Volume 3, Issue 9, September 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementing Multi-Attack Protecting Barrier Protocol in Intrinsic Network

D.Seethalakshmi,
Research Scholar,
Research & Development Centre,
Bharathiar University, Coimbatore,
India

Dr.R.Dhanapal
Professor & Head,
Department of Computer Application,
Eswari Engineering College, Affiliated to Anna University,
India

Abstract — Multi-tier architecture in web endures many attacks and several methodologies to overcome these attacks. Although abundant anti-attack system exists a single protocol to overcome multifarious attacks at a time is not available. When more than two anti-attack systems implemented it leads to performance degradation or encumbrance. Apart from system attacks there exists other menace that includes denial of service (dos), intrusion, session hijack, privilege escalation, and SQL injection attack. This paper establishes a protocol that proposes a new virtual lock and categorizes two levels of scrutiny. In primary level itself threshold checked to imminent attacks so the secondary in-depth level check done and invokes corresponding anti-attack application thus to eliminate performance degradation in multi-tier web services. Using this protocol we may upgrade the security and hikes the performance up to 88 percentages.

Keywords – Multi-tier, Denial of Service (dos), Intrusion, Session Hijack, Privilege Escalation, SQL Injection.

I. INTRODUCTION

Internet services and web applications becomes intricate as a part and parcel of our life, enabling communication and management of personal information from anywhere [1]. To pamper this increase need for applications and data complexity, web services have moved to a multi-tier design wherein the web server runs the application in front-end logic and the data outsourced to database or file server. There exists no built-in network security system to prevent malicious threats. Usual Network Control Systems (NCS) plays vital role in national critical infrastructures, such as nuclear reactor power plants, electric power distribution, transportation systems, and water and gas distribution [2]. There are concerns about the protection in NCS security. As an example, Internet-based NCS, real-time monitoring and control implementation, can easily accessible to large number of people on the internet. If the communication channel is not encrypted it increases vulnerability of the NCS to malicious attacks.

The data sharing and communication security is critical for the NCS to protect transmitted data from unauthorized access and modifications. Conventional NCS not designed with security protection features are vulnerable to various security attacks. Thus, there is a growing demand for efficient and scalable intrusion detection systems as the attacker's moves with different twists [3]. Even Experienced cyber analysts would not escape from these attacks. There are many convincing anti-Attack systems exists such as anti-Intrusion, anti-Trojan, anti-Phishing etc. But when there are two or more threats then there is no such system to scrutinize all the possible attacks. In this paper, we present PPP Protocol, a protocol that models the network behaviour of user sessions across both the front-end web server and the back-end database. By monitoring both web and subsequent database requests, we are able to eliminate attacks that an independent protocol would not be able to identify. Do not make the mistake of thinking that hackers simply attack systems.

Many different of attacks exist. We are preventing, predicting and protecting from these attacks through our protocol. Our protocol includes detection of dos, intrusion, session hijack, privilege escalation, direct db attack, SQL injection attack [6]. By provoking only the corresponding anti-attack system we can handle more number of attacks.

II. PROBABLE ATTACKS

More people deprive data from other users thus to conserve their resources such as important data, personal information, secured passwords etc. Hackers try to attack the systems in the network and intrude others personals through different ways. The possible types of attacks that we are going to prevent, predict and protect using our protocols are

A. Denial of Service (DoS) attack

Denial of service attack targets a server and exhausts its resources being available to the legitimate users. Some ways for DoS attacks are through consuming the computational resources, impeding configuration, overloading piles of process in cache so that it affects the communication between intended users and the targeted web service [10][11]. Thus they can no longer communicate with each other. Dos attack executes malware so that the processor will encumber with malicious coding which either forces the system to shut down or crash the entire system itself [19]. DoS attacks traditionally handled by routing through multiple servers or multiple cache memories so that even if one server is busy

the other can handle it [12]. Although attackers jam the system by providing congestion in data path through different IP addresses or through different source addresses.

B. Intrusion

Invading into victims system without their permission and controlling their system by performing their own actions is known as intrusion [7]. When such thing happens the intruder can extract information from the system possibly personal data. These kinds of attacks usually come through external commands which we allow inside our system without our knowledge and spare our valuable information [22]. The intruders may send commands to our system or by faking WebPages that acquire our information such as account number passwords etc.

The extraction of personal information through intrusion is traditionally handled by preventing phishy websites or by blocking the external commands which are suspected to intrude the system.

C. Session Hijack

By sending the tracking code to the system it exploits session key or cookie and gains unauthorized access to that system. This tracking code will track and send the users data through cookie [18]. Through this the cookie which has authenticated information for a user to use a remote server hijacked or looted by the intermediary computer so that it maintain sessions as if they were real user and hacks whatever they needed[13]. Session hijack is usually hacked through source routing or hacker using sniffing program in-between two systems to watch their entire conversation without the knowledge of them.

Techniques used like encrypting algorithms, using long random number or string as session key[21], by checking digital signatures for the trusted websites etc session hijack is prevented.

D. Privilege Escalation

The different users will be given different privileges or accessing databases corresponding to their levels. While users with fewer privileges performing unauthorized actions such as deleting or editing database information by invading directly to the database is known as privilege escalation [16]. Even when one user trying to access other user data's , Hacking passwords by guessing, faking or using random values and intruding others and if he can perform malicious activity then its a kind of privilege escalation or direct database attack.

To avoid privilege escalation fewer privileges given to the users and frequently monitors database activities. The users also aware of malicious web pages and do not give or store their personal information like passwords account numbers anywhere in their computers.

E. SQL Injection

It's a technique passes non-validated inputs or SQL sub-queries through web application and extracting the back-end database. Also by embedding vulnerable sub-queries inside the user provided parameters so that the attackers can execute arbitrary SQL queries or commands on backend database server [15]. Hackers inject sub-queries having hijacking codes instead of actual sub-query to be processed. Thus for eradicating SQL injection attack the sub queries monitored by checking their stored procedures.

Even though all these attacks have implemented their anti-attacking and protecting systems for eliminating network attacks there is no proposed model for handling more than one or two attacks. If such implementation done then the performance will be heavily degraded and affect its server [20]. This PPP Protocol provides scrutiny for primary level which establishes threshold for various attacks that are less time-consuming which invokes only the requisite secondary level. The PPP Protocol provides a technique that boosts the security to maximum performance approximately about 88 percent.

III. PRIMARY LEVEL SCRUTINY

In this paper we illustrate new virtual lock system which categorizes the security into two levels of analysis. The network attack handles various techniques which consumes much time when applied for every process. This PPP protocol eliminates the performance degradation problem in network security which is common when two or more attacks handled at a same time by implementing various techniques. Thus by splitting the scrutiny into two levels in which the primary level ascertains the traces for any type of above mentioned possible attacks through moderate thresholds. If the propounded threshold generated then the in-depth scrutiny for secondary level invoked. In addition to this the security enhanced by invoking all the anti-attack system when there are traces for cumbersome attacks and endures till needed. The primary level implements the threshold for different existing attacks by less time consuming techniques and enumerates the traces for attacks and indicates whether it needs secondary level check or not. In primary level the inspection done for attacks as below.

A. Denial of Service (DoS): This scrutinizes the network traffic for occurrence of congestion. If any encumbered service requests entangled then it asunder it to other cache [14]. If it persists longer then suspected to be malicious and scrutinized to secondary level.

B. Intrusion: External command or susceptible web pages linked checks for intrusion attacks along with their threshold perspective if any command susceptible to be intruded or any unperformed actions done in our system without our control then the secondary level check is performed.

C. Session Hijack: Examines the size of cookies in the session and checks the types of cookies vary within the session. If cookies or any session key is prone to threat then it scrutinizes to next level of in-depth checking for session hijack.

D. Privilege Escalation: Threshold for granted privileges in database and password awaiting database transactions checked. If any skeptic intensification of database occurs then it will be thoroughly checked for privilege permissions.

E. SQL Injection: Verifying the non-validated input data for keywords and the corresponding sub queries which invokes when non-validated input is given will be cross checked for malicious insertion of harmful query.

IV. IMPLEMENTING ULTIMATE SCRUTINY

The secondary level protocol examines more comprehensive techniques which establish thorough checked threshold for confirmation of the attack which happens. Then the anti-hacking system encountered for the corresponding attack and exists according to the factor of attack. This protocol assures the enhanced level of security system to the havoc by predicting; preventing and protecting the network controlled front-end system and back-end databases in the multi tier web services and elude the disruption of web services.

A. *Denial of Service (DoS):* In the secondary level of protocol checking this denial of service to the particular resources analysed. If the cache is brimming then it uses multiple caches to perform other actions. Even then all the cache overloaded it suspects but still there is a chance for false negative so it waits for two days which is our threshold level. If the congestion persists then it concludes that some other hacker is attacking our system and denying the services being served to other users thus anti denial of service attack will be invoked.

B. *Intrusion:* When a trace for intrusion conferred then the system detects whether it's a phishing website. If not then it thoroughly checks for external commands coding for codes specified for accessing the system's memory space other than provided. It ascertains whether any block of code is trying to access or saves in the system without user's permissions. If such things happen then it invokes anti phishing attack or anti intrusion to prevent and protect the system.

C. *Session Hijack:* When cookies size and the type suspected then the in-depth level verification of log file performed. The log file is checked for routing of the data from their source IP address and checks the pathway of data nodes till the destination IP address within time. If any interruption occurs in between then that suspected IP address checked for its genuineness. If any false factor obtained then that IP address invokes Anti -session hijack system and block that IP.

D. *Privilege Escalation:* When any suspicious accessing of data in database occurs then the secondary level invoked and performs three stages of checking which first finds out from which IP address the query is coming and checks for its authenticity. In second stage it acquires the information about the user and their levels of access to the database. Thus by knowing the authentication of user levels such as database administrator, programmer, developer etc and their accessibility such as who can view what from database, who can edit database, who controls password protected permissions over database accordingly it scrutinizes the genuineness of the user. Third stage scrutiny tries to detect the type of query and its intensity towards the database. Whether the query approached is a protected data or a subordinate data. Harmful query can be detected by observing the nature of access done by the user like whether they are escalating and corrupting data in main database or editing and modifying the sensitive information. The escalation of database done by taking backup of database thus it needs to check whether any uploads of sensitive information is taking place or not. Hence when privilege escalation proved strongly then Anti attacking system will be evoked.

E. *SQL Injection:* The execution of stored procedures checked whether it is executing already stored block of coding else trying to insert any new query inside already stored procedure. If so then what level of access the sub query had with the database functionality. It Examine the level of user and their permissions to access the phase of database. Performs query level checking if in case it is interlinking to any other harmful links. It checks with predefined data for the present queries so as to find the data is harmful or acceptable. When any query linked from other addresses it checks for last modifications done and its authorization level. The sub query sent by the external stored procedure interrogated for its presence in heuristics also performs cross checking by sending to database administrator.

V. PERFORMANCE AND RESULT ANALYSIS

In order to obtain the results for execution of primary level check and secondary level ultimate scrutiny a web connected simulation is developed for checking the performance of anti attacking system. As described in this paper first a model for connected network is developed. Then the data sent and received is monitored by performing the primary level scrutiny. This monitors the transactions and scrutinizes the threshold level. Once it reaches the specified threshold level the ultimate scrutiny for the particular attack is invoked. If any congestion for resources occurred then the second level scrutiny for checking the source ip address will be checked and the time the system encumbered will be monitored accordingly it decides whether to activate the anti-Denial of Service system or not, also how long it needs to be activated.

Likewise all the other attacks checked and their scrutinizing levels will be executed. The final analysis from other anti-attacks with this PPP protocol is distinguished by this simulation. When any one attack is predicted and protected then for the particular instance of time the performance will be higher. In case of checking more than two attacking systems the performance curtailed to lowest level thus it leads to system crash or overload.

This performance level for the individual protocol can be described with below graphical representation

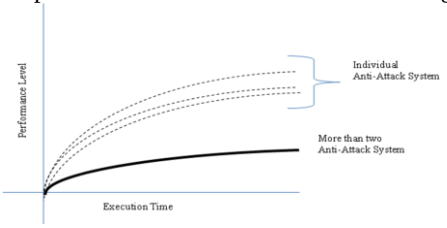

Fig. 1 Dotted Lines represents individual anti-attack system. Solid line denotes concurrent application of more than one attack.

In the above Fig. 1 the dotted lines represents the individual anti attacking systems such as anti-intrusion, anti-privilege escalation, Anti-denial of service attack. This shows high performance level when applied individually. The stronger line represents a combination of anti-attacks which has decreased level of performance when they all applied together. This protocol shows the level of performance for primary level is higher similar to individual protocol checking. Then the invoked secondary level check and its performance will slightly lesser than primary level but the stronger protection will have high performance than any other anti hacking system. Henceforth the next graph shows how the primary level and secondary level check will be analysed.

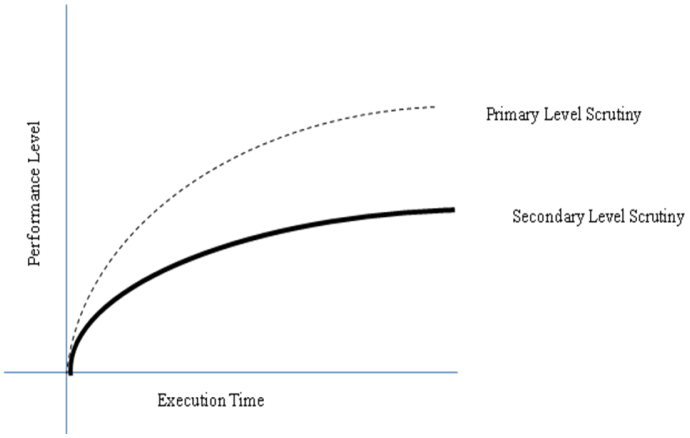

Fig. 2 Dotted lines represents primary level checking. Solid line represents secondary level check.

In this above Figure 2 the dotted line represents the primary level check which has high performance level more than some individual protocols. In case of secondary level scrutiny which is represented by stronger line determines high performance of the PPP protocol than. As a result for any multi-tier web services whatever profuse attacks occurs it will be predicted by primary level scrutiny by faster checks, then prevented by secondary level as such when the control transfers to secondary level the scheduled job will be stumbled. Then accordingly the invoked anti-attack system by the secondary level check will protect the system from being hacked.

VI. CONCLUSIONS

The implemented PPP protocol in this paper evaluates the imminent possible attacks by performing feeble checks in primary level. Only in case of suspected prediction of attacks the next in depth level will be scrutinized so that any imminent attacks will be prevented and protected. After simulation the performance within anticipated time will be higher for implementing these entire anti attacking system than any other anti hacking system is demonstrated. When the existing anti attack techniques for more than two types overload or crash the system our proposed protocol evaluates all the possible attacks and protect our information within the stipulated time.

REFERENCES

[1] SANS, "*The Top Cyber Security Risks*," http://www.sans.org/top-cyber-security-risks/, 2011.
[2] National Vulnerability Database, "*Vulnerability Summary for CVE-2010-4332*," http://web.nvd.nist.gov/view/vuln/detail? vulnId= CVE-2010-4332, 2011.
[3] "*A Policy Enforcing Mechanism for Trusted Ad Hoc Networks*" .Gang Xu, Member, IEEE, Cristian Borcea, Member, IEEE, and Liviu Iftode, Senior Member, IEEE
[4] *Autobench*, http://www.xenoclast.org/autobench/, 2011.
[5] "*Common Vulnerabilities and Exposures*," http://www.cve. mitre. org/, 2011.
[6] "*Five Common Web Application Vulnerabilities*," http://www. symantec.com/connect/articles/five-common-web-applicationvulnerabilities, 2011.
[7] A. Ghosh, A. Schwartzbard, and M. Schatz, "*Learning Program Behavior Profiles for Intrusion Detection*," Proc. First USENIX Workshop Intrusion Detection and Network Monitoring, pp. 51-62, Apr. 1999.
[8] J.B.D. Cabrera, L. Lewis, and R.K. Mehra, "*Detection and Classification of Intrusions and Faults Using Sequences of System Calls*," SIGMOD Record, vol. 30, no. 4, pp. 25-34, 2001.
[9] "*Anomaly Detection for Discrete Sequences: A Survey*" Varun Chandola, Arindam Banerjee, Member, IEEE, and Vipin Kumar, Fellow, IEEE.
[10] P. Du and S. Abe, "*IP packet size entropy-based scheme for detection of DoS/DDoS attacks,*" *IEICE Trans. Inf. Syst.*, vol. E91-D, no. 5, pp. 1274–1281, 2008.
[11] " *Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics*", Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou, Senior Member, IEEE
[12] G. Carl *et al.*, "*Denial-of-service attack-detection techniques*," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan./Feb. 2006..
[13] D. Brackney, T. Goan, A. Ott, and L. Martin, "*The Cyber Enemy within ... Countering the Threat from Malicious Insiders*," Proc. Ann. Computer Security Applications Conf. (ACSAC). pp. 346-347, 2004.

[14] Y. Chen, K. Hwang, and W.-S. Ku, "*Collaborative detection of DDoS attacks over multiple network domains*," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 12, pp. 1649–1662, Dec. 2007.
[15] "*sqlmap*", http://sqlmap.sourceforge.net/, 2011.
[16] J.A. Pereira, F. Fabret, F. Llirbat, and D. Shasha, "*Efficient Matching for Web-Based Publish/Subscribe Systems*," Proc. Int'l Conf. Cooperative Information Systems (CooplS), pp. 162-173, 2000.
[17] "*Wordpress*," http://www.wordpress.org/, 2011.
[18] "*Wordpress Bug*," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012
[19] "*Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach*." Ying Xuan Dept. of Comput. & Inf. Sci. & Eng., Univ. of Florida, Gainesville, FL, USA Incheol Shin ; Thai, M.T. ; Znati, T.
[20] "*Privacy-Preserving Updates to Anonymous and Confidential Databases* ",Alberto Trombetta, Wei Jiang, Member, IEEE, Elisa Bertino, Fellow, IEEE, and Lorenzo Bossi.
[21] " *MABS: Multicast Authentication Based on Batch Signature* ",Yun Zhou ; Xiaoyan Zhu ; Yuguang Fang Mobile Computing, IEEE Transactions on Volume: 9 , Issue: 7
[22] "*Securing Topology Maintenance Protocols for Sensor Networks*", Andrea Gabrielli, Luigi V. Mancini, Sanjeev Setia, and Sushil Jajodia, Senior Member, IEEE.

