ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

AppIDS- Defending against Multi-tier Web Application Attacks through Intrusion Detection

N. Sakthipriya[1], A.R. Arunachalam[2]

Assistant Professor, Dept. of Computer Science & Engineering, Bharath University, Chennai, Tamil Nadu, India [1,2]

ABSTRACT: The use of web applications are increasing tremendously but unfortunately it has been a valuable target for security attacks. To accommodate this increase in application and data complexity, web application adopted to multitier design. As the use of web applications has increased, the sophistication of attacks against these applications has grown as well. To protect the web application, intrusion detection system has emerged. This proposed work presents an intrusion detection system for multitier web application to detect attacks by using mapping model as well as taint inference technique, that provide a defense against both the attack occur in normal traffic and injection attacks.

KEYWORDS: web application, attacks, multitier, intrusion detection

I. INTRODUCTION

The web applications are undoubtedly becoming a dominant way to provide access to Internet services. At the same time the vulnerabilities are discovered

for exploiting and access to sensitive information. For this reason several security conscious methodologies are developed and that is able to provide early warning to the malicious activity.

Intrusion detection is the process of monitoring events occurring and reporting them accurately to proper authority when the suspicious activity occurs. There are two main types of intrusion detection methods. The one is anomaly detection which is based on finding deviations from normal user behavior are considered intrusion. The next one is misuse detection, it characterized as a' pattern' or 'signature' that IDS look for. Pattern or signature might be a static string or a set sequence of actions.

The attacks which are vulnerable to the web applications are sql injection, cross site scripting, remote code execution, Cross site request forgery, sophisticated HTTP attack, session hijacking, and buffer overflow attack ,etc.

II. RELATED WORK

Many researchers have introduced various techniques to defend against various attacks.

C. Kruegel and G. Vigna [6], presented an intrusion detection system that uses a number of different anomaly detection techniques to detect attacks against web based application. The system that connectswith the server side programs referenced by client queries with the parameter contained in the queries. The system derives spontaneously the parameter profiles associated with web application data.

M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna [1], they present Swaddler, an approach to anomaly based detection of attacks against web application. It analyzes the internal state of web application and acquires the relationship between the applications critical execution points and the application internal state. It is able to identify the attacks that attempt to bring an application in reliable anomalous state such as violation of intended workflow of web application

G. Vigna, W.K. Robertson, V. Kher, and R.A. Kemmerer [8], presented WebSTAT, an intrusion detection system that analyzes web requests looking for malicious behavior and it provides a sophisticated language to describe multistep attack in terms of states and transaction. It operates on multiple event streams and it is able to correlate both network and operating system level events with entries contained in the server logs.

M. Auxilia, D.Tamilselvan [2], proposed a negative security model based on misuse of web application is used. This model provides a web application firewall engine with a rule set, to confirm critical protection across every web architecture.WAF's are organized to establish an increase external security layer to detect and prevent attacks before they reach web application.

G. Vigna, F. Valeur, D. Balzarotti, W.K. Robertson, C. Kruegel, and E. Kirda [7], proposed the system composed of a web based anomaly detection system, a reverse HTTP proxy and a database anomaly detection system. The system serially composing a web based anomaly detector and a SQL query anomaly detector to increase the detection rate of the system. To report the system's capacity for producing false positives, they furthermore present anmethod to provide differentiated access to a website based on the anomaly score associated with web requests.

Juan Jose Garcia Adeva, Juan Manuel Pikatza Atxa [3], Intrusion detection software component based on text mining techniques attempts to detect either gaining unauthorized access or misusing a web application and by using text categorization, it is capable of learning the characteristics of both normal and malicious user behavior from log entries generated by web application server and therefore detection of misuse in web application is achieved.

Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel, Giovanni Vigna [5], proposed a novel approach to identification of class of application logic vulnerabilities, in the context of web application is presented. And this approach uses a composition of dynamic analysis and symbolic model checking to identify invariants that are a part of the intended program specification but are not enforced on all paths in the code of a web application.

Meixing Le, Angelos Starou, Bret ByungHoon Kang [9] , proposed Double Guard an IDS system that models the network behavior of user sessions across both back end database, by monitoring both web subsequent database requests, the system able to find attacks that independent IDS would not be able to identify. That quantifies the restrictions of any multitier IDS in terms of training sessions and functionality coverage.

R. Sekar [10], presented a new technique called taint inference and the technique operates by intercepting requests and responses from this application. For web applications, this interception may be accomplished using network layer interposition or library interposition. They established a class of policies called syntax and taint aware policies that can accurately detect and block most injection attacks.

Christopher Krueger, Giovanni Vigna, William Robertson [4], presented an intrusion detection system that uses a number of various anomaly detection techniques to detect attacks against web servers and web based application. The system analyzes client queries that reference server side programs and create models for a wide range of different features of queries. The system derives habitually the parameter profiles associated with the web applications and relationships between queries from analyzed data.

III. EXISTING SYSTEM

Web application has become one of the most indispensable communication channels between service providers and the users.[1] To accommodate this increase in application and data complexity, web application adopted multitier design. Web applications are normally written in scripting languages like java script, PHP embedded in HTML allowing connectivity to the databases for retrieving data. As the use of web application for critical services has increased, the sophistication of attacks against these applications has grown as well. In order to detect the existence of attacks, the intrusion detection system has been emerged. Most of the vulnerabilities result from improper input validation. So it is necessary to develop an intrusion detection model for multitier web application with proper input validation mechanism[2].

The existing Double Guard IDS system, create normality model of isolated user session that include both web front end and back end network transaction. It builds a causal mapping profile by taking both the web server and database server traffic into account. Here, all the user input values are normalized so as to build a mapping model based on the structure of HTTP request and database queries. For detection / prevention of attack such as SQL injection and cross site scripting attacks input validation is needed. But Double guard fails to validate the input. So it cannot detect the malicious or taint data hidden in the values. To overcome this limitation, a taint inference technique, syntax and taint aware policies are introduce as an additional defense for detection of this attacks.[3]

IV. PROPOSED WORK

For defending against multitier web application attacks with proper input validation, the intrusion detection system is proposed by combining both the mapping model and taint inference technique. This system provide proper input validation for detection of attack such as SQL injection , Cross site scripting etc, as well as the attack that occur even in a normal traffic. For example, if a person (attacker) with non admin privileges can log into a web server using normal user access credentials, he can find a way to issue a privileged database query by exploiting vulnerabilities in the web server.[4]

Mapping model can be created by considering the web request with the subsequent database query for an isolated session in order to detect the attack that occur in a normal traffic[5]. The taint inference technique detect the malicious or taint by observing data at the input and output side. The sensor is responsible for capturing the incoming as well as outgoing request that feeds into a syntax analyzer, which in turn feeds into the taint inference and attack detection component.[6]

The proposed AppIDS used to detect attacks such as injection attacks (SQL injection, Cross site scripting) and the attack which occur in normal traffic. Our approach uses two techniques for the detection of above attack. The first one is Causality mapping model and the second one is taint inference technique.[7]

Causality mapping model can be built by taking both the web server and database server traffic of isolated user session into account.[8]

The taint inference technique is used for input validation which includes syntax analyzer and attack detector module for detection of cross site scripting attack.

The proposed architecture which includes sensor, web server, database server, mapping model, syntax analyzer, taint inference and attack detector.[9] If the legitimate user or adversaries send a web request and it is processed by web server and made a subsequent database queries to retrieve information from the database server. In this case if any adversaries attempt any of the attack, the Intrusion detection system will monitor all the traffic and it report to the appropriate authority if the intrusion is detected. Here the IDS comprise the mapping model, syntax analyzer, taint inference and attack detector for the detection of attacks.[10]

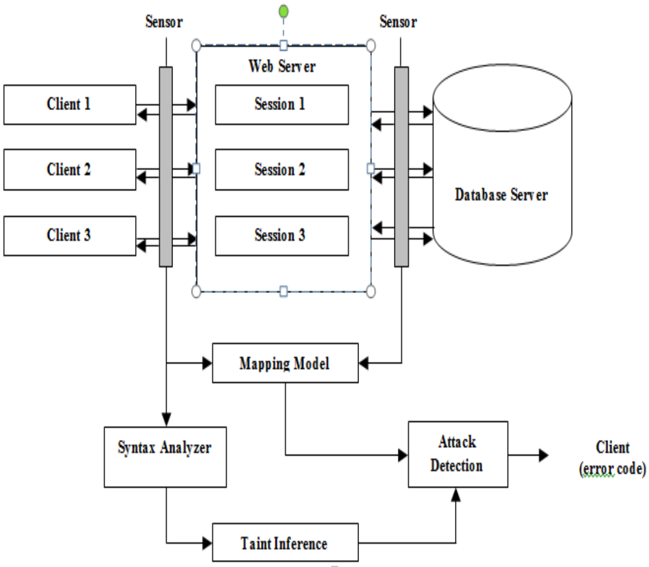


Figure 1: System Architecture

Syntax analyzer

The primary goal of syntax analyzer on the input side is to decompose the input into multiple components, perform normalization and decoding operation that are necessary on the request and parses it contents into an URI, form fields, cookies, HTTP header field etc. All this information is captured uniformly as <name, value> pairs.[11]

The output analyzer constructs an abstract syntax tree (AST), which is a data structure that is common to all output languages[12].

Taint inference

The goal of taint inference is to determine if any substring of output O contains data from I (value). They retrieve cookies and form fields from an input request and use them to construct an outgoing request.[13] Thus the value I would likely appear within the outgoing request O, possibly after some slight modification. Hence the technique infers a taint on a substring o of O if there is approximate string match between I and o , if edit distance between I and o is less than a given threshold. Then the malicious or taint is hidden in the value[14].

Attack detection

For the attack detection, syntax and taint aware policies are applied against this abstract syntax tree. If there is a policy violation, the output request is blocked by the sensor and an error code returned to the client.[15]

V. MAPPING RELATIONS

- **Deterministic mapping** – it's a perfectly matched patterns , a web request R appear in all traffic with the SQL queries set Q.
- **Empty Query Set** – SQL query set may be empty that the web request neither causes nor generates any database queries.
- **No Matched Request** – the web server may sporadically submit queries to database in order to conduct some scheduled task such as archiving or backup.
- **Nondeterministic mapping** –the same web request may result in different SQL query set based on input parameter or the status of the web page.

TAINT INFERENCE TECHNIQUE

- Web applications perform sanitization operation on their input parameters.
- Web application assembles an outgoing request from input parameter. Some part of these request are statically specified in the web application code while other parts are derived from inputs.
- Taint inference should be based on approximate string matching rather than exact string matching.[16]
- It should be based on finding substring rather than complete matches

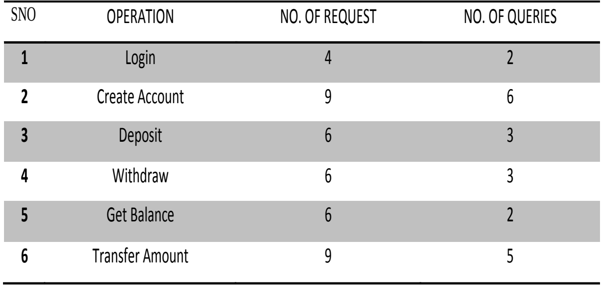
TAINT AWARE POLICIES

Attacks are detected using policies that govern the use of tainted data at an output point.[17] For building a causality model we first manually listed the operation of online banking web application

IMPLEMENTATION

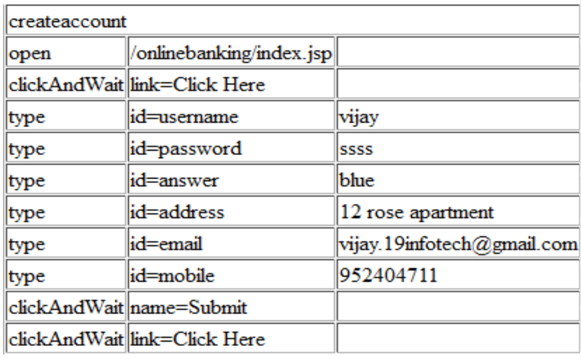
We implemented an AppIDS using a web server with a database. We also set up an online banking website for evaluation of the AppIDS. To evaluate the detection result for our system we analyzed various classes of attacks.[18]

We used Apache Tomcat as a web server, MS- Access as a database and for building a causality model we first manually listed the operation of Online Banking Web Application which are presented in the table. To build a model for each operation we used the automatic tool selenium to generate a traffic which is given below[19].

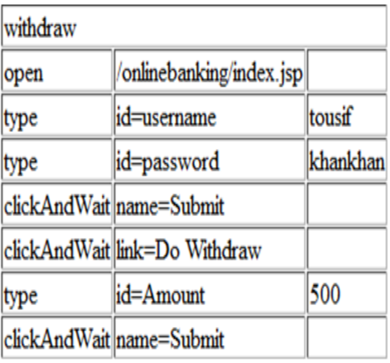


SNO	OPERATION	NO. OF REQUEST	NO. OF QUERIES
1	Login	4	2
2	Create Account	9	6
3	Deposit	6	3
4	Withdraw	6	3
5	Get Balance	6	2
6	Transfer Amount	9	5

We obtained a separate model for each operation



createaccount		
open	/onlinebanking/index.jsp	
clickAndWait	link=Click Here	
type	id=username	vijay
type	id=password	ssss
type	id=answer	blue
type	id=address	12 rose apartment
type	id=email	vijay.19infotech@gmail.com
type	id=mobile	952404711
clickAndWait	name=Submit	
clickAndWait	link=Click Here	



withdraw		
open	/onlinebanking/index.jsp	
type	id=username	tousif
type	id=password	khankhan
clickAndWait	name=Submit	
clickAndWait	link=Do Withdraw	
type	id=Amount	500
clickAndWait	name=Submit	

TAINT INFERENCE MODULE

- We implemented taint inference by using APPSENSOR IDS tool.
- Attack pattern is created for taint aware policies.

ATTACK PATTERN

SNO	ATTACK PATTERN	ATTACK
1	<script>	XSS Attack
2	"OR 1=1"	SQL Injection attack
3	Delete	SQL Injection attack
4	\"><script>	XSS Attack
5	script.*document. Cookie	XSS Attack
6	;	SQL Injection attack
7	Drop	SQL Injection attack
8	<IMG.*SRC.*=.*script	XSS Attack
9	<iframe>.*</iframe>	XSS Attack
10	Fetch	SQL Injection attack

PERFORMANCE EVALUATION

The result have shown that the proposed IDS is efficiently detected all the vulnerabilities listed in the table.[20]

SNO	OPERATION	SNORT	GSQL	DG	AppIDS
1	Privilege escalation attack	NO	NO	YES	YES
2	Sql injection attack	NO	YES	YES	YES
3	Cross Site Scripting attack	NO	NO	NO	YES
4	Webserver aimed attack	YES	NO	YES	YES
5	Direct DB	NO	NO	YES	YES
6	Linux/http/ddwrt_cgibin_exec*	NO	NO	YES	YES
7	Linux/http/linksys_apply_cgi*	NO	NO	YES	YES
8	Linux/http/piranha_passwd_exec*	NO	NO	YES	YES
9	Unix/webapp/oracle_vm_agent_utl*	NO	NO	YES	YES
10	Unix/webapp/php_include*	NO	NO	YES	YES
11	Unix/webapp/php_wordpress_lastpost*	NO	NO	YES	YES
12	Windows/http/altn_webadmin*	NO	NO	YES	YES
13	Windows/http/apache_modjk_overflow*	NO	NO	YES	YES
14	Windows/http/oracle9i_xdb_pass*	NO	NO	YES	YES
15	Windows/http/maxdb_webdbm_database*	NO	NO	YES	YES

AppIDS can detect the cross site scripting attack and SQL injection attack by using the taint inference technique

VI. CONCLUSION

In this proposed model a Mapping model is created in order to detect the attack occur in a normal traffic and Taint inference technique is used for input validation mechanism for detection injection attacks(SQL injection and Cross Site Scripting).We have shown that the AppIDS can detect the wide range of attacks. Future work is to develop an efficient IDSfor detecting buffer overflow and DDOS attacks.

REFERENCES

[1] M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna, “Swaddler: An Approach for the Anomaly-Based Detection of State Violations in Web Applications,” Proc. Int’l Symp. Recent Advances in Intrusion Detection (RAID ’07), 2007.
[2] Vijayaragavan S.P., Karthik B., Kiran T.V.U., Sundar Raj M., "Robotic surveillance for patient care in hospitals", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 16(12) (2013) pp. 1820-1824
[3] M. Auxilia, D.Tamilselvan, “ Anomaly Detection Using Negative Security Model in Web Application,”IEEE 2010.
[4] Juan Jose Garcia Adeva, Juan Manuel Pikatza Atxa,” Intrusion Detection in web applications using text mining,” Journal of Artificial Intelligence - Elsevier 2006.
[5] Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., Sundar Raj, M."Analysis of chaotic DC-DC converter using wavelet transform", Middle - East Journal of Scientific Research, ISSN : B27, 16(12) (2013) pp.1813-1819.
[6] Christopher Kruegel, Giovanni Vigna, William Robertson,” A multi model approach to the detection of web based attacks”, Journal of Computer Networks - Elsevier 2005.
[7] Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel, Giovanni Vigna,”Towards Automated detection of logic vulnerabilities in web applications “,USENIX Security'10 Proceedings of the 19th USENIX conference on Security, 2010
[8] C. Kruegel and G. Vigna, “Anomaly Detection of Web-Based Attacks,” Proc. 10th ACM Conf. Computer and Comm. Security (CCs’03), Oct. 2003.
[9] Vijayaraghavan K., Nalini S.P.K., Prakash N.U., Madhankumar D.,"Biomimetic synthesis of silver nanoparticles by aqueous extract of Syzygium aromaticum", Materials Letters, ISSN : 0167-577X, 75() (2012) pp. 33-35.
[10] G. Vigna, F. Valeur, D. Balzarotti,W.K. Robertson, C. Kruegel, and E. Kirda, “Reducing Errors in the Anomaly-Based Detection of Web-Based Attacks through the Combined Analysis of Web Requests and SQL Queries,” J. Computer Security, vol. 17, no. 3, pp. 305-329, 2009.
[11] 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.
[12] Meixing Le, Angelos Starou, Bret ByungHoon Kang,” DoubleGuard: Detcting Intrusions in Multitier Web Applications,” IEEE Transactions On Dependable and Secure Computing, Vol. 9, NO. 4, July/August 2012.
[13] Vijayaraghavan, K., Nalini, S.P.K., Prakash, N.U., Madhankumar, D., "One step green synthesis of silver nano/microparticles using extracts of Trachyspermum ammi and Papaver somniferum", Colloids and Surfaces B: Biointerfaces, ISSN : 0927-7765, 94() (2012) pp. 114-117.
[14] R. Sekar,” An Efficient Black box Technique for Defeating Web Application Attacks”, Proc. Network and Distributed system security sump.(NDSS),2009.
[15] Kulanthaivel L., Srinivasan P., Shanmugam V., Periyasamy B.M., "Therapeutic efficacy of kaempferol against AFB1 induced experimental hepatocarcinogenesis with reference to lipid peroxidation, antioxidants and biotransformation enzymes", Biomedicine and Preventive Nutrition, ISSN : 2210-5239, 2(4) (2012) pp.252-259.
[16] N.Sakthipriya, K.Palanivel , “ Intrusion Detection for web application : An Analysis” , International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013
[17].Dr.A.Muthu Kumaravel, KNOWLEDGE BASED WEB SERVICE, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 5881-5888, Vol. 2, Issue 9, September 2014
[18].Dr.A.Muthu Kumaravel, Data Representation in web portals, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 5693-5699, Vol. 2, Issue 9, September 2014
[19].Dr.Kathir.Viswalingam, Mr.G.Ayyappan,A Victimization Optical Back Propagation Technique in Content Based Mostly Spam Filtering ,International Journal of Innovative Research in Computerand Communication Engineering ,ISSN(Online): 2320-9801 , pp 7279-7283, Vol. 2, Issue 12, December 2014
[20].KannanSubramanian,FACE ECOGNITION USINGEIGENFACE AND SUPPORT ECTORMACHINE,International Journal of Innovative Research in Computerand Communication Engineering,ISSN(Online): 2320-9801,pp 4974-4980, Vol. 2, Issue 7, July 2014.
[21].Vinothlakshmi.S,To Provide Security & Integrity for StorageServices in Cloud Computing ,International Journal of Innovative Research in Computer and Communication Engineering ,ISSN(Online): 2320-9801 , pp 2381-2385 ,Volume 1, Issue 10, December 2013
[22]http://www.ossec.net/
[23]http://www.snort.org/
[24] http://sguil.sourceforge.net/
[25]http://www.tripwire.com/