 7(2): 203-216

Xu, J. and W. Lee, 2003. Sustaining availability of web services under severe denial of service attacks. IEEE Trans. Comput. Special Issue Reliable Distr. Syst., 52(2): 195-208.

Yaar, A., A. Perrig and D. Song, 2004. An Endhost Capability Mechanism to Mitigate DDoS Flooding Attacks, Proc. IEEE Symp. Security and Privacy (S&P ’04).

Yang, X., D. Wetherall and T. Anderson, 2005. A dos-limiting network architecture. Proceeding of ACM SIGCOMM, 05: 241-252.